Державний торговельно-економічний університет
Кафедра інженерії програмного забезпечення
та кібербезпеки

ПРОГРАМУВАННЯ ТА ЗАХИСТ ІНФОРМАЦІЇ

Збірник наукових статей студентів,
які здобувають освітній ступінь «магістр»
за спеціальностями
«Інженерія програмного забезпечення»,
«Кібербезпека та захист інформації»

Частина 2

Київ 2023

УДК 004.056.5
П 78

Програмування та захист інформації [Електронний ресурс] : П 78 у 3 ч. Ч. 2 : зб. наук. ст. студентів / відп. ред. Т. О. Жирова. – Київ : Держ. торг.-екон. ун-т, 2023. – 227 с.

У збірнику наукових статей студентів висвітлено результати теоретичних та експериментальних досліджень угалузі інженерії програмного забезпечення й кібербезпеки та захисту інформації.

Матеріали подано в авторській редакції. Відповідальність за зміст статей несуть автори.

УДК 004.056.5

Відповідальна за випуск О. В. Криворучко, д-р техн. наук, проф.

Видається за рекомендацією вченої ради факультету інформаційних технологій ДТЕУ
(протокол № 12 від 28.06.2023)

ЗМІСТ

ВСТУП

На глобальному рівні відбуваються значні трансформації в сфері обробки та захисту інформації, викликані інтенсивним зростанням і впровадженням інформаційних технологій.Інформаційні технології, що ґрунтуються на комп'ютерних рішеннях, мають значний вплив на усі галузі життя та вимагають радикальних змін організаційних структур управління, його регламенту, кадрового потенціалу, системи документації, фіксування та передачі інформації.

Важливість інформаційних технологій створює нові виклики,пов'язані з кібербезпекою та захистом інформації. Оскільки інформаційні технології стають не просто складовою частиною, але й активним каталізатором розвитку інформаційного суспільства, з'являється необхідність у забезпеченні надійності та безпеки цих технологій та відповідної інформації.

Нині одним з пріоритетних завданьє вивчення інформаційних процесів, що відбуваються в економіці, та ефективного управління ними в умовах інформаційного суспільства. При цьому неможливо обійти увагою аспекти кібербезпеки, які є необхідними длясучасного цифрового світу, де дані та системи стають вразливими перед кіберзагрозами.

На сьогодні актуальними є завдання розширення області інформаційної науки, зокрема зосередження на розвитку сучасних технологій програмування. Не менш вагомим є дослідження інформаційних процесів в економіці та розробка ефективних методів їх управління в умовах інформаційного суспільства. Слід зауважити, що кіберзагрози стають все більш поширеним явищем.Саме тому дедалі більше уваги приділяється підготовці фахівців у галузі кібербезпеки та захисту інформації, які мають бути компетентними у вирішенні практичних завдань, пов'язаних з розробкою, забезпеченням якості впровадження та супроводження програмних засобів, а також вміти знаходити раціональні методи та засоби їх вирішення, включаючи складні ситуації. Крім того, вони відіграють важливу роль у підтримці сталого розвитку ІТ-компаній щодо якості процесів і результатів розробки програмного забезпечення.

Програма магістерської підготовки студентів спеціальностей«Інженерія програмного забезпечення»,«Кібербезпека та захист інформації»орієнтовані на формування у майбутніх фахівців відповідних компетентностей для роботи в галузі наукомістких технологій, педагогічної, науково-дослідної роботи стосовно вирішення актуальних прикладних, виробничих і народногосподарських завдань.

Збірникнаукових статей студентів, які здобувають освітній ступінь «магістр»за спеціальностями «Інженерія програмного забезпечення», «Кібербезпека та захист інформації», містить матеріали досліджень, отриманих під час виконання їхніх випускних кваліфікаційних робіт.

РОЛЬ МАШИННОГО НАВЧАННЯ В УДОСКОНАЛЕННІ МОДУЛІВ HR

КОРОБКО О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Дане дослідження спрямоване на визначення ролі системи управління людськими ресурсами на основі машинного навчання в HR системах на основі світових наукових джерел. Технологія забезпечує унікальний спосіб введення, опрацювання та виведення даних, що, дає змогу підвищувати показники продуктивності фахівців у напрямку HR. Однак обсяг даних, що генеруються цими системами, ускладнює їхній аналіз та інтерпретацію сприйняття людиною. Машинне навчання стало потужним інструментом для обробки значних об'ємів вхідної інформації.

This study is aimed at determining the role of machine learning-based human resource management systems in HR systems based on global scientific sources. The technology provides a unique way to input, process and output data, which allows to increase the productivity of HR professionals. However, the volume of data generated by these systems makes it difficult to analyze and interpret it in a human way. Machine learning has become a powerful tool for processing large amounts of input.

Актуальність. З появою технологій управління людськими ресурсами зазнало революції, а машинне навчання стало невід'ємним компонентом HR. Алгоритми машинного навчання можуть автоматизувати різні HR-функції, включаючи рекрутинг, утримання співробітників, управління ефективністю та управління талантами. Тому важливо розуміти роль машинного навчання в удосконаленні HR-модулів.

Метою статті є вивчення ролі машинного навчання в удосконаленні модулів управління персоналом, а також визначення переваг і викликів впровадження машинного навчання в HR.

Завдання статті є аналіз алгоритмів машинного навчання, що використовуються в HR, та оцінити їхню ефективність у вдосконаленні HR-модулів.

Об'єктом дослідження є HR-модулі, які можна вдосконалити за допомогою алгоритмів машинного навчання.

Виклад основного матеріалу. Організації а тим паче в технологічних галузях завжди прагнуть наймати співробітників, які більш підковані в цифрових технологіях. В умовах конкурентного ринку вкрай важливо, щоб потенціал кандидата було використано по максимуму для кращого організаційного успіху. Саме тому кожен фахівець у сфері управління людськими ресурсами має на меті оптимізувати обробку потоку даних і скоротити час без шкоди для якості прийняття рішень. У таких умовах людські ресурси залишаються одним з основних відмінних факторів для організації, які можуть бути використані для конкурентного зростання для створення необхідної організаційної цінності. Кінцевою метою інтеграції машинного навчання в управління людськими ресурсами є забезпечення того, щоб людські ресурси організації були активом, а оптимальне використання людського капіталу – безперервним процесом. Тому організації повинні постійно докладати зусиль для вдосконалення своїх систем на основі машинного навчання, щоб йти в ногу з постійно мінливим технологічним ландшафтом і залишатися конкурентоспроможними на ринку.

Управління людськими ресурсами – це галузь знань, орієнтована на впровадження практик і підходів для досягнення організаційних цілей, а інтеграція машинного навчання може дозволити їм приймати рішення на основі даних і відбирати кандидатів з необхідними

навичками, щоб досягти успіху в сучасній технологічній індустрії. Кожен фахівець цієї галузі має основними цілями: оптимізувати опрацювання потоку даних і зниження часу без втрати якості ухвалення рішення. Для досягнення цих цілей, системи на основі машинного навчання повинні охоплювати безліч усталених стратегій і практик, які довели свою ефективність, а також створення нових, характерних для даного контексту, аналітика вхідної та вихідної інформації. Однак, для того щоб управління людськими ресурсами було ефективним, зміни та нововведення приносили позитивні результати або матимуть вигідні наслідки, система має бути орієнтована на більш глибший аналіз введених змінних, які будуть оброблятися за допомогою принципів обробки даних на основі нейронних зв'язків (машинного навчання). Щоб подолати проблеми, пов'язані з оцінкою аналізу, який виконує система, і поліпшити масштабованість систем, заснованих на машинному навчанні, в управлінні людськими ресурсами, організації можуть дослідити передові методи, такі як глибоке навчання, обробка природної мови і комп'ютерний зір. Ці методи дозволяють створювати більш складні моделі, які можуть навчатися на великих обсягах даних і видавати більш точні результати.

Для визначення доцільності використання принципів машинного навчання в HR-системах необхідно провести зіставлення основних принципів машинного навчання з одним із його підвидів, а саме - глибинне навчання (Deep Learning). Таке порівняння має місце через відмінності в способі обробки даних. Варто підкреслити важливість і цінність систем, які надають аналіз або можливість аналізу методів, на яких ґрунтується система під час ухвалення рішення. Оскільки будь-яка система з принципами машинного навчання, незалежно від алгоритмів, на яких вона була побудована, почати аналізувати ввідні дані за структурою, до якої ці дані не призначені або не піддаються аналізу за такими структурами.

Глибинне навчання адаптує багаторівневий підхід до прихованих пластів нейронної мережі. У традиційних підходах до машинного навчання функції визначають і витягують або вручну, або з використанням методів вибору функцій. Однак у цих моделях функції вивчаються і витягуються автоматично, що забезпечує більш високу точність і продуктивність. Як правило, гіперпараметри моделей класифікаторів також вимірюються автоматично. Потрібно враховувати відмінності в класифікації полярності між двома підходами: традиційним машинним навчанням (машина опорних векторів, байєсівські мережі або дерева рішень) і глибоким навчанням (Рис. 1). Так само глибинне навчання має багаторівневий нейронний кластерний зв'язок із прихованими пластами, подібний до нейронів людського мозку. Окрім того це цілісна структура, зібрати аналітику з прихованих пластів, тобто принципи, за якими була дана відповідна відповідь, важко або без відповідного ПЗ неможливо (рис. 2) [1]. Важко дізнатися, який нейронний вузол був активний і як вузли поводилися для видачі певного результату. Так як для HR систем з машинним навчанням, визначення причин є основним фактором під час вибору таких систем. Важливо вказати і той момент, що глибинне навчання розкриває свій потенціал на великих об'ємах даних, що, своєю чергою, вимагає значних обчислювальних можливостей, але точність обчислення при цьому підвищується [2].

Робота з даними відбувається за принципом «що більше даних, то точніший результат», тобто обчислювальні можливості зростають, на рівні з цим зростають і витрати ресурсів системою на обробку даних. Адміністрування та фінансові витрати вищі, ніж на подібні системи на інших алгоритмах машинного навчання [3].

Виходячи з відмінностей у принципах роботи алгоритмів машинного навчання та окремо глибинного навчання, є відмінності в побудові блоків обробки даних та інша структура аналізу даних (рис. 1). Після попереднього опрацювання даних, вхідний пласт передає попередньо відсортовану інформацію в приховані пласти, в них же алгоритм ухвалює певне рішення і дає результат. І як зазначалося раніше, важко або немає можливості дати оцінку аналізу, який було проведено системою. Інші алгоритми менш затратні з точки зору технічних вимог, але в той же час на великих обсягах даних кожен наступний обсяг дає менший приріст обчислювальних можливостей програмного забезпечення. Крім того,

необхідно знайти компроміс між складністю моделі та можливістю інтерпретації результатів. Хоча складні моделі можуть пропонувати кращу точність, їх часто складніше інтерпретувати, що може бути проблемою в таких контекстах, як управління людськими ресурсами, де рішення можуть мати значний вплив на життя людей.

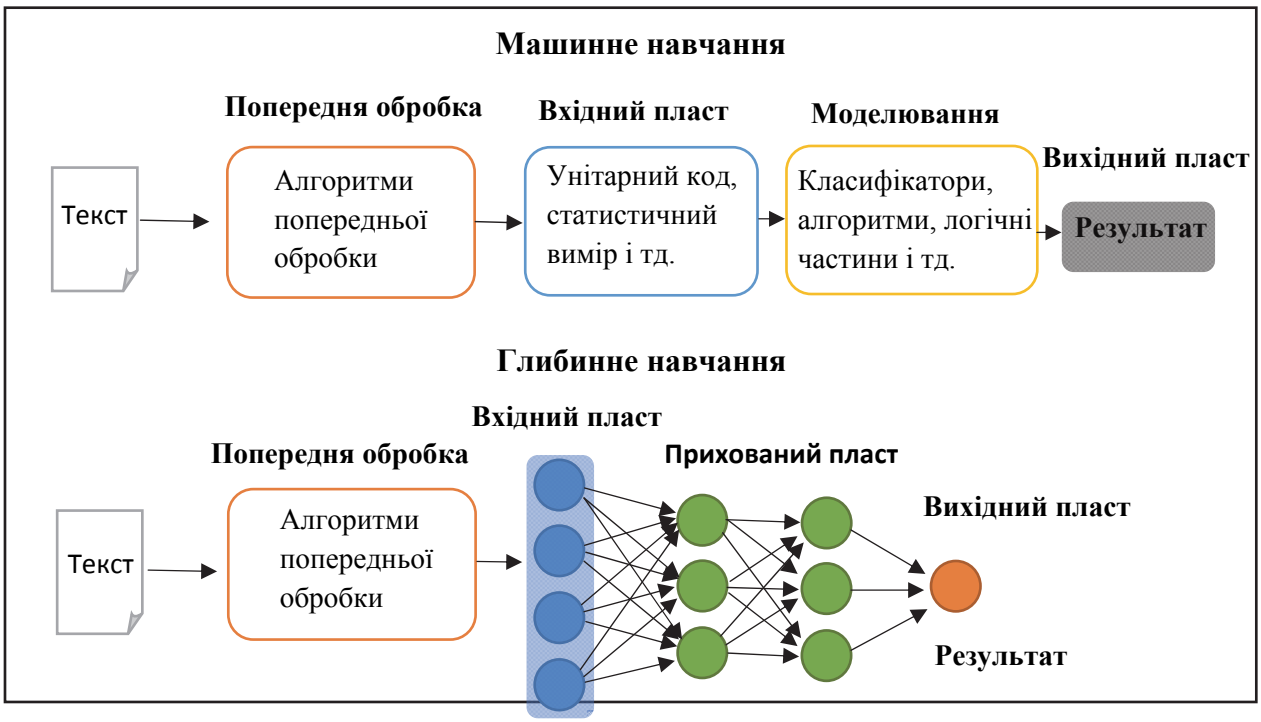


Рис. 1. Відмінності між двома підходами до класифікації полярності, машинного навчання (вгорі) і глибокого навчання (внизу)

Джерело: адаптовано автором з [4]

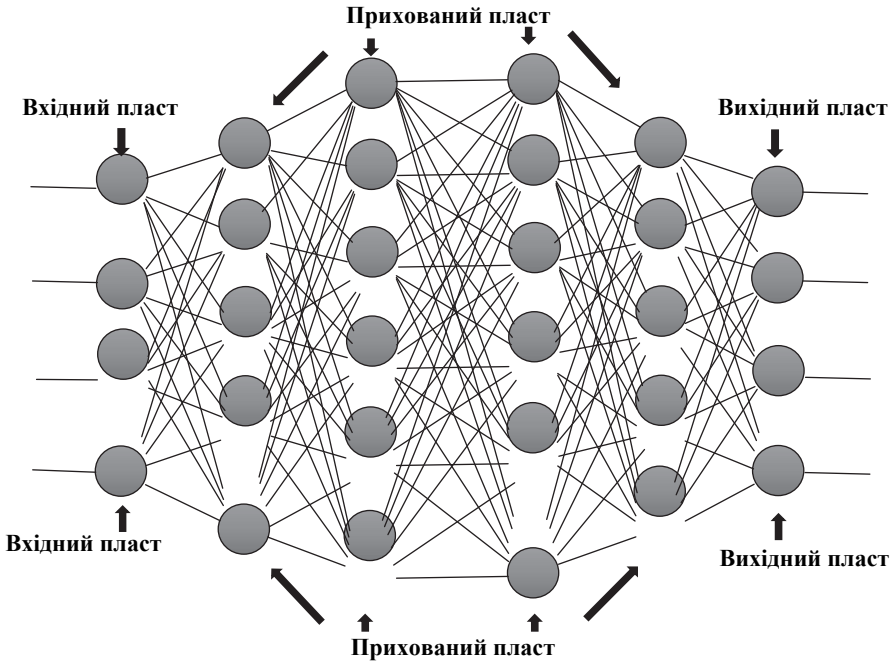


Рис. 2. Типи групування нейронних вузлів у глибинному навчанні

Джерело: Зроблено автором

Викладені вище дані дають розуміння в доцільності розглядати системи, які побудовані на принципах обох алгоритмів. Доповнювати систему, нівелювати недоліки різних алгоритмів машинного навчання для досягнення максимальної продуктивності системи. В свою чергу ці кроки дають можливість програмного аналізу даних, на яких ґрунтувалася система під час видачі результату, що є ключовим фактором під час вибору/створення таких систем.

Аналітика даних систем є важливим аспектом для досягнення результату і вносить у широку сферу HR певні технічні обмеження, як-от адміністрування та підтримка працездатності [5]. Дана аналітика дає можливість фахівцям HR реалізувати завдання поставленими керівництвом, а також залишає простір для зростання в цій галузі та вивчення актуальності аналітики в різних категоріях, що підпадають під категорії управління людськими ресурсами [6]. Що дає приріст у продуктивності даних фахівців. У системах на основі машинного навчання коректність даних і результати опрацювань, які можна витягти з них, мають значний вплив на продуктивність моделей і здатність до навчання. Як наслідок, перед подачею даних на вхід необхідно їх підготувати.

Роль рішень машинного навчання, що обробляють вхідні запити з управління ресурсами необхідні. Адже більшість організацій вже використовують штучний інтелект і різні системи в HR на основі машинного навчання, як-от чат-боти, системи які використовують машинне навчання й автоматизація роботизованих процесів в управлінні людськими ресурсами, що допомагають у рекрутингу, скринінгу, адаптації, інтерв'юванні тощо.

Оскільки використання машинного навчання в управлінні персоналом продовжує зростати, організаціям важливо розуміти потенційні переваги та обмеження цих систем. Однією з головних переваг є можливість спростити й автоматизувати багато HR-процесів, звільнивши час і ресурси для більш стратегічних ініціатив. Наприклад, чат-боти та автоматизовані системи скринінгу можуть швидко та ефективно обробляти первинну комунікацію та оцінку кандидатів, дозволяючи HR-фахівцям зосередитися на більш складних завданнях, таких як співбесіди та адаптація.

Ще однією перевагою HR-систем на основі машинного навчання є їхня здатність аналізувати великі обсяги даних для виявлення закономірностей і тенденцій, які можуть бути не одразу очевидними для аналітиків, що працюють з людьми. Це може бути особливо корисно в таких сферах, як залучення та утримання працівників, де відіграють роль такі складні фактори, як задоволеність роботою, баланс між роботою та особистим життям і компенсація. Аналізуючи дані опитувань працівників, оцінок ефективності роботи та інших джерел, алгоритми машинного навчання можуть допомогти організаціям визначити потенційні сфери для вдосконалення та розробити цільові стратегії для їх вирішення.

HR-системи на основі машинного навчання також можуть допомогти спростити багато адміністративних завдань, пов'язаних з управлінням персоналом, таких як перевірка резюме та складання шорт-листа кандидатів. Чат-боти та інші інструменти на основі машинного навчання можуть обробляти багато рутинних запитів і звернень, які відділ кадрів отримує щодня, звільняючи працівників відділу кадрів для виконання більш складних завдань. Однак важливо зазначити, що системи машинного навчання не є панацеєю від усіх проблем у сфері управління персоналом. Вони ефективні лише настільки, наскільки ефективні дані, на яких вони навчаються, а упередженість навчальних даних може призвести до упередженого прийняття рішень. Важливо також забезпечити прозорість і зрозумілість HR-систем на основі машинного навчання, щоб фахівці з управління персоналом і працівники могли розуміти, як приймаються рішення.

Крім того, машинне навчання можна використовувати для підвищення точності та ефективності програм навчання працівників. Аналізуючи дані про ефективність роботи співробітників і виявляючи слабкі місця, алгоритми машинного навчання можуть рекомендувати індивідуальні навчальні програми, спеціально розроблені для усунення наявних та майбутніх недоліків.

Загалом, використання машинного навчання в управлінні персоналом має потенціал докорінно змінити те, як організації управляють своїми людськими ресурсами. Однак організаціям важливо підходити до цих систем з обережністю і переконатися, що вони впроваджуються таким чином, щоб максимізувати їхні потенційні переваги, мінімізуючи ризики та обмеження. Таким чином, організації можуть гарантувати, що вони використовують новітні технології для підтримки своїх співробітників і досягнення успіху в бізнесі.

Машинне навчання виявляється надзвичайно важливим інструментом в удосконаленні модулів управління ресурсами людських відносин (HR). Аналіз результатів дослідження підтверджує, що машинне навчання може суттєво покращити робочі процеси, оптимізувати прийняття рішень та сприяти більш ефективному управлінню персоналом.

Однією з ключових ролей машинного навчання є здатність до аналізу великих обсягів даних. Модулі HR зазвичай включають велику кількість інформації про співробітників, вакансії, навчання та інші аспекти. Машинне навчання дозволяє автоматизувати процес обробки цих даних, виявляти в них корисні зв'язки та патерни, що забезпечує більш точне та швидке прийняття рішень.

Додатково, машинне навчання може використовуватися для прогнозування тенденцій на ринку праці та внутрішніх змін в компанії. Це дозволяє модулям HR бути готовими до майбутніх викликів та забезпечувати збалансовану робочу силу.

Висновки. Останнім часом спостерігається тенденція до впровадження в різних галузях систем на основі машинного навчання. Одним з головних чинників, що зумовлюють тенденцію впровадження цих систем в різних галузях, є потреба в постійному вдосконаленні. Компанії постійно прагнуть оптимізувати свої процеси, зменшити витрати та підвищити ефективність, і машинне навчання стало потужним інструментом для досягнення цих цілей. Штучний інтелект і машинне навчання використовуються багатьма компаніями у відділах кадрів, де такі системи виконують допоміжну, а інколи й основну роль у наборі персоналу, аналізу продуктивності, збиранню даних, надання інформації в режимі реального часу та наданні точної інформації. В результаті вони можуть надавати цінну інформацію, яка допоможе організаціям приймати обґрунтовані рішення та вдосконалювати HR-процеси в цілому. Впроваджуючи алгоритми машинного та глибокого навчання в HR-системи, організації можуть отримати конкурентну перевагу та краще управляти своїми людськими ресурсами. Ці технології дозволяють організаціям оптимізувати свої процеси, зменшити витрати, підвищити ефективність та приймати рішення на основі даних. Загалом, машинне навчання є потужним інструментом, який має потенціал для трансформації систем управління персоналом та вдосконалення способів управління найціннішим активом організацій - їхніми спеціалістами.

Список використаних джерел

1. Aggarwal C. «Neural Networks and Deep Learning». 2018. 20-43p. ISBN: 978-3-319-94463-0
2. Sukwoong Choi, Namil Kim, Junsik Kim, Hyo Kang. How Does AI Improve Human Decision Making. 2020. 4-6; dx.doi.org/10.2139/ssrn.3893835
3. Neural Networks and Deep Learning. Електронний ресурс. URL: http://neuralnetworksanddeeplearning.com/ (дата звернення 10.04.2023).
4. Gattan M. Deep Learning Technique of Sentiment Analysis for Twitter Database. dx.doi.org/10.3991/ijim.v16i01.27575
5. Abdulquddus Mohammed. HR ANALYTICS: A MODERN TOOL IN HR FOR PREDICTIVE DECISION MAKING. 2019. 52-58; dx.doi.org/10.34218/JOM.6.3.2019.007
6. Gloria Phillips-Wren. Artificial Intelligence for Decision Making. 2006. 2 -10.

Робота виконана під науковим керівництвом PhD, доцента
ДЕСЯТКО А. М.

ІНЖЕНЕРІЯ СОЦІАЛЬНИХ АТАК ЯК ЗАГРОЗА ФІЗИЧНОМУ ЗАХИСТУ ІНФОРМАЦІЇ

КОРОТИЧ І., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

Стаття,висвітлює тему інженерії соціальних атак як загрози фізичному захисту інформації. Інженерія соціальних атак – це процес маніпулювання людьми з метою отримання доступу до конфіденційної інформації або здійснення іншої злочинної діяльності.

Також стаття розглядає, як такі атаки можуть стати загрозою для фізичного захисту інформації, що означає захист інформації від фізичних загроз, таких як крадіжка комп'ютера або USB-накопичувача, підміна чи крадіжка пристроїв зберігання даних тощо.

The article covers the topic of social attack engineering as a threat to the physical protection of information. Social attack engineering is the process of manipulating people to gain access to confidential information or to carry out other criminal activities.

The article also examines how such attacks can pose a threat to physical information security, which means protecting information from physical threats such as theft of a computer or USB drive, substitution or theft of storage devices, etc.

Актуальність. Тема актуальна оскільки загроза атак соціальної інженерії на фізичну інформаційну безпеку є дуже актуальною і нагальною проблемою в сучасну цифрову епоху. Зі зростанням залежності від технологій та збільшенням обсягів конфіденційної інформації, що зберігається в цифровому вигляді, потенційні наслідки успішної атаки можуть бути руйнівними. Атаки соціальної інженерії стають все більш витонченими і їх все важче виявляти, тому організаціям необхідно вживати проактивних заходів для захисту своєї фізичної інформаційної безпеки.

За останні роки відбулося багато гучних атак соціальної інженерії на фізичну інформаційну безпеку, включаючи інциденти, спрямовані на державні установи, фінансові установи та медичні заклади. Ці атаки призвели до значних фінансових втрат, репутаційних збитків і навіть загрози національній безпеці.

Крім того, пандемія COVID-19 створила нові можливості для атак соціальної інженерії, оскільки віддалена робота та онлайн-спілкування полегшують зловмисникам використання вразливостей. Як наслідок, організаціям необхідно зберігати пильність і вживати проактивних заходів для навчання своїх співробітників та впровадження надійних заходів фізичної безпеки.

Дослідити загрозу атак соціальної інженерії для фізичної інформаційної безпеки та підкреслити важливість вжиття проактивних заходів для захисту від таких атак. Стаття має на меті надати всебічний огляд цього питання, включаючи різні форми атак соціальної інженерії, потенційні наслідки успішної атаки та способи, якими організації можуть захистити себе.

Стаття також має на меті підвищити обізнаність про важливість фізичного захисту інформації та надати рекомендації щодо найкращих практик, яких можуть дотримуватися організації, щоб зменшити ризик атак соціальної інженерії. Висвітлюючи останні тенденції та розробки в цій галузі, стаття має на меті озброїти читачів знаннями та інструментами, необхідними для захисту від атак соціальної інженерії та захисту їхньої конфіденційної інформації.

Інженерія соціальних атак полягає в тому, щоб використовувати соціальні і психологічні методи впливу на людей з метою зламування захисту інформації або отримання несанкціонованого доступу до системи. Такі атаки можуть бути надзвичайно ефективними, оскільки вони використовують людську довіру і схильність до певних видів поведінки.

Фізичний захист інформації включає в себе захист комп'ютерних систем та інших пристроїв, які зберігають, обробляють і передають конфіденційну інформацію. Однак, якщо людина стає слабким ланцюгом у цій системі захисту, то її поведінка може стати вразливою для соціальних атак.

Метою статті є інформування та навчання читачів про загрозу атак соціальної інженерії для фізичної інформаційної безпеки, а також заохочення організацій вживати проактивних заходів для захисту від цієї зростаючої загрози.

Об'єктом дослідження є інженерія соціальних атак.

Предметом дослідження є система захисту персональних даних від соціальних атак.

У сучасну цифрову епоху захист конфіденційної інформації має першорядне значення. Компанії та організації інвестують значні кошти у захист своїх даних від кібератак, але фізична безпека часто залишається поза увагою. Однією з найбільших загроз для фізичної безпеки інформації є атаки соціальної інженерії. Ці атаки використовують психологічні маніпуляції, щоб змусити людей розкрити конфіденційну інформацію або отримати несанкціонований доступ до захищених місць або систем. У цій статті ми розглянемо різні типи атак соціальної інженерії та їхній вплив на фізичну інформаційну безпеку, даний вплив на систему можемо помітити на рис. 1.

Рис. 1. Загрози які існують для безпеки

Соціальна інженерія - це форма психологічної маніпуляції, яка полягає у впливі на людей з метою змусити їх розголошувати конфіденційну інформацію, приймати рішення або вчиняти дії, яких вони зазвичай не роблять. Мистецтво соціальної інженерії передбачає використання таких методів, як переконання, обман і видавання себе за іншу особу, щоб завоювати довіру цільової аудиторії. Це метод, який використовують хакери, шахраї та аферисти, щоб обманом змусити людей розкрити конфіденційну інформацію, таку як паролі, номери кредитних карток та персональні дані [1].

Соціальна інженерія – це складна і багатогранна галузь, яка охоплює широкий спектр тактик і методів. Деякі з найпоширеніших методів включають фішинг, привід, приманку та послугу за послугу. Фішинг – це метод, який полягає у надсиланні шахрайських електронних листів або повідомлень, які виглядають як такі, що надходять з надійного джерела, наприклад, банку або соціальної мережі, з метою виманити у жертви конфіденційну інформацію. Створення фальшивого приводу або сценарію, щоб обманом змусити жертву розкрити інформацію або виконати певну дію. Приманка передбачає пропозицію винагороди або заохочення об'єкту, щоб переконати його виконати певну дію або розкрити інформацію. Послуга за послугу передбачає пропозицію вигоди в обмін на інформацію або дію. [2]

Соціальна інженерія – це потужний інструмент, який можна використовувати як для добрих, так і для поганих цілей. В умілих руках вона може бути використана для підвищення безпеки та захисту конфіденційної інформації. Наприклад, соціальну інженерію можна використовувати для перевірки безпеки системи, намагаючись отримати несанкціонований доступ за допомогою тактики соціальної інженерії. Це може допомогти виявити вразливі місця в системі та внести необхідні покращення.

Однак соціальну інженерію часто використовують у недобрих цілях. Хакери та кіберзлочинці часто використовують тактику соціальної інженерії, щоб отримати доступ до конфіденційної інформації, такої як реквізити банківських рахунків, персональні дані та облікові дані для входу в систему. Вони також можуть використовувати тактику соціальної інженерії для поширення шкідливих програм та іншого шкідливого програмного забезпечення. Атаки соціальної інженерії можуть бути дуже ефективними, оскільки вони використовують людський фактор безпеки, який часто є найслабшою ланкою в будь-якій системі безпеки.[5]

Щоб протистояти атакам соціальної інженерії, важливо бути обізнаним з різними тактиками і методами, які використовують соціальні інженери. Організації можуть впроваджувати навчальні програми з підвищення обізнаності про безпеку, щоб розповісти працівникам про небезпеку соціальної інженерії, а також про те, як розпізнавати атаки соціальної інженерії та реагувати на них. Вони також можуть впровадити технічні засоби контролю, такі як брандмауери, системи виявлення вторгнень та антивірусне програмне забезпечення, щоб запобігти успішним атакам соціальної інженерії.

На рис. 2 зображені типи атак соціальної інженерії.

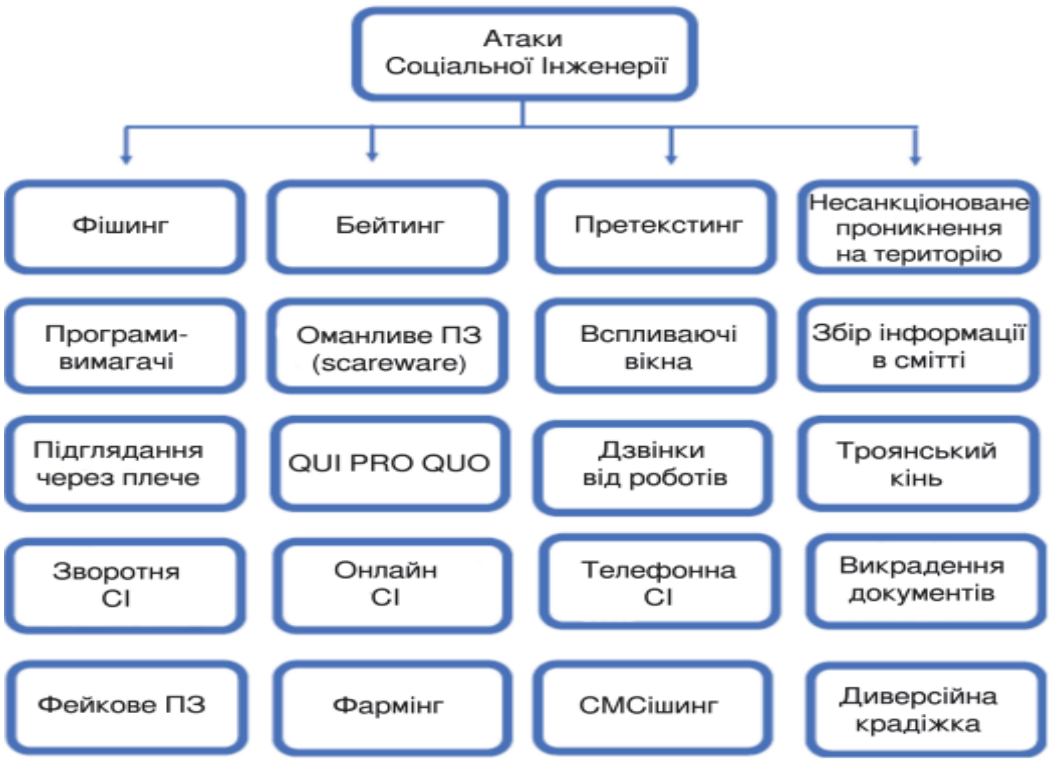


Рис. 2. Типи атак соціальної інженерії

Типи атак соціальної інженерії:

Фішинг: Фішингові атаки передбачають надсилання електронних листів або повідомлень, які виглядають як такі, що походять з легітимного джерела, але насправді походять від зловмисника. Мета цих атак – обманом змусити одержувача надати конфіденційну інформацію, наприклад, облікові дані для входу в систему або фінансову

інформацію. Фішингові атаки можуть бути особливо небезпечними, коли вони націлені на співробітників, які мають доступ до конфіденційної інформації[3].

Приховані атаки: Прихована атака передбачає створення фальшивого приводу або сценарію, щоб завоювати довіру жертви. Зловмисник може видавати себе за представника влади, наприклад, поліцейського або IT-спеціаліста, щоб переконати жертву розкрити конфіденційну інформацію або надати доступ до захищених зон.

Заманювання: Атаки з використанням приманки передбачають пропозицію чогось привабливого, наприклад, безкоштовного USB-накопичувача, в обмін на конфіденційну інформацію або доступ до захищених систем. Ці атаки часто націлені на працівників, які менш уважно ставляться до безпеки.

Quid Pro Quo: Атаки типу «послуга за послугу» передбачають пропозицію вигоди в обмін на конфіденційну інформацію або доступ до захищених систем. Наприклад, зловмисник може запропонувати подарункову картку в обмін на облікові дані для входу в систему[3].

Тейлгейтинг: Переслідування передбачає проходження за уповноваженою особою в безпечну зону без дозволу. Зловмисник може прикинутися загубленим або поспішаючим, щоб отримати доступ до захищеної зони.

Вплив на фізичну інформаційну безпеку:

Атаки соціальної інженерії можуть мати серйозні наслідки для фізичної інформаційної безпеки. Якщо зловмисник отримує доступ до конфіденційної інформації або захищених систем, він може завдати значної шкоди. Наприклад, зловмисник може викрасти конфіденційну інформацію або встановити шкідливе програмне забезпечення на захищену систему. Атаки соціальної інженерії також можуть скомпрометувати заходи фізичної безпеки, такі як системи контролю доступу, обманом змушуючи співробітників надавати несанкціонований доступ до захищених зон.

Атаки соціальної інженерії становлять значну загрозу фізичній інформаційній безпеці. Компанії та організації повинні вжити заходів для навчання співробітників про різні типи атак соціальної інженерії, а також про те, як їх розпізнавати і повідомляти про них. Також важливо впроваджувати надійні заходи фізичної безпеки, такі як системи контролю доступу та камери спостереження, щоб запобігти несанкціонованому доступу до захищених зон. Вживаючи таких заходів, компанії та організації можуть краще захистити свою конфіденційну інформацію від атак соціальної інженерії.[5]

Висновки. Інженерія соціальних атак - це важлива проблема в сфері кібербезпеки, яка потребує уваги та вивчення. Компанії та організації повинні бути обережними і навчати своїх співробітників впізнавати та запобігати соціальним атакам, щоб захистити свою конфіденційну інформацію від зловмисників.

Список використаних джерел

1. Mitnick, K., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. John Wiley & Sons.
2. Hadnagy, C. (2018). Social engineering: The science of human hacking. John Wiley & Sons.
3. Goel, S. (2016). Social engineering attacks: A comprehensive guide to phishing, pretexting, and other tactics. Apress.
4. Hadnagy, C. (2015). Unmasking the Social Engineer: The Human Element of Security. John Wiley & Sons.
5. Stajano, F., & Wilson, P. (2011). Security for ubiquitous computing. John Wiley & Sons.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л. О.

МЕТОДИ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ WI-FI

КОСТЮК Ю., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні засади побудови захищеної комп'ютерної мережі підприємства з використанням технології Wi-Fi. Зазначено переваги застосування обраної топології, архітектури комп'ютерної мережі підприємства, способів керування мережею, розглядаються питання інформаційної безпеки, надійності системи, вибору програмного та апаратного забезпечення.

The article discusses the basic principles of building a secure enterprise computer network using Wi-Fi technology. The advantages of using the chosen topology, the architecture of the enterprise's computer network, methods of network management are indicated, the issues of information security, system reliability, software and hardware selection are considered.

Актуальність. У сучасному світі активно розвиваються мережні й інформаційні технології. В даний час неможливо знайти підприємство, яке функціонує без впровадженої мережі передач даних. Подібна мережа дозволяє виконувати величезну кількість завдань, максимально спрощуючи різні дії, такі як: обмін інформацією; робота з документами; доступ до різних ресурсів; управління додатками; зберігання інформації. Інформація є дуже цінним ресурсом, тому зловмисники нерідко намагаються отримати доступ до системи підприємства. Вони можуть завдати шкоди, що складається в крадіжці персональних даних і даних компанії, і зараженні системи з повним знищенням ресурсів. Засоби масової інформації дуже часто повідомляють про кібератаки на різні підприємства. Виходить, щоб цього уникнути, потрібно дуже уважно підійти до питання модернізації мережі, особливо з боку безпеки. Не менш важливим є вирішення питання захисту комп'ютерних мереж від можливих атак, направлених на порушення функціонування мереж та окремих вузлів, несанкціонованого доступу до інформації та несанкціонованого використання сервісів мережі. Все це вказує на високу актуальність роботи.

Актуальність і значимість проблеми забезпечення інформаційної безпеки обумовлена наступними факторами: застосовуваними засоби забезпечення інформаційної безпеки, які не відповідають високому рівню; повсюдне використання Інтернет тягне до появи загроз з боку віддалених користувачів; постійне збільшення кількості персональних комп'ютерів, захист яких не відповідає вимогам безпеки; зростання обсягів інформації, що обробляється і зберігається з використанням інформаційних технологій; недосконаліть програм і мережевих технологій з точки зору інформаційної безпеки. Тому перед керівництвом будь-якого підприємства рано чи пізно постає питання про об'єднання своєї комп'ютерної мережі з віддаленими майданчиками. Філії в інших містах, замовники, партнери, віддалені співробітники – багатьом групам користувачів може знадобитися надання безпечного доступу до внутрішніх ресурсів мережі.

Метою статті є дослідження особливостей використання методів захисту комп'ютерної мережі підприємства з використанням технології Wi-Fi.

Об'єктом дослідження є розробка захищеної комп'ютерної мережі, яка розробляється для підприємства з використанням технології Wi-Fi.

Предмет дослідження – комп'ютерна мережа підприємства.

Аналіз попередніх досліджень. Загальнотеоретичні аспекти дослідження безпеки комп'ютерної мережі представлені в публікаціях вітчизняних та закордонних науковців:

В.О. Хорошко, В.П. Кучернюка, В.С. Заборовського, В.А. Світличного, М.В. Грайворонського, С.Е. Остапова та ін.

Виклад основного матеріалу. В даний час використання комп'ютерних мереж є невід'ємною частиною нашого життя, область їх застосування охоплює всі сфери людської діяльності. Комп'ютерна мережа – це сукупність комп'ютерів і різних пристроїв, що забезпечують інформаційний обмін між комп'ютерами в мережі без використання будь-яких проміжних носіїв інформації. Розвиток комп'ютерних мереж пов'язано як з розвитком власне ЕОМ, що входять до складу мережі, так і з розвитком засобів телекомунікацій [1,2].

З розвитком мережевих технологій виникла потреба в міжмережних екранах, потім в системах запобігання вторгнень. Зараз для захисту персональних даних, крім антивіруса, брандмауера і засобів запобігання вторгнень, необхідно також використовувати засоби контролю цілісності і сканер вразливостей. Коли мережа піддається вторгненню, DoS-атаці або вірусної епідемії, під загрозою опиняється діяльність всієї організації. Це відбувається тому, що збільшується небезпека для операційних ресурсів, призначених для користувача даних, власних коштів і технологій. Інтелектуальна власність може бути вкрадена і неправомірно використано третьою стороною. Захист локальних мереж підприємств з кожним роком стає все більш складним завданням і сьогодні є одним з основних факторів, з якими стикається бізнес. Нові загрози з'являються на регулярній основі, і жодна організація від них не застрахована. Варто зазначити, що кожен раз при появі нового виду небезпечних загроз змінюється саме поняття «безпечна мережа».

Створення захищеної комп'ютерної мережі – це найкращий спосіб організації єдиного інформаційного середовища підприємства. Завдяки їй користувачі отримають доступ до загальних ресурсів, зможуть спільно використовувати принтери та інше мережеве обладнання. Правильно налаштувавши мережу, адміністратор може забезпечити належний рівень секретності і запобігти витоку даних, що становлять комерційну таємницю [3].

Актуальність і значимість проблеми забезпечення інформаційної безпеки обумовлена наступними факторами: застосовувані засоби забезпечення інформаційної безпеки не відповідають високому рівню розвитку інформаційних технологій; повсюдне використання Інтернет тягне до появи загроз з боку віддалених користувачів; постійне збільшення кількості персональних комп'ютерів, захист яких не відповідає вимогам безпеки; зростання обсягів інформації, що обробляється і зберігається з використанням інформаційних технологій; недосконаліть програм і мережевих технологій з точки зору інформаційної безпеки.

Мета концепції захищеної корпоративної мережі – закрити трафік корпоративної мережі засобами захисту інформації мережевого рівня і організувати фільтрацію інформації в точках з'єднання з відкритими мережами [2].

В якості фільтрації інформації на інтерфейсах з відкритими мережами застосовуються традиційні рішення: міжмережний екран (firewall) або сервіси захисту типу proxy. Важливим елементом захисту від несанкціонованого проникнення в корпоративну мережу з відкритою є послідовне (каскадне) включення декількох фільтрів-ешелонів захисту. Як правило, між відкритою і корпоративною мережею встановлюється зона контрольованого доступу.

При побудові безпровідних мереж однією з найбільш гострих проблем є забезпечення їх безпеки. Якщо в звичайних мережах інформація передається по дротах, то радіохвилі, які використовуються для бездротових рішень, досить легко перехопити при наявності відповідного обладнання. Принцип дії бездротової мережі призводить до виникнення великої кількості можливих вразливостей для атак і вторгнень. При використанні безпровідного доступу до локальної мережі загрози безпеки істотно зростають. Весь процес організації захищеної комп'ютерної мережі можна розділити на наступні етапи:

1. Розробка мережі. На цьому етапі фахівці обстежують територію банківського підприємства, вислуховують побажання замовника по функціоналу, складають план, технічне завдання і готують обладнання, необхідне для установки.

2. Монтаж. На цьому етапі прокладаються кабелі, проводиться монтаж обладнання та налаштування необхідного програмного забезпечення.

3. Тестування. Фахівці перевіряють роботу, відповідність встановленої мережі загальноприйнятим стандартам якості.

4. Обслуговування. Цей етап включає модернізацію і при необхідності усунення неполадок.

Створена захищена мережа підприємства повинна задовольняти таким основним вимогам: бути легко керованою; захищеною від хакерських атак (захист корпоративної мережі передбачає установку спеціального програмного забезпечення – міжмережного екрана); бути адаптованої до основних типів мережевих пристроїв і кабелів. Завдяки цьому мережу в будь-який момент можна модернізувати.

У зв'язку з швидким розвитком інформаційних технологій і технічних засобів статичні механізми захисту від мережевих погроз часто виявляються неефективними. Забезпечити ефективний захист інформації дозволяють динамічні методи, здатні оперативно виявляти і усувати загрози. Робота динамічних технологій будується на оцінки рівня підозрілості дій в мережі з боку певної служби або процесу [2].

Алгоритм дії щодо усунення атак спрямований на ідентифікацію підозрілих об'єктів. Після цього система реагує необхідним чином на діяльність таких об'єктів, яка може бути націлена на ресурси мережі або комп'ютерного обладнання.

Для захисту мереж від зовнішніх загроз можуть застосовуватися наступні основні методи і технології: застосування портів високої надійності, шифрування даних; використання ефективних антивірусів і сканерів; застосування програмного або апаратного мережевого екрану; установка блокаторів «руткітів» і «сніфферів».

Управління безпекою для мереж може бути різним для різних ситуацій. Домашній або малий офіс може вимагати тільки базової безпеки, у той час як великим підприємствам може знадобитися обслуговування з високим рівнем надійності і розширене програмне і апаратне забезпечення для запобігання злому і розсилання небажаних атак. Інформаційна безпека в комп'ютерних мережах починається з аутентифікації, пов'язаної з введенням імені користувача і пароля – однофакторна. З двофакторної аутентифікацією додатково використовується і додатковий параметр (токен безпеки або «ключ», мобільний телефон), з трехфакторной застосовується і унікальний користувальницький елемент (відбиток пальця або сканування сітківки). Після аутентифікації брандмауер застосовує політику доступу. Ця служба безпеки комп'ютерної мережі ефективна для запобігання несанкціонованого доступу, але цей компонент може не перевірити потенційно небезпечний контент, такий як комп'ютерні черв'яки або трояни, що передаються по мережі. Антивірусне програмне забезпечення або система запобігання вторгнень (IPS) допомагають виявляти і блокувати дію таких шкідливих програм. Система виявлення вторгнень, заснована на скануванні даних, може також відстежувати мережу для подальшого аналізу на високому рівні. Нові системи, які об'єднують необмежену машинне навчання з повним аналізом мережевого трафіку, можуть виявляти активних мережевих зловмисників вигляді шкідливих інсайдерів або цільових зовнішніх шкідників, які зламали комп'ютер користувача або обліковий запис. Крім того, зв'язок між двома хостами може бути зашифрована для забезпечення більшої конфіденційності [1,3].

У забезпеченні безпеки комп'ютерної мережі застосовуються контрзаходи – дії, пристрої, процедура або техніка, які зменшують загрозу, вразливість або атаку, усуваючи або запобігаючи її, мінімізуючи заподіяну шкоду або виявляючи і повідомляючи про його наявність.

Методи і засоби забезпечення інформаційної безпеки утворюють власне інструмент, з допомогою якого сили інформаційної безпеки вирішують весь комплекс завдань із захисту життєво важливих інтересів особистості, суспільства та держави в цілому. Тому необхідне чітке юридичне оформлення при розробці нормативних актів, які регулюють діяльність органів інформаційної безпеки. Безпека комп'ютерних мереж забезпечується за рахунок

політики та практик, прийнятих для запобігання та моніторингу несанкціонованого доступу, незаконного використання, модифікації або відключення мережі і доступних для неї ресурсів. Вона включає в себе авторизацію доступу до даних, яка контролюється мережевим адміністратором. Користувачі обирають або призначають ідентифікатор і пароль або іншу аутентифікаційну інформацію, яка дозволяє їм отримувати доступ до даних і програм в межах своїх повноважень.

Політика захисту мережі має описувати технологію і процедури, що використовуються для моніторингу стану захисту системи. За допомогою моніторингу виявляються загрози мережі. Контроль активності в мережі може виявити спроби компрометації системи і допомагає виконати аналіз атак. Моніторинг забезпечує відповідність налагоджень засобів мережного захисту вимогам політики безпеки. Загрози для IT-інфраструктури з кожним роком стають все складніше, для захисту від них потрібно застосовувати різні системи і засоби.

Політика захисту мережі має визначати процедури, що використовуються для аудита, тестування і підтримки захисту мережі. Аудит і тестування можуть допомогти при визначенні загального технічного стану та вразливостей мережних компонентів і всієї системи в цілому. Безперервний контроль, супроводження і модифікація системи захисту забезпечує безпеку мережі.

При проєктуванні мережі та вибору безпровідного обладнання також потрібно враховувати не тільки висоту, периметр кімнат, кількість поверхів будівлі, а й інші перешкоди, так як відстань між будівлями-об’єктами підприємства, коли між ними вона досить велика.

При обранні способу з’єднання декількох філій, вибір зазвичай лежить між прокладкою оптоволоконного кабелю та бездротовим каналом зв’язку. До переваг першого варіанту можна віднести: постійну гарантовану широку смуга пропускання; низьку затримку; підвищення пропускної здатності за рахунок заміни модулів на кінцях каналу.

Безпровідний канал зв’язку – Wi-Fi використовується, коли прокладка кабелю неможлива або занадто дорога, він дозволяє прискорити процес створення мережі. Окрім цього, на відміну від стільникового зв’язку, Wi-Fi мережі використовують діапазон частот, для якого не потрібно придбання ліцензії, відповідно, витрати на мережу зменшуються ще більше. На ринку представлений широкий вибір обладнання Wi-Fi. Однією з основних проблем, характерних для Wi-Fi, є інтерференція, тобто, перетин зон покриття різних станцій. По причині того, що передача сигналу ведеться на вільній частоті, якість зв’язку може значно погіршитися через завади від радіоприладів та домашніх приладів, наприклад, мікрохвильової печі. Окрім цього, умови прийому та передачі погіршують стіни, залізобетонні покриття, сталеві перегородки та ін. Нарешті, до недоліків WLAN можна віднести обмежений радіус дії, який не перевищує 100 метрів в зоні прямої видимості і 50 метрів при передачі інформації всередині приміщення.

Захист WI-FI мережі – досить важливе й актуальне питання при використанні домашньої точки доступу. Захищати її необхідно у зв’язку з тим, що сьогодні існує досить багато способів злому і підключення до мережі сторонніх. Уберегти і захистити свій роутер можна кількома способами, крім цього важливо періодично проводити спеціальні заходи, щоб зберегти його від несанкціонованої атаки або злому. Тільки тоді можна убезпечити особисте з’єднання.

Є три варіанти захисту.

- WEP (Wired Equivalent Privacy) – застарілий і небезпечний метод перевірки автентичності. Це перший і не дуже вдалий метод захисту. Зловмисники без проблем отримують доступ до бездротових мереж, які захищені за допомогою WEP. Не потрібно встановлювати цей режим в налаштуваннях свого роутера, хоч він там і присутній (не завжди).
- WPA (Wi-Fi Protected Access) – надійний і сучасний тип безпеки. Максимальна сумісність з усіма пристроями і операційними системами.

- WPA2 – нова, допрацьована і більш надійна версія WPA. Є підтримка шифрування AES CCMP. На даний момент, це кращий спосіб захисту Wi-Fi мережі. Саме його рекомендують використовувати.
- WPA / WPA2 може бути двох видів:
- WPA/WPA2-Personal (PSK) – це звичайний спосіб аутентифікації. Коли потрібно задати тільки пароль (ключ) і потім використовувати його для підключення до Wi-Fi мережі. Використовується один пароль для всіх пристроїв. Сам пароль зберігається на пристроях. Де його при необхідності можна подивитися, чи змінити. Рекомендується використовувати саме цей варіант.
- WPA/WPA2-Enterprise – більш складний метод, який використовується в основному для захисту бездротових мереж в офісах і різних закладах. Дозволяє забезпечити більш високий рівень захисту. Використовується тільки в тому випадку, коли для авторизації пристроїв встановлений RADIUS-сервер (який видає паролі).

В топології КМ (комп'ютерної мережі) комутатори використовуються як пристрої для сегментації. Як і мости, вони відносяться до другого рівня моделі OSI. Відрізняються тим, що комутація трафіку значно швидша через те, що вона проходить на апаратному рівні завдяки ASICs (Application Specific Integrated Circuits). Комутатори також мають значно більшу кількість портів. Вони запам'ятовують, який вузол під'єднаний до порту, через IP-адресу вузла. Не можна плутати це мережеве обладнання з комутаторами 3-го рівня. Комутатори 3-го рівня потужніші, переймають усі функції звичайних комутаторів і здатні маршрутизувати трафік. Зазвичай вони використовуються на рівні розподілу та рівні ядра ієрархічної моделі мережі.

Ієрархічна модель КМ представляє собою фундамент для мережевої інфраструктури: підключення користувачів, принтерів, сканерів, WAN маршрутизаторів, мережних екранів, серверів і т.д. Ієрархічна модель ділить мережу на три основні рівні:

1. Рівень доступу (Access Layer) – надає користувачам або пристроям доступ до мережі;

2. Рівень розподілу (Distribution Layer) – поєднує комутатори рівня доступу і надає доступ до різних сервіс організації. Поєднання зазвичай відбуватися по агрегованим каналам;

3. Рівень ядра (Core Layer) – поєднує мережеве обладнання рівня розподілу в великим мережах.

Залежно від ситуації можуть використовуватися один, два або три рівні. Наприклад, для офісу з кількістю користувачів менше десяти можна обмежитися рівнем доступу. Для великої організації, що займає декілька поверхів або цілу будівлю, буде краще побудувати мережу на перших двох рівнях. Для ще більших організацій потрібно використовувати всі три рівня. На Рис. 1 зображена типова 3-рівнева ієрархічна модель мережі, де комутатори рівня доступу підключені до комутаторів рівня розподілу агрегованими каналами, а останні підключені до рівня ядра оптоволоконними з'єднаннями. На другому рівні також використовується технологія стеку.

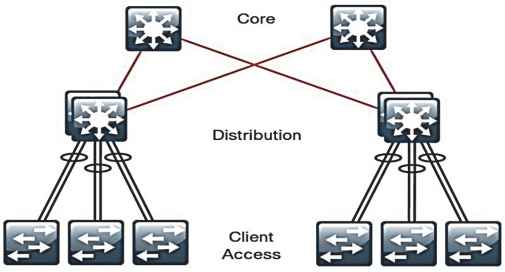


Рис. 1. Ієрархічна модель мережі

Рівень доступу є вхідною точкою для користувачів та мережевих пристроїв. Наприклад: ПК користувача під'єднаний до комутатора рівня доступу крученою парою; мобільний телефон під'єднаний до точки доступу Wi-Fi. Мережеве обладнання не обов'язково повинно мати функції маршрутизації. Воно відповідає за первинну сегментацію мережі. Наприклад, це комутатори рівня доступу. Рівень доступу повинен забезпечити безпеку користувачів та пристроїв мережі від підключених зловмисників або заражених робочих станцій. Засоби захисту:

- DHCP-snooping;
- IP Source guard;
- Port security;
- Dynamic ARP inspection.

Головною задачею рівня розподілу є об'єднання комутаторів рівня доступу в єдину мережу. Це суттєво зменшує кількість лінків. Як правило, саме комутатори рівня розподілу підключають до мережі найнеобхідніші сервіси та модулі. Рівень розподілу є найважливішою частиною всієї мережевої інфраструктури і вимагає високу продуктивність, відмовостійкість. Мережеве обладнання рівня розподілу – це, як правило, комутатори 3-го рівня моделі OSI. Вони здійснюють маршрутизацію трафіку між сегментами мережі (між різними VLAN).

Система безпеки не є однією з головних задач на цьому рівні. Комутатори рівня доступу підключаються до рівня розподілу по агрегованим каналам (Ether Channel), одночасно забезпечуючи відмовостійкість та високу продуктивність. Агрегований канал є поєднанням 2, 3-х або більше фізичних лінків в один логічний. При цьому всі з'єднання передають інформацію, що суттєво збільшує пропускну здатність каналу. У разі відмови одного з лінків, що входить до агрегованого каналу, інформація продовжить передаватися по працездатним лінкам без жодної затримки в роботі мережі. Це головна різниця від традиційної надлишкової моделі, де блокуються додаткові з'єднання (протоколи STP, RSTP) для уникнення петель. При використанні традиційної моделі продуктивність не зростає, лише досягається відмовостійкість. Один логічний лінк замість багатьох фізичних також дозволяє полегшити адміністрування мережею. Комутатори рівня розподілу об'єднуються в стек за допомогою такої технології, як, наприклад, StackWise Plus. Агрегований канал утворюється при об'єднанні портів різних комутаторів стека (Рис. 2).

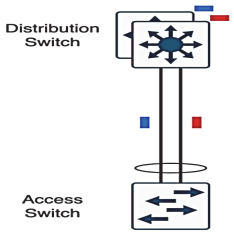


Рис. 2. Схема агрегованого каналу між комутатором доступу та стеком комутаторів розподілу

Іншими словами, логічний інтерфейс утворюється внаслідок об'єднання двох (або більше) портів, при цьому один порт належить першому комутатору стека, а другий – другому комутатору. Обидва порти приймають участь в передачі даних. Таким чином задіяні всі пристрої, забезпечуючи високу продуктивність і відмовостійкість.

Дизайн великих корпоративних мереж підприємства, що охоплюють дві або більше будівлі, зобов'язує використання рівня ядра. Головним завданням рівня ядра є об'єднання всіх комутаторів рівня розподілу в єдину мережу та маршрутизація трафіку. Засобів захисту на цьому рівні не так багато, так як безпека має менший пріоритет, ніж інші функції.

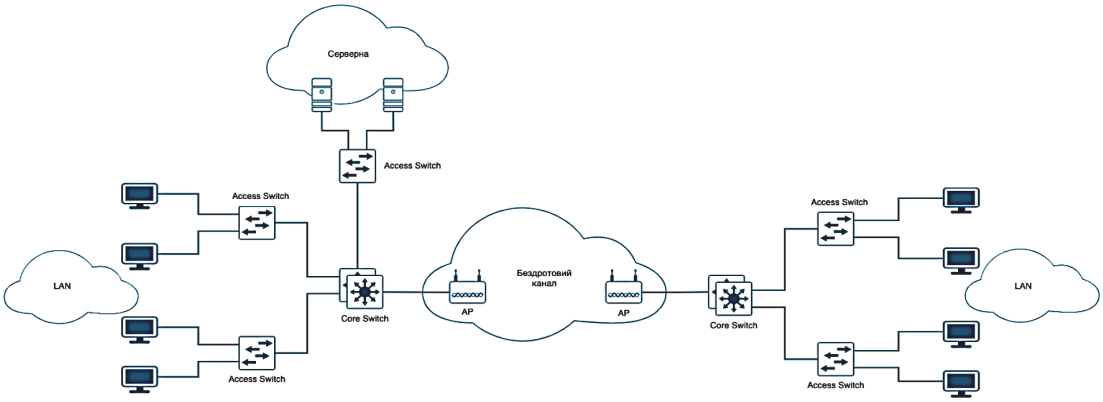


Рис. 3. Структурна схема комп'ютерної мережі в будівлях підприємства

Зрозуміло, що без рівня розподілу в КМ підприємства не обійтися, так як трафік між різними сегментами мережі повинен маршрутизуватися. Комутатори рівня ядра розраховані на велику завантаженість мережі і здатні передавати дані зі швидкістю 40 Гбіт/с. Немає ніякого сенсу придбавати таке обладнання, коли швидкість бездротового каналу між будівлями лише 24 Мбіт/с. По цій причині рекомендується об'єднати рівень розподілу з рівнем ядра (Рис. 3). Це доволі часта практика, і, хоча рівень ядра не буде мати окремого мережевого обладнання, всі його важливі функції будуть будуть виконуватися на рівні розподілу (Рис. 4). Рівень розподілу, до речі, матиме назву Collapsed Core. Проєкт мережі, зображений на Рис. 3 та Рис. 4, підходить підприємству, в якому більша кількість трафіку проходить всередині локальних мереж, а канал зв'язку між ними використовується не так часто. Тепер щодо кількості L2 комутаторів (комутаторів другого рівня моделі OSI, що використовуються на рівні доступу).

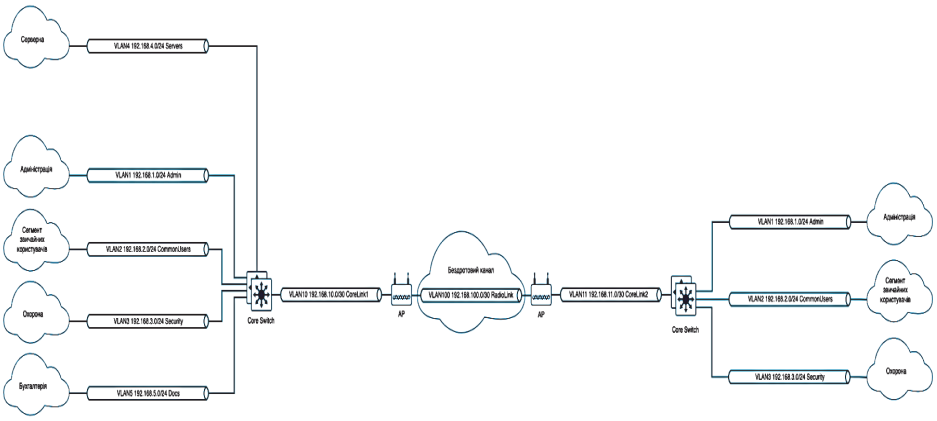


Рис. 4. L3 схема комп'ютерної мережі в будівлях підприємства

Висновки. Задача створення ефективних комплексних систем захисту комп'ютерних мереж може бути вирішена з використанням сукупності методів та технологій, які реалізовані в сучасному телекомунікаційному обладнанні для комп'ютерних мереж, як основи технічної складової таких систем. При виборі та реалізації технологій захисту для конкретної мережі необхідно враховувати особливості структури мережі, спеціалізації роботи підприємства, вірогідність проведення конкретних атак. Налаштування відповідного функціоналу на мережевому обладнанні дозволяє здійснювати контроль відповідності політиці мережевої безпеки та реалізовувати захист максимально близько до можливого джерела порушень, що, у свою чергу, мінімізує можливі негативні наслідки для корпоративної мережі моделі OSI.

Список використаних джерел

1. Yanko A. Система захисту комп'ютерної мережі / A. Yanko, R. Vyhivskyi // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2022. – Т. 2 (68). – С. 91–94. – doi: https://doi.org/10.26906/SUNZ.2022.2.091 (останнє звернення 09.03.2023 р.).
2. Кучернюк В. П. Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні). Мікросистеми, електроніка та акустика. 2017. № 6. Том 22. С. 64-70. URL: http://elc.kpi.ua/article/view/113191 (останнє звернення 09.03.2023 р.)
3. Cisco Network Admission Control (NAC) Solution Data Sheet // Cisco. January 23, 2017. \\ Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean (останнє звернення: 09.03.2023 р).

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ЗВЄРЄВА В. П.

ВИМОГИ ДО СИСТЕМИ БЕЗПЕКИ ПІДПРИЄМСТВА ТА ОСНОВНІ ПРИНЦИПИ ЇЇ ПОБУДОВИ

КРАВЧУК Ю., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто вимоги функціонального призначення систем контролю та управління доступ (СКУД), функціональний склад і загальні вимоги СКУД, інтеграція та побудова мережі СКУД, охоронна сигналізація, пожежна сигналізація, система управління контроль доступу, функція СКУД, система контролю доступу, система відеоспостереження.

The article discusses the requirements for the functional purpose of access control and control systems (ACC), the functional composition and general requirements of ACC, integration and construction of the ECU network, security alarm, fire alarm, access control management system, ACS function, access control system, video surveillance system.

Актуальність. Системи контролю та управління доступом (СКУД) є необхідним атрибутом будь-якої організації. Існує необхідність обмежити доступ до важливих процесів та захистити ресурси і активи в різних місцях виробництва, включаючи цехи, конвеєри, склади та лабораторії. В сучасному виробництві часто трапляються такі прикрі випадки, як крадіжки, вандалізм власності підприємства, пошкодження майна і навіть напади на співробітників [1]. На теперішній час тенденція розробників зводиться до створення багатофункціональних централізованих систем контролю та управління доступом із використанням радіочастотних технологій (RF) та технологій безконтактних смарт-карт.

Сучасна централізована СКУД може принести користь підприємствам, які не мають контролю доступу або використовують автономні системи на критичних об'єктах. Автономні системи дещо обмежені за своєю природою, і однією з їхніх слабких сторін є нездатність ефективно відстежувати людей, які входять у приміщення, що ускладнює розслідування інцидентів. Різноманітні технології, такі як штрих-коди, QR-коди, Bluetooth, біометрія, RFID, безконтактні смарт-картки та NFC спочатку вивчалися шляхом консультацій з відповідними академічними журналами, статтями та технічними статтями в

Інтернеті. Дослідження показують, що найкращі техніки для реалізації є безконтактна смарт-карта.

Основна мета цієї роботи полягає в тому, щоб підкреслити проектування та розробку централізованої системи контролю доступу для загального підприємства, яка також здатна ефективно використовувати зібрані дані для інших корисних завдань, таких як автоматичний хронометраж, планування робочих місць і керування в режимі реального часу.

Об'єкт дослідження – дослідження вимоги щодо функціонального призначення систем контролю та управління доступом (СКУД), функціональний склад СКУД і загальні вимоги до неї, інтеграційна та мережева побудова СКУД, системи охоронної сигналізації, системи пожежної сигналізації, системи контролю і управління доступом, можливості СКУД, систем контролю управління доступом, системи відеоспостереження.

Предмет дослідження – системи контролю та управління доступом.

Виклад основного матеріалу.

Основним завданням СКУД є управління доступом на задану територію, включаючи також обмеження доступу на задану територію, ідентифікація особи, яка має доступ на задану територію, а також облік робочого часу; розрахунок заробітної плати (при інтеграції з системами бухгалтерського обліку); ведення бази персоналу/відвідувачів; інтеграція зі всіма системами безпеки.

Користувацькі права для доступу та ідентифікації можуть бути реалізовані різними методами і засобами, наприклад, використанням паролів, особистих PIN-кодів, радіо-частотних технологій, біометрії. Для підтвердження своїх прав особа може пред'явити ті, чи інші ідентифікатори, такі як електронні картки, радіочастотні ідентифікатори, особисті біометричні дані для зчитування системою.

Ключові технології СКУД. З тих пір, як вперше з'явилася концепція електронної системи контролю доступу, вона була протестована та впроваджена з використанням різних технологій. Різні підходи мають свої власні переваги та недоліки.

Далі розглядаються основні технології, які можуть бути використані при проектуванні СКУД.

Штрих-коди та коди швидкого реагування (QR). Обидві технології вимагають прямої видимості, що може спричинити деякі затримки, особливо коли користувачеві важко розташувати коди належним чином для сканування. Хоча вони є недорогим рішенням контролю доступу, вони є технологіями з низьким рівнем безпеки, оскільки коди можна дублювати дуже легко.

Біометрія. Біометрія забезпечує найвищу форму захисту, оскільки усуває певні пристрої облікових даних, забезпечуючи таким чином контроль доступу, який неможливо передавати на відміну від ключів або карток. Однак, завдяки високому рівню безпеки, він також має високі витрати на впровадження. Розгортання біометричних даних для безпеки підприємства на об'єктах з великою кількістю користувачів та великим трафіком може бути нерозумним, оскільки його характер автентифікації може спричинити збої доступу у точках входу.

Bluetooth. На ринку вже є декілька комерційних продуктів, зокрема Kevo Smart Lock та EC Key, які перетворюють пристрої з підтримкою Bluetooth на ключ. Головною проблемою цього підходу є споживання батареї пристрою (смартфона) користувача. Для того, щоб користувачі могли швидко та зручно подорожувати через точки входу, їх Bluetooth рекомендується вмикати та постійно залишати у видимому режимі. Це розряджає заряд акумулятора мобільних пристроїв, і в разі несправності мобільних пристроїв або розрядження пристроїв слід розглянути плани резервного копіювання.

Радіочастотна ідентифікація (RFID). Все більш поширена технологія з 1970-х років, оскільки ця технологія стає більш доступною. Однією з її головних переваг є той факт, що вона не вимагає прямої видимості і може мати велику дальність читання, що робить її одним з найкращих кандидатів для ідентифікації та відстеження об'єкта. Однак використання

пристроїв RFID, які працюють на високій частоті, отже, мають високий діапазон зчитування, не може обмежувати пропускну здатність системи. Тож в ідеалі пристрої, що працюють на низькій частоті (НЧ), були б кращим вибором для систем контролю доступу.

Системи ближнього поля (NFC). Нова технологія, яка дозволила використовувати смартфони як облікові дані користувача. Перевагою такої технології є можливість використання єдиного (комунікаційного) пристрою доступу. Але відсутність стандартизації серед операторів стільникових телефонів, виробників телефонів та виробників безпеки є найбільшою перешкодою на шляху адаптації технології [3].

Безконтактна смарт-карта. Безконтактна смарт-карта використовує радіочастоту між картою та зчитувачем, що не вимагає фізичного вставлення картки, оскільки зчитування здійснюється шляхом її проходження вздовж зовнішньої частини зчитувача. Ці картки відповідають стандарту ISO-14443, із варіаціями типів A, B та C. Оснащені пам'яттю та можливістю шифрування роблять ці карти ідеальним варіантом для програм, які вимагають певного рівня безпеки. Смарт-карта Сантандера є прикладом використання безконтактних смарт-карт для безпечного застосування в навчальних закладах у великих масштабах [2].

Готові комплекти систем контролю доступу – це комплекти складаються з контролера, зчитувача, замку (магнітного або електромеханічного), кнопки виходу, додаткового обладнання (куточок для магнітного замку), кабелю, ключів стандарту Proximity Key (EM-Marine), блоку живлення 12 Вольт та іншого обладнання для самостійного монтажу. Комплекти СКУД обмежують доступ у приміщення на підприємстві, в офісах і виробництвах, кафе і ресторанах. Системи обмеження доступу зустрічаються практично скрізь і вирішують головні завдання по обмеженню доступу в приміщення. Системи управління контролем доступу дозволяють не тільки обмежувати доступ, але й фіксувати всі події (час приходу і відходу, відпрацьований час тощо), які зберігаються в пам'яті контролера або ж в комп'ютері. Згідно з отриманими звітів на багатьох підприємствах відбувається нарахування заробітної плати.

Перспективна структура централізованої СКУД.

На сьогоднішній день існує дуже багато різновидів СКУД різних виробників, а також її компонентів. Незважаючи на унікальність кожної конкретної системи контролю доступу, вона повинна містити наступні основні елементи (рис. 1).

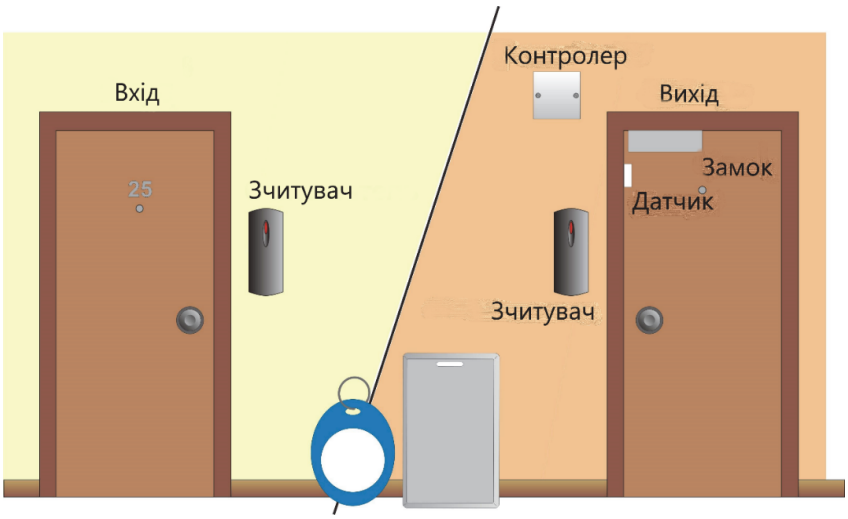


Рис. 1. Схема системи СКУД

Точка контролю. Точка входу, де необхідний бар'єр. Поширені приклади фізичного контролю доступу до точок доступу включають ворота, турнікети та дверні замки. Захищений простір може мати одну точку доступу, наприклад, офіс всередині великого комплексу, або багато точок доступу.

Панель керування. Панель керування СКУД отримує облікові дані від пристрою зчитування та перевіряє, чи є такі дані дійсними. Якщо облікові дані підтверджуються, панель управління передає дані авторизації до точки доступу через сервер контролю доступу, і двері відчиняться. Якщо дані не підтверджені, користувач не зможе отримати доступ.

Зчитувачі розташовуються у точці доступу і надсилають дані з облікових даних на панель керування для автентифікації облікових даних та запит на авторизацію доступу. Якщо використовується клавіатура або біометричний термінал (наприклад, сканування відбитків пальців, ідентифікатор обличчя або сканування сітківки ока), користувачі вводять свій PIN-код або виконують сканування для отримання доступу.

Особисті облікові дані. Більшість СКУД вимагають, щоб користувач мав ідентифікаційні облікові дані, щоб ввести об'єкт або отримати доступ до даних. Прикладами фізичного контролю доступу є облікові дані, зокрема (карти, ключі, токени) та системи введення карток, зашифровані носії, мобільні пристрої, PIN-коди та паролі. Особисті дані відповідають користувачу, який намагається отримати доступ.

Сервер контролю доступу. Сервер контролю доступу зберігає дані користувача, привілеї доступу та журнали аудиту. Залежно від вашої системи, сервер може бути локальним або керованим у хмарі. Необхідно регулярно проводити технічне обслуговування системи та оновлення програмного забезпечення, щоб захистити систему від злому та можливих порушень безпеки.

*Допоміжне обладнання***.** Це блоки безперебійного живлення, датчики, кнопки, проводка тощо.

Програмне забезпечення – здійснює налаштування та управління обладнанням, моніторинг його параметрів, систематизацію та архівування всієї інформації системи. Воно також здійснює підтримку обміну даними між контролерами і комп'ютером моніторингу, управління доступом і моніторинг пунктів проходу, роботу з базами даних і реєстрацію власників ідентифікаторів, дозволяють здійснювати візуальну ідентифікацію власників «електронних перепусток» на прохідній і для формування різних звітів, а також виконувати додатковий набір функцій.

СКУД повинна забезпечувати виконання таких основних функцій [4]:

- відкривання перерегороджуючих пристроїв контролю (ППК) при зчитуванні ідентифікаційної картки, доступ за яким дозволено в дану зону доступу (приміщення) в заданий часовий інтервал або по команді оператора СКУД;
- заборона відкривання ППК при зчитуванні ідентифікаційної картки, доступ за яким не дозволено у дану зону доступу (приміщення) в заданий часовий інтервал;
- санкціонована зміна (додавання, видалення) ідентифікаційних карток в пристроях керування (ПК) і зв'язок їх з зонами доступу (приміщеннями) і часовими інтервалами доступу;
- захист від несанкціонованого доступу до програмних засобів ПК для зміни (додавання, видалення) ідентифікаційних карток;
- захист технічних і програмних засобів від несанкціонованого доступу до елементів управління, установки режимів і до інформації;
- збереження налаштувань і бази даних ідентифікаційних карток при відключенні електроживлення;
- ручне, напівавтоматичне або автоматичне відкривання ППК для проходу при аварійних ситуаціях, пожежі, технічні несправності відповідно до правил установлених режимом і правилами протипожежної безпеки;
- автоматичне закриття ППК за відсутності факту проходу через певний час після зчитування дозволеної ідентифікаційної картки;
- видачу сигналу тривоги (або блокування ППК на певний час) при спробах підбору ідентифікаційних карток (коду);

- реєстрацію і протоколювання поточних і тривожних подій;
- автономну роботу зчитувача з ППК в кожній точці доступу при відмові зв'язку з ПК.

На об'єктах підприємства, де необхідний контроль збереження предметів, слід встановлювати СКУД, контролюючих несанкціонований винос даних предметів з ОІД по спеціальних ідентифікаційних мітках.

Вимоги до перспективної системи контролю та управління доступом.

Коли справа доходить до вибору системи контролю доступу, слід враховувати багато факторів. Це може варіюватися від того, як система впроваджена, а також від того, як користувачі виглядають для управління та доступу до своєї системи контролю доступу.

Хмарні сервіси.

Впровадження та управління системою доступу до організації починається з вибору між локальною системою контролю доступу та хмарним рішенням. Різниця між двома факторами полягає в тому, як ваша організація буде керувати, масштабувати та керувати своїм повсякденним доступом до будівель.

Інтеграція систем доступу.

Хоча побудова систем контролю доступу відіграє ключову роль у забезпеченні фізичних просторів, більшість систем традиційно вирішують лише половину проблем. На додаток до знання ситуації за дверима, система може бути більш корисною в інтеграції з іншими системами фізичного захисту, такими як відеоспостереження. Однак різниця між технічними рішеннями щодо відеоспостереження та контролю доступу може призвести до несумісності різних систем.

Формати карток користувачів.

Окрім технічної оцінки систем контролю доступу, організації також повинні враховувати типи облікових даних та методи побудови доступу, які вони будуть використовувати у своїх фізичних просторах. Починаючи з форматів зчитувачів карток, таких як Wiegand та OSDP, розширюючи широкий спектр форматів карток на вибір, захист вашої організації часто починається з тих самих облікових даних, якими володіють користувачі.

Масштабованість.

На початковому етапі досить важко визначити основні параметри системи і тому бажано, щоб система була масштабованою. На додаток до того, як знати, скільки дверей та зареєстрованих користувачів вам знадобиться для побудови доступу, необхідно також врахувати, як системи будуть взаємодіяти між собою під час управління декількома системами контролю доступу або місцями.

Ціна.

Є багато. факторів, які відіграють значну роль у визначенні ціни на систему контролю доступу до організації. Основні витрати, такі як обладнання та програмне забезпечення контролера, можуть складати більшу частину витрат організації, однак існують різні інші витрати, пов'язані з такими речами, як зчитування карток ключів, обслуговування системи та встановлення системи контролю доступу.

Безпека.

На додаток до фізичної безпеки, яку забезпечує контроль доступу, важливо також оцінити додаткові міркування щодо безпеки. Це може варіюватися від того, як ваші контролери доступу до дверей підключаються до системи, а також від вибору правильної форми RFID / безконтактних карток, щоб найкраще захистити вашу організацію.

Зчитувачі пристроїв введення ідентифікаційних об'єктів (ПВІО) повинні забезпечувати [4]:

- зчитування ідентифікаційної картки; порівняння введеної ідентифікаційної інформації зі збереженням в пам'яті або базі даних ПК;
- формування сигналу на відкривання ППК при ідентифікації користувача;

- обмін інформацією з ПК. ПВІО повинні бути захищені від маніпулювання шляхом перебору або підбору ідентифікаційних даних.

Ідентифікатори ПВІО повинні забезпечити зберігання ідентифікаційних даних протягом усього терміну експлуатації для ідентифікаторів без вбудованих елементів електроживлення та не менше 3 років – для ідентифікаторів з вбудованими елементами електроживлення.

Конструкція, зовнішній вигляд і написи на ідентифікаторі і зчитувачі не повинні призводити до розкриття застосовуваних кодів.

Перегороджуючі пристрої контролю з виконавчими пристроями повинні забезпечувати [2]:

- часткове або повне перекриття отвору проходу;
- автоматичне і ручне (в аварійних ситуаціях) відкривання;
- блокування людини всередині ППК (для шлюзів, прохідних кабін);
- необхідну пропускну спроможність.

Пристрої керування мають забезпечувати:

- прийом інформації від ПВІО, її обробку, відображення в заданому вигляді і вироблення сигналів управління ППК;
- ведення баз даних співробітників і відвідувачів ОІД з можливістю завдання характеристик їх доступу (коду, часового інтервалу доступу, рівня доступу та інші);
- ведення електронного журналу реєстрації проходів співробітників і відвідувачів через точки доступу;
- пріоритетний висновок інформації про тривожних ситуаціях в точках доступу.

Установка СКУД на підприємстві вирішує три першочергові проблеми:

- обмеження доступу сторонніх осіб на об’єкт, приміщення, що захищається;
- контроль за пересуванням працівників;
- облік робочого часу.

Обмеження доступу сторонніх осіб – одне з найважливіших завдань. Воно реалізується за рахунок установки блокуючих, керованих пристроїв (електричні замки, турнікети) на входах і виходах приміщень і територій, що захищаються.

Контроль за пересуванням співробітників є не менш важливою функцією, що дозволяє визначити, куди і коли заходив працівник. Ця інформація є корисною як у разі розгляду нештатних ситуацій (наприклад, крадіжка), так і для організації правильної роботи підприємства. Для реалізації цього необхідно, щоб у кожного співробітника був свій унікальний ідентифікатор (карта, електронний ключ, відбиток пальця тощо).

Облік робочого часу, дозволяє керівництву фірми бути в курсі того, скільки годин відпрацював співробітник і наскільки добре дотримувався робочої дисципліни. На деяких підприємствах, за даними автоматизованої системи обліку робочого часу, проводиться розрахунок заробітної плати працівника, згідно з фактично відпрацьованим часом.

Система СКУД, поєднана з охоронною сигналізацією, дає надійний захист будь-якого підприємства. Така система охорони реагуватиме на наступні фактори: несанкціонований доступ на територію підприємства, що охороняється, злам дверей, розбиття вікон та інші подібні дії [5].

В Україні на сьогодні існує близько 35 компаній, які виробляють як технічні засоби, так і програмне забезпечення і надають послуги для формування СКУД під конкретні потреби підприємства. Серед них – CYPHRAX, U-Pro, Orion, SmartSecurity, Tescom, Elko, ВТП Трансекспо Бренд-Енерго Тов., ООО Енерго Інжиніринг, ООО «Ексимтек ПЛЮС», Vel-Trade та ін.

Висновки. Таким чином, з проведеного аналізу можна зробити висновок, що системи контролю та управління доступом є невід’ємною частиною інтегрованої системи підприємства та одним з найважливіших компонентів забезпечення інформаційної та фізичної безпеки на об’єктах інформаційної діяльності.

Список використаних джерел

1. Ворона В.А., Тихонов В.А. Системи контролю та управління доступом. – К.: Телеком, 2010. – 272 с.
2. Системи контролю доступу. – URL: http://studopedia.com.ua/1_30311_sistema-kontrolyu-dostupu.html
3. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури / ДержНДІ Спецзв'язку, 2015. – С. 58–60.
4. Дурденко В.А. Розробка класифікації та архітектури побудови інтегрованих систем безпеки / Дурденко В.А. Рогожин А.А. – К.: Інформаційно-обчислювальні керуючі та мережеві системи, 2012. – 336 с.
5. Юдін О.К. Інформаційна безпека держави / О.К. Юдін. – К. : Консум. – 2005. – 576 с.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
САВЧЕНКО Т. В.

ВИКОРИСТАННЯ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ДЛЯ ЗАХИСТУ ВЕБЗАСТОСУНКІВ

КРАСНОПОЛЬСЬКИЙ О., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто використання двофакторної автентифікації як засобу захисту вебзастосунків. Описано процес встановлення та налаштування двофакторної автентифікації для вебзастосунків. Зазначено переваги та недоліки використання двофакторної автентифікації, а також те, які фактори впливають на вибір конкретного методу двофакторної автентифікації. Наведено приклади реалізації двофакторної автентифікації для вебзастосунків та діляться порадами щодо того, як можна покращити безпеку вебзастосунків за допомогою двофакторної автентифікації.

The article discusses the use of two-factor authentication as a means of protecting web applications. The process of installing and configuring two-factor authentication for web applications is described. The advantages and disadvantages of using two-factor authentication are mentioned, as well as the factors that influence the choice of a specific method of two-factor authentication. Examples of implementing two-factor authentication for web applications are provided, and advice is given on how to improve the security of web applications using two-factor authentication.

Актуальність. Актуальність використання двофакторної автентифікації для захисту вебзастосунків полягає в тому, що з кожним роком зловмисники стають все більш винахідливими у способах вторгнення до систем та викрадення даних. Найбільш поширеним методом злому є перехоплення паролів, які користувачі використовують для входу до своїх акаунтів. Також існують атаки, які спираються на соціальну інженерію та інші методи викрадення інформації.

Одним із найефективніших способів захисту є двофакторна автентифікація (2FA), процес безпеки, який вимагає від користувачів надання двох форм ідентифікації для доступу до онлайн-облікового запису або платформи. Як правило, це включає пароль або PIN-код, а

також вторинну форму автентифікації, таку як відбиток пальця або код безпеки, надісланий на мобільний пристрій. 2FA необхідна, оскільки вона додає додатковий рівень безпеки обліковим записам користувачів, ускладнюючи їх зламати. За допомогою традиційної автентифікації лише за паролем хакер, який вгадає або викрадає пароль користувача, може отримати доступ до його облікового запису та потенційно викрасти конфіденційну інформацію або здійснити зловмисні дії. Однак за допомогою 2FA, навіть якщо хакер має пароль користувача, йому все одно потрібен другий фактор (наприклад, телефон або токен користувача), щоб отримати доступ. Це значно ускладнює хакерам отримати несанкціонований доступ до облікових записів користувачів.

Використання двофакторної автентифікації дозволяє підвищити безпеку вебзастосунків, оскільки для входу до акаунту користувач повинен підтвердити свою ідентичність за допомогою двох факторів. Це ускладнює завдання зловмисників, які намагаються вторгнутися до системи та зламати акаунт. Крім того, використання двофакторної автентифікації є одним з вимог для деяких законодавчих актів та стандартів щодо захисту конфіденційної інформації, наприклад, PCI DSS, HIPAA, GDPR.

Отже, використання двофакторної автентифікації є актуальним для підвищення безпеки вебзастосунків і захисту конфіденційної інформації.

Метою статті є дослідження важливості використання двофакторної автентифікації для захисту вебзастосунків та допомога користувачам у виборі оптимального методу захисту своїх даних від несанкціонованого доступу.

Об'єктом дослідження є використання двофакторної автентифікації для захисту вебзастосунків від несанкціонованого доступу та розгляд методів її впровадження в різних типах вебзастосунків.

Предмет дослідження – вебзастосунків, які можуть використовувати двофакторну автентифікацію для забезпечення більш високого рівня захисту.

Аналіз попередніх досліджень. Попередні дослідження підтверджують, що методи двофакторної автентифікації є більш надійним та безпечним порівняно з однофакторною автентифікацією. Використання двох незалежних механізмів автентифікації ускладнює процес злому пароля, а також дозволяє користувачеві перевірити свій акаунт у випадку викрадення або втрати своїх доступів. Дослідження науковців доводять те, що успішність методу двофакторної автентифікації залежить від реалізації та налагодження системи. Недостатня захист може призвести до порушення безпеки, тоді як надмірний захист може призвести до складнощів для користувачів та зниження продуктивності. Дослідженню двофакторної автентифікації присвячені праці наступних науковців: T.Petsas(Т. Петсас), G.Tsirantonakis(Г. Цірантонакіс), E.Athanasopoulos (Е. Атанасопулос), Claudia Ziegler Acemyan (Клаудія Зіглер Асемян), Philip Kortum (Філіп Кортум), Jeffrey Xiong (Джеффрі Сюн) та інші.

Виклад основного матеріалу. Захист вебзастосунків є критично важливим, оскільки ці застосунки можуть містити конфіденційну інформацію, таку як особисті дані користувачів, банківські дані та інші конфіденційні дані. Зламані вебзастосунки можуть призвести до викрадення цієї інформації, що може призвести до серйозних наслідків, таких як крадіжка грошей або ідентичності. Для захисту вебзастосунків можна використовувати різні методи, такі як шифрування даних, використання паролів складної структури, контроль доступу та двофакторну автентифікацію. Кожен з цих методів може забезпечити додатковий рівень захисту вебзастосунків та допомогти у запобіганні злому. Захист вебзастосунків також може бути забезпечений за допомогою використання безпечних протоколів, таких як HTTPS. HTTPS забезпечує шифрування даних між веб-сайтом та користувачем, що допомагає у запобіганні злому та доступу до конфіденційної інформації. Незважаючи на застосування різних методів захисту вебзастосунків, важливо знати, що ці методи не є 100 % ефективними та можуть мати певні вразливості. Тому важливо постійно підтримувати та оновлювати системи захисту, щоб убезпечити веб-застосунки від потенційних загроз [1].

Захист вебзастосунків є дуже важливим аспектом в сучасній інформаційній безпеці. Зловмисники можуть використовувати різні техніки для отримання несанкціонованого доступу до вебзастосунків, таких як використання вразливостей у програмному забезпеченні, фішингові атаки, підбір паролів та багато іншого. Для захисту вебзастосунків використовують різні методи, включаючи криптографічні методи, контроль доступу, моніторинг та аудит безпеки. Одним з найпоширеніших методів захисту вебзастосунків є автентифікація користувачів. Цей метод дозволяє підвищити рівень безпеки, оскільки зловмиснику не вистачить лише знання пароля, щоб отримати доступ до веб-застосунку. Окрім автентифікації, веб-застосунки можуть бути захищені за допомогою різних інших методів, таких як шифрування даних, моніторинг активності користувачів та застосування правил контролю доступу. Усі ці методи повинні бути використані разом для забезпечення максимальної безпеки вебзастосунків.

Використання двофакторної автентифікації є важливим для забезпечення високого рівня безпеки вебзастосунків. У порівнянні зі звичайною автентифікацією, яка базується лише на знанні логіну та пароля, двофакторна автентифікація вимагає від користувачів підтвердження своєї ідентичності через два різних механізми, що зменшує ризик несанкціонованого доступу до даних [2].

У випадку, якщо зловмисник зламає логін та пароль користувача, він все ще не зможе отримати доступ до системи, якщо двофакторна автентифікація буде використана. Наприклад, у разі використання автентифікації на основі SMS-повідомлень, користувач буде мати доступ до введення додаткового коду, який буде відправлено на його телефон, що зменшить ризик несанкціонованого доступу.

Таким чином, використання двофакторної автентифікації є важливим інструментом для захисту вебзастосунків від кібератак і забезпечення безпеки користувачів. На (Рис. 1) зображено принцип роботи двофакторної автентифікації.

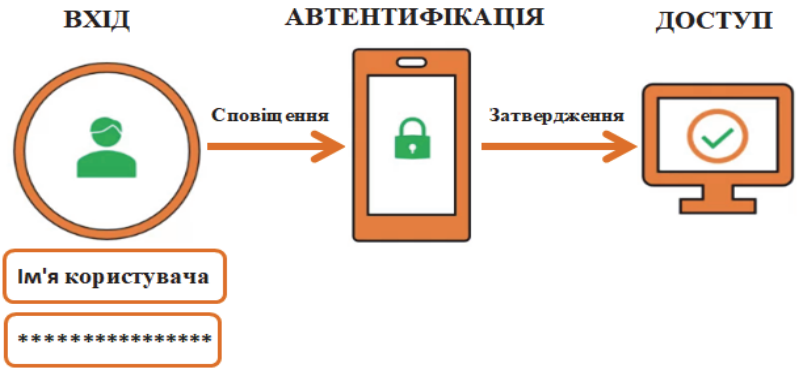


Рис. 1. Принцип роботи двофакторної автентифікації

Двофакторна автентифікація - це процес перевірки ідентичності користувача з використанням двох різних методів аутентифікації. Це забезпечує додатковий рівень безпеки для входу в обліковий запис та захисту від несанкціонованого доступу до вебзастосунків. Зазвичай двофакторна автентифікація використовує комбінацію чогось, що користувач знає (наприклад, пароль або пін-код) та чогось, що користувач має (наприклад, фізичний пристрій, такий як мобільний телефон, на якому встановлено додаток або отримує SMS з кодом). Під час двофакторної автентифікації, коли користувач вводить свої ім’я користувача та пароль на веб-сайті або в додатку, він зобов’язаний підтвердити свою ідентичність через другий крок. Зазвичай це виконується шляхом введення додаткового коду, який надсилається на мобільний телефон, або за допомогою генерування одноразового коду в додатку. Після успішної автентифікації в обліковий запис, користувач може мати доступ до вебзастосунків або додатків, які вимагають автентифікацію, забезпечуючи вищий рівень безпеки та захисту від несанкціонованого доступу [1].

Двофакторна автентифікація (або двоетапна перевірка) – це параметр безпеки, за допомогою якого користувач може захистити свої облікові записи в Інтернеті, додатково підтверджуючи особистість під час авторизації. Замість того, щоб використовувати лише один спосіб підтвердження особистості, такий як пароль, при 2FA необхідно ще вказати одноразовий пароль (OTP), надісланий SMS або електронною поштою.

Таким чином, щоб отримати доступ до облікового запису, зазвичай потрібно вказати лише логін та пароль. Це називається одноетапною перевіркою . Все, що потрібно зробити, це просто ввести облікові дані та увійти в систему. Подібний спосіб авторизації ненадійний. Будь-хто може отримати доступ до адреси електронної пошти. Хакери також легко здатні зламати пароль, якщо він не відповідає нормам безпеки і досить простий (наприклад, «123456»). Двофакторна автентифікація додає додатковий рівень захисту, вимагаючи при авторизації надати набір облікових даних, доступ до яких має лише законний власник облікового запису. В результаті сторонні особи не зможуть отримати доступ до конфіденційних даних [2, 3].

Використання двофакторної автентифікації для захисту вебзастосунків є ефективним способом зменшення ризиків несанкціонованого доступу до конфіденційної інформації та збільшення безпеки користувачів. Для реалізації двофакторної автентифікації можна використовувати різні методи, такі як:

1. Підтвердження через SMS-повідомлення або телефонний дзвінок: у такому випадку користувачеві на його телефон відправляється спеціальний код, який потрібно ввести на сайт для підтвердження ідентичності.
2. Використання автентифікатора: спеціального додатку, який генерує тимчасові одноразові коди або QR-коди, які потрібно ввести на сайт.
3. Використання біометричних даних: таких як відбиток пальця або сканування обличчя.
4. Використання фізичних ключів: таких як USB-ключі або NFC-карти.

Крім того, важливо забезпечити використання надійних паролів та їх регулярну зміну, а також захистити сесії користувачів від зловмисників за допомогою механізмів, таких як HTTPS-захист та токени доступу.

Усі ці заходи разом з використанням двофакторної автентифікації можуть забезпечити високий рівень захисту вебзастосунків від кібератак та зберегти конфіденційну інформацію користувачів.

Сьогодні багато вебзастосунків та сервісів підтримують двофакторну автентифікацію як додатковий рівень безпеки для входу в систему. Наприклад, такі відомі компанії, як Google, Facebook, Twitter, Dropbox, Microsoft та інші, надають можливість використовувати двофакторну автентифікацію для своїх користувачів. Деякі веб-застосунки також надають можливість налаштувати свій власний двофакторний механізм аутентифікації. Зазвичай, використання двофакторної автентифікації в таких сервісах є необов’язковим, але рекомендується для підвищення рівня безпеки користувачів.

Для використання механізму двофакторної автентифікації для захисту вебзастосунків, необхідно виконати декілька кроків [1]:

1. Вибрати механізм двофакторної автентифікації: існують різні типи механізмів, такі як SMS-підтвердження, генератори одноразових паролів (OTP) і біометрична автентифікація. Вибір механізму залежить від ваших потреб та можливостей.
2. Активувати механізм двофакторної автентифікації: більшість веб-сайтів та сервісів мають налаштування для активації двофакторної автентифікації в розділі налаштувань облікового запису. Для активації зазвичай потрібно підтвердити свій номер телефону, електронну пошту або налаштувати генератор OTP.
3. Використовувати механізм двофакторної автентифікації: після активації двофакторної автентифікації, при кожному вході в обліковий запис буде запитуватись додатковий код підтвердження з механізму двофакторної автентифікації. Цей код може бути відправлений на телефон або згенерований з генератора OTP.

Найбільш ефективним вважається використання механізму генератора одноразових паролів (OTP), оскільки він генерує унікальний код підтвердження, який може бути використаний лише один раз. Також слід пам'ятати про необхідність збереження ключа від генератора OTP в безпечному місці, оскільки він є ключовим елементом для отримання коду підтвердження [2].

Основними рекомендаціями щодо використання двофакторної автентифікації для забезпечення максимального рівня безпеки є:

1. Використання двофакторної автентифікацію на всіх облікових записах, які підтримують цю функцію. Це дозволить максимально захистити ваші дані та уникнути можливого взлому облікового запису.
2. Використання сильних паролі для всіх облікових записів та не використовувати один і той же пароль для декількох облікових записів. Використання різних паролів для кожного облікового запису зменшує ризик взлому ваших облікових записів.
3. Використання механізми двофакторної автентифікації, які базуються на різних типах автентифікації. Наприклад, використання пароля та SMS-повідомлення або пароля та автентифікаційного токена зменшує ризик використання одного й того ж механізму автентифікації.
4. Не зберігати свої паролі та інші конфіденційні дані на комп'ютері, який не захищений від злому або віддаленого доступу. Не зберігати свої паролі на публічних комп'ютерах, таких як кіоски, кафе або бібліотеки.
5. Регулярне оновлення своїх паролів та перевірка активних сесій на своїх облікових записах, щоб переконатися, що ніхто не має доступу до особистої інформації без дозволу.
6. Забезпечення безпеки особистих пристроїв та мереж, які використовуються для доступу до особистих облікових записів. Регулярне встановлення оновлення програмного забезпечення на особистих пристроях.

При виборі механізму двофакторної автентифікації для захисту вебзастосунків важливо враховувати кілька факторів, таких як рівень безпеки, зручність використання, сумісність зі смартфоном та іншими пристроями. Основні механізми двофакторної автентифікації, які варто розглянути, включають [1, 3]:

- СМС-повідомлення або телефонний дзвінок - цей метод включає надсилання коду підтвердження на зареєстрований номер мобільного телефону користувача. Для використання цього методу необхідно мати доступ до мобільного телефону.
- Мобільний додаток - цей метод включає використання спеціального додатку для генерації кодів підтвердження. Коди генеруються на основі унікального ідентифікатора акаунту користувача та секретного ключа, який зберігається в додатку. Для використання цього методу необхідно мати смартфон та встановлений на ньому додаток.
- Фізичний токен - цей метод включає використання спеціального фізичного пристрою для генерації кодів підтвердження. Простіші варіанти таких пристроїв виглядають як картки з індикатором або спеціальні USB-ключі. Для використання цього методу необхідно мати доступ до фізичного пристрою.
- Біометричні дані - цей метод включає використання біометричних даних, таких як відбитки пальців або розпізнавання обличчя, для підтвердження особи. Для використання цього методу необхідно мати пристрій зі вбудованим біометричним сканером.

При виборі механізму двофакторної автентифікації важливо враховувати кілька факторів, щоб забезпечити найвищий рівень безпеки [3]:

- Спосіб отримання другого фактору: важливо вибрати спосіб отримання другого фактору, який є зручним і безпечним для користувача. Наприклад, можна використовувати SMS-повідомлення, мобільні додатки або фізичні пристрої, такі як токени або ключі безпеки.

- Рівень безпеки: різні механізми двофакторної автентифікації мають різний рівень безпеки. Наприклад, SMS-повідомлення можуть бути підвержені атакам з використанням перехоплення повідомлень, тоді як фізичні ключі безпеки є найбільш безпечними.
- Вартість та складність реалізації: різні механізми двофакторної автентифікації мають різні вартості і рівні складності реалізації. Наприклад, використання мобільних додатків може бути безкоштовним, але вимагати більшої складності налаштування, тоді як використання фізичних ключів безпеки може бути дорожчим, але більш простим у використанні.
- Підтримка: важливо вибрати механізм двофакторної автентифікації, який підтримується веб-застосунком або сервісом, який ви використовуєте. Наприклад, якщо сервіс не підтримує фізичні ключі безпеки, ви не зможете використовувати їх для автентифікації.

Двофакторна автентифікація має як переваги, так і недоліки. Основні переваги використання двофакторної автентифікації включають [1, 3]

1. Підвищена безпека: використання двох факторів для автентифікації зменшує ризик несанкціонованого доступу до облікового запису.
2. Легкість використання: більшість механізмів двофакторної автентифікації досить прості для використання і не потребують додаткових технічних знань.
3. Гнучкість: користувачі можуть вибирати різні способи другого фактора, що дозволяє їм використовувати той, який їм більше підходить.
4. Зменшення ризику втрати даних: якщо зловмисник зламає пароль, він не зможе отримати доступ до облікового запису без другого фактора.
5. Захист від фішингу: двофакторна автентифікація може захистити від фішингу, коли зловмисник намагається отримати пароль, шляхом підміни веб-сайту або відправлення підробленого листа.

Незважаючи на ці переваги, двофакторна автентифікація має деякі недоліки, зокрема :

1. Складність використання: двофакторна автентифікація може викликати додаткові труднощі для користувача, особливо якщо він не знайомий з процесом. Це може призвести до незадоволення та відмови від використання такого механізму автентифікації.
2. Залежність від доступу до другого фактора: двофакторна автентифікація може бути неефективною, якщо користувач не має доступу до другого фактора, такого як мобільний телефон або ключ-токен.
3. Витрати на впровадження: використання двофакторної автентифікації може бути додатковою витратою для компанії, особливо якщо вона використовує платні механізми автентифікації.

Висновки. Захист вебзастосунків є дуже важливим завданням для підприємств та користувачів. У цьому контексті, двофакторна автентифікація може бути ефективним механізмом для забезпечення безпеки вхідних даних. Основна ідея двофакторної автентифікації полягає у використанні двох різних механізмів для перевірки ідентичності користувача. Це може включати використання пароля та фізичного пристрою, який можна мати при собі, такого як токен або смарт-карту, або використання біометричних даних, таких як відбиток пальця або розпізнавання обличчя. Переваги двофакторної автентифікації включають зниження ризику порушення безпеки від зломів паролів та фішингу, підвищення рівня захисту особистих даних, а також можливість встановлення додаткових прав доступу для різних користувачів. Однак, двофакторна автентифікація також має деякі недоліки, такі як додаткові витрати на обладнання та ресурси, які потрібні для підтримки цього механізму, а також можливість блокування доступу до веб-застосунку в разі втрати пристрою або забутого пароля.

У цілому, двофакторна автентифікація є ефективним механізмом для забезпечення безпеки вебзастосунків, який може допомогти у запобіганні багатьом видам кібератак. При

виборі механізму двофакторної автентифікації важливо розглядати функціональні та безпекові вимоги конкретного веб-застосунку, а також забезпечити правильні налаштування та підтримку механізмів для забезпечення безпеки.

Список використаних джерел

1. A Summative Usability Assessment of Google's Two-factor Authentication (2FA) Methods\\ Режим доступу: https://citeseerx.ist.psu.edu/document? repid=rep1&type= pdf&doi=199a71f02c63b 4b84a00e9b73fd538d28ed92362 (останнє звернення 13.04.2023р.)
2. Empirical Measurement of Systemic 2FA Usability \\ Режим доступу: https://www. usenix.org/system/files/sec20-reynolds.pdf (останнє звернення 10.04.2023р.)
3. A Usability Study of Five Two-Factor Authentication Methods \\ Режим доступу: https://www. usenix.org/system/files/soups2019-reese.pdf (останнє звернення 10.04.2023р.)

Робота виконана під науковим керівництвом старшого викладача
КОСТЮК Ю. В.

МЕТОДИ ПРОТИДІЇ ЗЛОЯКІСНОМУ КОДУ ТА ШПИГУНСЬКОМУ ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННЮ

КРИВЕНКО О., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні технологія створення системи протидії злоякісному коду та шпигунського програмного забезпечення. Зазначено види злоякісного коду та їх засоби протидії. Розглянуто зразки захисту від шкідливих програм за допомогою «Cisco».

The article discusses the basic technology of creating a system for countering malicious code and spyware. The types of malicious code and their countermeasures are specified. Samples of protection against malicious programs with the help of «Cisco»

Актуальність. Шпигунське програмного забезпечення – це ряд шкідливих програм, які дозволяють стежити за діями користувача в мережі Інтернет, а також збирати його конфіденційні дані. Вперше цей термін було вжито в публікації служби новин Usenety в 1995 році [1]. З розвитком технологій кібербезпеки багато шпигунських програм зникли, натомість з'явилися інші, більш складні форми шпигунського програмного забезпечення. Кіберзлочинці можуть використовувати шпигунське програмне забезпечення для отримання особистої інформації, для крадіжки даних або шахрайства.

Злоякісний код або шкідливий програмний засіб – це програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем. Може проявлятися у вигляді коду, скрипту, активного контенту, і іншого програмного забезпечення. Треба зазначити що, зловмисні програмні засоби відрізняються від дефективного програмного забезпечення тим, що останнє є легальним програмним забезпеченням, але містить шкідливі помилки, які не були виправлені до випуску. Програмне забезпечення, яке може бути віднесене до «шкідливих програм» може бути заснованим на різних технологіях, володіти абсолютно різним набором функцій і можливостей. Єдине, що об'єднує всі типи шкідливих програм – це мета, з якою вони створюються.

Шпигунське програмне забезпечення (ШПЗ) це як вірус або злоякісний код, який використовується для «шпигунства», він записує всі дії, записує місцезнаходження, IP-адресу, електронні листи, паролі, номери кредитних карт та різні інші дані, з метою передачі цієї інформації третім особам через Інтернет [2].ШПЗ має високу прихованість, - його дуже важко розпізнати без допомоги антивірусного програмного забезпечення, оскільки володіє важким проникненням у систему. ШПЗ гарно шифрується навіть, коли пристрій намагається видалити його з реєстру Windows, і перехоплює всі спроби це зробити. Іноді шпигунське програмне забезпечення ховається всередині нормальної програми.

ШПЗ може розповсюджуватися через офіційні канали, наприклад веб-сайти розробників або веб-магазин Google. У деяких випадках програми містять не саме шпигунське програмне забезпечення, а функції, які можна використовувати як шпигунське програмне забезпечення. Такі функції часто додаються ненавмисно, і розробник зазвичай видаляє ці функції одразу після повідомлення про них. Тим не менш, існує ще багато сумнівних утиліт, які, як повідомляється, містять елементи шпигунського програмного. Оскільки шпигунське програмне забезпечення може збирати інформацію про вас і надсилати її в інше джерело, тому воно становить величезну загрозу конфіденційності та безпеці.

Метою статті є дослідження ефективних технологій та методів захисту від злоякісного коду з метою збереження конфіденціальної інформації.

Об'єктом дослідження є програмне забезпечення для боротьби з шкідливими програмами.

Предмет дослідження – технології системи протидії злоякісному коду.

Аналіз попередніх досліджень. Дослідженню методів протидії злоякісному коду та шпигунському програмному забезпеченню присвячені праці вітчизняних та закордонних науковців: Чобаль О.І., Різак В.М., Пригара М.П., Ковальов О.О., R. Islam, R. Tian, L. Batten, S. Versteeg та інші.

Аналізуючи дослідження проведені рядом вчених можна дійти висновку, що лідируючу позицію займає Symantec на частку якої припадає 13,56 % антивірусів. З них 10,75 % відносяться до Symantec Endpoint Protection. На другому місці йде антивірус ESET з часткою 12,84 %. ESET Endpoint Antivirus та ESET Endpoint Security займають 4,53 % та 3,7 % відповідно [7] (див. рис. 1).

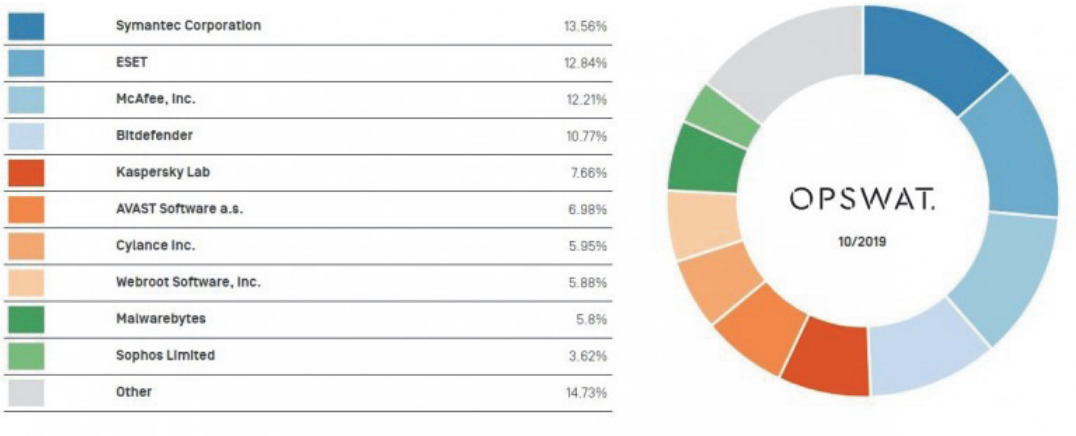


Рис. 1. Популярність антивірусів

Виклад основного матеріалу. В умовах сьогодення можна зазначити велику кількість видів шпигунського програмного забезпечення та злоякісного коду (рис. 2).

Як зазначалося вище основною особливістю таких програм є те, що вони для збору інформації з системи використовують стандартні методи, якими користується ряд інших програм. Завдяки цьому вони можуть не лише збирати, обробляти та передавати зібрані дані третім особам, але і при цьому залишаються непомітними як для користувача так і для захисних програм [8].

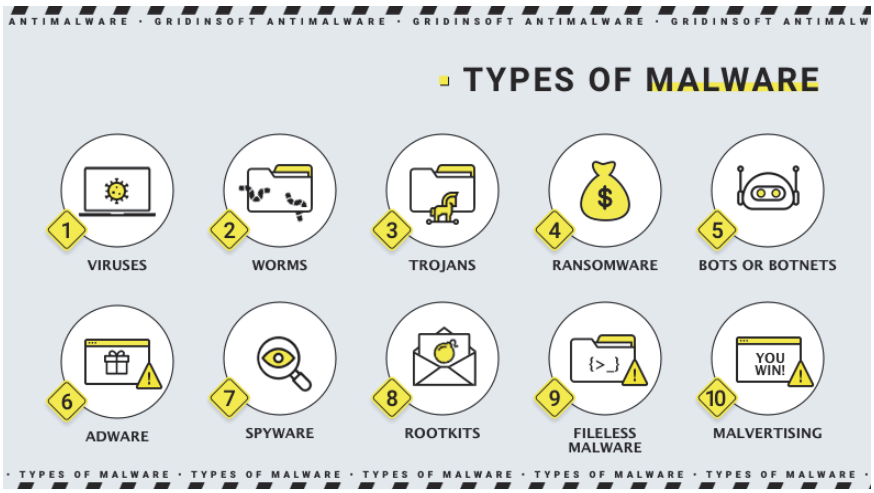


Рис. 2. Види злоякісного коду

Технології постійно розвиваються, як і нові віруси, тому простіше класифікувати їх на типи та види шпигунських програм. Їх можна розділити на чотири основні групи: рекламне програмне забезпечення, файли cookie, трояни та системи моніторингу. Розглянемо найпопулярніші шпигунські програми та шкідливі програми, а саме [3]:

- Кейлоггер – один з найпопулярніших видів шпигунських програм використовується для контролю за натисканням кнопок на клавіатурі.
- Рекламне програмне забезпечення – це вся реклама, яка перекидає користувача в інше місце призначення.
- Троянські програми – надзвичайно небезпечні, тому що вони переймають паролі. Особливо для банківської справи.
- Вебмаяк – зображення, які найчастіше прикріплюються до повідомлень електронної пошти й дозволяють відстежувати поведінку користувачів.
- Руткіт – дозволяє хакеру встановлювати інструменти, які нададуть йому віддалений доступ до обладнання.
- Cookie – файли є різновидом шпигунських програм. Правда, вони менш шкідливі і багато користувачів погоджуються з ними, але вони також дозволяють відстежувати вас в Інтернеті.
- Черви – це шматочки шкідливого коду, які роблять копії. Умови повинні бути правильними, щоб глист розмножувався. Вони створюються переважно за допомогою мов сценаріїв [4].

Технології захисту не стояли на місці, вони теж вдосконалилися. Методи захисту від шкідливих програм стали набагато краще ніж були раніше, тому і шкідливих програм стало набагато менше. Але щоб злоякісний код не зміг видалити або викрасти наші дані, треба проходити процедури захисту персонального комп'ютера, такі як:

Інструменти захисту кінцевих точок забезпечують захист, щоб запобігти зламам кінцевих точок і захистити IT системи від загроз кінцевих точок, включаючи зараження зловмисним програмним забезпеченням і різні кібератаки.

Захист кінцевих точок розширює видимість пристроїв, які традиційно знаходяться за межами периметра безпеки, наприклад особистих ноутбуків і планшетів, які використовуються для роботи, а також корпоративних серверів і робочих станцій.

Антивірусні рішення наступного покоління (NGAV) відстежують і реагують на тактику, прийоми та процедури зловмисників (TTP), щоб допомогти запобігти як відомим, так і невідомим загрозам. Ця технологія була створена, щоб заповнити прогалини, залишені традиційним антивірусним програмним забезпеченням, яке може захищати лише від відомих файлових атак зловмисного програмного забезпечення.

Технологія NGAV пропонує хмарний, системо центричний підхід. Він використовує прогнозну аналітику на основі машинного навчання (ML) і штучного інтелекту (AI) у поєднанні з аналізом загроз для виявлення атак, збору даних криміналістики та реагування на загрози. NGVA може ідентифікувати без файлові атаки без зловмисного програмного забезпечення, зловмисну поведінку та зловмисне програмне забезпечення, реагувати на загрози та збирати дані кінцевої точки для визначення першопричини.

Система запобігання вторгненням (IPS) постійно відстежує мережевий трафік, щоб виявити постійне зараження зловмисним програмним забезпеченням або порушення безпеки. Він також може виконувати відповідні дії в конкретних випадках, які були попередньо визначені адміністратором мережі.

IPS постійно моніторить мережу в режимі реального часу, щоб швидко виявляти й реагувати на потенційні загрози, виконуючи дії для запобігання спостережуваних подій. Він працює, перевіряючи потоки мережевого трафіку на наявність шкідливого програмного забезпечення. Технологія визначає зловмисну діяльність, записує виявлені загрози, повідомляє про виявлені загрози та вживає профілактичних дій для блокування загрози.

Безпека ізольованого програмного середовища забезпечує додатковий рівень захисту від загроз безпеці. Це передбачає використання пісочниці, ізольованого середовища, що імітує операційне середовище кінцевого користувача, для виконання підозрілого коду. Пісочниця забезпечує безпечне середовище, яке відокремлює загрозу від головного пристрою чи мережі. Це особливо корисно під час роботи зі зловмисним програмним забезпеченням нульового дня та стелс-атаками, гарантуючи, що ви можете ізолювати та перевіряти ці загрози, щоб запобігти їх поширенню.

Брандмауер наступного покоління (NGFW) забезпечує застосування політик безпеки для виявлення та блокування складних атак на рівні протоколу, порту та програми. Ви можете реалізувати цю технологію брандмауера третього покоління в апаратному чи програмному забезпеченні.

Дані, що проходять через Інтернет або мережу, розбиваються на невеликі частини, які називаються пакетами. Брандмауери перевіряють ці пакети, оскільки вони містять вміст, який вимагає доступу до мережі. Брандмауер відповідає за блокування або дозвіл пакетів, запобігаючи потраплянню в мережу зловмисного вмісту, зокрема зловмисного програмного забезпечення.

NGFW використовують традиційні можливості брандмауера разом із новими та покращеними функціями. Традиційні можливості включають: фільтрування пакетів, переклад адреси порту (PAT), трансляція мережевих адрес (NAT), віртуальні приватні мережі (VPN), блокування URL.

NGFW розширює вищезазначене за допомогою функції якості обслуговування (QoS) і додаткових функцій, таких як: запобігання вторгненням, глибока перевірка пакетів, перевірка SSL і SSH, обізнаність із застосуванням, виявлення шкідливих програм на основі репутації [5], нульова довіра.

Модель нульової довіри – це підхід до безпеки, який усуває неявну довіру та забезпечує сувору автентифікацію користувачів і пристроїв для захисту мережі. Це допомагає забезпечити надійний захист від різних атак, включаючи крадіжку даних і скомпрометовані облікові дані. Ця модель припускає, що довіра особам або пристроям може спричинити багато вразливостей, оскільки навіть авторизовані сторони можуть бути скомпрометовані. Мережа ніколи не повинна довіряти жодному користувачеві та вимагати автентифікації особи та пристрою в усій мережі, а не лише на периметрі. Реалізація безпеки з нульовою довірою зазвичай передбачає використання мікросегментації для розділення мережевих ресурсів. Ізоляція ресурсів допомагає стримувати загрози в одному мікросегменті мережі, запобігаючи поширенню загрози на інші області. Це мінімізує поверхню атаки та зменшує масштаб шкоди, завданої атакою.

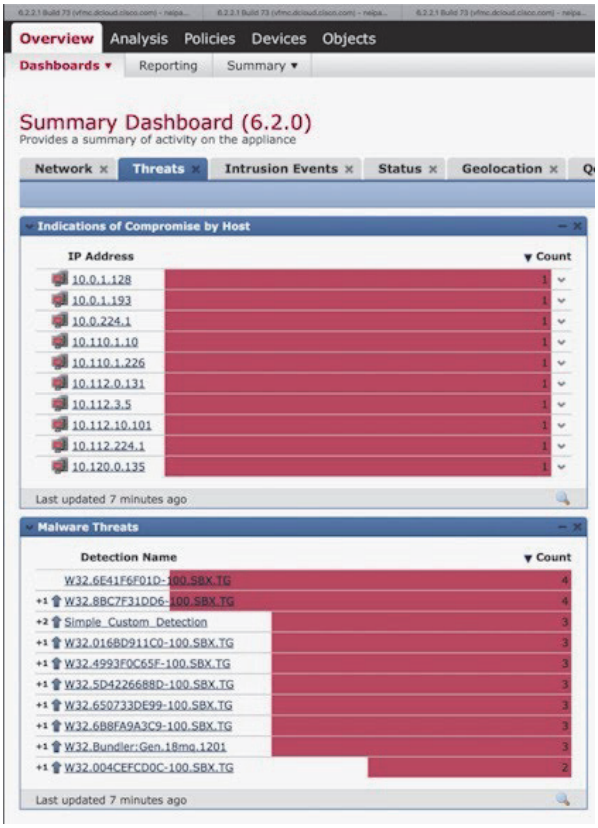


Рис. 3. Приклад роботи Firewall NGFW Demo

Нульова довіра допомагає створити більш комплексний захист від атак зловмисного програмного забезпечення та програм-вимагачів, надаючи розширені можливості моніторингу та виявлення. Нульова довіра може суттєво обмежити здатність зловмисного програмного забезпечення та програм-вимагачів виконувати боковий рух і заражати додаткові частини корпоративної мережі. Крім того, оскільки людська помилка часто є основною причиною кібератаки, нульова довіра зосереджується на ідентифікації користувача та управлінні доступом.

Висновок: кожна компанія з розробки антивірусного програмного забезпечення рекламує свій продукт переконуючи, що він найкращий. Проте у Топ -5 найкращих програм 2023 року увійшла програма Norton 360, TotalAV, McAfee (лише для США),Bitdefender, Intego. Все більшої популярності набувають антивірусні програми з використанням штучного інтелекту.

Список використаних джерел

1. Матеріал від компанії ESET, «Шпигунські програми». Режим доступу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/shpionskiye-programmy/ (останнє звернення 04.04.2023 р.)
2. Матеріал від gridinsoft, «Що таке шпигунські програми?» державності. Режим доступу: https://gridinsoft.ua/spyware (останнє звернення 04.04.2023 р.)
3. Матеріал від dalistrategies, «Що таке шпигунське програмне забезпечення? Як захиститися від нього?» державності. Режим доступу: https://dalistrategies.com/ua/shho-take-shpigunske-programne-zabezpechennya-yak-zahistitisya-vid-nogo/ (останнє звернення 04.04.2023 р.)
4. Матеріал від theastrologypage, «Що таке шкідливий код? - визначення з техопедії» державності. Режим доступу: https://uk.theastrologypage.com/malicious-code (останнє звернення 04.04.2023 р.)

5. Матеріал від cynet, «Malware Protection Technologies and Techniques» державності. Режим доступу: https://www.cynet.com/malware/malware-protection-6-technologies-to-protect-your-organization/#heading-1 (останнє звернення 04.04.2023 р.)
6. ALISA SHEVCHENKO, The evolution of technologies used to detect malicious code. Режим доступу: https://securelist.com/the-evolution-of-technologies-used-to-detect-malicious-code/36177/ (останнє звернення 04.04.2023 р.)
7. Найпопулярніші антивіруси. Режим доступу: https://overclockers.ru/blog/Scorpion81/show/31789/samye-populyarnye-antivirusy-na-windows-na-noyabr-2019
8. Програмний продукт для пошуку та виявлення програм типу spyware О. Ковальов, О. Чобаль, В. Різак, М. Пригара . Режим доступу file:///C:/Users

Робота виконана під науковим керівництвом старшого викладача
БЕБЕШКО Б. Т.

«ХМАРНИЙ» КВАЛІФІКОВАНИЙ ЕЛЕКТРОННИЙ ПІДПИС

КРИВЕНКО С., 2мз курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто процес використання та зберігання особистого ключа кваліфікованого електронного підпису чи печатки (далі – КЕП), що згенеровано у засобі КЕП – захищеному апаратно-програмному пристрої – криптомодулі, що призначений для реалізації криптографічних перетворень на апаратному рівні та безпечного зберігання особистих ключів зареєстрованих користувачів (далі – Хмарне сховище) кваліфікованого надавача електронних довірчих послуг. Зазначено переваги зберігання та використання особистого ключа КЕП у Хмарному сховищі. Розглянуто як зразок порядок генерації особистого ключа КЕП у Хмарному сховищі кваліфікованого надавача електронних довірчих послуг.

The article discusses the process of using and storing the personal key of a qualified electronic signature or seal (hereinafter – KEP), generated in the KEP tool – a secure hardware and software device – a cryptomodule, which is designed to implement cryptographic transformations at the hardware level and securely store personal keys of registered users (hereinafter – Cloud storage) of a qualified provider of electronic trust services. The advantages of storing and using the KEP personal key in the Cloud storage are indicated. The procedure for generating a personal KEP key in the Cloud storage of a qualified provider of electronic trust services is considered as a sample.

Актуальність. У сучасних умовах розвитку економіки та програмно-технічного прогресу, більшість підприємств намагаються використовувати сучасні технології для оптимізації робочого процесу, зокрема, впровадження електронних сервісів є одним з пріоритетних напрямків, що забезпечує фінансовий розвиток та конкурентоздатність у порівнянні з іншими суб'єктами господарювання.

Обмін електронними даними з контролюючими органами, з іншими підприємствами чи організаціями та у середині підприємства дозволяє покращити процеси управління та контролю діяльності.

Електронний документ – документ, інформацію в якому викладено у вигляді електронних даних, включаючи обов'язкові реквізити документа, одним з яких є електронний підпис автора документи, що відповідає вимогам зазначеним у Законі України «Про електронні довірчі послуги»[1].

В свою чергу електронний підпис це електронні дані, які додаються або логічно пов'язуються з електронного документу [2, с. 6].

Електронна взаємодія користувачів електронних довірчих послуг, що передбачає отримання, відправлення чи зберігання документів, які у паперовому вигляді повинні містити власноручний підпис автора документа, повинна здійснюватися з використанням кваліфікованих електронних довірчих послуг.

Якщо електронний підпис створюється з використанням засобу КЕП та базується на кваліфікованому сертифікаті відкритого ключа то такий підпис вважається кваліфікованим електронним підписом [3].

Метою статті є дослідження особливостей генерації та використання особистих ключів КЕП, що зберігаються у Хмарному сховищі кваліфікованих надавачів електронних довірчих послуг.

Об'єктом дослідження є сервіс Хмарного сховища кваліфікованого надавача електронних довірчих послуг.

Предмет дослідження – Хмарне сховище кваліфікованого надавача електронних довірчих послуг.

Аналіз попередніх досліджень. Дослідження процедури генерації, зберігаються та використання особистих ключів користувачів електронних довірчих послуг, вагоме значення мають дослідження присвячені вивченню електронного підпису (М. Вовк, І. Шепель, Ю. Горбенко, І. Горбенко. та ін.)

Виклад основного матеріалу. Особисті ключі електронного підпису користувачів електронних довірчих послуг можуть бути згенеровано на:

– Незахищений носій користувачів (USB накопичував, CD чи DVD диски та ін.);

– Захищені носії користувачів (Кристал-1, SECURE TOKEN-338, Алмаз-1К та ін.);

– Хмарне сховище кваліфікованого надавача електронних довірчих послуг.

Законодавством встановлені обмеження щодо генерації особистих ключів співробітниками державних органів, генерація здійснюється за особистої присутності працівника державної установи у кваліфікованого надавача електронних довірчих послуг з використанням засобів КЕП.

Також, представники державних органів повинні використовувати виключно кваліфіковані сертифікати відкритих ключів та захищені носії ключової інформації [4].

Деякі надавачі електронних довірчих послуг надають своїм клієнтам послугу дистанційного перевипуску кваліфікованих сертифікатів відкритих ключів, що полягає у формуванні нових кваліфікованих сертифікатів на певний термін (1–2 роки) без особистого відвідування надавача електронних довірчих послуг, у такому випадку ідентифікація користувача здійснюється за даними, що містяться у раніше сформованих сертифікатах відкритих ключів, при цьому здійснюється генерація нового особистого ключа КЕП [3].

У період дії воєнного стану в Україні та протягом місяця з дня його скасування надавачі електронних довірчих послуг можуть здійснювати автоматичний перевипуск кваліфікованих сертифікатів відкритих ключів користувачів без їх особистої присутності. При автоматичному формуванні нових кваліфікованих сертифікатів відкритих ключів генерація нового особистого ключа КЕП не здійснюється, а термін дії скасованого та нового сформованого сертифікатів не повинен перевищувати три роки.

Також, на період воєнного стану та протягом шести місяців з дня його припинення дозволяється використання електронних підписів чи печаток, що базуються на кваліфікованому сертифікаті відкритого ключа без відомостей про те, що особистий ключ зберігається на захищеному носію ключової інформації, окрім випадків передбачених абзацом другим частини другої статті 17 Закону України «Про електронні довірчі послуги» [5].

Перелік надавачів, що здійснюють надання кваліфікованих електронних довірчих послуг зазначається у Довірчому списку, що розміщується на офіційному вебсайті Центрального засвідчувального органу (Міністерство цифрової трансформації України), який здійснює його впровадження та підтримує в актуальному стані (https://czo.gov.ua/trustedlist).

Крім цього, Національний банк України, як засвідчувальний центр, формує та підтримує в актуальному стані відповідний Довірчий список кваліфікованих надавачів електронних довірчих послуг (банків, операторів платіжних систем та організацій, що здійснюють свою діяльність на ринку фінансових послуг та інших) [3].

На вебсайті Центрального завідчувального органу реалізовано сервіс Інструменту моніторингу (https://czo.gov.ua/tool), який дає можливість сформувати тестові сертифікати відкритих ключів для здійснення випробування їх функціонування в різних інформаційно-комунікаційних системах [6].

Хмарний КЕП – це одна з послуг, що може надаватися кваліфікованими надавачами електронних довірчих послуг. На даний час в України тільки деякі кваліфіковані надавачі електронних довірчих послуг реалізували даний сервіс для своїх клієнтів. Їх перелік можливо переглянути скориставшись послугою підпису даних чи автентифікації найпопулярніших надавачів електронних сервісів, наприклад Електронний кабінет Державної податкової служби України (рис. 1).

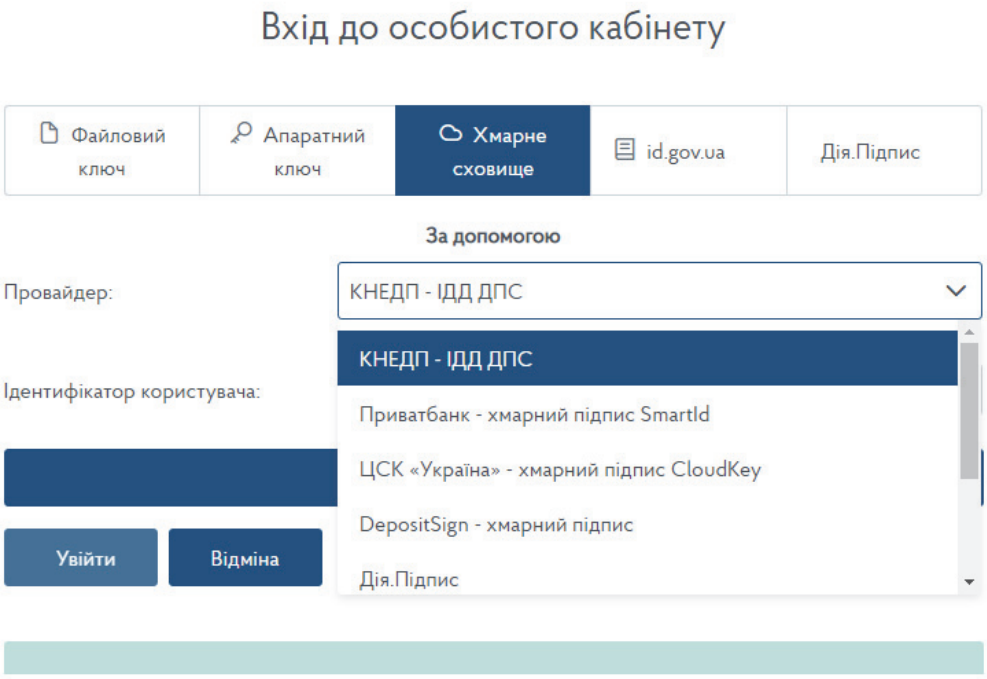


Рис. 1. Перелік кваліфікованих надавачів електронних довірчих послуг

Також, слід розглянути Інтегровану систему електронної ідентифікації id.gov.ua (далі – Сервіс id.gov.ua), що надає можливість здійснити електронну ідентифікацію за допомогою Хмарного КЕП більш ніж на 380 системах автентифікації (рис. 2).

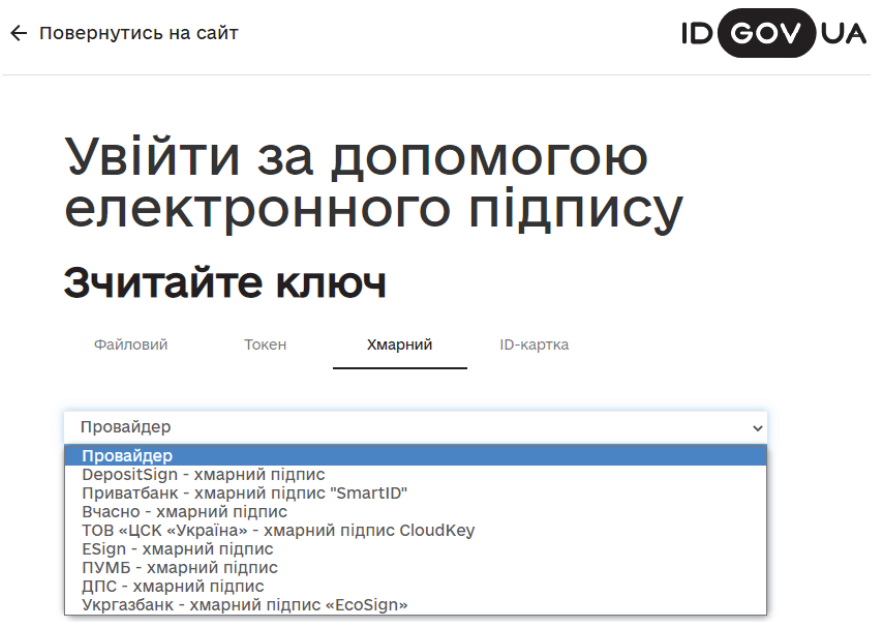


Рис. 2 Інтегрована система електронної ідентифікації

Скориставшись оцінкою стану розвитку сфери електронних довірчих послуг за 2022 рік, що публікується на офіційному вебсайті Центрального засвідчувального органу (Таб. 1), можна визначити, які саме кваліфіковані надавачі електронних довірчих послуг користуються найбільшим попитом серед клієнтів [7].

Таблиця 1

Кількість сформованих сертифікатів

Кількість сформованих кваліфікованих сертифікатів електронних підписів (без урахування сертифікатів шифрування) за 2022 рік		
Надавач	Усього	Активні
КНЕДП АЦСК АТ КБ «ПРИВАТБАНК»	6 849 563	6 592 641
КНЕДП «ДІЯ»	5 205 525	2 896 064
КНЕДП ТОВ «Центр сертифікації ключів Україна»	748 717	1 068 675
КНЕДП ДПС	511 364	887 668
КНЕДП АЦСК АТ «Державний ощадний банк України»	132 506	327 257
КНЕДП АТ «УКРСИББАНК»	55 354	148 256
КНЕДП Державної казначейської служби України	74 509	125 295
КНЕДП ДП «УСС»	11 180	130 125
КНЕДП «MASTERKEY»	67 540	64 479
КНЕДП - АЦСК МВС України	29 811	95 044
АТ «СЕНС БАНК»	58 122	53 289
ПАТ АБ «УКРГАЗБАНК»	30 855	28 525
КНЕДП органів прокуратури України	31 336	26 176
КНЕДП ЦСК АТ «УКРЗАЛІЗНИЦЯ»	31 718	21 168
АТ «ПУМБ»	22 176	21 038
КНЕДП ТОВ «ДЕПОЗИТ САЙН»	18 940	19 253
КНЕДП «Військова частина 2428»	11 351	16 271
КНЕДП «eSign»	12 001	14 346
КНЕДП «Центр сертифікації ключів Збройних Сил України»	9 860	8 515

Кількість сформованих кваліфікованих сертифікатів електронних підписів (без урахування сертифікатів шифрування) за 2022 рік		
Надавач	Усього	Активні
КНЕДП ТОВ «Вчасно Сервіс»	4 483	4 110
АЦСК Національного банку України	1 883	4 919
АТ «БАНК АЛЬЯНС»	1 710	1 501
КНЕДП «АЦСК ринку електричної енергії»	271	420
АТ «КРЕДІ АГРІКОЛЬ БАНК»	156	129
Засвідчувальний центр	18	38
КНЕДП ЦЕЗАІС ТОВ «ІНТЕР-МЕТЛ»	7	0

Проаналізувавши інформацію можна виділити трьох надавачів, що надають послугу Хмарного КЕП та користуються найбільшим попитом серед клієнтів:

1. Кваліфікований надавач електронних довірчих послуг АЦСК АТ КБ «ПРИВАТБАНК»;
2. Кваліфікований надавач електронних довірчих послуг «ДІЯ»;
3. Кваліфікований надавач електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна».

Розглянемо детальніше процедуру генерації особистого ключа у Хмарному сховищі та формування кваліфікованого сертифіката відкритого ключа на прикладі Кваліфікований надавач електронних довірчих послуг «ДЕПОЗИТ САЙН» (далі – Надавач «ДЕПОЗИТ САЙН») (https://ca.depositsign.com).

Для початку необхідно зареєструватися у особистому кабінеті Надавача «ДЕПОЗИТ САЙН» та заповнивши відповідну форму (https://cabinet.depositsign.com/register) (рис. 3).

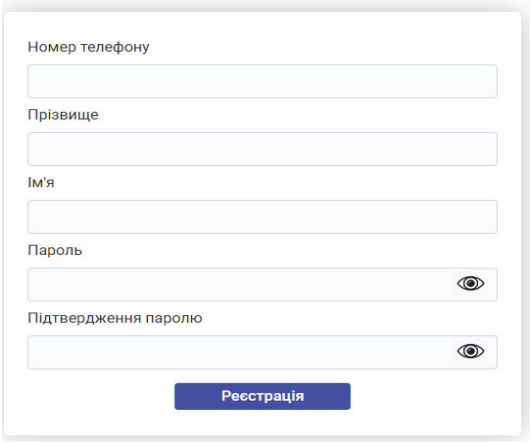


Рис. 3. Форма реєстрації

Підтвердити реєстрацію, зазначивши у відповідному полі код реєстрації, що направляється повідомленням на вказаний номер телефону (рис. 4).

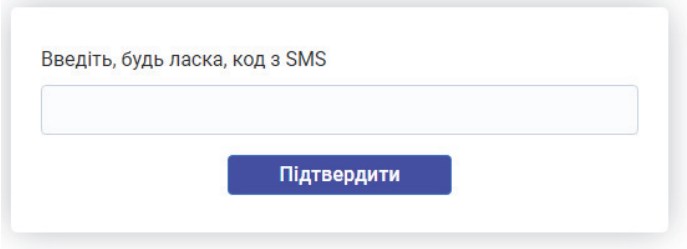


Рис. 4. Форма підтвердження реєстрації

Здійснити авторизацію та натиснути «Сформувати заявку» (рис. 5).

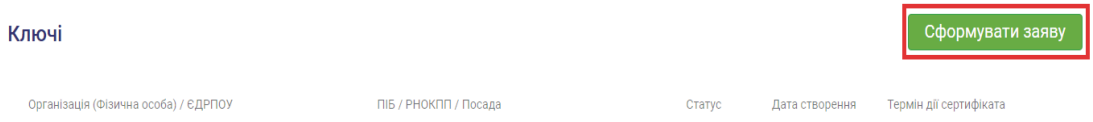


Рис. 5 Формування заявки

Заповнити відповідні поля у заявці та натиснути «Зберегти» (рис. 6).

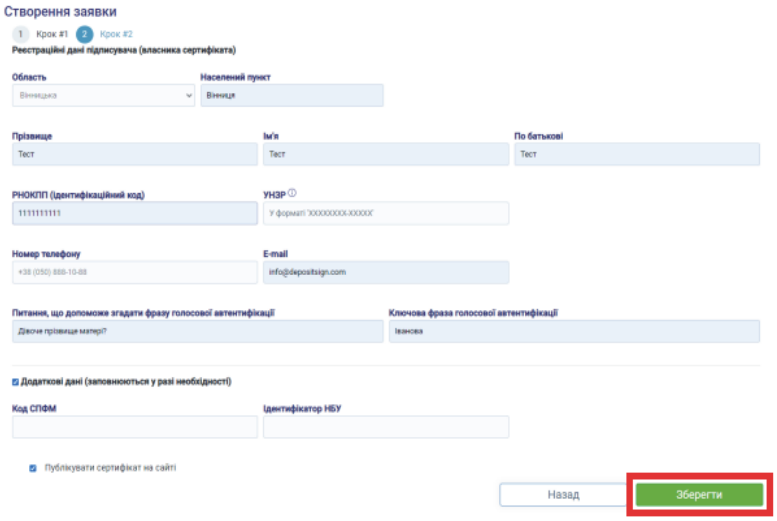


Рис. 6 Формування заявки

Здійснити генерацію особистого ключа КЕП. Після генерації в особистому кабінеті сформується обліковий запис хмарного підпису.

Для формування кваліфікованих сертифікатів відкритих ключів необхідно підготувати відповідний перелік документів та особисто звернутися до представництва Надавача «ДЕПОЗИТ САЙН» для здійснення ідентифікації користувача електронних довірчих послуг.

Розглянемо процедуру підписання електронного документу з використанням особистого ключа що зберігається у Хмарному сховищі Надавача «ДЕПОЗИТ САЙН» у Сервісі id.gov.ua:

1. Обираємо «Підпис файлів» (https://id.gov.ua/sign);
2. Натискаємо «Електронний підпис» та обираємо тип носія, з якого буде зчитано особистий ключ і зазначаємо кваліфікованого надавача електронних довірчих послуг та вводимо Ідентифікатор користувача (рис. 7).

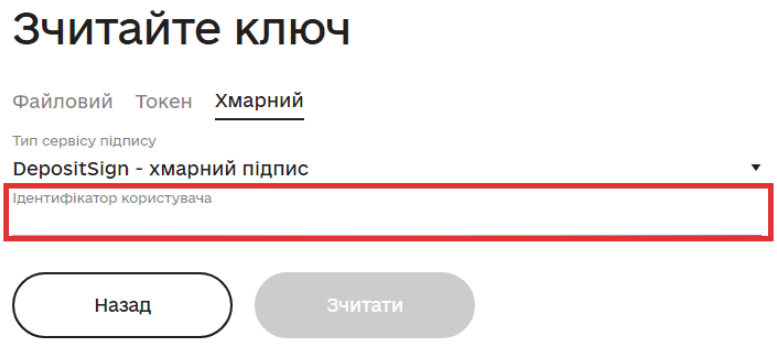


Рис. 7. Формування зчитування ключа

3. Під час зчитування особистого ключа на Ваш смартфон, у додаток «DepositSign» надійде PUSH-повідомлення з посиланням, за яким необхідно перейти для обрання особистого ключа який буде використовуватись для авторизації та підтвердити його використання (рис. 8);

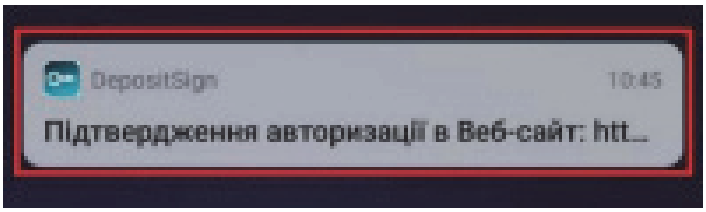


Рис. 8. Формування сповіщення

4. У Сервіс id.gov.ua необхідно перевірити особисті дані та натиснути «Далі» (рис. 9);

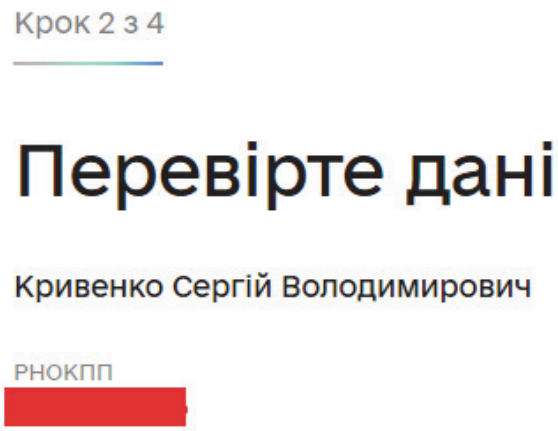


Рис. 9. Формування перевірки даних

5. Обираємо спосіб підписання та файл який необхідно підписати та натискаємо «Підписати» (рис. 10);

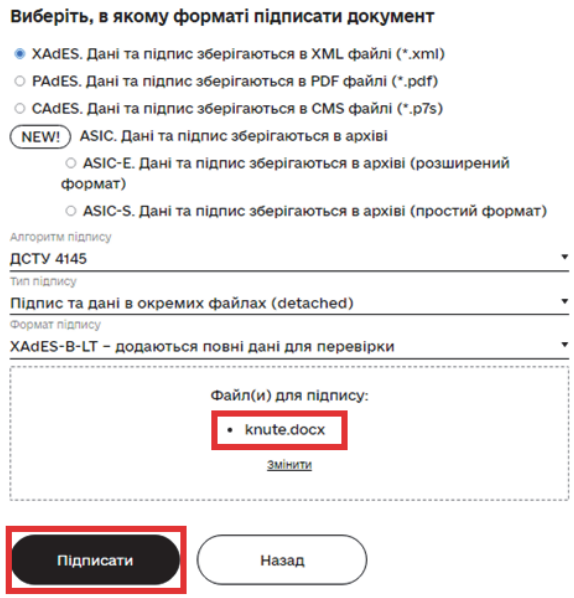


Рис. 10 Формування підпису та зберігання

6. У додаток «DepositSign» надійде PUSH-повідомлення, за яким необхідно перейти для обрання особистого ключа який буде використовуватись для підпису електронного документу;

7. Завантажуємо підписаний електронний документ (рис. 11);

Рис. 11. Формування завантаження підписаного документу

Висновки. За умови використання особистого ключа, що зберігається у Хмарному сховищі кваліфікованого надавача електронних довірчих послуг, сертифікат, що сформується буде містити відмітку про те, що особистий ключ, який відповідає відкритому ключу збережено у засобі КЕП. Такий спосіб зберігання особистого ключа дозволяє уникнути його викрадення, пошкодження чи втрати. КЕП, який сформований з використанням особистого ключа, що зберігається у Хмарному сховищі кваліфікованого надавача електронних довірчих послуг повністю відповідає всім вимогам законодавства України у сфері електронних довірчих послуг.

Список використаних джерел

1. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV. – Режим доступу: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=851-15#Text. – Назва з екрана.
2. Горбенко І. Д., Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: Монографія. – Видавництво «Форт», 2010. – 608 с.
3. Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text. – Назва з екрана.
4. Порядок використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності: Постанова Кабінету Міністрів України від 19.09.2018 № 749. – Режим доступу: https://zakon.rada.gov.ua/laws/show/749-2018- %D0 %BF#Text. – Назва з екрана.
5. Деякі питання забезпечення безперебійного функціонування системи надання електронних довірчих послуг: Постанова Кабінету Міністрів України 17.03.2022 № 300. – Режим доступу: https://zakon.rada.gov.ua/laws/show/300-2022- %D0 %BF#Text. – Назва з екрана.
6. Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг: Наказу Міністерства цифрової трансформації України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30.09.2020 № 140/614. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z1039-20#Text. – Назва з екрана.
7. Центральний засвідчувальний орган Міністерство цифрової трансформації України. URL: https://czo.gov.ua/development?tab=1 (дата звернення: 28.03.2023).

Робота виконана під науковим керівництвом доцента
ВЛАСЕНКО Л. О.

ПОЛІТИКА БЕЗПЕКИ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

КРИВОРОТ М., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто питання політики безпеки конфіденційної інформації на підприємстві, зокрема визначення основних принципів захисту конфіденційної інформації, встановлення відповідальності працівників за її збереження та методи захисту конфіденційної інформації. Досліджено ризики, які пов'язані з неякісним захистом конфіденційної інформації. Описано процедуру створення політики безпеки конфіденційної інформації на підприємстві, що допоможе забезпечити безпеку даних та захистити їх від несанкціонованого доступу та від можливих загроз.

The article deals with the issues of confidential information security policy at an enterprise, in particular, defining the basic principles of confidential information protection, establishing the responsibility of employees for its preservation and methods of confidential information protection. The risks associated with poor protection of confidential information are investigated. The procedure for creating a security policy for confidential information at an enterprise is described, which will help ensure data security and protect it from unauthorized access and possible threats.

Актуальність. Актуальність політики безпеки конфіденційної інформації на підприємстві визначається значущими загрозами, які існують у сфері захисту даних та інформації. Зокрема, зростають кібератаки, вірусні атаки, крадіжки даних та інші загрози, які можуть спричинити серйозні наслідки для діяльності підприємства. Крім того, підприємства повинні дотримуватися законодавства щодо захисту конфіденційної інформації, зокрема згідно зі Законом України «Про захист персональних даних» та іншими нормативними документами. Тому розробка і виконання політики безпеки конфіденційної інформації на підприємстві є важливим заходом для забезпечення захисту конфіденційної інформації та зменшення ризиків втрати даних.

Таким чином, розробка та впровадження політики безпеки конфіденційної інформації на підприємстві є актуальною та необхідною умовою забезпечення стійкої та ефективної діяльності підприємства в умовах зростаючих загроз захисту даних та інформації.

Метою статті є дослідження питання політики безпеки конфіденційної інформації на підприємстві та визначення параметрів, які необхідно враховувати для безпеки конфіденційної інформації на підприємстві.

Об'єктом дослідження є процес захисту конфіденційної інформації від несанкціонованого доступу, збереження цілісності та конфіденційності інформації, а також визначення відповідальності працівників за збереження конфіденційної інформації.

Предметом дослідження є заходи, процедури та політики, що використовуються для захисту конфіденційної інформації в організації.

Аналіз попередніх досліджень. У більшості досліджень щодо захисту конфіденційної інформації на підприємствах зазвичай досліджується ефективність та раціональність політики безпеки конфіденційної інформації на підприємстві, оцінюються наслідки витоків інформації, а також визначаються можливі ризики, що пов'язані з використанням інформації в організації.

Більшість досліджень з цієї області зосереджені на проблемах технічного захисту інформації та використанні різних методів шифрування, проте не менш важливим є врахування людського фактору в безпеці інформації. Деякі дослідження акцентують увагу на питаннях психологічного навчання працівників та розробці процедур управління персоналом в цій області.

Одним зі заслужених дослідників в області захисту конфіденційної інформації є Брюс Шнайер, який є автором декількох книг на тему криптографії та захисту даних. У своїх дослідженнях він зосереджується на аналізі загроз та ризиків, пов'язаних з цифровою безпекою та захистом даних. Також, на цю тему було опубліковано декілька досліджень з боку міжнародних організацій, таких як Міжнародне агентство з атомної енергії (МАГАТЕ) та Європейський союз. У цих дослідженнях було визначено низку стандартів та рекомендацій з приводу захисту конфіденційної інформації на підприємствах [1].

Багато досліджень зосереджуються на визначенні рівня конфіденційності даних та видів інформації, що підпадають під захист, а також на розробці процедур та політик збереження конфіденційної інформації. Окремі дослідження присвячені правилам доступу до конфіденційної інформації, вимогам до користування електронною поштою та соціальними мережами, а також процедурам повідомлення про можливі порушення безпеки даних та визначенню способів ліквідації наслідків інциденту.

Виклад основного матеріалу. У сучасному цифровому світі, де інформація стала найціннішим активом, забезпечення безпеки конфіденційної інформації на підприємстві стає критично важливим завданням. В умовах зростаючих кіберзагроз, крадіжок даних та інших кібератак, розробка та впровадження ефективної політики безпеки стають необхідністю для збереження довіри клієнтів, збереження репутації підприємства та забезпечення стійкого розвитку.

Політика безпеки конфіденційної інформації відіграє роль надійного щита, що захищає не лише цифрові активи, а й репутацію та довіру до організації. Вона передбачає комплексний підхід до захисту даних від несанкціонованого доступу, витоку та порушень конфіденційності. У своєму суттєвому аспекті, політика безпеки охоплює не лише технічні аспекти, але й культурну складову, де всі співробітники беруть активну участь у формуванні безпечного інформаційного середовища.

У світлі постійно зростаючої комплексності кіберзагроз та вимог до захисту даних, розуміння політики безпеки конфіденційної інформації стає важливішим ніж будь-коли. Ця стаття намагатиметься прояснити сутність, важливість та ключові складові цієї політики, щоб сприяти зміцненню безпеки та надійності інформаційних ресурсів підприємства.

Захист конфіденційної інформації є критично важливим завданням для будь-якого підприємства, оскільки від його ефективності залежать не тільки фінансові показники, а й репутація компанії, її взаємовідносини з клієнтами та іншими стейкхолдерами. Проблематика захисту конфіденційної інформації на підприємствах полягає у тому, що незаконний доступ до такої інформації може призвести до витоку даних, крадіжки ідентифікаційних даних, шахрайства, розкриття комерційної таємниці, а також порушення різних законів, які регулюють обіг конфіденційної інформації.

Підприємства повинні бути готові до захисту конфіденційної інформації, що збирається, обробляється та зберігається у їхніх інформаційних системах. Проте, на жаль, багато підприємств не мають достатнього рівня знань та досвіду у цій галузі, що призводить до частих випадків порушення безпеки даних.

Для того, щоб забезпечити ефективний захист конфіденційної інформації на підприємствах, необхідно провести аналіз потенційних загроз та ризиків, розробити відповідні політики та процедури збереження конфіденційної інформації, визначити відповідальних осіб та розподіл обов'язків, встановити правила доступу до інформації та розробити програму навчання для співробітників щодо захисту конфіденційної інформації. Також важливо дотримуватись вимог законодавства та стандартів, що регулюють захист персональних даних та конфіденційної інформації. Ці терміни та поняття пов'язані з захистом конфіденційної інформації на підприємствах. Для забезпечення ефективного захисту конфіденційної інформації необхідно розуміти ці поняття та використовувати відповідні методи та інструменти, такі як шифрування, бекап, авторизація, ідентифікація та автентифікація, аудит тощо.

Навчання співробітників про правила доступу до конфіденційної інформації повинно бути включене до їх вступного навчання та регулярно повторюватися. Співробітники повинні бути свідомі про важливість конфіденційної інформації, про заходи, які повинні бути вжиті для її захисту, та про наслідки її можливої втрати чи неправомірного доступу.

Крім того, підприємство повинно визначити відповідальність за порушення правил збереження та доступу до конфіденційної інформації. Це може включати дисциплінарні заходи для співробітників, які порушують правила, а також відшкодування збитків, спричинених незаконним доступом до конфіденційної інформації. Для забезпечення ефективного захисту конфіденційної інформації, необхідно спочатку визначити рівень конфіденційності даних, тобто ступінь їх важливості та значимості для підприємства. Зазвичай використовуються три рівні конфіденційності даних [1]:

- Високий рівень конфіденційності – це дані, які можуть спричинити серйозні наслідки для підприємства, якщо вони потраплять в руки несанкціонованих осіб. Це можуть бути фінансові дані, персональні дані клієнтів, плани розвитку підприємства та інші важливі дані.
- Середній рівень конфіденційності – це дані, які можуть мати обмежений вплив на підприємство, якщо вони стануть відомі несанкціонованим особам. Це можуть бути, наприклад, інформація про продукти або послуги підприємства, інформація про роботу підприємства тощо.
- Низький рівень конфіденційності – це дані, які не мають значного впливу на підприємство, якщо вони потраплять в руки несанкціонованих осіб. Це можуть бути, наприклад, загальна інформація про підприємство, новини тощо [1, 2].

Після визначення рівня конфіденційності даних, необхідно визначити види інформації, що підпадають під захист. Це можуть бути такі види інформації, як: фінансові дані; персональні дані; комерційна інформація; плани розвитку підприємства; договори та угоди; конкурентна інформація; інтелектуальна власність.

Політика безпеки конфіденційної інформації на підприємстві має на меті забезпечення захисту важливих даних від несанкціонованого доступу, використання, розголошення, пошкодження та втрати. Ця політика передбачає встановлення системи заходів та процедур, які мають на меті запобігти загрозам, що можуть виникнути при обробці та зберіганні конфіденційної інформації.

Вимоги законодавства та стандартів є важливими компонентами в розробці політики безпеки конфіденційної інформації на підприємстві. Організації повинні дотримуватися різноманітних правил та норм, щоб забезпечити належний рівень захисту конфіденційної інформації та виконувати свої обов’язки перед клієнтами та партнерами. Одним з ключових документів є Закон України «Про захист персональних даних», який встановлює вимоги до обробки та захисту персональних даних громадян. Закон вимагає, щоб організації, які обробляють персональні дані, мали відповідні технічні та організаційні заходи для захисту цих даних. Закон також встановлює вимоги щодо зберігання та обмеження доступу до персональних даних.

Іншим документом є міжнародний стандарт ISO/IEC 27001, який встановлює вимоги до систем управління інформаційною безпекою. Стандарт містить вимоги щодо політики безпеки інформації, управління ризиками, захисту від несанкціонованого доступу та ведення журналів, сертифікації та аудиту систем управління інформаційною безпекою. Додатково, існують інші стандарти та регуляторні вимоги, які стосуються захисту конфіденційної інформації, такі як Payment Card Industry Data Security Standard (PCI DSS) для захисту платіжної інформації, або General Data Protection Regulation (GDPR) в Європейському Союзі, що встановлює вимоги до захисту персональних даних. Таким чином, вимоги законодавства та стандартів є важливими складовими політики безпеки конфіденційної інформації на підприємстві. Наприклад, є ряд законодавчих актів, які вимагають від підприємств забезпечувати високий рівень захисту конфіденційної інформації, таких як Закон України «Про захист персональних даних», Закон України «Про інформацію», Закон України «Про електронний підпис», тощо [2].

Також існують різні стандарти, наприклад, ISO/IEC 27001, які встановлюють вимоги до систем управління інформаційною безпекою та захисту інформації. У практиці, багато компаній використовують стандарти та рекомендації для розробки власних політик безпеки, або ж стежать за відповідністю своїх процедур та практик зазначеним вимогам.

Врахування вимог законодавства та стандартів є важливим елементом впровадження політики безпеки конфіденційної інформації, який допомагає забезпечити високий рівень захисту даних та уникнути можливих юридичних проблем. Окрім того, виконання вимог законодавства та стандартів допомагає встановити спільну базу знань та практик в галузі інформаційної безпеки, що сприяє розвитку цієї галузі та підвищенню її рівня.

Потенційні загрози та ризики – це можливі небажані події або дії, які можуть спричинити втрату конфіденційної інформації або порушення її конфіденційності. До потенційних загроз та ризиків можуть належати: кібератаки – хакери можуть намагатися зламати системи захисту даних на підприємстві і викрасти конфіденційну інформацію; внутрішні загрози – співробітники підприємства можуть ненавмисно або навмисно витікати конфіденційну інформацію, яка може завдати шкоди підприємству або його клієнтам; соціальний інжиніринг – зловмисники можуть використовувати соціальний інжиніринг, щоб отримати доступ до конфіденційної інформації; втрати даних – погане зберігання або резервне копіювання даних може призвести до втрати конфіденційної інформації; недосконаліть процедур – недосконаліть політики безпеки може призвести до неправильного зберігання чи обробки конфіденційної інформації, що призведе до викрадення чи витікання даних.

Розробка процедур та політик збереження конфіденційної інформації – це процес визначення і впровадження набору правил та процедур, які гарантують захист конфіденційної інформації від несанкціонованого доступу, використання або розголошення. Для розробки таких процедур та політик необхідно визначити рівень конфіденційності інформації та види інформації, що підпадають під захист, а також потенційні загрози та ризики, що можуть виникнути [3].

При розробці процедур та політик збереження конфіденційної інформації необхідно враховувати наступні аспекти:

- Доступ до конфіденційної інформації має бути обмеженим та контрольованим.
- Встановити процедури авторизації та ідентифікації користувачів, які мають право отримувати доступ до конфіденційної інформації.
- Визначити, які види інформації підпадають під захист та встановити заходи для забезпечення конфіденційності цих даних.
- Встановити процедури забезпечення захисту інформації від несанкціонованого доступу, використання та розголошення.
- Встановити процедури збереження інформації та регулярну перевірку на наявність вірусів, шкідливих програм, а також зберігати резервні копії даних.
- Встановити процедури утилізації конфіденційної інформації та надійного знищення даних після закінчення їх терміну зберігання.

Визначення відповідальних осіб та розподіл обов’язків є важливим елементом політики безпеки конфіденційної інформації на підприємстві. Це допомагає забезпечити ефективне управління ризиками та підвищити рівень захисту конфіденційної інформації.

Одним з основних відповідальних осіб є керівник підприємства або відповідний менеджер, який відповідає за розробку та впровадження політики безпеки конфіденційної інформації. Ця особа має визначати рівень конфіденційності даних та види інформації, що підпадають під захист, а також забезпечувати відповідний рівень захисту. До інших відповідальних осіб можуть відноситись керівники відділів, відповідальні за обробку та зберігання конфіденційної інформації, технічні спеціалісти, відповідальні за захист мережі та інфраструктури підприємства, та інші працівники, які мають доступ до конфіденційної інформації.

Розподіл обов’язків між відповідальними особами повинен бути чітко визначеним, зокрема стосовно забезпечення фізичного та логічного захисту інформації, здійснення процедур контролю доступу до інформації, забезпечення безпеки мережі та інфраструктури, а також забезпечення процедур повідомлення про можливі порушення безпеки даних та розслідування інцидентів.

Крім того, відповідальні особи повинні бути ознайомлені з політикою безпеки конфіденційної інформації та виконувати свої обов'язки відповідно до неї. Вони повинні знати, які дані вважаються конфіденційними, які процедури повинні бути виконані для захисту цих даних, як повідомляти про можливі порушення безпеки даних, і які наслідки можуть мати такі порушення. Розподіл обов'язків між відповідальними особами повинен бути чітко визначений, і кожна особа повинна мати ясний опис своїх обов'язків. Це допоможе забезпечити, що всі аспекти захисту конфіденційної інформації покриті та що відповідальні особи знають, які дії потрібно вживати у випадку порушення безпеки даних.

Обробка та зберігання конфіденційної інформації повинні відповідати вимогам законодавства та стандартам безпеки інформації. Основні вимоги щодо обробки та зберігання конфіденційної інформації можуть включати наступне: обмеження доступу до конфіденційної інформації; захист від несанкціонованого доступу, використання та розголошення; захист від вірусів та шкідливих програм; резервне копіювання даних; утилізація конфіденційної інформації; аудит доступу. Правила доступу до конфіденційної інформації повинні бути визначені у процедурах та політиках збереження конфіденційної інформації. Основні правила доступу до конфіденційної інформації на підприємстві повинні бути регулюванні політикою безпеки і можуть варіюватися залежно від типу і обсягу конфіденційної інформації. Однак деякі загальні правила, які повинні дотримуватися співробітниками, що мають доступ до конфіденційної інформації, включають наступне:

- Аутентифікація: перед тим, як дати доступ до конфіденційної інформації, необхідно переконатися, що користувач, що звертається до інформації, є дійсною особою, яка має право на доступ.
- Авторизація: після того, як була здійснена аутентифікація, користувачеві повинно бути дозволено або заборонено доступ до конфіденційної інформації в залежності від його ролі і функцій на підприємстві.
- Захист даних: конфіденційна інформація повинна зберігатися в безпечному місці з обмеженим доступом, захищеному паролем і шифруванням.
- Оновлення паролів: співробітники, які мають доступ до конфіденційної інформації, повинні оновлювати свої паролі на регулярній основі.
- Моніторинг доступу: необхідно вести журнали доступу до конфіденційної інформації та регулярно перевіряти їх на виявлення підозрілих дій.
- Навчання співробітників: співробітники підприємства повинні бути навчені правилам та процедурам зберігання та обробки конфіденційної інформації, а також підвищувати свою обізнаність щодо потенційних загроз та ризиків безпеки даних.

Під час теоретичного та практичного аналізу політики безпеки конфіденційної інформації на підприємстві були отримані наступні основні висновки [2, 3]:

- Конфіденційна інформація є важливим активом будь-якого підприємства, який потребує захисту від потенційних загроз та ризиків.
- Основні загрози та ризики для конфіденційної інформації на підприємстві пов'язані з несанкціонованим доступом, крадіжкою, втратою, пошкодженням, витоком або неправомірним використанням даних.
- Для забезпечення захисту конфіденційної інформації необхідно розробити та впровадити на підприємстві політику безпеки, яка має включати такі елементи, як розподіл доступу до інформації, шифрування, аутентифікацію та ідентифікацію користувачів, контроль доступу до мережі та інтернет-ресурсів, а також правила використання електронної пошти та соціальних мереж.
- Для забезпечення ефективності політики безпеки конфіденційної інформації необхідно проводити регулярні навчання співробітників підприємства з питань безпеки інформації, а також проводити аудит системи безпеки та вживати необхідні заходи для її покращення.

- Для ефективної реалізації політики безпеки конфіденційної інформації на підприємстві необхідна підтримка керівництва, яка полягає в призначенні відповідальної особи, яка буде відповідати за виконання політики безпеки.

Процедури повідомлення про можливі порушення безпеки даних важливі для того, щоб оперативно виявляти, реагувати та запобігати потенційним загрозам безпеці даних в організації. Опис загальних процедур повідомлення про можливі порушення безпеки даних включає:

- Встановлення каналів повідомлення: в організації повинен бути встановлений канал повідомлення про можливі порушення безпеки даних, такий як електронна пошта, телефонна лінія підтримки або спеціальна онлайн-форма.
- Створення процедур повідомлення: необхідно розробити процедури, які визначають, які дані повинні бути включені в повідомлення про можливі порушення безпеки даних, як швидко повідомлення має бути зроблено та кому повідомлення повинно бути адресовано.
- Своєчасне повідомлення: персонал повинен бути навчений, як повідомляти про можливі порушення безпеки даних та негайно повідомляти відповідні служби.
- Аналіз порушення безпеки даних: служба безпеки повинна аналізувати отримані повідомлення та вживати відповідних заходів для запобігання подібних випадків у майбутньому.
- Інформування сторонніх осіб: у разі порушення безпеки даних, яке може вплинути на сторонніх осіб, необхідно повідомити їх про це та надати необхідну інформацію.
- Збереження записів: організація повинна зберігати записи про повідомлення про можливі порушення безпеки даних та вжиті заходи для їх усунення.

Ці процедури повинні бути регулярно оглядати та оновлювати з метою врахування змін у середовищі та загрозах безпеці даних. Перевірка і оновлення процедур повинні проводитись не рідше одного разу на рік або частіше, якщо з’являються нові загрози або змінюються умови використання даних. Крім того, процедури повідомлення про можливі порушення безпеки даних повинні бути чітко визначені та доступні всім користувачам і співробітникам організації. Всі співробітники повинні бути навчені, як діяти у випадку виявлення можливого порушення безпеки даних та куди повідомляти про це [1, 3].

Розслідування та оцінка ризиків пов’язаних з порушенням безпеки даних є важливим етапом у процесі збереження конфіденційної інформації. Це дозволяє визначити причину порушення та прийняти необхідні заходи для запобігання подібних ситуацій у майбутньому. При розслідуванні порушення безпеки даних слід виконувати такі кроки:

- Визначення масштабів порушення: необхідно визначити, яка кількість даних була скомпрометована, чи були викрадені фінансові дані, персональні дані або інші конфіденційні дані.
- Виявлення причини порушення: необхідно визначити, яким чином відбулося порушення. Чи була порушена процедура збереження даних, чи була допущена помилка працівником, чи була використана нещодавно виявлена вразливість системи безпеки.
- Встановлення наслідків порушення: необхідно визначити, які наслідки можуть бути для компанії та її клієнтів.
- Вжиття необхідних заходів для запобігання подібних ситуацій у майбутньому: на основі отриманих даних необхідно вжити необхідних заходів для запобігання подібних ситуацій у майбутньому.

Визначення способів ліквідації наслідків інциденту є важливою складовою політики безпеки конфіденційної інформації. Це означає, що організація повинна мати план дій у випадку, якщо станеться інцидент з конфіденційною інформацією. План повинен бути регулярно переглядовий та оновлюваний, щоб відповідати змінам в організації та змінам у загрозах безпеки інформації та повинен включати: визначення виду інциденту та його серйозності; визначення осіб, які повинні бути повідомлені про інцидент, включаючи

внутрішніх спеціалістів з безпеки і зовнішніх фахівців, якщо це необхідно; визначення кроків, які повинні бути прийняті для ліквідації інциденту; визначення термінів, у які необхідно повідомити про інцидент і провести його ліквідацію; визначення кроків, які повинні бути прийняті після ліквідації інциденту, щоб запобігти подібним інцидентам у майбутньому [3].

Для забезпечення ефективного захисту конфіденційної інформації на підприємстві можна рекомендувати наступні заходи: встановити політику безпеки конфіденційної інформації на підприємстві, яка має бути доступна для всіх співробітників і регулярно оновлюватися; ввести обов'язкову процедуру ознайомлення з політикою безпеки конфіденційної інформації для всіх нових співробітників і проводити її періодично для старих; встановити систему контролю доступу до конфіденційної інформації, яка повинна бути доступна лише обраним співробітникам, які мають потребу в такій інформації; забезпечити належний рівень захисту інформації на технічному рівні, зокрема шифруванням даних, встановленням брандмауерів та антивірусного програмного забезпечення; забезпечити охорону інформації на фізичному рівні, зокрема обмеженням доступу до приміщень, де зберігається конфіденційна інформація; забезпечити безпеку електронної пошти та соціальних мереж, встановивши обмеження на використання особистих аккаунтів для робочих цілей та шифруванням електронних листів; здійснювати регулярний моніторинг систем безпеки та аудит інформаційної безпеки на підприємстві; проводити навчання та тренінги для співробітників з питань інформаційної безпеки, включаючи засоби виявлення та запобігання соціальному інжинірингу.

Висновки. Для забезпечення безпеки конфіденційної інформації на підприємстві необхідно враховувати багато параметрів, таких як типи даних, їх обсяг, рівень доступу до інформації, рівень конфіденційності інформації , вимоги до зберігання та передачі даних, потенційні загрози та ризики, кваліфікацію персоналу, систему контролю доступу, відповідність нормативно-правовим вимогам тощо. Ці параметри повинні бути враховані у процесі розробки та впровадження системи захисту конфіденційної інформації на підприємстві. Дотримання відповідних параметрів дозволить забезпечити ефективний захист конфіденційної інформації на підприємстві та запобігти її витоку. Помітно, що забезпечення безпеки конфіденційної інформації на підприємстві є важливим елементом забезпечення безпеки в цілому, оскільки викриття такої інформації може призвести до значних матеріальних і моральних збитків для підприємства, його клієнтів та партнерів.

Список використаних джерел

1. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.
2. Ортинський, В. Л. Економічна безпека підприємств, організацій та установ // Режим доступу: http://westudents.com.ua/glavy/16530-model-pobudovi-sistemi-nformatsyno-bezpeki.html (останнє звернення 12.04.2023р.).
3. Мохнюк А.М., Скорук О.В. Організація та управління інформаційною безпекою на підприємстві: конспект лекцій / Укладачі А.М. Мохнюк, О.В. Скорук. – Луцьк: ПП «Поліграфія», 2017. – 99 с.

Робота виконана під науковим керівництвом старшого викладача
КОСТЮК Ю. В.

МОДЕЛЬ ІНТЕРАКТИВНОЇ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ВІДЕОЗВ'ЯЗКУ

КРИКЛЯ В., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади побудови та функціонування моделі інтерактивної системи забезпечення відеозв'язку. Зазначено переваги впровадження систем відеозв'язку та розглянуто типові рішення щодо цього питання.

The article deals with the basic principles of construction and functioning of the model of the interactive video communication system. Let's note the advantages of implementing a video system and some typical solutions to this issue.

Актуальність. Система відеозв'язку є потужним інструментом в комунікаційному арсеналі будь-якої компанії. Відеозв'язок дозволяє істотно економити на відрядженнях співробітників і проводити ділові переговори, наради та семінари в режимі реального часу в стінах офісу. Сучасні рішення відеозв'язку, що володіють функціональністю систем високого класу і доступністю простого телефону, істотно розширюють можливості бізнес-комунікацій. Відеозв'язок дозволяє додати до засобів передачі даних і голосу обмін візуальною інформацією.

Метою статті є дослідження особливостей використання моделі інтерактивної системи забезпечення відеозв'язку та створення моделі класів.

Об'єктом дослідження є розробка інтерактивної системи забезпечення відеозв'язку.

Предмет дослідження - модель інтерактивної системи забезпечення відеозв'язку.

Аналіз попередніх досліджень. Дослідженням моделей інтерактивної системи забезпечення відеозв'язку присвячені праці вітчизняних та закордонних науковців: Вікторія Мізюк, Олександр Коваленко, Томас Могі та Аліна Румі.

Виклад основного матеріалу. Розробка програмного забезпечення для відеоконференцій знаходиться на піку розвитку. Причина – підвищений попит на засоби віддаленої співпраці. Людям потрібно продовжувати спілкуватися і працювати, а платформи, що забезпечують відеозв'язок стали, альтернативою спілкуванню в реальному житті.

Ринок програмного забезпечення для відеоконференцій розширюється шаленими темпами. У 2022 році його оцінювали в 25 мільярдів доларів, згідно з іноземними дослідженнями. До 2032 року прогнозується, що він досягне 95 мільярдів доларів.

Існує ряд переваг впровадження системи відеозв'язку, а саме: оптимізація бізнес-процесів, підвищення лояльності клієнтів та співробітників компаній, а також економія їх часу, підвищення ефективності бізнесу.

Відеозв'язок забезпечує:

- проведення презентацій та одночасну роботу з документами учасників;
- оперативність прийняття рішень в надзвичайних ситуаціях;
- ухвалення більш обгрунтованих рішень за рахунок залучення сторонніх експертів;
- швидке і ефективне розподілення ресурсів;
- ефект спілкування співрозмовників в одній кімнаті;
- дистанційне навчання.

Перш ніж почати процес розробки, Необхідно визначити тип майбутнього програмного забезпечення, дані наведені у таблиці 1.

Таблиця 1

Типи платформ для відеоконференцій

Тип	Опис	Переваги	Недоліки
Платформи для відеоконференцій	Ці платформи забезпечують відеоконференції, функції обміну повідомленнями та записи екрану. Крім того, деякі з них мають зовнішню інтеграцію для керування зустрічами	Ці платформи не потребують багато ресурсів, оскільки вони адаптуються до пристроїв користувачів і можливостей Інтернету. Зазвичай вони підтримують до 50 учасників конференції одночасно	Вони можуть не відповідати корпоративним потребам деяких компаній, тому не є найкращим варіантом для віддаленої роботи
Месенджери	Це такі месенджери, як Facebook, Telegram, WhatsApp і Facetime/iMessage від Apple, які мають функцію відеочату	Окрім швидкого обміну повідомленнями, вони надають різні можливості для відеочатів. Деякі з месенджерів дозволяють поєднувати дзвінки зазвичай для 2–30 осіб. Деякі застосовують технології AR/VR, щоб дозволити користувачам використовувати спеціальні маски та анімацію	Месенджери служать додатковим інструментом спілкування для віддалених співробітників, але не можуть замінити програмне забезпечення для відеоконференцій і онлайн-рішення для співпраці
Програмне забезпечення для онлайн-спільної роботи	Відеоконференції – не єдиний варіант для компаній, яким потрібна віддалена співпраця. Вони вимагають належного підключення, яке покриває всі корпоративні потреби, що пропонує цей тип програмного забезпечення	Онлайн-інструменти для співпраці пропонують розширені функції, включаючи обмін повідомленнями, відео- та аудіодзвінки, обмін документами, інтеграцію зовнішніх інструментів, таких як Jira та Google Calendar, і групові канали	Багато рішень на ринку забезпечують ту саму функціональність, що й Microsoft Teams і G-Suite, але все-таки вони побудовані по-різному
Розважальні платформи	Відеочати використовуються не тільки для роботи, але й для відпочинку. Розваги з друзями чи відеоігри стали стандартом для таких розважальних платформ, як Discord	Ці платформи дозволяють грати в ігри, влаштовувати відеоконференції, транслювати улюблені ігри та проводити групові та приватні чати	Ці платформи зазвичай не підходять для роботи, а лише для розваг

Етапи створення програмного забезпечення для відеозв’язку:

1. Визначення вимог. По-перше, потрібно зрозуміти цільову аудиторію. По-друге, розглянути всі можливі варіанти використання платформи. Скласти їх список, щоб команда краще зрозуміла вимоги.

2. Формування команди. Цей пункт включає в себе пошук команди. Від кількості членів команди буде залежати швидкість розробки.

3. Розробка шаблону інтерфейсу. Дозволить оцінити потенційні випадки використання та зручність використання програмного забезпечення. Від інтерфейсу буде залежати успішність додатку, якщо інтерфейс буде незручний, то додатком не будуть користуватись.

4. Backend розробники. Розробники бекенда відповідають за побудову серверної логіки, впровадження відео та протоколів безпеки та підключення всіх необхідних API. Останній використовується для зовнішньої інтеграції програмного забезпечення, наприклад, платіжних шлюзів або хмарних сервісів.

5. Розробники інтерфейсу. Розробники інтерфейсу відповідальні за створення остаточного вигляду спеціального програмного забезпечення для відеоконференцій. Вони отримують усі проекти та макети та впроваджують їх як окремі робочі елементи на платформі.

6. Дизайнери. Вони розробляють макети та передають їх команді розробників інтерфейсу.

7. QA спеціалісти. Команда із забезпечення якості проводить ручне тестування програмного забезпечення. Якщо спеціалісти з контролю якості виявлять будь-які помилки, вони миттєво повідомлять розробників, щоб вони їх виправили. Контроль якості дозволяє уникнути критичних проблем до випуску.

8. Керівник проекту. Керівники проекту - це ключові люди. Вони також можуть надавати оновлення та пропозиції щодо покращення проекту.

9. DevOps. Інженери DevOps об’єднують всі елементи, які складають проект, налаштовують та розгортають програмного забезпечення. Вони знають специфіку програмістів, тестувальників, системних адміністраторів і допомагають спростити їх роботу.

10. Архітектор рішень. Архітектори рішень надають команді технічну документацію, стандарти та робочі процеси для створення єдиного продукту.

11. Технічний стек. Стек технологій для платформ може відрізнятися залежно від потреб і вимог. Інтерфейс: Adobe Photoshop, figma, HTML, CSS, JavaScript, Redux, React Native, Angular. Backend: c#, Java, Python, NodeJs. Бази даних: MySQL, PostgreSQL, MongoDB, RethinkDB. Розгортання програмного забезпечення: TeamCity, GitLab. Особливу увагу слід виділити захисту даних, шифруванню та відео протоколам.

Основні характеристики програмного забезпечення для відеоконференцій наведено на рис. 1.

Рис. 1. Основні характеристики програмної платформи відеоконференції

Опис основних характеристик програмної платформи відеоконференції:

- Реєстрація. Дозволить користувачам реєструватися у внутрішній системі та отримувати ідентифікатор. Процес реєстрації повинен мати простий інтерфейс. Також можем підключити сторонні API, такі як Facebook Login і Google Sign-In, щоб забезпечити швидкий доступ до платформи.

- Обмін повідомленнями. Дозволить людям спілкуватися без відеодзвінків та обмінюватися текстовими повідомленнями під час дзвінка або навіть без нього.
- Профіль користувача. Є обов'язковими для платформ відеоконференцій. Вони містять основну інформацію, як-от ім'я, номер телефону, адресу електронної пошти, посаду та дату народження.
- Сповіщення. Ця функція використовується для сповіщення користувачів про майбутні події або вхідні дзвінки та повідомлення.
- Список контактів. Користувачі повинні мати можливість знаходити інших людей. Платформа має містити пошук за телефоном, іменем або електронною поштою. Можем застосувати додаткові API від Microsoft, Google або будь-якої внутрішньої системи для автоматизованої синхронізації контактів.
- Приватні дзвінки. Є ключовою функцією платформи. Повинен мати простий інтерфейс із аудіо- та відеодзвінками. Користувачі повинні мати доступ до вимкнення мікрофонів або камер і бачити імена один одного.
- Групові дзвінки. Подібний до попереднього з кількома новими функціями. По-перше, повинен бути власник, який може контролювати кімнату. Він може вимкнути звук учасників або дозволити ділитися екранами. У кімнаті також має бути список контактів для запрошення інших учасників.
- Управління даними. Це блок, який можна побачити на стартовому екрані, який вказує на майбутні дзвінки. Існує також можливість інтеграції із зовнішніми календарями для призначення зустрічей.
- Спільний доступ до екрана. Використовується для демонстрації вмісту вашого екрана. Спільний доступ до екрана стане в нагоді під час семінарів, вебінарів і оглядів. Крім того, користувачі можуть вибрати програми, якими вони хочуть поділитися.
- Спеціальний фон. Дозволить вашим користувачам замінити свій фон на власні зображення. Ця функція може бути корисною для досягнення конфіденційності та маркетингових цілей, якщо ви плануєте спілкуватися з клієнтами

Для реалізації поданих вище характеристик необхідно створити відповідні класи, до яких належать:

1. Клас «користувач» має такі поля: ідентифікатор: «Snowflake»; ім'я: рядок; дискримінатор: рядок; аватар: рядок; бот: логічне значення; прапори: ціле число; тип преміуму: ціле число; багатофакторна автентифікація: логічне значення; локаль: рядок; перевірений: логічне значення; електронна пошта: рядок.
2. Клас «підключення» має такі поля: ідентифікатор: рядок; назва: рядок; тип: рядок; скасовано: логічне значення; інтеграції: масив.
3. Клас «сервер» має такі поля: ідентифікатор: «Snowflake»; ім'я: рядок; значок: рядок; власник: логічне значення; ідентифікатор власника: «Snowflake»; дозволи: ціле число; регіон: рядок; канали: масив; учасники: масив.
4. Клас «канал» має такі поля: ідентифікатор: «Snowflake»; тип: рядок; унікальний ідентифікатор: «Snowflake»; позиція: ціле число; дозвіл перезапису: масив; ім'я: рядок; тема: рядок; «nsfw»: логічне значення; останній ідентифікатор повідомлення: «Snowflake»; обмеження користувача: ціле число; обмеження швидкості на користувача: ціле число; одержувачі: масив; значок: рядок; ідентифікатор власника: : «Snowflake».
5. Клас «запросити» має такі поля: код: рядок; сервер: сервер; канал : канал; приблизна кількість присутніх: ціле число; приблизна кількість учасників: ціле число.
6. Клас «вкладення» має такі поля: ідентифікатор: «Snowflake»; ім'я фалу: рядок; розмір: ціле число; адреса веб-сторінки: рядок; проксі адреси веб-сторінки: рядок; висота: ціле число; ширина: ціле число.
7. Клас «повідомлення» має такі поля: ідентифікатор: «Snowflake»; ідентифікатор каналу: «Snowflake»; автор: «Snowflake»; контент: рядок; позначка часу: позначка часу; відредагована позначка часу: позначка часу; перетворення тексту в мовлення: логічне

значення; вкладення: масив; вбудовані: масив; реакції: масив; згадати всіх: логічне значення; згадки: масив; ролі згадок: масив; закріпити: логічне значення; тип: ціле число.

8. Клас «вбудова» має такі поля: ідентифікатор: «Snowflake»; ім’я файлу: рядок; розмір: ціле число; адреса веб-сторінки: рядок; проксі адреси веб-сторінки: рядок; висота: ціле число; ширина: ціле число.

9. Клас «реакція» має такі поля: кількість: ціле число; я: логічне значення.

10. Клас «емодзі» має такі поля: ідентифікатор: «Snowflake»; ім’я: рядок; ролі: масив; вимагає двокрапки: логічне значення; керований: логічне значення; анімований: логічне значення.

Модель класів інтерактивної системи забезпечення відеозв’язку подано на рис. 2.

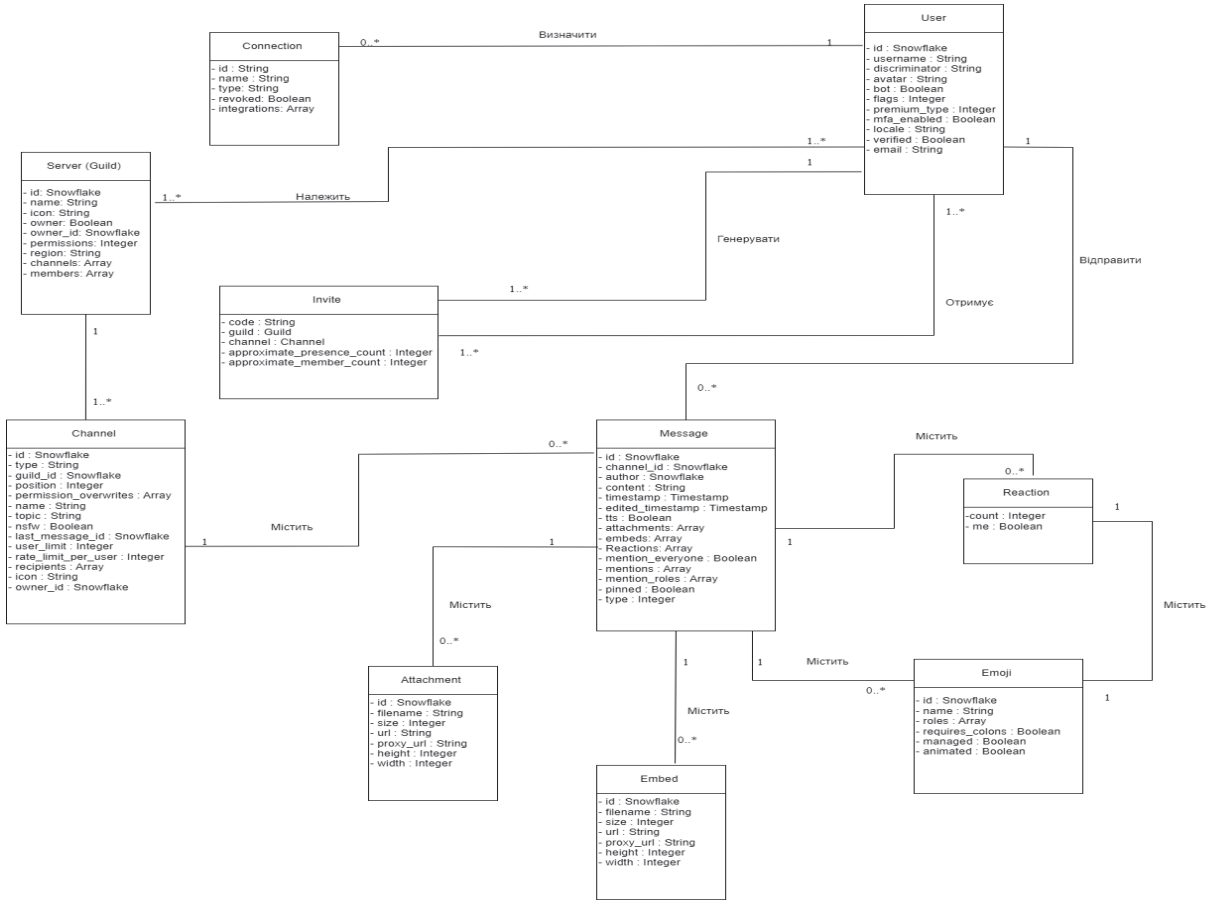


Рис. 2. Модель класів інтерактивної системи забезпечення відеозв’язку

Висновки. Отже, на сьогоднішній день системи забезпечення відеозв’язку – найпопулярніший вид бізнес-зв’язку. Система складається зі спеціального обладнання та програмного забезпечення, створює якісний відео та аудіо контакт між віддаленими учасниками. Те, для чого зовсім недавно потрібно було оформляти тижневе відрядження та летіти через океан, за допомогою системи відеозв’язку можна організувати за лічені хвилини. Саме тому розробка нових моделей забезпечення відеозв’язку є такою необхідною справою у сучасному світі. Було створено модель класів інтерактивної системи забезпечення відеозв’язку, яка є важливою в реалізації основних характеристик платформ відеозв’язку.

Список використаних джерел

1. 31 програмне забезпечення для відеоконференцій на 2023 рік // Режим доступу: https://www.ringcentral.com/us/en/blog/video-conferencing-software/ (останнє звернення 04.04.2023 р.)

2. Посібник із інтерактивної відеостатистики на 2022 рік // Режим доступу: https://tomislavhorvat.com/interactive-video-statistics/ (останнє звернення 04.04.2023р.)
3. Що таке інтерактивне відео? \\ Режим доступу: https://www.wyzowl.com/what-is-interactive-video/ (останнє звернення 04.04.2023 р.)

Робота виконана під науковим керівництвом канд. техн. наук, доцента
РЗАЄВОЇ С. Л.

НАВІГАЦІЙНІ СИСТЕМИ ТОРГОВО-РОЗВАЖАЛЬНИХ ЦЕНТРІВ ТА МОЖЛИВІСТЬ ЇХ ПОЄДНАННЯ З ТЕХНОЛОГІЯМИ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

КУБАТІН О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади побудови та функціонування навігаційної системи у Торгівельно розважальних центрах. Зазначено переваги застосування нових технологій, таких як доповнена реальність. Розглянуто як зразок типової навігаційної системи торговельно розважального центру додаток «River Mall».

The article considers the basic principles of construction and operation of the information and management system at retail enterprises. The advantages of using software products in the automation of a commercial enterprise are indicated. The «River Mall» application is considered as an example of a typical navigation system of a shopping and entertainment center.

Актуальність. Сфера людської діяльності торгівля, є однією з ключових для економічного розвитку регіону та країни в цілому. Саме це зумовлює швидкий розвиток інтеграції інформаційних технологій у процес економічної взаємодії між компаніями та остаточним споживачем. Для забезпечення ефективності економіки держави механізми взаємодії виробництва (пропозиції) і споживання (попиту) удосконалюються щороку, а інтеграція інформаційних технологій дедалі стає більш вагомою.

Ми можемо спостерігати як роздрібні торговельні мережі, з власною системою збуту товарів об’єднуються в великі торговельні центри, сумісно використовуючи спільну базу покупців. Така кооперація зумовлює більший попит та змогу привертати ще більше клієнтів до своїх товарів.

Зазвичай жоден магазин не в змозі викласти на прилавки весь асортимент товарів, які є в наявності, або покрити весь спектр потреб покупця. Також потрібно враховувати що кожний магазин має свою цільову аудиторію, і саме таке розташування надає змогу створити центри у яких люди можуть знайти майже всі групи товарів на будь-який смак та гаманець, та мають змогу відпочити.

Всі ці фактори зумовлюють ще більше зростання розмірів торговельно-розважальних центрів та обсяг магазинів які до нього входять. Кожен торговельний центр має свою специфічну архітектурну особливість і дедалі більше стає складніше орієнтуватись у самому центрі, особливо якщо ти маєш на меті знайти магазин конкретного виробника або групи товарів. Звичайно кожен торговельно-розважальний центр має інформаційні столи та електронні вказівники. Але не завжди ці засоби можуть дати людині вичерпне уявлення та інформацію щодо його запиту.

Через це ми дедалі більше можемо спостерігати інтеграцію різних технологій, наприклад таких як використання QR-коду, завдяки якому в комбінації зі смартфоном ми можемо отримати швидкий доступ до відповідного джерела інформації та значно спростити час пошуку. Також один з прикладом такого перетворення є інтеграція навігаційних систем у додатки, які повинні допомогти людині швидше робити пошуки товарів, знаходити потрібні бренди або магазини, та в висновок збільшити швидкість та обсяг продажу до того часу, як людина виснажиться і буде змушена покинути торговельно-розважальний центр.

Метою статті є дослідження особливостей використання навігаційних систем у торговельно-розважальних центрах з метою підвищення ефективності їх функціонування.

Об'єктом дослідження є розробка навігаційної системи торговельно-розважального центру з використанням технології доповненої реальності.

Предмет дослідження – навігаційна система.

Аналіз попередніх досліджень. Дослідженню навігаційних систем, визначенню структури, основних характерних рис присвячені праці вітчизняних та закордонних науковців: Н.О. Голошубова, О.О. Кавун, В.М. Торопков, Бозуленко О. Я.

Виклад основного матеріалу. В економічній системі торгівля посідає особливе місце. Вона забезпечує товарно-грошовий обмін у формі купівлі-продажу у величезних розмірах і відіграє суттєву роль у реалізації соціальної політики, стабілізації реального сектору економіки, розширенні міжгалузевого та міжрегіонального обміну.

Торгівля як галузь господарської діяльності має розгорнуту мережу оптових і роздрібних підприємств, забезпечує зберігання, транспортування і реалізацію товарної продукції предметів споживання. Оскільки більшість предметів особистого споживання проходить через торгівлю, то рівень її розвитку характеризує обсяг і структуру споживання. Торгівля інформує і впроваджує в споживання нові товари, виробництво яких тільки починається, які для споживача є ще невідомими або незвичними. Таким чином, розвиток торгівлі, будучи обумовленим рівнем і темпами розвитку виробництва товарів, в свою чергу, здійснює вплив на промисловість, сільське господарство з одного боку, і на споживання людей – з іншого. Важливе значення торгівлі в тому, що вона сприяє особистій матеріальній зацікавленості людей у підвищенні продуктивності праці, в збільшенні виробництва, в повнішому задоволенні потреб. Торгівля як сфера національної економіки за своєю формою і змістом належить до складних соціально-економічних систем і виконує життєво важливі завдання і функції економічних відносин [1, с. 10].

Саме це і зумовлює її постійний розвиток, видозмінення та перетворення, пошуки та вдосконалення методів покращення ефективності взаємодії виробника товарів та покупців. Одним із таких методів можна зазначити сучасні навігаційні системи, їх появу як явище та розвиток як у сучасних торговельних центрах, так і в інших соціально-економічних сферах життєдіяльності.

Навігаційні системи торговельно-розважальних центрів (надалі ТРЦ) є невід'ємною частиною сучасного міста. Вони дозволяють відвідувачам швидко знайти потрібний магазин або розважальний заклад, а також допомагають орієнтуватись на території ТРЦ. Зараз у використанні є безліч різних навігаційних систем, від простих табличок з написами до складних електронних систем з підключенням до смартфонів.

Однак, з появою технологій доповненої реальності (AR), навігаційні системи стали ще більш ефективними та зручними для відвідувачів ТРЦ. AR дозволяє накладати віртуальну інформацію на реальний світ, що забезпечує користувачам додаткову інформацію про те, де знаходиться певне місце, яку має розміщення та як до нього найлегше дістатись.

Одним з прикладів використання AR в навігаційних системах ТРЦ є додаток (наприклад QR Reader), що дозволяє відвідувачам сканувати QR-коди пересуваючись по

самому ТРЦ та отримувати інформацію про певне місце, наприклад, меню ресторану, графік роботи магазину або акційні пропозиції. Такий додаток може бути зручним тим, що дозволяє зекономити час та знайти необхідну інформацію з одного джерела. Наразі на більшості смартфонів достатньо просто навести камеру на QR-код і посилання одразу з'явиться на самому екрані що значно спрощує процес зчитування інформації. Але назвати таке використання AR повноцінним є дуже складним, адже можливості доповненої реальності є значно ширшими ніж можливість швидко зчитувати посилання на різні джерела.

Однією з проблем використання таких методів навігації є певна не упорядкованість та не систематизація інформації яку можна знайти в самому Торговельно-розважальному центрі – певні магазини та ресторани можуть використовувати такі можливості, інші не бачать в цьому ніякої потреби.

Віртуальна реальність досить популярна і в ігровій та освітній сфері, проте використовується і в культурі. Один із найвідоміших музеїв культури і мистецтва у віртуальній реальності – Artheon. У ньому зібрані тисячі оцифрованих творів мистецтва з колекцій світових музеїв. У додатку можна розглядати експонати з будь-якого боку, створювати свою експозицію та головне – у будь-який час [2].

Цю ідею можна використати для віртуального перегляду товарів з усіх боків без фізичної наявності у самому магазині. Також дуже зручно можна переглянути певний товар у специфічному кольорі, адже не завжди можливо покупцю привезти один товар у десятках, або навіть сотнях варіаціях – наприклад меблева продукція. Через свої габарити це значно спростить і навантаження на торговельну площу, і водночас розширить можливості для передпоказу товару.

Наразі немає прикладів типової імплементації, але розробка даного рішення та його впровадження у торговельний процес вже відбувається. Наприклад, незабаром клієнти інтернет-магазину epicentrk.ua матимуть змогу використати доповнену реальність для придбання меблів. Ця технологія дозволить максимально реалістично візуалізувати товар та показати, як він виглядатиме у конкретній кімнаті та інтер'єрі.

Зокрема, за допомогою функції доповненої реальності покупці зможуть через камеру свого смартфона або планшета подивитися, як виглядатимуть меблі в їхній кімнаті. Щоб скористатися цією функцією, клієнту компанії не потрібно буде встановлювати жодне програмне забезпечення – достатньо лише просканувати QR-код.

Неперервне масштабування корпоративних торгівельних мереж зумовлює постійний пошук для ще більш потужного розвитку, чим по суті й виявляється поява брендованих ТРЦ. Ефект масштабу у корпоративних торговельних мережах виявляє передусім економічний характер наслідків (збільшення кількості магазинів у складі об'єднання відображається на темпах зростання фінансово-економічних показників і передбачає отримання очікуваного рівня прибутковості діяльності) та психологічний характер (збільшення кількості магазинів під однією торговельною маркою забезпечує підвищення рівня запам'ятовування, завоювання та утримання прихильності споживачів) [3, с.84].

Типову сучасну навігаційну систему торговельно-розважального центру можна розглянути на прикладі додатка 'River Mall'. Такі додатки дедалі стають популярніші у сьогодення. Цей додаток розроблений для розв'язання питань по типу паркування, пошуку одягу відповідно до бренду або іншими характеристиками, та є корисним тільки щодо конкретного торговельно-розважального центру. Всі функціональні модулі об'єднує одне завдання – покращити навігацію у торговельному центрі та надати покупцю максимальний комфорт задля покращення товарообігу між виробником та покупцем (рис. 1).

Рис. 1. Інтерфейс додатку «River Mall»

Карта центру частково інтегрована в більш звичну карту міста, якщо розглянути перший поверх, та має навіть певні особливості територіальні для більшого уявлення простору навколо. Ця ж сама система працює і щодо парувальних місць.

Як ми можемо побачити на малюнку покупець може побачити реальну карту торгового центру, перевірити будь-який поверх та зробити сортування за тими товарами в яких він потребує у цей час. Відповідно до запиту додаток надає певний магазин або магазини, після чого стає можливим прокласти маршрут (рис. 2).

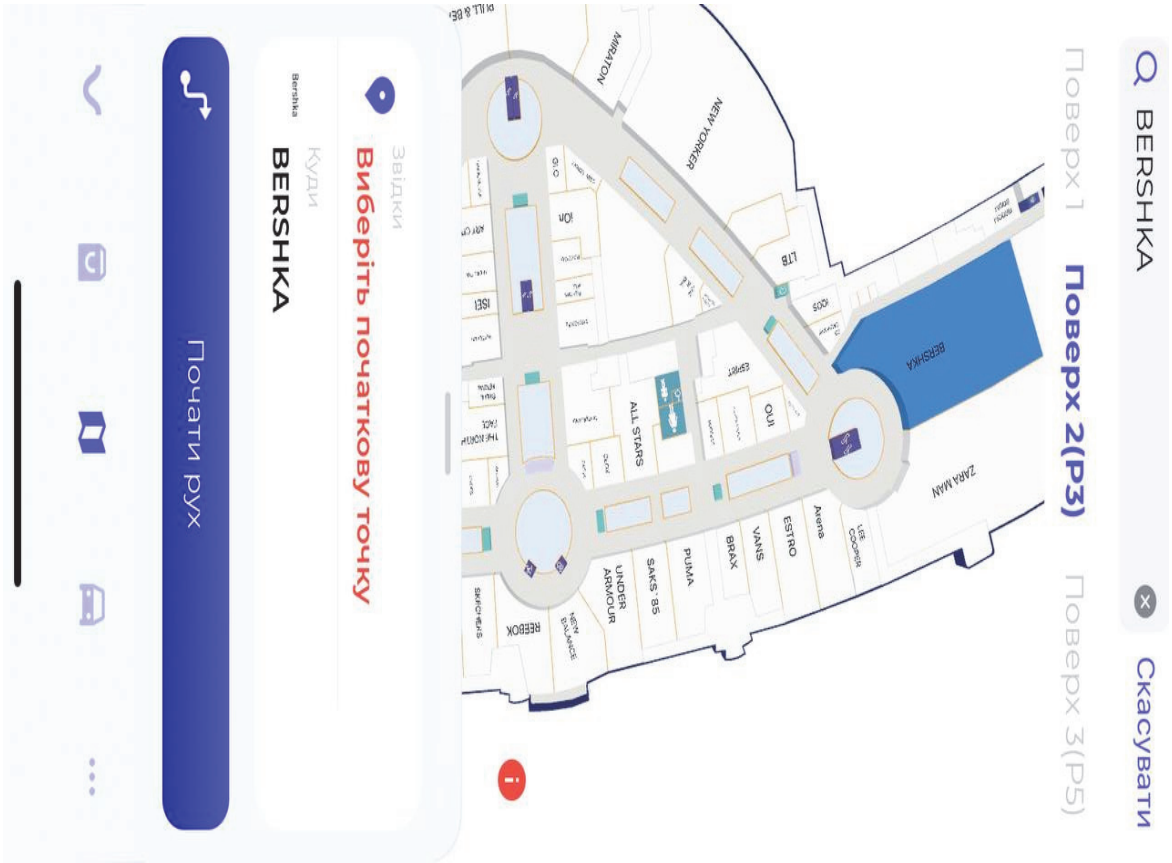


Рис. 2. Навігація у додатку «River Mall»

При виборі певного магазину додаток прокладає маршрут та надає підказки щодо пересування, використовуючи звичайну GPS навігацію в поєднанні з іншими технологіями для покращеного орієнтування у просторі. Відправну локацію можна задавати самостійно не використовуючи автознаходження пристрою (рис. 3).

Наразі AR в цьому додатку використовується тільки як можливість просканувати свій паркувальний талон для його подальшої сплати. Можливість більшої інтеграції з AR надала б змогу зробити навігацію більш інтерактивною, інформативною, та логічною. Пересуваючись по території використовуючи AR додаток можна як включити до функціонала персонального помічника який саме на екрані звичайного смартфону надавав вказівки щодо пересування або інформацію щодо магазинів які також можна перевірити щодо наявності групи товарів або розвал які викликали інтерес. Навіть більше, в цю навігацію можна інтегрувати будь-що, від звичайної інформації щодо бренду до популярних товарів тощо [4].

Рис. 3. Маршрут у додатку «River Mall»

Іншим прикладом є використання AR-окулярів для навігації в ТРЦ. Окуляри можуть накладати відображення на реальний світ, що дозволяє відвідувачам ТРЦ дізнатись більше про місце, на якому вони знаходяться, а також про певні пропозиції, акції та події, які відбуваються в магазинах та розважальних закладах. Такий підхід дозволяє зробити навігацію більш інтерактивною та зручною для відвідувачів ТРЦ, а інтеграцію AR ще більш реалістичною. Але наразі практичне використання такого методу є дуже складним, адже AR окуляри є мало популяризовані, а розробка програмного забезпечення може вийти значно дорожче ніж реальна ефективність.

В перспективі, AR може бути використана для створення віртуальної мапи ТРЦ. Наприклад, відвідувач може встановити додаток на свій смартфон та сканувати коди, розташовані на стінах ТРЦ, щоб побачити віртуальну мапу. Такий підхід дозволяє відвідувачам швидко знайти потрібне місце та дістатись до нього. Крім того, такий додаток має багато інших можливостей, наприклад окрім QR-кодів можна додати можливість зчитувати логотипи брендів та видавати інформацію щодо них прямо на смартфоні.

Ще одним важливим аспектом є можливість поєднання навігаційних систем з іншими технологіями, такими як інтернет-маркетинг та інтелектуальний аналіз даних. Наприклад, на основі даних, зібраних навігаційною системою, можна створити персоналізовані рекламні

пропозиції для відвідувачів ТРЦ, що дозволить ефективніше залучати клієнтів до магазинів та розважальних закладів.

Навігаційні системи ТРЦ є невід'ємною частиною сучасного міста та можуть бути дуже ефективними з використанням технологій доповненої реальності. AR дозволяє створювати інтерактивні та зручні для відвідувачів ТРЦ навігаційні системи, що покращує їх досвід відвідування ТРЦ та збільшує ефективність маркетингових кампаній магазинів та розважальних закладів.

Однак, при використанні AR для навігації у ТРЦ необхідно враховувати певні технічні та етичні аспекти. Наприклад, необхідно забезпечити належний рівень захисту персональних даних відвідувачів, які використовують AR-додатки. Крім того, додатки повинні бути доступні для користувачів з різними рівнями технічної грамотності, що може вимагати розробки додаткових інтерфейсів та інструкцій користувача.

В заключення, можна сказати, що навігаційні системи ТРЦ з використанням технологій доповненої реальності мають великий потенціал для покращення якісного рівня обслуговування відвідувачів та підвищення ефективності маркетингу магазинів та розважальних закладів. Проте, враховуючи певні технічні та етичні аспекти, необхідно забезпечувати належну реалізацію цих систем та збалансований підхід до використання нових технологій.

Ще однією можливістю для покращення навігації в ТРЦ є використання системи «інтелектуальної» карти. Ця система полягає у використанні датчиків, що відстежують рух відвідувачів та показують їм найближчі магазини, ресторани та інші заклади в ТРЦ. Крім того, система може відображати інформацію про акції, знижки та інші спеціальні пропозиції для відвідувачів.

Але однією із особливостей сучасних навігаційних систем ТРЦ є те, що усі доступні можливості AR використовуються лише частково і не усіма учасниками торговельного процесу.

Висновки. Таким чином, можна зробити висновок, що використання навігаційних систем та технологій доповненої реальності у торговельно-розважальних центрах є важливим інструментом для залучення та задоволення клієнтів, покращення їх досвіду покупок та збільшення прибутків компаній-операторів цих центрів. Ці технології також можуть бути використані для збору даних про поведінку та інтереси клієнтів, що дозволить покращити ефективність маркетингових кампаній та рекламних пропозицій.

Проте, необхідно пам'ятати про те, що використання технологій повинне бути збалансованим та не надто інтенсивним, оскільки це може негативно позначитися на досвіді покупок та безпеці клієнтів. Також, необхідно забезпечити високу якість технічної підтримки та забезпечення безпеки даних, щоб запобігти можливим технічним проблемам та злому систем.

Впровадження навігаційних систем та технологій доповненої реальності у торговельно-розважальних центрах є перспективною та важливою тенденцією розвитку цієї галузі, яка дозволяє покращити досвід покупок та залучити нових клієнтів. Проте, необхідно забезпечити правильний баланс між використанням технологій та потребами клієнтів, щоб забезпечити позитивний ефект від їх впровадження.

У підсумку, можна стверджувати, що навігаційні системи тоговельно-розважальних центрів мають великий потенціал для покращення ефективності та якості обслуговування відвідувачів. Технології доповненої реальності та «інтелектуальної» карти можуть допомогти вирішити багато проблем, пов'язаних з навігацією та пошуком потрібних магазинів та закладів. Однак, при розробці та впровадженні таких систем необхідно враховувати певні технічні та етичні аспекти, щоб забезпечити належний рівень захисту персональних даних та забезпечити доступність та зручність для всіх відвідувачів.

Список використаних джерел

1. Бозуленко О. Я., Організація торгівлі : навчальний посібник [для студ. вищ. навч. закл.]. Чернівці : ЧТЕІ КНТЕУ, 2021. 240 с
2. Вигаданий світ: українські проєкти у VR та AR від 04 Липня 2020 \\ Режим доступу: https://creativeeurope.in.ua/posts/ukrainian-projects-vr-ar
3. Підприємницькі мережі в торгівлі: монографія / [Н.О. Голошубова, О.О. Кавун, В.М. Торопков та ін.]; за заг. ред. Н.О. Голошубової. – К.: Київ. нац. торг.-екон. ун-т, 2014. – 344 с
4. Додаток ‘River Mall’ \\ режим доступу: https://apps.apple.com/ua/app/river-mall/id1498766659?l=ua

Робота виконана під науковим керівництвом канд. екон. наук, доцента
ТИЩЕНКА Д. О.

CRM СИСТЕМИ ЯК ОБОВ’ЯЗКОВА СКЛАДОВА ОПТИМІЗАЦІЇ УСПІШНОГО БІЗНЕСУ В ІНДУСТРІЇ КРАСИ

КУКЛА В., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У цій статті розглянуто актуальність використання системи управління взаємовідносинами з клієнтами у салонах краси, зазначено переваги застосування програмних продуктів в процесі автоматизації надання послуг, а також наведено опис основних функцій CRM систем.

In this article examined the relevance of using a customer relationship management system in beauty salons. In addition, we indicated the advantages of using software products in service providing automation, as well as we made a description of the main CRMsystems functions.

Актуальність. Індустрія краси в Україні – це стрімко зростаюча галузь економіки. За даними дослідницької компанії Euromonitor International, обсяг ринку краси в Україні в 2020 році становив більше 2,7 мільярдів доларів США. Ця галузь займає важливе місце в економіці країни, адже забезпечує працевлаштування більше ніж 300 тисяч осіб, включаючи косметологів, майстрів манікюру та педикюру, перукарів та інших спеціалістів. [1] Відсоток ВВП, який генерується галуззю, також є суттєвим. Згідно з даними Міністерства розвитку економіки, торгівлі та сільського господарства України, у 2020 році внесок індустрії краси в ВВП склав близько 1,5 %. [2]

Варто зазначити, що CRM (Customer Relationship Management) системи є необхідним інструментом для будь-якого бізнесу, який забезпечує зберігання та управління інформацією про клієнтів. У сегменті індустрії краси актуальність CRM систем також дуже висока. Саме тут залежність від клієнтів є найвищою, оскільки це визначає успіх або невдачу у веденні бізнесу.

За даними статистики, 70 % клієнтів салонів краси повертаються за послугами, якщо їх задоволеність першим візитом перевищує 90 %. Тому зберігання та аналіз інформації про клієнтів є вкрай важливим, адже допомагає визначити їх потреби і бажання.

Крім того, CRM система дозволяє також автоматизувати процеси запису на послуги, створення розкладу роботи майстрів, розсилку повідомлень про акції та знижки. Як наслідок – мінімізується ймовірність внесення помилкової інформації про клієнтів, а збереження цієї інформації стає більш організованим та ефективним.

Загалом впровадження CRM системи допомагає салонам краси удосконалювати обслуговування клієнтів та збільшувати їх задоволеність. Також це сприяє збільшенню доходів та покращенню репутації бізнесу. [3]

Відповідно, розробка та впровадження CRM систем у салонах краси є важливим етапом в розвитку галузі індустрії краси. Їх використання підвищує конкурентоспроможність бізнесу та робить його більш зручним для клієнтів.

Метою статті є дослідження особливостей використання CRM систем у салонах краси для підвищення продуктивності їх функціонування.

Об'єктом дослідження є розробка компоненти CRM системи салону краси.

Предмет дослідження – CRM система.

Аналіз попередніх досліджень. Дослідження та аналіз CRM систем салонів краси проводять як відомі міжнародні компанії, так і незалежні науковці. Наприклад, компанія «Salesforce», яка є однією з провідних світових розробників CRM систем, має багато публікацій та наукових досліджень на тему використання їхньої системи в салонах краси.

Також є багато науковців, які займаються дослідженням CRM систем в салонах краси. Наприклад, відомий американський науковець Марк Гроув займається дослідженням CRM систем в салонах краси та публікує свої результати у наукових журналах.

У вітчизняному контексті є декілька науковців, які займаються дослідженням CRM систем в салонах краси. Так, М. Самойленко та І. Горбаченко з Харківського національного університету імені В. Н. Каразіна досліджували використання CRM систем в салонах краси України та розробляли рекомендації для їхнього впровадження.

Виклад основного матеріалу. CRM системи в наш час стають незамінними інструментами управління клієнтською базою та автоматизації бізнес-процесів. Ці системи стали особливо популярними в останні роки завдяки збільшенню конкуренції на ринку та необхідності в удосконаленні процесів взаємодії з клієнтами. У сучасному інформаційному світі це невід'ємна частина дієвого управління бізнесом. На фоні пандемії COVID-19, яка значно вплинула на галузь краси, автоматизація бізнес-процесів стала необхідністю для більшості салонів краси.

CRM (управління взаємовідносинами з клієнтами) – це поняття, що включає концепції, які компанії використовують для управління взаємовідносинами зі споживачами, включаючи збір, зберігання та аналіз інформації про споживачів, постачальників, партнерів та їх взаємодію (рис. 1).

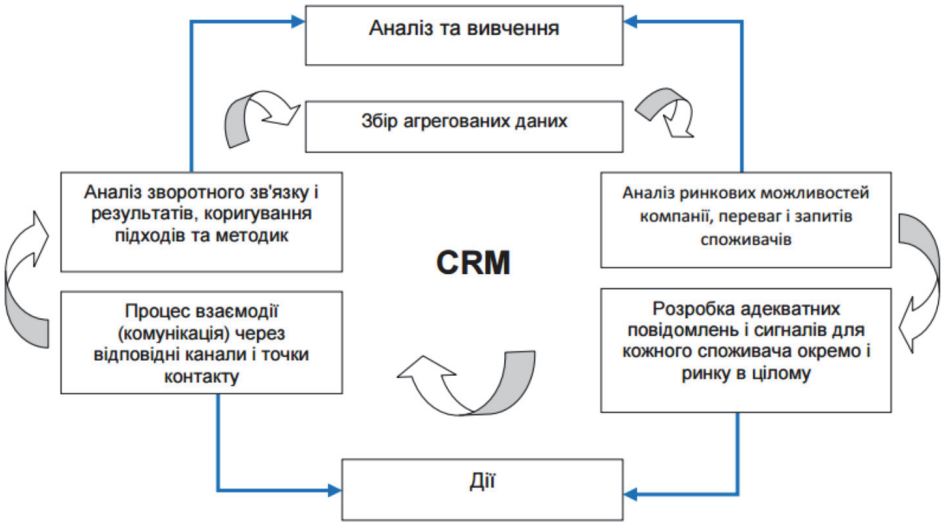


Рис. 1. Цикл інформаційних процесів в CRM розроблено автором за джерелом [4]

Сучасна CRM-концепція спрямована на вивчення ринку та конкретних потреб клієнтів. Існують три підходи до автоматизації управління взаємовідносинами з клієнтами, які можуть бути реалізовані окремо. CRM – концепція:

• оперативний підхід – автоматизація споживчих бізнес-процесів для допомоги персоналу з роботи з клієнтами

• аналітичний підхід – аналіз інформації про споживачів з різноманітними цілями

• клієнтський підхід – програма взаємодії зі споживачами без участі персоналу з роботи з клієнтами. З розвитком інноваційних технологій CRM стала функціонувати у віртуальному просторі, поєднавшись з глобальною мережею Інтернет та здобула ряд інструментів, одним з яких є e-CRM-система. Стандартна офлайн CRM-система – це набір додатків, функцій та інструментів, пов'язаних єдиною бізнес-логікою та інтегрованих в єдину корпоративну інформаційну середу компанії. E-CRM-система додає до типових функцій такого класу систем можливості індивідуальної взаємодії з клієнтами у віртуальному просторі. Тобто, вона привносить переваги та динаміку взаємодії з клієнтами за допомогою електронних інструментів

Основна ідея e-CRM-системи полягає у тому, що вона дає можливість підприємствам ефективно керувати взаємодією з клієнтами, зокрема, за допомогою електронної пошти, чат-ботів, месенджерів та інших онлайн інструментів.

До переваг використання E-CRM-системи можна віднести:

• зниження витрат на обслуговування клієнтів. E-CRM-система дозволяє підприємствам знизити витрати на обслуговування клієнтів, так як автоматизує багато процесів, що раніше виконувались вручну;

• підвищення рівня задоволеності клієнтів. За допомогою e-CRM-системи підприємства можуть забезпечити швидкий відгук на запити клієнтів, знизити час очікування відповіді на запит та забезпечити більш індивідуальний підхід до кожного клієнта;

• підвищення ефективності маркетингових кампаній. E-CRM-система допомагає збирати та аналізувати дані про клієнтів, що допомагає підприємствам створювати більш дієві маркетингові кампанії та пропонувати індивідуальні пропозиції для кожного клієнта;

• підвищення конкурентоспроможності. Використання e-CRM-системи на підприємствах робить їх більш конкурентоспроможними на ринку, забезпечуючи якісне обслуговування клієнтів та знижуючи витрати на обслуговування;

• підвищення продажів. E-CRM-система може допомогти підприємствам створити персоналізовану рекламну кампанію для певної групи клієнтів, що збільшить ймовірність їхньої участі в акції та покупки товару.

Збір даних про клієнтів з допомогою e-CRM-системи включає в себе дані про історію замовлень, переглядів товарів, поведінку на сайті та в інших каналах взаємодії з підприємством. Аналізуючи ці дані, менеджери підприємств підвищують результативність спілкування з клієнтами, отримують краще розуміння їхніх потреб для подальшої розробки індивідуальних пропозицій.

Важливим фактором впровадження CRM системи є правильний вибір програмного забезпечення, яке відповідатиме потребам конкретного салону краси. За різними дослідженнями, на сьогоднішній день на ринку представлено багато різних CRM систем для салонів краси, серед яких можна виділити Beauty Pro, CleverBox, YCLIENTS, BloknotApp та інші.

Розглянемо деякі приклади успішного впровадження CRM систем на підприємствах індустрії краси в Україні.

Приміром, мережа салонів ZEBRA є найбільшою в місті Дніпро. Перший салон був відкритий ще сімнадцять років тому, зараз мережа налічує п'ять салонів краси, розміщених у великих торгових центрах. Персонал салонів сумарно складає понад сто майстрів, а у мережі щомісяця обслуговується понад п'ять тисяч клієнтів.

Керувати бізнесом такого масштабу в ручному режимі практично неможливо, тому три роки тому мережа салонів ZEBRA автоматизувала свою роботу за допомогою сервісу для управління салонами краси та клініками Beauty Pro CRM.

Найперше, що треба було виправити – це неефективне управління клієнтською базою даних. Клієнти звикли звертатися в різні салони мережі, але не мали єдиного обліку своїх послуг та знижок. Це призводило до невдоволеності клієнтів та як результат зниження обсягів надання послуг. Для вирішення цієї проблеми за допомогою Beauty Pro було створено єдину базу даних клієнтів, у якій зберігалися дані про послуги, знижки та історію відвідувань. Завдяки цьому зараз клієнти отримують персоналізований підхід до своїх потреб.

Управління запасами інвентарю було іншою проблемою, яку вирішили за допомогою Beauty Pro CRM. Раніше співробітники салону самостійно вводили дані про продаж і замовлення товарів на склад мережі. Це вимагало багато часу і зусиль, а також часто призводило до помилок в обліку запасів. Beauty Pro CRM дозволила автоматизувати цей процес, введення даних про продажі та замовлення тепер здійснюється в режимі онлайн і безпосередньо з касового апарату. Інформація про продажі, запаси та замовлення постійно оновлюється і доступна для аналізу в режимі реального часу. Менеджери взмозі вчасно приймати рішення про замовлення товарів, враховуючи попит клієнтів та стан запасів.

Крім того, Beauty Pro CRM дає можливість плідно вести маркетингові кампанії, що є важливим елементом в успішному функціонуванні будь-якого салону краси. Завдяки системі Beauty Pro менеджери можуть створювати та відстежувати маркетингові кампанії, спрямовані на залучення нових клієнтів та збереження вже існуючих. За допомогою даних клієнтів салонів, менеджери можуть створювати персоналізовані пропозиції та акції, які будуть цікаві для кожного клієнта окремо.

Також система Beauty Pro CRM дозволяє вести ефективний контроль за роботою персоналу. За допомогою системи менеджери можуть відстежувати роботу кожного співробітника, контролювати та аналізувати його особистий результат. (Рис. 2).

Рис. 2. Основні напрями використання CRM Beauty Pro

Отже, Beauty Pro CRM є потужним інструментом для автоматизації бізнес-процесів салонів краси. Ця система дозволяє ефективно вести бізнес, забезпечує кращу взаємодію з клієнтами та забезпечує стабільну роботу підприємств. Крім того, Beauty Pro є надійним інструментом для управління бізнесом в умовах пандемії COVID-19, коли салони краси мусять дотримуватись соціальної дистанції та інших заходів безпеки.

Застосування Beauty Pro CRM у салоні краси може мати значний вплив на розвиток і популяризацію салону серед потенційних клієнтів. Дізнавшись більше про своїх клієнтів, власники салону можуть персоналізувати свої послуги та пропозиції, оптимізувати використання ресурсів та забезпечити зростання прибутку. [5]

Іншим провідним розробником CRM систем є компанія CleverBox. Це українська компанія, яка спеціалізується на розробці та впровадженні CRM систем. Компанія відрізняється високою якістю своїх продуктів та високим рівнем сервісу.

Компанія CleverBox розробила спеціальні інструменти для ведення дієвого діалогу з клієнтами. Так, одним із цих інструментів є автоматична розсилка повідомлень. Ця функція встановлює автоматичну відправку повідомлень клієнтам в певних ситуаціях, наприклад, при підтвердженні запису до майстра або при нагадуванні про поточний стан замовлення. Також зазначена система веде облік дзвінків та електронних листів клієнтів, контролює якість комунікації для вчасного реагування на запити клієнтів.

Окрім автоматизації комунікації з клієнтами, CleverBox CRM має інші важливі функції. Наприклад, з використанням системи можливе планування роботи кол-центру та контроль за якістю обслуговування клієнтів. Примітно, що компанія CleverBox CRM забезпечує підтримку своїх клієнтів протягом всього процесу використання системи. Команда підтримки завжди готова надати кваліфіковану допомогу та відповісти на всі запитання щодо роботи системи.

Важливо, що система компанії CleverBox CRM постійно вдосконалюється, додаються нові функції та можливості. Багаторічний досвід роботи зі своїми клієнтами дає можливість компанії зрозуміти потреби ринку та розробляти інструменти, які повністю задовільнять їхні очікування.

Таким чином, компанія CleverBox CRM пропонує своїм клієнтам функціональну систему, автоматизувати бізнес-процеси та покращувати комунікації з клієнтами. [6]

YCLIENTS також є інноваційною CRM системою для бізнесу, яка була створена в 2014 році у Литві, а пізніше була перенесена в Україну.

Основна ідея системи полягає в тому, щоб допомогти підприємствам з легкістю інтегруватися з потенційними та поточними клієнтами, оптимізувати робочий процес і забезпечити якість обслуговування. Ця CRM система, у першу чергу, призначена для тих, хто працює в сфері краси та здоров'я, таких як салони краси, масажні кабінети, фітнес-центри та інші.

Одна з найбільш важливих функцій YCLIENTS – це онлайн-бронювання послуг в будь-який час та з будь-якого пристрою. Це робить процес бронювання набагато зручнішим для клієнтів, а для бізнесу можливість планувати свій робочий час.

Крім того, система має функціонал для створювання та відстежування рекламних кампаній, аналізу маркетингу, ведення статистики та створення звітів.

Одним з головних переваг YCLIENTS є її зручний та легкий інтерфейс. Користувачі з легкістю орієнтуються в системі та ефективно використовують всі її можливості.

Система також пропонує зручні інструменти для керування співробітниками, зокрема змінами та графіками роботи. Користувач може додавати нових співробітників, встановлювати їхні ролі та обмеження доступу до інформації в залежності від потреб бізнесу. Можливі налаштування автоматичних повідомлень для співробітників, які нагадують про необхідність зробити нові записи або про терміни проведення процедур.

Більше того, система YCLIENTS дозволяє проводити успішний маркетинг, зокрема, створювати рекламні кампанії, розсилки, акції та бонусні програми для клієнтів. Для цього в системі є зручний редактор рекламних оголошень та інструменти для налаштування цільової аудиторії.

У загальному, YCLIENTS – це зручна CRM система, яка допомагає салонам краси оптимізувати свою роботу та підвищити результативність бізнесу. [7]

Також популярною CRM системою для б'юті індустрії в Україні є BloknotApp. Компанія BloknotApp була заснована в Україні в 2017 році. На сьогоднішній день вона є однією з провідних компаній, що працюють в галузі розробки програмного забезпечення для салонів краси.

Важливою функцією BloknotApp є можливість онлайн-бронювання послуг через мобільний додаток. Це зменшує навантаження на адміністраторів та дає змогу клієнтам забронювати зручний для них час без необхідності телефонування до салону.

Також BloknotApp зберігає всю інформацію про клієнтів у централізованій базі даних. Завдяки цьому знаходити необхідну інформацію про клієнтів, таку як історія відвідувань, побажання та пропозиції щодо нових послуг, дуже легко. Як результат клієнти можуть отримувати персоналізований сервіс та почувати себе унікальними і важливими для салону краси.

Водночас, BloknotApp дозволяє керувати фінансами салону краси: створювати рахунки-фактури, виставляти рахунки, відслідковувати оплати та виконувати інші фінансові операції.

Особливістю BloknotApp є можливість підключення до банківської системи, швидко та безпечно проводити фінансові операції з клієнтами та іншими партнерами. BloknotApp надає широкий спектр функціоналу для керування бізнесом в галузі краси та здоров'я.

Крім того, BloknotApp має високий рівень безпеки. Компанія надає велику увагу захисту даних своїх клієнтів. Програма побудована на сучасних технологіях для захисту важливої інформації про клієнтів та про фінансові операції. BloknotApp веде історію змін, що забезпечує контроль за всіма діями співробітників та покращує якість обслуговування.

Додатковою перевагою BloknotApp є можливість інтеграції з іншими популярними сервісами, такими як Google Calendar та MailChimp. BloknotApp має зручний та інтуїтивно зрозумілий інтерфейс, можливість роботи з клієнтами та робочими графіками в одній системі.

Крім того, BloknotApp пропонує низку додаткових функцій, таких як відстеження запасів та замовлень, статистичний аналіз продажів та багато іншого. Загалом, BloknotApp є однією з найкращих CRM систем для б'юті індустрії на сьогоднішній день. Компанія продовжує розвиватися та вдосконалюватися, щоб залишатися лідером на ринку. [8]

Як бачимо, впровадження CRM системи для салону краси є важливим кроком до автоматизації бізнесу, покращення якості обслуговування клієнтів, забезпечення збільшення обсягів продажів та зниження витрат підприємства, а також ведення успішного бізнесу в індустрії краси. Правильний вибір програмного забезпечення та комплексного підходу до автоматизації допоможе салону краси стати конкурентоздатнішим та забезпечити високу якість обслуговування.

Висновок. Відома експертка галузі, засновниця порталу Salonmarketing.pro та авторка книг «Мій салон краси» та «Ми відкрились!» Наталія Гончаренко в одному із своїх інтерв'ю запевнила, що індустрію краси чекає бурхливий розвиток після перемоги України над Російською Федерацією.

По-перше, навіть попри війну, салони краси працюють. Навіть відкриваються нові підприємства. Складнощі, з якими стикаються власники зростають майже щодня, але це не зупиняє відданих своїй справі підприємців.

По-друге, салони краси, які зачинились замінять нові салони.

По-третє, споживацька поведінка послуг краси в Україні сприяє розвитку галузі. На ринок прийдуть більш професійні інвестори, які мають досвід або щонайменше розуміння того, що ринку потрібні різноманітні, а не тільки дорогі послуги.

В-четверте, ще до війни в Україні почав розвиватись б'юті та медичний туризм і ця тенденція відновиться після перемоги дуже швидко, враховуючи репутацію нашої країни в цілому і індустрії краси зокрема. [9]

Отже, актуальність CRM системи для салонів краси не може бути переоцінена. У сучасному світі цифровізація проникає в усі сфери життя людини, зокрема і в індустрію надання послуг. В умовах, коли зовнішнє середовище трансформується, нікому не вдасться опинитися осторонь від процесів, що відбуваються. Адже постає питання: підлаштовуватися під нові умови взаємодії з постачальниками, клієнтами, майстрами або втрачати свої позиції. Саме завдяки цифровізації надання послуг в салонах краси стає більш оперативними та більш зручними як для власників підприємств та їх співробітників, так і для кінцевого споживача.

Список використаних джерел

1. Дослідницька компанія Euromonitor International / Електронний ресурс. – Режим доступу: https://www.euromonitor.com/
2. Міністерство розвитку економіки, торгівлі та сільського господарства України / Електронний ресурс. – Режим доступу: https://www.me.gov.ua/
3. Інформація із блогу компанії по розробці CRM Beauty Pro / Електронний ресурс. – Режим доступу: https://beautyprosoftware.com/ru/blog/
4. Можливості використання CRM-систем / Електронний ресурс. – Режим доступу: https://www.terrasoft.ua
5. Сайт компанії Beauty Pro CRM / Електронний ресурс. – Режим доступу: https://beautyprosoftware.com/
6. Сайт компанії CleverBox / Електронний ресурс. – Режим доступу: https://cleverbox-crm.com/
7. Інформація з Інтернет-видання 032.ua / Електронний ресурс. – Режим доступу: https://www.032.ua/news/3514027/biznes-saloniv-krasi-v-2023-2025-rokah-cogo-cekati.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
РЗАЄВОЇ С. Л.

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ ВІД КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

КУКЛІНСЬКИЙ Д., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні види криптографічних методів, такі як симетричне шифрування, асиметричне шифрування, хешування даних та цифровий підпис. Детально проаналізовано, як криптографічні методи можуть бути використані для захисту інформації на серверах підприємства, робочих станціях та переносних пристроях, а також при передачі інформації через мережу. Описано приклад використання криптографічних методів на підприємстві та розглянуто його результати. Розглянуто переваги та недоліки використання криптографічних методів, а також запропоновано рекомендації щодо їх використання на підприємстві.

The article discusses the main types of cryptographic methods, such as symmetric encryption, asymmetric encryption, data hashing, and digital signatures. It analyzes in detail how cryptographic methods can be used to protect information on enterprise servers, workstations, and mobile devices, as well as when transmitting information over the network. A case study of the use of cryptographic methods in an enterprise is described, and its results are discussed. The advantages and disadvantages of using cryptographic methods are considered, and recommendations for their use in the enterprise are proposed.

Актуальність. Актуальність криптографічних методів захисту інформації на підприємстві від комп'ютерних злочинів полягає в тому, що в даний час комп'ютерні атаки є дуже поширеними і можуть спричинити серйозні наслідки для підприємства. Інформація про клієнтів, фінансові дані, розробки, плани і стратегії підприємства можуть бути скомпрометовані або викрадені зловмисниками. Криптографічні методи дозволяють захистити

інформацію від несанкціонованого доступу та зберігати її в зашифрованому вигляді. Крім того, вони можуть забезпечити цілісність даних та підтвердження автентичності відправника. Також вони допомагають забезпечити відповідність законодавству щодо захисту персональних даних та іншої конфіденційної інформації. Крім того, за допомогою криптографічних методів можна перевірити автентичність інформації та забезпечити її недоступність для зловмисників, що забезпечує більш високий рівень захисту.

Актуальність криптографічних методів захисту інформації на підприємстві полягає в тому, що ці методи є одними з найефективніших і надійних способів захисту інформації від комп'ютерних злочинів. Вони дозволяють підприємствам забезпечувати конфіденційність, цілісність та доступність інформації, а також забезпечувати надійний захист від різних видів атак. Отже, використання криптографічних методів є важливим елементом у захисті інформації на підприємстві від комп'ютерних злочинів і може допомогти уникнути серйозних наслідків для підприємства.

Мета статті – є дослідження криптографічних методів захисту інформації на підприємстві від комп'ютерних злочинів та визначення їх ролі у цьому процесі.

Об'єктом дослідження є аналіз криптографічних методів, їх застосування для захисту інформації на різних пристроях та в мережі, а також оцінка ефективності та обґрунтування рекомендацій щодо використання цих методів.

Предмет дослідження – криптографічні методи захисту інформації на підприємстві від комп'ютерних злочинів, зокрема симетричне шифрування, асиметричне шифрування, хешування даних та цифровий підпис.

Аналіз попередніх досліджень. Аналіз попередніх досліджень з криптографічних методів захисту інформації на підприємствах від комп'ютерних злочинів показує, що використання криптографічних методів є важливим елементом в захисті конфіденційної інформації від несанкціонованого доступу. Дослідження в цій області зосереджувалися на різних аспектах криптографії, включаючи симетричне і асиметричне шифрування, хешування даних, цифровий підпис та інші методи. Українські та закордонні вчені: І.С. Самойленко, Брюс Шнайер, Ніл Фергюнсон, Дуглас Стайнберг, Брюс Шнайр займалися дослідженням криптографічних методів захисту інформації на підприємствах від комп'ютерних злочинів. У своїх дослідженнях вони аналізували переваги та недоліки кожного з методів, а також вивчали практичні аспекти їх використання на підприємствах. Зокрема, вони досліджували, як криптографічні методи можуть бути використані для захисту інформації на серверах підприємства, робочих станціях та переносних пристроях, а також при передачі інформації через мережу.

Виклад основного матеріалу. На сьогоднішній день комп'ютерні злочини стали серйозною загрозою для підприємств. Ці злочини можуть призвести до крадіжки конфіденційної інформації, порушення нормативно-правових актів, втрати даних, відключення від Інтернету та збоїв в роботі комп'ютерних систем. Комп'ютерні злочини – це кримінальна діяльність, яка використовує комп'ютерні технології та Інтернет з метою здійснення шахрайства, шпигунства, вандалізму, крадіжки конфіденційної інформації, а також інших кримінальних дій. Крім того, комп'ютерні злочини можуть мати серйозні фінансові наслідки для підприємств, такі як витрати на відновлення інформації та відновлення роботи систем, втрати прибутку, штрафи за порушення нормативно-правових актів та судові витрати.

Отже, захист інформації на підприємстві є дуже важливою задачею, оскільки комп'ютерні злочини можуть стати серйозною загрозою для його діяльності та призвести до значних фінансових втрат. Захист інформації на підприємствах є дуже важливою задачею, оскільки конфіденційність та цілісність даних є критично важливими аспектами успішної діяльності підприємства. Недостатній захист може призвести до наслідків, які мають серйозний вплив на бізнес-процеси підприємства, такі як втрата клієнтів та партнерів, зменшення прибутку, втрата репутації, штрафні санкції та навіть банкрутство. Крім того, захист інформації є важливим для дотримання нормативно-правових вимог та регулювання в

галузі захисту даних, що може забезпечити надійність та довіру серед споживачів та інвесторів. Захист інформації також є важливим для забезпечення безпеки працівників та клієнтів підприємства, оскільки в разі порушення безпеки даних можуть стати доступними особисті дані та фінансова інформація, що може призвести до крадіжки особистих коштів та ідентичності, шахрайства та інших злочинів.

Криптографічні методи захисту інформації – це методи та технології, що застосовуються для забезпечення конфіденційності, цілісності та доступності інформації. Криптографічні методи захисту інформації є одним з найбільш ефективних інструментів боротьби з комп'ютерними злочинами. Основні криптографічні методи включають:

1. Симетричне шифрування – метод, який використовує один ключ для шифрування та розшифрування повідомлення. Найпоширенішими алгоритмами симетричного шифрування є AES (Advanced Encryption Standard), DES (Data Encryption Standard) та 3DES (Triple Data Encryption Standard).

Симетричне шифрування – це криптографічний метод, який використовує один ключ як для шифрування, так і для дешифрування повідомлень. Цей метод є одним з найстаріших та найпростіших методів шифрування і використовується для захисту інформації від несанкціонованого доступу. У симетричному шифруванні повідомлення перетворюються в криптограму (шифрований текст) за допомогою алгоритму шифрування і ключа. Коли отримувач отримує криптограму, він використовує той же ключ та алгоритм для дешифрування повідомлення. Одним з найпоширеніших симетричних алгоритмів шифрування є AES (Advanced Encryption Standard), який зараз використовується у багатьох системах та програмах для захисту даних. Одним з недоліків симетричного шифрування є необхідність безпечного обміну ключами між відправником та отримувачем, а також можливість взлому ключа методом брутфорсу, коли зловмисник перебирає всі можливі комбінації ключів до того моменту, поки не знайде правильний ключ

2. Асиметричне шифрування – метод, що використовує пару ключів – приватний та відкритий – для шифрування та розшифрування повідомлення. Найпоширенішими алгоритмами асиметричного шифрування є RSA та ECC (Elliptic Curve Cryptography).

Асиметричне шифрування – це криптографічний метод, у якому використовується пара ключів: публічний ключ і приватний ключ. Публічний ключ відкритий для використання всіма, тоді як приватний ключ є прихованим і відомим тільки власнику. Коли повідомлення шифрується за допомогою публічного ключа, то тільки власник приватного ключа може його розшифрувати. Це дозволяє захистити повідомлення від прослуховування та збереження конфіденційності даних. Асиметричне шифрування також використовується для підпису повідомлень. Власник приватного ключа може підписати повідомлення, й інші користувачі можуть перевірити цей підпис за допомогою публічного ключа, щоб переконатися в тому, що повідомлення було підписано саме власником приватного ключа, а не кимось іншим. Одним з найпопулярніших алгоритмів асиметричного шифрування є RSA (Rivest–Shamir–Adleman). Він використовується в багатьох криптографічних протоколах, включаючи SSL / TLS для захисту передачі даних в Інтернеті.

3. Хешування даних – метод, який використовує хеш-функції для створення унікального коду з повідомлення або даних. Хеш-функції, такі як SHA (Secure Hash Algorithm), використовуються для створення цифрових підписів та перевірки цілісності даних.

Хешування даних – це процес перетворення вхідних даних будь-якої довжини в фіксований вихідний хеш-код фіксованої довжини. Хеш-функція приймає на вхід блок даних і генерує хеш-код – унікальний ідентифікатор, який можна використовувати для перевірки цілісності даних. Хеш-код зазвичай представляється у вигляді невеликого числа або рядка символів. Хеш-функції повинні відповідати вимогам безпеки та надійності, тобто вони мають бути стійкими до колізій (тобто дві різні вхідні послідовності не повинні генерувати однаковий хеш-код) та малопридатними для зламу. Хеш-функції використовуються в різних

областях, таких як криптографія, збереження паролів, контроль цілісності даних, пошук та індексація даних. Наприклад, хеш-функції використовуються для створення підписів цифрових даних, перевірки автентичності повідомлень та ідентифікації відомостей про користувачів в системах аутентифікації. Одним з найбільш відомих алгоритмів хешування є SHA (Secure Hash Algorithm), який розробив Національний інститут стандартів і технологій США. Також існують інші алгоритми, такі як MD5, які використовуються для хешування даних. Проте MD5 вважається менш безпечним, оскільки може бути легко зламано.

4. Цифрові підписи – це електронний еквівалент підпису на папері, який можна використовувати для підтвердження автентичності документа або повідомлення в електронному вигляді. Цифровий підпис створюється за допомогою алгоритму криптографічного хешування та асиметричного шифрування.

Для перевірки цифрового підпису необхідно розшифрувати хеш-код за допомогою відкритого ключа власника підпису і порівняти його з хеш-кодом повідомлення або документа, який також розраховується за допомогою хеш-функції. Якщо значення збігаються, то цифровий підпис вірний і повідомлення або документ вважається автентичним.

Цифрові підписи використовуються в різних областях, таких як електронна комерція, електронна пошта, електронний документообіг та банківські операції. Вони дозволяють забезпечити надійність, цілісність та конфіденційність електронної інформації та перешкоджають можливості підробки даних. Для створення цифрового підпису використовується асиметричний алгоритм шифрування. Підпис складається з двох частин: відкритого ключа та цифрової підпису. Відкритий ключ повідомляється отримувачу повідомлення, тоді як цифровий підпис створюється за допомогою закритого ключа, який зберігається в таємниці від автора.

5. VPN (Virtual Private Network) – це технологія, яка дозволяє створювати безпечне з'єднання між комп'ютерами за допомогою зашифрованого тунелю. VPN дозволяє захистити інтернет-трафік від шпигунів та хакерів.
6. Електронний підпис – метод, який використовується для забезпечення відповідності електронних документів законодавству про електронний документообіг.
7. Протоколи аутентифікації – методи, що використовуються для перевірки ідентифікації користувачів та встановлення їхнього права доступу до інформації.
8. Кодування повідомлень – метод захисту інформації, при якому повідомлення перетворюються в інший формат. Наприклад, алгоритми кодування можуть перетворювати символи повідомлення в числа або замінювати символи на інші.
9. Розподіл ключів – метод, що використовується для безпечного обміну ключами між віддаленими користувачами. Розподіл ключів може використовувати симетричні та асиметричні шифри.

Захист інформації на серверах підприємства є критично важливим для забезпечення конфіденційності, цілісності та доступності даних. Деякі з основних методів захисту інформації на серверах підприємства включають наступне: фізичний захист: серверні приміщення повинні бути захищені від несанкціонованого доступу. Це може бути досягнуто за допомогою контролю доступу, системи відеоспостереження, біометричних систем та ін; захист мережі: мережеві з'єднання повинні бути захищені від атак, таких як DDOS, фішинг та ін. Це може бути досягнуто за допомогою захисту мережі, який може включати в себе мережеві фільтри, системи виявлення вторгнень та інші; парольний захист: доступ до серверів повинен бути захищений за допомогою паролів та інших методів аутентифікації. Користувачі повинні мати сильні паролі та система повинна бути налаштована таким чином, щоб вона вимагала зміну пароля з регулярністю; шифрування даних: дані, які зберігаються на сервері, повинні бути захищені за допомогою шифрування. Це може бути досягнуто за допомогою симетричного або асиметричного шифрування, які були описані вище; резервне копіювання даних: резервне копіювання даних є важливим елементом захисту інформації на серверах. Це може бути досягнуто за допомогою регулярних резервних копій, які

зберігаються в окремих фізичних приміщеннях, а також використання систем відновлення даних в разі аварійного відновлення системи.

Захист інформації на робочих станціях та переносних пристроях є важливим аспектом забезпечення безпеки даних в офісному середовищі. Деякі з основних методів захисту інформації на робочих станціях та переносних пристроях включають наступне:

1. Парольний захист: використання паролів для захисту доступу до робочих станцій та переносних пристроїв є основним методом захисту. Користувачі повинні мати сильні паролі та система повинна бути налаштована таким чином, щоб вона вимагала зміну пароля з регулярністю.

2. Шифрування даних: шифрування даних на робочих станціях та переносних пристроях може бути досягнуто за допомогою симетричного або асиметричного шифрування, які були описані вище. Також можна використовувати програми для шифрування даних, які зберігаються на переносних пристроях.

3. Захист від шпигунського програмного забезпечення: використання антивірусного програмного забезпечення та фаєрволів є важливим для захисту робочих станцій та переносних пристроїв від шпигунського програмного забезпечення.

4. Регулярне оновлення програмного забезпечення: регулярне оновлення програмного забезпечення допомагає запобігти вразливостям, які можуть бути використані для атак на робочі станції та переносні пристрої.

5. Захист мережі: мережеві з’єднання повинні бути захищені від атак, таких як DDOS, фішинг та ін. Це може бути досягнуто за допомогою захисту мережі, який може включати в себе мережеві фільтри, системи виявлення вторгнень та ін.

Захист інформації при передачі через мережу є критично важливим для забезпечення конфіденційності, цілісності та доступності даних. Деякі з основних методів захисту інформації при передачі через мережу включають наступне:

1. Шифрування даних: шифрування даних може бути досягнуто за допомогою симетричного або асиметричного шифрування, які були описані вище. Це допоможе забезпечити захист від прослуховування та перехоплення даних під час їх передачі через мережу.

2. Використання віртуальних приватних мереж (VPN): використання VPN дозволяє створити безпечний тунель для передачі даних через небезпечні мережі. Дані шифруються та передаються через тунель, що дозволяє забезпечити конфіденційність даних.

3. Використання протоколів безпеки: використання протоколів безпеки, таких як Secure Sockets Layer (SSL) та Transport Layer Security (TLS), є важливим для захисту даних при передачі через мережу. Ці протоколи шифрують дані та забезпечують їх цілісність.

4. Захист від атак: мережеві з’єднання повинні бути захищені від атак, таких як DDOS, фішинг, мережеві вторгнення та інші. Це може бути досягнуто за допомогою захисту мережі, який може включати в себе мережеві фільтри, системи виявлення вторгнень та ін.

5. Використання SSL / TLS: SSL / TLS – це протоколи захисту, які шифрують дані перед їх передачею через мережу. SSL / TLS використовується для захисту веб-сайтів, електронної пошти та інших додатків, що працюють через мережу.

6. Аутентифікація: передача інформації через мережу повинна бути аутентифікована, щоб запобігти підробці та перехопленню даних. Для цього можна використовувати різні методи аутентифікації, такі як логіни та паролі, біометричні методи та інші.

Вибір правильного криптографічного методу залежить від конкретних вимог до захисту даних, ризиків, які необхідно зменшити, та здатності виконувати розрахунки на обраному пристрої. Ось кілька критеріїв, які можна використовувати при виборі криптографічного методу:

1. Вартість застосування: вартість застосування криптографічних методів може бути дуже високою, залежно від використовуваної технології. Тому при виборі методу потрібно враховувати вартість його застосування, а також можливості фінансування проекту.

2. Можливість використання: методи шифрування можуть бути складними для використання та реалізації, тому потрібно забезпечити, що вони можуть бути ефективно застосовані для захисту інформації в конкретній ситуації.
3. Сумісність з іншими системами: при виборі криптографічних методів необхідно забезпечити сумісність з іншими системами та забезпечити можливість обміну даними з ними.
4. Рівень захисту: в залежності від рівня захисту, який потрібно досягти, може бути вибрано різні методи криптографії. Наприклад, якщо потрібно захистити відомості від зламу, може бути використаний асиметричний алгоритм шифрування. Якщо потрібно захистити дані від прослуховування, може бути використано шифрування SSL/TLS.
5. Надійність та стійкість до атак: криптографічний метод повинен бути надійним та стійким до атак, які можуть бути спрямовані на злам цієї системи. Для цього потрібно розуміти можливі загрози та використовувати методи, які забезпечують стійкість до таких атак.

Криптографічні методи є важливою складовою систем захисту інформації, але самі по собі вони не можуть забезпечити повної безпеки даних. Інші методи захисту інформації, такі як фізична безпека, контроль доступу, аудит та моніторинг, повинні використовуватись разом з криптографічними методами для забезпечення повної безпеки інформації. Наприклад, для захисту інформації на серверах підприємства можуть використовуватись криптографічні методи, такі як SSL/TLS, для захисту даних, які передаються по мережі. Однак, для забезпечення повної безпеки інформації також потрібно використовувати інші методи захисту, такі як регулярні аудити безпеки серверів, захисний периметр, брандмауер та системи моніторингу і виявлення інцидентів. Крім того, для захисту інформації на робочих станціях та переносних пристроях можуть використовуватись криптографічні методи, такі як шифрування диска, яке захищає дані на пристрої в разі його втрати або крадіжки. Однак, щоб забезпечити повну безпеку, також потрібно використовувати інші методи захисту, такі як контроль доступу до пристроїв та фізична безпека. Таким чином, використання криптографічних методів у поєднанні з іншими методами захисту інформації є необхідним для забезпечення повної безпеки даних в організації. Кожен метод захисту повинен бути вибраний в залежності від конкретних потреб організації та способів ризику, які повинні бути усунені.

У криптографії ключі є важливими елементами, які використовуються для шифрування та розшифрування даних, підпису та перевірки цифрових підписів. Ключове управління та зберігання ключів є важливими аспектами криптографії, оскільки вони забезпечують безпеку ключів та інформації, зашифрованої цими ключами.

Ключове управління означає забезпечення безпеки та ефективного використання ключів в організації. Це включає в себе генерацію ключів, дистрибуцію ключів, контроль доступу до ключів та їх використання, а також знищення ключів за потреби. Ключі можуть бути симетричні та асиметричні, і кожний тип ключа має свої вимоги до ключового управління. Зберігання ключів також є важливим аспектом криптографії. Ключі повинні бути збережені в безпечному місці, щоб запобігти їхньому викраденню або використанню несанкціонованими особами. Для зберігання ключів можна використовувати різні методи, такі як використання безпечних пристроїв зберігання ключів (HSM), використання захищених електронних ключниць, розподіл ключів на різних серверах, що забезпечує резервні копії ключів, тощо. Для забезпечення безпеки ключів та інформації, зашифрованої цими ключами, важливо використовувати різні методи захисту, такі як шифрування ключів, використання двофакторної автентифікації при доступі до ключів, встановлення правил контролю доступу до ключів, редагування журналів дій з ключами, тощо.

Розглянемо приклад використання криптографічних методів на підприємстві для захисту даних клієнтів. Припустимо, що підприємство займається продажем товарів онлайн, тому має доступ до особистих даних своїх клієнтів, таких як імена, адреси електронної

пошти, номери телефонів і банківські реквізити. Щоб захистити ці дані, підприємство може використовувати криптографічні методи. Один з можливих підходів – використовувати SSL (Secure Sockets Layer) або його наступника TLS (Transport Layer Security) для захищеної передачі даних між веб-сервером підприємства та веб-браузерами клієнтів. Це забезпечує захист від перехоплення даних під час їх передачі через мережу.

Також підприємство може використовувати криптографічні методи для зберігання паролів клієнтів. Замість зберігання паролів у відкритому вигляді, підприємство може зберігати їх у захешованому вигляді, використовуючи алгоритми хешування, такі як SHA-256 або bcrypt. Це знижує ризик вторгнення в систему та компрометації паролів клієнтів. Це дозволяє клієнтам перевірити, що повідомлення дійсно надіслано підприємством та не було підроблено зловмисниками.

Використання криптографічних методів на підприємстві дозволяє значно покращити рівень захисту інформації та запобігти її незаконному доступу. Результати використання криптографічних методів на підприємстві можуть бути наступними:

1. Збільшення рівня безпеки: застосування криптографічних методів дозволяє захистити інформацію від несанкціонованого доступу, зменшити ризики витоку даних, злому систем та інших загроз.
2. Підвищення рівня довіри: використання криптографічних методів дозволяє підтверджувати автентичність даних та ідентифікацію користувачів, що підвищує довіру до системи.
3. Зменшення ризику втрати даних: застосування методів шифрування та резервного копіювання даних дозволяє зменшити ризик втрати даних в результаті випадкового або зловмисного знищення.
4. Підвищення ефективності: застосування криптографічних методів дозволяє збільшити ефективність обробки даних, оскільки шифрування та розшифрування можуть виконуватись автоматично.
5. Забезпечення відповідності вимогам законодавства: використання криптографічних методів дозволяє підприємствам виконувати вимоги законодавства щодо захисту персональних даних та конфіденційності інформації.

Однак, слід зазначити, що використання криптографічних методів не є панацеєю і не забезпечує повну безпеку інформації. Для ефективного захисту необхідно використовувати комплексний підхід та поєднувати криптографічні методи з іншими методами захисту інформації. Також важливо забезпечувати правильне управління ключами та робити регулярну перевірку.

Висновки. Криптографічні методи відіграють важливу роль у захисті інформації на підприємстві. Вони забезпечують конфіденційність, цілісність та доступність даних, що є важливими аспектами у будь-якій організації. Криптографія також дозволяє підприємствам дотримуватись вимог законодавства щодо захисту персональних даних та іншої конфіденційної інформації. Крім того, застосування криптографічних методів допомагає підприємствам забезпечити довіру між сторонами, що сприяє розвитку бізнесу та співпраці з партнерами та клієнтами. Отже, використання криптографічних методів у захисті інформації на підприємстві є дуже важливим для забезпечення конфіденційності, цілісності та доступності даних, зменшення ризику витоку даних та кібератак, дотримання вимог законодавства та забезпечення довіри між сторонами. Основними перевагами використання криптографічних методів у захисті інформації на підприємстві є конфіденційність, цілісність; аутентифікація; незалежність від інших методів захисту. Хоча криптографічні методи забезпечують високий рівень захисту інформації на підприємстві, вони мають деякі недоліки, серед яких: високі витрати на впровадження, складність управління ключами, потреба в постійному оновленні, вплив на продуктивність, ризик втрати ключів. Тому важливо належним чином зберігати та управляти ключами. Ці недоліки не означають, що криптографічні методи не ефективні. Вони лише вказують на те, що підприємство повинно

добре розуміти свої потреби та можливості, перш ніж впроваджувати криптографічні методи захисту інформації.

Використання криптографічних методів є важливим кроком для захисту інформації на підприємстві, проте це не єдиний метод захисту. Правильне поєднання криптографічних методів з іншими методами захисту інформації може забезпечити найвищий рівень захисту даних на підприємстві.

Список використаних джерел

1. Лагун А.Е. Криптографічні системи та протоколи: нав. посібник / А.Е. Лагун. – Львів: Видавництво Львівської політехніки, 2013. – 96 с.
2. Горобцов В.О. Криптографічний захист інформації – URL: *http://esu.com.ua/search_articles.php?id=1575.*
3. Сушко С.А. Практична криптологія – URL: *https://bit.nmu.org.ua/ua/student/metod/cryptology/ %D0 %BB %D0 %B5 %D0 %BA %D1 %86 %D0 %B8 %D1 %8F %201.pdf.*
4. Класифікація сучасних криптографічних методів – URL: *https://lickeys.ru/uk/zhestkijj-disk/klassifikaciya-sovremennyhkriptograficheskihmetodov//*

Робота виконана під науковим керівництвом канд. техн. наук, доцента
САВЧЕНКО Т. В.

АСПЕКТИ НАЛАШТУВАННЯ ПРИСТРОЇВ КОМУТАЦІЇ КОМП'ЮТЕРНИХ МЕРЕЖ

КУПІН О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні аспекти налаштування пристроїв комутації комп'ютерних мереж Кампусів та підприємств. Зазначено переваги застосування програмного забезпечення для організації швидкого налаштування пристроїв комутації комп'ютерних мереж. Розглянуто як зразок виробників сучасних пристроїв комутації Cisco, Aruba, Ruckus.

The article discusses the main aspects of setting up switching devices for computer networks of Campuses and enterprises. The advantages of using software for the organization of quick configuration of computer network switching devices are indicated. Considered as a model of manufacturers of modern switching devices Cisco, Aruba, Ruckus.

Актуальність. У наш час мережі мають вирішальне значення для підтримки компаній, пропонування підключених послуг і можливості співпраці. Оскільки вони з'єднують пристрої, які спільно використовують ресурси. Мережеві комутатори є життєво важливим компонентами усіх мереж.

Метою статі є дослідження аспектів налаштування пристроїв комутації в комп'ютерних мережах з метою підвищення кваліфікації користувачів.

Об'єктом дослідження є пристрої комутації комп'ютерних мереж.

Предмет дослідження – пристрої комутації.

Аналіз попередніх досліджень. Дослідженню особливостей аспектів налаштування пристроїв комутації комп'ютерних мереж, основних характерних рис присвячені праці

закордонних науковців: Алессандра Делліні, Леонарда Клейнрока., Аннандро Датта, Фредеріка Й. Хіллса, Волтера Класса.

Виклад основного матеріалу. У наш час мережі відіграють велике значення у підтримці діяльності не лише великих компаній та установ, а й малих підприємств. Ключовими вузлами у всіх цих мережах виступають комутатори. Оскільки вони з'єднують пристрої, які спільно використовують ресурси.

Пристрій комутації, іншими словами комутатор – це апаратний компонент, відповідальний за ретрансляцію даних із мережі до кінцевої точки призначення за допомогою комутації пакетів, ідентифікації MAC-адреси та системи багатопортового мосту.

Якщо розглянути модель OSI – побачимо, що мережевий комутатор працює на рівні 2 каналу передачі даних архітектури взаємодії відкритих систем (рис. 1).

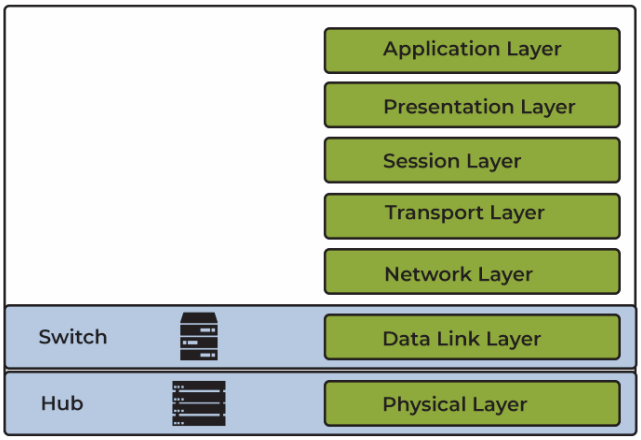


Рис. 1. Модель OSI

Вони також можуть функціонувати там, де маршрутизація відбувається на мережевому рівні 3. Комутатори є стандартними компонентами в мережах Ethernet, Fiber Channels, InfiniBand і асинхронному режимі передачі (ATM). Однак більшість сучасних комутаторів використовують Ethernet.

Розглянувши площу інтеграції мережевого комутатора, ми можемо зробити висновок, що він з'єднує майже всі мережеві пристрої (принтери, комп'ютери та бездротові пристрої/точки доступу) і дозволяє користувачам обмінюватися пакетами даних. Комутатори можуть бути, як апаратними, так і програмними віртуальними пристроями, які керують фізичними системами. У сучасних мережевих системах комутатори складають переважну масу мережевого обладнання.

Якщо розглянути принцип роботи комутаторів ми побачимо наступне – коли пристрої під'єднанні до комутаторів, вони записують інформацію про керування доступом до медіа (MAC) пристрою. Ця адреса є кодом, який зберігається на картці мережевого інтерфейсу пристрою (NIC), яка є частиною пристрою, яка підключається до комутатора через кабель Ethernet.

Комутатор перевіряє адресу пункту призначення та передає пакет на пристрої через відповідні порти. Більшість комутаторів оснащені можливостями повного дуплексу, щоб мінімізувати ймовірність колізій у мережевому трафіку. Це дає пакетам всю пропускну здатність з'єднання між пристроєм і комутатором.

Незважаючи на те, що комутатори зазвичай виконують функції на рівні 2, вони можуть працювати на рівні 3. Це необхідно для того, щоб можна було створити віртуальні локальні мережі (VLAN) – тобто логічні сегменти мережі, які виходять за межі підмереж. Трафік повинен проходити між комутаторами, щоб переходити з однієї підмережі в іншу, що полегшується завдяки їх вбудованим можливостям маршрутизації.

Мережеві комутатори доступні в різних типах і категоріях для різних випадків використання (рис. 2).

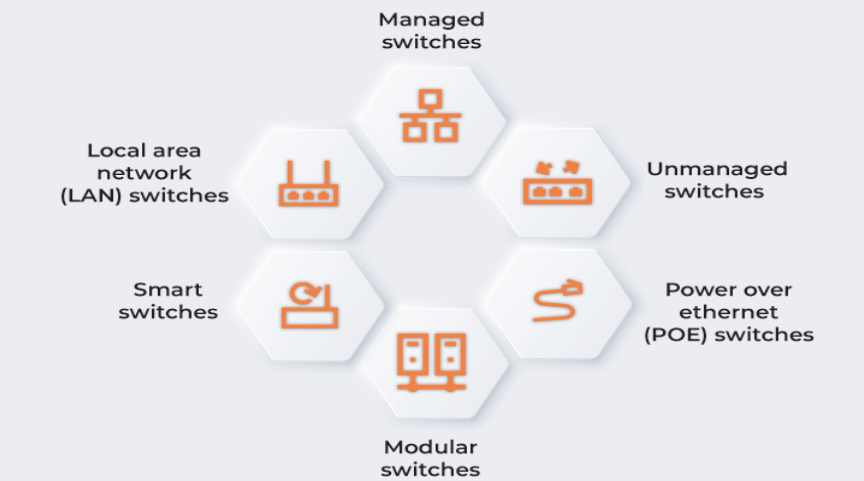


Рис. 2. Типи мережевих комутаторів

Комутатори діляться на 6 основних типів [1]:

- Некеровані комутатори
- Керовані комутатори
- Комутатори Power over Ethernet (POE)
- Комутатори локальної мережі (LAN)
- Smart комутатори
- Модульні комутатори

Найпростіші у використанні комутаційні пристрої – це некеровані комутатори. Вони розширюють з'єднання Ethernet локальної мережі, дозволяючи додаткові підключення до Інтернету для локальних пристроїв. Некеровані комутатори відносно дешеві, але низькі можливості роблять їх непридатними для багатьох корпоративних задач.

А ось керовані комутатори використовуються частіше всього у комерційних і корпоративних мережах. Вони забезпечують більшу ємність і можливості для IT-фахівців. Для налаштування керованих комутаторів використовуються інтерфейси командного рядка та Web-інтерфейси.

Для швидкої і зручної інтеграції у свою мережу точок доступу, відеоспостереження, телефонії використовуються комутатори з підтримкою Power over Ethernet (POE). PoE – це спосіб подачі живлення постійного струму на малопотужні пристрої через дріт локальної мережі. Пристрої з цією технологією дозволяють уникнути потреби в додаткових розетках і робить встановлення ефективним. Комутатор із підтримкою PoE також безпечніший, оскільки вихідна потужність низька та інтелектуально керована.

Комутатори локальної мережі зазвичай використовуються для зв'язку між розташуваннями у внутрішній локальній мережі компанії. Ефективний розподіл пропускної здатності запобігає накладанню пакетів даних під час їх переміщення по мережі. Ці комутатори зменшують перевантаженість мережі або вузькі місця, надсилаючи пакет даних лише призначеному отримувачу.

Smart комутатори називають розумними або інтелектуальними. Вони виходять по функціоналу за межі некерованого комутатора, але менші, ніж у звичайного керованого комутатора.

Найгабаритнішими є модульні комутатори. Вони дозволяють за потреби додавати модулі розширення, джерела живлення та вентилятори охолодження забезпечуючи більшу гнучкість у міру зростання мережі. Однак ці комутатори значно дорожчі за стаціонарні та часто використовуються у великих мережах.

Усі ці комутатори окрім некерованих та Smart, ще можуть підтримувати таку функцію, як стекування.

Розібравшись з типами комутаторів, тепер потрібно перейти до аспектів налаштування пристроїв комутації комп'ютерних мереж. До аспектів налаштування відноситься:

- Першим і найголовнішим аспектом у побудові мережі є налаштування мережевої топології (рис. 3). Це означає визначення фізичної структури мережі, включаючи кількість пристроїв, їх розташування та зв'язки між ними.

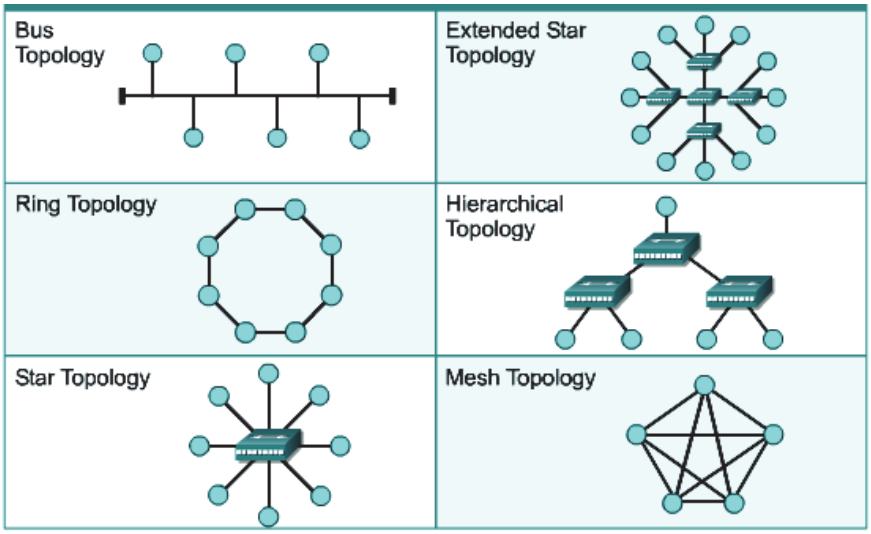


Рис. 3. Топологія мереж

- Конфігурація портів. Налаштування портів комутатора є одним із основних аспектів налаштування пристроїв комутації. Це включає в себе налаштування портів для певних типів трафіку, встановлення швидкості передачі даних, дуплексу та увімкнення/вимкнення функцій, таких як Port Security, VLAN.
- Окремо потрібно винести VLAN конфігурацію. Налаштування Virtual Local Area Network (VLAN) дозволяє розділити мережу на логічно окремі сегменти, що може покращити безпеку та керованість мережі (рис. 4).

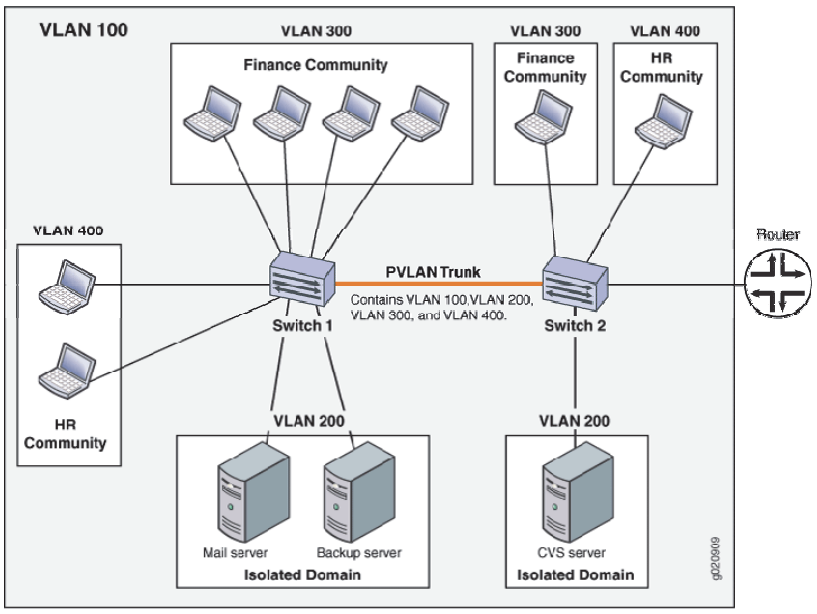


Рис. 4. Розбиття мережі на VLAN

На (рис. 4) видно, що користувачі та пристрої поділені на групи: HR, Finance, Servers. Вони всі поєднані комутаторами та певна група знаходиться у відповідному VLAN`і. У такому випадку група користувачів HR ні при яких обставинах не отримає дані від групи Finance, що у свою чергу може гарантувати збереження конфіденційної інформації.

Ще однією функцією налаштування VLAN виступає налаштування тегованих та нетегованих портів.

- Конфігурація безпеки. Безпека є ключовим аспектом налаштування комутаційних пристроїв. До таких функцій безпеки можна віднести: Port Security, ACL, RADIUS і т.п. Ці функції допомагають забезпечити безпеку мережі, запобігти несанкціонованому доступу та захистити від атак.
- Наступним не менш важливим аспектом є налаштування QoS. Quality of Service (QoS) дозволяє оптимізувати продуктивність мережі для різних типів трафіку. Налаштування QoS включає встановлення пріоритету для різних типів трафіку і налаштування засобів контролю трафіку, таких як policing і shaping.
- Моніторинг. Він включає встановлення засобів моніторингу та аналізу трафіку, таких як SPAN і NetFlow. Моніторинг дозволяє адміністраторам відстежувати використання мережних ресурсів та швидко реагувати на проблеми у мережі [2].

Це лише деякі з аспектів налаштування пристроїв комутації. Кінцевий список залежить від конкретних вимог та налаштувань у кожній мережі.

Пристрої комутації як і технології розвиваються з кожним роком. Не так давно у мережах використовувались прості концентратори, а вже зараз за допомогою мов програмування можна керувати керованими комутаторами та всією мережею в цілому.

Як приклад було розглянуто пристрої комутації корпорації Hewlett Packard Enterprise підрозділу Aruba Network. Одже Python є однією з мов програмування, які можна використовувати для програмування комутаторів Aruba [3]. Для програмування комутаторів Aruba з використанням Python доступний набір інструментів ArubaOS-CX, який надає розширений доступ до комутатора за допомогою REST API та бібліотек Python для взаємодії з ним. Ось один з прикладів (рис. 5).

```python
from pycentral.base import ArubaCentralBase
from pprint import pprint

# Create an instance of ArubaCentralBase using API access token
# or API Gateway credentials.
central_info = {
    "base_url": "<api-gateway-domain-url>",
    "token": {
        "access_token": "<api-gateway-access-token>"
    }
}
ssl_verify = True
central = ArubaCentralBase(central_info=central_info,
                           ssl_verify=ssl_verify)

# Sample API call using 'ArubaCentralBase.command()'
# GET groups from Aruba Central
apiPath = "/configuration/v2/groups"
apiMethod = "GET"
apiParams = {
    "limit": 20,
    "offset": 0
}
base_resp = central.command(apiMethod=apiMethod,
                            apiPath=apiPath,
                            apiParams=apiParams)
pprint(base_resp)
```

Рис. 5. Здійснення виклику API за допомогою pycentral base

ArubaOS-CX також підтримує використання мови програмування Ansible, що дозволяє автоматизувати задачі на комутаторах Aruba.

Висновок: Сучасний світ, потреби сучасних підприємств та установ не може обійтись без пристроїв комутації та маршрутизації. Будь яка інформація зараз у більшості випадків передається через мережу. Тому актуальність цих пристроїв завжди є на вищому рівні. Згідно із потреб бізнесу, комутаційні пристрої поділені на сегменти: малий бізнес, середній бізнес та Enterprise. В свою чергу кожен сегмент має свої аспекти та правила налаштування пристроїв комутації. А кожен пристрій комутації має різні рівні апаратного та програмного забезпечення, для гарантування безпеки даних.

Список використаних джерел

1. Портал Cisco, Правильний вибір комутаторів для вашого бізнесу \\ Режим доступу: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/understanding-the-different-types-of-network-switches.html (останнє звернення 02.04.2023)
2. Портал Aruba Networks, AOS-CX Monitoring Guide \\ Режим доступу: https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/monitoring_83xx.pdf (останнє звернення 04.04.2023)
3. Публікація Linkedin, Dinusha Madusanka Chandrasinghe System Engineer у Zone24x7, Запуск автоматизації комутатора з Python \\ Режим доступу: https://www.linkedin.com/pulse/start-automation-arubaos-cx-switch-python-chandrasinghe (останнє звернення 21.03.2023)

Робота виконана під науковим керівництвом доцента
ДЕСЯТКО А. М.

АНАЛІЗ ПІДХОДІВ ДО ВИЯВЛЕННЯ РОСІЙСЬКИХ СЛІВ В УКРАЇНСЬКИХ ВЕБДОДАТКАХ

ЛАВРІНЕНКО В., 2мз курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті проаналізовано сучасні принципи створення інформаційної системи для виявлення російських слів, у вебдодатках. Розглянуто створення інформаційної-системи та використання готових рішень. Зазначено переваги та недоліки методів виявлення російських слів.

The article discusses modern principles of creating an information system for detecting Russian words in web applications. The creation of an information system and the use of ready-made solutions are considered. The advantages and disadvantages of methods for detecting Russian words are noted.

Актуальність. Згідно з законом «Про забезпечення функціонування української мови як державної» всі українські вебресурси повинні використовувати українську мовну версію. Якщо українська версія вебресурсу відсутня, її необхідно створити. За відсутності української мовної версі, з 16 червня 2022 року передбачається штраф в розмірі від 3400 до 7500 грн, сума штрафу залежить від багатьох чинників, таких як кількість порушень, то що. Якщо вебресурс не відреагує, та не приділить вирішення цьому питанні свій час, повторний штраф буде сягати в розмірі 7500 грн до 11900 грн, інформація актуальна на час написання

цієї статті. Даний закон впливає на бізнес, та має на мету забезпечення і захист мовних прав та потреб українців, української мови, зокрема, забезпечення її використання в усіх сферах життя, включаючи офіційне спілкування, освіту, науку та культуру. Забезпечувати доступність та якість мовної освіти, а також розвивати мовну культуру серед населення.

Метою статті є дослідження використання різних методів, для створення антоматизованої інформаційної системи для виявлення російських слів, в українських вебдодатках.

Об'єктом дослідження є процес виявлення російських слів в українських вебдодатках.

Предмет дослідження – підходи, методи та інструменти, які можуть бути використані для ефективного виявлення російських слів в українських вебдодатках.

Аналіз попередніх досліджень. Демонструє що багато вебдодатків, розроблених в Україні, містять російські слова, що порушує мовні права українців і може призвести до отримання штрафів, втрати національної ідентичності. Для виявлення таких слів використовують різні методи та інструменти, які потребують подальшого дослідження та удосконалення.

Для виявлення російських слів в українських вебдодатках існує кілька підходів, кожен з яких має свої переваги та недоліки. Один з таких підходів – це використання морфологічного аналізу. Цей метод ґрунтується на аналізі граматичних ознак слова, таких як час, кількість, рід тощо. Використання морфологічного аналізу дозволяє виявляти російські слова, які були написані українськими літерами.

Цей метод ґрунтується на аналізі морфологічних характеристик слів, таких як закінчення, префікси та суфікси:

- Порівнювати закінчення слів української та російської мов, оскільки вони часто відрізняються одне від одного.
- Під час морфологічного аналізу слово розбивається на основу та закінчення, після чого проводиться перевірка основи на належність до української або російської мови. Слова, які мають російську основу та українське закінчення, можуть бути віднесені до російської мови.
- Аналіз префіксів та суфіксів, які можуть бути специфічні для російської мови. Наприклад, російське слово «перервати» має префікс «пере-», який не використовується в українській мові. Таким чином, якщо слово містить російський префікс або суфікс, то це може вказувати на його походження.
- Використання списку ключових слів з російської мови. Наприклад, такий список може включати такі слова, як «россия», «москва», «рубль», «кремль», «путин» тощо. Після того, як список ключових слів складено, можна провести пошук цих слів у тексті сторінки. При цьому варто враховувати не лише точне співпадіння слів, але й їх форми - наприклад, російське слово «москва» може зустрічатися у формі «Москви», «Москві», «Москвою» тощо.
- Використання програмного забезпечення, яке виконує автоматичний аналіз тексту і визначає мову, до якої він належить.

Інший підхід полягає в застосуванні статистичного аналізу тексту. Цей метод базується на виявленні частоти вживання певних слів і виразів у тексті. Використання статистичного аналізу дозволяє виявляти російські слова, які були написані кирилицею. Один із методів є використання навчальної вибірки текстів, що містять російські та українські слова, для побудови статистичних моделей. Далі ці моделі можна використовувати для визначення ймовірності того, що дане слово є російським. За допомогою цього методу можна виявляти російські слова в українських текстах, навіть якщо вони були додані в текст з помилкою або намірено змінені.

- Розрахунку відсотку вживання російських слів в тексті в порівнянні з українськими словами. Наприклад, якщо відсоток вживання російських слів перевищує певний поріг, можна вважати, що текст містить російський контент.
- Використання біграм для виявлення російських слів. Біграми називаються пари слів, які зустрічаються разом у тексті. За допомогою статистичного аналізу можна визначити, які біграми є типовими для російської мови, і використовувати ці знання для виявлення російських слів у тексті..
- Аналіз контексту для виявлення російських слів. Наприклад, якщо слово часто зустрічається поряд з російськими словами, ймовірно, що воно також є російським.
- Метод TF-IDF. Цей метод дозволяє визначити ступінь важливості певного слова в тексті, порівнюючи його частоту в тексті з частотою використання цього слова в інших текстах. Якщо слово зустрічається рідко в інших текстах, але досить часто в конкретному тексті, то це свідчить про те, що це слово є важливим для розуміння змісту цього тексту.
- Використання алгоритму машинного навчання, який навчається розпізнавати певні ознаки російської мови в тексті, наприклад, наявність специфічних закінчень слів, використання певних словосполучень чи граматичних форм.

Всі ці методи можна поєднувати між собою та з іншими підходами, такими як морфологічний аналіз та інші методи машинного навчання, для досягнення більш точного виявлення російських слів в українських вебдодатках.

В розробці дуже важкі умови, програма має працювати та відповідати критеріям, розробка повинна супроводжуватись документацією, а спеціалісти мають відповідати критеріям. Умови мають бути написані зрозумілі, і завдання які будуть виникати повинні виконуватись в відповідні строки. Розробка автоматизованої системи пошуку російських слів, має починатись зі зрозумілих умов, та призначені самої системи. На даний час та в майбутньому виникає потреба в розробці автоматизованої системи пошуку російських слів в українських вебдодатках. Така система має бути достатньо ефективною та точною, щоб забезпечити максимальний захист мовних прав громадян та виконання законодавства. Автоматизована система пошуку російських слів може використовувати різні методики, наприклад ті що було описані вище.

Автоматизовані системи пошуку слів використовуються в різних сферах, наприклад, в комп’ютерних програмах для обробки текстів, в пошукових системах Інтернету, в системах розпізнавання мови тощо. Ось декілька прикладів автоматизованих систем пошуку слів:

- Пошукові двигуни в Інтернеті, такі як Google, використовують різні алгоритми для пошуку та відображення результатів. Одним з таких алгоритмів є алгоритм TF-IDF (term frequency–inverse document frequency), який визначає важливість кожного слова в тексті, враховуючи частоту вживання слова в тексті та частоту вживання слова в інших документах.
- Програми для обробки текстів, такі як Microsoft Word, можуть автоматично підсвічувати слова, які використовуються надто часто або надто рідко. Такі програми також можуть автоматично відображати синоніми для вибраних слів, що полегшує процес написання тексту.
- Системи розпізнавання мови, такі як Siri від Apple, використовують алгоритми для розуміння мовлення користувача та відповіді на його запити. Для цього системи використовують навчальні моделі, які навчаються розпізнавати та інтерпретувати різні слова та фрази.

Розглянемо приклад використання морфологічного аналізу для виявлення російських слів. Один з прикладів використання морфологічного аналізу для виявлення російських слів на вебсайтах є програмний засіб LanguageTool (рис. 1).

LanguageTool дозволяє перевіряти текст на наявність помилок, в тому числі й російських слів. LanguageTool використовує морфологічний аналіз для визначення мови слів та їхньої орфографії.

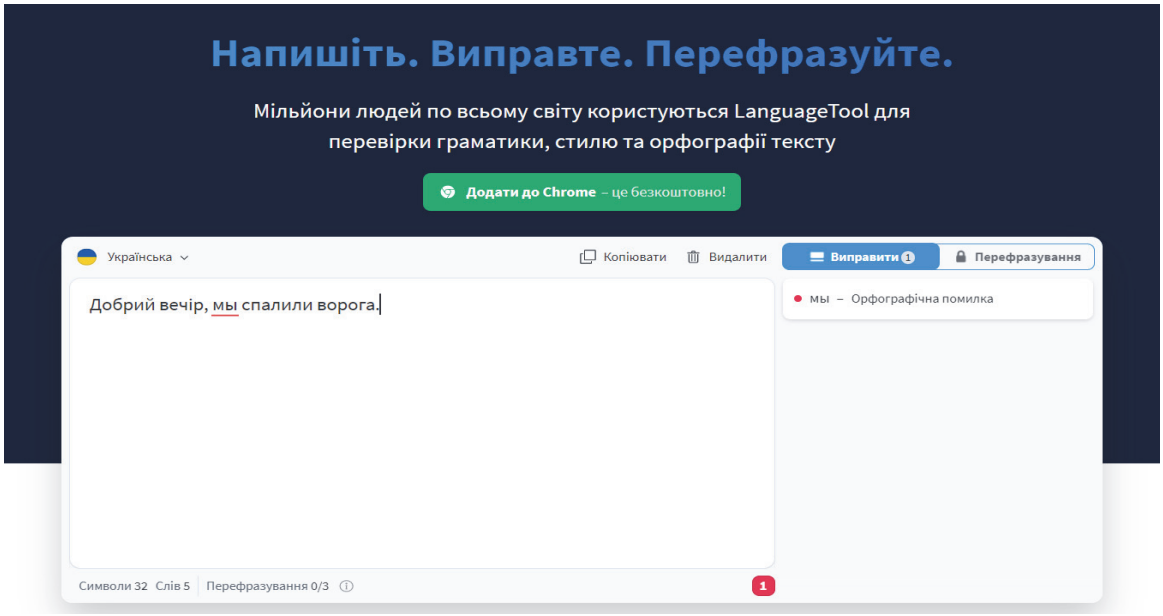


Рис. 1. Інтерфейс вебдодату Language Tool

Другий приклад полягає в використання морфологічного аналізу програмного засобу Hunspell, що дозволяє проводити перевірку правопису тексту на основі словника та правил морфології різних мов. У налаштуваннях Hunspell можна вказати список мов в тому числі українську, які повинні бути використані для перевірки тексту, та налаштувати правила перевірки правопису. Hunspell – це засіб перевірки орфографії LibreOffice, OpenOffice.org, Mozilla Firefox і Thunderbird, Google Chrome, а також використовується пакетами пропрієтарного програмного забезпечення, такими як macOS, InDesign, memoQ, Opera і SDL Trados. Основні можливості. Розширена підтримка мовних особливостей; Кодування символів Unicode, складення та складна морфологія.

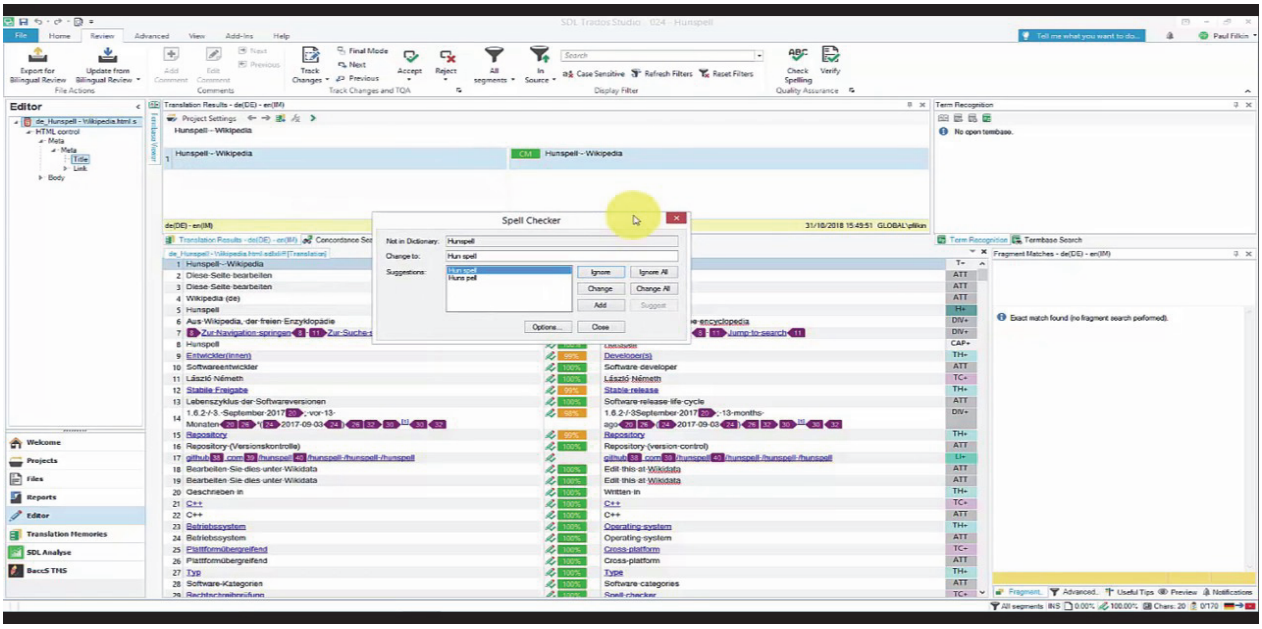


Рис. 2. Інтерфейс Hunspell

Покращена пропозиція з використанням схожості n-грам, даних про вимову на основі правил і словника. Hunspell базується на MySpell і також працює зі словниками MySpell. Бібліотека C++ під триліцензією GPL/LGPL/MPL. Інтерфейси та порти: AndroidHunspellService (для Android, на основі форка Chromium Hunspell), Enchant (загальна бібліотека орфографії з проєкту Abiword), XSpell (порт macOS, але Hunspell є частиною macOS з версії 10.6 (Snow Leopard) і тепер достатньо помістити файли словника Hunspell у ~/Library/Spelling або /Library/Spelling для перевірки орфографії), Delphi, Java (JNA, JNI), Perl, .NET, .NET Standard, Python, Ruby (1, 2, 3), UNO, RichEdit. Переклади: Hunspell було перекладено кількома мовами.

Наступна програма з застосуванням морфологічного аналізу для пошуку російських слів на вебсайтах є розробка програми мовою програмування Python з використанням бібліотеки Natural Language Toolkit (NLTK). Ця програма може виявляти російські слова на вебсторінках, використовуючи морфологічний аналіз. Програма спочатку завантажує текст сторінки, а потім проводить морфологічний аналіз кожного слова у тексті. Якщо слово має російську морфологію, то воно додається до списку російських слів. Ще одним прикладом застосування морфологічного аналізу є розробка системи автоматичного виявлення російських слів на вебсайтах з використанням відкритих даних WordNet. Ця система використовує WordNet для знаходження синонімів російських слів. Після отримання списку синонімів, система проводить морфологічний аналіз кожного слова та видаляє слова, які не є російськими. Для розробки автоматизованої системи пошуку російських слів на вебсайтах можна використовувати різні програмні засоби та бібліотеки морфологічного аналізу, такі як Mystem, Pymorphy2, NLTK та інші.

Розглянемо приклади використання статистичного аналізу для виявлення російських слів. Статистичного аналіз пошуку російських слів на сайтах полягає у виявленні російських слів шляхом аналізу тексту сторінки без необхідності виконання запитів до бази даних або зовнішніх ресурсів. Цей метод зазвичай використовується для оцінки мовної ситуації на вебсайтах, а також для виявлення потенційно небезпечного контенту, що може містити пропаганду агресивних чи ворожих до України інтересів. Прикладом є програма YARA, яка є відкритою системою виявлення шаблонів для пошуку специфічних рядків у тексті. Вона може використовуватися для пошуку російських слів та інших специфічних виразів на вебсайтах. Також можна використовувати спеціальні скрипти або програми, які виконують статистичний аналіз HTML-коду вебсторінок для пошуку російських слів та інших специфічних виразів. Один з прикладів такої програми - grep, який є утилітою командного рядка в UNIX-подібних операційних системах.

- Інструмент Ahrefs: Ahrefs є платним інструментом SEO-аналізу, який може бути використаний для виявлення російських слів на вебсторінках. Це робиться за допомогою функції Content Explorer, яка дозволяє ввести URL-адресу вебсторінки і отримати список всіх слів на сторінці, разом з інформацією про їх частоту вживання та контекст вживання.
- Інструмент Diffbot: Diffbot - це API, яке надає доступ до структурованої інформації з вебсторінок. Цей інструмент може бути використаний для отримання списку всіх слів на вебсторінці, а також для відфільтрування російських слів за допомогою регулярних виразів або мовних аналізаторів.
- Сайт-аналізатор Ahrefs - платформа для вивчення та аналізу SEO-показників вебсайту. Для аналізу слів на сайті, можна використовувати інструмент «Site Explorer», який надає статистику по кількості слів та фраз на сайті, а також їх розташування на сторінках.
- Консоль розробника браузера - це інструмент, який надається у браузері для дебагу вебсайтів. Вона може бути використана для відстеження різних аспектів вебсторінок, включаючи використання слів.

- Власноруч написана програма – програмування статистичного аналізу для виявлення слів можна виконати самостійно з використанням різних мов програмування та бібліотек, таких як Python, Java, JavaScript тощо.

Розглянемо відмінності та різницю в підходах статистичного аналізу, та морфологічного в пошуку російських слів. Статистичний та морфологічний аналіз – це дві різні методи, які можуть використовуватися для пошуку російських слів на вебдодатках. Морфологічний аналіз базується на збігу морфологічної форми слів. Це означає, що програма виявлятиме російські слова, незалежно від того, як вони написані - у відмінкових формах, зі зміненою закінченням чи зі складними похідними словами. Статистичний аналіз використовує інший підхід - він базується на виявленні конкретних слів або фраз, що відповідають певним шаблонам. Наприклад, можна створити список слів або фраз, що зазвичай вживаються у російській мові, і потім знайти їх на сайті. Такий підхід може бути менш точним, оскільки існує можливість пропустити деякі російські слова, які не входять до списку, або знайти слова, які не мають російського походження, але збігаються з шаблоном. Обидва підходи можуть бути корисними для виявлення російських слів на сайтах, але їх ефективність залежить від конкретної ситуації та використовуваної методології.

Проаналізуємо які варіанти продукту вибере кінцевий користувач або бізнес. А саме готове рішення програму для пошуку російський слів у вебдодатках, або написання своєї власної програми. Використання готових програм для виявлення російських слів в українських вебдодатках може бути ефективним та зручним варіантом для користувачів, які не мають досвіду у програмуванні. Готові програми зазвичай мають зроблену значну частину роботи, таку як написання алгоритму виявлення слів, розробку інтерфейсу користувача та відлагодження програми. Однак, написання своєї програми має свої переваги. Зокрема, це дозволяє точніше налаштувати алгоритм виявлення слів під конкретні потреби користувача. Також, при розробці власної програми користувач може бути впевнений у безпеці та конфіденційності своїх даних. Розглянемо основні різниці між використанням готових програм та написанням своєї програми для виявлення російських слів в українських вебдодатках:

- Розробка: для написання власної програми потрібно мати знання з програмування та мати достатньо часу для розробки та відлагодження програми. Готові програми можна встановити та використовувати без необхідності розробки.
- Налаштування: написання власної програми дозволяє точніше налаштувати алгоритм виявлення слів під конкретні потреби користувача. Готові програми можуть мати обмежені налаштування та можуть не задовольняти потребам користувача.
- Вартість: використання готових програм зазвичай коштує гроші, тоді як написання власної програми може бути безкоштовним.
- Безпека та конфіденційність: написання власної програми дозволяє користувачеві бути впевненим у безпеці.

Можемо зробити висновок що остаточний вибір за користувачем або компанією, тому що ситуації різні, та підходи в виборі. Але вибір повинен відповідати вимогам, повністю, або хоч би частково.

Висновки. Виявлення російських слів на українських вебсайтах є актуальною проблемою, особливо в контексті бізнесу, та боротьби з інформаційною агресією. Для виявлення російських слів на українських вебсайтах можна використовувати як морфологічний аналіз, так і статистичний аналіз. Готові програми для виявлення російських слів на українських вебсайтах можуть бути корисним інструментом для розв’язання даної проблеми. Проте, написання своєї програми для виявлення російських слів може бути більш ефективним варіантом, оскільки дозволяє більш гнучко налаштувати алгоритм під конкретні потреби користувача. Оскільки виявлення російських слів на українських вебсайтах є складною задачею, необхідно розвивати та вдосконалювати існуючі методи і інструменти для її вирішення.

Список використаних джерел

1. Шуба М. О. (2018) Підходи до виявлення російських слів в українських вебдодатках, 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)
2. LanguageTool – Перевірка граматики, стилю та орфографії онлайн URL: https:// languagetool.org/uk
3. Hunspell dictionaries in Studio. URL: https://multifarious.filkin.com/2018/10/31/hunspell-dictionaries-in-studio/
4. Ahrefs – SEO Tools & Resources To Grow Your Search Traffic URL: https://ahrefs.com/
5. Diffbot Knowledge Graph, AI Web Data Extraction and Crawling URL: https://www.diffbot.com/
6. YARA – The pattern matching swiss knife for malware researchers URL: https:// virustotal.github.io/yara/
7. Харченко В. (2017) Виявлення російської мови на українських сайтах за допомогою регулярних виразів. Видавництво Springer серія Communications in Computer and Information Science Том 711.
8. Швець А., Василенко В., Кулик О. (2019) Виявлення російської мови в українському вебпросторі за допомогою регулярних виразів. Соловйов В., Харченко В., Кривінська Н. (ред.) Інженерія перспективних інформаційних систем. CAiSE 2019. Конспекти лекцій з обробки бізнес-інформації, том 353.
9. Манжелій Ю. І., Качмар М. М. Автоматичне виявлення російських слів у текстах українською мовою з використанням засобів морфологічного аналізу. Вісник Хмельницького національного університету. https://core.ac.uk/download/pdf/268531695.pdf
10. Гарбера, І.В. Прикладна морфологія: основи автоматичного морфологічного аналізу тексту: Навчально-методичний посібник. https://r.donnu.edu.ua/handle/123456789/2418

Робота виконана під науковим керівництвом канд. пед. наук, доцента
КОТЕНКО Н. О.

ОСНОВНІ ВИМОГИ ДО ПРОГРАМНОЇ КОМПОНЕНТИ ДЛЯ ЗАБЕЗПЕЧЕННЯ РОБОТИ СТРУКТУРНОГО ПІДРОЗДІЛУ ГОТЕЛЬНОГО ГОСПОДАРСТВА

ЛЕЛЕТІНА Є., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Даний дослід присвячений визначенню основних вимог до програмної компоненти для забезпечення роботи структурного підрозділу готельного господарства. В статті проаналізовано технічні та функціональні вимоги до програмної компоненти, а також відмічені проблеми, які можуть виникнути при розробці та впровадженні програмного забезпечення в готельний бізнес. Було проведено порівняння різних програмних продуктів та методів їх впровадження з метою вибору оптимального рішення для структурного підрозділу готельного господарства. Дослідження також включало розгляд аспектів безпеки та моніторингу роботи програмної компоненти.

This study is dedicated to determining the main requirements for a software component that provides the operation of the structural unit of hotel management. The article analyzes technical and functional requirements for the software component, as well as identifies issues that may arise during the development and implementation of software in the hotel industry. A comparison of different software products and methods of their implementation was carried out in order to choose the optimal solution for the structural unit of hotel management. The research also included consideration of aspects of security and monitoring of the software component.

Актуальність. Зараз готельний бізнес розпочинає поступово відновлюватися після пандемії та в умовах воєнного стану. Зростання попиту на готельні послуги вимагає від підприємств готельного господарства ефективного використання ресурсів та автоматизації процесів управління. У зв'язку з цим, програмне забезпечення для готелів стає все більш популярним.

Однак, розробка та впровадження програмного забезпечення в готельний бізнес можуть викликати ряд проблем, пов'язаних з вимогами до програмної компоненти. Ці вимоги можуть бути технічними та функціональними. Технічні вимоги стосуються апаратної та програмної частини комп'ютерного обладнання, на якому буде запущена програмна компонента, а також мережевих можливостей. Функціональні вимоги стосуються можливостей програмної компоненти та її інтеграції з іншими системами готельного бізнесу.

Об'єктом нашої статті є програмна компонента забезпечення роботи структурного підрозділу підприємств готельного господарювання.

Метою даного дослідження є визначення основних вимог до програмної компоненти для забезпечення роботи структурного підрозділу готельного господарства. Для досягнення цієї мети було поставлено наступні *завдання*:

- проаналізувати технічні та функціональні вимоги до програмної компоненти для забезпечення роботи структурного підрозділу готельного господарства;
- визначити основні проблеми, які можуть виникнути при розробці та впровадженні програмного забезпечення в готельний бізнес;
- провести порівняння різних програмних продуктів та методів їх впровадження з метою вибору оптимального рішення для структурного підрозділу готельного господарства;
- розглянути аспекти безпеки та моніторингу роботи програмної компоненти.

У програмній компоненті для структурного підрозділу готельного господарства мають бути враховані технічні вимоги, пов'язані з апаратним забезпеченням та мережевими можливостями.

Один з головних параметрів апаратного забезпечення, що впливає на швидкість роботи програмної компоненти, є процесор. Найбільш оптимальним варіантом для запуску програмної компоненти є процесор з такими характеристиками: кількість ядер – не менше 4; тактова частота – не менше 2,5 ГГц; кеш – не менше 8 Мб. Також важливим параметром є обсяг оперативної пам'яті (ОЗУ), який повинен бути не менше 8 Гб.

Однак, не менш важливими є мережеві можливості, оскільки програмна компонента повинна мати змогу працювати в мережевому середовищі, щоб мати доступ до інших систем готельного бізнесу. Тому, необхідно встановити на комп'ютер програмне забезпечення для мережевого з'єднання.

Функціональні вимоги стосуються можливостей програмної компоненти та її інтеграції з іншими системами готельного бізнесу. Основні функції програмної компоненти повинні включати:

- резервування номерів готелю;
- прийом та обробка заявок на бронювання номерів;
- розрахунок вартості проживання;
- облік фінансових операцій;
- формування звітів та аналітики.

Також, програмна компонента повинна бути інтегрована з іншими системами готельного бізнесу, наприклад, з системою керування запасами, щоб забезпечити своєчасну доставку необхідних ресурсів, або з системою контролю доступу, щоб забезпечити безпеку проживання гостей.

Розробка та впровадження програмної компоненти для структурного підрозділу готельного господарства може стикнутися з рядом проблем. Одна з найбільш значущих проблем - це складність інтеграції програмної компоненти з іншими системами готельного бізнесу. Ця проблема може виникнути через відмінність форматів та структури даних.

Іншою проблемою може стати відсутність відповідного кваліфікованого персоналу для впровадження та підтримки програмної компоненти. Це може призвести до збільшення витрат на навчання персоналу та на залучення зовнішніх консультантів.

Також важливою проблемою є забезпечення безпеки даних, оскільки програмна компонента зберігає конфіденційну інформацію про клієнтів готелю. Для забезпечення безпеки даних необхідно застосовувати захист інформації за допомогою шифрування та автентифікації.

Після розробки програмної компоненти необхідно провести тестування та валідацію, щоб переконатися в правильному функціонуванні компоненти та відповідності її вимогам. Для цього можна використовувати такі методи:

- функціональне тестування;
- тестування на відповідність вимогам;
- тестування на продуктивність;
- тестування на надійність.

Розробка програмної компоненти для структурного підрозділу готельного господарства є важливим завданням, оскільки вона дозволяє автоматизувати процеси бронювання номерів, розрахунку вартості проживання та обліку фінансових операцій. Однак, для успішної реалізації проекту необхідно врахувати вимоги до апаратного та програмного забезпечення, а також вирішити проблеми, пов’язані з інтеграцією компоненти з іншими системами готельного бізнесу, забезпеченням безпеки даних та підготовкою персоналу.

Тестування та валідація програмної компоненти - важливий етап в розробці програмної компоненти, який дозволяє переконатися в правильному функціонуванні компоненти та відповідності її вимогам. Для успішної розробки та впровадження програмної компоненти для структурного підрозділу готельного господарства необхідно дотримуватися певних етапів розробки та тестування, а також враховувати вимоги до апаратного та програмного забезпечення.

Важливими аспектами для успішного впровадження програмної компоненти є відповідність бізнес-процесам готельного господарства, безпека даних, можливість інтеграції з іншими системами та зручний інтерфейс користувача.

На основі проведеного аналізу та порівняння існуючих рішень для автоматизації роботи готелів було визначено, що найбільш ефективною є інтегрована програмна платформа, що включає в себе різні модулі для автоматизації різних бізнес-процесів готельного господарства, таких як бронювання номерів, облік послуг та продуктів, управління персоналом та інше.

Для забезпечення безпеки даних необхідно застосовувати заходи, такі як шифрування, резервне копіювання та забезпечення захисту доступу до системи. Також важливим аспектом є можливість інтеграції програмної компоненти з іншими системами, такими як системи електронного документообігу та системи обліку витрат.

Зручний інтерфейс користувача є важливим фактором успішного використання програмної компоненти. Необхідно забезпечити зручний та інтуїтивно зрозумілий інтерфейс для користувачів різних рівнів кваліфікації та досвіду роботи з комп’ютером.

Схема взаємодії програмної компоненти з іншими системами та базами даних може виглядати наступним чином:

1. Користувачі взаємодіють з програмною компонентою через веб-інтерфейс, що забезпечує взаємодію з додатком на веб-сервері.

2. Програмна компонента взаємодіє з базою даних, що містить інформацію про персонал готелю, зокрема список працівників і їхні робочі графіки.

3. Програмна компонента взаємодіє з системою електронної пошти для надсилання листів повідомлень про робочі графіки із змінами співробітникам.

4. Програмна компонента може взаємодіяти з системою електронної оплати, щоб оплачувати заробітну плату співробітникам.

5. Програмна компонента може взаємодіяти з системою бронювання готелів, щоб забезпечити інформацію про наявність вільних номерів та розміщення гостей в номерах.

6. Програмна компонента може взаємодіяти з системою контролю доступу, щоб забезпечити безпеку та обмежити доступ до певних приміщень для співробітників і гостей готелю.

7. Програмна компонента може взаємодіяти з системою відеоспостереження, щоб забезпечити безпеку на території готелю та контролювати дотримання правил працівниками та гостями.

8. Програмна компонента може взаємодіяти з системою обліку запасів і забезпечення готелю, щоб забезпечити своєчасне поповнення запасів та підтримання оптимального рівня запасів.

9. Крім того, програмна компонента може інтегруватись з системою онлайн-бронювання, щоб автоматично оновлювати інформацію про наявність номерів та їх ціни на веб-сайті готелю. Це значно спростить процес бронювання та зменшить ризик помилкових бронювань.

10. Нарешті, програмна компонента може забезпечувати гостьовий портал, на якому гості зможуть отримувати необхідну інформацію про готель та його послуги, здійснювати онлайн-замовлення послуг та розваг, а також зв’язуватись з адміністрацією готелю. Це підвищить рівень комфорту для гостей та зменшить навантаження на персонал готелю.

Однією з важливих складових програмної компоненти є система звітності, яка дозволяє отримувати різноманітну статистику і звіти щодо роботи структурного підрозділу готельного господарства. Система звітності взаємодіє з базою даних компоненти, а також може взаємодіяти з системами зберігання даних або відправлення звітів електронною поштою.

Програмна компонента для структурного підрозділу готельного господарства має бути розроблена з врахуванням вимог до її архітектури та функціональності, а також забезпечувати високу надійність та безпеку даних. Для успішної реалізації проекту також необхідно врахувати вимоги до апаратного та програмного забезпечення, а також вирішити проблеми, пов’язані з інтеграцією компоненти з іншими системами готельного бізнесу, забезпеченням безпеки даних та підготовкою персоналу.

Для успішної реалізації проекту необхідно використовувати сучасні методи та інструменти розробки програмного забезпечення, такі як Agile-методології, DevOps-підходи, контроль версій та автоматизоване тестування.

Вибір архітектури програмної компоненти є ключовим етапом в процесі розробки програмного забезпечення. Архітектура повинна відповідати вимогам продукту та принципам проектування програмного забезпечення.

При виборі архітектури програмної компоненти для забезпечення роботи структурного підрозділу готельного господарства було враховано такі фактори:

1. Вимоги до функціональності: програмна компонента повинна забезпечувати можливість бронювання номерів, розрахунку вартості послуг, створенню звітів, підтримки бази даних клієнтів та персоналу готелю.

2. Вимоги до продуктивності: програмна компонента повинна забезпечувати швидку обробку запитів та ефективне використання ресурсів системи.

3. Принципи проектування ПЗ: програмна компонента повинна бути забезпечена високою модульністю, масштабованістю та гнучкістю.

Враховуючи ці фактори, оптимальною є клієнт-серверна архітектуру. Клієнтська частина забезпечує інтерфейс користувача та взаємодію з сервером, а серверна частина забезпечує доступ до бази даних та обробку запитів.

Така архітектура є популярною та має декілька переваг. Клієнтська частина може бути реалізована на різних платформах, що забезпечує більшу гнучкість та доступність для користувачів. Крім того, серверна частина може бути масштабована, що забезпечує підтримку більшого обсягу запитів.

Вибір архітектури програмної компоненти здійснюється з урахуванням вимог до функціональності, продуктивності та простоти системи. Також потрібно враховувати принципи проектування ПЗ, такі як розширюваність, модульність та зручність тестування. В результаті аналізу різних варіантів, можна стверджувати, що найкраще використовувати мікросервісну архітектуру, що дозволяє розділити систему на окремі сервіси, що функціонують незалежно один від одного та забезпечують більшу гнучкість та масштабованість системи. Така архітектура також сприяє зменшенню залежностей між компонентами та полегшує розгортання та підтримку системи.

Архітектура мікросервісів дозволяє розділити систему на невеликі, незалежні модулі - мікросервіси, кожен з яких відповідає за свою функціональність та може бути розгорнутий та масштабований окремо. Це дозволяє досягти більшої гнучкості та швидкості розробки та розгортання, а також покращує можливості масштабування та забезпечує високу доступність системи.

Крім того, мікросервісна архітектура підтримує розподілений розвиток, що дозволяє розробникам працювати паралельно над різними частинами системи та підтримувати їх незалежність. Також, ця архітектура дозволяє легко замінювати та розширювати окремі мікросервіси без впливу на роботу інших частин системи.

У контексті програмної компоненти для забезпечення роботи структурного підрозділу готельного господарства, мікросервісна архітектура дозволить розділити систему на окремі модулі, що відповідають за різні функції, такі як бронювання номерів, ресторанна служба, облік фінансів тощо. Кожен мікросервіс може мати свою власну базу даних, що сприяє відокремленості та безпеці даних.

Застосування мікросервісної архітектури також дозволить підвищувати масштабованість системи, що є критичним для розвитку бізнесу. Крім того, використання мікросервісів дозволить зменшити залежність між різними компонентами системи та спростити процес розгортання та моніторингу окремих сервісів. В результаті, вибір мікросервісної архітектури допоможе забезпечити більш високу гнучкість, масштабованість, надійність та продуктивність програмної компоненти.

Одним з головних викликів при розробці програмної компоненти для структурного підрозділу готельного господарства є забезпечення її інтеграції з іншими системами готельного бізнесу, такими як система бронювання номерів, система обліку фінансів та система управління ресурсами. Для успішної інтеграції необхідно визначити стандарти та протоколи комунікації між компонентами та забезпечити взаємодію з системами, які вже використовуються в готелі.

Крім того, врахування вимог до безпеки даних є критичним аспектом при розробці програмної компоненти для готельного бізнесу. Забезпечення конфіденційності, цілісності та доступності даних є ключовими вимогами до програмного забезпечення готельного господарства. Для досягнення цієї мети необхідно використовувати шифрування, аутентифікацію та авторизацію, а також резервне копіювання даних та моніторинг безпеки.

Розробка програмної компоненти для структурного підрозділу готельного господарства є складним та відповідальним завданням, яке потребує уважного вивчення вимог до функціональності та безпеки даних, використання сучасних методів та інструментів розробки програмного забезпечення та інтеграції з іншими системами готельного бізнесу.

Для успішної реалізації проекту необхідно визначити та проаналізувати потреби та вимоги клієнтів та користувачів, а також розробити ефективну стратегію тестування та впровадження програмної компоненти. Дотримання всіх цих критеріїв дозволить досягти високої якості та ефективності роботи структурного підрозділу готельного господарства.

В цілому, розробка програмної компоненти для структурного підрозділу готельного господарства є складним та відповідальним завданням, але за дотриманням всіх вимог та рекомендацій може бути успішно реалізована. Така компонента допоможе підвищити ефективність та якість обслуговування гостей, знизити витрати та покращити управління готельним бізнесом в цілому. Для того, щоб досягти успіху, необхідно забезпечити високу якість програмного забезпечення, а також забезпечити його безпеку та надійність.

Висновки У цій статті ми дослідили основні вимоги до програмної компоненти для забезпечення роботи структурного підрозділу готельного господарства. Зокрема, ми розглянули такі вимоги, як підтримка різноманітних функцій готельної діяльності, надійність та безпека, зручність та ефективність використання, можливість інтеграції з іншими системами, масштабованість та гнучкість.

В цілому, розробка програмної компоненти для забезпечення роботи структурного підрозділу готельного господарства є важливим кроком у покращенні ефективності та якості обслуговування гостей готелю. З використанням сучасних методів та інструментів розробки програмного забезпечення, можна створити надійну та ефективну систему, яка забезпечить успішну діяльність готелю та задоволення потреб клієнтів.

Список використаних джерел

1. Liu, Y., & Chen, C. A service quality evaluation model for hotel online booking systems. Journal of Hospitality and Tourism Technology, №7(2),-2016.- 168-183. doi: 10.1108/JHTT-06-2015-0025
2. Горбачук, В. Використання програмного забезпечення у готельному господарстві. Технології та дизайн, № 4(32). – 2019. – С. 51–55.
3. Павленко, О. Розробка програмного забезпечення для автоматизації роботи готельного бізнесу. Молодий вчений, № 3(35). – 2016. – С. 186–189.
4. Ходаківська, Ю.. Застосування програмного забезпечення у готельному бізнесі. Економічний часопис-XXI, № 3-4(2). – 2019. – С. 64–68.

Робота виконана під науковим керівництвом канд. екон. наук, доцента
ТИЩЕНКА Д. О.

ПРОГРАМНО-АПАРАТНІ ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

ЛІЩУК О., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні програмно-апаратні засоби криптографічного захисту інформації, зокрема принципи роботи симетричного та асиметричного шифрування на прикладі шифрів AES та RSA, а також вітчизняного шифру «Калина». Зазначено переваги використання базових принципів стеганографії для захисту інформації від несанкціонованого доступу.

The article discusses the main software and hardware tools for cryptographic protection of information, in particular, the principles of symmetric and asymmetric encryption on the example of AES and RSA ciphers, as well as the national cipher «Kalyna». The advantages of using the basic principles of steganography to protect information from unauthorized access are noted.

Актуальність. У всі часи інформація була важливим ресурсом, і володіння достовірною та актуальною інформацією завжди давало перевагу одній зі сторін. Проблема захисту інформації виникла на зорі зародження людського суспільства, і актуальність цієї проблеми з кожним днем все зростала. Уже сьогодні людство ступило на новий етап свого розвитку – перехід до нового типу постіндустріального суспільства, де головну роль відіграє інформація. Паралельно з прогресом у сфері інформаційних технологій постійно збільшується і кількість можливих загроз, починаючи від технічних несправностей і закінчуючи діями зловмисників. Постійне збільшення обсягу конфіденційної інформації, широке використання різноманітних технічних засобів для її оброблення, зберігання та передавання, поява нових методів і засобів несанкціонованого доступу до інформації потребують відповідні програмно-апаратні комплекси у сфері криптографічного захисту інформації.

Характерною рисою сучасного суспільства є той факт, що інформація являє собою один із найважливіших ресурсів, а засоби її обробки та зберігання використовуються практично в усіх сферах нашої діяльності – від забезпечення національної безпеки та охорони здоров'я до купівель через інтернет і звичайного спілкування. Постійно збільшується кількість людей, зайнятих виробництвом і споживанням інформації, дедалі більше зростає значущість знань і частка розумової праці. Найостанніші досягнення людства в галузі ІТ активно використовуються в нашому повсякденному житті, і з кожним днем збільшується частка інформаційних технологій у житті суспільства. Цей соціальний і технологічний процес, що є основною движучою силою сучасного суспільства, називається «інформатизація».

Таким чином, людство вже на даному етапі свого розвитку залежить від інформації та інформаційних технологій, що забезпечують її зберігання, обробку та поширення. Тому проблема забезпечення захищеності інформації та інформаційних систем є однією з найважливіших проблем сучасності.

Метою статті є ознайомлення з методами захисту інформації від несанкціонованого доступу, зокрема використання програмно-апаратних засобів криптографічного захисту інформації, а також вивчення стандартів шифрування.

Об'єктом дослідження є дослідження програмно-апаратних засобів захисту інформації та принципів роботи деяких стандартів симетричного та асиметричного шифрування.

Предмет дослідження – програмно-апаратні засоби криптографічного захисту інформації.

Аналіз попередніх досліджень. Дослідженню програмно-апаратних засобів захисту інформації та питанням інформаційної безпеки присвячені праці вітчизняних та закордонних вчених: Тагер Ель-Ґамаля, Ю.Я. Бобало, Б.А. Бабаяна, М.Д. Кіселичника, А.П. Бондарєва, С.С. Войтусіка, А.Я. Горпенюка, Є.І. Яковенко, В.І. Отенко, І.Я. Тишика та ін.

Виклад основного матеріалу. Сукупністю методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації є захист інформації. Для його забезпечення, сьогодні, використовуються засоби захисту інформації та інформаційних систем, реалізованих на апаратному та програмному рівнях. Важливо зазначити, що організаційні, технологічні й апаратні методи захисту, як правило, не можуть бути здійснені без програмної складової, тому захист інформації досягається реалізацією програмних і апаратних засобів разом.

Найпоширенішими прикладами програмних засобів захисту інформації є такі:

- система контролю і управління доступом;
- антивірусне програмне забезпечення;

- шифрувальне програмне забезпечення;
- мережевий екран або брандмауер;
- система виявлення вторгнень (IDS).

На сьогодні шифрування широко застосовують у комп'ютерній техніці для приховування конфіденційної інформації від несанкціонованого використання і для захищеної передачі інформації між різними елементами інформаційної системи. Існує два основних типи алгоритмів шифрування, заснованих на ключах: симетричні та асиметричні, які називаються алгоритмами із закритим і алгоритмами з відкритим ключем.

Симетричні алгоритми являють собою криптографічні алгоритми, у яких ключ шифрування може бути розрахований за ключем дешифрування і навпаки (рис. 1). У більшості симетричних алгоритмів ключі шифрування і дешифрування одні й ті самі. Такі алгоритми вимагають, щоб відправник і одержувач узгодили ключ, що використовується, перед початком зашифрованої передачі повідомлень. Безпека симетричного алгоритму визначається ключем, розкриття якого означає, що будь-хто зможе прочитати зашифровані повідомлення.

Схема симетричного шифрування має п'ять компонентів:

- Відкритий текст: це оригінальне повідомлення або дані, які подаються на вхід алгоритму.
- Алгоритм шифрування: виконує різні заміни і перетворення над відкритим текстом.
- Секретний ключ: секретний ключ також вводиться в алгоритм. Точні заміни та перетворення, що виконуються алгоритмом, залежать від перетворення, які виконує алгоритм та залежать від ключа.
- Зашифрований текст: зашифроване повідомлення, яке отримується на виході. Залежить від відкритого тексту і секретного ключа.
- Алгоритм розшифрування – це, по суті, алгоритм шифрування, який виконується у зворотному порядку.

Для сучасних систем криптографічного захисту інформації сформульовано такі загальноприйняті вимоги:

- зашифроване повідомлення має піддаватися читанню тільки за наявності ключа;
- число операцій, необхідних для розшифровування інформації шляхом перебору всіляких ключів, має виходити за межі можливостей сучасних комп'ютерів;
- знання алгоритму шифрування не повинно впливати на надійність захисту;
- незначна зміна ключа має призводити до суттєвої зміни вигляду зашифрованого повідомлення;
- структурні елементи алгоритму шифрування мають бути незмінними;
- довжина шифрованого тексту має дорівнювати довжині вихідного тексту;
- не повинно бути простих залежностей між ключем і відкритим текстом;
- будь-який ключ із множини можливих ключів повинен забезпечувати надійне шифрування;
- алгоритм має допускати як програмну, так і апаратну реалізацію[1, с. 125–128].

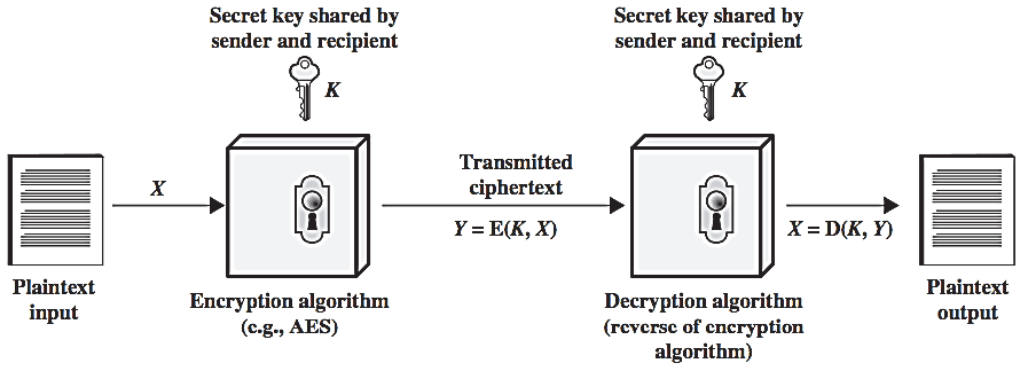


Рис. 1. Модель симетричного шифрування

Ключі, використовувані в криптосистемах мають бути випадковими. Неприпустимо використовувати словникові слова та інші ключі, що легко запам'ятовуються. Часто криптографічні засоби містять у собі засоби генерації випадкових послідовностей, що також забезпечує додатковий захист.

Одна з найпоширеніших операцій при шифруванні це XOR (виключне АБО) – це логічна операція, яка порівнює дві двійкові цифри (біти). Результатом операції XOR є 1, якщо два порівнювані біти різні, і 0, якщо вони однакові. Оператор XOR позначається символом «^».

У криптографії XOR часто використовується для виконання операцій шифрування і дешифрування. Наприклад, простий алгоритм шифрування на основі XOR може використовувати секретний ключ для виконання операції XOR між кожним бітом відкритого тексту повідомлення і відповідним бітом ключа. Розшифрування полягає у виконанні тієї ж операції XOR між зашифрованим текстом і ключем для відновлення вихідного відкритого повідомлення.

До алгоритмів, який відповідає сучасним вимогам відноситься симетричний алгоритм блочного шифрування AES (Advanced Encryption Standard) який ухвалено як стандарт шифрування урядом США. Специфікації алгоритму були опубліковані Національним інститутом стандартів і технологій США 26 листопада 2001 року. AES є найпоширенішим алгоритмом симетричного шифрування в даний час. Підтримка цього алгоритму введена фірмою Intel у сімейство процесорів, починаючи з мікроархітектури Sandy Bridge. Алгоритм прийнято як державний стандарт шифрування. Алгориитм шифрування AES (рис. 2) передбачає певну кількість раундів, яка визначається довжиною ключа. Наприклад, 128-бітний ключ вимагає 10 раундів, а 256-бітний ключ – 14 раундів. Першим кроком є створення секретного ключа, який буде використовуватися для шифрування та розшифрування даних. Ключ може бути різної довжини, але AES підтримує ключі довжиною 128, 192 і 256 біт. Після того, як секретний ключ згенеровано, він розширюється для створення розкладу ключів. Розклад ключів використовується для створення серії круглих ключів, які будуть використовуватися в процесі шифрування і дешифрування.

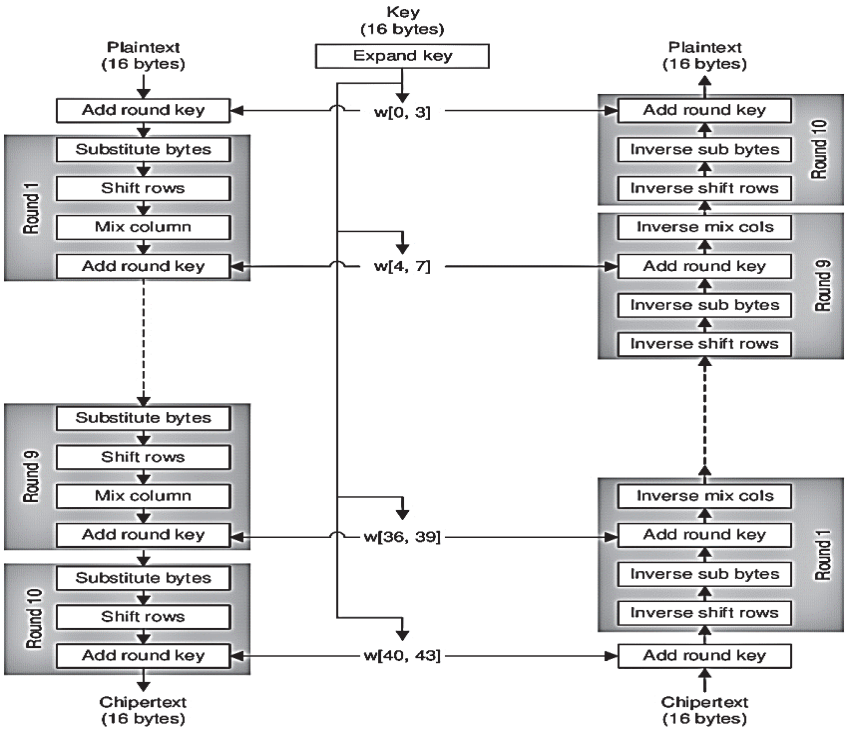


Рис. 2. Блок-схема процесу шифрування та дешифрування AES

AES використовує крок заміни «Substitute Bytes». Цей крок передбачає заміну кожного байта у вхідних даних відповідним байтом з таблиці підстановок (відомої як S-box).

На кроці «Shift Rows» рядки матриці даних зсуваються на певну кількість байт. Перший рядок не зсувається, другий рядок зсувається на один байт вліво, третій рядок зсувається на два байти вліво, а четвертий рядок зсувається на три байти вліво.

Крок «MixColumn» передбачає виконання матричного множення на кожен стовпець матриці даних з фіксованою матрицею.

На наступному кроці круглий ключ, згенерований з розкладу ключів, додається до матриці даних за допомогою операції XOR.

Кроки з 3 по 6 повторюються для певної кількості раундів, залежно від довжини ключа. Для 128-бітного ключа – 10 раундів, для 192-бітного ключа – 12 раундів, а для 256-бітного ключа – 14 раундів.

Фінальний раунд: останній раунд AES дещо відрізняється від інших раундів. Кроки підстановки та зсуву рядків виконуються як зазвичай, але крок перемішування стовпців пропускається. Ключ останнього раунду потім об'єднується з матрицею даних для отримання зашифрованого результату.

Щоб розшифрувати дані, процес виконується у зворотному порядку. Зашифровані дані піддаються операції XOR з остаточним круглим ключем, після чого кожен з етапів виконується у зворотному порядку.

Український криптографічний стандарт для блокових шифрів, який також відомий як «шифр Калина». Він був розроблений командою українських криптографів і опублікований у 2015 році як Державний стандарт України ДСТУ 7624:2014. Шифр «Калина» – це блоковий шифр із симетричним ключем, який підтримує розміри блоків 128, 256 і 512 біт з розмірами ключів 128, 256 і 512 біт відповідно. Він заснований на шифрі переможця конкурсу AES Rijndael, але має деякі відмінності в конструкції, а саме: інший графік ключів, інша кількість раундів і використання операцій побітового обертання замість операцій зсуву.

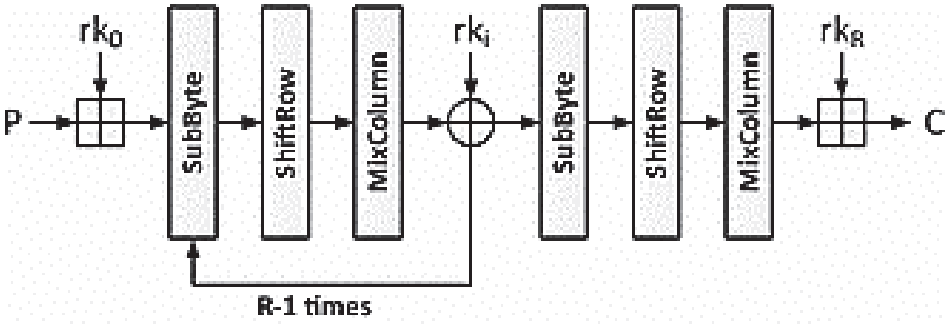


Рис. 3. Функція шифрування Kalyna, де R – кількість раундів

Шифр «Калина» (Рис. 3) розроблений для захисту від широкого спектру атак, включаючи диференціальний та лінійний криптоаналіз, і він був детально проаналізований криптографічною спільнотою. Він також вважається відносно ефективним з точки зору продуктивності, і його було реалізовано в ряді програмних і апаратних платформ. Шифр «Калина» був прийнятий як національний стандарт в Україні і поданий до Міжнародної організації зі стандартизації (ISO) на розгляд як світовий стандарт.

Шифр Kalyna є симетричним блоковим шифром, що означає, що він використовує один і той же секретний ключ для шифрування і розшифрування даних. Працює наступним чином:

- Розширення ключа. 128, 256 або 512-бітний секретний ключ розширюється до більшого набору круглих ключів, які будуть використовуватися в процесі шифрування і розшифрування. Це робиться за допомогою розкладу ключів, який генерує серію раундів ключів.

- Ініціалізація. Відкриті дані розбиваються на блоки фіксованого розміру 128 біт (або 256 чи 512 біт, залежно від обраного розміру блоку). Перший блок піддається операції XOR з «відбілюючим» ключем, який є фіксованим значенням, що слугує для рандомізації вхідних даних.
- Раунди шифрування. Блок відкритого тексту проходить через серію раундів шифрування, де в кожному раунді застосовується комбінація операцій заміни і перестановки. Операція заміни замінює кожен байт відкритого тексту відповідним байтом з таблиці заміни. Операція перестановки змінює порядок байтів у блоці відповідно до фіксованого шаблону.

Після останнього раунду шифрування кінцевий блок зашифрованого тексту створюється шляхом XOR-об'єднання результату останнього раунду з ключем останнього раунду.

Для розшифрування зашифрованого тексту застосовується той самий процес у зворотному порядку. Блок зашифрованого тексту проходить через таку ж кількість раундів розшифрування, в яких застосовуються зворотні операції підстановки і перестановки, що використовуються при шифруванні. Ключ останнього раунду додається до результату останнього раунду дешифрування, щоб отримати вихідний блок відкритого тексту.

Кількість раундів шифрування і розшифрування залежить від обраного ключа і розміру блоку. Наприклад, з 256-бітним ключем і розміром блоку 128 біт, шифр використовує 10 раундів шифрування і розшифрування. З 512-бітним ключем і 256-бітним розміром блоку шифр використовує 14 раундів шифрування і розшифрування.

Асиметричне шифрування – це також процес шифрування даних між двома сторонами, але замість одного ключа для цього використовуються два унікальні, але математично пов'язані ключі. Перший ключ, відомий як відкритий ключ, шифрує дані перед відправкою через Інтернет; другий, закритий ключ, розшифровує дані на стороні одержувача. Ось чому асиметричне шифрування (рис. 4) також відоме як шифрування з відкритим ключем.

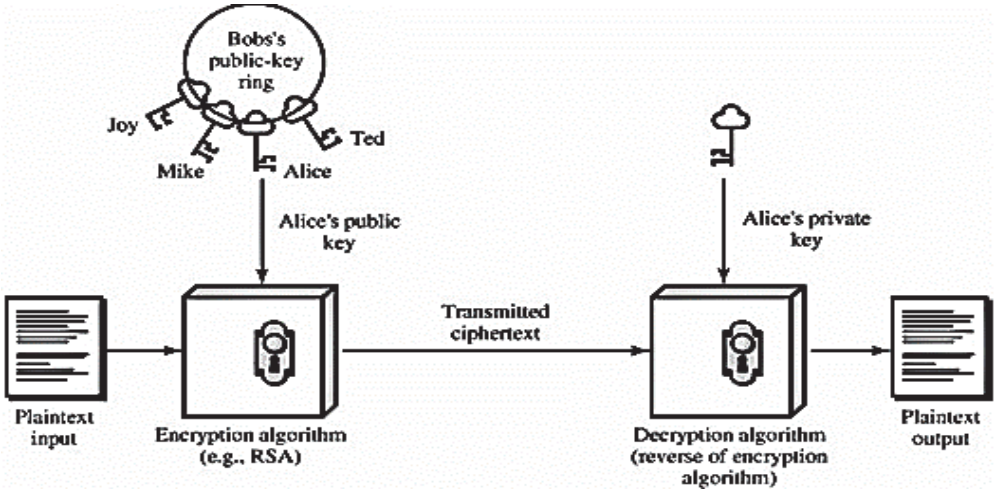


Рис. 4. Модель асиметричного шифрування

Важливою перевагою асиметричних алгоритмів перед симетричними є відсутність необхідності попередньої передачі секретного ключа. Основним недоліком є обчислювальна складність, а отже, більші витрати ресурсів порівняно із симетричними алгоритмами. Тому на практиці асиметричні криптосистеми використовуються для передавання секретного ключа, а подальший обмін інформацією здійснюється вже за допомогою симетричних криптосистем.

Нині найрозвиненішим методом криптографічного захисту інформації з відомим ключем є RSA, названий так за початковими літерами прізвищ його винахідників (Rivest, Shamir і Adleman). Криптостійкість цього алгоритму ґрунтується на припущенні, що

винятково важко визначити секретний ключ за відомим, оскільки для цього необхідно розв'язати задачу про існування дільників цілого числа, тобто на принципі складності факторизації цілих чисел. Ця задача є NP – повною. Відомі точні алгоритми для розв'язання цієї задачі мають експоненціальну оцінку обчислювальної складності, наслідком чого є неможливість отримання точних розв'язків для задач великої та навіть середньої розмірності.

RSA використовує блок шифрування змінного розміру та ключ змінного розміру. Ця криптосистема, заснована на теорії чисел, яка є системою блочного шифрування. Вона використовує два простих числа для генерації відкритого і закритого ключів розміром від 1024 до 4096 біт. Ці два різні ключі використовуються для шифрування і дешифрування. Відправник шифрує повідомлення за допомогою відкритого ключа одержувача, і коли повідомлення передається одержувачу, одержувач може розшифрувати його за допомогою власного закритого ключа. Операції RSA можна розбити на три великі етапи: генерація ключа, шифрування та дешифрування [2].

RSA має деякі недоліки у своїй конструкції, тому не є кращим для комерційного використання. Коли для створення ключа вибираються малі значення p та q, то процес шифрування стає занадто слабким, і можна розшифрувати дані, використовуючи теорію випадкових ймовірностей та атаки побічних каналів. З іншого боку, якщо вибираються великі довжини p і q, то це займає більше часу і продуктивність погіршується в порівнянні з AES. Крім того, алгоритм також вимагає однакових довжин для p та q, що на практиці є дуже складною умовою для виконання. У таких випадках необхідна техніка підстановки, яка збільшує накладні витрати системи за рахунок більшого часу обробки. Послідовність подій (Рис.5) виконує алгоритм RSA для шифрування декількох блоків, а розшифрування – для блоків даних, що складаються з 64 біт, за допомогою 64-бітного ключа [2, 3].

Сайфер «Шифр-HSM» – сімейство універсальних високопродуктивних програмно-апаратних мережних криптографічних модулів, які виконують криптографічні перетворення і можуть бути використані у різноманітних прикладних системах.

Мережний криптографічний модуль (Рис. 6) «Шифр-HSM» (далі МКМ «Шифр-HSM» чи HSM) призначений для захищеної генерації, надійного збереження та використання ключів у швидких криптографічних перетвореннях. Для взаємодії користувачів з МКМ «Шифр-HSM» використовуються мережні протоколи транспортного рівня.

Мережний криптомодуль належить до апаратно-програмних засобів криптографічного захисту інформації виду Б підвиду Б2, категорій «Ш», «К» та «П» та класу В2 згідно з Наказом № 141 від 20.07.2007 Держспецзв'язку України. Мережний криптомодуль використовується лише у локальній захищеній мережі установи [1, 3].

Даний криптографічний модуль підтримує розглянуті симетричні алгоритми шифрування ДСТУ 7624 та AES, у режимах ECB, OFB, CFB, CBC, CTR. А також асиметричне шифрування алгоритмом RSA за схемами RSAES-PKCS1-v1.5 RSAES-OAEP.

Використання PKCS#11 інтерфейсу для взаємодії з пристроєм дозволяє забезпечити аналогічну функціональність, як і рішення від: Thales (Luna HSM) і nCipher (nShield Connect).

До основних функцій мережного криптографічного модуля «Шифр-HSM» належать:

- Відновлення з резервної копії та відновлення до заводських налаштувань.
- Автентифікація адміністраторів на HSM з використанням захищених носіїв.
- Використання захищених носіїв, як локально, так і віддалено.
- Створення резервних копій внутрішнього стану.
- Зберігання резервних копій модуля на окремому захищеному засобі – МКМ виключно для зберігання резервних копій.
- Реплікація поточного внутрішнього стану одного МКМ на кілька МКМ (до 16 у режимі Master-Slave).
- Віддалене адміністрування з використанням web-інтерфейсу.
- Віддалений моніторинг з використанням web-інтерфейсу та за SNMP.

- Можливість зберігання не лише ключів, а й конфіденційних даних у великій кількості (обмежується обсягом внутрішньої пам’яті, 256, 512 ГБ та 1 ТБ).
- Захист від відкриття та проникнення до МКМ, з фізичним знищенням чи видаленням конфіденційної інформації.
- Виконання криптографічних операцій [3].
-

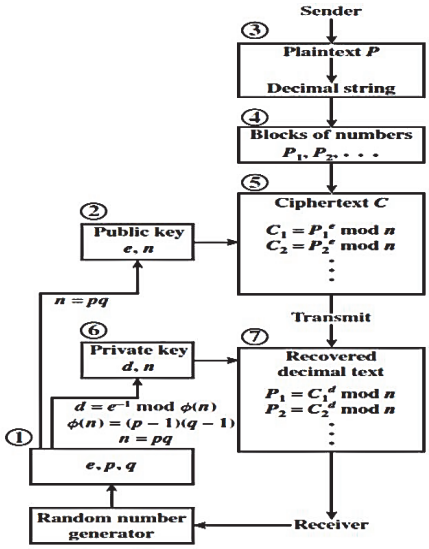


Рис. 5. Обробка RSA декількох блоків

Також для захисту інформації використовується стеганографія – наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі повідомлення.

Слово «стеганографія» в перекладі з грецької буквально означає «тайнопис» (steganos – секрет, таємниця; graphy – запис). До неї належить величезна безліч секретних засобів зв’язку, таких як невидиме чорнило, мікрофотознімки, умовне розташування знаків, таємні канали та засоби зв’язку на плаваючих частотах тощо.

На відміну від криптографії, яка приховує вміст повідомлення, стеганографія приховує сам факт його існування. Як правило, повідомлення буде виглядати як що-небудь інше, наприклад, як зображення, стаття, список покупок або лист. Стеганографію зазвичай використовують спільно з криптографією. Перевага стеганографії над чистою криптографією в тому, що повідомлення не привертають до себе уваги. Таким чином, криптографія захищає зміст повідомлення, а стеганографія захищає сам факт наявності будь-яких прихованих посилань. Цифрова стеганографія – напрям стеганографії, заснований на приховуванні або впровадженні додаткової інформації в цифрові об’єкти. Найчастіше цей метод ґрунтується на надмірності аудіовізуальної інформації. Як правило, внесення спотворень, які перебувають нижче порога чутливості людини, не призводить до помітних змін цієї інформації [1].

Рис. 6. Мережний криптографічний модуль «Шифр-HSM»

Цифрова стеганографія – напрям стеганографії, заснований на приховуванні або впровадженні додаткової інформації в цифрові об’єкти. Найчастіше цей метод ґрунтується на надмірності аудіовізуальної інформації. Як правило, внесення спотворень, які перебувають нижче порога чутливості людини, не призводить до помітних змін цієї інформації. Захист конфіденційної інформації від несанкціонованого доступу – це сфера, в якій використання комп’ютерної стеганографії є найбільш ефективним. Наприклад, одна секунда оцифрованого звуку з частотою дискретизації 44100 Гц і розрядністю 8 біт дає змогу приховати за рахунок заміни найменш значущих розрядів близько 10 кілобайт інформації. Стеганографічні методи, спрямовані на протидію системам моніторингу та управління мережевими ресурсами, дають змогу протистояти спробам промислового шпигунства. Ще однією сферою використання стеганографії є захист авторського права. На графічні зображення може наноситися спеціальна мітка, яка залишається невидимою для очей, але розпізнається спеціальним ПЗ і дає змогу однозначно ідентифікувати файл [1, 3].

Таким чином, сучасна стеганографія поряд із криптографією представляє безліч засобів захисту інформації, і найкращим рішенням буде комбінування як криптографічних, так і стеганографічних методів.

Висновки. Хоча програмне та апаратне забезпечення для захисту інформації має вирішальне значення для захисту даних, воно не є надійним. Кіберзлочинці продовжують розробляти витончені методи обходу заходів безпеки, і витоки даних все ще є поширеним явищем. Тому важливо використовувати кілька рівнів захисту та регулярно оновлювати програмне та апаратне забезпечення, щоб забезпечити найвищий рівень безпеки. Найперспективнішим напрямком у сфері програмно-апаратного захисту інформації є створення комплексних систем, що вирішують широке коло завдань. Розглянуті криптографічні засоби захисту інформації не зможуть надати належний рівень захисту без використання разом з ними мережевих екранів, антивірусних програм та систем виявлення вторгнень та інших засобів в загальній, комплексній системі захисту. Прикладом модулю, що входить до таких систем є розглянутий в статті мережний криптографічний модуль «Шифр-HSM». Загалом, програмне та апаратне забезпечення для захисту даних є необхідними компонентами стратегії кібербезпеки будь-якої організації. Вони повинні використовуватися разом з іншими заходами безпеки, такими як навчання співробітників і оцінка ризиків, для створення комплексної та ефективної системи безпеки.

Список використаних джерел

1. О. Кузнецов, Р. Олійников, Ю. Горбенко, А. Пушкарьов, О. Дирда, І. Горбенко, Обґрунтування вимог, побудування та аналіз перспективних симетричних криптоперетворень на основі блочних шифрів. – 2014. – С. 130–141.
2. A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention \\ Режим доступу: https://symbiosisonlinepublishing.com/computer-science-technology/computerscience-information-technology32.php (останнє звернення 13.03.2023 р.)
3. Матеріали Української ІТ компанії з захисту інформаційних систем «Сайфер» \\ Режим доступу: https://cipher.com.ua/uk (останнє звернення 13.03.2023 р.)

Робота виконана під науковим керівництвом старшого викладача
КОСТЮК Ю. В.

МЕТОДИ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ: ВІД БІОМЕТРІЇ ДО БЛОКЧЕЙНУ

ЛОБУЦЬКИЙ В., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто методи автентифікації користувачів, які застосовуються в інформаційно-телекомунікаційних системах, що використовуються для ідентифікації користувачів, включаючи традиційні методи, такі як логіни та паролі, біометрична автентифікація та блокчейн-технології. Досліджено можливі загрози для безпеки та приватності, пов'язані з використанням біометричних даних та блокчейн-технологій, і запрпоновано можливі способи зменшення цих ризиків. Розглянуто питання безпеки та приватності використання цих методів.

The article discusses authentication methods used in information and telecommunications systems for identifying users, including traditional methods such as usernames and passwords, biometric authentication, and blockchain technology. Possible security and privacy threats associated with the use of biometric data and blockchain technologies are explored, and potential ways to mitigate these risks are proposed. Security and privacy concerns regarding the use of these methods are also discussed

Актуальність. Методи автентифікації користувачів в інформаційно-телекомунікаційних системах мають велику актуальність у сучасному цифровому світі, де відбувається швидкий розвиток технологій і збільшується кількість онлайн-сервісів та додатків. Автентифікація користувачів є ключовим елементом забезпечення безпеки та захисту приватності в інтернеті, оскільки вона дозволяє переконатися у тому, що користувач має право доступу до системи або додатку, і зменшує ризики кіберзлочинності та зловживання даними. Біометричні технології та блокчейн-підходи до автентифікації стають все більш популярними і мають великий потенціал для покращення безпеки та забезпечення приватності в інтернеті. Однак, їх використання також може мати певні ризики та виклики, пов'язані з захистом персональних даних та можливістю їх зламу.

Тому, розуміння та оцінка різних методів автентифікації є дуже важливою темою для дослідників, працівників галузі інформаційної безпеки та кібербезпеки, а також для користувачів, які хочуть бути впевненими у тому, що їхні дані захищені від несанкціонованого доступу. З цієї причини, забезпечення безпеки та приватності в інформаційно-телекомунікаційних системах є надзвичайно важливим завданням.

Метою статті є дослідження методів автентифікації користувачів в цифровому середовищі, починаючи від біометричних технологій та закінчуючи блокчейн-підходами.

Об'єктом дослідження є аналіз можливостей технологій автентифікації в забезпеченні кібербезпеки та захисту конфіденційної інформації.

Предмет дослідження – методи та технології, що використовуються для ідентифікації та перевірки користувачів у цифровому середовищі.

Аналіз попередніх досліджень. Аналіз попередніх досліджень з питань методів автентифікації користувачів в інформаційно-телекомунікаційних системах показує, що більшість досліджень зосереджена на вдосконаленні методів біометричної автентифікації, таких як розпізнавання обличчя, відбитків пальців, голосу та інших біометричних характеристик. Деякі дослідження також зосереджені на застосуванні методів машинного навчання для вдосконалення процесу автентифікації. Інші дослідження вивчають використання різних методів автентифікації, таких як одноразові паролі та біометричні

токени. Загалом, попередні дослідження показують, що методи автентифікації користувачів є важливою та актуальною темою, і вони постійно вдосконалюються для забезпечення безпеки та приватності користувачів в інформаційно-телекомунікаційних системах. Дослідженню методів автентифікації присвячені праці вітчизняних та закордонних науковців: І. О. Гончаренко, М. С. Карпенко, Ю. А. Довгань, В. М. Колісник, О. І. Нікітіна, М. В. Ісаєва та ін.

Виклад основного матеріалу. У сучасному світі, де інформація є одним із найбільш цінних ресурсів, забезпечення безпеки даних та доступу до них є дуже важливим завданням. Методи автентифікації користувачів є одним із основних засобів забезпечення безпеки в інформаційно-телекомунікаційних системах. В інформаційно-телекомунікаційних системах (ІТС) автентифікація користувачів є важливим і невід'ємним елементом забезпечення безпеки даних та інформаційних ресурсів. Існує багато методів автентифікації користувачів, починаючи від традиційних методів, таких як логіни та паролі, до новітніх, таких як біометрична автентифікація та блокчейн. Основні методи автентифікації користувачів в інформаційно-телекомунікаційних системах включають наступні:

- Логін та пароль: це найбільш поширений метод автентифікації, який вимагає від користувача ввести свій логін та пароль для доступу до акаунту.
- Біометричні методи – методи, які включають використання фізіологічних або поведінкових рис користувача, таких як відбиток пальця, розпізнавання обличчя, голосу або почерку.
- Карти або токені – метод, який використовує фізичний об'єкт, який користувач повинен мати при собі, наприклад, карту з чипом або USB-ключ.
- Двофакторна автентифікація – метод, який включає використання двох або більше методів автентифікації, наприклад, комбінації логіна та пароля з біометричним методом або картою або токеном.
- Одноразові паролі – метод, що використовується для тимчасового доступу до аккаунту та вимагає від користувача ввести одноразовий пароль, який зазвичай надсилається на мобільний телефон або електронну пошту.
- Сертифікати – метод використовує сертифікати, що видаються відповідними органами, для перевірки ідентичності користувача.
- Соціальна автентифікація – метод, що використовується для входу на сайти або додатки за допомогою профілю в соціальній мережі, такі як Facebook або Google.
- Блокчейн-автентифікація – блокчейн може використовуватись як метод автентифікації, особливо в контексті криптовалют та інших децентралізованих додатків. Блокчейн – це розподілена база даних, яка зберігає транзакції у вигляді блоків, кожен з яких містить хеш попереднього блоку. Це створює ланцюжок блоків, який є відкритим і невід'ємним, тому що будь-яка зміна в одному блоку вимагає зміни всіх наступних блоків.

Автентифікація користувачів в інформаційно-телекомунікаційних системах є важливою складовою захисту інформації та даних від несанкціонованого доступу. Проте існують деякі виклики та проблеми, пов'язані з автентифікацією користувачів:

1. Компрометація облікових даних: користувачі часто використовують слабкі паролі або взагалі не змінюють стандартні облікові дані, що легко стає об'єктом атаки хакерів або кіберзлочинців. Також можуть використовуватися атаки підбору паролів.
2. Специфікація стандартів: різні інформаційно-телекомунікаційні системи можуть використовувати різні стандарти для автентифікації користувачів, що може призвести до проблем з сумісністю між системами.
3. Конфіденційність даних: у деяких випадках, при автентифікації користувачів, деякі приватні дані можуть бути збережені на сервері. Це може стати об'єктом атак і злому.

4. Ризик витоку даних: при автентифікації через Інтернет.
5. Вартість та складність розгортання: деякі методи автентифікації можуть бути дорогими у розгортанні та підтримці, а також можуть потребувати значних зусиль користувачів для використання.

В умовах сьогодення автентифікацію можна представити за такими сегментами (рис. 1).

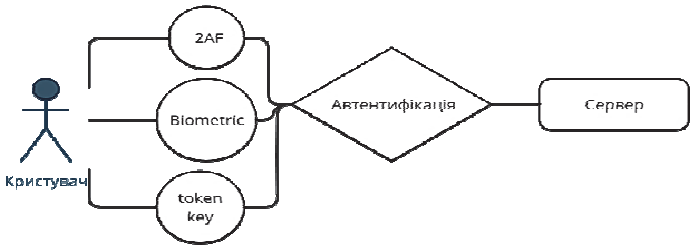


Рис. 1. Сегментація автентифікації

Авторизація за допомогою логіну та пароля – це дуже поширений метод авторизації у багатьох системах, від електронної пошти до соціальних мереж та інтернет-банкінгу. Цей метод авторизації дозволяє користувачам отримувати доступ до своїх особистих акаунтів та зберігати інформацію у захищеній середовищі. Процес авторизації за допомогою логіну та пароля зазвичай складається з наступних етапів: спочатку користувач вводить свій логін та пароль на сторінці авторизації, потім система перевіряє введені дані та перевіряє, чи існує в базі даних користувач з таким логіном та паролем. Якщо введені дані правильні, то користувач отримує доступ до свого акаунта, в іншому випадку він отримує повідомлення про помилку та може спробувати ввести дані знову. Після успішної авторизації система зазвичай встановлює «сесію» - унікальний ідентифікатор, який дозволяє користувачеві працювати з системою без потреби повторного введення логіну та пароля на протязі певної години. У разі авторизації за допомогою логіну та пароля важливо забезпечити безпеку введення та збереження цих даних. Користувач повинен вибирати надійний пароль та не повинен нікому розкривати його. Також система повинна забезпечувати захист від несанкціонованого доступу до бази даних користувачів, де зберігаються логіни та паролі.

Рис. 2. Вікно автентифікації

Хоча паролі є важливим інструментом для захисту від несанкціонованого доступу до облікових записів, вони також можуть стати джерелом уразливостей та ризиків для безпеки. Недосконаліть людської пам’яті та легкість забування паролів можуть призвести до використання слабких та недостатньо складних паролів, які можуть бути легко зламані хакерами. Крім того, паролі можуть бути вкрадені шляхом використання шкідливих програм, таких як кейлогери, або через атаки соціального інжинірингу, які маніпулюють людською поведінкою для отримання доступу до паролів.

Одним із найпоширеніших методів автентифікації користувачів є метод введення логіна та пароля. Проте, цей метод є досить уразливим до атак, таких як фішинг та перехоплення даних. Для забезпечення вищого рівня безпеки до застосування приходять методи біометрії. Біометрія – це метод автентифікації користувачів за допомогою їх біологічних рис. До найпоширеніших методів біометрії належать відбитки пальців (Рис.2), розпізнавання обличчя (рис. 3), розпізнавання голосу та розпізнавання раковини вуха. Використання методів біометрії дозволяє забезпечити вищий рівень безпеки, оскільки біометричні дані неможливо підробити чи скопіювати.

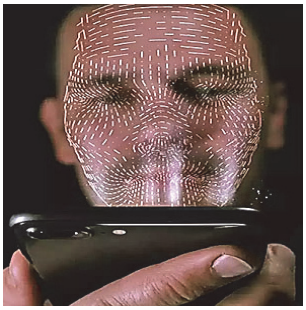


Рис. 3. Принцип дії ехнології Face ID

Технологія Face ID використовується на пристроях компанії Apple, таких як iPhone та iPad. Основним принципом дії є використання технології розпізнавання обличчя за допомогою TrueDepth-камери, розташованої на екрані пристрою. Під час налаштування Face ID, користувач сканує своє обличчя, і пристрій зберігає його математичну модель у спеціальній безпечній зоні, що знаходиться на процесорі пристрою. При подальшому використанні, коли користувач підносить пристрій до свого обличчя, TrueDepth-камера збирає інформацію про форму обличчя, положення очей, ніздрі, рота та інші параметри, і передає її на процесор для порівняння зі збереженою математичною моделлю. Якщо отримана інформація відповідає збереженій моделі, пристрій розблоковується. Основна перевага технології Face ID полягає у її точності та надійності. Крім того, вона працює в широкому діапазоні умов освітлення та дозволяє розпізнавати обличчя у різних позах та уголках. Також вона є безпечнішою порівняно з іншими методами автентифікації, такими як введення пароля, оскільки не може бути підмінена або скопійована [1].

Технологія Touch ID використовує сканер відбитків пальців, що вбудований у кнопку домашнього екрану на пристроях Apple. Кнопка домашнього екрану містить датчик, що реагує на тиск пальця, та сканер відбитків пальців, який визначає унікальні характеристики шкірного відбитка. При реєстрації відбитка пальця датчик сканує пальці користувача та зберігає характеристики відбитка у зашифрованому вигляді на пристрої. При подальшому використанні Touch ID користувач просто натискає на кнопку домашнього екрану для активації датчика сканування відбитка пальця. Сканер відбитків пальців порівнює характеристики нового відбитка зі збереженим, що використовується для перевірки автентичності користувача. Якщо знайдені відбитки збігаються, то пристрій дозволяє доступ користувача до пристрою. Технологія Touch ID забезпечує високий рівень безпеки, оскільки відбитки пальців є унікальними для кожної особи, що зменшує ризик несанкціонованого доступу до пристрою. Крім того, застосування технології Touch ID забезпечує зручність та швидкість використання, оскільки користувачеві не потрібно вводити пароль або пін-код, достатньо лише натиснути на кнопку домашнього екрану [2].

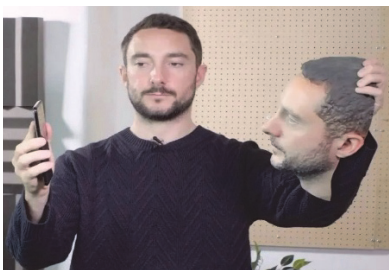


Рис. 4. Обхід блокування за допомогою 3D маски

Одна з можливих уразливостей Face ID та Touch ID полягає в тому, що вони можуть бути обмануті фальшивими відбитками пальців або обличчя (рис. 4). Наприклад, дослідники групи CCC (Chaos Computer Club) використали фотографію обличчя користувача та

3D-друкований макет обличчя, щоб успішно обійти захист Face ID на iPhone X. Також були повідомлення про успішне обходження захисту Face ID з використанням маски, зробленої на 3D-принтері, яка була створена на основі фотографії обличчя.

Також можливе виникнення проблем зі зберіганням біометричних даних, таких як відбитки пальців та обличчя, що може призвести до можливості їх викрадення.

Автентифікація типу картка або токен – це методи авторизації, які дозволяють користувачам отримувати доступ до облікових записів та інших ресурсів шляхом використання карток або токенів замість паролів. Ці методи авторизації дозволяють уникнути багатьох проблем, пов'язаних із паролями, таких як їх вразливість до атак і легкість забування.

Валідація за допомогою картки використовується давно і зазвичай здійснюється за допомогою спеціальних карт-читачів. Користувач вставляє картку в читач, який зчитує інформацію з неї та перевіряє, чи є права доступу до акаунту. Цей метод авторизації є досить безпечним, оскільки картки зазвичай містять вбудовані захисти від копіювання та підробки.

Токені є іншим методом авторизації, який вживається дедалі більше в сучасних системах. Токені – це унікальні коди, які генеруються програмно і використовуються для авторизації користувача. Коди можуть бути відправлені на мобільний телефон або інше зареєстроване пристрій. Користувачі можуть ввести токен у відповідному полі на сайті або у додатку, щоб отримати доступ до ресурсів. Токени є більш безпечними, ніж паролі, оскільки вони є одноразовими та не можуть бути використані знову. Існує також концепція токенів доступу, яка використовується в багатьох API. Токени доступу – це спеціальні коди, які використовуються для авторизації користувача для взаємодії з певним API. Кожен токен є унікальним та має обмежений час дії.

Система автоматично формує заявки на оплату, що дозволяє уникнути помилок в розрахунках, а також спланувати витрати коштів на закупівлю.

Які картки для авторизації можна використовувати різні пристрої та технології, залежно від того, які ресурси та системи необхідно захищати. Найбільш поширеними формами карт для авторизації є:

- Кредитні та дебетові картки – для доступу до банківських ресурсів та операцій з фінансами.
- Смарт-картки – це картки із вбудованим мікропроцесором та пам'яттю. Вони можуть використовуватися для авторизації доступу до комп'ютерних систем, облікових записів, мереж, будівель, автоматизованих систем контролю доступу та інших ресурсів.
- RFID-картки – це картки із вбудованим радіочастотним ідентифікатором (RFID). Вони використовуються для авторизації доступу до приміщень, паркінгів, облікових записів, товарів та інших ресурсів, які потребують ідентифікації за допомогою бездротових технологій.
- USB-токені – це пристрої, що підключаються до USB-портів комп'ютера та містять вбудовані ключі шифрування та інші методи захисту. Вони використовуються для авторизації доступу до комп'ютерів, мереж та інших ресурсів.
- NFC-карти – це картки із вбудованим чіпом та бездротовими технологіями, які можуть використовуватися для авторизації доступу до різних пристроїв, таких як мобільні телефони, планшети та інші ресурси.
- QR-код – це спеціальні зображення, які можуть бути розпізнані за допомогою камери смартфону або сканера. Вони можуть бути використані для авторизації доступу до сайтів, додатків та інших ресурсів [3].

Цей метод автентифікації на основі ключ-токен зазвичай використовується для забезпечення безпеки веб-додатків та API або для фізичних замків. Однак такий метод не є ідеальним і може бути уразливим до деяких атак. Однією з можливих атак на цей метод є крадіжка токена. Якщо зловмисники змогли отримати доступ до токена, то вони можуть використовувати його для отримання несанкціонованого доступу до захищеного ресурсу. Ця

проблема може бути розв'язана за допомогою шифрування токенів та використанням протоколів, які забезпечують безпеку токенів, наприклад, OAuth.

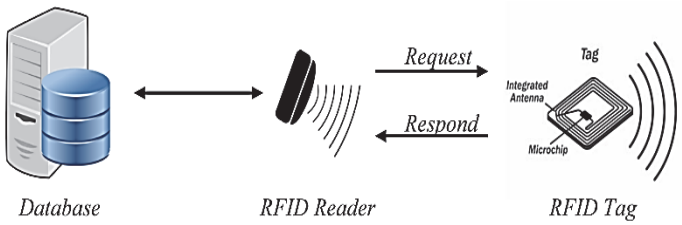


Рис. 5. Принцип дії інфраструктури для автентифікації з використанням технології RFID

Ще однією потенційною вразливістю є можливість підробки токена. Якщо зловмисники змогли підробити токен, вони можуть використовувати його для отримання доступу до захищеного ресурсу. Цю проблему можна вирішити за допомогою регулярної перевірки токенів та використання безпечних протоколів обміну інформацією. Крім того, при використанні ключ-токена методом автентифікації можуть бути вразливі, пов'язані зі зберіганням ключів. Якщо ключі зберігаються недостатньо захищеними або вони можуть бути викрадені, це може призвести до загрози для безпеки ресурсу. Загалом, метод автентифікації на основі ключ-токена є досить безпечним і надійним, якщо його використовувати з належною обачністю та застосовувати відповідні заходи безпеки, такі як шифрування токенів та перевірка їх правильності.

Блокчейн-автентифікація (Рис.6). є одним із найбезпечніших методів автентифікації в даний час. Замість того, щоб передавати конфіденційні дані через централізовані сервери, як у традиційних методах, блокчейн-автентифікація використовує технологію розподілених реєстрів для збереження та обробки даних. Основним перевагою блокчейн-автентифікації є те, що вона забезпечує високий рівень безпеки. Блокчейн використовує криптографію для забезпечення безпеки транзакцій та зберігання конфіденційних даних. Це означає, що цей метод автентифікації надає високий рівень захисту від шахрайства та злому. Іншою перевагою блокчейн-автентифікації є її децентралізованість. У традиційних методах автентифікації централізовані сервери зберігають конфіденційні дані користувачів, що робить їх уразливими до атак із боку зловмисників. Блокчейн-автентифікація, з іншого боку, зберігає дані у розподілених регістрах, що робить їх менш уразливими до атак та злому. Однак блокчейн-автентифікація також має деякі недоліки, такі як обмежена масштабованість та повільна швидкість обробки транзакцій. Крім того, використання блокчейн-автентифікації потребує спеціальних технічних знань та ресурсів [4].

2FA на базі блокчейну – це додатковий рівень безпеки, (рис. 7), який використовується для автентифікації користувачів в інформаційно-телекомунікаційних системах. За допомогою 2FA, користувач може підтвердити свою ідентичність, використовуючи два різні методи автентифікації.

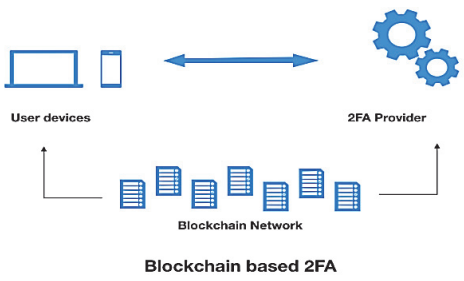


Рис. 6. Двофакторна аутентифікація на основі технології Blockchain

Методи автентифікації користувачів застосовуються у різних сферах діяльності, включаючи фінанси, медицину, урядові організації та бізнес.

У фінансовій сфері, особливо у онлайн-банкінгу, методи автентифікації використовуються для захисту фінансових транзакцій та даних клієнтів. Наприклад, банки можуть використовувати методи біометрії, такі як сканування відбитків пальців або розпізнавання обличчя, або використовувати двофакторну автентифікацію, яка включає в себе введення паролю та отримання коду через смс або електронну пошту. Окрім банківської сфери та мереж Wi-Fi, вони знаходять застосування в онлайн-магазинах, соціальних мережах, медичній сфері, громадському транспорті, аеропортах та інших місцях. У соціальних мережах використовуються різні методи автентифікації, такі як логін через обліковий запис Google або Facebook, введення коду, відправленого на електронну пошту, або відбитків пальців на смартфонах зі спеціальними сенсорами. У медичній сфері методи автентифікації можуть використовуватись для захисту медичних даних пацієнтів та контролю доступу до них. Наприклад, лікарі можуть використовувати біометричні методи для входу до систем електронної медичної документації або для доступу до медичних пристроїв, таких як електрокардіографи. Урядові організації також використовують методи автентифікації для захисту даних та забезпечення безпеки державних систем. Наприклад, урядові служби можуть використовувати біометричні методи для контролю доступу до певних приміщень або для автентифікації працівників у системах електронного документообігу.

Висновки. Розвиток методів автентифікації користувачів є однією з актуальних проблем сучасного інформаційного світу, оскільки залежно від використовуваних методів можуть бути різні рівні безпеки і захисту від несанкціонованого доступу до інформації. Однією з перспективних тенденцій є застосування багатофакторної автентифікації, коли для доступу до ресурсів вимагається використання не одного, а кількох методів автентифікації (наприклад, пароля та біометричних даних). Також важливими напрямками розвитку є застосування штучного інтелекту та машинного навчання для покращення точності і швидкості автентифікації, а також застосування блокчейн технологій для забезпечення безпеки та надійності процесу автентифікації. До інших перспективних напрямків розвитку методів автентифікації користувачів можна віднести використання квантових технологій, стандартизацію методів та уніфікацію протоколів, що дозволить забезпечити взаємодію між різними системами та пристроями з різною інфраструктурою і зменшити витрати на розробку та впровадження методів автентифікації. Усі ці напрямки розвитку методів автентифікації користувачів спрямовані на забезпечення максимального рівня безпеки та захисту від несанкціонованого доступу до інформації, що є особливо важливим у сучасному цифровому світі. Використання правильних методів автентифікації є дуже важливим аспектом в забезпеченні безпеки інформаційних систем та даних. Неправильне використання або відсутність методів автентифікації може призвести до різних загроз, таких як несанкціонований доступ до системи, викрадення даних, крадіжка особистої інформації тощо. Застосування сильних методів автентифікації, таких як двофакторна автентифікація з використанням біометричних даних, зменшує ризик порушення безпеки системи та даних, оскільки такі методи є надійними і складними для підробки. Отже, використання правильних методів автентифікації є необхідним елементом забезпечення безпеки інформаційних систем та даних, і має важливе значення у практичній діяльності.

Список використаних джерел

1. Lomas, N. (2017). How Apple’s Face ID facial recognition system works.\\Режим доступу: https://techcrunch.com/2017/09/12/how-apples-face-id-facial-recognition-system-works/ (останнє звернення 09.04.2023р.) .
2. «Touch ID vs. Face ID: Which is faster?» by Christian Zibreg, iDownloadBlog.\\Режим доступу: https://www.idownloadblog.com/tag/face-id/ (останнє звернення 09.04.2023р.) .

3. Офіційна документація провайдерів послуг платіжних систем, таких як Visa \\Режим доступу: https://developer.visa.com/docs (останнє звернення 09.04.2023р.) .
4. Документація технології блокчейну на сайті Blockchain \\Режим доступу: https://www.blockchain.com/ru/explorer/api (останнє звернення 09.04.2023р.).

Робота виконана під науковим керівництвом канд. пед. наук, доцента
ЧУБАЄВСЬКОГО В. І.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ РОЗПІЗНАВАННЯ ШТРИХКОДУ АБО QR-КОДУ ЛОГІСТИЧНОЇ КОМПАНІЇ

ЛЮТИЙ А., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто застосування технології штрихкодів у логістичному менеджменті та ланцюгу постачання. Оглянуто історію та типи штрихкодів, а також переваги та недоліки їх використання в логістиці. Досліджено роль штрихкодів у покращенні ефективності логістичного менеджменту та забезпеченні точності інформації про складський облік та відстеження вантажів.

The article deals with the application of barcode technology in logistics management and supply chain. The history and types of barcodes, as well as the advantages and disadvantages of their use in logistics are reviewed. The role of barcodes in improving the efficiency of logistics management and ensuring the accuracy of information on warehouse accounting and cargo tracking is investigated.

Предметом дослідження є інформаційна технологія розпізнавання штрихкоду або QR-коду логістичної компанії.

Об'єктом дослідження виступає процес розпізнавання штрихкоду або QR-коду та використання його даних для автоматизації логістичних процесів.

Мета дослідження полягає у визначення ефективності використання інформаційної технології розпізнавання штрихкоду або QR-коду для забезпечення автоматизації та оптимізації логістичних процесів логістичної компанії.

Також можемо виділити такі *підцілі:*

- Дослідження основних технологій розпізнавання штрихкодів та QR-кодів.
- Аналіз використання інформаційної технології розпізнавання штрихкоду або QR-коду в логістичних компаніях.
- Оцінка впливу інформаційної технології розпізнавання штрихкоду або QR-коду на ефективність логістичних процесів.
- Розроблення пропозицій щодо вдосконалення використання інформаційної технології розпізнавання штрихкоду або QR-коду в логістичних компаніях.

Виклад основного матеріалу. Зараз у світі швидко розвивається логістична індустрія, що потребує швидкої та точної інформаційної обробки даних. Інформаційні технології стали необхідним інструментом у цьому процесі, тому розробка та впровадження систем розпізнавання штрихкодів та QR-кодів є актуальною проблемою для логістичних компаній.

У сучасному світі логістичні компанії стикаються зі значними труднощами в управлінні своїм складом та постачальним ланцюгом. Одним зі способів рішення цих

проблем є застосування технології штрихкодів. Штрихкоди стали незамінним інструментом у логістичному менеджменті та ланцюгу постачання завдяки своїм перевагам, таким як забезпечення точності та швидкості обліку товарів, зниження рівня помилок та підвищення ефективності роботи складу.

Історія та типи штрихкодів:

Штрихкоди були розроблені у 1948 році та використовувалися в першу чергу у супермаркетах для швидкого сканування товарів при реєстрації їх продажу. З тих пір вони стали широко використовуватися у логістиці та ланцюгу постачання.

Існує кілька типів штрихкодів, зокрема EAN-13, EAN-8, UPC-A, Code 128 та інші. Кожен тип штрихкоду має свої особливості та використовується залежно від конкретних потреб.

Рис. 1. Типи штрихкодів

Опис технології.

Штрихкод та QR-код – це графічні символи, які зберігають інформацію про товар або послугу. Штрихкоди зазвичай використовуються для ідентифікації товару, а QR-коди можуть містити більш різноманітну інформацію, наприклад, URL-адреси, контактні дані, текстові повідомлення тощо.

Система розпізнавання штрихкодів та QR-кодів складається з двох основних компонентів: обладнання для зчитування кодів та програмного забезпечення для обробки даних.

Обладнання для зчитування кодів може бути різним. Для штрихкодів це зазвичай сканер, а для QR-кодів може бути використана камера смартфону. Програмне забезпечення, що обробляє дані, зазвичай складається з декількох етапів: зчитування коду, декодування, перевірка на правильність та збереження інформації.

Для зчитування штрихкодів та QR-кодів використовуються спеціальні алгоритми, як і методи, які дозволяють зчитувати та обробляти інформацію з кодів. Ці алгоритми можуть використовувати різні методи зчитування, наприклад, метод читання лінійних штрихкодів або метод читання двовимірних QR-кодів. Використання відповідного методу залежить від типу коду та специфікацій обладнання, яке використовується.

У разі зчитування штрихкодів, програмне забезпечення зчитує штрихкод та декодує інформацію, яка міститься в коді. Далі виконується перевірка на правильність зчитування коду, щоб уникнути помилок при обробці даних. Якщо дані відповідають специфікаціям штрихкоду, то інформація зберігається у відповідній базі даних.

Для зчитування QR-кодів зазвичай використовуються камери смартфону, що дозволяє швидко та легко зчитувати QR-коди у будь-якому місці. Програмне забезпечення спочатку зчитує QR-код, далі декодує інформацію та виконує перевірку на правильність зчитування коду. Якщо дані відповідають специфікаціям QR-коду, то інформація зберігається у відповідній базі даних.

Використання технології штрихкодів в логістиці має декілька переваг порівняно з традиційними методами. Найбільш важливі з них наведені нижче:

Підвищена точність: Сканування штрихкоду забезпечує доставку правильного товару в потрібне місце в потрібний час, зменшуючи ризик помилок в управлінні запасами та обробці замовлень.

Покращена ефективність: Сканування штрихкоду набагато швидше за ручне введення даних, що зменшує час, необхідний для управління запасами та обробки замовлень.

Поліпшена трасованість: Технологія штрихкодів дозволяє легко відслідковувати та відстежувати продукти через ланцюг постачання, від виробника до кінцевого користувача, що полегшує видимість ланцюга постачання.

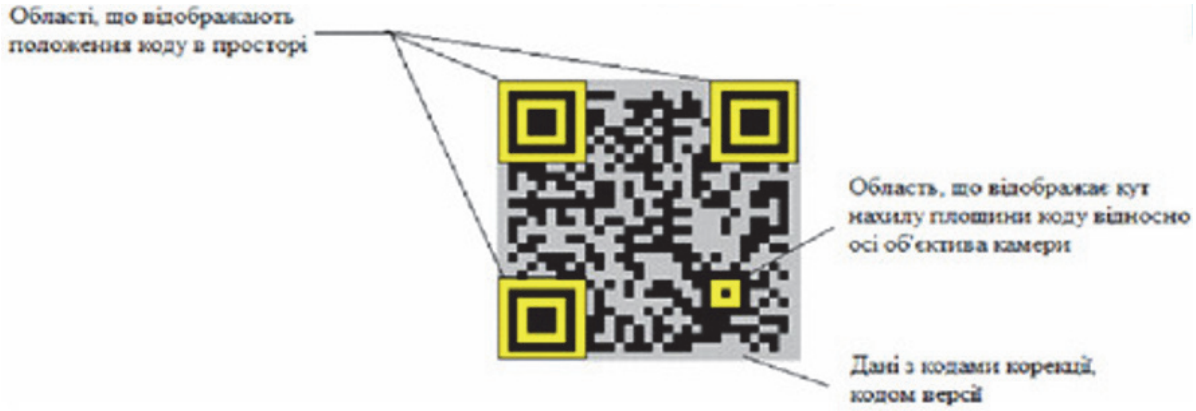


Рис. 2. Складові QR-коду

Недоліки використання штрихкодів в логістиці

Хоча технологія штрихкодів має багато переваг, є деякі недоліки, про які важливо знати:

- Вимоги до обладнання: Щоб використовувати технологію штрихкодів, потрібне спеціальне обладнання, яке може бути досить дорогим.
- Потребує навчання: Щоб користуватися технологією штрихкодів, працівники повинні бути навчені, як правильно сканувати та обробляти дані, що може зайняти час та кошти.
- Чутливість до пошкоджень: Штрихкоди можуть бути пошкоджені або зіпсовані, що може призвести до помилок у скануванні та неправильного розпізнавання даних.
- Обмежена інформація: Технологія штрихкодів обмежується короткими кодами, що може не дозволити передавати достатньо інформації про товар, що є обмеженням для деяких видів продуктів.

Незважаючи на ці недоліки, технологія штрихкодів все ще є популярною в логістичній галузі через свої переваги в ефективності та точності управління запасами та обробки замовлень.

Роль штрихкодів у покращенні ефективності логістичного менеджменту

Штрихкоди забезпечують точність даних та знижують кількість помилок, що дозволяє логістичним компаніям поліпшити свої процеси управління запасами, відстеження та виконання замовлень, а також контролювати рух товарів. Використання штрихкодів дозволяє значно скоротити час на ручне введення даних та уникнути помилок, що може призвести до затримок у доставці товарів та несправностей в системі управління запасами.

- Покращення комунікації: Штрихкоди можуть допомогти покращити комунікацію між різними логістичними частинами компанії, такими як склад, виробництво, транспортування тощо. За допомогою штрихкодів можна легко та швидко передавати інформацію про товари та їх рух, що дозволяє уникнути помилок та покращити співпрацю між різними відділами компанії. Крім того, штрихкоди дозволяють вести документацію про товари та їх рух автоматично, що спрощує процес обліку та звітності.

- Зменшення витрат: Використання штрихкодів дозволяє зменшити витрати на ручне введення даних та уникнути помилок, що може призвести до затримок у доставці товарів та несправностей в системі управління запасами. Крім того, використання штрихкодів дозволяє покращити ефективність роботи працівників та знизити кількість помилок, що може призвести до затримок у доставці товарів та несправностей в системі управління запасами.
- Управління запасами: Штрихкоди дозволяють логістичним компаніям точно відстежувати кількість товарів на складах та здійснювати швидкий облік запасів. Це дозволяє компаніям планувати замовлення, уникати надлишковості та нестачі товарів, що забезпечує більш ефективне використання ресурсів.
- Обробка замовлень: Штрихкоди дозволяють швидко та точно сканувати та обробляти замовлення, що зменшує час обробки та ризик помилок. Також, за допомогою штрихкодів можна відстежувати рух товарів від моменту отримання замовлення до його доставки, що забезпечує більш точну та швидку обробку замовлень.
- Відстеження вантажів: За допомогою штрихкодів можна відстежувати рух товарів від моменту їх відправки до моменту доставки. Це дозволяє вчасно виявляти та вирішувати проблеми, що виникають під час транспортування товарів, а також підвищує рівень відповідальності за доставку вантажу.

Роль штрихкодів у забезпеченні точності інформації про складський облік

Штрихкоди грають важливу роль у забезпеченні точності інформації про складський облік. Завдяки використанню штрихкодів, можна ефективно відстежувати всі операції з товарами на складі, від приймання до відвантаження, і зберігати цю інформацію в центральній базі даних. Це дозволяє підтримувати точний та актуальний інвентарний облік та запобігати помилкам та втратам товарів.

Крім того, штрихкоди можуть використовуватись для позначення місця розташування товарів на складі, що забезпечує їх точне та швидке знаходження в разі потреби. Також, штрихкоди можуть бути використані для визначення термінів зберігання та керування стоком, що дозволяє уникнути непотрібного складування товарів та зменшити втрати через застарілість.

Отже, використання штрихкодів у складському обліку дозволяє збільшити точність та швидкість операцій, зменшити помилки та втрати товарів та покращити ефективність управління складом в цілому.

Роль штрихкодів у забезпеченні відстеження вантажів

Штрихкоди є важливою технологією в логістиці, особливо у забезпеченні відстеження вантажів. Кожен товар може бути маркований індивідуальним штрихкодом, що дозволяє легко та точно відстежувати його рух по всьому логістичному ланцюжку. Коли товар прибуває на склад, штрихкод сканується, і відомість про його прибуття автоматично оновлюється в системі складського обліку. Так само, коли товар відправляється до клієнта, штрихкод знову сканується, і інформація про відвантаження оновлюється в системі.

Штрихкоди також дозволяють забезпечити точне відстеження термінів придатності товарів на складі. Кожен товар може бути позначений своїм індивідуальним штрихкодом, на якому зберігається інформація про дату виробництва та термін придатності. Коли товар прибуває на склад, його штрихкод сканується, і система автоматично розраховує, скільки часу залишилося до дати закінчення терміну придатності. Це дозволяє операторам складу вчасно забрати товар з полиць, які наближаються до кінця терміну придатності, та запобігти збиткам від зіпсованих продуктів.

Штрихкоди також можуть допомогти у відстеженні використання ресурсів на складі. Кожна одиниця товару може мати свій індивідуальний штрихкод, на якому зберігається інформація про вагу, розмір та інші характеристики. Це дозволяє вести облік кількості відправлених та отриманих вантажів, включаючи інформацію про їхнє місцезнаходження, дату та час пересування та багато іншого. За допомогою штрихкодів можна також визначити, коли та де виникають затримки в доставці, що дозволяє швидко вживати заходів для їх усунення та покращення ефективності логістичного процесу.

Штрихкоди можуть також допомогти забезпечити безпеку вантажу, оскільки вони дозволяють легко відстежувати відправлення з моменту його пакування до моменту доставки. Це дозволяє компаніям вчасно виявляти будь-які втрати або пошкодження вантажу та приймати заходи для їх запобігання в майбутньому.

Загалом, штрихкоди є незамінним інструментом у логістиці та управлінні ланцюгом постачання. Вони допомагають забезпечити точність та швидкість обробки інформації, покращують комунікацію та співпрацю між різними відділами компанії, зменшують час та витрати на складський облік та вантажоперевезення, а також забезпечують безпеку вантажу та вчасне виявлення будь-яких проблем в логістичному процесі.

Однак, при використанні інформаційної технології розпізнавання штрихкодів та QR-кодів необхідно враховувати різні виклики та складнощі. Необхідно забезпечити високу точність та швидкість зчитування, враховуючи різні типи штрихкодів та QR-кодів, а також забезпечити безпеку даних та зручність використання.

Для досягнення цих цілей необхідно ретельно спроектувати інформаційну технологію, використовуючи відповідні програмні засоби та обладнання. Також необхідно забезпечити високу якість обслуговування та підтримку користувачів, що дозволить компаніям успішно використовувати інформаційну технологію розпізнавання штрихкодів та QR-кодів у своїй діяльності.

Високоякісна інформаційна технологія розпізнавання штрихкодів та QR-кодів має багато переваг для логістичних компаній. Наприклад, вона дозволяє зменшити час, необхідний для обробки даних, а також зменшити кількість помилок, пов’язаних з ручним введенням даних. Крім того, вона дозволяє компаніям легко відстежувати маршрути доставки та відслідковувати рух товарів у режимі реального часу.

Для використання інформаційної технології розпізнавання штрихкодів та QR-кодів у логістиці необхідно використовувати відповідні програмні засоби та обладнання, що дозволяють забезпечити високу точність та швидкість зчитування. Зокрема, для зчитування штрихкодів необхідно використовувати сканери штрихкодів, які можуть бути зв’язані з комп’ютером або мобільним пристроєм за допомогою USB-порту або Bluetooth. Для зчитування QR-кодів можна використовувати камеру мобільного пристрою або спеціальні QR-сканери.

Щоб забезпечити високу якість обслуговування та підтримки користувачів, логістичні компанії повинні мати кваліфіковані технічні служби та надавати регулярні навчання для співробітників, які використовують інформаційну технологію розпізнавання штрихкодів та QR-кодів. Крім того, компанії повинні надавати високоякісну технічну підтримку, яка допоможе користувачам вирішувати проблеми, пов’язані з використанням технології.

Висновок: використання штрихкодів у логістиці та ланцюгу постачання є важливим і корисним інструментом для покращення ефективності та точності обліку вантажів, зниження витрат на перевезення, складання та зберігання товарів, а також для підвищення рівня контролю за рухом товарів в логістичному ланцюзі. Впровадження технології штрихкодів дозволяє компаніям забезпечити точність та своєчасність інформації про товари, покращити комунікацію між різними логістичними частинами компанії та забезпечити більш ефективний контроль за вантажами. Проте, для успішного використання технології штрихкодів у логістиці необхідно вирішувати проблеми, пов’язані з несправністю обладнання, низькою якістю штрихкодів, несправністю системи сканування та можливістю зламу.

Список використаних джерел

1. Р. Р. Панде та Р. К. Шарма, «Barcode technology: A review,» Journal of Engineering Science and Technology Review, vol. 5, no. 3, pp. 44–49, 2012.
2. М. С. Сарвар та С. Соомро, «Bar code technology and its application,» Journal of Basic and Applied Scientific Research, vol. 2, no. 2, pp. 1198–1204, 2012.

3. А.М.М. Шаріф Уддін та М. А. Хоссейн, «Application of bar code in inventory management: A case study on Olympic Industries Limited, Bangladesh,» Journal of Management and Business Administration, vol. 1, no. 1, pp. 11–18, 2015.
4. С.А. Адейемо, «Application of bar code technology in supply chain management in Nigerian firms,» International Journal of Research in Management, Science & Technology, vol. 3, no. 1, pp. 79–87, 2015.
5. Ю.К. Двіведі, М. Р. Вейд та С. Л. Лал, «Barriers to the adoption of RFID and barcode technology in hospitals,» Knowledge and Process Management, vol. 15, no. 2, pp. 64–72, 2008.

Робота виконана під науковим керівництвом канд. екон. наук, доцента
ТИЩЕНКА Д. О.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ПАЦІЄНТІВ КЛІНІКИ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ БЛОКЧЕЙН

МАРТИНЕЦЬ А., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

Проблема, порушена у статті, це використання технології блокчейн задля захисту особистої інформації пацієнтів, що звертаються до медичних закладів. У цій статті розглядається важливість захисту персональних даних у медичній сфері, принципи роботи блокчейну, переваги цієї технології та досвід використання на державному рівні. З якими викликами блокчейн стикається відповідно до Загального регламенту захисту даних ЄС (GDPR) та яким чином ця технологія може законно бути впроваджена.

The problem raised in the article is the use of blockchain technology to protect the personal information of patients who seek medical care. This article discusses the importance of protecting personal data in the medical field, the principles of blockchain operation, the advantages of this technology, and the experience of its use at the state level. It covers the challenges that blockchain faces under the European Union's General Data Protection Regulation (GDPR) and how this technology can be legally implemented.

Актуальність. Пандемія COVID-19 та повномасштабна війна підкреслили необхідність цифрової трансформації медицини. Однак, це створило й додаткові ризики для конфіденційності пацієнтів. Медична інформація містить багато деталей про різні аспекти життя індивіда, окрім очевидного стану здоров'я та плану лікування, це можуть бути деталі майнового характеру, особистого життя та біометричні дані. І, як уся інша персональна інформація, вона є під загрозою незаконного збору та використання. Тож, захист персональних даних, які люди надають задля якісного медичного обслуговування, особливо важливий. Необхідно впроваджувати нові, більш якісні технології, що підвищать безпеку персональної інформації та попередять порушення права людини на приватність особистого життя.

Однією із технологій, що має високий рівень безпеки та невразливості, є блокчейн. Платформа на основі блокчейну є ідеальним варіантом для зберігання та обміну даними пацієнтів. Хоча є необхідність в детальному аналізі того, якими способами можливо запровадити цю технологію та які юридичні нюанси слід врахувати.

Ця технологія має ряд переваг, які зможуть спростити медичні дослідження, транспортування медикаментів, створити єдиний медичний реєстр, що полегшить

адміністративні процеси та поліпшить взаємодію в галузі охорони здоров'я. Таким чином, впровадження блокчейну в медичну сферу має великі перспективи та майбутнє.

Метою статті є аналіз важливості захисту персональних даних в медичній галузі, аспекти роботи блокчейн-платформ та їх використання в сфері охорони здоров'я задля підвищення рівня безпеки, дослідити яким чином має бути впроваджена ця технологія аби це відповідало законодавчим вимогам.

Об'єкт дослідження – блокчейн як технологія, що забезпечує безпечне зберігання та передачу персональної інформації.

Предмет дослідження – захист персональної інформації у сфері охорони здоров'я за допомогою використання технологій блокчейн, переваги, принципи роботи та її впровадження.

Аналіз попередніх досліджень. Дослідження блокчейн як технології для захисту персональної інформації пацієнтів є не широко досліджуваною у вітчизняній науковій спільноті. Загалом це невеликого об'єму статті в інтернеті від адвокатів, що пояснюють важливість захисту медичної інформації та коментують тонкощі, що пов'язані з правом обробки даних та логікою роботи блокчейн, що може суперечити регламенту про захист персональних даних. Більше про цю тему пишуть закордонні науковці. Однією із ґрунтовних робіт є робота університетів Об'єднаних Арабських Еміратів факультетів промислової та системної інженерії, електротехніки та комп'ютерних наук та медицини. «Blockchain for Patient Safety: Use Cases, Opportunities and Open Challenges» написана у 2022 році, як і більшість інших статей є нещодавно опублікованою, що свідчить про те, що ця тема є досить новою і багато досліджень цієї теми варто чекати в майбутньому.

Виклад основного матеріалу. Захист медичної інформації пацієнтів є юридичним та етичним обов'язком суб'єктів, що пов'язані з сферою постачання медичних послуг. Згідно зі статтею 3 Закону України «Основи законодавства України про охорону здоров'я» медичною інформацією є «інформація про медичне обслуговування особи або його результати, викладена в уніфікованій формі відповідно до вимог, встановлених законодавством, у тому числі інформація про стан здоров'я, діагнози та будь-які документи, що стосуються здоров'я та обмеження повсякденного функціонування/ життєдіяльності людини» [1]. Окрім того, що персональні дані у медичній сфері інформують щодо стану здоров'я пацієнта, його діагнозу та результатів медичного обстеження, вони також можуть містити деталі про генетику (спадкові властивості особи та способи успадкування характеристик у межах групи людей), статеве життя (дані про сексуальну поведінку та орієнтацію), біометричні дані (наприклад, відцифрований підпис, образ обличчя, відбитки пальців, малюнок сітківки ока тощо), інформацію про приватне та сімейне життя (дані немайнового та майнового характеру, інформацію про обставини, події та стосунки, пов'язані з особою та її сім'єю) [2].

Пацієнти (суб'єкти персональних даних), що користуються послугами медичних закладів надають згоду на надання та використання особистої інформації для проведення якісного лікування. Іноді поширення особистої інформації трапляється через недбале ставлення працівників медичної сфери до своїх обов'язків, а з розвитком технологій та цифровізацією даних проблемою можуть стати недосконалі технології захисту. У будь-якому випадку захист медичних даних пацієнтів є юридичним обов'язком лікарень і, як будь-яка інша персональна інформація, вона регулюються Законом України «Про захист персональних даних», що «спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних», і відповідно до статті 7 «забороняється обробка персональних даних (…), що стосуються здоров'я, статевого життя, біометричних або генетичних даних» [3].

Очевидно, що кожна людина прагне до належної реалізації всіх прав, наданих їй законом. Особливої уваги заслуговує сфера охорони здоров'я, в якій людина, звертаючись за медичною допомогою чи консультацією, прагне не лише отримати кваліфіковану послугу, а й бути впевненою що її дані захищенні.

Таким чином, впровадження сучасних та якісних технологій в системи безпеки клінік є необхідним кроком до мінімізування ризиків та попередження ситуацій витоку персональної інформації та неправомірне її використання, а також це сприяє розвитку відчуття довіри пацієнтів до медичних закладів.

Блокчейн є децентралізованою криптографічною системою зберігання та обміну даними. Технологія має шанс бути реалізованим у сферах, де захист персональних даних має надважливе значення тому, що робота блокчейну здійснюється таким чином, що нові блоки завжди зберігаються лінійно за логікою часового порядку. Тобто вони завжди додаються в «кінець» ланцюгу. Після того, як блок додано, важко змінити вміст блоку, оскільки кожен блок містить свій власний хеш (hash), а також хеш блоку перед ним. Хеш-коди створюються математичною функцією, яка перетворює числову інформацію в рядок цифр і літер. Якщо цю інформацію будь-яким чином відредагувати, хеш-код також змінюється.

Припустімо, хакер намагається відредагувати дані транзакцій таким чином, що клієнту доведеться заплатити за покупку двічі, та зі зміною суми транзакції – змінюється хеш блоку. Наступний блок у ланцюжку все ще міститиме старий хеш, і хакерам потрібно буде оновити і цей блок, щоб не залишити слідів. Щоб змінити блок, хакеру потрібно змінити кожен блок у блокчейні. Перерахування всіх цих хешів вимагає вагомої обчислювальної потужності. Іншими словами, як тільки блок додано до блокчейну, його важко редагувати та неможливо видалити. Щоб вирішити проблему довіри, мережа блокчейн тестує комп'ютери, які хочуть приєднатися та додати блоки. Так, маючи можливість розв'язати складні обчислювальні математичні задачі, комп'ютер має право додати блок до блокчейну. Але процес додавання блоків до блокчейну, відомий у світі криптовалют як «майнінг», непростий. Якщо хакери хочуть скоординувати атаку на блокчейн, їм потрібно буде вирішити складну обчислювальну математичну задачу, вартість якої може перевищити вигоди [4].

Технологія блокчейну використовується у кіберфізичних процесах та явищах, які функціонують через посередників і таким чином наражаються на проблеми, оскільки у більшості випадків дані зберігаються у незашифрованому вигляді і недобросовісні працівники організацій можуть незаконно розповсюджувати приватну інформацію. До того ж зберігання даних на єдиному сервері робить систему вразливою. Тому блокчейн має перспективу активного розвитку у таких галузях як: освіта, наука, фінанси, медицина, туризм, кадри тощо.

Наразі блокчейн використовується, зокрема у боротьбі із корупцією, на державних рівнях багатьох країн. З метою боротьби з корупцією, уряд Грузії ініціював розробку проєкту з реєстрації прав на землю на базі технології блокчейн, що дозволило зменшити операційні витрати на 90 %. Сьогодні система дозволяє оформити право власності на земельну ділянку за 10 хвилин, а не за дні. Громадяни мають цифрові сертифікати, які ніхто не може змінити без їхнього дозволу. На рівні Європи варто згадати про систему EBSI, яка була запроваджена у 2018 році, коли 29 країн (усі країни-члени ЄС, Норвегія, Ліхтенштейн) і Європейська комісія об'єднали зусилля для створення блокчейн-партнерства і створення транскордонних сервісів для державних адміністрацій, підприємств, громадян та їхніх екосистем [5].

Отже, технологія блокчейн використовує складні алгоритми для шифрування та захисту даних, що надзвичайно ускладнює доступ хакерам до особистих даних або їх зміну і серед переваг використання блокчейн-технології для захисту даних можна назвати:

– Децентралізоване зберігання: технологія блокчейн – це розподілена база даних, у якій дані зберігаються в мережі комп'ютерів, а не в центральному місці. Децентралізоване сховище дуже ускладнює хакерам вразити систему та викрасти особисті дані, оскільки немає центральної точки збою.

– Захист від несанкціонованого втручання: після запису даних у блокчейні їх майже неможливо змінити чи видалити, що гарантує цілісність і автентичність персональних даних.

– Підвищена транспарентність: технологія блокчейн забезпечує високий ступінь прозорості, оскільки всі транзакції видно та реєструються в загальнодоступній базі. Це дозволяє легко відстежувати, хто і коли отримав доступ до персональних даних.

– Конфіденційність: забезпечення анонімності користувачів, які на відкритих блокових ланцюгах представлені буквено-цифровими загальнодоступними адресами.

Традиційні методи захисту персональних даних є недостатньо ефективними, зокрема в Україні. Інцидент з масовим витоком персональних даних громадян України з додатку «Дія», переважно з водійських прав, є тому підтвердженням. Справжню причину витоку даних ще належить встановити. Проте це грубе порушення прав людей, яке не можна не оминути [6]. А Європейський Союз для удосконалення захисту даних підійшов з юридичної сторони. У 2018 році був прийнятий Загальний регламент захисту даних (GDPR), який встановлює жорсткі вимоги до обробки персональних даних. Вони включають те, що персональні дані мають збиратися законно, прозоро та з дотриманням цільових обмежень, а також важливо те, що юридичні особи несуть значну відповідальність за порушення вимог Регламенту про захист персональних даних. Про ефективність застосування GDPR свідчить статистика, адже за два роки роботи за невідповідність зібрано майже 360 млн євро. Водночас ця статистика свідчить про те, що в Європі все ще є проблеми із захистом персональних даних.

Впровадження блокчейну як технології для захисту персональної інформації має також включати законодавчі нюанси. Відповідно до Загального регламенту захисту даних ЄС (GDPR) є певні протиріччя між технологією блокчейн і захистом даних [7]. GDPR був розроблений за умови того, що персональні дані обробляються централізовано, а застосування децентралізованих технологій, таких як блокчейн, не відповідають вимогам GDPR. До того ж суть безпеки блокчейну суперечить конфіденційності, необхідної для захисту персональних даних. Щодо України, то, по-перше, за статтею 32 Конституції України встановлено, що конфіденційна інформація про особу не може збиратися, зберігатися, використовуватися та поширюватися без її згоди, а по-друге, виклики, що створює цифрова трансформація українського бізнесу та державних інституцій, та бажання України вступити до ЄС потребує удосконалення законодавства і впровадження правил міжнародного регламенту з GDPR [8] . Тож, в Україні правила регламенту мають діяти.

Про «значне напруження між сутністю технології блокчейну та загальною структурою Загального регламенту захисту персональних даних» було зазначено European Parliamentary Research Service («EPRS») у своєму брифінгу до дослідження 2019 року «Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law» [9]. У результаті розробка проекту блокчейну повинна включати ретельний аналіз того, які дані зберігаються.

Загалом, обробка персональних даних без дозволу суб’єкти є забороненою. Згідно зі статтею 2 Закону України «Про захист персональних даних» «обробка персональних даних - будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем».

Фактично кожен процес блокчейн-системи включений в поняття «обробка даних». Це стосується транзакцій інформації через вузли, зберігання хешів, процесу перевірки, а також це збереження та синхронізація за допомогою децентралізованої системи. Блокчейн повинен регулярно оновлюватись серед усіх учасників мережі, щоб кожен мав найновішу версію повної бази даних – це також вважається обробкою даних. Усі учасники роботи блокчейну – не лише партнери по транзакціях і майнери, а й вузли – беруть участь в обробці даних.

Також виникає проблема з принципом мінімізації даних, коли резервне зберігання обмежене і записи, про персональну інформацію зокрема, зберігаються доти, поки вони потрібні з певної мети. А ось принцип блокчейну і аспект його безпеки якраз полягає в тому, щоб поширювати мережу. Відкритість і прозорість також є проблемами для конфіденційності.

Отже, необхідно знайти умови за яких обробка і мінімізація персональної інформації буде можливою. Першим і найочевиднішим буде запит дозволу клієнта на обробку даних, але є певні перешкоди, що роблять цей метод недієвим. Декларація про згоду вимагає, щоб суб'єкт, що надає дані був проінформований про те, кому будуть передані дані. Неможливо визначити до яких вузлів чи майнерів потрапить ця інформація, неможливо передбачити, хто в майбутньому може бути залучений до мережі чи перегляне дані. Видалення блоків блокчейн взагалі є неможливим, адже основа безпеки технології. Але є варіант в побудові системи таким чином, щоб не можна не було ідентифікаційних даних або обмеження доступу.

Прикладом успішного використання технологій блокчейну, що сумісний із GDPR, є блокчейн заснований на платформі Emercoin, що зберігає дані поза мережею.

Суб'єкти даних вводять персональні дані через веб-інтерфейс, захищений протоколом HTTPS. Внутрішня система шифрує дані, обчислює їхній хеш-ідентифікатор, зберігає зашифровані дані разом із хеш-ідентифікатором і вставляє хеш-ідентифікатор у сховище Emercoi. Таким чином за використання public-private-key cryptography асиметрична криптографія чи криптографічні хеш функції» дані стають анонімними, хоча водночас існування obfuscation techniques (технологія дешифрування кодів), уможливлює доступ до значення хеш-кодів.

За такої логіки роботи та протоколів блокчейн є сумісним із GDPR: легко ідентифікувати того, хто обробляє дані, може бути укладена прозора і законна згода з суб'єктом даних, забезпечується право знати, які дані обробляються, з якою метою та кому вони надаються, дані обробляються безпечним способом, суб'єкти даних мають контроль над особистими даними: дані можуть бути зміненими і хеш-код буде також оновленим, видалення здійснюється щойно закінчиться термін зберігання чи за запитом суб'єкта даних [10].

Технології блокчейн мають великий потенціал застосування у галузях, що працюють з персональною інформацією, якщо вони будуть врегульовані на законодавчому рівні. Серед таких галузей є медицина та охорона здоров'я. Принципи блокчейну підходять для ведення єдиного бази пацієнтів, лікарів та медичних записів, відстеження поставок лікарських препаратів, дистанційний моніторинг пацієнтів за допомогою мобільних технологій, що зменшує потребу в амбулаторних відвідуваннях і дозволяє дистанційно перевіряти рецепти та інші медичні дані. Це підвищить точність і повноту медичної документації, зменшить адміністративне навантаження.

Електронні медичні записи, що містять персональні дані, використовують задля ефективного обстеження, діагностики та лікування. Цими записами обмінюються лікарі різного профілю аби провести якісну медичну послугу, але під час обміну такою інформацією може виникнути ряд проблем: дані можуть бути втрачені, незареєстровані або змінені. У 2015 році CRICO, підрозділ Фонду управління ризиками Гарвардської медичного університету, проаналізував понад 23 000 заяв і позовів про медичну недбалість, у яких пацієнти зазнали певної шкоди, і виявили, що три з кожних десяти випадків (7149 випадків) включають принаймні один конкретний збій у комунікації [11]. На збій комунікації можуть вплинути не лише навички спілкування, а й випадки того, що медична інформація були неправильно сформована чи незафіксована. Рішенням цієї проблеми є створення бази інформації, що буде сумісною та доступною для всіх. Прозорий обмін даними забезпечить підвищення якості діагностики, інформування про медичні рішення та лікування, а також зменшить ситуації, що шкодять пацієнтам.

Є ряд переваг блокчейну для медичної сфери (табл. 1).

Таблиця 1

Переваги застосування блокчейну для персональних даних пацієнтів клінік

Безпека	Доступ є децентралізованим, що мінімізує ризики хакерських атак.
Хронологія	Інформація в ланцюзі розташована в часовому порядку.
Конфіденційність	Інформація є закодованою і доступна лише за наявності паролю.
Цілісність інформації	Фальсифікація даних є неможливою, інформація в блокчейні не може бути змінена чи видалена без дозволу.
Доступність	До бази можна підключитися з будь-якого пристрою з доступом до Інтернету.

Прикладом впровадження технологій блокчейну в медичній сфері є Естонія. У 2011 році уряд Естонії разом із Guardtime, компанією з кібербезпеки, заснованою в Естонії в 2007 році, застосував технології блокчейну Keyless Signature Infrastructure (KSI) для захисту медичних записів. Основна передумова KSI полягає в тому, що, використовуючи лише криптографію з хеш-функціями В Естонії кожен, хто звертався до лікаря, має власну електронну медичну картку, яку можна переглядати онлайн. Національна інформаційна система охорони здоров'я об'єднує дані від різних постачальників медичних послуг в Естонії для створення спільного запису для кожного пацієнта (станом на 2015 рік понад 95 % даних, отриманих лікарнями та лікарями, було оцифровано). Це дозволяє лікарям легко отримувати доступ до електронних медичних записів (тобто результатів аналізів, рентгенівських знімків). Пацієнти можуть переглянути свої попередні візити до лікаря, поточні рецепти, отримати загальні поради щодо здоров'я тощо [12].

Висновки. Блокчейн – це технологія, яка забезпечує захист даних від маніпуляцій завдяки складнощам керування кожною копією блокчейну в мережі. Отже, у цьому сенсі це підвищує безпеку даних. Безпека досягається завдяки тому, що записи, збережені в блокчейні, стають прозорими та незмінними. А це, у свою чергу, досягається за рахунок резервного та розподіленого зберігання кожного запису на кількох вузлах у великій мережі. Впровадження технології блокчейн у клініках має потенціал для революції в галузі охорони здоров'я та покращення захисту персональних даних. Переваги використання технології блокчейн для захисту даних у галузі охорони здоров'я численні (прозора платформа для обміну персональної інформацією про пацієнтів між постачальниками медичних послуг без шкоди для конфіденційності пацієнтів, точність і послідовність даних, що мінімізує помилки і шахрайство, доступ пацієнтів до контролю над своїми особистими даними про здоров'я, зокрема, хто має до них доступ і як вони використовуються).

Список використаних джерел

1. Основи законодавства України про охорону здоров'я : Закон України від 19.11.1992 р. № 2801-XII : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text
2. Захист персональних даних у сфері охорони здоров'я: Ірина Сенюта розповіла про дієві інструменти в роботі адвоката | ADVOKAT POST. ADVOKAT POST. URL: https://advokatpost.com/zakhyst-personalnykh-danykh-u-sferi-okhorony-zdorov-ia-iryna-seniuta-rozpovila-pro-diievi-instrumenty-v-roboti-advokata/ (дата звернення: 03.04.2023).

3. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
4. Костюк П. П. Використання технології блокчейн для забезпечення інформаційної безпеки. *Сучасний захист інформації*. 2020. № 3 (43). С. 22–28.
5. Ярова М. Навіщо впроваджувати блокчейн в державний устрій і як це допоможе у боротьбі з корупцією. *AIN.UA*. URL: https://ain.ua/2022/12/29/bornjakov-pro-blockchain/
6. Фісун В. Проблеми захисту персональних даних: досвід України та інших країн – Юридична Газета. *Юридична газета*. URL: https://yur-gazeta.com/publications/ practice/ informaciyne-pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html
7. Zimprich S. Data protection and blockchain. *dotmagazine*. URL: https://www.dotmagazine. online/issues/security-trust-in-digital-services/data-protection-and-blockchain.
8. Керівник напряму GDPR компанії Nota Group Олена Колченогова виступила на круглому столі «Захист персональних даних в Україні: перспективи європеїзації», організованному асоціацією DigitalUkraine - Nota Group. *Nota Group*. URL: http://surl.li/jzvhb/ (дата звернення: 06.04.2023).
9. European Parlament. Blockchain and the General Data Protection Regulation. *BRIEFING*. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445(ANN1)_EN.pdf.
10. Dighmelashvili E., Nanadze A., Kotliarov Y., Tsyba S., Blockchain technology is here – is it compliant with GDPR? Електронний ресурс. URL: http://surl.li/ghzxl
11. Malpractice Risks in Communication Failures. CRICO. URL: http://surl.li/ghzxb
12. E-health in Estonia. Republic of Estonia (Ministry of Social Affairs). URL: https://na.eventscloud.com/file_uploads/c5da2a5e465f932e6debe55020e70899_E-health-factsheet.pdf

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ТОКАРА В. В.

SDN МЕРЕЖА ТА ЇЇ ЗАГРОЗИ

МАРЧЕНКО Б., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

Програмно-конфігуровані Мережі (Software Defined Networking/SDN) – це поділ площини передачі та управління даними, що дозволяє здійснювати програмне управління площиною передачі, яке може бути фізично або логічно відокремлено від апаратних комутаторів та маршрутизаторів.

Software-defined Networks (Software Defined Networking/SDN) are division of the plane of transmission and data management, which allows to carry out software control of the transmission plane, which can be physical or logically separated from hardware switches and routers.

Актуальність. В останні роки відбулося величезне зростання мережевого трафіку операторів. Значною мірою це було викликано вибуховим зростанням використання онлайн-додатків і хмарних сервісів постійно зростаючим набором дротових і мобільних пристроїв, підключених до мережі. Сьогодні мережеві оператори мають працювати з великою кількістю форматів даних, типів послуг і онлайн-пристроїв, і все це без збільшення операційних витрат і витрат на обладнання.

Однак застарілі мережеві архітектури та їхні інструменти керування не були розроблені, щоб впоратися з таким надзвичайно еластичним попитом. Це суттєво обмежує здатність оператора рентабельно реагувати на вимоги до масштабу, продуктивності та взаємодії з користувачем у сучасних динамічних середовищах або розгортати диференційовані послуги.

SDN забезпечує поділ між функціями площини керування (контролер) і площини даних (комутатор) мереж за допомогою протоколу, який змінює таблиці пересилання в мережевих комутаторах. Це дає змогу оптимізувати мережі на льоту та швидко реагувати на зміни у використанні мережі без необхідності вручну переналаштовувати існуючу інфраструктуру чи купувати нове обладнання. SDN відокремлює керування мережевими пристроями від даних, які вони передають, а комутаційне програмне забезпечення від фактичного мережевого обладнання. Загалом, системи захисту інформації в SDN-мережах на основі протоколу OpenFlow є важливим напрямом досліджень в області мережевої безпеки. Вони дозволяють забезпечити високий рівень захисту мережевої інфраструктури від різних видів атак, що забезпечує надійність та безпеку роботи мережі.

OpenFlow – це протокол зв'язку, який надає доступ до площини пересилання мережевого комутатора або маршрутизатора через мережу.

OpenFlow дозволяє мережевим контролерам визначати шляхи мережевих пакетів у мережі комутаторів. Контролери відрізняються від перемикачів. Це відокремлення контролю від пересилання дозволяє більш складне керування трафіком, ніж це можливо за допомогою списків контролю доступу (ACL) і протоколів маршрутизації.

Метою статті є дослідження основних методів захисту SDN-мереж, включаючи захист від атак на різних рівнях мережі.

Об'єктом дослідження є розробка програмного забезпечення системи захисту інформації в SDN мережі.

Предмет дослідження – SDN мережа.

Аналіз попередніх досліджень. Дослідженню SDN мереж та їх загроз присвячені праці наступних науковців: Jamison Kush (Джемісон Куш), Jim Doherty (Джим Доерті), Kingston Smiler (Кінгстон Сміллер), Doug Marschke (Дуг Марке) та інші.

Виклад основного матеріалу. На сьогоднішній день необхідно знати різницю між традиційною мережею та мережею. Порівняльна характеристика подана в табл. 1.

Таблиця 1

Порівняльна характеристика SDN мережі та традиційної мережі

№	SDN	ТРАДИЦІЙНА МЕРЕЖА
1	Мережа, визначена програмним забезпеченням, – це віртуальний мережевий підхід	Традиційна мережа – це старий традиційний мережевий підхід.
2	Програмно визначена мережа – це централізоване керування	Традиційна мережа – це розподілене управління.
3	Ця мережа є програмованою	Ця мережа не програмується.
4	Програмно визначена мережа є відкритим інтерфейсом	Традиційна мережа має закритий інтерфейс.
5	У програмно визначеній мережі площина даних і площина керування роз'єднані програмним забезпеченням	У традиційній мережі площина даних і площина керування монтуються на одній площині.
6	Він підтримує автоматичне налаштування, тому це займає менше часу	Він підтримує статичну/ручну конфігурацію, тому це займає більше часу
7	Він може визначати пріоритети та блокувати певні мережеві пакети	Він веде всі пакети однаково без підтримки пріоритетів

№	SDN	ТРАДИЦІЙНА МЕРЕЖА
8	Його легко програмувати відповідно до потреб	Важко заново запрограмувати та замінити існуючу програму відповідно до використання
9	Вартість програмно визначеної мережі низька	Вартість традиційної мережі висока
10	Структурна складність у програмно визначеній мережі низька	Структурна складність традиційної мережі висока
11	Розширюваність висока в програмно визначеній мережі.	Розширюваність у традиційній мережі низька
12	У SDN легко виявляти несправності та звітувати, оскільки вона централізована	У традиційній мережі важко усунути несправності та повідомити про них, оскільки вона розподіляється під контролем
13	Його вартість обслуговування нижча, ніж традиційна мережа	Вартість обслуговування традиційної мережі вища, ніж SDN

Традиційна мережа відноситься до старого традиційного способу роботи в мережі, який використовує фіксовані та виділені апаратні пристрої, такі як маршрутизатори та комутатори, для контролю мережевого трафіку.

Неможливість масштабування, безпека та продуктивність мережі є головною проблемою в нинішній зростаючій бізнес-ситуації, тому SDN бере під контроль традиційну мережу. Традиційна мережа є статичною та базується на апаратних мережевих пристроях.

SDN означає мережу, визначену програмним забезпеченням, яка є підходом до мережевої архітектури. Він дозволяє контролювати та керувати мережею за допомогою програмних додатків. Через програмно визначену мережу (SDN) мережева поведінка всієї мережі та її пристроїв програмується централізовано за допомогою програмних додатків із використанням відкритих API.

Програмно визначена мережа покращує продуктивність завдяки віртуалізації мережі. У SDN керовані програмним забезпеченням додатки або API працюють як основа повного керування мережею, яка може спрямовувати трафік у мережі або спілкуватися з основною апаратною інфраструктурою [1]. Пропоную розглянути архітектуру SDN мережі (рис. 1).

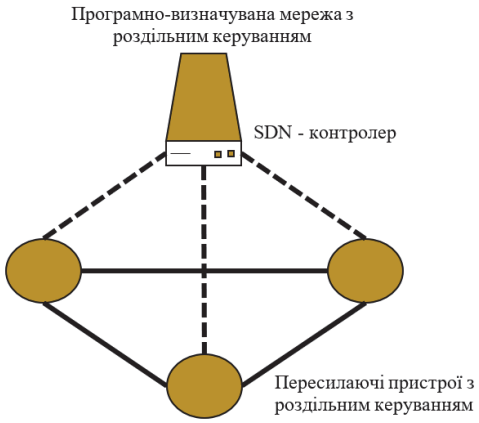


Рис. 1. Архітектура SDN мережі

Архітектура SDN містить п’ять основних компонентів. Кожен з цих компонентів має невід’ємну роль у роботі мережі, у полегшенні роботи обладнання та його обслуговуванні адміністратором мереж.

1. Компонент керування

У SDN використовується набір мережевих додатків для гнучкого керування та простоти реалізації нових додатків та сервісів (маршрутизації, балансування навантаження, застосування політик або рекомендований додаток від постачальника послуг). За допомогою існуючих API організується та автоматизується мережа.

2. Компонент контролю

Є найбільш інтелектуальним та важливим рівнем архітектури SDN. Містить один або кілька контролерів, що пересилають різні типи правил та політик на рівень інфраструктури через південний інтерфейс.

3. Компонент даних

По-третє, рівень даних, також відомий як рівень інфраструктури, представляє пристрої пересилання мережі (маршрутизатори, комутатори, балансувальники навантаження тощо. буд.). Він використовує південні API-інтерфейси для взаємодії з площиною управління, отримуючи правила та політики переадресації для застосування їх до відповідних пристроїв.

4. Північний інтерфейс

Інтеграція між контролером та додатком. В основному інтерфейси є набір інтерфейсів прикладного програмування (API) з відкритим вихідним кодом.

5. Південні інтерфейси

Інтеграція між контролером та мережевими пристроями. Інтерфейси дозволяють передавати політики на площину пересилання.

SDN мережа, в порівнянні з іншими традиційними мережами з розподіленим керуванням має наступні переваги:

- Збільшення видимості мережі;

Огляд мережі в одному місці, що усуває сліпі зони, які є у традиційних мережах.

- Масштабованість;

Гнучкість SDN значно полегшує масштабування бізнес-операцій без ризику перебоїв в обслуговуванні.

- Сумісність із великими даними;

Висока пропускна здатність для паралельної обробки даних та управління ними.

- Поліпшена безпека

З централізацією SDN адміністратори зможуть розробляти та розповсюджувати важливі політики та протоколи безпеки по всій мережі по всіх пристроях та важливих компонентах.

- Відкритий вихідний код;

SDN слід відкритим стандартам та використовується з мережевим обладнанням будь-якого постачальника. Тобто SDN може підключатися до різних хмар, пристроїв та програм.

- Більш ефективний IT-відділ;

Оскільки SDN оптимізує та спрощує керування мережею, ваші IT-фахівці зможуть зосередитися на покращенні надання послуг.

- Економічна ефективність;

SDN дешевше в експлуатації та має нижчу сукупну вартість, вимагаючи менше витрат та підвищуючи ефективність використання сервера [2].

В період сьогодення, більшість SDN мереж використовують стандарт OpenFlow. Давайте розглянемо, що ж таке OpenFlow.

OpenFlow (OF) вважається одним із перших програмно-визначених мережевих стандартів (SDN) .

Він спочатку визначив протокол зв'язку в архітектурах SDN , який дозволив контролеру SDN безпосередньо взаємодіяти з площиною пересилання мережевих пристроїв, таких як комутатори та маршрутизатори, як фізичні, так і віртуальні (на основі гіпервізора), щоб він міг краще адаптуватися до мінливих вимог бізнесу.

Контролер SDN у SDN – це «мозок» мережі SDN, який передає інформацію на комутатори/маршрутизатори «внизу» (через південні API), а програми та бізнес-логіку «вгорі» (через північні API). Останнім часом, коли організації розгортають більше віртуальних накладених мереж SDN , контролерам SDN було доручено об'єднати домени контролерів SDN за допомогою загальних інтерфейсів додатків, таких як OpenFlow і відкрита база даних віртуальних комутаторів (OVSDB).

Щоб працювати в середовищі OF, будь-який пристрій, який хоче спілкуватися з контролером SDN, повинен підтримувати протокол OpenFlow . За допомогою цього інтерфейсу контролер SDN вносить зміни в таблицю потоків комутатора/ маршрутизатора , дозволяючи мережевим адміністраторам розділяти трафік [3].

SDN на основі OpenFlow наразі розгортається в різноманітних мережевих пристроях і програмному забезпеченні, надаючи значні переваги як підприємствам, так і операторам, зокрема:

- Централізоване управління та контроль мережевих пристроїв від кількох постачальників;
- Швидкі інновації завдяки можливості надавати нові мережеві можливості та послуги без необхідності налаштовувати окремі пристрої чи чекати випусків від постачальників;
- Можливість програмування операторами, підприємствами, незалежними постачальниками програмного забезпечення та користувачами (не лише виробниками обладнання) за допомогою загального середовища програмування, що дає всім сторонам нові можливості для підвищення прибутку та диференціації;
- Підвищена надійність і безпека мережі завдяки централізованому й автоматизованому управлінню мережевими пристроями, уніфікованому застосуванню політики та меншій кількості помилок конфігурації;
- Більш детальний контроль мережі з можливістю застосування комплексних і широкомасштабних політик на рівні сеансу, користувача, пристрою та програми;
- Кращий досвід роботи з кінцевим користувачем, оскільки додатки використовують централізовану інформацію про стан мережі [4].

Записи таблиці потоків, якими можна маніпулювати в комутаторі OF (рис. 2).

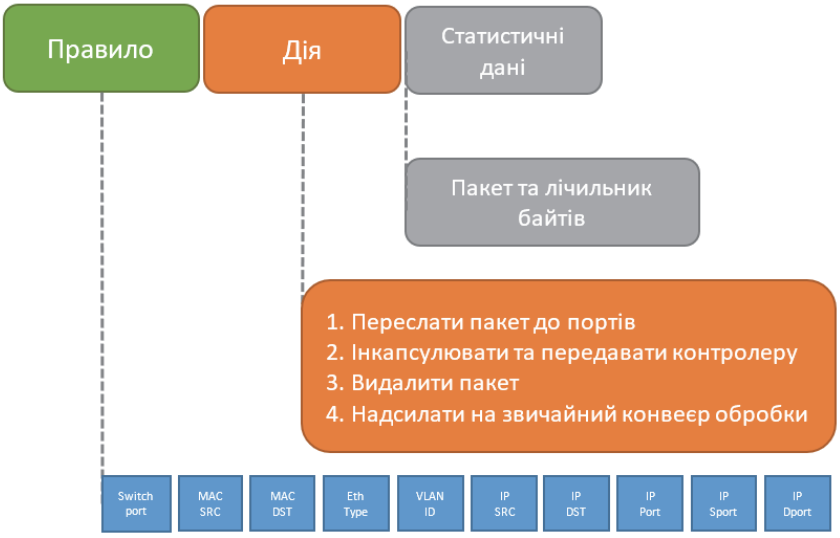


Рис. 2. Робота в комутаторі OpenFlow

Розвиток мереж породжує нові типи атак, виявлені та невизначені ризики та експлойти нульового дня. Наразі немає історії попередніх реальних атак SDN, тому важко визначити наявні вразливості та створити на їх основі захист.

1. Маніпуляція мережею : критична атака, яка відбувається на площині керування. Зловмисник компрометує контролер SDN, створює неправдиві дані мережі та ініціює інші атаки на всю мережу.

Як захиститися: щоб пом'якшити цю атаку, контролер SDN повинен мати надлишковий об'єкт, а канали зв'язку мають бути захищені за допомогою надійного шифрування.

2. Перенаправлення трафіку : ця атака відбувається на елементи мережі в площині даних. Атака компрометує мережевий елемент, щоб перенаправити потоки трафіку та дозволити прослуховування.

Як захиститися: Захистіть елементи мережі та її канали зв'язку за допомогою надійного шифрування.

3. Атака по бічному каналу : об'єктом цієї атаки можуть бути елементи мережі в площині даних. Інформація про час, наприклад, скільки часу потрібно для встановлення нового мережевого з'єднання, може повідомити зловмиснику, чи існує правило потоку, чи ні.

Як захиститися: Захистіть елементи мережі за допомогою надійного алгоритму шифрування.

4. Маніпуляція програмою : ця атака відбувається в площині програми. Використання вразливості програми може спричинити несправність, перебої в роботі служби або прослуховування даних. Зловмисник може отримати доступ із високими привілеями до програми SDN і виконувати незаконні операції.

Як захиститися: постійно оновлюйте сервери останніми виправленнями.

5. Відмова в обслуговуванні «DoS» : це одна з найпоширеніших атак, яка може впливати на всі частини SDN. Застосувавши DoS, зловмисник може призвести до зниження або повного зриву служб SDN.

Як захиститися: використовуйте методи обмеження швидкості та скидання пакетів.

6. ARP Spoofing Attack : атака Man-in-the-middle, яка також називається отруєнням кешу ARP. Хакер може використовувати ARP-спуфінг, щоб проникнути в мережу, перехопити трафік, змінити його та навіть зупинити. Цей тип атаки пошкоджує інформацію про топологію мережі та додатки SDN, що володіють топологією. Отруєння також може статися через інші протоколи, такі як LLDP або IGMP.

Як захиститися: Рекомендується використовувати надійні методи автентифікації.

7. Експлуатація API : API компонента програмного забезпечення можуть містити вразливості, які можуть дозволити хакеру здійснити несанкціоноване розкриття інформації. Експлуатація API також може статися на північному інтерфейсі та може призвести до руйнування мережевих потоків.

Як захиститися: постійно оновлюйте сервери останніми виправленнями.

8. Перехоплення трафіку : атаки перехоплення – це популярний метод, який використовують хакери для захоплення та аналізу інформації мережевого зв'язку. За допомогою сніфінгу хакер також може підслуховувати дані з мережевих елементів або посилань і викрадати важливу інформацію. Нюхання може статися будь-де, де є постійний рух. У SDN хакер може скористатися перевагами незашифрованого зв'язку, щоб перехопити трафік від центрального контролера та до нього. Зібрані дані можуть включати важливу інформацію про потоки або трафік, дозволений у мережі.

Як захиститися: використовуйте надійний метод шифрування.

9. Вгадування пароля або груба сила : ця атака може відбутися на елементі, що не є SDN. За допомогою вгадування пароля або грубої сили неавторизований користувач може отримати доступ до SDN.

Як захиститися: змініть паролі постачальників за замовчуванням, використовуйте надійні паролі та часто оновлюйте їх [5].

Висновки. Чи може SDN підвищити безпеку? Розгортання SDN все ще незріле, і важко передбачити, як зловмисники будуть націлюватися на інфраструктуру SDN. Знання про атаки та загрози SDN дуже обмежені. Те, що ми бачили та дізналися в історії кібератак і контратак у традиційних мережах, це те, що нові технології приходять разом із новими вразливими місцями .

Щоб повністю присвятити себе SDN, потрібно подбати про деякі проблеми безпеки, наприклад централізоване керування мережею та функції програмування . Але технологія не поверне нас назад у часі, SDN набирає популярності, а її вдосконалення відбуваються надзвичайно швидко. Ймовірно, завдяки SDN ми побачимо набагато більше переваг безпеки порівняно з традиційними мережами.

Список використаних джерел

1. Topology Discovery in Software Defined Networks: Threats, Taxonomy, and State-of-the-Art \\ Режим доступу: https://ieeexplore.ieee.org/abstract/document/7534866 (останнє звернення 27.02.2023 р.)
2. Security in Software-Defined Networking: Threats and Countermeasures \\ Режим доступу: https://link.springer.com/article/10.1007/s11036-016-0676-x (останнє звернення 27.02.2023 р.)
3. Software-Defined Networking: A Comprehensive Survey \\ Режим доступу: https:// ieeexplore.ieee.org/abstract/document/6994333 (останнє звернення 01.03.2023 р.)
4. Jennia Hizver, Taxonomic Modeling of Security Threats in Software Defined Networking \\ Режим доступу: https://www.gti.bh/Library/assets/us-15-hizver-taxonomic-modeling-of-security-threats-in-software-defined-networking-wp.pdf (останнє звернення 01.03.2023 р.)
5. SDN-Enabled Hybrid DL-Driven Framework for the Detection of Emerging Cyber Threats in IoT\\ Режим доступу: https://www.mdpi.com/2079-9292/10/8/918 (останнє звернення 05.03.2023 р.)

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л. О.

ТЕХНОЛОГІЇ IDS ТА IPS ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПІДПРИЄМСТВА РИТЕЙЛУ

МАРЧУК Б., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

Підприємства роздрібної торгівлі збирають величезну кількість персональних даних своїх клієнтів, включаючи імена, адреси, номери телефонів та інформацію про кредитні картки. Таким чином, захист цих даних має вирішальне значення для підтримки довіри клієнтів і уникнення дорогого витоку даних. Останніми роками багато підприємств роздрібної торгівлі запровадили технологію захисту персональних даних, щоб захистити особисту інформацію своїх клієнтів.

Retail businesses collect vast amounts of personal data about their customers, including names, addresses, phone numbers and credit card information. Protecting this data is therefore critical to maintaining customer trust and avoiding costly data breaches. In recent years, many retailers have implemented data protection technology to protect their customers' personal information.

Актуальність. Однією з поширених технологій, що використовується роздрібними підприємствами, є шифрування даних. Це передбачає перетворення конфіденційної інформації в нечитабельний код, який можна розшифрувати лише за допомогою правильного ключа. Підприємства роздрібної торгівлі можуть використовувати шифрування для захисту даних клієнтів як під час передачі через Інтернет, так і під час їх зберігання на своїх серверах.

Ще одна важлива технологія для захисту персональних даних – брандмауери. Брандмауери – це програми, які обмежують несанкціонований доступ до мережі компанії. Впроваджуючи брандмауери, підприємства роздрібної торгівлі можуть запобігти доступу кіберзлочинців до особистої інформації своїх клієнтів.

Окрім шифрування та брандмауерів, підприємства роздрібної торгівлі також можуть впроваджувати системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS). IDS та IPS – це програми, які можуть виявляти та блокувати кібератаки в реальному часі. Ці технології можуть допомогти підприємствам роздрібної торгівлі запобігти витоку даних і захистити особисту інформацію своїх клієнтів.

Нарешті, роздрібні підприємства також можуть використовувати технологію маскування даних. Маскування даних передбачає заміну конфіденційних даних фіктивними, щоб вихідні дані були недоступні неавторизованим користувачам. Роздрібні підприємства можуть використовувати маскування даних для захисту конфіденційних даних, таких як номери кредитних карток або номери соціального страхування.

Метою статті є дослідження та класифікація технологій захисту на підприємствах роздрібної торгівлі.

Об'єктом дослідження є розробка програмного забезпечення захисту підприємств роздрібної торгівлі.

Предмет дослідження – захист персональних даних.

Аналіз попередніх досліджень. Дослідженню менеджерів паролів присвячені праці наступних науковців: Wanda Presthus(Ванда Престус), Linda Andersen(Лінда Андерсен), David Prepletany(Девід Преплетані), Deyan Chen(Деян Чен), Hong Zhao(Хонг Чжао), Indu Niranjan (Інду Ніранджан), Varun Tandon(Варун Тандон) та інші.

Виклад основного матеріалу. У даній статті ми розглянемо систему виявлення вторгнень (IDS), та систему запобігання вторгнень (IPS) на підприємстві. На рис. 1 зображена схема роботи системи виявлення вторгнень.

Система виявлення вторгнень (IDS) – це технологія мережевої безпеки, спочатку розроблена для виявлення уразливостей цільової програми або комп'ютера.

IDS також є пристроєм лише для прослуховування. IDS відстежує трафік і повідомляє результати адміністратору. Він не може автоматично вжити заходів, щоб запобігти виявленому експлойту захопити систему.

Зловмисники здатні швидко використовувати вразливі місця, коли вони проникають у мережу. Таким чином, IDS не підходить для профілактики. Системи виявлення та запобігання вторгненням важливі для безпеки інформації та керування подіями.

Коли була розроблена IDS, глибина аналізу, необхідна для виявлення вторгнення, не могла бути виконана досить швидко. Швидкість не встигає за компонентами на прямому шляху зв'язку мережевої інфраструктури.

Системи виявлення мережевих вторгнень використовуються для виявлення підозрілої активності, щоб зловити хакерів до того, як буде завдано шкоди мережі. Існують мережеві та хост-системи виявлення вторгнень. IDS на основі хоста встановлюються на клієнтські комп'ютери; мережеві IDS знаходяться в самій мережі.

IDS працює, шукаючи відхилення від нормальної активності та відомі сигнатури атак. Аномальні шаблони надсилаються в стек і перевіряються на протокольному та прикладному рівнях. Він може виявляти такі події, як отруєння DNS, неправильно сформовані інформаційні пакети.

IDS може бути реалізований, як пристрій безпеки мережі або програмне забезпечення. Для захисту даних і систем у хмарних середовищах також доступні хмарні IDS.

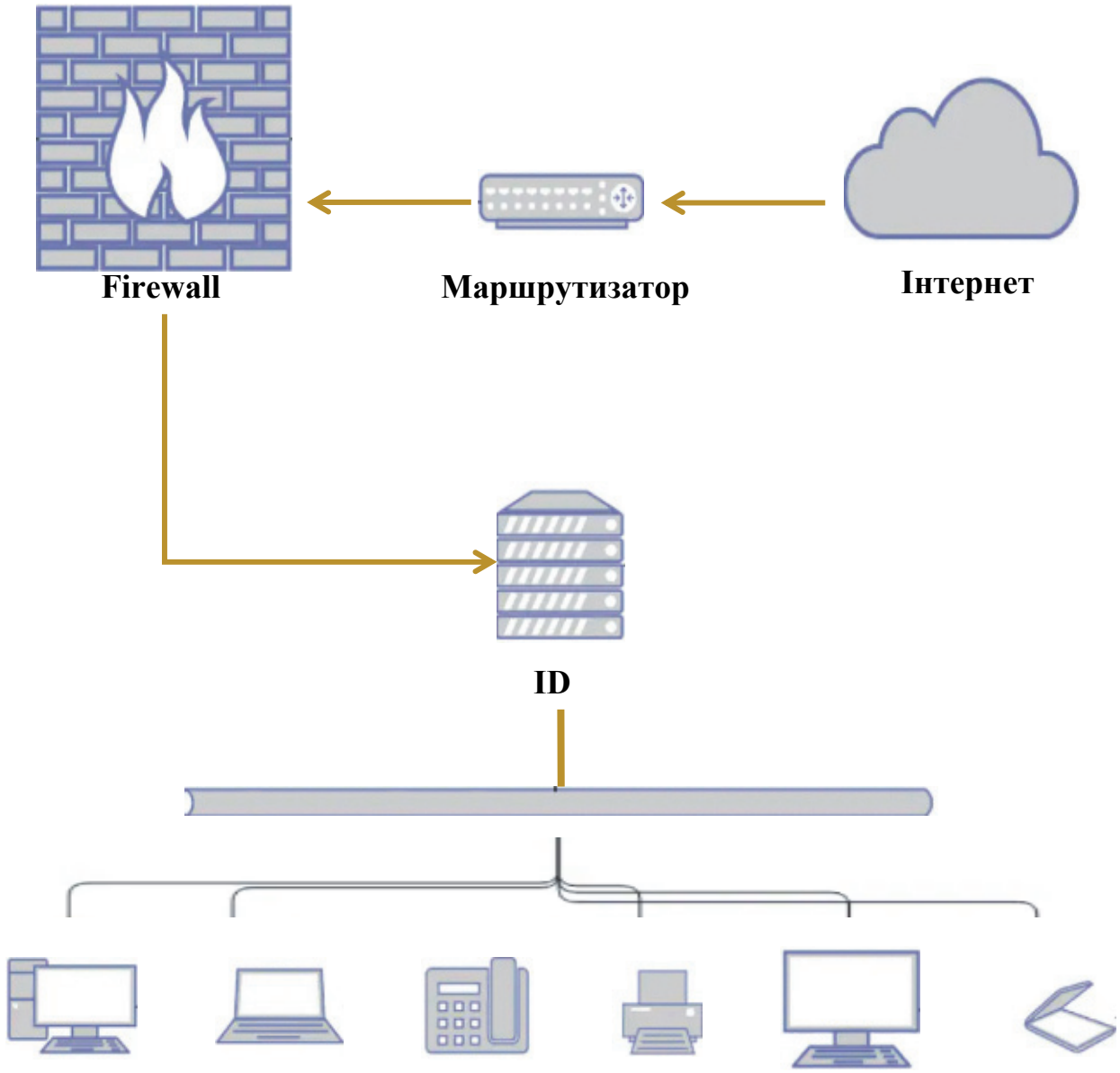


Рис. 1. Принцип роботи системи IDS

Тепер пропоную розглянути основні типи IDS: на основі мережі, на основі хоста, на основі протоколу, на основі протоколу програми та гібридний.

Два найпоширеніші типи IDS:

1. Мережева система виявлення вторгнень (NIDS).

Мережева IDS контролює всю захищену мережу. Він розгортається по всій інфраструктурі в стратегічних точках, таких як найбільш уразливі підмережі. NIDS відстежує весь трафік, що надходить до та від пристроїв у мережі, роблячи визначення на основі вмісту пакетів і метаданих.

2. Система виявлення вторгнень на основі хоста (HIDS).

IDS на основі хоста відстежує комп'ютерну інфраструктуру, на якій її встановлено. Іншими словами, він розгортається на певній кінцевій точці, щоб захистити її від внутрішніх і зовнішніх загроз. IDS досягає цього, аналізуючи трафік, реєструючи зловмисну активність і повідомляючи призначені органи.

Решта три типи можна описати так:

3. На основі протоколу (PIDS).

Система виявлення вторгнень на основі протоколу зазвичай встановлюється на веб-сервері. Він відстежує та аналізує протокол між користувачем/пристроєм і сервером. PIDS зазвичай знаходиться на передній частині сервера та контролює поведінку та стан протоколу.

4. На основі протоколу додатків (APIDS).

APIDS – це система або агент, який зазвичай знаходиться всередині серверної сторони. Він відстежує та інтерпретує листування за протоколами, що стосуються окремих програм. Наприклад, це відстежуватиме протокол SQL для проміжного програмного забезпечення під час транзакцій із веб-сервером.

5. Гібридна система виявлення вторгнень.

Гібридна система виявлення вторгнень поєднує два або більше підходи до виявлення вторгнень. Використання цієї системи, даних системи або хост-агента в поєднанні з мережевою інформацією для повного уявлення про систему. Гібридна система виявлення вторгнень більш потужна порівняно з іншими системами.

Але зловмисники можуть використовувати численні методи, щоб уникнути виявлення IDS. Ці методи можуть створити проблеми для IDS, оскільки вони призначені для обходу існуючих методів виявлення:

- Фрагментація.

Фрагментація ділить пакет на менші фрагментовані пакети. Це дозволяє зловмиснику залишатися прихованим, оскільки не буде сигнатур атаки для виявлення.

Фрагментовані пакети пізніше реконструюються вузлом одержувача на рівні IP. Потім вони пересилаються на прикладний рівень. Атаки фрагментації генерують шкідливі пакети шляхом заміни даних у складових фрагментованих пакетах новими даними.

- Затоплення

Ця атака спрямована на перевантаження детектора, викликаючи збій механізму керування. Коли детектор виходить з ладу, весь трафік буде дозволено.

Популярним способом спричинити затоплення є підробка законного протоколу дейтаграм користувача (UDP) і протоколу керуючих повідомлень Інтернету (ICMP). Затоплення трафіку потім використовується для маскування аномальної діяльності зловмисника. У результаті IDS матиме великі труднощі з пошуком шкідливих пакетів у величезному обсязі трафіку.

- Обфускація.

Обфускацію можна використовувати, щоб уникнути виявлення, роблячи повідомлення складним для розуміння, тим самим приховуючи атаку. Термінологія обфускації означає зміну програмного коду таким чином, щоб він залишався функціонально нерозрізненим.

- Шифрування

Шифрування пропонує численні можливості безпеки, включаючи конфіденційність даних, цілісність і конфіденційність. На жаль, розробники шкідливих програм використовують атрибути безпеки, щоб приховати атаки та уникнути виявлення [1].

Також необхідно розібратися у роботі системи запобігання вторгненням (IPS). На рис. 2 показано, як працює дана система.

Система запобігання вторгненням (IPS) – це інструмент безпеки мережі (який може бути апаратним пристроєм або програмним забезпеченням), який постійно відстежує мережу на наявність зловмисної активності та вживає заходів для її запобігання, зокрема повідомляє, блокує або видаляє її, коли вона відбувається.

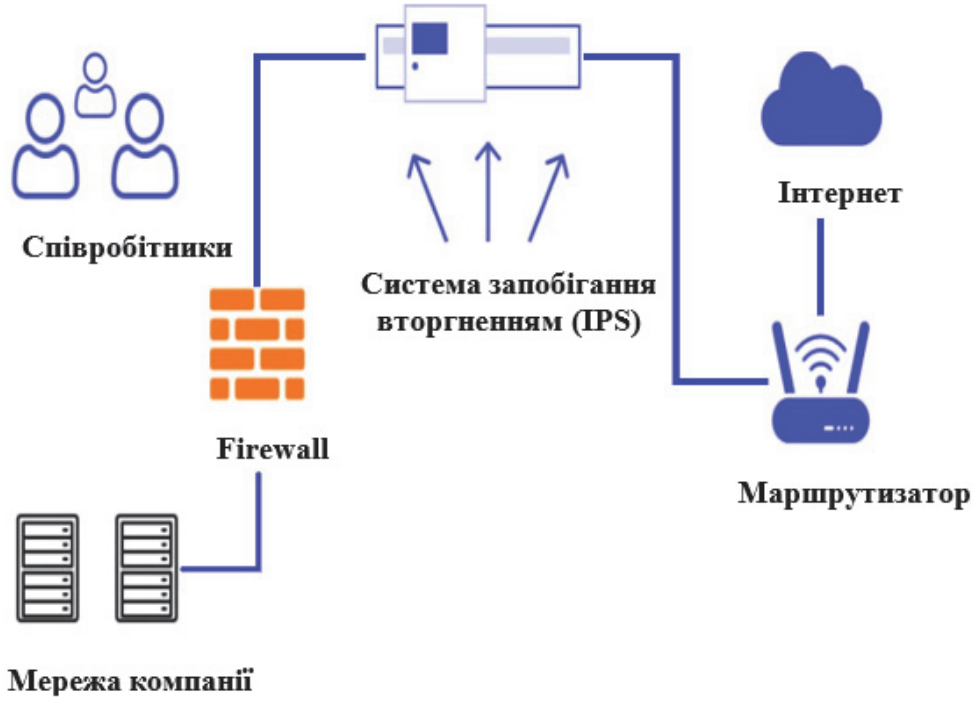


Рис. 2. Принцип роботи системи IPS

Вона є більш досконалою, ніж система виявлення вторгнень (IDS), яка просто виявляє зловмисну активність, але не може вжити заходів проти неї, окрім сповіщення адміністратора. Системи запобігання вторгненням іноді входять до складу брандмауера наступного покоління (NGFW) або рішення для єдиного управління загрозами (UTM). Як і багато інших технологій захисту мережі, вони мають бути достатньо потужними, щоб сканувати великий обсяг трафіку без зниження продуктивності мережі.

Система запобігання вторгненням розміщується в мережі, в потоці мережевого трафіку між джерелом і одержувачем, і зазвичай розташована безпосередньо за брандмауером. Існує кілька методів, які використовують системи запобігання вторгненням для виявлення загроз:

1. На основі сигнатур.

Цей метод зіставляє активність із сигнатурами відомих загроз. Одним із недоліків цього методу є те, що він може зупинити лише раніше ідентифіковані атаки та не зможе розпізнати нові.

2. На основі аномалій.

Цей метод відстежує аномальну поведінку шляхом порівняння випадкових зразків мережевої активності з базовим стандартом. Він більш надійний, ніж моніторинг на основі сигнатур, але іноді може давати помилкові спрацьовування. Деякі новіші та вдосконалені системи запобігання вторгненням використовують штучний інтелект і технологію машинного навчання для підтримки моніторингу на основі аномалій.

3. На основі політики.

Цей метод дещо менш поширений, ніж моніторинг на основі сигнатур або аномалій. Він використовує політики безпеки, визначені підприємством, і блокує дії, які порушують ці політики. Для цього потрібен адміністратор, щоб установити та налаштувати політики безпеки.

Як тільки IPS виявляє зловмисну активність, вона може виконувати багато автоматичних дій, включаючи сповіщення адміністраторів, скидання пакетів, блокування трафіку з адреси джерела або скидання з'єднання. Деякі системи запобігання вторгненням також використовують «приманку» або приманку цінних даних, щоб залучити зловмисників і не дати їм досягти своїх цілей [2].

Існує кілька типів IPS, кожен з яких має дещо інше призначення:

- Система запобігання вторгненню в мережу (NIPS).

Цей тип IPS встановлюється лише в стратегічних точках для моніторингу всього мережевого трафіку та проактивного сканування на наявність загроз.

- Система запобігання вторгнень на хост (HIPS).

На відміну від NIPS, HIPS встановлюється на кінцевій точці (наприклад, ПК) і переглядає вхідний і вихідний трафік лише з цієї машини. Він найкраще працює в поєднанні з NIPS, оскільки служить останньою лінією захисту від загроз, які подолали NIPS.

- Аналіз поведінки мережі (NBA).

Аналізує мережевий трафік для виявлення незвичайних потоків трафіку, таких як атаки DDoS (розподілена відмова в обслуговуванні).

- Система запобігання бездротовому вторгненню (WIPS).

Цей тип IPS просто сканує мережу Wi-Fi на предмет несанкціонованого доступу та відключає неавторизовані пристрої з мережі.

Система запобігання вторгненням пропонує багато переваг:

- Додаткова безпека.

IPS працює в парі з іншими рішеннями безпеки та може ідентифікувати загрози, які не можуть ці інші рішення. Особливо це стосується систем, які використовують виявлення аномалій. Він також забезпечує чудову безпеку програм завдяки високому рівню обізнаності про програми.

- Підвищена ефективність інших елементів керування безпекою.

Оскільки IPS відфільтровує зловмисний трафік до того, як він досягне інших пристроїв безпеки та елементів керування, це зменшує навантаження на ці засоби керування та дозволяє їм працювати ефективніше.

- Економія часу.

Оскільки IPS значною мірою автоматизована, вона потребує менше часу від IT-команд.

- Відповідність.

IPS відповідає багатьом вимогам відповідності, встановленим PCI DSS, HIPAA та іншими. Він також надає цінні дані аудиту.

- Налаштування.

IPS можна налаштувати з налаштованими політиками безпеки, щоб забезпечити контроль безпеки, специфічний для підприємства, яке його використовує.

Однак організаціям слід бути обережними з IPS, оскільки вони також можуть бути схильні до помилкових спрацьовувань. Помилкове спрацьовування IPS, швидше за все, буде більш серйозним, ніж хибне спрацьовування IDS, оскільки IPS перешкоджає проходженню законного трафіку, тоді як IDS просто позначає його як потенційно шкідливий[3].

Декілька постачальників інтегрують IDS та IPS разом в один продукт – відомий як уніфіковане керування загрозами (UTM), – що дозволяє організаціям впроваджувати обидві технології, одночасно разом із брандмауерами та системами у своїй інфраструктурі безпеки.

Але нам необхідно вирішити, яка з цих систем надійніша. Тому пропоную вам розглянути таблицю 1, щоб зрозуміти основні відмінні риси цих двох технологій захисту персональних даних.

Таблиця 1

Порівняльна характеристика технологій захисту даних

	IDS	IPS
Ім’я	Система виявлення вторгнень	Система запобігання вторгненням
Опис	Система, яка відстежує мережевий трафік на наявність підозрілої активності та попереджає користувачів, коли така активність виявлена	Система, яка відстежує мережевий трафік і попереджає про підозрілу активність, як IDS, але також вживає запобіжних заходів щодо підозрілої активності

	IDS	IPS
Розташування	На клієнтському комп'ютері встановлено систему виявлення вторгнень на основі хоста. Мережева система виявлення вторгнень знаходиться в мережі	Розташований між брандмауером компанії та рештою мережі
Використання	Попереджає про підозрілу активність, але не запобігає їй.	Попереджає про підозрілу активність і запобігає їй
Помилково спрацьовує	Помилкові спрацьовування IDS зазвичай викликають невеликі незручності. Хоча IDS неправильно позначає законний трафік як зловмисний, це не запобігає входженню трафіку в мережу	Хибні спрацьовування IPS можуть бути серйознішими. Коли IPS приймає законний трафік за загрозу, він зупиняє легітимний трафік від входу в мережу, що може вплинути на будь-яку частину організації, а не лише на IT-команду

Висновки. Підсумовуючи, технологія захисту персональних даних є важливою для підприємств роздрібної торгівлі для захисту особистої інформації своїх клієнтів. Застосовуючи шифрування IDS та IPS, підприємства роздрібної торгівлі можуть запобігати кібератакам і захищати особисті дані своїх клієнтів.

Список використаних джерел

1. Information privacy from a retail management perspective \\ Режим доступу: https://www.researchgate.net/profile/WandaPresthus/publication/329040915_Information Privacy_from_a_Retail_Managment_Perspective/links/5c29f060a6fdccfc70732ba0/Information-Privacy-from-a-Retail-Managment-Perspective.pdf (останнє звернення 27.03.2023 р.)
2. Data Security and Privacy Protection Issues \\ Режим доступу: https://ieeexplore.ieee.org/ abstract/document/6187862 (останнє звернення 27.03.2023 р.)
3. Threat to Retail Business Information Security: Cybersecurity in the Retail Industry \\ Режим доступу: https://www.proquest.com/openview/52d446e8bcd092c8d8464d76976eb89e/1?pqo-rigsite=gscholar&cbl=18750 (останнє звернення 03.04.2023 р.)

Робота виконана під науковим керівництвом старшого викладача
БЕБЕШКА Б. Т.

ВПЛИВ АНАЛІТИЧНИХ СИСТЕМ НА ПРОЦЕС ПРИЙНЯТТЯ РІШЕНЬ У БІЗНЕСІ

МАШЕВСКИЙ О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуті основні аспекти використання аналітичних систем в бізнесі та їх вплив на процес прийняття рішень. Розглянуто як зразок конкретні використання аналітичних систем, які допомогли покращити ефективність бізнесу, а також приведені рекомендації щодо вибору та впровадження аналітичних систем у практичну діяльність компанії.

The article covers the main aspects of using analytical systems in business and their impact on the decision-making process. Concrete examples of the specific uses of analytical systems that have helped to improve business efficiency are examined, and recommendations for selecting and implementing analytical systems in a company's practical activities are provided.

Актуальність. З появою великої кількості даних та розширенням можливостей аналітичних систем, компанії почали все більше використовувати їх для прийняття рішень в бізнесі.

Аналітичні системи дозволяють збирати, обробляти та аналізувати великі обсяги даних, в тому числі дані про попит та пропозицію, ринок та конкурентів, фінансові показники та інші фактори, що впливають на діяльність компанії. Застосування аналітичних систем дозволяє компаніям розуміти свій бізнес, виявляти тенденції та прогнозувати результати, а також приймати обґрунтовані та ефективні рішення.

Окрім того, використання аналітичних систем є необхідністю для компаній в умовах надзвичайної конкуренції та швидкісного розвитку технологій. Компанії, які не використовують аналітичні системи, можуть втратити конкурентну перевагу та не мати можливості адаптуватися до змін на ринку та в своїй галузі. Таким чином, тема є надзвичайно актуальною, оскільки використання аналітичних систем є ключовим фактором успіху для компаній в сучасному світі.

Метою статті є розгляд основних аспектів використання аналітичних систем у бізнесі та їх вплив на процес прийняття рішень. Стаття має допомогти зрозуміти, як аналітичні системи можуть допомогти вдосконалити процес прийняття рішень в компанії, які переваги та проблеми пов'язані з використанням таких систем, а також як вибрати та впровадити аналітичну систему в практичну діяльність бізнесу. Метою статті є також зробити свій внесок у розвиток та популяризацію використання аналітичних систем у сфері бізнесу.

Об'єктом дослідження э розробка аналітичної системи для впливу на процес прийняття рішень в бізнесі.

Предметом дослідження є аналітичні системи.

Аналіз попередніх досліджень показав, що використання аналітичних систем в бізнесі може мати значний вплив на процес прийняття рішень. Наприклад, за дослідженнями McKinsey, компанії, які активно використовують аналітичні системи, мають в 2,6 рази більшу вірогідність досягнути високих показників фінансової ефективності, ніж ті, що не використовують такі системи. Дослідники також відзначають, що аналітичні системи можуть допомогти бізнесу збільшити ефективність процесів, знизити витрати і покращити якість продуктів та послуг. Крім того, вони можуть допомогти виявити нові можливості для зростання та розширення бізнесу, зокрема шляхом аналізу ринку та відстеження поведінки споживачів. Однак, дослідження також показали, що успіх використання аналітичних систем залежить від багатьох факторів, включаючи якість даних, адекватність моделей, які використовуються для аналізу даних, та належну інтеграцію систем в бізнес-процеси. Також важливо, щоб співробітники компанії були готові до використання аналітичних систем та мали необхідні знання та навички для їх використання.

Виклад основного матеріалу. Впровадження аналітичних систем в бізнесі значно змінило процес прийняття рішень. Раніше рішення приймалися на основі інтуїції, досвіду та зібраних даних. Завдяки аналітичним системам, бізнес може опиратися на більш об'єктивні дані та аналітику, що дозволяє приймати рішення на основі фактів, а не припущень. В сучасних умовах аналітичну систему можна представити таким чином (рис. 1):

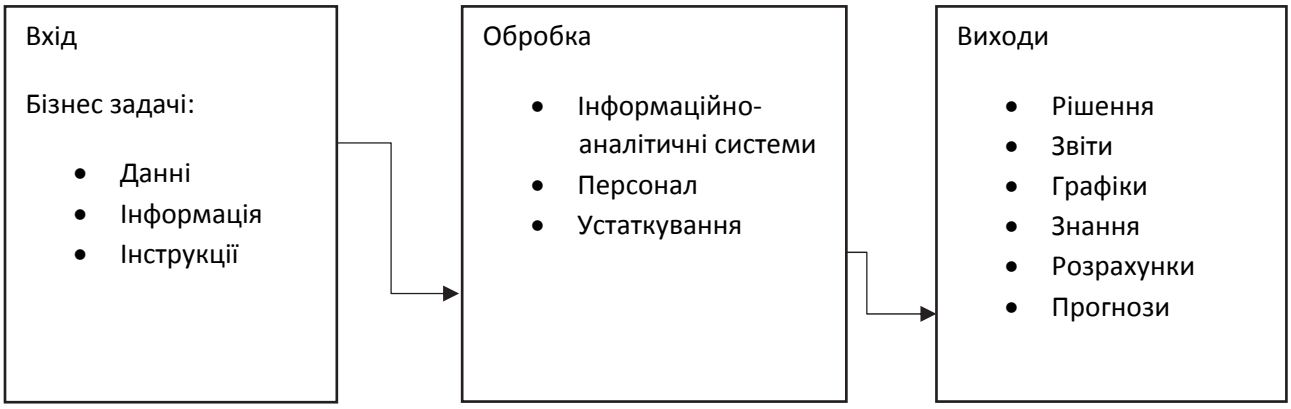


Рис. 1. Аналітична система

Процес управління в аналітичних системах можна поділити на три основні етапи: вхідні дані, обробка і аналіз даних, і вихідні дані. Кожен з цих етапів має свої особливості:

- Вхідні дані. На цьому етапі збираються та введені дані, які використовуються в аналітичній системі. Ці дані можуть бути зібрані з різних джерел, таких як бази даних, веб-сайти, соціальні мережі, сенсори тощо. Для забезпечення якості та достовірності даних, можуть використовуватися різноманітні методи валідації та очистки даних.
- Обробка і аналіз даних. Після отримання інформації проводиться обробка та аналіз вхідних даних. Для цього використовуються різні методи та техніки, такі як статистичний аналіз, машинне навчання, нейронні мережі тощо. Основною метою цього етапу є виявлення залежностей та патернів в даних, що може допомогти в розумінні тенденцій та прогнозуванні майбутніх подій.
- Вихідні дані. Коли данні отримані і обробленні виконується візуалізація та передача отриманих результатів користувачам. Для цього можуть використовуватися різні методи та інструменти, такі як дашборди, звіти, графіки тощо. Користувачі можуть використовувати ці дані для прийняття рішень або для подальшого аналізу.

Після того, як дані були оброблені і проаналізовані, результати можуть бути відображені у вигляді звітів, дашбордів або інших візуальних інтерфейсів. Це дозволяє користувачам легко зрозуміти результати і прийняти правильні рішення. Управління зазвичай здійснюється через інтерфейс користувача, який дозволяє налаштувати параметри аналізу та моніторингу [1]. Це може включати в себе налаштування прав доступу для різних користувачів, налаштування різних видів звітів та дашбордів, а також налаштування різних показників та метрик для аналізу.

Розвиток аналітичних систем дозволяє компаніям збільшувати швидкість та точність процесу прийняття рішень. Замість інтуїтивного підходу, керівництво компанії отримує об’єктивні дані, на основі яких можна зробити правильний висновок. Однак, важливо не забувати, що вони не є універсальним рішенням на всі випадки, тому досвід та інтуїція керівництва також залишаються важливими факторами в процесі прийняття рішень.

В бізнес плануванні системи для аналізу даних допомагають як для крупних компаній так і для середніх або малих. Для крупних компаній використовуються складні аналітичні системи, які дозволяють обробляти великі обсяги даних та робити прогнози щодо подальшого розвитку бізнесу. Один з прикладів такої системи що використовуються у крупних компаній – SAP BusinessObjects, яка надає інструменти для збору та аналізу даних з різних джерел, зокрема з баз даних, електронної пошти, соціальних мереж тощо. Вона дозволяє створювати звіти та графіки, які відображають стан бізнесу та його поточні та прогнозовані результати (рис. 2).

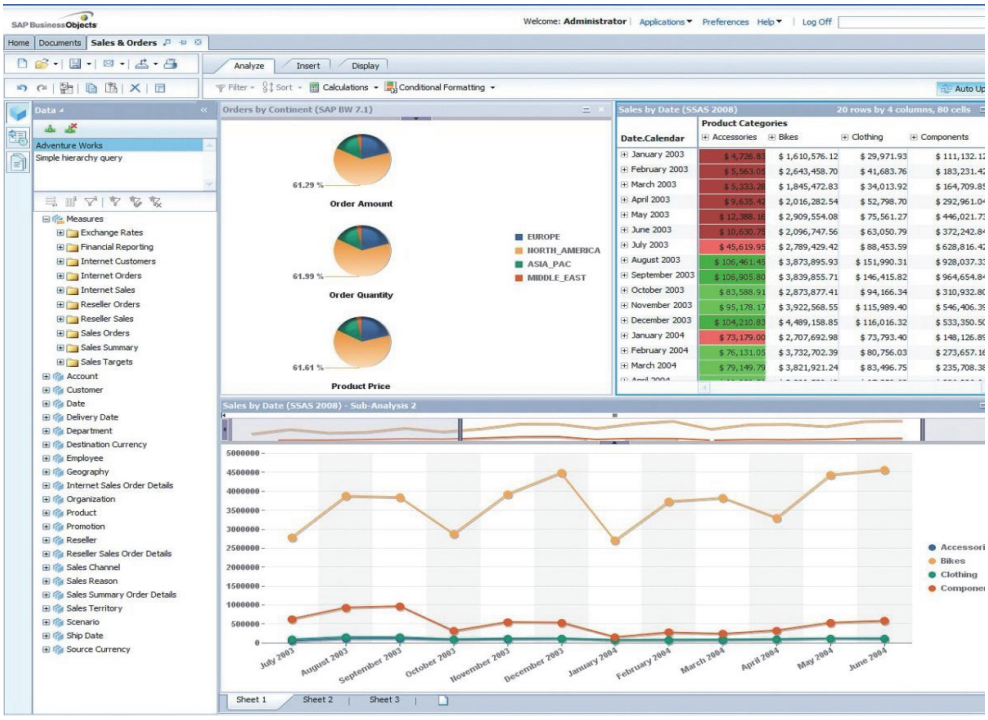


Рис. 2. Sap BusinessObjects інтерфейс програми з вхідними даними, графіками, та діаграмами після обробки даних

SAP BusinessObjects є однією з найбільш популярних аналітичних систем у бізнесі. Вона надає користувачам широкі можливості для збору, аналізу та візуалізації даних[2]. SAP BusinessObjects використовується в багатьох крупних компаніях, таких як Coca-Cola, Nestle та Procter & Gamble.

У компанії Coca-Cola SAP BusinessObjects використовується для підтримки процесу прийняття рішень та для виконання аналітики даних. Завдяки SAP BusinessObjects аналітики компанії можуть швидко та ефективно аналізувати великі обсяги даних і знаходити тенденції та взаємозв'язки між ними. Компанія також використовує SAP BusinessObjects для підтримки внутрішнього звітності та для автоматизації процесів збору та аналізу даних. У Nestle SAP BusinessObjects використовується для підтримки процесу планування ресурсів підприємства (ERP). Система допомагає спростити та автоматизувати процеси збору та аналізу даних, що дозволяє компанії зосередитися на стратегічних питаннях та підвищенні ефективності бізнесу. SAP BusinessObjects також допомагає Nestle виявляти проблемні зони у процесах виробництва та управління запасами, що дозволяє компанії швидко реагувати на проблеми та покращувати ефективність. У Procter & Gamble SAP BusinessObjects використовується для підтримки процесу прийняття рішень та для виконання аналізу даних. Система дозволяє компанії ефективно збирати та аналізувати дані з різних джерел, що допомагає у прийнятті рішень на основі фактичних даних.

Крім того, SAP BusinessObjects може бути використана для розробки та виконання різних звітів та аналітичних досліджень, таких як аналіз фінансових показників, відстеження витрат на проектах та моніторинг виконання бізнес-планів. Завдяки вбудованій системі Business Intelligence (BI) можливість візуалізації даних у вигляді графіків, діаграм та інших візуальних засобів, що полегшує сприйняття та аналіз отриманих даних. Система може інтегруватися з різноманітними джерелами даних, такими як бази даних, Excel-файли та інші програмні продукти, що дозволяє отримувати доступ до необхідних даних та інформації безпосередньо з одного місця.

Важливою функцією SAP BusinessObjects є можливість створення панелей керування (dashboards), які дають змогу отримати швидкий огляд найважливіших показників та метрик, що дозволяє швидко реагувати на зміни та приймати вчасні рішення. Також слід зазначити,

що SAP BusinessObjects може бути налаштована для різних відділів та функціональних областей, що дозволяє компаніям використовувати систему для вирішення різноманітних завдань та задач. Наприклад, система може бути використана для моніторингу продажів, відстеження витрат на виробництві, аналізу даних про клієнтів та багато іншого.

Однією з кращих програмних забезпечень слід зазначити про Oracle Business Intelligence (рис. 3).

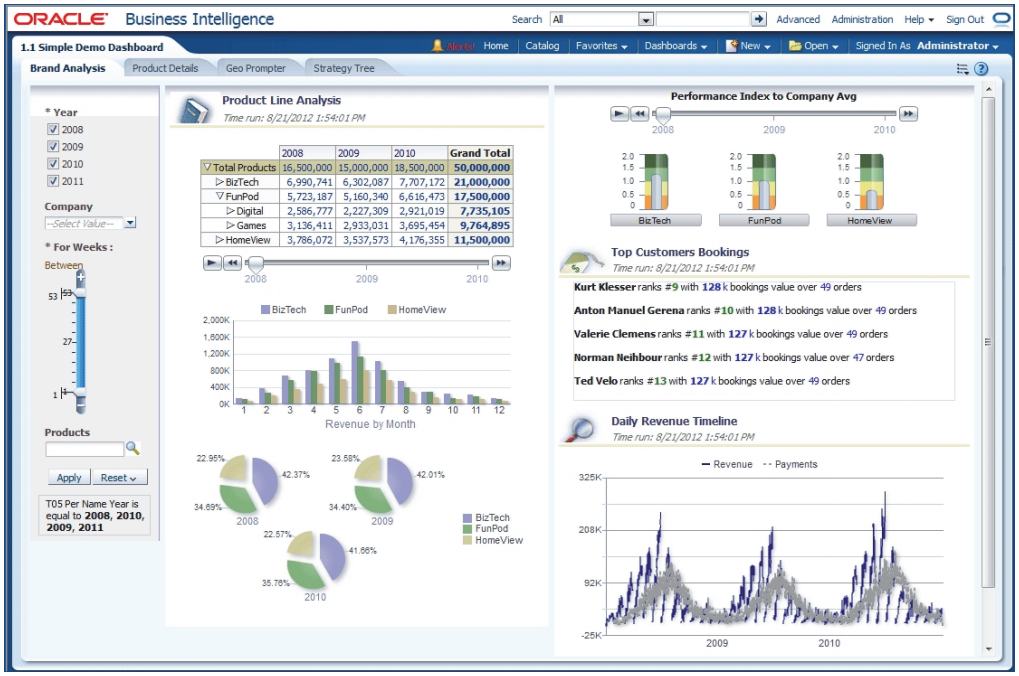


Рис. 3. Інтерфейс звітів Oracle Business Intelligence

Oracle Business Intelligence (OBI) – це повний комплекс рішень для аналітики даних та бізнес-інтелекту, який розробляється компанією Oracle. Ця система надає користувачам різноманітні можливості для створення звітів, аналізу даних та взаємодії з ними в режимі реального часу. Программа складається з таких компонентів, як Oracle BI Server, Oracle BI Answers, Oracle BI Publisher та Oracle BI Interactive Dashboards. Всі ці компоненти взаємодіють між собою, забезпечуючи зручний та ефективний інтерфейс для користувачів.

Один з головних компонентів це Oracle BI Server, який надає доступ до даних з різних джерел, таких як бази даних, файли, веб-сервіси тощо. Сервер забезпечує зручний та швидкий доступ до даних незалежно від їх формату та розміру. Крім того, BI Server надає можливості для створення зв'язків між різними джерелами даних, що дозволяє користувачам аналізувати дані з різних джерел в єдиному інтерфейсі.

Oracle BI Answers представляє собою інтерактивну систему аналізу даних, яка дозволяє користувачам створювати запити до даних, використовуючи візуальний інтерфейс та шаблони запитів. Запити можуть бути збережені та використовуватись для подальшого аналізу даних.

Oracle BI Publisher – це інструмент для створення та розповсюдження звітів. Він дозволяє користувачам створювати звіти в різних форматах, таких як PDF, Excel та HTML, та розповсюджувати їх з максимальною ефективністю.

Oracle BI Interactive Dashboards є однією з ключових компонентів Oracle Business Intelligence. Це інтерактивне веб-додаток, який дозволяє користувачам здійснювати аналіз даних в режимі реального часу та створювати інформаційні панелі з необхідною для них інформацією. Він дозволяє використовувати графіки, таблиці, діаграми та інші візуалізації для представлення даних. Користувачі можуть легко переглядати та порівнювати дані, а також здійснювати фільтрацію та пошук інформації за допомогою вбудованих функцій.

Oracle BI Interactive Dashboards також дозволяє використовувати інтерактивні заходи для взаємодії з даними, наприклад, можна здійснювати вибір певних елементів на діаграмі для фільтрації даних в інших частинах інформаційної панелі. Крім того, користувачі можуть експортувати дані з Oracle BI Interactive Dashboards у формати Excel або PDF, що дозволяє зберігати та обмінюватися даними з колегами. Программа також має вбудований функціонал для роботи з безпекою та доступом до даних. Адміністратори можуть налаштовувати рівні доступу до інформації для різних користувачів, груп та ролей. Це дозволяє забезпечити безпеку даних та контролювати доступ до конфіденційної інформації.

Щодо малих та середніх підприємств, часто використовуються простіші аналітичні системи, які дозволяють вести облік продажів, складу та виробництва, а також аналізувати фінансову діяльність. Один з прикладів – QuickBooks (рис. 4), який дозволяє вести бухгалтерський облік, створювати звіти та аналізувати фінансові показники бізнесу[3].

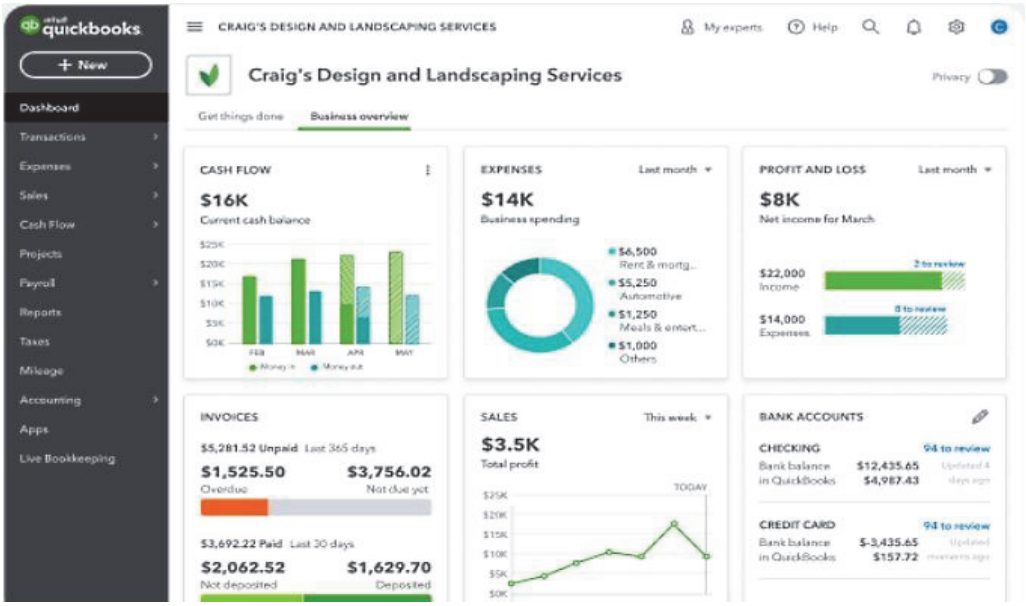


Рис. 4. QuickBooks інтерфейс програми, графіки та звіти

Основні можливості QuickBooks включають:

- Облік рахунків і платежів: в програмі можна створювати та зберігати інформацію про рахунки клієнтів, постачальників та платежі за них. Можна також додавати оплати та надходження коштів, що спрощує процес взаємодії з контрагентами.
- Операції з банківськими рахунками: програма дозволяє створювати рахунки та відслідковувати операції з банківськими рахунками, включаючи поповнення та виведення коштів.
- Створення звітів: QuickBooks має вбудовані засоби для створення звітів про фінансову діяльність компанії, таких як баланс, звіт про прибутки та збитки, звіт про заборгованості тощо. Звіти можна створювати як за певний період часу, так і за конкретний проект або контрагента.
- Інтеграція з іншими програмними засобами: QuickBooks може інтегруватись з іншими програмними засобами, такими як PayPal, Shopify, Amazon тощо, що дозволяє автоматизувати процеси продажу та звітності.

У загальному, QuickBooks допомагає компаніям ефективно керувати фінансовою діяльністю, складом, проектами та клієнтами, що є особливо важливим для малих та середніх підприємств, які не можуть дозволити собі велику бухгалтерську та фінансову команду.

Крім того, існують спеціалізовані аналітичні системи для різних галузей, наприклад, для логістики, маркетингу, ресторанного бізнесу тощо. Наприклад, у ресторанному бізнесі

може використовуватися Toast, який дозволяє вести облік продажів, керувати запасами та персоналом, а також аналізувати відвідуваність та задоволеність клієнтів [4]. Варто відзначити, що у бізнесі можуть використовуватися не тільки готові аналітичні системи, але й спеціально розроблені інструменти, які відповідають потребам конкретної компанії та її галузі.

Висновки. Аналітичні системи є незамінним інструментом для прийняття рішень в бізнесі. Проте, як і будь-який інструмент, вони мають свої переваги та недоліки.

Переваги таких систем включають:

- Підвищення ефективності та продуктивності: аналітичні системи дозволяють бізнес-лідерам отримати доступ до точних даних та статистичної інформації, що забезпечує зростання ефективності та продуктивності в діяльності компанії.
- Збільшення точності прийнятих рішень: аналітичні системи допомагають компаніям приймати рішення на основі даних, що забезпечує більш точне та обґрунтоване прийняття рішень.
- Покращення стратегічного планування: аналітичні системи дозволяють компаніям отримувати значну кількість даних, які можна використовувати для планування та розробки стратегій.
- Отримання конкурентної переваги: за допомогою аналітичних систем компанії можуть аналізувати діяльність своїх конкурентів та знаходити нові можливості для покращення власної продуктивності.

До негативних аспектів відносяться такі пункти:

- Висока вартість: впровадження та підтримка аналітичних систем можуть бути витратними для компаній.
- Складність впровадження: впровадження аналітичних систем може бути складним та вимагати значних зусиль з боку IT-команди.
- Недостатність якісних даних: якість даних може впливати на якість прийнятих рішень. Якщо дані не є достатньо точними, то результати аналітичних систем можуть бути неправильними.

Отже, прийняття рішень на основі аналітичних систем має свої переваги та недоліки. Щоб максимально використовувати переваги аналітики та зменшувати ризики недоліків, важливо ретельно планувати та розробляти відповідну стратегію, залучати експертів та забезпечувати необхідну підготовку персоналу.

Список використаних джерел

1. Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. MIS Quarterly, 36(4), 1165-1188.
2. Srivastava, D., & Saxena, S. (2018). Business Intelligence: Concepts, Methodologies, Tools, and Applications. IGI Global.
3. Turban, E., Sharda, R., & Delen, D. (2019). Decision Support and Business Intelligence Systems. Pearson.
4. Kimball, R., Ross, M., Thornthwaite, W., Mundy, J., Becker, B., & Thornthwaite III, W. (2013). The Kimball Group Reader: Relentlessly Practical Tools for Data Warehousing and Business Intelligence. Wiley.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ХАРЧЕНКА О. А.

МЕНЕДЖЕР ПАРОЛІВ ТА ЙОГО РІЗНОВИДИ

МИРОВЕЦЬ М., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

Менеджери паролів – це інструменти, які допомагають користувачам створювати, зберігати та керувати складними та унікальними паролями для їхніх різноманітних облікових записів в Інтернеті. Таким чином, вони відіграють вирішальну роль у підвищенні онлайн-безпеки та запобіганні кібератакам. Одним з важливих аспектів менеджерів паролів є механізм обміну даними, який дозволяє їм обмінюватися даними користувача між пристроями та програмами.

Password managers are tools that help users generate, store, and manage complex and unique passwords for their various online accounts. As such, they play a critical role in enhancing online security and preventing cyberattacks. One essential aspect of password managers is the data exchange mechanism that allows them to share user data between devices and applications.

Актуальність. Більшість людей ненавидять реєструвати облікові записи, а тим більше створювати паролі. Це може бути причиною, чому вони повторно використовують їх кілька разів під час створення облікових записів.

Однак зараз 2023 рік, і рішення є. Одним із них можуть бути менеджери паролів. З ними ви можете створювати складні паролі та зберігати їх.

Менеджер паролів – це програма, яка дозволяє створювати та зберігати всі ваші паролі в безпечному місці. Більшість із них дозволяють також зберігати дані кредитної картки, а також безпечні нотатки. Для ще більшої безпеки та зручності менеджери паролів також підтримують використання біометричних даних (відбитків пальців або обличчя) замість головного пароля для ще більшої безпеки та зручності.

Паролі необхідні для захисту ваших облікових записів, але вони також можуть дратувати. Автономний менеджер паролів може зробити це безпечнішим і менш виснажливим.

Для більшості інструментів керування паролями користувачу потрібно лише ввести головний пароль, щоб розшифрувати секретні сховища. Це, звичайно, краще, ніж мати справу з десятками і десятками паролів.

Коли ви створюєте новий елемент у менеджері паролів, ви можете створити випадковий пароль. Ці машинно створені рядки складні та довгі з різними типами символів, тому їх практично неможливо вгадати.

Синхронізація є стандартною частиною менеджерів паролів . Ви можете працювати на робочому столі Windows і використовувати телефони iPhone і Android – це не має значення. Усі ваші паролі можуть бути синхронізовані та ідентичні незалежно від того, який пристрій ви використовуєте.

Метою статті є дослідження та класифікація менеджерів паролів, а також їх типи.

Об'єктом дослідження є розробка програмного забезпечення обміну даними між менеджерами паролів.

Предмет дослідження – менеджери паролів.

Аналіз попередніх досліджень. Дослідженню менеджерів паролів присвячені праці наступних науковців: Karen Scarfone(Карен Скарфон), Murugiah Souppaya(Муругія Суппая), Shirley Gaw(), Edward W. Felten(Едвард В. Фелтен), Sruthi Anand (Шруті Ананда), Dr.N. Susila1 (доктор Н. Сусіла), Dr.S. Balakrishnan (доктор С. Балакрішнан) та інші.

Виклад основного матеріалу. На перший погляд здається, що користуватися таким менеджером просто, але все одно треба розуміти принцип його роботи. На рис. 1 показано принцип роботи такого менеджеру.

Рис. 1. Принцип роботи менеджера паролів

Менеджер паролів – це невелике сховище (зазвичай база даних), яке зберігає всі ваші облікові дані та паролі (зашифровані) і зазвичай захищене головним паролем або біометричними даними, іноді з додатковим захистом автентифікації, наприклад двоетапною або багатофакторною автентифікацією (MFA). . У більшості конфігурацій, на жаль, додатковий захист автентифікації вимкнено за замовчуванням і має бути увімкнений користувачем.

Зазвичай можна створити кілька сховищ, кожне з яких захищено головним паролем. Найпоширенішим способом створення нових записів у сховищі є розширення браузера. Потім, коли ви вводите інформацію в поле імені користувача та пароля у веб-формі, розширення запропонує зберегти ці облікові дані в сховищі. Після цього поля можуть автоматично заповнюватися під час наступного переходу на той самий веб-сайт.

Сховище можна синхронізувати між кількома пристроями, забезпечуючи вам легкий спосіб заповнити ім'я користувача та пароль у веб-формах без необхідності запам'ятовувати пароль або вводити його безпосередньо. Менеджер паролів допомагає створювати надійні паролі для кожного облікового запису та перевіряти надійність ваших унікальних паролів.

Деякі версії менеджерів паролів дозволяють ділитися обліковими даними з членами родини.

Що робить особисті менеджери паролів привабливими для споживачів, так це те, що багато базових програм менеджерів паролів пропонують безкоштовні версії, хоча й з обмеженими можливостями. Коли ви досягаєте ліміту пароля або вам потрібні додаткові функції, як-от можливість синхронізації між кількома пристроями, потрібно платити, і що більше функцій вам потрібно, то вища ціна.

У менеджерів паролів є свої сильні сторони. За допомогою менеджерів паролів паролі шифруються, і їх можна розшифрувати, лише якщо отримати доступ до них із створеним користувачем головним паролем. Більшість менеджерів паролів зберігають облікові дані, які використовуються для доступу до кількох облікових записів і програм: ім'я користувача, пароль, назву програми, URL-адресу веб-сайту або IP-адресу системи. Їх можна встановити локально, отримати доступ у хмарі або через мобільні програми. І вони створені для створення довгих складних паролів і автоматичного заповнення пароля в правильному полі, тому людям не потрібно вручну вводити його або вирізати та вставляти [1].

Але давайте задамося питанням, чи є менеджери паролів кращими, ніж створення власних паролів і їх запис?

Для особи, яка хоче захистити особисті паролі, використання менеджера паролів може бути прийнятним. Це, безперечно, краще, ніж паролі, написані на листочках, приклеєних до монітора чи під клавіатурою, збережених у електронних таблицях Excel чи Google-документах або збережених у вигляді звичайного тексту за допомогою плагіна браузера.

Але чи є сенс використовувати один із цих персональних менеджерів паролів для захисту корпоративних паролів?

Якщо ваші цілі – безпека та ефективність підприємства, менеджерів паролів недостатньо. Для компаній перевагу надається рішенням керування привілейованим доступом (Privileged Access Management, або PAM) з причин, які виходять далеко за межі безпеки.

Керування привілейованим доступом – це категорія кібербезпеки, яка стосується того, хто може отримати доступ до привілейованого облікового запису та що вони можуть робити після входу в мережу вашої організації за допомогою цього привілейованого облікового запису. За даними Gartner Research, це один із головних пріоритетів безпеки для зменшення ризику кібератак.

Уніфікований підхід до корпоративного керування паролями за допомогою PAM корпоративного рівня безпечніший і ефективніший, ніж тисячі відключених персональних менеджерів паролів.

Керування привілейованим доступом є більш надійним рішенням безпеки, ніж менеджери паролів. Шукайте рішення PAM, яке пропонує такі функції:

- Висока доступність
- Контроль відповідності та нормативної безпеки
- Автоматичне виявлення привілейованого облікового запису
- Можливість налаштування робочих процесів підтвердження доступу
- Інтеграція з такими корпоративними рішеннями, як ITSM, IGA (керування ідентифікацією та адміністрування) і SIEM (інформація про безпеку та керування подіями)
- Можливість масштабувати бізнес
- Автоматична ротація паролів
- Аудит і звітність щодо використання пароля та безпеки
- Послідовний контроль безпеки

Організації використовують програмне забезпечення PAM, щоб контролювати, хто може використовувати привілейований обліковий запис або отримувати доступ до конфіденційної інформації з можливістю коригувати дозволи та змінювати або видаляти важливі дані. Вони розглядають привілейований обліковий запис як об'єкт, який захищається, обмежуючи розголошення пароля та спільний доступ, надаючи при цьому обмежений за часом доступ до критичних систем. Коли пароль більше не потрібен, він змінюється або термін дії закінчується, тому співробітники та треті сторони не можуть продовжувати отримувати доступ до конфіденційної інформації зі старим паролем.

Менеджери паролів вимагають, щоб окремі користувачі налаштували, підтримували та завжди використовували додаток. Користувач бере на себе всю відповідальність за підтримку технології в актуальному стані та її належне функціонування.

За допомогою LastPass, KeePass, Dashlane та інших персональних менеджерів паролів користувач несе відповідальність за безпеку паролів. Вони повинні виконати важку роботу з налаштування, ротації паролів і, що найважливіше, переконатися, що сховище паролів використовується постійно.

Завдяки корпоративному PAM-рішенню IT-команда бере на себе відповідальність за технологію захисту корпоративних паролів. Вони роблять роботу, щоб розпочати й підтримувати її.

Менеджери паролів – це охоронці вашого онлайн-світу. Вони захищають ваші облікові записи від зловмисників, генеруючи та запам'ятовуючи надійні унікальні паролі для ваших облікових записів. У той час як деякі зосереджені лише на захисті ваших паролів, деякі виходять за межі, щоб надати вам додаткову гнучкість.

Про деякі з різних типів ми зараз поговоримо:

1. Хмарні менеджери паролів.

Це один із найпопулярніших варіантів для приватних осіб і компаній. Хмарні менеджери паролів шифрують ваші паролі та інші конфіденційні дані та зберігають їх на власних серверах. Основною перевагою хмарного менеджера паролів є легкість доступу з будь-якої точки світу за допомогою будь-якого комп'ютерного пристрою. Основі можливості хмарного менеджера паролів:

- служба централізовано розміщена та підтримується постачальником послуг, тому їх можна розгорнути та отримати доступ до них миттєво;
- модель на основі передплати потребує менших початкових витрат;
- можна збільшити або зменшити відповідно до зростання команди;
- Безпека даних користувача безпосередньо залежить від вибору постачальника послуг.

2. Локальні менеджери паролів.

Локальні менеджери паролів зазвичай віддають перевагу окремим особам і компаніям, які бажають розмістити та керувати менеджером паролів у власному закритому середовищі. Зазвичай вони пропонують функції керування паролями, подібні до хмарного менеджера паролів, але вони дорожчі й зазвичай використовуються підприємствами, які мають доступ до ресурсів і фінансів для підтримки власної інфраструктури. Можливості локальних менеджерів паролів:

- розміщується та обслуговується приватно, щоб уникнути зовнішніх загроз;
- корисно для команд, яким потрібен доступ до паролів навіть за відсутності стабільного підключення до Інтернету;
- вищі початкові витрати;
- додаткові накладні витрати, пов'язані з обслуговуванням, розгортанням і оновленням інфраструктури;
- довший час впровадження, оскільки рішення потрібно розгортати вручну.

3. Мобільні менеджери паролів.

Хоча для мобільних пристроїв доступно багато хмарних програм для керування паролями, iOS і Android пропонують власні менеджери паролів, такі як Apple Keychain і Google Password Manager, що дозволяє користувачам безпечно зберігати паролі на своїх мобільних пристроях. Вони також допомагають, автоматично заповнюючи паролі на веб-сайтах і в мобільних додатках. Можливості мобільних менеджерів паролів:

- легко почати;
- миттєвий доступ до паролів з будь-якої точки світу;
- безкоштовно (входить у вартість мобільного пристрою);
- обмежено для особистого використання через відсутність широких функцій;

- Паролі не можна синхронізувати між пристроями, що працюють на різних платформах.

4. Браузерні менеджери паролів.

Такі популярні браузери, як Chrome, Safari, Firefox і Edge, пропонують вбудовані менеджери паролів, які допомагають користувачам зберігати та керувати своїми паролями. Паролі, збережені в цих менеджерах паролів, можна синхронізувати між пристроями, які підтримують ці браузери.

- Легко розпочати та керувати;
- Підтримує автоматичне заповнення пароля та автоматично зберігає нові облікові дані облікового запису;
- Безкоштовно;
- Обмежено для особистого використання через відсутність широких функцій;
- Паролі не можна синхронізувати в різних браузерах;
- Небезпечно на спільних пристроях, на яких кілька користувачів мають доступ до браузерів.

Тепер постає питання, який тип менеджера паролів вибрати?

Пристойний менеджер паролів повинен перш за все мати необмежену пам’ять для облікових даних і бути доступним принаймні для основних платформ Windows, macOS, Android та iOS. А оскільки дані передаватимуться між пристроями, вибраний менеджер паролів має переважно шифрувати дані на локальному рівні, оскільки це гарантує, що ваші дані стануть незрозумілими для потенційних хакерів до того, як вони потраплять у хмару або щоразу, коли вони будуть викликані як частина надбудови браузера.

Вибір найкращого менеджера паролів для ваших потреб залежить від кількох факторів. Наприклад, краще використовувати вбудований у пристрій або браузер менеджер паролів, а не використовувати жодного. Однак ви повинні пам’ятати, що вони обмежені та пропонують значно меншу цінність порівняно з безкоштовним хмарним менеджером паролів.

Через постійно зростаючу кількість спроб злому та постійні витоки даних за участю таких великих компаній, як Google, користувачі Інтернету приділяють усе більше уваги збереженню облікових даних облікового запису якомога безпечнішими, використовуючи надійні паролі. Однак запам’ятати десятки, якщо не сотні різних логінів для кожного облікового запису неможливо з людської точки зору, особливо якщо вони настільки складні, як це необхідно для належної безпеки. Менеджери паролів допомагають згадати будь-які дані для входу , серед іншого, але оскільки їхні найважливіші функції в основному однакові, вибрати правильне програмне забезпечення може бути важко навіть для найбільш поінформованих користувачів.

Однак завдяки паралельним порівнянням прийняти таке рішення буде так само легко, як і використовувати саме вибране програмне забезпечення. У таблиці 1 продемонстровані найвідоміші менеджери паролів та їх переваги один над одним.

Таблиця 1

Порівняльна характеристика менеджерів паролів

Основні риси	Lastpass	Dashlane	1Password
Спеціальні поля	НІ	НІ	ТАК
Користувацькі шаблони	ТАК	НІ	НІ
Безкоштовні запрошення клієнтів	НІ	НІ	НІ
Розширення для браузера	ТАК	ТАК	ТАК
Генератор паролів	ТАК	ТАК	ТАК
Сховище	НІ	1ГБ	1ГБ/на користувача
Імпорт даних	ТАК	ТАК	ТАК

Пропоную також поговорити про ризики використання менеджера паролів.

Немає способу залишатися в безпеці на 100 % в Інтернеті. Навіть якщо ви використовуєте надійний менеджер паролів, вам слід знати про певні ризики:

1. Усі конфіденційні дані в одному місці.

Ви, мабуть, чули, що більшість людей робить так само. Це саме те, що ви будете робити з менеджером паролів. Ця інформація, ймовірно, також включатиме дані кредитної картки та безпечні нотатки. У разі зламу блокування всіх варіантів оплати та зміна паролів для всіх облікових записів може зайняти достатньо часу, щоб зловмисник завдав шкоди.

2. Резервне копіювання не завжди можливо .

Якщо сервер виходить з ладу, ваша єдина надія – це те, що ваш провайдер зробив резервну копію. Цей ризик зростає в рази, якщо ви вирішите залишити своє сховище в автономному режимі на одному зі своїх пристроїв. Природно, збереження власної резервної копії на незахищеному диску або погано захищеному хмарному сервісі також не допоможе.

3. Не всі пристрої достатньо безпечні.

Хакери використовують ту саму вразливість, щоб отримати всі ваші логіни за одну атаку. Менеджери паролів можуть бути зламані, якщо ваш пристрій інфікований шкідливим програмним забезпеченням . У цьому випадку, якщо ввести головний пароль, він буде записаний, і кіберзлочинці отримають повний доступ до збережених даних. Ось чому користувачам менеджера паролів слід інвестувати в надійний антивірус , який спочатку захистить усі їхні пристрої та зменшить ризики.

4. Не використовує біометричну автентифікацію.

Біометрична автентифікація – це чудовий спосіб підвищити рівень безпеки. Якщо ви налаштуєте свій менеджер паролів на запит відбитків пальців або сканування обличчя, шанси на те, що хтось уразить ваше сховище, стануть незначними.

5. Поганий менеджер паролів.

Якщо він має слабше шифрування, пропонує мало функцій і має погані відгуки, вам не слід його використовувати. Коли мова заходить про безпеку вашого сховища, економія кількох доларів на місяць не повинна бути вашим головним пріоритетом. Це особливо вірно для безкоштовних менеджерів паролів, які часто не мають необхідних функцій безпеки для ефективного захисту ваших облікових даних у будь-який час.

6. Забули головний пароль.

Ви єдина людина, яка це знала, і ваш менеджер паролів не має функції скидання? У цьому випадку ви вже можете розпочати відновлення кожного входу один за одним. Крім того, ви можете зберегти свій головний пароль (або підказку) у фізично безпечному місці [3].

Висновки. Порівняно з альтернативою, яка передбачає запам’ятовування всього або записування облікових даних на наліпках, менеджери паролів є кращим вибором.

Це простий спосіб захистити ваші облікові записи від поширених онлайн-загроз. Усиновлення спочатку може бути дивним і громіздким. Але в цілому менеджер паролів може покращити вашу цифрову безпеку в усіх аспектах.

Список використаних джерел

1. Usability, security and trust in password managers: A quest for user-centric properties and features \\ Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S1574013718302533 (останнє звернення 17.03.2023 р.)
2. The Emperor’s New Password Manager: Security Analysis of Web-based Password Managers \\ Режим доступу: https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-li-zhiwei.pdf (останнє звернення 23.03.2023 р.)
3. Why people (don’t) use password managers effectively \\ Режим доступу: https://www.usenix.org/system/files/soups2019-pearman.pdf (останнє звернення 27.03.2023 р.)

Робота виконана під науковим керівництвом старшого викладача
ШЕСТАКА Я. І.

ПІДХОДИ ДО ПРОЄКТУВАННЯ ТА РОЗРОБКИ ПРОГРАМНИХ ПЛАТФОРМ ЕЛЕКТРОННИХ РИНКІВ

МІРКО І., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади щодо проектування та розробки платформ е-торгівлі як програмного продукту. Розглянуто як зразок архітектуру програмної компоненти e-Market places.

The article discusses the basic principles of designing and developing software platforms of electronic markets. The architecture of the software component is considered as an example e-Market places.

Актуальність. Із зростанням кількості електронних торгових майданчиків зростає потреба в ефективному проєктуванні та розробці програмної платформи, яка може забезпечити безперебійну, надійну та захищену роботу тандему система-користувач, а також відповідати вимогам різних бізнес-моделей.

Розробка платформ електронного ринку є складним процесом, який включає різні проблеми, такі як масштабованість, безпека та зручність використання [2; 3]. Крім того, платформи електронного ринку повинні бути розроблені для підтримки різних бізнес-моделей, таких як B2B, B2C і C2C, що може ще більше ускладнити процес розробки.

В останні роки зростає цікавість до дизайну та розробки платформ електронного ринку. В IT-сегменті було запропоновано численні підходи для вирішення різноманітних викликів, проте все ще бракує комплексних та систематизованих досліджень, які б порівнювали різні підходи проєктування, дизайну, розробки та оцінювали їх ефективність [1; 2; 3].

Метою статті є аналіз та порівняння різних підходів до проєктування та розробки платформи електронного ринку та надання оптимальних висновкіт та практичних рекомендацій для створення ефективної платформи електронного ринку.

Об'єктом дослідження є процес побудова архітектури та проєктування програмних додатків платформ електронних ринків..

Предмет дослідження – платформа е-торгівлі як програмний продукт.

Аналіз попередніх досліджень. Дослідженню архітектури ПЗ, дизайну та проєктуванню додатків, визначенню структури, основних характерних рис платформ електронного ринку присвячені праці вітчизняних та закордонних науковців: В.В. Соколова, Дж. Мартін, Н.М. Тюріна, та ін.

Виклад основного матеріалу.

Платформи електронних ринків стали популярним каналом для компаній, щоб охопити нових клієнтів і розширити свої ринки збуту [4]. Ці платформи є онлайн-платформами, які оптимізують транзакції між покупцями та продавцями та можуть бути класифіковані на різні типи залежно від цільових користувачів, наприклад бізнес-бізнес (B2B), бізнес-споживач (B2C) і споживач-споживач (C2C) [5]. Платформи електронного ринку також можна класифікувати залежно від їхнього масштабу, наприклад, глобальні, регіональні чи локальні [6].

В останні роки відбулося значне збільшення кількості доступних платформ електронного ринку, таких як Amazon, Alibaba та eBay [7]. Платформи електронного ринку забезпечують переваги як для покупців, так і для продавців, такі як розширення доступу до продуктів і послуг, зниження трансакційних витрат і підвищення ефективності ринку [8].

Однак проєктування та розробка платформ електронного ринку може бути складним через такі фактори, як масштабованість, безпека та зручність використання. Вирішення цих проблем вимагає ретельного планування та врахування різних факторів, таких як вибір архітектури програмного забезпечення, методології розробки та стеку технологій [9].

Загальні проблеми при проєктуванні та розвитку електронних ринків сформувались як у практиків, так і у науковців.

Зокрема, науковці визначили різні проблеми при проєктуванні та розвитку електронних ринків, які необхідно вирішити, щоб забезпечити успіх платформи. Деякі з типових проблем, з якими стикаються розробники електронного ринку, включають:

- Масштабованість: електронні ринки повинні мати можливість обробляти велику кількість користувачів і транзакцій, не відчуваючи проблем із продуктивністю [10; 12; 14].
- Безпека: електронні ринки повинні забезпечувати безпеку даних користувачів і транзакцій, щоб створити довіру та запобігти шахрайству [11; 13].
- Зручність використання: електронні ринки повинні бути розроблені з урахуванням досвіду користувачів, щоб полегшити користувачам навігацію та використання платформи [15].
- Інтероперабельність: електронні ринки повинні мати можливість інтегруватися з іншими системами та платформами для полегшення обміну даними та взаємодії [16].
- Адаптивність: електронні ринки повинні мати можливість адаптуватися до мінливих ринкових умов і мінливих потреб бізнесу [10; 11;15].

Проаналізувавши праці вчених та практиків, агрегуємо підходи до проєктування, моделювання та розробки ПЗ:

1. Монолітна архітектура: у цьому підході весь електронний ринок розробляється як єдине інтегроване ціле. Цей підхід є простим і легким у розробці, але він не може бути масштабованим або адаптованим до мінливих потреб бізнесу [1; 2; 5].
2. Архітектура мікросервісів: цей підхід передбачає поділ електронного ринку на менші незалежні сервіси, які можна розробляти та розгортати окремо. Цей підхід пропонує більшу масштабованість, адаптивність і відмовостійкість, але може потребувати більше зусиль у розробці [3; 4; 6].
3. Спеціальне програмне забезпечення: цей підхід передбачає розробку електронного ринку з нуля за допомогою спеціального коду. Цей підхід забезпечує більшу гнучкість і контроль над функціями платформи, але може потребувати більше часу та зусиль для розробки та підтримки [7].
4. Платформа як послуга (PaaS): цей підхід передбачає використання попередньо створеної платформи для розробки електронного ринку. Цей підхід пропонує більшу швидкість і легкість розробки, але він може бути менш гнучким або настроюваним [8; 9].
5. Програмне забезпечення з відкритим кодом: цей підхід передбачає використання програмного забезпечення з відкритим кодом для розробки електронного ринку. Такий підхід забезпечує більшу гнучкість і контроль над функціями платформи, але може потребувати більше зусиль у розробці [10; 11].
6. Власне програмне забезпечення: цей підхід передбачає використання власного програмного забезпечення для розробки електронного ринку. Цей підхід пропонує більшу легкість розробки та підтримки, але він може бути менш гнучким або настроюваним [12; 13].
7. Гнучка розробка програмного забезпечення: цей підхід передбачає ітераційну та поступову розробку, зосереджену на відгуках користувачів і швидкому створенні прототипів. Такий підхід забезпечує більшу адаптивність і задоволення споживачів, але може потребувати більше зусиль у розробці [14; 15].

8. Традиційна розробка програмного забезпечення: цей підхід передбачає послідовну та структуровану розробку, зосереджену на повних і остаточних вимогах. Цей підхід пропонує більший контроль і передбачуваність, але він може бути менш адаптованим до мінливих потреб бізнесу [16; 17].

Зазначимо, що вибір підходу до створення архітектури ПЗ, концептуальної моделі, дизайну ПЗ та розробки ПЗ залежить від різних факторів. Основними факторами є вимоги бізнесу, наявні ресурси та навички і обов'язково досвід команди розробників.

Обираючи шлях та інструменти моделювання, макетування та створення дизайну потрібно визначити критерії оцінки, проаналізувати та порівняти підходи.

Щоб оцінити ефективність різних підходів до комплексної побудови е-платформ потрібно застосувати критеріальний підхід, тобто розглянути кілька критеріїв. Загальноприйнятими критеріями оцінки ПЗ зазвичай є критерії, які відповідають міжнародному Стандарт ISO/IEC 9126, який визначає якість ПЗ , а саме:

1. Масштабованість і продуктивність: цей критерій оцінює здатність платформи е-торгівлі як програмного продукту справлятися зі зростаючим навантаженням користувачів і транзакцій, зберігаючи при цьому прийнятні рівні продуктивності.
2. Безпека та конфіденційність: цей критерій оцінює здатність платформи е-торгівлі як програмного продукту забезпечувати безпеку та конфіденційність даних користувачів, транзакцій та комунікацій.
3. Гнучкість і адаптивність: цей критерій оцінює здатність платформи е-торгівлі як програмного продукту адаптуватися до мінливих бізнес-потреб, можливість запроваджувати нові фічі та функції і інтегруватися з іншими системами.
4. Взаємодія з користувачем та зручність використання: цей критерій оцінює здатність платформи е-торгівлі як програмного продукту забезпечувати зручний та інтуїтивно зрозумілий інтерфейс, що забезпечує ефективне використання клієнтами та іншими зацікавленими сторонами.

Наведені вище критерії можуть допомогти оцінити та порівняти сильні та слабкі сторони різних підходів до архітектури, моделювання, макетування, дизайну та розробки е-платформи як програмного продукту. В якісь мірі можна застосувати один із найпоширеніших аналітичних методів, який дозволяє в комплексі оцінити сильні й слабкі сторони досліджуваного об'єкту, а також можливості й загрози, що впливають на неї - SWOT-аналіз.

Однак відносна важливість кожного критерію може змінюватися в залежності від конкретних потреб і пріоритетів організації. Одним з етапів життєвого циклу програмного продукту, а в нашому випадку, платформи е-торгівлі, є процес створення концептуальної моделі та архітектури додатка.

Опишемо та порівняємо монолітну архітектуру та мікросервіси. Одне з ключових рішень, яке необхідно прийняти під час проєктування та розробки електронних ринків, полягає в тому, чи прийняти монолітну архітектуру чи архітектуру мікросервісів. Монолітна архітектура передбачає розробку електронного ринку як єдиної уніфікованої програми, тоді як архітектура мікросервісів передбачає розбиття програми на менші незалежні служби, які спілкуються одна з одною [17; 18]. Монолітна архітектура має перевагу в тому, що її простіше розробити та розгорнути, оскільки вона вимагає менше компонентів і нею можна керувати як єдиним блоком. Однак це може бути складніше масштабувати та підтримувати, оскільки додаток росте та стає складнішим. З іншого боку, архітектура мікросервісів забезпечує більшу гнучкість, масштабованість і відмовостійкість, оскільки окремі сервіси можна оновлювати, замінювати або масштабувати незалежно один від одного [19; 20]. Вибір між монолітною архітектурою та архітектурою мікросервісів має ґрунтуватися на конкретних потребах і вимогах платформи е-торгівлі. Монолітна архітектура може бути більш доцільною для невеликих, менш складних програм із меншими вимогами до масштабованості та продуктивності. Архітектура мікросервісів може краще підходити для великих, складніших додатків з вищими вимогами до масштабованості та продуктивності.

Ще один важливий фактор при проєктуванні та розробці платформ е-торгівлі – використовувати програмне забезпечення з відкритим кодом чи пропрієтарне програмне забезпечення. Програмне забезпечення з відкритим вихідним кодом є у вільному доступі, і будь-хто може отримати доступ до його вихідного коду, змінити його та розповсюдити. Власницьке програмне забезпечення, з іншого боку, належить певній компанії, і його вихідний код зазвичай зберігається в таємниці [25; 26]. Програмне забезпечення з відкритим кодом пропонує кілька переваг, таких як економічна ефективність, підтримка спільноти, гнучкість і прозорість. Однак він може мати обмеження щодо безпеки, якості та сумісності з іншими системами. Власницьке програмне забезпечення, з іншого боку, пропонує більшу безпеку, якість і підтримку, але може бути дорожчим і мати обмежені можливості налаштування [27; 28].

Рішення про використання програмного забезпечення з відкритим кодом або пропрієтарного програмного забезпечення має ґрунтуватися на кількох факторах, таких як конкретні потреби та вимоги електронного ринку, наявність досвіду та підтримки, необхідний рівень безпеки та бюджет.

Наприклад сформована концептуальна модель на прикладі програмної компоненти e-Market places (рис. 1) відображає всі складові платформи.

Рис. 1. Концептуальна модель програмної компоненти e-Market places

Джерело: Розроблено автором

Відповідно для розроки архітектури ПЗ застосовується мова UML. Основною причиною використання мови UML є спілкування розробників між собою. Крім того, UML спеціально створювалася для оптимізації процесу розробки програмних систем, що дозволяє збільшити ефективність їх реалізації у кілька разів і помітно поліпшити якість кінцевого продукту.

При модифікації системи об'єктний підхід дозволяє легко включати в систему нові об'єкти і виключати застарілі без істотної зміни її життєздатності. Використання побудованої моделі при модифікаціях системи дає можливість усунути небажані наслідки змін, оскільки вони не ламають структури системи, а тільки змінюють поведінку об'єктів [5].

Приклад архітектури програмної компоненти e-Market places розробленої засобами універсальної мови моделювання UML маємо на рис. 2.

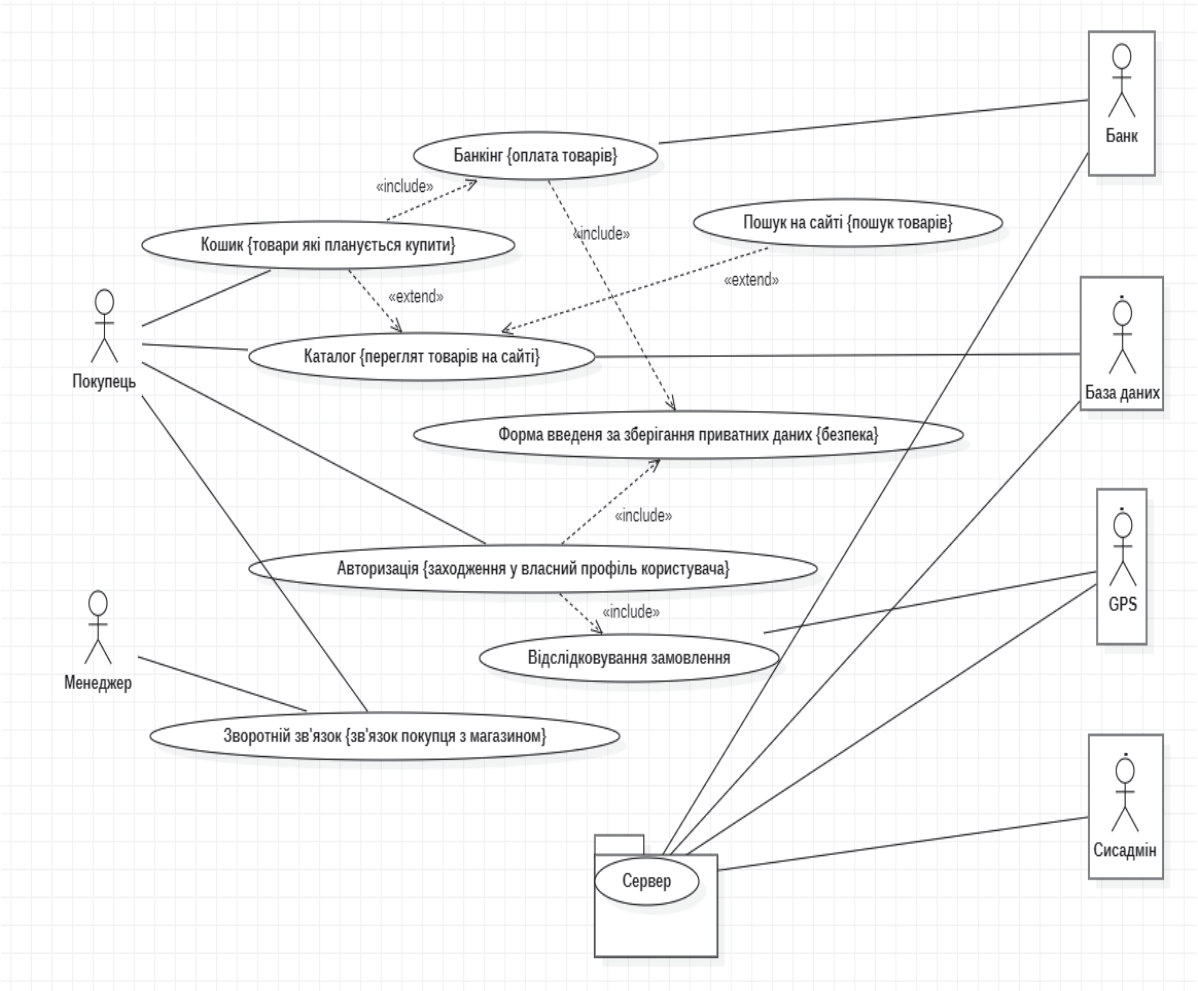


Рис. 2. USE-case програмної компоненти e-Market places

Джерело: Розроблено автором в середовищі StarUML

Висновки. Результати цього дослідження мають кілька наслідків для проєктування та розробки платформ е-торгівлі як програмного продукту. По-перше, використання архітектури мікросервісів може надати переваги з точки зору масштабованості та гнучкості. Однак необхідно ретельно розглянути складність управління та координації мікросервісів, а також запровадити відповідні інструменти та процеси, щоб забезпечити ефективну розробку, розгортання та підтримку платформ на основі мікросервісів.

Використання програмного забезпечення з відкритим вихідним кодом може надати переваги з точки зору економії коштів і внесків інвесторів, але також може вимагати більше зусиль для інтеграції та обслуговування. Слід враховувати рівень підтримки, доступний для програмного забезпечення з відкритим кодом, і досвід, необхідний для його впровадження та підтримки.

Використання гнучкої розробки програмного забезпечення може забезпечити переваги з точки зору ефективності та швидкості реагування. Однак гнучка розробка вимагає більшої координації та спілкування, і може не підійти для всіх організацій чи проєктів.

Нарешті, використання дизайну, орієнтованого на користувача, може покращити взаємодію з користувачем і зручність використання платформ е-торгівлі. Однак це вимагає більшої участі користувачів і відгуків і не завжди може відповідати бізнес-цілям платформи.

Таким чином, проєктування та розробка платформи е-торгівлі як програмного продукту вимагає ретельного розгляду різних факторів, включаючи архітектуру, технологію, методології розробки та досвід користувача. Потрібно оцінити компроміси між різними підходами та розглянути їхні конкретні вимоги та можливості.

Це дослідження дає розуміння підходів до проектування та розробки платформ електронного ринку та критеріїв їх оцінки. Однак у цій галузі ще належить провести багато досліджень. На підставі результатів цього дослідження зроблено наступні рекомендації для майбутніх досліджень:

1. Подальше дослідження компромісів між монолітною та мікросервісною архітектурами, включно з їхнім впливом на продуктивність, масштабованість і зручність обслуговування.
2. Більш поглиблені дослідження переваг і недоліків різних постачальників PaaS і їх придатності для різних типів платформ електронного ринку.
3. Подальше дослідження проблем і можливостей використання програмного забезпечення з відкритим кодом у розробці платформ електронного ринку.
4. Дослідження ефективності різних гнучких методологій розробки програмного забезпечення в контексті розробки платформи електронного ринку.
5. Більше досліджень про вплив дизайну, орієнтованого на користувача, на взаємодію з користувачем і зручність використання платформ електронного ринку, а також про те, як його можна інтегрувати з гнучкими методологіями розробки.
6. Дослідження використання штучного інтелекту та машинного навчання при проектуванні та розробці платформ електронного ринку, а також їх вплив на масштабованість, продуктивність та досвід користувача.
7. Більше досліджень про проблеми та можливості інтеграції платформ електронного ринку з іншими системами, такими як логістика та платіжні шлюзи.

Загалом ці напрямки досліджень є важливими для вдосконалення дизайну та розвитку платформ електронного ринку, а також для покращення їх масштабованості, продуктивності, безпеки, взаємодії з користувачем та зручності використання.

Список використаних джерел

1. Cao, L., & Zhang, Z. (2011). Supply chain collaboration: Impact on collaborative advantage and firm performance. Journal of Operations Management, 29(3), 163–180.
2. Gao, Q., Liu, J., & He, L. (2018). The effect of online reviews on the performance of new products. Journal of Business Research, 89, 269–280.
3. Kurnia, S., & Chien, S. W. (2017). Electronic marketplaces: A literature review and a call for supply chain management research. International Journal of Operations & Production Management, 37(1), 54–87.
4. Choudhury, M. M., & Harrigan, P. (2014). E-marketplace adoption in the global south: A comparative analysis of institutional drivers and barriers in Egypt and New Zealand. Journal of Global Information Technology Management, 17(2), 73–96.
5. Lee, J. N., & Turban, E. (2001). A trust model for consumer internet shopping. International Journal of Electronic Commerce, 6(1), 75–91.
6. Zhang, L., Xue, Y., & Huang, L. (2018). The impact of trust on sellers' performance in cross-border e-commerce platform. International Journal of Information Management, 38(1), 155–166.
7. Amazon. (nd). Отримано 23 березня 2023 року з https://www.amazon.com/
8. Liang, T. P., Ho, Y. T., Li, Y. W., & Turban, E. (2011). What drives social commerce: The role of social support and relationship quality. International Journal of Electronic Commerce, 16(2), 69–90.
9. Wang, D., & Liang, T. P. (2011). Introduction to the special issue: E-commerce trust and governance. Journal of Electronic Commerce Research, 12(4), 266–270.
10. Chen, J., Xu, Y., Li, L., & Du, R. (2018). Design and implementation of e-commerce platform based on microservice architecture. International Journal of Wireless and Mobile Computing, 14(4), 303–311.

11. Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80–89.
12. Ma, X., Ma, J., & Wang, F. (2019). Cloud computing and intelligent logistics: A review and future directions. Computers & Industrial Engineering, 136, 1–13.
13. Pani, A. K., & Mishra, D. (2021). E-commerce logistics: A comprehensive review. Journal of Industrial Integration and Management, 6(3), 1–33.
14. Sun, H., & Zhang, P. (2018). Consumer behavior in social commerce: A literature review. Decision Support Systems, 109, 27–39.
15. Wang, Y., Wang, T., & Zhang, D. (2019). Exploring factors that influence the continuous use of mobile commerce apps: A hierarchical perspective. International Journal of Information Management, 47, 172–184.
16. Wu, L., & Wang, Q. (2020). Knowledge sharing in online health communities: A social commerce perspective. International Journal of Information Management, 50, 366-375.
17. Newman, S. (2015). Building Microservices: Designing Fine-Grained Systems. O'Reilly Media.
18. Dragoni, N., Giallorenzo, S., Lafuente, A. L., Mazzara, M., Montesi, F., Mustafin, R., & Safina, L. (2017). Microservices: yesterday, today, and tomorrow. Communications of the ACM, 60(6), 85–93.
19. Lewis, J., & Fowler, M. (2014). Microservices: a definition of this new architectural term. Retrieved from https://martinfowler.com/articles/microservices.html
20. Gorton, I. (2018). Essential software architecture (2nd ed.). Springer.
21. Markham, S., & Azevedo, L. (2015). Custom-built versus software-as-a-service (SaaS) e-commerce platforms: An exploratory study. Journal of Electronic Commerce Research, 16(4), 299–310.
22. Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: implementation, management, and security. CRC Press.
23. Han, S., & Lee, Y. (2017). Platform-as-a-Service (PaaS) adoption: The role of service quality and computer self-efficacy. Journal of Business Research, 75, 177–185.
24. Choudhary, R., & Choudhary, S. (2019). Cloud computing and its evolution: a study of platform as a service. In Proceedings of the 3rd International Conference on Communication and Electronics Systems (pp. 128–132). IEEE.
25. von Krogh, G., Haefliger, S., Spaeth, S., & Wallin, M. W. (2012). Carrots and rainbows: Motivation and social practice in open-source software development. MIS Quarterly, 36(2), 649–676.
26. Red Hat (2020). What is open source software? Retrieved from https://www.redhat.com/en/topics/open-source/what-is-open-source
27. Wohlin, C. (2014). Software quality: the future is already here. Journal of Systems and Software, 89, 3–12.
28. Curtis, B., & Krasner, H. (2015). The business value of open-source software. Journal of Systems and Software, 107, 1–12.
29. Royce, W. (1970). Managing the development of large software systems. In Proceedings of IEEE WESCON (pp. 1–9). IEEE.
30. Beck, K., Beedle, M., Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., ... & Thomas, D. (2001). Manifesto for agile software development. Retrieved from https://agilemanifesto.org/
31. Boehm, B., & Turner, R. (2003). Balancing agility and discipline: Evaluating and integrating agile and plan-driven methods. Addison-Wesley.
32. Schwaber, K. (2004). Agile project management with Scrum. Microsoft Press.

Робота виконана під науковим керівництвом д-ра техн. наук, професора
КРИВОРУЧКО О. В.

МОДЕЛЬ КОМПОНЕНТА ІНФОРМАЦІЙНОЇ СИСТЕМИ ЕЛЕКТРОННОГО СУДУ

МІТУЛ Д., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Стаття присвячена моделі компоненту інформаційної системи електронного суду. Вона розглядає основні складові цієї моделі, їх функції та особливості. Крім того, у статті розглянуто основні вимоги до компонентів інформаційної системи електронного суду, а також важливість використання такої системи для забезпечення швидкого та ефективного судочинства. Для дослідження були використані різні джерела інформації, зокрема законодавчі акти та наукові статті. У результаті проведеного аналізу було зроблено висновок, що інформаційна система електронного суду є важливим елементом сучасної юстиції та є необхідною для забезпечення швидкого та доступного судочинства.

This article is devoted to the model of the component of the electronic court information system. It considers the main components of this model, their functions and features. In addition, the article considers the main requirements for the components of the electronic court information system, as well as the importance of using such a system to ensure fast and efficient judicial proceedings. Various sources of information were used for the research, including legislative acts and scientific articles. As a result of the analysis, it was concluded that the information system of the electronic court is an important element of modern justice and is necessary to ensure fast and accessible justice.

Актуальність: стаття присвячена моделі компоненту інформаційної системи електронного суду, яка є актуальною у зв'язку зі збільшенням кількості судових справ та необхідністю підвищення ефективності роботи судів.

Отже, дана робота має велике значення, оскільки вона допоможе користувачам розібратися з перевагами та недоліками різних типів програмного забезпечення для обміну захищеними даними, а також надасть інформацію про найкращі практики та технології для забезпечення безпеки даних в цифровому світі. Крім того, стаття також може бути корисною для розробників програмного забезпечення, які прагнуть створити оптимальні та безпечні продукти для обміну захищеними даними.

Метою даної роботи є розгляд моделі компоненту інформаційної системи електронного суду та її структури. Крім того, метою є проаналізувати функціональні можливості кожного компоненту та їх взаємодію в системі. За допомогою дослідження моделі компоненту інформаційної системи електронного суду можна зробити висновки про її ефективність та доцільність використання в судовій системі.

Об'єктом дослідження є інформаційна система електронного суду, а предметом – модель компоненту цієї системи. *Предметом дослідження* можна визначити саму модель, її компоненти та особливості їх функціонування в інформаційній системі електронного суду. Також можна зосередитись на аналізі технологічних рішень, що використовуються для забезпечення роботи компонентів моделі, та розглянути їх застосування в інформаційних системах електронного суду.

Аналіз попередніх досліджень. Дослідження теми електронного суду займається багато науковців та дослідників з різних країн світу. Деякі з них: Ф. Гао та І. Ван – у своїй статті «Аналіз реалізації електронного суду в Китаї» досліджують розвиток електронного суду в Китаї, а також аналізують основні проблеми, з якими цей суд стикається [1]. А. К. Іслам – у своїй статті «Електронний суд в Бангладеш: стан та проблеми розвитку» аналізує розвиток електронного суду в Бангладеш, виявляє проблеми, з якими цей суд стикається, та запропоновує шляхи їх вирішення В. Г. Павленко та ін. – у статті «Модель

електронного суду в Україні: теоретичні та прикладні аспекти» досліджують теоретичні та практичні аспекти розробки моделі електронного суду в Україні. М. Г. Сергеєва – у статті «Розвиток електронного судочинства в Україні» досліджує розвиток електронного суду в Україні, описує основні досягнення та проблеми, з якими стикається цей суд [2].

Завданням даної роботи є дослідження структури моделі компоненту інформаційної системи електронного суду та визначення його основних складових. Крім того, метою дослідження є аналіз можливостей використання цієї моделі для покращення ефективності роботи судів та забезпечення доступу до правосуддя для громадян.

Виклад основного матеріалу. В Україні з 15 грудня 2021 року було запроваджено інформаційну систему електронного судочинства. Ця система повинна забезпечити доступність та якість послуг, знизити витрати на адміністративні процеси та підвищити ефективність судової системи в цілому. Для забезпечення функціонування цієї системи необхідно розробити модель компоненту інформаційної системи електронного суду [3].

Одним з головних завдань моделювання є створення систематичного та логічного опису процесів, які відбуваються в системі. Для цього необхідно розробити відповідну модель, що дозволить аналізувати, описувати та управляти процесами електронного судочинства.

Компонент інформаційної системи електронного суду може включати в себе такі елементи:

- Система електронного документообігу, що дозволяє обмінюватися документами між судовими органами, сторонами судового процесу та іншими органами державної влади [4].
- Система підтримки прийняття рішень, що забезпечує можливість ефективного аналізу та обробки інформації, необхідної для прийняття правильного та обґрунтованого рішення.
- Система доступу до бази даних, що містить інформацію про рішення, які були ухвалені в рамках судових процесів, а також про сторони, які беруть участь у цих процесах.
- Система забезпечення безпеки даних, що забезпечує захист персональних даних.

Також, модель компоненту інформаційної системи електронного суду може містити такі складові, як модуль автентифікації користувачів, модуль керування доступом, модуль ідентифікації суб'єктів права, модуль обліку виконання судових рішень, модуль розподілу завдань між користувачами та модуль звітування [3].

Проте, на виконання моделі компоненту інформаційної системи електронного суду впливає ряд факторів, зокрема технічні можливості, доступність та якість програмного забезпечення, рівень кваліфікації персоналу та інші. Тому, для успішного функціонування інформаційної системи електронного суду необхідно враховувати ці фактори та забезпечувати постійне вдосконалення та підтримку системи.

Отже, модель компоненту інформаційної системи електронного суду є важливою складовою ефективного функціонування судової системи та забезпечення доступу до правосуддя. Проте, для її успішного впровадження необхідно враховувати технічні та організаційні аспекти та забезпечувати постійну підтримку та вдосконалення системи.

Однак, існують певні проблеми з використанням компонентної моделі в IT-індустрії, зокрема, змістовне описання компонентів може бути складним завданням, а також необхідно ретельно прораховувати залежності між компонентами, щоб уникнути можливих помилок [5].

Загалом, модель компоненту інформаційної системи електронного суду є важливим елементом створення сучасного та ефективного електронного суду. Для її успішної реалізації необхідно здійснювати ретельний аналіз потреб та вимог користувачів, а також враховувати сучасні технології та стандарти в галузі IT. Проектування та розробка моделі компоненту повинні здійснюватися згідно зі стандартами, що гарантуватимуть її стабільну роботу та безпеку.

Під час розробки моделі компоненту інформаційної системи електронного суду важливо враховувати низку вимог та рекомендацій, які висуваються до електронних судів.

Однією з таких вимог є забезпечення безпеки та конфіденційності даних, які обробляються в системі. Зокрема, це може стосуватися персональних даних учасників судового процесу, текстів рішень суду та інших документів.

Для забезпечення безпеки та конфіденційності даних у системі електронного суду можуть застосовуватися різні технічні та організаційні заходи. Наприклад, для захисту даних від несанкціонованого доступу можуть використовуватися криптографічні методи, а для забезпечення цілісності даних – методи цифрового підписування.

Окрім того, важливим елементом моделі компоненту інформаційної системи електронного суду є забезпечення доступності системи. Для цього можуть використовуватися різноманітні технічні та організаційні заходи, наприклад, використання резервного копіювання даних, запобігання збоїв у роботі системи та інші.

У цілому, розробка моделі компоненту інформаційної системи електронного суду - це складний процес, який потребує уваги до деталей та врахування різноманітних вимог і рекомендацій. Проте, забезпечення якості та безпеки роботи електронного суду дозволяє покращити якість та ефективність судової системи в цілому, що є важливим аспектом для будь-якої демократичної держави [7].

Для побудови компонентної моделі інформаційної системи електронного суду необхідно визначити функціональні блоки, які будуть складатися з цієї системи. Одним із таких блоків є реєстраційний блок, який містить в собі інформацію про справи та їх стан. До складу реєстраційного блоку входять компоненти, такі як:

- блок реєстрації справ;
- блок реєстрації користувачів;
- блок реєстрації документів;
- блок реєстрації електронних повідомлень [7].

Ще одним важливим блоком є блок авторизації та аутентифікації користувачів. Він забезпечує перевірку ідентифікаційних даних користувачів та надає їм права доступу до відповідних ресурсів системи. Цей блок може включати компоненти, такі як:

- блок авторизації користувачів;
- блок аутентифікації користувачів.

Інші важливі компоненти моделі інформаційної системи електронного суду включають такі блоки:

- блок зберігання та обробки даних;
- блок керування доступом;
- блок звітності та аналітики [7];
- блок інтеграції з іншими інформаційними системами.

Крім того, необхідно звернути увагу на аспекти безпеки інформації. У зв’язку з особливостями роботи інформаційної системи електронного суду, до неї пред’являються підвищені вимоги щодо захисту інформації. Тому в модель системи слід включити блок забезпечення безпеки інформації.

У загальному плані, модель компоненту інформаційної системи електронного суду може мати наступну структуру:

- Компонент авторизації та ідентифікації користувачів. Цей компонент забезпечує перевірку ідентифікаційних даних користувачів та контроль доступу до різних ресурсів системи.
- Компонент електронного документообігу. Цей компонент забезпечує обробку електронних документів, включаючи прийом, зберігання, обробку та передачу електронних документів в рамках судових процесів.
- Компонент судової інформації та аналізу. Цей компонент забезпечує збір та аналіз судової інформації для створення бази знань, яка допомагає вирішувати різні питання в судових процесах.

- Компонент електронної служби підтримки користувачів. Цей компонент забезпечує надання користувачам електронної підтримки з питань, пов’язаних з використанням системи електронного суду.
- Компонент забезпечення безпеки. Цей компонент забезпечує захист інформації в системі електронного суду від несанкціонованого доступу, знищення та модифікації [8].

Ці компоненти можуть мати різну структуру та складатися з різних модулів, але вони взаємодіють між собою для забезпечення повного функціонування інформаційної системи електронного суду.

Однією з ключових складових компонентної моделі інформаційної системи є модель компонентів. Модель компоненту визначає функціональні можливості компоненту, його інтерфейси та протоколи взаємодії з іншими компонентами системи, а також його залежності від інших компонентів.

Модель компоненту інформаційної системи електронного суду має на меті забезпечення ефективної роботи судової системи шляхом створення високопродуктивної та масштабованої інформаційної інфраструктури.

Іншим компонентом моделі є компонент «Інтерфейс користувача», який забезпечує інтерфейс для користувачів системи. Цей компонент забезпечує доступ до функцій системи та можливість управління даними користувачів.

Крім того, модель включає компонент «Система управління даними», який забезпечує зберігання, організацію та обробку даних, що використовуються в системі. Цей компонент забезпечує безпеку та цілісність даних, а також можливість доступу до них відповідно до встановлених правил доступу.

У процесі розробки моделі компоненту інформаційної системи електронного суду, необхідно враховувати вимоги до безпеки та конфіденційності даних, а також забезпечувати швидкий доступ до інформації та її ефективну обробку [8].

Нова модель інформаційної системи електронного суду в Україні відповідає найвищим стандартам якості та безпеки, що дозволяє забезпечити швидкий та ефективний доступ до інформації та забезпечує високий рівень захисту персональних даних.

Проте, важливо зазначити, що успішність реалізації цієї моделі залежить від різних факторів, таких як рівень підготовки фахівців, забезпечення відповідної інфраструктури та налагодження ефективної системи контролю якості. Для досягнення максимальної ефективності та успішної реалізації моделі, важливо забезпечити всі необхідні ресурси та провести необхідний ряд заходів для підготовки фахівців та створення відповідних умов для ефективного впровадження цієї моделі.

Реалізація цієї моделі компоненту інформаційної системи електронного суду є важливим завданням для забезпечення якісної та ефективної роботи електронного судового установи. При використанні такої моделі, можливе створення інтегрованої системи, яка дозволить автоматизувати багато процесів та процедур, що покращить швидкість та якість прийняття рішень. Крім того, ця модель дозволить забезпечити високий рівень захисту інформації та забезпечити її доступність для користувачів. Важливо зазначити, що реалізація такої моделі потребує значних зусиль, в тому числі забезпечення необхідних ресурсів та кваліфікації персоналу.

Отже, модель компоненту інформаційної системи електронного суду є важливою складовою для забезпечення ефективної та безпечної роботи всієї системи. Вона дозволяє забезпечити необхідну функціональність та інтеграцію різних компонентів системи, що дозволяє ефективно вирішувати завдання судової влади та забезпечувати доступ до юстиції для громадян [6].

Висновки: Заключаючи, можна сказати, що модель компоненту інформаційної системи електронного суду є важливою складовою для забезпечення якісного та ефективного функціонування електронної системи юстиції в Україні. Вона передбачає використання різних компонентів, таких як адаптер, мережа, база даних, програмне забезпечення та інші,

щоб забезпечити швидку та точну обробку інформації про судові справи та забезпечити доступ до цієї інформації для відповідних сторін.

Нова модель інформаційної системи електронного суду в Україні відповідає найвищим стандартам якості та безпеки, що дозволяє забезпечити швидкий та ефективний доступ до інформації та забезпечує високий рівень захисту персональних даних.

Проте, важливо зазначити, що успішність реалізації цієї моделі залежить від різних факторів, таких як рівень підготовки фахівців, забезпечення відповідної інфраструктури та налагодження ефективної системи контролю якості. Для досягнення максимальної ефективності та успішної реалізації моделі, важливо забезпечити всі необхідні ресурси та провести необхідний ряд заходів для підготовки фахівців та створення відповідних умов для ефективного впровадження цієї моделі.

Можна зробити висновок, що модель компоненту інформаційної системи електронного суду є важливим елементом в ефективному функціонуванні системи юстиції в Україні.

Реалізація цієї моделі компоненту інформаційної системи електронного суду є важливим завданням для забезпечення якісної та ефективної роботи електронного судового установи. При використанні такої моделі, можливе створення інтегрованої системи, яка дозволить автоматизувати багато процесів та процедур, що покращить швидкість та якість прийняття рішень. Крім того, ця модель дозволить забезпечити високий рівень захисту інформації та забезпечити її доступність для користувачів. Важливо зазначити, що реалізація такої моделі потребує значних зусиль, в тому числі забезпечення необхідних ресурсів та кваліфікації персоналу.

Отже, можна стверджувати, що модель компоненту інформаційної системи електронного суду має важливе значення для покращення роботи судових установ та забезпечення якісного та ефективного надання юридичних послуг. Реалізація цієї моделі може стати важливим кроком вперед у розвитку електронної юстиції в Україні.

Список використаних джерел

1. Шаблій, С. Модель компонентів системи електронного документообігу / С. Шаблій, М. Короткін, Н. Шатова // Науковий вісник Полісся. – 2018. – № 1 (13). – С. 31–39.
2. Бреславська, Г. Моделювання та аналіз процесів в електронних судах / Г. Бреславська, Т. Чуєв // Наукові записки. Серія: Проблеми інформатизації та управління. – 2019. – Т. 33. – С. 62–71.
3. Хамам, М. Розвиток електронного судочинства в Україні: тенденції та перспективи / М. Хамам, С. Буцьо // Правова держава. – 2018. – № 5. – С. 44–51.
4. Урядовий портал: «Електронний суд стане доступним усім українцям до кінця року» (https://www.kmu.gov.ua/news/elektronniy-sud-stane-dostupnim-usim-ukrayincam-do-kincya-roku)
5. Інформаційний портал «Судова влада України»: «Електронний суд - це новітній етап розвитку юстиції» (https://www.court.gov.ua/sudova-vlada/elektronniy-sud-tse-novitniy-etap-rozvitku-yustitsiyi)
6. Інтернет-видання «Українська правда»: «Електронний суд відкриває можливості, про які раніше не мріяли» (https://www.pravda.com.ua/articles/2020/11/17/7277641/)
7. Інформаційний портал «Yuridicheskaya Gazeta»: «Україна відкрила перший в Європі електронний суд» (https://yur-gazeta.com/publications/ukrayina-vidkryla-pershyj-v-yevropi-elektronnyj-sud.html)
8. Інформаційний портал «Legal Practice»: «Електронний суд: як працює нова система судочинства» (https://lp.ua/ua/blog/elektronnyj-sud-yak-pracyuye-nova-systema-sudochynstva/)

Робота виконана під науковим керівництвом канд. пед. наук, доцента
КОТЕНКО Н. О.

КОНЦЕПТУАЛЬНІ ПІДХОДИ ПОБУДОВИ АРХІТЕКТУРИ ВЕБДОДАТКУ ЗАСОБАМИ UML

МІЩЕНКО В., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто концептуальні підходи до побудови архітектури вебдодатків з використанням засобів UML. Проаналізовано ефективність та універсальність використання засобів UML. Представлено аналоги засобів UML та їх недоліки в порівнянні з засобами UML. Для основних діаграм UML надано приклад використання та описано її внесок у побудову архітектури веб-додатка, розробленого в розрізі магістерського дослідження.

The article discusses conceptual approaches to building the architecture of web applications using UML tools. The efficiency and versatility of using UML tools are analyzed. Analogues of UML tools and their shortcomings in comparison with UML tools are presented. For basic UML diagrams, an example of use is provided and its contribution to the construction of the architecture of a web application developed as part of a master's study is described.

Актуальність. Інтернет займає важливе місце в повсякденному житті людей. Інтернет-технології надають можливість здійснювати багато різних дій, від замовлення товарів та послуг до соціальних інтеракцій. Веб-додатки є однією з ключових складових інтернету. Використовуючи веб-додатки, можна забезпечити швидкий та зручний доступ до інформації, зберігати дані в хмарних сховищах та забезпечувати роботу з великими обсягами даних. Такі додатки дозволяють користувачам забезпечувати взаємодію з різноманітними джерелами даних та оброблювати їх у режимі реального часу. В цілому, веб-додатки є важливими засобами для забезпечення взаємодії з користувачами та ефективного використання ресурсів інтернету. Вони є необхідним елементом інформаційної інфраструктури та економіки.

З огляду на все більше зростаючу популярність веб-додатків, розробники повинні мати достатні знання та навички для створення надійної та ефективної архітектури веб-додатку. У зв'язку з цим, побудова якісної архітектури веб-додатків є критично важливою для їх успішного впровадження та функціонування.

Використання засобів UML при побудові архітектури веб-додатків є найбільш розповсюдженим та ефективним підходом, оскільки UML надає зручний та стандартизований мовник для опису архітектури системи. Детальний аналіз концептуальних підходів до побудови архітектури веб-додатків з використанням засобів UML може бути корисним для розробників програмного забезпечення, які прагнуть забезпечити масштабованість, розширюваність та безпеку своїх веб-додатків.

Також актуальність статті полягає в тому, що побудова архітектури веб-додатків є складним та багатоаспектним процесом, тому знання концептуальних підходів до її побудови може допомогти розробникам зменшити кількість помилок та забезпечити високу якість свого програмного забезпечення.

Метою статті є аналіз концептуальних підходів до побудови архітектури веб-додатків з використанням засобів UML, щоб допомогти розробникам програмного забезпечення зрозуміти основні принципи побудови архітектури веб-додатків та використання засобів UML для її моделювання.

Об'єктом дослідження є розробки архітектури веб-додатку з використанням засобів UML, розгляд підходів до побудови архітектури веб-додатку, з використанням UML, а також оцінку ефективності використання UML для розробки веб-додатків.

Основним завданням статті є дослідити важливість побудови якісної архітектури веб-додатків, проаналізувати концептуальні підходи до її побудови та продемонструвати практичне застосування засобів UML для моделювання архітектури веб-додатків.

Предметом дослідження статті є концептуальні підходи до побудови архітектури веб-додатків з використанням засобів UML. У статті розглядається теоретичний аспект побудови якісної архітектури веб-додатків, що базується на концептуальних принципах, та їх відображення в моделях UML.

Виклад основного матеріалу. Веб-додатки стали необхідним інструментом для бізнесу та користувачів. За допомогою веб-додатків можна здійснювати покупки, забронювати квитки, знаходити інформацію та взагалі отримувати доступ до безлічі різноманітних сервісів. Однак, побудова веб-додатків не є простим завданням, оскільки вони повинні бути ефективними, безпечними та зручними в користуванні.

У цьому контексті концептуальні підходи побудови архітектури веб-додатків грають важливу роль.

Перед появою UML існувало багато мов моделювання, таких як Structured Analysis and Design Technique (SADT), Yourdon Systems Method (YSM), Data Flow Diagrams (DFD) та інші. Однак, жодна з цих мов не була стандартизована і не забезпечувала єдиного підходу до моделювання.

У 1994 році Об’єднана група експертів з об’єктно-орієнтованого моделювання (Object Management Group, OMG) визначила потребу в єдиній мові моделювання для об’єктно-орієнтованого програмування. Це призвело до створення UML в 1997 році. [1].

UML став стандартом моделювання програмного забезпечення і отримав широке використання в індустрії програмного забезпечення і в академічних кругах.

Для побудови архітектури веб-додатку можна використовувати різні підходи.

UML (Unified Modeling Language) – це стандартизована мова моделювання, яка використовується для побудови програмного забезпечення. UML надає засоби для опису різних аспектів програмного забезпечення, включаючи структуру, поведінку та взаємодію між складовими. UML має багато різних діаграм, кожна з яких описує різний аспект програмного забезпечення [2].

BPMN (Business Process Model and Notation) – це мова моделювання бізнес-процесів, яка використовується для опису послідовності роботи бізнес-процесів. Вона дозволяє представити бізнес-процеси у вигляді графів, які відображають послідовність дій [3].

ER-діаграми (Entity-Relationship Diagrams) – це мова моделювання, яка дозволяє описувати концептуальні схеми за допомогою узагальнених конструкцій блоків. Вона дозволяє відобразити взаємозв’язки між таблицями баз даних [4].

FD-діаграми (Data Flow Diagrams) – це мова моделювання, що використовується для опису потоків даних у системі. Вона дозволяє відображати, як дані рухаються в системі та як вони обробляються [5].

ArchiMate – це мова моделювання, що використовується для побудови архітектури додатків та систем. Вона дозволяє описати архітектуру системи з різних точок зору, включаючи бізнес, технічну та інформаційну архітектуру [6].

Аналоги мов моделювання мають свої недоліки в порівнянні з UML. BPMN призначений для моделювання бізнес-процесів, а не архітектури програмного забезпечення, тому він може бути менш корисним для розробників програмного забезпечення. ER-діаграми зосереджені на моделюванні відносин між таблицями баз даних, тому ввони можуть бути менш ефективними для моделювання архітектури програмного забезпечення, яка може містити більше ніж просто бази даних. DFD-діаграми зосереджені на моделюванні потоків даних. ArchiMate більш орієнтований на бізнес-процеси і менш на опис технічних аспектів системи.

UML залишається одним з найпопулярніших та найбільш широко використовуваних засобів для моделювання архітектури програмного забезпечення.

У дослідженнях UML брали участь вчені та дослідники з усього світу, включаючи представників відомих університетів, інститутів та корпорацій такі як Граді Буч [1], Івар Якобсон [1], Джеймс Рамбо [1], Бертран Мейє [7] , Мартін Фаулер [8]. З їхніх напрацювань, можна зробити висновок, що універсальність UML полягає у можливості моделювання різних аспектів програмного забезпечення, можливості використання для будь-якої мови програмування, ефективному спілкуванні зі стейкхолдерами, плануванні та управлінні проектами, проведенні аналізу та тестуванні програмного забезпечення, наявності великої спільноти користувачів та підтримки, можливості створення готових шаблонів та бібліотек. Всі ці переваги дозволяють розробникам програмного забезпечення більш ефективно розробляти та управляти проектами, зменшуючи час та кошти, та забезпечувати якість програмного забезпечення.

UML є ефективною та адаптивною до будь якого проекту мовою моделювання, оскільки надає засоби для опису різних аспектів програмного забезпечення, включаючи структуру, поведінку та взаємодію між складовими. UML має багато різних діаграм, кожна з яких описує різний аспект програмного забезпечення. Це дозволяє розбити архітектуру веб-додатку на окремі складові та моделювати кожну з них окремо. Наприклад, можна використовувати діаграму взаємодії для опису поведінки додатку, діаграму компонентів для опису структури компонентів та їх взаємодії, діаграму послідовності для опису послідовності виконання дій тощо. Використання UML дозволяє візуалізувати архітектуру веб-додатку, що допомагає зрозуміти його структуру та функціональність. Це може бути корисним для комунікації з іншими учасниками проекту, включаючи розробників, тестувальників та замовників.

Архітектура веб-додатку описує структуру та взаємодію між складовими додатку. Веб-додатки складаються з трьох основних складових: клієнтської сторони, серверної сторони та бази даних. Клієнтська сторона - це інтерфейс, який користувач використовує для взаємодії з додатком. Серверна сторона - це програмне забезпечення, яке забезпечує функціональність додатка та взаємодію з базою даних. База даних - це система, яка зберігає дані, які використовуються додатком [9].

UML дозволяє розробникам побудувати детальну модель системи, яка може включати в себе діаграми класів, діаграми послідовностей та діаграми діяльності, діаграма прецедентів, діаграма станів, діаграма компонентів, діаграма розгортання.

Діаграми дозволяють розробникам зрозуміти функціональність системи, її структуру та взаємодії компонентів, що в свою чергу сприяє якості та ефективності розробки веб-додатку. Після створення всіх необхідних діаграм розробники можуть використовувати їх для створення коду системи та розробки веб-додатку.

У веб-додатках архітектура визначає, як різні компоненти системи взаємодіють між собою та як вони розташовані. Побудова архітектури веб-додатків з використанням UML дозволяє розробникам зосередитися на суттєвих аспектах системи та забезпечити її ефективну та безпечну роботу.

Узагальнюючи, побудова архітектури веб-додатку з використанням UML є важливим етапом розробки будь-якої системи. Вона дозволяє розробникам краще зрозуміти вимоги до системи, визначити її основні компоненти та забезпечити її ефективну та безпечну роботу. Використання UML дозволяє зменшити ризики помилок та підвищити якість розробки, що є важливим для будь-якої компанії, що займається розробкою веб-додатків.

Для візуального представлення структури, поведінки та взаємодії системи або програмного забезпечення розглянемо діаграми UML на прикладах.

Інформація про акторів, та опис випадків використання:

Актори-користувачі: Клієнт – клієнт інтернет-магазину. Менеджер з продажу: користувач, що використовує функції адміністрування сайту.

Актори-зовнішні системи: База даних – база даних, яка зберігає інформацію.

В даній діаграмі наведені відношення між акторами та використаннями, що демонструє зв’язки між акторами та їх поведінкою в системі (рис. 1).

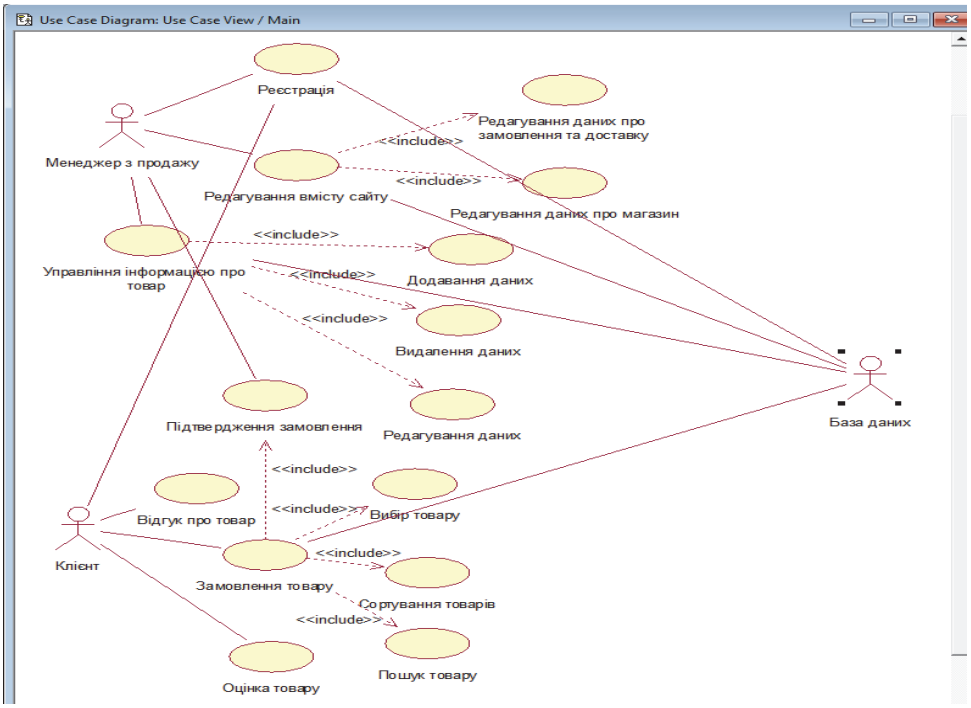


Рис. 1. UML-діаграма використання програмного продукту інтернет-магазину

Джерело:розроблено автором в середовищі IBM Rational Rose Enterprise Edition (скріншот з екрану)

Діаграма демонструє опис процесу авторизації клієнта. Якщо логін та пароль було введено коректно, в браузері відображається особистий кабінет користувача (рис. 2).

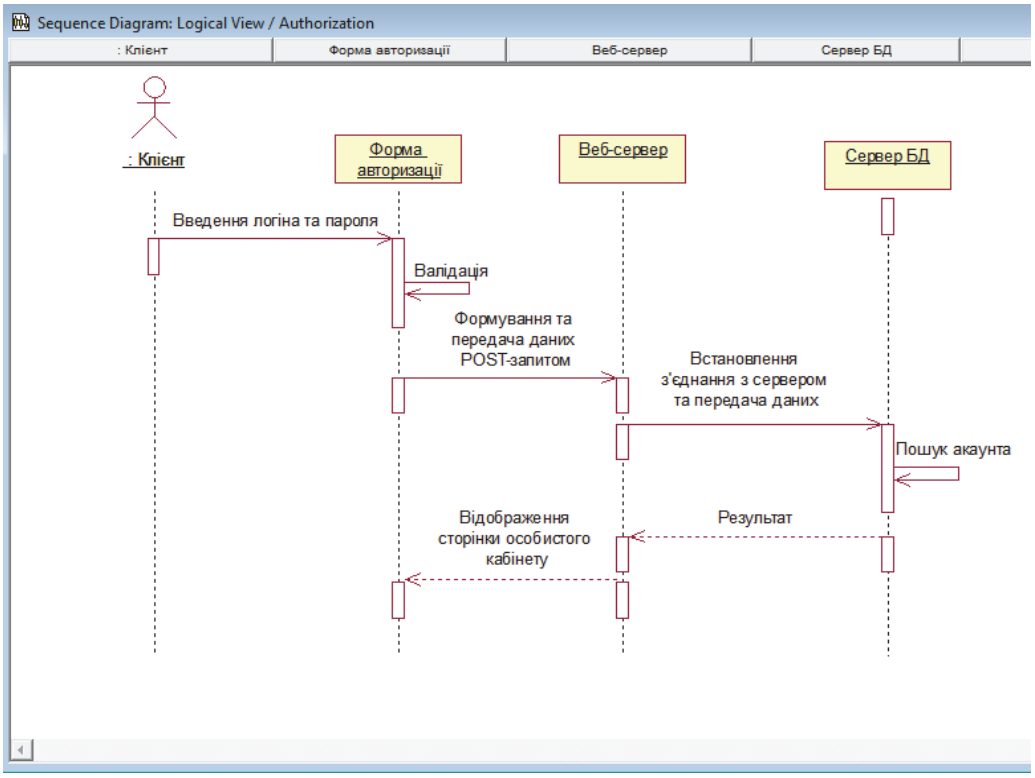


Рис. 2. UML-діаграма послідовності авторизації програмного продукту інтернет-магазину

Джерело:розроблено автором в середовищі IBM Rational Rose Enterprise Edition (скріншот з екрану)

Дана схема демонструє роботу інтернет-магазину, а саме:

При вході на сайт інтернет-магазину користувачу відображається головна сторінка, на якій необхідно зареєструватись або ввести персональні дані, якщо він зареєстрований. Далі потрібно обрати товар, скориставшись функціоналом сайту. Після вибору товару зареєстрованим користувачам запропонують вибрати метод оплати та доставки. Після перевірки всіх даних необхідно підтвердити замовлення. Інформація про зроблене замовлення переглядається менеджером магазину та передається на виконання (рис. 3).

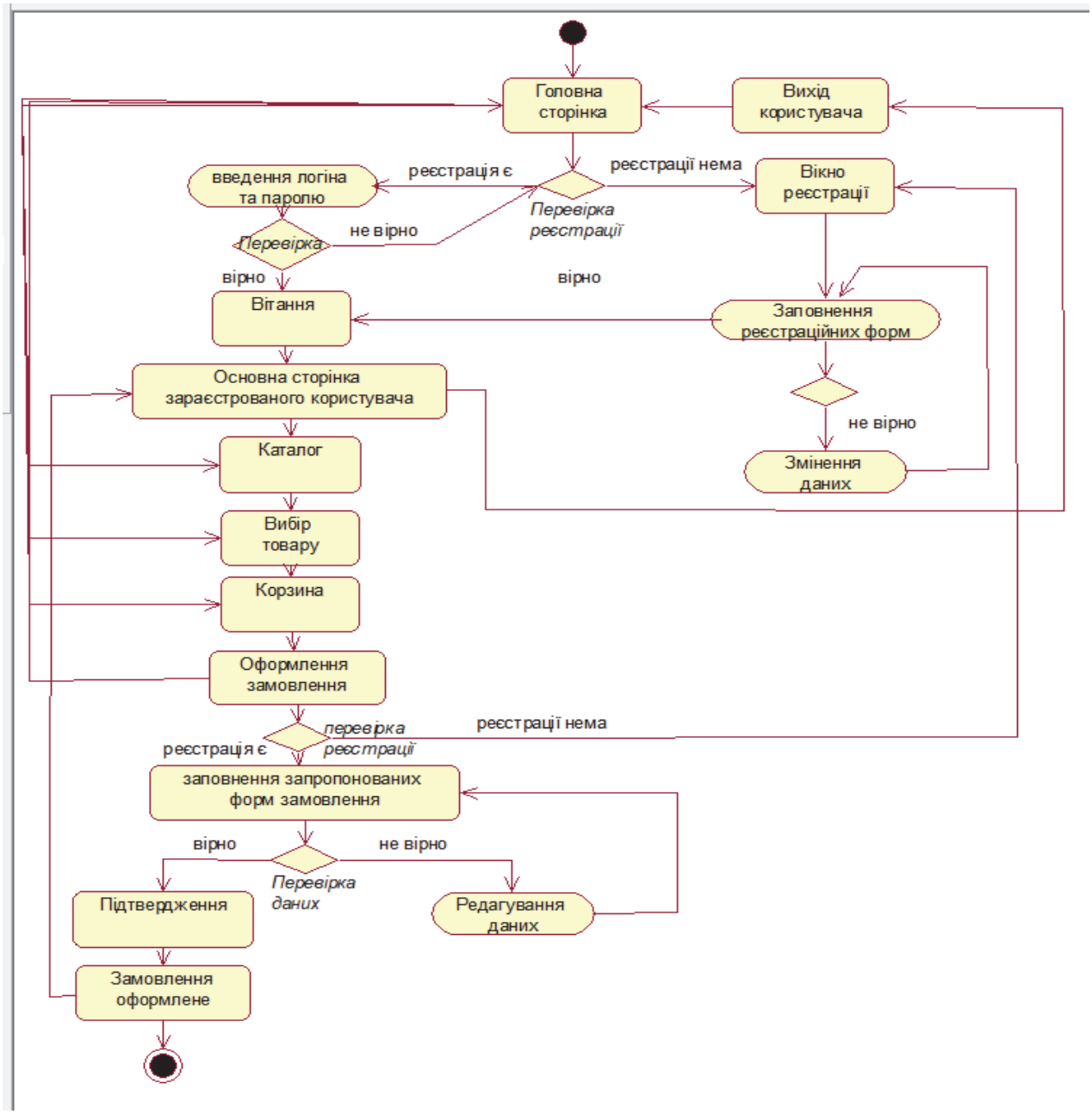


Рис. 3. UML-діаграма діяльності програмного продукту інтернет-магазину

Джерело:розроблено автором в середовищі IBM Rational Rose Enterprise Edition (скріншот з екрану)

Таким чином, основні переваги використання діаграм UML включають:

1. Спрощення спілкування між розробниками та іншими зацікавленими сторонами: діаграми UML надають зручний спосіб спілкування між розробниками та іншими зацікавленими сторонами, які можуть не мати технічних знань.

2. Допомога в розумінні структури системи: діаграми UML допомагають розробникам розуміти структуру системи та взаємодію її компонентів.

3. Виявлення проблем та помилок на ранніх етапах розробки: діаграми UML допомагають виявляти проблеми та помилки на ранніх етапах розробки, коли виправлення їх вартує менше.

4. Підвищення ефективності розробки: діаграми UML допомагають розробникам швидко та ефективно розуміти та змінювати систему.

5. Підтримка документації: діаграми UML можуть бути використані для створення документації про систему.

Висновки. У цій статті було розглянуто деякі концептуальні підходи до побудови архітектури веб-додатків за допомогою засобів UML. Використання UML діаграм допомагає створити чітке та зрозуміле опис програмного забезпечення, його компонентів та взаємодії між ними.

Незалежно від обраної діаграми, основним завданням при побудові архітектури веб-додатку є забезпечення його масштабованості та ефективності. Особливо важливою є підтримка розширюваності, що дозволяє додавати нові функції до додатку без необхідності переписування вже існуючого коду.

Крім того, побудова архітектури веб-додатка повинна враховувати вимоги до безпеки даних та захисту від зловмисників. У цьому контексті важливо розглянути різні варіанти зберігання даних та забезпечення їх конфіденційності та цілісності.

Усі ці аспекти повинні бути враховані при побудові архітектури веб-додатку, тому використання засобів UML може значно полегшити цей процес. Діаграми UML надають можливість створювати чіткі та зрозумілі описи програмного забезпечення, які дозволяють розробникам краще розуміти структуру додатка та взаємодію між його компонентами.

Список використаних джерел

1. Booch G, Rumbaugh J., Jacobson I. Tutorial «The Unified Modeling Language User Guide (2nd Edition)» – USA: Wesley Professional, 1998. – 512 p. ISBN: 0-201-57168-4
2. Larman C. Tutorial «Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development (3rd ed.)» – USA: Prentice Hall, 2004. – 630 p. ISBN: 978-0131489066
3. Silver B. Tutorial «Bpmn Method and Style, 2nd Edition, with Bpmn Implementer's Guide» – USA: Cody-Cassidy Press, 2011. – 286 p. ISBN: 978-0982368114
4. Модель «сутність – зв'язок». Електронний ресурс URL: https://uk.wikipedia. org/wiki/Модель_»сутність_–_зв'язок» (останнє звернення 23.03.2023р.)
5. Shelly G., Cashman T., Rosenblatt H. Tutorial «Systems Analysis and Design 7th Edition 4» – USA: Course Technology, 2007. – 702 p. ISBN: 978-1423912224
6. Archimate-overview. Електронний ресурс URL: https://www.opengroup.org/archimate-overview (останнє звернення 25.03.2023р.)
7. B. Meyer. Tutorial «Object-Oriented Software Construction» – USA: Pearson College Div, 2000. – 1296 p.. ISBN: 978-0136291558
8. M. Fowler. Tutorial «UML Distilled: A Brief Guide to the Standard Object Modeling Language» – USA: Addison-Wesley Professional, 2003. – 208 p. ISBN: 978-0321193681
9. L.Shklar, R.Rosen. Tutorial «Web Application Architecture: Principles, Protocols and Practices» – USA: John Wiley & Sons Ltd , 2003, – 357 p. ISBN: 0-471-48656-6

Робота виконана під науковим керівництвом PhD, доцента
ДЕСЯТКО А. М.

СТРУКТУРИ ДАНИХ У ФУНКЦІОНАЛЬНОМУ ОТОЧЕННІ

МОСКАЛЕНКО В., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Ця стаття має на меті проаналізувати властивості, операції та характеристики продуктивності двох модифікацій куп: біноміальних куп та лівоцентрованих куп. Надаючи детальний аналіз цих структур даних та їх застосування в різних контекстах, ця робота сприяє розумінню та проектуванню структур даних у функціональному середовищі. Зокрема, ця робота має на меті дослідити переваги та недоліки біноміальних та лівоцентрованих куп, їхні характеристики продуктивності та придатність для використання у графових алгоритмах та чергах з пріоритетами.

This article aims to analyze the properties, operations, and performance characteristics of two modifications of heaps: binomial heaps and left-centered heaps. By providing a detailed analysis of these data structures and their application in various contexts, this work contributes to the understanding and design of data structures in a functional environment. In particular, this paper aims to investigate the advantages and disadvantages of binomial and left-centered heaps, their performance characteristics, and their suitability for use in graph algorithms and priority queues.

Актуальність. Структури даних відіграють важливу роль в інформатиці, надаючи засоби для організації та маніпулювання даними в ефективний та раціональний спосіб. В останні роки зростає інтерес до функціонального програмування - парадигми, яка наголошує на використанні функцій та незмінних структур даних. Ця стаття досліджує тему структур даних у функціональному середовищі, зосереджуючись на двох специфічних модифікаціях куп: біноміальних купах та лівоцентрованих купах.

Хоча купи є добре відомою структурою даних, їх модифікації у функціональному середовищі є відносно новими і не були широко вивчені. Ця робота має на меті заповнити цю прогалину, надавши детальний аналіз біноміальних та лівоцентрованих куп, їх властивостей, операцій та характеристик продуктивності.

Метою статті є аналіз переваг та недоліків цих структур даних, їхніх характеристик продуктивності та застосування в різних контекстах. Таким чином, ми прагнемо надати уявлення про проектування та використання структур даних у функціональному середовищі.

Для досягнення мети цієї роботи були поставленні наступні **завдання**:

- Надамо детальне визначення біноміальної купи та лівоцентрованої купи.
- Опишемо їх властивості та операції.
- Проаналізуємо їхні характеристики, включаючи часову та просторову складність.
- Обговорити їх застосування в різних контекстах, таких як графові алгоритми та черги з пріоритетами.

Предметом дослідження є структури даних у функціональному середовищі, зокрема біноміальні купи та лівоцентровані купи.

Об'єктом дослідження є аналіз властивостей, операцій та характеристик продуктивності біноміальних та лівоцентрованих куп, а також обговорення їх застосування в різних контекстах.

Виклад основного матеріалу. Біноміальна купа – це структура даних, яка використовується для реалізації пріоритетних черг у функціональному середовищі програмування. Це набір бінарних дерев, де кожне дерево задовольняє властивості купи: батьківський вузол має вищий пріоритет, ніж його дочірні. Дерева в біноміальній купі будуються за певним шаблоном, де i-те дерево має 2^i вузлів, а корінь кожного дерева має ступінь і. Ступінь вузла - це кількість дочірніх вузлів, які він має.

Біноміальні купи підтримують такі операції: вставка, пошук мінімуму, злиття, зменшення та видалення мінімуму. Щоб вставити елемент у купу, створюється нове дерево, яке об'єднується з існуючою купою. Операція find-minimum повертає елемент з мінімальним пріоритетом, не видаляючи його з купи. Операція злиття об'єднує дві біноміальні купи в одну купу. Операція зменшення використовується для зменшення пріоритету елемента, що вже знаходиться в купі. Операція delete-minimum видаляє елемент з мінімальним пріоритетом з купи.

Біноміальні купи мають кілька переваг над іншими структурами даних у функціональному середовищі. По-перше, вони забезпечують ефективні операції з логарифмічною часовою складністю для вставки, пошуку мінімуму та видалення мінімуму. По-друге, вони підтримують об'єднання двох куп з логарифмічною часовою складністю. По-третє, вони мають гарантовану амортизовану постійну часову складність для операцій зменшення ключа.

Однак біноміальні купи також мають деякі недоліки. Вони вимагають більше місця у порівнянні з іншими структурами даних з пріоритетною чергою. Крім того, операція злиття може вимагати створення та об'єднання нових дерев, що призводить до збільшення використання пам'яті та зниження продуктивності.

Характеристики продуктивності біноміальних куп можна проаналізувати за допомогою математичних формул. Часова складність операції вставки становить $O(\log n)$, де n – розмір купи. Часова складність операції пошуку мінімуму становить $O(1)$, а операції видалення мінімуму – $O(\log n)$. Часова складність операції злиття становить $O(\log n)$, а просторова складність – $O(n)$.

На рис. 1 зображений алгоритм для біноміальних та лівоцентрованих куп.

На додаток до своїх переваг і недоліків, біноміальні купи мають кілька цікавих властивостей, які роблять їх унікальними серед структур даних. Наприклад, біноміальну купу розміру n можна представити у вигляді двійкового числа, де біти 1 відповідають кореням дерев у купі. Ця властивість дозволяє ефективно об'єднувати дві біноміальні купи за допомогою побітових операцій.

Ще однією цікавою властивістю біноміальних куп є їх зв'язок з двійковими числами та зв'язок з двійковим представленням цілих чисел. Зокрема, біноміальну купу можна використовувати для представлення двійкового розкладу цілого числа, при цьому степінь кожного вузла представляє позицію відповідного біта у двійковому представленні.

Ці властивості демонструють багату математичну структуру, що лежить в основі біноміальних куп, і підкреслюють їх потенціал для використання в різних додатках за межами черг пріоритетів. Загалом, біноміальні купи є цікавою структурою даних, яка заслуговує на подальше вивчення та аналіз в контексті функціонального програмування.

Ще однією цікавою властивістю біноміальних куп є їх зв'язок з графовими алгоритмами. Зокрема, біноміальні купи можна використовувати для реалізації алгоритму Дейкстри, відомого графового алгоритму, який використовується для пошуку найкоротшого шляху між двома вершинами у зваженому графі. Використовуючи біноміальну купу для зберігання набору невідвіданих вершин та їх відстаней від початкової вершини, алгоритм Дейкстри може досягти часової складності O(E + V log V), де E – кількість ребер, а V – кількість вершин у графі.

На додаток до алгоритму Дейкстри, біноміальні купи також можна використовувати для реалізації інших графових алгоритмів, таких як алгоритм Прима для пошуку мінімального основного дерева та алгоритм Крускала для пошуку мінімального остовного лісу. Це підкреслює універсальність біноміальних куп та їхній потенціал для використання у різноманітних додатках, окрім пріоритетних черг.

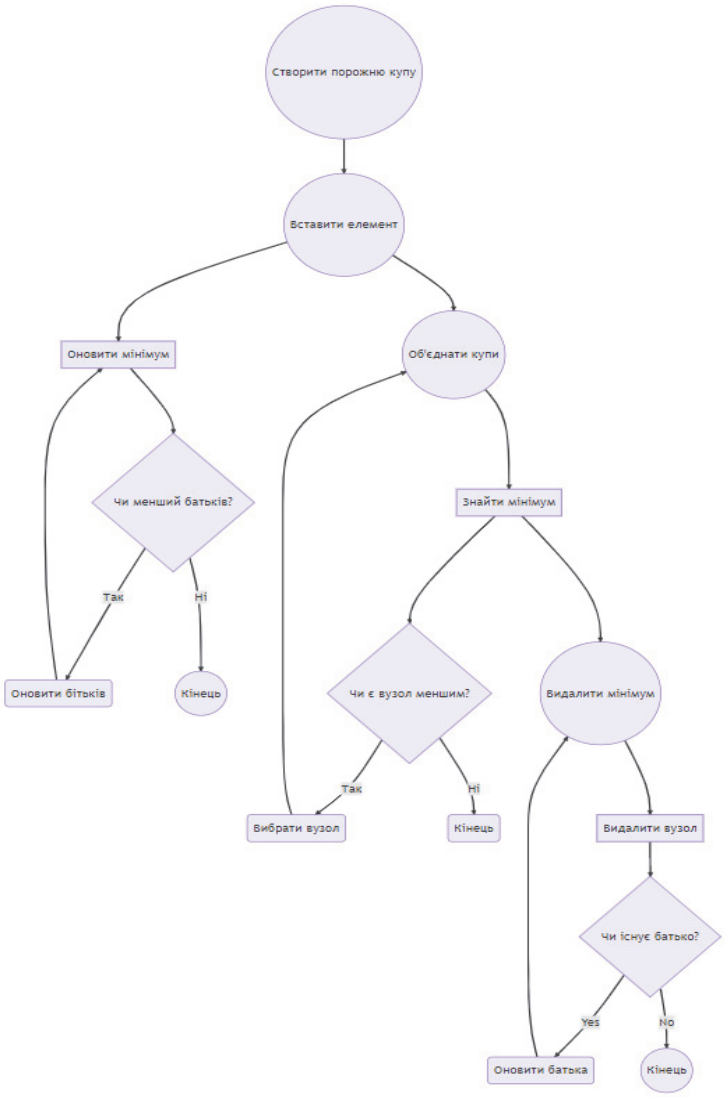


Рис. 1. Алгоритм роботи досліджуваних куп

Загалом, зв'язок між біноміальними кучами і графовими алгоритмами демонструє потужність і гнучкість цієї структури даних в контексті функціонального програмування. Розуміючи і використовуючи цей зв'язок, функціональні програмісти можуть скористатися унікальними властивостями біноміальних куп для ефективного розв'язання широкого спектру задач в теорії графів і не тільки.

Тож, біноміальні купи є корисною структурою даних для реалізації пріоритетних черг у функціональному середовищі програмування. Вони забезпечують ефективні операції і підтримують злиття двох куп, але також мають деякі недоліки, зокрема, збільшене використання пам'яті і повільнішу продуктивність під час операцій злиття. Формули для часової та просторової складності допомагають проаналізувати характеристики продуктивності біноміальних куп і зрозуміти їхню застосовність у різних контекстах.

Лівоцентровані купи – це модифікація стандартної двійкової структури даних купи, що використовується у функціональному програмуванні. У лівоцентрованій купі батьківський вузол завжди більший, ніж обидва його дочірні. Однак, на відміну від двійкової купи, лівий нащадок завжди є повним деревом, а правий нащадок завжди менший за лівий. Це означає, що лівий нащадок завжди є коренем піддерева, а правий нащадок завжди менший за свого батька.

Операції, які підтримуються лівоцентрованими кучами, включають вставку, пошук мінімуму, об'єднання, зменшення та видалення мінімуму. Щоб вставити елемент у купу, його додають як листовий вузол на останній рівень лівого піддерева, а потім відновлюють

властивість купи, помінявши вузли місцями за необхідності. Операція пошуку мінімуму повертає елемент з мінімальним пріоритетом, не видаляючи його з купи. Операція злиття об'єднує дві купи, розташовані зліва по центру, в одну купу. Операція decrease-key використовується для зменшення пріоритету елемента, що вже знаходиться у купі. Нарешті, операція delete-minimum видаляє елемент з мінімальним пріоритетом з купи.

У функціональному середовищі лівоцентровані купи мають кілька переваг над бінарними купами. По-перше, вони забезпечують ефективні операції з логарифмічною часовою складністю для вставки, пошуку мінімуму та видалення мінімуму. По-друге, вони підтримують об'єднання двох куп з логарифмічною часовою складністю, але це може бути повільніше порівняно з двійковими кучами. По-третє, вони використовують менше пам'яті, ніж двійкові купи, завдяки своїй структурі.

Однак, лівоцентровані купи також мають деякі недоліки. Операція зменшення клавіші може вимагати перестановки вузлів, що може бути повільнішим порівняно з двійковими кучами. Крім того, властивість лівоцентрованості може ускладнювати виконання деяких операцій.

Характеристики продуктивності лівоцентрованих куп можна проаналізувати за допомогою математичних формул. Часова складність операції вставки становить $O(\log n)$, де n – розмір купи. Часова складність операції пошуку мінімуму становить $O(1)$, а операції видалення мінімуму – $O(\log n)$. Часова складність операції злиття становить $O(\log n)$, а просторова складність – $O(n)$.

Лівоцентровані купи також мають цікаві властивості, які відрізняють їх від інших структур даних пріоритетної черги. Однією з таких властивостей є те, що їх можна використовувати для ефективної підтримки ковзного вікна над послідовністю елементів. Зокрема, ліве піддерево лівоцентрованої купи можна використовувати для представлення поточного вікна, а праве піддерево - для представлення елементів, яких немає у поточному вікні. Ця властивість дозволяє ефективно оновлювати дані та виконувати запити у ковзних вікнах, що є поширеним явищем у багатьох програмах, таких як потокове передавання даних та аналіз часових рядів.

Ще однією цікавою властивістю лівоцентрованих куп є їх зв'язок з числами Фібоначчі. Зокрема, розмір лівого піддерева лівоцентрованої купи з n елементами дорівнює n-му числу Фібоначчі. Ця властивість демонструє зв'язок між лівоцентрованими кучами та послідовністю Фібоначчі, відомою математичною послідовністю з багатьма цікавими властивостями.

Ці властивості підкреслюють потенціал лівоцентрованих куп для використання у різноманітних додатках, окрім черг пріоритетів, зокрема, у ковзних вікнах та послідовностях, пов'язаних з послідовністю Фібоначчі. Загалом, лівоцентровані купи є цікавою структурою даних з унікальними властивостями, які роблять їх цінним доповненням до інструментарію функціональних програмістів.

Ще однією цікавою властивістю лівоцентрованих куп є їх зв'язок зі структурою даних парних куп. Парні купи – це ще один тип пріоритетних структур даних, які підтримують ефективні операції вставки та пошуку мінімуму. Вони засновані на рекурсивній структурі, де кожен вузол має список своїх дочірніх елементів, а мінімальний елемент зберігається в корені.

Лівоцентровані купи можна розглядати як спрощену версію парних куп, де ліве піддерево кожного вузла відповідає списку його дочірніх елементів. Цей зв'язок між лівоцентрованими кучами і парними кучами підкреслює потенціал використання лівоцентрованих куп як будівельного блоку для більш складних структур даних.

Крім того, лівоцентровані купи мають природну рекурсивну структуру, яку можна використовувати для ефективної реалізації рекурсивних алгоритмів. Наприклад, операція злиття двох лівоцентрованих куп може бути реалізована рекурсивно, при цьому менша купа

об’єднується з більшою, роблячи її правим дочірнім елементом кореневого вузла. Ця рекурсивна структура також може бути використана для реалізації інших алгоритмів, які вимагають обходу та маніпулювання деревами, таких як обхід та обертання дерев.

Загалом, зв’язок між лівоцентрованими кучами і парними кучами, а також природна рекурсивна структура лівоцентрованих куп демонструють потенціал цих структур даних для використання у різноманітних додатках, окрім черг пріоритетів. Розуміючи і використовуючи ці зв’язки, функціональні програмісти можуть скористатися унікальними властивостями лівоцентрованих куп для ефективного вирішення широкого кола завдань.

Тож, лівоцентровані купи є корисною модифікацією двійкових куп для реалізації пріоритетних черг у функціональному середовищі програмування. Вони забезпечують ефективні операції і використовують менше пам’яті порівняно з бінарними кучами. Однак їхня властивість лівоцентрованості може ускладнювати деякі операції, а операція зменшення може бути повільнішою порівняно з двійковою купою. Формули для часової та просторової складності допомагають проаналізувати характеристики продуктивності лівоцентрованих куп і зрозуміти їхню застосовність у різних контекстах.

Висновки. Отже, у цій статті було досліджено тему структур даних у функціональному середовищі, зосередившись на двох специфічних модифікаціях куп: біноміальних купах та лівоцентрованих купах. Метою цієї роботи було проаналізувати переваги та недоліки цих структур даних, їхні характеристики продуктивності та застосовність у різних контекстах.

Біноміальні купи є добре відомою структурою даних для реалізації пріоритетних черг у функціональному середовищі. Вони забезпечують ефективні операції з логарифмічною часовою складністю для вставки, пошуку-мінімуму та видалення-мінімуму, підтримують об’єднання двох куп та мають гарантовану амортизовану постійну часову складність для операцій зі зменшенням ключа. Лівоцентровані купи - це модифікація двійкових куп, яка забезпечує ефективні операції з логарифмічною часовою складністю для операцій вставки, пошуку-мінімуму та видалення-мінімуму. Вони також використовують менше пам’яті порівняно з бінарними кучами завдяки своїй структурі.

Загалом, ця робота сприяла розумінню та проектуванню структур даних у функціональному середовищі, надаючи уявлення про переваги та недоліки біноміальних та лівоцентрованих куп.

Список використаних джерел

1. Кормен, Т. Х., Лейзерсон, К. Е., Рівест, Р. Л. та Штейн, К. (2009). Вступ до алгоритмів (3-тє вид.). MIT Press.
2. Окасакі, К. (1999). Чисто функціональні структури даних. Cambridge University Press.
3. Brodal, G. S., & Okasaki, C. (1996). Оптимальні чисто функціональні черги пріоритетів. Журнал функціонального програмування, 6(6), 839–857.
4. Sleator, D. D., & Tarjan, R. E. (1986). Самоналагоджувальні бінарні дерева пошуку. Журнал ACM, 32(3), 652–686.

Робота виконана під науковим керівництвом канд. екон. наук, доцента
ТИЩЕНКА Д. О.

МОДЕЛЬ ЗАГРОЗ БЕЗПЕКИ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ПІДПРИЄМСТВА

НАГУЛЯК Л., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розроблено модель загроз безпеки конфіденційної інформації підприємства. Описано різні типи загроз, які можуть стати причиною витоку конфіденційної інформації, а також визначено методи, які можуть бути використані для їх виявлення та захисту від них.

The article develops a model of threats to the security of the company's confidential information. The different types of threats that can lead to the leakage of confidential information are described, and the methods that can be used to detect and protect against them are defined.

Актуальність. Питання створення та використання моделей загроз конфіденційної інформації підприємства є дуже актуальним у сучасному світі, де діджиталізація та розвиток інформаційних технологій призвели до збільшення кількості та різноманітності загроз для підприємств. Конфіденційна інформація є важливим активом для більшості підприємств, оскільки вона може включати в себе плани розвитку, стратегії маркетингу, фінансові відомості та інші персональні дані. Якщо ця інформація потрапляє в руки конкурентів або зловмисників, то це може призвести до значних фінансових збитків, втрати довіри та інших негативних наслідків. Тому, моделювання та аналіз загроз конфіденційної інформації є дуже важливим для захисту підприємств від потенційних кібератак та інших загроз, що можуть призвести до витоку конфіденційної інформації. Захист інформації є однією з найбільш важливих задач для керівництва будь-якого підприємства.

Метою статті є розробка моделі загроз безпеки інформації підприємства «IT громада».

Стаття включає опис різних заходів, які можуть бути прийняті підприємствами для захисту своєї конфіденційної інформації від потенційних загроз, таких як кібератаки, фізичний доступ до приміщень, втрати даних тощо. Вона визначає склад і джерела загроз, оцінку можливості їх прояву, шляхи їх здійснення, оцінку очікуваного збитку від реалізації загроз.

Об'єктом дослідження є конфіденційна інформація, якою підприємство володіє та обробляє.

Предмет дослідження – вивчення загроз, які можуть вплинути на конфіденційність інформації, та побудова моделі загроз безпеки конфіденційної інформації підприємства.

Аналіз попередніх досліджень. Дослідження моделі загроз безпеки конфіденційної інформації підприємства були проведені як вітчизняними, так і закордонними дослідниками: Борисенко О.І., Мельник І.А., Шевчук І.В., R. L. Popp, A. T. Sherman, C. M. Eloff, J. E. Labuschagne.

Ці дослідження дозволяють розглянути різні аспекти загроз безпеки конфіденційної інформації підприємства та пропонують різноманітні методи боротьби з цими загрозами. Найбільш ефективним є комплексний підхід до захисту інформації, який враховує різні аспекти безпеки та використовує різноманітні заходи для її захисту – комплексна система захисту інформації. Велику роль при цьому відіграє побудова моделі загроз безпеки інформації.

Виклад основного матеріалу.

Модель загроз безпеки конфіденційної інформації підприємства – це методика оцінки ризиків для конфіденційності, цілісності та доступності інформації та забезпечення інформаційної безпеки на основі ідентифікації та аналізу потенційних загроз. Розглянемо розробку моделі загроз конфіденційної інформації підприємства.

Модель загроз безпеки конфіденційної інформації підприємства «ІТ ГРОМАДА»

1. Загальні положення

1.1 Призначення документу

Модель загроз безпеки конфіденційної інформації (далі – ІзОД) підприємства (далі – Модель загроз) є офіційним керівним документом для керівного складу і співробітників, що обслуговують та експлуатують інформаційно-комунікаційну систему (далі – ІКС) підприємства «ІТ громада» (далі – Підприємства), і призначений для аналізу ризиків, визначення політики безпеки інформації та реалізації заходів захисту ІзОД.

1.2 Види ресурсів ІКС Підприємства

Інформаційно-комунікаційна система (ІКС) Підприємства включає в себе наступні ресурси:

- *Інформаційні ресурси:* дані та інформація, які зберігаються та обробляються в ІКС.
- *Апаратні ресурси:* фізичне обладнання, яке використовується для зберігання, обробки та передачі інформації.
- *Програмне забезпечення:* набір програм, що встановлюється на апаратне забезпечення, яке відповідає за обробку та передачу інформації.

1.3 Склад та вимоги до безпеки ресурсів ІКС Підприємства

Склад та вимоги до безпеки ресурсів ІКС Підприємства наведено в табл. 1. Опис цих ресурсів формує розуміння того, що необхідно захищати на підприємстві, щоб не було витоку конфіденційної інформації.

Таблиця 1

Склад та вимоги до безпеки ресурсів ІКС Підприємства

№	Вид ресурсу	Назва ресурсу	Вимоги
1	Інформаційні ресурси	Загальнодоступна інформація. Контактна інформація, інформація про надання послуг та тарифи	Цілісність, доступність
		Організаційно-правові документи Підприємства: установчий договір, статут, штатна чисельність, штатний розпис, посадові інструкції	Цілісність, доступність, конфіденційність
		Конфіденційна інформація. Фінансові документи Підприємства: головна та касові книги, кошториси, баланси, рахунки, плани закупівель, плани робіт, бухгалтерські звіти. Інформація про клієнтів, постачальників	Цілісність, доступність, конфіденційність
		Технологічна інформація: плани розміщення обладнання, формуляри на ЕОТ, склад встановленого програмне забезпечення, облікові записи, журнали подій, бази, архіви баз, атрибути доступу, облікові записи	Цілісність, доступність, конфіденційність
		Персональні дані. Документи щодо особового складу Підприємства: особисті дані, адресні дані працівників, особові рахунки	Цілісність, доступність, конфіденційність
2	Апаратні ресурси	Сервери баз даних	Цілісність, доступність
		Персональні електронно-обчислювальні машини	Цілісність, доступність
		Комутатори, модеми	Цілісність, доступність
		Дротові та бездротові мережі	Цілісність, доступність
		Службові з’ємні носії	Цілісність, доступність
		Носії ключової інформації	Цілісність, доступність
3	Програмне забезпечення	Операційна система	Цілісність, доступність
		Текстові редактори загального призначення	Цілісність, доступність
		Антивірусне програмне забезпечення	Цілісність, доступність

№	Вид ресурсу	Назва ресурсу	Вимоги
		ПЗ для бухгалтерії	Цілісність, доступність
		ПЗ для керуванням сайтом	Цілісність, доступність
		ПЗ для обробки баз даних	Цілісність, доступність

2. Загрози безпеці інформації, яка обробляється на підприємстві

Можливі загрози безпеці інформації зведено до табл. 2. Перелік загроз наведено з передумовами виникнення і з вказівкою на який ресурс направлена загроза.

Таблиця 2

Перелік загроз безпеці інформації, яка обробляється на Підприємстві

№	Загроза	На що спрямовано	Передумови виникнення / джерело
1	Випадкові зміни умов зовнішнього середовища	Апаратні та інформаційні ресурси. Приміщення Підприємства	Стихійні лиха, аварії, землетрус, повінь, пожежа
2	Випадкові зміни внутрішнього середовища	Апаратні та інформаційні ресурси. Приміщення Підприємства	Руйнування будівельних конструкцій, аварії комунікацій, пожежа
3	Збої в роботі компонентів ІКС	Апаратні ресурси	Помилки під час проєктування і розробки компонентів, кібератаки та кіберзлочини, віруси та інші шкідливі програми
4	Помилки та зловживання персоналу	Апаратні та інформаційні ресурси	Порушення правил експлуатації обладнання та технічних засобів
5	Несанкціоноване отримання інформації	Інформаційні ресурси	Помилки та системні неузгодження під час проєктування, порушення правил експлуатації обладнання, розголошення, передача або втрата атрибутів розмежування доступу, кібератаки та кіберзлочини, віруси та інші шкідливі програми
6	Модифікація інформації	Інформаційні ресурси	Неправильне введення, впровадження програмної закладки, кібератаки та кіберзлочини, віруси та інші шкідливі програми
7	Порушення конфіденційності	Інформаційні ресурси	Недостатня безпека мережі, передача або втрата атрибутів розмежування доступу, кібератаки та кіберзлочини, віруси та інші шкідливі програми
8	Соціальний інжиніринг	Інформаційні та апаратні ресурси	Злам систем безпеки за допомогою маніпулювання людьми, що працюють на підприємстві
9	Інсайдерська загроза	Інформаційні ресурси	Небезпека від працівників підприємства, які мають доступ до конфіденційної інформації і можуть намагатися використовувати цю інформацію для своєї користі або в користь конкурентів
10	Перехоплення побічних електромагнітних випромінювань і наведень від пристроїв	Інформаційні та апаратні ресурси	Недостатня безпека мережі, передача або втрата атрибутів розмежування доступу, кібератаки та кіберзлочини, віруси та інші шкідливі програми
11	Несанкціонована зміна конфігурації	Апаратні ресурси	Недостатня безпека мережі, передача або втрата атрибутів розмежування доступу, кібератаки та кіберзлочини, віруси та інші шкідливі програми. Використання систем передачі, що знаходяться під управлінням інших операторів, і надання послуг користувачам, які не є співробітниками підприємства

№	Загроза	На що спрямовано	Передумови виникнення / джерело
12	Порушення режимів функціонування (виведення з ладу) систем життєзабезпечення	Інформаційні та апаратні ресурси	Навмисне виведення з ладу елементів ІКС, порушення правил експлуатації обладнання
13	Порушення зв'язку за рахунок порушення каналу (тракту) передачі	Інформаційні та апаратні ресурси	Атаки на протоколи мережі, комунікаційні служби, нав'язування помилкової службової інформації і режимів роботи в системі управління, як окремих мереж, так і ІКС в цілому, включаючи зміну маршруту передачі інформації та ін.
14	Погіршення стану носіїв даних	Апаратні та інформаційні ресурси	Відсутність передбаченої процедури періодичної заміни
15	Розкрадання обладнання чи носіїв	Апаратні та інформаційні ресурси	Незахищене зберігання, безвідповідальне розміщення
16	Втрата програмних засобів	Програмні засоби	Відсутність резервних копій
17	Порушення функціонування програмного забезпечення	Програмні засоби	Відсутність механізмів контролю власної цілісності
18	Несанкціоноване копіювання програмного забезпечення	Програмні засоби	Неконтрольоване поводження з програмним забезпеченням
19	Використання контрафактного чи скопійованого програмного забезпечення	Програмні засоби та інформаційні ресурси	Неконтрольоване завантаження та використання програмних засобів
20	Обхід механізмів захисту	Інформаційні ресурси	Некомпетентність обслуговуючого персоналу, навмисні дії потенційних порушників

3. Способи нейтралізації загроз безпеки інформації

Способи нейтралізації загроз безпеки інформації, яка обробляється на Підприємстві зведено до табл. 3.

В таблиці наведено організаційні, фізичні та технологічні засоби захисту, які необхідно виконати для нейтралізації загроз безпеки інформації.

Таблиця 3

Способи нейтралізації загроз безпеки інформації

Загроза	Заходи захисту		
	Організаційні	Фізичні	Технічні
Зміна програмного забезпечення для здійснення модифікації інформації	Визначення повноважень користувачів системи, прав доступу до ресурсів. Проведення навчання користувачів. Встановлення відповідальності. Проведення періодичних оглядів та аудитів	Розмежування доступу до приміщення. Фізичний захист приміщень	Завантаження операційної системи та програм з гнучких магнітних дисків. Використання цифрового підпису. Створення кожному користувачеві системи замкнутого середовища, де він може запускати лише певні програми, які дозволені адміністратором системи. Регулярний контроль цілісності виконуваних файлів та налаштувань програмних засобів. Реєстрація подій, здійснення аналізу журналів подій

Загроза	Заходи захисту		
	Організаційні	Фізичні	Технічні
Впровадження програмної закладки	Визначення повноважень користувачів. Встановлення відповідальності. Надання інструкцій користувачам.	Розмежування доступу до приміщення. Фізичний захист приміщень.	Захист виконуваних і системних файлів від зміни. Створення кожному користувачеві системи замкнутого середовища, де він може запускати лише певні програми, які дозволені адміністратором системи. Контроль цілісності системи. Використання засобів виявлення нападів
Перехоплення	Надання інструкцій користувачам, проведення навчання. Укладання договорів із зовнішніми організаціями	Розмежування доступу в приміщенні. Фізичний захист приміщень	Забезпечення безпеки під час пересування конфіденційної інформації між різними відділами підприємства, а також під час її транспортування до зовнішніх контрагентів. Відправлення даних повинно бути зашифровано і захищено від несанкціонованого доступу. Використання паролів. Використання КЕП. Контроль часу
Несанкціоно-ване копіювання	Встановлення відповідальності. Інструкції користувачам	Розмежування доступу в приміщенні. Фізичний захист приміщень	Реєстрація подій Використання засобів виявлення нападів. Створення облікових записів для кожного користувача з відповідними правами доступу. Використання засобів виявлення вторгнення. Реєстрація подій. Використання КЕП
Дублювання	Інструкції користувачам. Встановлення відповідальності за порушення правил	Ізоляція системи, що захищається, від інших систем	Використання КЕП. Контроль часу. Реєстрація подій
Несанкціоно-ваний доступ до РС	Встановлення відповідальності за порушення правил. Обмеження людей, що мають право конфігурувати ІКС.	Фізичний захист приміщень. Розмежування доступу в приміщення.	Обмеження, розмежування доступу Реєстрація подій. Зміна стандартного імені адміністратора системи захисту. Дозвіл роботи в мережі тільки одного адміністратора. Використання засобів виявлення атак.
Несанкціонова ний доступ до каналу передачі даних	Інструкції користувачам. Встановлення відповідальності за порушення правил	Захист кабельної системи	За рамками повноважень
Напад із зовнішньої мережі	Інструкції користувачам. Встановлення відповідальності за порушення правил	Ізоляція системи, що захищається, від інших систем.	Обмеження числа модемів, що використовуються. Фізична ізоляція робочих станцій для доступу в глобальні мережі від робочих станцій системи. Обмеження доступу до робочих станцій. Реєстрація подій. Використання засобів виявлення нападів. Використання всіх вбудованих в систему засобів захисту
Несанкціоно-вана зміна конфігурації	Інструкції користувачам. Встановлення відповідальності за порушення правил.	Розмежування доступу в приміщеннях. Фізичний захист приміщень.	Обмеження числа модемів, що використовуються. Фізична ізоляція робочих станцій для доступу в глобальні мережі від робочих станцій системи. Обмеження доступу до робочих станцій. Реєстрація подій. Використання засобів виявлення нападів. Використання всіх вбудованих в систему засобів захисту

Оцінка передбачуваного збитку у разі реалізації загроз

Ціна втрат інформації може бути визначена шляхом експертної оцінки, в якій розглядаються такі фактори, як рівень конфіденційності інформації, сфера використання інформації, можливості її використання для виробництва прибутку, репутаційні витрати та інші фактори. При оцінці збитку розглядаються різні комбінації еквівалентів втрат інформації. Вартість збитків залежить від ефективності її використання порушником, а також від сфери використання інформації – політичної, економічної та ін.

3. Оцінка ризиків

Оцінка ризиків здійснюється на основі вимог ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT) «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки» та інших нормативних документів з оцінки ризиків.

Ризики оцінюються за такою формулою:

*РИЗИК = ВРАЗЛИВІСТЬ * НАСЛІДКИ РЕАЛІЗАЦІЇ ЗАГРОЗ*

ВРАЗЛИВІСТЬ = ЗАГРОЗА / (ЗАХОДИ НЕЙТРАЛІЗАЦІЇ ЗАГРОЗИ + АКТИВ),

де: «загроза» має значення 0 за її відсутності, 1 при низькій ймовірності або 2 за її наявності; «заходи нейтралізації загрози» мають значення 0 за відсутності гарантій щодо їх ефективної протидії реалізації загроз щодо певного активу або 2, якщо вони здатні ефективно протидіяти реалізації загроз щодо певного активу; «актив» має значення 1; «/» є математичною операцією ділення; «+» є математичною операцією додавання; «наслідки реалізації загроз» мають значення від 1 до 5 (Значення 1 приймається, коли немає наслідків для діяльності. Значення 5 приймається, коли є критичні наслідки, які можуть призвести до припинення діяльності); «*» є математичною операцією множення. Ризики, які приймають значення більше/рівно 4, вважаються неприйнятними та потребують обов'язкового вжиття заходів щодо їх нейтралізації [1].

Для розрахунку ризиків введемо наступні позначення. Активи Підприємства: А01 – апаратне забезпечення; А02 – програмне забезпечення; А03 – USB та захищені носії інформації, які використовуються в системі; А04 – мережева інфраструктура; А05 – приміщення; А06 – працівники Підприємства; А07 – ділова репутація; А08 – клієнтська база; А09 – журнали аудиту; А10 – архіви (паперові та на носіях).

Джерелом списку загроз візьмемо IT-Grundschutz Catalogues (скорочений варіант каталогу) [2]. Кожній загрозі надано умовне позначення: З01 – пожежа; З02 – несприятливі кліматичні умови; З03 – вода; З04 – забруднення, пил, корозія; З05 – стихійні лиха; З06 – екологічні катастрофи; З07 – важливі події в навколишньому середовищі; З08 – відсутність або збій електропостачання; З09 – відмова або збій мереж зв'язку; З10 – відмова або збій в роботі мережі живлення; З11 – відмова або збій в роботі постачальників послуг; З12 – перешкоджаюче випромінювання; З13 – витік каналами побічних електромагнітних випромінювань і наведень (ПЕМВН); З14 – перехоплення інформації / Шпигунство; З15 – підслуховування.

Оцінка ймовірності впливу загроз на активи наведено в табл. 4.

Таблиця 4

Вплив загроз на активи

	А01	А02	А03	А04	А05	А06	А07	А08	А09	А10
З01	2	0	1	1	1	1	0	0	2	1
З02	2	0	1	1	0	0	0	0	2	1
З03	1	0	0	0	0	0	0	0	0	1
З04	1	0	1	0	0	0	0	0	0	2
З05	1	0	0	0	1	1	0	0	0	1
З06	1	0	0	0	1	1	0	0	0	1
З07	0	0	0	0	1	1	0	0	0	0
З08	1	0	0	0	0	0	0	0	0	0

	A01	A02	A03	A04	A05	A06	A07	A08	A09	A10
309	0	0	0	0	0	0	1	1	0	0
310	1	0	0	0	0	0	1	1	0	0
311	0	0	0	0	1	0	1	1	0	0
312	1	0	1	1	0	0	0	0	0	0
313	1	0	0	1	0	0	1	1	1	0
314	0	0	0	0	0	0	1	1	1	1
315	0	0	0	0	0	0	1	1	0	0

Для кожної загрози проводимо аналіз та визначаємо наслідки впливу загроз за шкалою від 1 балу за відсутності впливу до 5 балів за наявністю максимального впливу загрози. Результати зводимо до табл. 5.

Таблиця 5

Наслідки впливу загроз на активи

	A01	A02	A03	A04	A05	A06	A07	A08	A09	A10
301	4	1	4	4	4	3	1	1	4	4
302	4	1	2	3	1	1	1	1	3	3
303	5	1	1	1	1	1	1	1	1	4
304	4	1	2	1	1	1	1	1	1	3
305	4	1	1	1	4	5	1	1	1	4
306	3	1	1	1	4	4	1	1	1	3
307	1	1	1	1	4	4	1	1	1	1
308	4	1	1	1	1	1	1	1	1	3
309	1	1	1	1	1	1	4	4	1	1
310	4	1	1	1	1	1	4	4	1	3
311	1	1	1	1	3	1	4	4	1	1
312	4	1	3	4	1	1	1	1	4	1
313	4	1	1	4	1	1	4	4	4	1
314	1	1	1	1	1	1	4	4	1	1
315	1	1	1	1	1	1	4	4	1	1

Також для кожної загрози визначаємо ефективність протидії реалізації загроз. Величина ефективності протидії реалізації загроз має значення 0 за відсутності гарантій щодо їх ефективної протидії реалізації загроз щодо певного активу або 2, якщо вони здатні ефективно протидіяти реалізації загроз щодо певного активу. Результати ефективності протидії загроз внесені до таблиці 6.

Таблиця 6

Ефективність протидії загроз

	A01	A02	A03	A04	A05	A06	A07	A08	A09	A10
301	2	0	2	2	2	2	0	0	2	2
302	2	0	0	0	0	2	0	0	2	0
303	0	0	0	0	0	0	0	0	0	0
304	2	0	0	0	2	0	0	0	0	2
305	0	0	0	0	0	0	0	0	0	0
306	0	0	0	0	0	0	0	0	0	0
307	0	0	0	0	0	0	0	0	0	0
308	2	0	0	0	0	0	0	0	0	0
309	0	0	0	0	0	0	2	0	0	0

	A01	A02	A03	A04	A05	A06	A07	A08	A09	A10
З10	0	0	0	0	0	0	0	0	0	0
З11	0	0	0	0	0	0	2	2	0	0
З12	2	0	0	2	0	0	0	0	0	0
З13	2	0	0	0	0	0	0	0	2	0
З14	0	0	0	0	0	0	2	2	2	2
З15	0	0	0	0	0	0	2	2	2	0

Використовуючи формули, наведені вище, здійснюємо оцінку ризиків. Результати зводимо в табл. 7. Процедури оцінки ризиків повинні містити заходи з визначення активів, загроз, вразливостей, ймовірності реалізації загроз та оцінки їх наслідків, заходи з нейтралізації. Значення ризиків є відносною величиною, яка дозволяє оцінювати їх вплив на діяльність Підприємства.

Ризики, які приймають значення більше/рівно 4, вважаються неприйнятними та потребують обов'язкового вжиття заходів щодо їх нейтралізації.

Таблиця 7

Оцінка ризиків

	A01	A02	A03	A04	A05	A06	A07	A08	A09	A10
З01	3	0	1	1	1	1	0	0	3	1
З02	3	0	2	3	0	0	0	0	2	3
З03	**5**	0	0	0	0	0	0	0	0	**4**
З04	1	0	2	0	0	0	0	0	0	2
З05	**4**	0	0	0	**4**	**5**	0	0	0	**4**
З06	3	0	0	0	**4**	**4**	0	0	0	3
З07	0	0	0	0	**4**	**4**	0	0	0	0
З08	1	0	0	0	0	0	0	0	0	0
З09	0	0	0	0	0	0	1	**4**	0	0
З10	**4**	0	0	0	0	0	**4**	**4**	0	0
З11	0	0	0	0	3	0	1	1	0	0
З12	1	0	3	1	0	0	0	0	0	0
З13	1	0	0	**4**	0	0	**4**	**4**	1	0
З14	0	0	0	0	0	0	1	1	0	0
З15	0	0	0	0	0	0	1	1	0	0

У Підприємства наявна можливість реалізації загроз конфіденційності, цілісності і доступності інформації шляхом несанкціонованого доступу, тому необхідно дотримуватися вимог політики безпеки інформації. Рекомендується також використовувати апаратно-програмні засоби криптографічного захисту інформації: електронні ключі, IP-шифратори, шлюзи захисту [3].

Модель підлягає перегляду при зміні планів розміщення, умов функціонування і характеристик Підприємства.

Висновки. Модель загроз безпеки конфіденційної інформації підприємства є важливим інструментом для підвищення рівня безпеки інформації та захисту від небажаних вторгнень та атак на корпоративні мережі та інформаційні системи. Оцінка загроз безпеки повинна проводитися періодично для виявлення нових загроз, що можуть виникнути, та оновлення оцінки існуючих загроз. Результати оцінки можуть допомогти організації приймати рішення щодо запобігання потенційним атакам, забезпечення безпеки даних та захисту інформаційної системи в цілому.

Список використаних джерел

1. Наказ від 14.05.2020 № 269 Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації».
2. IT-Grundschutz catalogues. – URL: https://www.scribd.com/document/534182501/IT-Grundschutz-catalogues-15th-version-2015-Draft.
3. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Монографія. – Харків: Видавництво «Форт», 2012. – 880 с.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
САВЧЕНКО Т. В.

ДОСЛІДЖЕННЯ МЕТОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА РИЗИКИ НЕСАНКЦІОНОВАНОГО ДОСТУПУ

НЕЧАЄВ М., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто методи інформаційної безпеки та ризики несанкціонованого доступу. Сформульована мета дослідження, якою є аналіз основ інформаційної безпеки та ризиків несанкціонованого доступу. Основні засади інформаційної безпеки: викладення ключових принципів та методів, які допомагають забезпечити безпеку цифрових ресурсів, включаючи сильні паролі, шифрування даних, багаторівневу аутентифікацію. Загрози та ризики несанкціонованого доступу: Аналіз типів загроз, з якими стикаються користувачі та організації, такі як фішинг, віруси, хакінг, соціальний інжиніринг. Стратегії та заходи захисту: Вказані рекомендації та практики, які допомагають уникнути ризиків несанкціонованого доступу та забезпечують ефективний захист цифрових активів. Інновації та майбутні виклики: Вказані перспективи розвитку галузі інформаційної безпеки, такі як використання штучного інтелекту, квантової криптографії, захист Інтернету речей та інші інноваційні підходи, а також підкреслено майбутні виклики, пов'язані із забезпеченням кібербезпеки.

The article discusses methods of information security and risks of unauthorized access. The purpose of the research is formulated, which is the analysis of the basics of information security and the risks of unauthorized access. Fundamentals of information security: laying out the key principles and methods that help ensure the security of digital resources, including strong passwords, data encryption, multi-level authentication. Threats and risks of unauthorized access: Analysis of the types of threats that users and organizations face, such as phishing, viruses, hacking, social engineering. Protection strategies and measures: Recommendations and practices are provided to help avoid the risks of unauthorized access and ensure effective protection of digital assets. Innovations and future challenges: Prospects for the development of the field of information security are indicated, such as the use of artificial intelligence, quantum cryptography, protection of the Internet of Things and other innovative approaches, and future challenges related to ensuring cyber security are highlighted.

Актуальність. У сучасному цифровому віці, коли технології залишаються невід'ємною частиною нашого життя, питання інформаційної безпеки виходять на передній план. Швидкий розвиток цифрових засобів спілкування, обміну даними та зберігання інформації до зростання загрози несанкціонованого доступу до конфіденційної та особистої інформації. Актуальність цієї теми обумовлена не лише розширенням можливостей для зловмисників, але й прагненням захистити індивідуальні, корпоративні та державні інтереси в онлайн-середовищі. Однією з найбільших загроз сучасності є несанкціонований доступ до цифрової інформації. Хакерські атаки, фішингові кампанії, крадіжка особистих даних – це лише деякі зі відомих методів атаки, які можуть призвести до серйозних наслідків. Зловмисники можуть отримати доступ до фінансових ресурсів, конфіденційних корпоративних документів, медичних записів чи особистих повідомлень. Порушення конфіденційності та розширення недозволених даних може завдати шкоди як окремим користувачам, так і суспільству в цілому. Зростання кількості пристроїв входу, підключених до Інтернет-речей (IoT), створює нові точки для зловмисників. Від вбудованих систем у побутовій техніці до промислових контролерів, усі вони можуть стати об'єктами атак. Розробка нових методів захисту та забезпечення безпеки IoT-пристроїв стає завданням для дослідників та інженерів. Ризики несанкціонованого доступу також впливають на державну безпеку. Кібершпигунство та кібератаки можуть бути спрямовані проти критичної інфраструктури, електронних систем голосування, військових систем та інших стратегічно важливих об'єктів. Наслідки таких атак можуть бути драматичними і мають потенціал спровокувати глобальну кризу. Отже, актуальність теми «Інформаційна безпека та ризики несанкціонованого доступу» є безаперечною. Зростання кількості цифрових загроз вимагає постійного вдосконалення стратегій захисту, розробки нових технологій та навчання користувачів основам цифрової безпеки. Тільки шляхом спільних зусиль науковців, інженерів та користувачів можна надійно захистити цифровий світ від загроз несанкціонованого доступу.

Метою статті є висвітлення основ інформаційної безпеки та ризиків несанкціонованого доступу в цифровому середовищі. Основний акцент робиться на аналізі загроз, які виявляються у зв'язку з несанкціонованим доступом до інформації, та розгляді стратегій, спрямованих на їх запобігання та управління. Дана стаття має наступні конкретні мети: Визначте поняття інформаційної безпеки: Стаття пояснює, що така інформаційна безпека та чому вона є важливою для окремих користувачів, організацій та держав; Висвітлити загрози несанкціонованого доступу: Стаття аналізує різноманітні методи та техніку, які створюють зловмисники для отримання несанкціонованого доступу до інформації. Вона розглядає різні типи атак, включаючи хакінг, риболовлю, соціальний інжиніринг; Виявити слідки та ризики: Стаття розглядає можливість слідки несанкціонованого доступу для осіб, організацій та суспільства загалом. Вона досліджує можливості наслідків порушення конфіденційності, цільності та доступності інформації; Пропонувати стратегії запобігання ризикам: Стаття надає конкретні поради та стратегії, які можуть допомогти індивідам і організаціям зменшити ризики несанкціонованого доступу. Це включає в себе використання сильних паролів, багаторівневу аутентифікацію, оновлення програмного забезпечення та інші заходи; Підкреслити важливість освіти та свідомості: Стаття акцентує увагу на необхідності навчання користувачів основам інформаційної безпеки, розпізнавання загроз та вчасного реагування на них; Визначити шлях подолання викликів: Стаття вказує на важливість співпраці між науковцями, інженерами, законодавцями та користувачами для розробки та впровадження ефективних стратегій інформаційної безпеки; В цілому, стаття має на меті поглибити розуміння читачів про важливість інформаційної безпеки, небезпеки, які пов'язані з несанкціонованим доступом, а також способи їх мінімізації та подолання.

Об'єктом дослідження є комплексний спектр цифрових ресурсів, даних, інформаційних систем, мереж та технологій, які є вразливими перед різними загрозами та можуть стати об'єктом атак несанкціонованого доступу.

Предмет дослідження – інформаційна безпека та ризики несанкціонованого доступу в контексті сучасного цифрового середовища.

Аналіз попередніх досліджень. Інформаційної безпеки та ризиків несанкціонованого доступу є місцем для побудови наукової статті. Цей аналіз допомагає використовувати поточний стан знань у цій області, ідентифікувати невирішені аспекти та потреби програми в нових дослідженнях. Огляд літератури; Ключові концепції та теорії; Сфери застосування; Технічні аспекти; Соціальні та психологічні аспекти; Уразливості та вразливі групи; Дієвість заходів безпеки.

Виклад основного матеріалу. Інформаційна безпека – це комплекс заходів та практичних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації. Конфіденційність виникає у забезпеченні обмеженого доступу до інформації, цілеспрямованість – у запобіганні недозволеним змінам даних, а доступність – у забезпеченні доступу до інформації для авторизованих користувачів. Основи інформаційної безпеки включають принципи, методи та практики, спрямовані на забезпечення захисту конфіденційності, цілісності та доступності інформації в цифровому середовищі. Це важлива галузь, яка має на меті запобігання несанкціонованому доступу, втраті даних та іншим загрозам, які можуть виникнути в результаті використання інформаційних технологій. Основні аспекти інформаційної безпеки включають:

1. Конфіденційність: Цей принцип передбачає забезпечення та збереження конфіденційності інформації. Інформація повинна бути доступна тільки тим особам або суб'єктам, які мають право на її перегляд. Криптографія, контроль доступу та обмеження прав користувачів - це інструменти, які допомагають забезпечити конфіденційність.

2. Цілісність: Цей аспект означає збереження точності та цільності інформації. Дані не повинні бути незаконно змінені, підроблені або втрачені. Для досягнення цільності використовують методи контролю цільності даних та застосування цифрових підписів.

3. Доступність: Принцип доступності, що інформація має бути доступною для авторизованих користувачів у відповідний момент часу. Забезпечення доступності може включати в себе використання резервних копій, механізмів відновлення після збоїв та інші практики.

4. Аутентифікація та авторизація: Аутентифікація при ідентифікації користувача або суб'єкта, щоб забезпечити пізнаваність та перевірку його запису. Авторизація забезпечує рівень доступу, який має користувач після успішної аутентифікації.

5. Захист від загроз: цей аспект включає в себе застосування технічних, організаційних та процедурних заходів для запобігання загрозам, таким як хакінг, віруси, рибальство та інші атаки.

6. Аудит та моніторинг: Системи інформаційної безпеки повинні бути постійно та моніторингу для контролю виявлення аномалій, інцидентів та порушення безпеки. Аудит відстежувати дії користувачів та виявляти незвичну активність.

7. Навчання та свідомість: Освіта користувачів щодо загроз і практичної інформаційної безпеки є ключовою для забезпечення безпеки. Люди повинні розуміти основні ризики та вміти уникати пасток. Ці основи інформаційної безпеки є ключовими для забезпечення надійного захисту інформації в сучасному цифровому світі. Вони допомагають окремим користувачам, бізнесам та організаціям виявляти та запобігати потенційним загрозам та забезпечувати безпеку даних.

Загрози та ризики несанкціонованого доступу: загрози несанкціонованого доступу створює негативні ризики для окремих осіб та організацій. Хакери можуть використовувати техніку хакінгу для проникнення в системи та крадіжки даних. Фішингові атаки включають маніпулювання користувачами з метою отримання їхньої конфіденційної інформації. Соціальний інжиніринг використовує психологічні методи для отримання доступу до системи. Загрози та ризики несанкціонованого доступу є серйозними проблемами для інформаційної безпеки в сучасному цифровому світі. Ці загрози можуть створюватися

індивідуальних користувачів, бізнесів, державних структур і суспільства в цілому. Деякі з ключових загроз та ризиків несанкціонованого доступу включають:

1. Хакінг та Кібератаки: Зловмисники можуть використовувати різні методи хакінгу для незаконного доступу до комп'ютерних систем та мереж. Це може включати в себе використання вразливостей програмного забезпечення, включення в систему та вироблення даних.

2. Фішинг: Фішингові атаки передають використання підступних електронних повідомлень або веб-сайтів для отримання конфіденційної інформації, такої як паролі або фінансові дані, від користувачів.

3. Соціальний інжиніринг: Зловмисники можуть використовувати психологічні методи для впливу на людей і отримання доступу до конфіденційної інформації. Це може включати в себе маніпулювання, обман та використання довіри.

4. Викрадання облікових даних: Зловмисники можуть викрасити облікові дані користувачів, такі як ім'я користувачів та паролі, для незаконного доступу до різних облікових записів.

5. Віруси та шкідливий код: Зловмисники можуть розробляти та поширювати віруси, черв'яки та інший шкідливий код, який може пошкодити системи, викрасити дані або навіть знищити інформацію.

6. Внутрішні загрози: Інсайдери, такі як співробітники, можуть завдати шкоди, розкривши конфіденційну інформацію або зловживаючи доступом до системи.

7. Викрадання даних та вимагання викупу: Зловмисники можуть викрадати важливі дані та вимагати викуп для їх повернення або невикладення публічно.

8. Порушення конфіденційності: несанкціонований доступ може привести до витоку конфіденційної інформації, такої як медичні дані, фінансові дані або персональні відомості.

9. Втрати фінансових ресурсів: Зловмисники можуть використовувати незаконний доступ для крадіжки грошей або викрадання фінансової інформації.

10. Загрози для критичної інфраструктури: Атаки на критичну інфраструктуру, так само як енергетичні мережі, можуть викликати серйозні наслідки для суспільства та безпеки.

Ці загрози та ризики підлягають постійному моніторингу, оновлення заходів безпеки та освіти користувачів щодо яких загроз і способів їх запобігання.

Наслідки несанкціонованого доступу: Несанкціонований доступ може призвести до серйозних наслідків. Крадіжка конфіденційних даних може призвести до фінансових втрат для бізнесменів і особистих користувачів. Порушення конфіденційності може вразити репутацію організацій та осіб. Внесення змін у цільність даних може призвести до недостовірних інформаційних потоків. Несанкціонований доступ до інформації може привести до серйозних наслідків для окремих користувачів, бізнесів, установ і суспільства в цілому. Ці слідки можуть мати фінансовий, репутаційний, юридичний та етичний вплив. Деякі з основних наслідків несанкціонованого доступу включають:

1. Фінансові втрати: Зловмисники можуть використовувати незаконний доступ для крадіжки грошей, фінансової інформації або використання фінансових ресурсів.

2. Крадіжка особистої інформації: Несанкціонований доступ може призвести до крадіжки особистої інформації, такої як імена, адреси, номери соціального страхування, медичні записи тощо. Ця інформація може бути використана для шахрайства або ідентифікаційної крадіжки.

3. Порушення конфіденційності: несанкціонований доступ може призвести до витоку конфіденційної інформації, такої як комерційні та технічні дані. Це може вразити репутацію організації та осіб.

4. Втрата даних: Зловмисники можуть спричинити втрату даних або їх видалення, що може мати серйозний вплив на роботу бізнесу, наукових досліджень або особисті дані.

5. Розширення дезінформації: Несанкціонований доступ може призвести до внесення змін в інформацію та її поширення, що може призвести до розширення дезінформації та неправильної інтерпретації фактів.

6. Втрата контролю над системами: Незаконний доступ може призвести до втрати контролю над комп'ютерними системами, мережами та пристроями, які можуть відкрити двері для подальших атак та вікрадення даних.

7. Юридичні наслідки: несанкціонований доступ може призвести до юридичних наслідків, у тому числі судових позовів, штрафів та кримінального переслідування.

8. Завдання шкоди репутації: У випадках втрати конфіденційності інформації або вразливості в безпеці, репутація фізичних осіб, бізнесів або організацій може бути важко пошкоджена.

Стратегії та заходи захисту: Для запобігання ризикам несанкціонованого доступу індивіди та організації можуть використовувати різні стратегії. Важливим кроком є використання сильних паролів та багаторівневої аутентифікації. Регулярне оновлення програмного забезпечення та встановлення патчів є кількістю для зменшення вразливостей. Криптографічний захист даних може забезпечити їх безпеку під час передачі. Для запобігання загрозам та ризикам несанкціонованого доступу індивіди та організації можуть використовувати різні стратегії та заходи захисту. Нижче наведено деякі ключові стратегії та практики, які можуть допомогти забезпечити безпеку інформації:

1. Сильні паролі та багаторівнева аутентифікація: Використовуйте складні паролі, які складаються з комбінації великих та маленьких літер, цифр та спецсимволів. Додатково використовуйте багаторівневий аутентифікатор, який вимагає двох або більше способів перевірки особи.

2. Оновлення програмного забезпечення: Регулярно оновлюйте операційні системи, програми та програмне забезпечення, щоб виправити вразливість та захистити системи від атак.

3. Використання антивірусного програмного забезпечення: Встановіть та оновіть антивірусне програмне забезпечення для виявлення та блокування шкідливого коду.

4. Файрволі: Встановіть файрволі для моніторингу та контролю мережевого трафіку, що входить і виходить із вашої мережі.

5. Шифрування даних: використовуйте шифрування для захисту конфіденційної інформації під час її передачі через мережу або збереження на пристроях.

6. Резервне копіювання: Регулярно створюйте резервні копії важливої інформації, щоб уникнути її втрати в разі атаки або випадкового видалення.

7. Обмеження доступу: Надавайте доступ до інформації лише авторизованим користувачам та обмежуйте їх права відповідно до їх ролі та обов'язків.

8. Освіта та навчання користувачів: Проведіть навчальні програми та інформуйте користувачів про наявні загрози та способи їх запобігання, вчіть їх розпізнавати сприйнятливу ситуацію.

9. Моніторинг та аудит: Встановіть системи моніторингу для виявлення аномалій та незвичайної активності, а також зберігайте перевірені дані про дії користувачів.

10. Фізична безпека: Захищайте фізичний доступ до комп'ютерів, серверів та інших пристроїв, встановлюючи фізичні бар'єри та обмежуючи доступ до приміщень.

Ці стратегії та заходи захисту взаємодіють із єдиною, допомагаючи створити комплексний підхід до інформаційної безпеки та мінімізувати ризики несанкціонованого доступу. Освіта та навчання: Важливою складовою інформаційної безпеки є освіта користувачів. Індивіди повинні бути освіченими щодо методів фішингу, соціального інжинірингу та інших загроз. Організації можуть проводити навчальні програми для співробітників та давати рекомендації щодо безпеки. Освіта та навчання грають критичну роль у забезпеченні інформаційної безпеки та запобіганні ризикам несанкціонованого доступу. Свідомість користувачів щодо наявних загроз та навичок розпізнавання також є великими факторами у забезпеченні безпеки інформації. Ось деякі аспекти освіти та навчання в контексті інформаційної безпеки:

1. Відомість про загрози: Освіта повинна розкрити користувачам різні типи загроз, такі як фішинг, соціальний інжиніринг, віруси, хакінг тощо. Пояснити їхню сутність, можливість наслідки та шляхи запобігання.

2. Безпечне користування мережею: Навчання користувачів правилам безпечного користування Інтернетом та мережевими сервісами. Це може включати в себе використання безпечних паролів, обережне завантаження файлів, обмеження особистої інформації в мережі тощо.

3. Соціальний інжиніринг: Навчання користувачів розпізнавати типові сценарії соціального інжинірингу, які використовують зловмисники для отримання конфіденційної інформації або доступу.

4. Навички розпізнавання фішингу: Користувачі повинні помічати розпізнавати підозрілі електронні повідомлення та веб-сайти, які можуть бути фішинговими атаками.

5. Правила використання паролів: Навчання користувачів про створення сильних паролів, регулярну їх зміну та неповторне використання паролів для різних облікових записів.

6. Впровадження багаторівневої аутентифікації: Пояснення переваг використання багаторівневої аутентифікації та навчання користувачів її на аналізі.

7. Публікація основних принципів інформаційної безпеки: Розробка та розповсюдження матеріалів, які пояснюють основні принципи інформаційної безпеки та надають поради щодо безпеки в мережі.

8. Симуляція атаки: організація симуляційної атаки для користувачів, щоб показати, як швидко можна стати жертвою атаки, якщо не дотримуватися правил безпеки.

9. Тренінг безпеки для персоналу: Для бізнесу та організацій важливо проводити навчання з питань безпеки для свого персоналу, включаючи особливі навички та процедури для конкретної діяльності.

10. Створення культури безпеки: Залучення всього колективу до усвідомлення важливості інформаційної безпеки та сприяння виробленню культури безпеки в організації або спільноті.

Навчання та освіта є постійним процесом, після загрози та технологічний контекст змінюється. Ціль - підготувати користувачів до ефективного реагування на нові виклики та впровадження найкращих практичних заходів безпеки в їх повсюдну діяльність. Інновації та майбутні виклики: З розвитком технологій з’являються нові можливості та виклики в галузі інформаційної безпеки. Використання штучного інтелекту та машинного навчання може сприяти виявленню аномалій та атак. Однак разом з цим викликаються нові загрози, такі як використання штучного інтелекту зловмисниками. Інновації в галузі інформаційної безпеки важливі для адаптації до зростаючих загроз та викликів у цифровому світі. Ось деякі інноваційні тенденції та майбутні виклики, з якими може стикнутися галузь інформаційної безпеки:

1. Штучний інтелект та машинне навчання: використання штучного інтелекту та машинного навчання допоможе автоматично виявити та протидіяти загрозам, а також швидко проаналізувати великий обсяг даних для незвичайної активності.

2. Кібербезпекові аналітичні інструменти: Розробка більш ефективних аналітичних інструментів допоможе передбачати, виявляти та аналізувати нові типи загроз та атак.

3. Квантова криптографія: Розвиток квантової криптографії може забезпечити більшу стійкість до квантових обчислювальних атак та забезпечити безпеку даних у майбутньому.

4. Блокчейн для кібербезпеки: технологія блокчейн може бути використана для забезпечення безпеки транзакцій, ідентифікації та контролю доступу до даних.

5. Захист Інтернету речей (IoT): З ростом кількості підключених до Інтернету пристроїв стає все розробити ефективні методи захисту IoT-пристроїв від атак.

6. Боротьба зі зловмисниками на державному рівні: Зростає важливість співпраці між державами та міжнародними організаціями для виявлення та протидії кібератакам, які можуть порушити роботу країни та глобальної інфраструктури.

7. Гібридні загрози: Зловмисники залишаються більш витонченими та планують гібридні атаки, використовуючи різні канали та методи для досягнення своїх цілей.

8. Підготовка та навчання: Персоналу та користувачам слід надавати постійну підготовку та навчання, після чого загрози змінюються та еволюціонують.

9. Конфіденційність даних: Зростає усвідомлення важливості конфіденційності даних, тому заходи захисту та шифрування залишаються ще актуальнішими.

10. Етичні аспекти інформаційної безпеки: З'являється більше обговорень щодо етики використання інформаційної безпеки, зокрема в галузі збору та обробки персональних даних. Ці інновації та виклики вказують на постійну необхідність розвитку та вдосконалення стратегій інформаційної безпеки, а також на важливість співпраці та обміну досвідом між організаціями та державами для ефективного захисту від сучасних та майбутніх загроз.

Висновки. даної наукової статті підкреслюють критичну важливість інформаційної безпеки та ризиків несанкціонованого доступу в сучасному цифровому світі. Розглянуті аспекти підкреслюють надання постійного зосередження на цю проблему для забезпечення безпеки та конфіденційності інформації. Основні висновки статті включають такі аспекти: Зростання загроз: Сучасний цифровий світ стикається з постійним зростанням кількості та складності загроз несанкціонованого доступу. Хакерські атаки, фішингові кампанії та соціальний інжиніринг стають все більш винахідливими та небезпечними. Наслідки порушено: Несанкціонований доступ може призвести до серйозних наслідків, які впливають на окремих осіб, організацію та суспільство в цілому. Від фінансових втрат до порушення конфіденційності та поширення дезінформації - слідки можуть бути руйнівними. Можливість освіти: Освіта та навчання грають важливу роль у запобіганні ризикам несанкціонованого доступу. Свідомість користувачів про наявні загрози та навички розпізнавання можуть значно знизити ризики. Технологічний прогрес: Впровадження нових технологій, таких як штучний інтелект та блокчейн, може підвищити рівень інформаційної безпеки. Однак разом з цим, з'являються нові виклики та загрози, пов'язані з використанням цих технологій зловмисниками. Загальна відповідальність: Забезпечення інформаційної безпеки є спільною відповідальністю окремих осіб, організацій та держав. Тільки спільними зусиллями можна досягти надійного захисту від загрози несанкціонованого доступу. Узагальнюючи, ця стаття підкреслює актуальність та важливість інформаційної безпеки та ризиків несанкціонованого доступу в сучасному світі. Розуміння загроз та використання ефективних стратегій захисту є вирішальними для забезпечення безпеки інформації та підтримки стабільності цифрового середовища.

Список використаних джерел

1. Андерсон, Р. (2008). Інженерія безпеки: посібник зі створення надійних розподілених систем. Wiley.
2. Pfleeger, CP, & Pfleeger, SL (2015). Безпека в обчисленнях. Пірсон.
3. Вітмен, М., і Маторд, Х. (2016). Принципи інформаційної безпеки. Cengage Learning.
4. Dhillon, G., & Backhouse, J. (2001). Управління безпекою інформаційних систем у новому тисячолітті. Повідомлення ACM, 44 (4), 125-128.
5. Вакка, JR (2013). Довідник з комп'ютерної та інформаційної безпеки. Морган Кауфман.
6. Шнайєр, Б. (2015). Дані та Голіаф: приховані битви за збір ваших даних і контроль над світом. WW Norton & Company.
7. Мелл П. та Гренс Т. (2011). Визначення хмарних обчислень NIST (Спеціальна публікація 800-145). Національний інститут стандартів і технологій.
8. Cisco. (2020). Річний звіт Cisco про Інтернет (2018–2023). Отримано з https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
9. Symantec. (2019). Звіт про загрози безпеці в Інтернеті: Том 24. Отримано з https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf
10. Verizon. (2020). Звіт про розслідування витоку даних. Отримано з https://enterprise.verizon.com/resources/reports/dbir/

Робота виконана під науковим керівництвом ст. наук. співроб., доцента
ЗВЄРЄВА В. П.

РОЛЬ BYOD У ЗАХИСТІ ПЕРСОНАЛЬНИХ ДАНИХ ПРАЦІВНИКІВ ВІД КІБЕРАТАК

ОЛЕКСЮК В., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розгянуто політику BYOD, її роль у захисті персональних даних працівників у випадку кібератак, а також у діяльності підприємства в цілому. Дана практика може знизити витрати на обладнання для компанії, а також покращити продуктивність працівників, але вона також може створювати загрозу для безпеки даних.

This article examines the BYOD policy and its role in protecting employees' personal data in the event of cyberattacks, as well as in the work of the enterprise as a whole. This practice can reduce a company's hardware costs and increase employee productivity, but it can also pose a threat to data security.

Актуальність. Тема BYOD (Bring Your Own Device, українською – «бери свій власний пристрій») та захисту персональних даних працівників від кібератак є дуже актуальною в сучасному бізнес-середовищі.

BYOD – це підхід, коли працівники використовують власні мобільні пристрої, такі як смартфони, планшети або ноутбуки, для роботи в офісі або поза ним. Цей підхід став дуже популярним, оскільки дозволяє працівникам бути більш продуктивними та ефективними, а також зменшує витрати компанії на придбання дорогих пристроїв.

Однак, з використанням BYOD виникає ризик втрати та зловживання персональних даних працівників. Це може стати наслідком недостатнього захисту пристроїв, що використовуються працівниками, від кібератак.

Кібератаки можуть стати причиною витоку конфіденційної інформації про компанію, її клієнтів та працівників. Зловмисники можуть використовувати віруси, троянські програми, фішинг та інші методи для отримання доступу до пристроїв працівників та викрадення конфіденційної інформації.

Метою статті є аналіз ризиків, пов'язаних з використанням BYOD у бізнес-середовищі, та висвітлення важливості захисту персональних даних працівників від кібератак. Стаття має на меті надати інформацію про те, як вирішити проблему захисту персональних даних від кібератак з використанням BYOD, а також про заходи безпеки, яких необхідно вжити для захисту пристроїв співробітників від кібератак. Крім того, стаття має на меті допомогти керівникам підприємств та IT-спеціалістам у визначенні оптимальних стратегій BYOD для захисту персональних даних співробітників від кібератак.

Об'єктом дослідження є використання BYOD (Bring Your Own Device) в бізнес-середовищі та захист персональних даних працівників від кібератак.

Предметом дослідження є ризики, пов'язані з використанням BYOD в бізнес-середовищі, та заходи безпеки, необхідні для захисту персональних даних працівників від кібератак з використанням BYOD.

Використання власних пристроїв (BYOD) стало популярною тенденцією на сучасних підприємствах, що дозволяє працівникам використовувати свої особисті пристрої, такі як смартфони, ноутбуки та планшети, для виконання робочих завдань. Така практика має численні переваги, зокрема підвищення продуктивності, гнучкості та економію коштів. Однак вона також створює значні ризики для особистих і організаційних даних, особливо в умовах кібератак. У цій статті досліджується роль BYOD у захисті персональних даних співробітників від кібератак, висвітлюються ризики, пов'язані з цією практикою, та стратегії їх зменшення [1].

Тенденція BYOD набула популярності завдяки численним перевагам, які вона пропонує працівникам та організаціям. Працівники все частіше вимагають гнучкості, щоб працювати з будь-якого місця, в будь-який час і на будь-якому пристрої. З іншого боку, організації впроваджують BYOD, щоб зменшити витрати, пов'язані з придбанням та обслуговуванням пристроїв, підвищити задоволеність і продуктивність працівників, а також покращити співпрацю.

Однак BYOD також створює значні ризики для кібербезпеки, які можуть поставити під загрозу безпеку і конфіденційність особистих і організаційних даних. Деякі з найпоширеніших ризиків, пов'язаних з BYOD, включають наступне.

Несанкціонований доступ. Коли працівники використовують особисті пристрої для виконання робочих завдань, вони часто підключаються до публічних мереж Wi-Fi або використовують незахищені мережі, піддаючи конфіденційні дані несанкціонованому доступу.

Втрачені або вкрадені пристрої. Персональні пристрої частіше губляться або викрадаються, відкриваючи доступ до конфіденційних даних стороннім особам. Відсутність шифрування пристрою або надійних паролів також може поставити під загрозу безпеку персональних даних.

Шкідливі програми та віруси. Персональні пристрої можуть бути заражені шкідливими програмами або вірусами, які можуть поширитися на мережу організації, ставлячи під загрозу безпеку особистих і організаційних даних.

Внутрішні загрози. Працівники, які використовують персональні пристрої для виконання робочих завдань, можуть навмисно чи ненавмисно порушити безпеку особистих та організаційних даних, наражаючи їх на кібератаки.

Організації можуть вжити кілька заходів для зменшення ризиків кібербезпеки, пов'язаних з власними пристроями. До них відносяться наступні [2].

Створення політики щодо використання власних пристроїв. Організації повинні розробити чітку політику та інструкції щодо використання персональних пристроїв на робочому місці. Політика повинна визначати прийнятне використання персональних пристроїв, заходи безпеки, необхідні для персональних пристроїв, і наслідки порушення політики.

Проведення регулярних тренінгів з безпеки. Працівники повинні бути навчені найкращим практикам кібербезпеки, зокрема, як виявляти та повідомляти про потенційні кіберзагрози, як захистити персональні пристрої від кібератак та як уникнути ненавмисного розголошення особистих та організаційних даних стороннім особам.

Впровадження контролю доступу. Організації повинні впровадити контроль доступу, який обмежує доступ до конфіденційних даних на основі ролі та обов'язків користувача. Цього можна досягти за допомогою політики паролів, багатофакторної автентифікації та інших засобів контролю доступу.

Шифрування. Шифрування є важливим заходом безпеки, який може захистити персональні дані від несанкціонованого доступу в разі втрати або крадіжки пристрою. Організації повинні вимагати від працівників шифрування їхніх персональних пристроїв, зокрема жорстких дисків, електронних листів і повідомлень.

Віддалене стирання. Віддалене стирання – це функція безпеки, яка дозволяє організаціям видаляти дані з втрачених або викрадених персональних пристроїв. Це гарантує, що конфіденційні дані не будуть скомпрометовані, якщо пристрій потрапить до чужих рук.

Захист персональних даних є важливим аспектом сучасних робочих місць. Зі зростанням залежності від технологій та інтернету персональні дані стають вразливими до кібератак, витоків даних та інших загроз безпеці. BYOD посилює ці ризики, оскільки працівники використовують свої особисті пристрої для виконання робочих завдань, а організація має менше контролю над заходами безпеки, що застосовуються на цих пристроях. Тому організаціям вкрай важливо враховувати захист персональних даних при впровадженні політики BYOD.

Закони про захист персональних даних, такі як Загальний регламент про захист даних (GDPR) і Каліфорнійський закон про конфіденційність споживачів (CCPA), встановлюють керівні принципи і вимоги для організацій, які збирають і обробляють персональні дані. Ці закони вимагають від організацій впроваджувати відповідні заходи безпеки для захисту персональних даних від несанкціонованого доступу, використання, розкриття чи знищення. У контексті BYOD організаціям необхідно забезпечити відповідність своїх політик і заходів безпеки цим законам, щоб уникнути потенційної юридичної відповідальності.

Одним із способів захисту персональних даних у середовищі BYOD є впровадження рішень для управління мобільними пристроями (MDM). Рішення MDM дозволяють організаціям контролювати та керувати персональними пристроями, що використовуються для виконання робочих завдань. Програмне забезпечення MDM може впроваджувати політики безпеки, такі як вимоги до паролів, шифрування та віддалене стирання, щоб забезпечити захист персональних даних у разі втрати або крадіжки пристрою. Крім того, рішення MDM можуть надавати організаціям можливість бачити в реальному часі пристрої, якими користуються співробітники, що дозволяє їм оперативно виявляти потенційні загрози безпеці.

Ще один спосіб захистити персональні дані в середовищі BYOD – впровадити рішення для запобігання втраті даних (DLP). Рішення DLP дозволяють організаціям відстежувати і контролювати передачу даних, запобігати витоку даних і забезпечувати дотримання законів про захист даних. Рішення DLP також можуть виявляти і запобігати несанкціонованому доступу до персональних даних, забезпечуючи додатковий рівень захисту в середовищі BYOD [3].

Організації також можуть використовувати рішення віртуальних приватних мереж (VPN) для захисту персональних даних у середовищі BYOD. Рішення VPN забезпечують безпечне з’єднання між персональними пристроями та мережею організації, дозволяючи працівникам безпечно отримувати доступ до робочих ресурсів. Рішення VPN також шифрують передачу даних, запобігаючи несанкціонованому доступу до персональних даних.

Нарешті, організаціям слід розглянути можливість впровадження плану реагування на інциденти безпеки (SIRP) для швидкого реагування на інциденти безпеки в середовищі BYOD. SIRP визначає кроки та процедури, яких організація повинна дотримуватися у випадку інциденту безпеки, наприклад, витоку даних або кібератаки. Добре розроблений SIRP може допомогти організаціям мінімізувати вплив інциденту безпеки на персональні дані та зменшити ризик юридичної відповідальності.

Впровадження політики BYOD та заходів безпеки для захисту персональних даних не позбавлене викликів. Однією з головних проблем є відсутність контролю над персональними пристроями. Організації не можуть впроваджувати політику безпеки на персональних пристроях, які їм не належать, що ускладнює забезпечення належного захисту персональних даних. Крім того, працівники можуть не дотримуватися політики та заходів безпеки щодо використання власних пристроїв, наражаючи персональні дані на потенційні загрози безпеці.

Ще однією проблемою є складність впровадження та управління політиками та заходами безпеки щодо використання власних пристроїв. Політики та заходи безпеки BYOD можуть відрізнятися залежно від типу персонального пристрою, операційної системи та інших факторів. Тому організаціям необхідно впроваджувати гнучкий і масштабований підхід до політик і заходів безпеки BYOD, щоб гарантувати, що вони можуть відповідати різним персональним пристроям і операційним системам.

Нарешті, впровадження політик і заходів безпеки BYOD може бути дорогим і трудомістким процесом. Організаціям необхідно інвестувати в MDM, DLP, VPN та інші рішення, щоб забезпечити належний захист персональних даних. Крім того, організаціям необхідно регулярно навчати співробітників передовим практикам кібербезпеки, що збільшує витрати і час, необхідні для впровадження політик і заходів безпеки щодо принесених з собою пристроїв.

Тенденція BYOD набула популярності завдяки численним перевагам, які вона пропонує працівникам та організаціям. Однак вона також створює значні ризики для кібербезпеки, які можуть поставити під загрозу безпеку та конфіденційність особистих та організаційних даних. Організації можуть зменшити ці ризики, встановивши чіткі політики та інструкції щодо використання персональних пристроїв, проводячи регулярні тренінги з безпеки, впроваджуючи контроль доступу, шифруючи персональні пристрої та уможливлюючи віддалене стирання даних. Застосовуючи ці стратегії, організації можуть підвищити безпеку особистих і організаційних даних, користуючись при цьому перевагами BYOD.

Однією з альтернатив BYOD є надання компаніями своїм працівникам власних пристроїв, спеціально призначених для робочих цілей. Такий підхід може запропонувати кілька переваг над BYOD, що зазначено нижче [4].

Підвищена безпека. Пристрої, що належать компанії, можуть підлягати більш суворим політикам і процедурам безпеки, таким як обов'язкове шифрування і можливість віддаленого стирання, що може допомогти забезпечити захист конфіденційних даних у разі порушення безпеки.

Зменшення відповідальності. Коли працівники використовують свої особисті пристрої для роботи, завжди існує ризик того, що конфіденційні дані можуть бути скомпрометовані, якщо пристрій буде втрачено або викрадено. Надаючи пристрої, що належать компанії, роботодавці можуть зменшити свою відповідальність і мінімізувати ризик витоку даних.

Спрощене управління пристроями. В умовах BYOD IT-відділам часто доводиться керувати безліччю різних пристроїв і операційних систем, що може займати багато часу і бути складним завданням. Надаючи пристрої, що належать компанії, IT-відділи можуть зосередитися на управлінні стандартизованим набором пристроїв, які налаштовані для оптимальної безпеки та продуктивності.

Підвищення продуктивності. Пристрої, що належать компанії, можуть бути попередньо налаштовані з необхідним програмним забезпеченням і додатками, які потрібні співробітникам для виконання своєї роботи, що може допомогти усунути необхідність для співробітників витрачати час на налаштування власних пристроїв або усунення технічних неполадок.

Кращий контроль над даними. Коли працівники використовують свої особисті пристрої для роботи, завжди існує ризик того, що дані компанії можуть бути випадково або навмисно передані стороннім особам. Надаючи пристрої, що належать компанії, роботодавці можуть краще контролювати дані та гарантувати, що доступ до них матимуть лише уповноважені особи.

Останніми роками використання власних пристроїв (Bring Your Own Device, BYOD) на робочому місці стає все більш поширеним явищем. Хоча BYOD може запропонувати багато переваг як для роботодавців, так і для працівників, він також створює низку викликів, особливо коли йдеться про безпеку даних.

Однією з головних переваг BYOD є підвищена гнучкість і продуктивність, яку вона може запропонувати працівникам. Завдяки власним пристроям працівники можуть працювати з будь-якого місця і в будь-який час, не прив'язуючись до стаціонарного комп'ютера чи іншої стаціонарної робочої станції. Це може допомогти працівникам краще керувати балансом між роботою та особистим життям і підвищити їхню загальну задоволеність роботою.

Для роботодавців BYOD може запропонувати економію коштів за рахунок зменшення необхідності купувати та обслуговувати власні пристрої для кожного працівника. Крім того, BYOD може допомогти компаніям залучати та утримувати найкращі таланти, пропонуючи більш гнучке та сучасне робоче середовище.

Висновки. Незважаючи на переваги, BYOD може створювати значні ризики безпеки як для працівників, так і для роботодавців. Коли працівники використовують свої особисті пристрої для роботи, вони часто отримують доступ до конфіденційних даних компанії та зберігають їх на своїх пристроях. Ці дані можуть включати конфіденційну ділову

інформацію, персональну ідентифікаційну інформацію (PII) та інші конфіденційні дані, які повинні бути захищені відповідно до різних нормативних актів і стандартів відповідності.

Щоб протистояти цим ризикам, компанії, які дозволяють використання власних пристроїв, повинні впроваджувати надійні політики та процедури безпеки. Ці політики повинні стосуватися таких питань, як шифрування, надійні паролі, можливості віддаленого стирання та використання віртуальних приватних мереж (VPN) для захисту даних під час передачі. Компанії також повинні інвестувати в програмне забезпечення для управління мобільними пристроями (MDM), яке може відстежувати і контролювати доступ до конфіденційних даних на персональних пристроях співробітників.

Однак, незважаючи на ці заходи, немає жодних гарантій, що пристрої, які належать працівникам, можуть бути повністю захищені, що призвело до того, що деякі компанії повністю відмовилися від BYOD на користь пристроїв, що належать компанії. Хоча такий підхід може забезпечити більшу безпеку та контроль, він також може бути більш дорогим і менш привабливим для працівників, які віддають перевагу гнучкості у використанні власних пристроїв.

Зрештою, рішення про те, впроваджувати BYOD чи ні, залежатиме від конкретних потреб і культури організації. Компанії повинні ретельно зважити переваги та ризики BYOD і розробити комплексну стратегію захисту та управління пристроями співробітників, незалежно від того, який підхід вони оберуть.

Отже, BYOD пропонує численні переваги з точки зору підвищення гнучкості та продуктивності, але він також створює значні проблеми з безпекою, які необхідно вирішувати шляхом ретельного планування та впровадження політик і процедур безпеки. Компанії, які вирішили дозволити BYOD, повинні бути готові інвестувати в необхідні технології та ресурси для захисту та управління пристроями, що належать працівникам, а ті, хто обирає пристрої, що належать компанії, повинні бути готові взяти на себе додаткові витрати, пов’язані з таким підходом. Зрештою, ключ до успіху полягає в розробці комплексної стратегії, яка збалансовує переваги та ризики BYOD і відповідає конкретним потребам організації.

Список використаних джерел

1. M.T. Banday, M.M. Algahtany, «Bring Your Own Device (BYOD) security in the organizations: Challenges and solutions», International Journal of Computer Science and Information Security, vol. 17, no. 2, 2019.
2. K.S. Ali, «Personal data protection in BYOD environments: An overview of mobile device management», International Journal of Advanced Computer Science and Applications, vol. 10, no. 9, 2019.
3. N. Hasan and M. H. Azman, «BYOD security in the workplace: A review of the challenges and solutions», 2018 International Conference on Information and Communication Technology for the Muslim World (ICT4M), Kuala Lumpur, Malaysia, 2018.
4. S. M. Aslam, S. M. Shiraz, A. Zafar, «BYOD security: Challenges, issues and solutions», 2019 International Conference on Computer and Information Sciences (ICCIS), Karachi, Pakistan, 2019.
5. Наказ від 14.05.2020 №269 Адміністрації Державної служби спеціального зв’язку та захисту інформації України «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації».
6. IT-Grundschutz catalogues. – URL: https://www.scribd.com/document/534182501/IT-Grund-schutz-catalogues-15th-version-2015-Draft.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
САВЧЕНКО Т. В.

ЕКСПЕРТНА СИСТЕМА ДЛЯ ВИБОРУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ВИМОГ ТА УПОДОБАНЬ ІТ-ФАХІВЦІВ

ОСАДЧУК М., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті описано розробку експертної системи для вибору програмного забезпечення на основі вимог та уподобань ІТ-фахівців. Система забезпечує можливість введення користувачем необхідної функціональності та характеристик, що повинні бути враховані при виборі ПЗ. На основі цих даних система надає рекомендації щодо оптимальних варіантів програмного забезпечення. Розроблена система була протестована на декількох прикладах вибору ПЗ, і була успішно використана для вирішення задачі вибору програмного забезпечення. Результати дослідження підтверджують, що розроблена експертна система може бути корисною для ІТ-фахівців, які займаються вибором ПЗ.

The article describes the development of an expert system for selecting software based on the requirements and preferences of IT professionals. The system provides the user with the ability to enter the necessary functionality and characteristics that should be considered when selecting software. Based on this information, the system provides recommendations for optimal software options. The developed system was tested on several examples of software selection and was successfully used to solve the software selection problem. The research results confirm that the developed expert system can be useful for IT professionals involved in software selection.

Актуальність. В сучасному світі ІТ-технології швидко розвиваються, а ринок програмного забезпечення пропонує величезну кількість продуктів, які мають різні характеристики та можливості. Вибір оптимального програмного забезпечення для виконання конкретних завдань може стати справжнім викликом для ІТ-фахівців. У цьому контексті розробка експертної системи, яка допоможе вибрати найбільш відповідне програмне забезпечення на основі вимог та уподобань користувачів, стає актуальною та необхідною.

Метою дослідження є розробка ефективного та точного інструменту для вибору програмного забезпечення, який забезпечує задоволення вимог та уподобань ІТ-фахівців.

Об'єктом дослідження є процес вибору програмного забезпечення, а предметом дослідження є експертна система для автоматизації цього процесу.

Завданнями дослідження є аналіз попередніх досліджень в цій області, вивчення особливостей процесу вибору програмного забезпечення, розробка алгоритмів та методів роботи експертної системи, тестування та оцінка її ефективності.

Предметом цієї наукової статті є розробка експертної системи для вибору програмного забезпечення на основі вимог та уподобань ІТ-фахівців.

Для досягнення поставленої мети, було проведено аналіз попередніх досліджень та визначено основні проблеми, що виникають під час вибору програмного забезпечення. На основі отриманих результатів була розроблена експертна система, яка використовує методи штучного інтелекту для аналізу вимог та уподобань користувачів та вибору оптимального програмного забезпечення для їх потреб.

Аналіз попередніх досліджень в області вибору програмного забезпечення показав, що це завдання може бути досить складним, особливо коли необхідно враховувати вимоги та уподобання різних ІТ-фахівців. Одним з підходів до вирішення цієї проблеми є використання експертних систем.

Експертні системи – це комп'ютерні програми, які імітують поведінку людини-експерта, щоб допомогти вирішити складні проблеми. Ці програми особливо корисні в

додатках зі штучним інтелектом, оскільки їх можна використовувати, коли немає експерта або якщо найняти його занадто дорого. Експертні системи можуть полегшити навчання та оптимізувати час, що призведе до підвищення продуктивності праці. Вони також часто використовуються для ознайомлення з галуззю та висвітлення поточних і потенційних застосувань.

Побудова експертної системи може бути тривалим, багаторічним процесом, який потребує багато правок зі сторони кінцевих користувачів які будуть використовувати її вже під свої певні унікальні задачі. Однак, незважаючи на те, що вони не вимагають великих і релевантних наборів даних для навчання, експертні системи страждають від обмежень ефективності, масштабованості та застосовності. Крім того, інтерфейси користувача для експертних систем часто розробляються з використанням Visual Basic[1], що робить їх популярним вибором для багатьох програм.

Основні компоненти експертної системи включають базу знань, механізм виведення (логічний двигун) та інтерфейс користувача. База знань містить інформацію, яка відображає знання та досвід експертів у певній галузі. Механізм виведення відповідає за аналіз інформації, яка надходить від користувача, та генерацію рекомендацій на основі знань, зібраних у базі знань.

З точки зору переваг, діагностика несправностей виявилася однією з найбільш корисних областей застосування для впровадження систем, заснованих на знаннях, а діагностичні системи, засновані на неглибоких знаннях, були високоефективними у вузькому домені, пов’язаному з конкретними завданнями. З іншого боку, недоліки експертних систем включають відсутність сприйняття системи користувачами, неможливість утримати розробників, і відносно мало опубліковано саме стосовно модельних підходів для розробки експертних систем [5]. Щоб подолати ці недоліки, архітектура нейронної експертної системи дозволяє автоматично створювати базу знань шляхом навчання на прикладах висновків, що дає змогу вивчати шаблони з нерелевантними входами та виходами. Крім того, до системи можна додати евристику для роботи з неповною інформацією та для пояснення висновків.

Експертна система може бути корисною для вибору програмного забезпечення, оскільки вона може виконувати багато виснажливих завдань, які люди можуть бути не в змозі виконати. Це також може допомогти зменшити кількість часу та грошей, необхідних для вибору програмного забезпечення, оскільки воно може швидко проаналізувати дані та надати список рекомендованого програмного забезпечення. Крім того, це може бути корисним в інших сферах управління людськими ресурсами, наприклад, під час найму, навчання та оцінки ефективності. В результаті експертна система може забезпечити ефективне рішення для вибору програмного забезпечення. Крім того, експертна система може допомогти підвищити точність і якість процесу відбору. Він може забезпечити більш надійні та послідовні результати, ніж людська система, оскільки він може ідентифікувати та усувати будь-яке потенційне упередження. Крім того, оскільки експертна система може швидко і точно аналізувати дані, вона може надати більш точні та надійні рекомендації щодо вибору програмного забезпечення. Це може допомогти скоротити кількість часу та грошей, необхідних для вибору програмного забезпечення. Підсумовуючи, експертні системи можуть бути корисними при виборі програмного забезпечення та інших сферах управління людськими ресурсами. Вони можуть надати швидші, точніші та надійніші результати, ніж людські системи, а також можуть зменшити кількість часу та грошей, необхідних для вибору програмного забезпечення.

Експертна система – це комп’ютерна програма, призначена для імітації поведінки людини-експерта . Це одна з найкорисніших програм штучного інтелекту , яка складається з інтерфейсу користувача, підсистеми пояснення, механізму логічного висновку та бази знань. Ядром експертної системи є база знань, яка зберігає правила, об’єкти, загальні випадки, винятки та відношення. Компоненти експертної системи дозволяють людині-експерту впоратися з певною проблемою, а систематичний дизайн експертної системи може бути розроблений за допомогою Уніфікованої мови моделювання (UML).

Експертні системи є програмними системами, які використовують бази знань та правил, щоб допомогти користувачеві вирішувати складні задачі в певній галузі. У випадку вибору програмного забезпечення, експертна система може аналізувати вимоги та уподобання користувачів, оцінювати різні параметри програмного забезпечення, такі як функціональність, продуктивність та безпека, та надавати рекомендації щодо вибору найбільш підходящого варіанту. Результати тестування експертної системи показали її ефективність та точність в роботі.

Різні автори пропонують різні підходи до розробки експертних систем для вибору програмного забезпечення. Деякі автори пропонують використання методів штучного інтелекту, таких як нейронні мережі та генетичні алгоритми, для покращення ефективності експертної системи. Інші автори пропонують використання методів множинного критерію прийняття рішень, які дозволяють враховувати різні критерії та обмеження при виборі програмного забезпечення.

Одним з основних етапів процесу вибору програмного забезпечення є збір вимог та уподобань користувачів. Для ефективного використання експертної системи для вибору програмного забезпечення, необхідно детально проаналізувати ці вимоги та уподобання та перетворити їх на формальні критерії та обмеження.

Після збору вимог та уподобань, експертна система може провести аналіз різних варіантів програмного забезпечення та згенерувати список підходящих варіантів. Цей список може бути відфільтрований та відсортований за різними критеріями, такими як ціна, функціональність та безпека. Після цього користувач може ретельно ознайомитися з кожним з варіантів та визначитися з вибором, що найкраще відповідає його потребам.

Процес вибору програмного забезпечення є складним і може включати в себе різні критерії, такі як вартість, функціональність, масштабованість та інші. Крім того, можуть бути наявні обмеження, такі як сумісність з існуючим програмним забезпеченням та обмеженнями на час впровадження. Експертна система повинна враховувати ці критерії та обмеження для того, щоб дати користувачеві якісну рекомендацію.

Для розробки експертної системи для вибору програмного забезпечення можна використовувати різні методології. Нижче наведені деякі з них.

1 Методологія знань. Методологія знань є однією з основних методологій розробки експертних систем. Вона передбачає розробку бази знань, що містить правила та факти з певної галузі. Ця база знань потім використовується для прийняття рішень. В експертній системі для вибору програмного забезпечення правила та факти можуть бути пов’язані з різними критеріями та обмеженнями, які необхідно враховувати при виборі програмного забезпечення.

2 Методологія множинного критерію прийняття рішень. Методологія множинного критерію прийняття рішень передбачає врахування різних критеріїв та обмежень при виборі програмного забезпечення. В експертнній системі для вибору програмного забезпечення ця методологія може використовуватися для призначення вагових коефіцієнтів для кожного критерію та обмеження, що дозволить зробити більш об’єктивний вибір.

3 Методологія аналізу ієрархій. Методологія аналізу ієрархій (AI) - це методологія, що дозволяє порівнювати різні критерії та обмеження на основі їх важливості. В експертній системі для вибору програмного забезпечення AI може використовуватися для визначення важливості різних критеріїв та обмежень для користувача та призначення вагових коефіцієнтів кожному критерію та обмеженню.

Розробляючи експертну систему для IT-фахівців, слід враховувати кілька основних факторів. Важливо, що система розроблена з використанням модульного підходу, щоб її було легко оновлювати та покращувати в майбутньому. Крім того, система повинна бути розроблена так, щоб вона була зручною для користувача, з ясним і лаконічним інтерфейсом користувача, який легко зрозуміти. Крім того, система повинна бути розроблена з можливістю масштабування вгору або вниз залежно від потреб користувача, дозволяючи системі рости разом з вимогами користувача. Безпека також є важливим фактором, оскільки

система повинна бути розроблена таким чином, щоб захищати дані та інформацію користувача. Нарешті, система повинна бути розроблена таким чином, щоб мати можливість інтегруватись з іншими існуючими IT-системами, забезпечуючи безперебійну взаємодію між користувачем і системою.

Першим кроком у розробці експертної системи для вибору програмного забезпечення є збір вимог та уподобань користувача. Цей крок включає в себе визначення критеріїв, які важливі для користувача, таких як функціональність, масштабованість, вартість та інші. Крім того, можуть бути визначені обмеження, такі як сумісність з існуючим програмним забезпеченням та обмеження на час впровадження.

Після збору вимог та уподобань користувача наступним кроком є розробка бази знань, яка містить правила та факти з певної галузі. У випадку експертної системи для вибору програмного забезпечення ця база знань міститиме правила та факти, пов'язані з критеріями та обмеженнями, які були визначені на першому кроці. Наприклад, якщо одним з критеріїв є масштабованість, то база знань може містити правила, які вказують на те, які програмні продукти є більш масштабованими за інші.

Для того, щоб користувач міг взаємодіяти з експертною системою, необхідно розробити інтерфейс користувача. Цей інтерфейс може бути у вигляді веб-сторінки або додатка, що встановлюється на комп'ютер користувача. В інтерфейсі користувач може ввести свої вимоги та уподобання, а також переглянути рекомендації, які згенерувала експертна система.

Після розробки бази знань та інтерфейсу користувача необхідно розробити правила інтерпретації, які допоможуть експертній системі зрозуміти вимоги та уподобання користувача. Ці правила можуть бути в основному у вигляді логічних правил, які забезпечують виконання порівняння та забезпечення рекомендацій.

Останнім кроком у розробці експертної системи для вибору програмного забезпечення є розробка алгоритму вибору. Цей алгоритм використовується для порівняння вимог та уподобань користувача з базою знань та визначення найбільш підходящого програмного забезпечення для користувача.

Розробка користувацького інтерфейсу експертної системи може допомогти IT-фахівцям зробити його зручним для користувача. Наприклад, TaxCut – зручна експертна система, призначена для полегшення взаємодії користувачів із програмним забезпеченням. Розробка гнучкого та зручного для користувача інтерфейсу є важливою для забезпечення високої якості обслуговування клієнтів. Щоб забезпечити зручність, інтерфейс користувача повинен бути розроблений з використанням знайомих користувачеві термінів. Крім того, інтерфейс користувача має бути розроблений таким чином, щоб він дозволяв користувачеві розробляти власну систему та був простим у використанні та надавав дані для ситуацій «що, якщо».

Інтерфейс користувача також повинен містити назву системи та призначення експертної системи. Усі ці компоненти необхідно об'єднати для створення комплексної та зручної експертної системи . Інтерфейс користувача також повинен мати можливості та дедуктивну силу, щоб зробити СУБД зручною для користувача. Нарешті, інтерфейс користувача повинен бути розроблений таким чином, щоб включати як спеціалістів, так і неспеціалістів. Отже, це зробить систему зручною та гнучкою для користувачів.

При розгляді функцій, які повинні бути включені в експертну систему, є важливі функції, які повинні бути присутніми для того, щоб гарантувати, що програма не потребує технологій, що виходять за межі сучасного рівня. Ці функції включають набір правил, базу даних відповідної інформації, спосіб пошуку інформації, інтерфейс, який дозволяє користувачам вводити запитання та отримувати відповіді, а також спосіб оновлення системи за потреби. Крім того, бажані функції допоможуть вказати програми, які мають найбільші шанси на успішне впровадження. Такі функції включають зручний інтерфейс, можливість навчатися на основі введених користувачем даних, здатність інтегруватися з іншими програмами чи базами даних і здатність надавати користувачеві зворотний зв'язок. Добре

спроектована експертна система також повинна включати механізм відстеження та моніторингу продуктивності системи з метою виявлення будь-яких потенційних проблем або покращень, які можна зробити. Нарешті, система повинна мати можливість тестування та перевірки для забезпечення точності та надійності. Усі ці функції необхідні для того, щоб експертна система була корисною для ІТ-фахівців і надавала їм інформацію та знання, необхідні для прийняття обґрунтованих рішень.

Висновки. У цій статті було розглянуто експертну систему для вибору програмного забезпечення на основі вимог та уподобань ІТ-фахівців. Визначено ціль, мету, завдання, об'єкт дослідження та предмет дослідження даної експертної системи. Було описано процес розробки експертної системи та її складові елементи, які включають базу знань, інтерфейс користувача, правила інтерпретації та алгоритм вибору.

Експертні системи здатні забезпечити велику кількість переваг, зокрема, вони здатні розглядати велику кількість варіантів вирішення проблеми, забезпечують однаковість вирішення проблеми при однакових вихідних даних та здатні підтримувати та оновлювати свою базу знань.

Експертні системи для вибору програмного забезпечення можуть бути корисним інструментом для ІТ-фахівців, які шукають оптимальне програмне забезпечення для вирішення конкретної задачі. Вони допомагають скоротити час на пошук та вибір програмного забезпечення та зменшити ризики неправильного вибору.

У майбутньому, експертні системи для вибору програмного забезпечення можуть бути ще більш розробленими та удосконаленими. Наприклад, вони можуть використовувати машинне навчання для покращення рекомендацій та врахування нових продуктів програмного забезпечення. Також можливим є використання експертних систем для вибору інших типів технічних засобів, таких як апаратне забезпечення.

У цілому, експертні системи для вибору програмного забезпечення мають великий потенціал для вирішення проблем в галузі ІТ, забезпечуючи швидке та ефективне рішення при виборі програмного забезпечення на основі вимог та уподобань ІТ-фахівців. Це може значно зменшити час та зусилля, необхідні для вибору програмного забезпечення, та допомогти забезпечити якість та продуктивність у роботі з програмним забезпеченням.

Список використаних джерел

1. Григор'єва І. А., Євтух М. Д. Методика формування експертної системи підтримки процесу вибору програмного забезпечення // Вісник Національного університету «Львівська політехніка». Серія: Комп'ютерні системи та мережі. – 2014. – № 807. – С. 118–126.
2. Довгань В. І., Сотнікова О. М. Експертна система вибору програмного забезпечення для автоматизованої системи управління // Наукові праці ДонНТУ. Серія «Інформатика, кібернетика та обчислювальна техніка». – 2015. – Вип. 2 (28). – С. 75–81.
3. Дударєв О. В. Експертна система вибору програмних продуктів на основі вимог користувачів // Вісник Чернігівського національного технологічного університету. Серія: Технічні науки. – 2018. – № 1 (85). – С. 114–120.
4. Костенко А. І., Лавренюк Є. М., Осьмак О. В. Експертна система підтримки прийняття рішень з вибору програмного забезпечення // Наукові праці ДонНТУ. Серія «Інформатика, кібернетика та обчислювальна техніка». – 2019. – Вип. 1 (35). – С. 68–75.
5. Кузнецов О. О., Ярмак Н. М. Експертна система вибору платформи для розробки програмного забезпечення // Вісник Київського національного університету технологій та дизайну. Серія: Технічні науки та архітектура. – 2017. – № 1 (89). – С. 119–125.

Робота виконана під науковим керівництвом канд. екон. наук, старшого викладача
ФРАНЧУК Т. М.

ПРОГРАМНА РЕАЛІЗАЦІЯ ОНЛАЙН-СЕРВІСУ ПІДБОРУ КОМПЛЕКТУЮЧИХ ДЛЯ ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА

ПАВЛІВСЬКИЙ Я., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади розробки прогрмної платформи сервісу онлайн-підбору комплектуючих для персонального комп'ютера. Зазначено переваги користуванням даного сервісу та варіанти розробки. Також було враховано фактор конкурентоспроможності на ринку серед подібних сервісів.

The article discusses the basic principles of building an online component selection service for a personal computer. The advantages of using this service and development options are indicated. The factor of competitiveness in the market among similar services was also taken into account.

Актуальність. Онлайн-сервіси підбору комплектуючих для персонального комп'ютера стали дуже популярними останніми роками. Це пов'язано з тим, що люди стали частіше замовляти комплектуючі в Інтернеті, а не в магазинах. Онлайн-сервіси дозволяють користувачам легко знайти потрібні комплектуючі та порівняти їх характеристики та ціни.

Один з головних факторів, що зумовили популярність сервісів підбору комплектуючих, – це зростання інтересу до геймінгу та розвиток інтернет-технологій. Люди стали більше часу проводити за комп'ютерами, а отже, інтересуватись якістю та продуктивністю своїх комп'ютерів.

Існує також зростаючий інтерес до збільшення продуктивності комп'ютера за допомогою підбору правильних комплектуючих. Онлайн-сервіси дозволяють користувачам знайти оптимальний баланс між ціною та характеристиками.

Сервіси онлайн-підбору комплектуючих для персонального комп'ютера є дуже актуальними в наш час. Розвиток інтернет-технологій та електронної комерції дозволяє людям з усього світу купувати товари в мережі з будь-якого місця та в будь-який час. Особливо це стосується комплектуючих для персональних комп'ютерів.

Основні переваги використання сервісів онлайн-підбору комплектуючих для персонального комп'ютера такі:

1. Зручність та швидкість: Користувачі можуть знайти необхідні комплектуючі за допомогою спеціальних сервісів всього за кілька хвилин. Вони можуть шукати комплектуючі за різними параметрами, такими як ціна, виробник, характеристики, розмір і т.д.
2. Великий вибір: Онлайн-магазини пропонують великий вибір комплектуючих для персональних комп'ютерів, що значно збільшує ймовірність того, що користувач знайде необхідний товар.
3. Знижки та пропозиції: Онлайн-магазини часто пропонують різні знижки, акції та пропозиції, що дозволяє зекономити кошти під час покупки комплектуючих.
4. Доставка до дому: Більшість онлайн-магазинів пропонують доставку товарів до дому, що дозволяє користувачам зекономити час та зусилля, не відходячи від комп'ютера.
5. Комфортний відбір товару: Онлайн-магазини надають можливість детального ознайомлення з товарами, їхніми характеристиками та відгуками користувачів. Це дозволяє зробити збір даних та прийняти рішення про покупки.

Метою статті є дослідження особливостей використання сервісів з онлайн-підбором комплектуючих для персонального комп'ютера та їх ефективність.

Об'єктом дослідження є розробка сервісу онлайн-підбору комплектуючих для персонального комп'ютера.

Предмет дослідження – програмні інструменти онлайн сервіс підбору.

Аналіз попередніх досліджень. Дослідженню оптимізації процесу підбору комплектуючих для пк за допомогою програмної реалізації онлайн-сервісу присвячені праці: Самара О. С., Гаврилюк Дмитро, Пилипенко Оксана, Коваленко Олександр.

Виклад основного матеріалу. За останні кілька років, ринок комп'ютерних комплектуючих значно змінився, і з'явилися нові можливості для тих, хто шукає спосіб оновити свій персональний комп'ютер. Однією з таких можливостей є використання сервісів онлайн-підбору комплектуючих. Ці сервіси дозволяють користувачам знайти все необхідні для свого ПК, враховуючи їх потреби та бюджет.

Онлайн конфігуратор ПК – це спеціальна програма, за допомогою якої користувач зможе підібрати потрібну йому конфігурацію ПК, не виходячи з дому. Іншими словами конфігуратор ПК - автоматизований ресурс по підбору комплектуючих для персонального комп'ютера. Можна сказати, що конфігуратор ПК – це аналог продавця-консультанта в магазині. У даній системі також, як і запитавши у консультанта, можна також отримати інформацію про сумісність тих або інших комплектуючих між собою, отримати пораду про вибір ПК для роботи з конкретними програмами, дізнатися вартість комп'ютера і, виходячи з цієї інформації, одержати найбільш підходящий варіант готової конфігурації ПК.

У цій статті ми розглянемо переваги та недоліки використання таких сервісів.

Переваги сервісу онлайн-підбору:

1. Ефективність. Онлайн-підбір комплектуючих дозволяє швидко знайти їх для вашого ПК. Вам не потрібно витрачати час на пошук та порівняння різних товарів, а сервіс зробить це за вас.
2. Придатність до використання. Більшість сервісів онлайн-підбору дуже прості та зрозумілі в користуванні. Вони надають зручний інтерфейс, який дозволяє з легкістю знайти необхідні комплектуючі.
3. Гнучкість. Сервіси онлайн-підбору дозволяють вибрати комплектуючі з різних виробників, моделей та цінових категорій. Вам не потрібно обмежувати себе тільки одним виробником або моделлю.
4. Економічність. Використання даних сервісів може допомогти зекономити кошти. Вони дозволяють знайти комплектуючі за кращими цінами та зіставити різні варіанти.

Сервіси онлайн-підбору комплектуючих для ПК є корисними для людей, які не розуміються в складних технічних аспектах комп'ютерів, але хочуть зібрати або оновити свій ПК. Ці сервіси надають можливість легко і швидко знайти потрібні компоненти, враховуючи всі необхідні технічні характеристики, такі як сумісність, розмір, потужність, вартість та інші.

Це особливо корисно для тих, хто не має часу або можливості досліджувати різні компоненти та їх характеристики, або не має достатньої кваліфікації, щоб правильно підібрати компоненти для свого ПК. Сервіси онлайн-підбору комплектуючих для ПК надають їм зручний та легкий спосіб знайти всі необхідні деталі для свого ПК та зберегти час та гроші, які можна було б витратити на невдалі спроби вибрати потрібні компоненти самостійно.

Оптимізація процесу підбору комплектуючих для ПК з використанням програмної реалізації онлайн-сервісу може принести численні переваги для користувачів, що шукають оптимальний варіант конфігурації свого комп'ютера.

Однією з головних переваг є часова ефективність. Замість того, щоб витрачати час на пошук і аналіз різноманітних комплектуючих, користувач може скористатися сервісом та отримати швидкий та точний варіант підбору, що значно зберігає час.

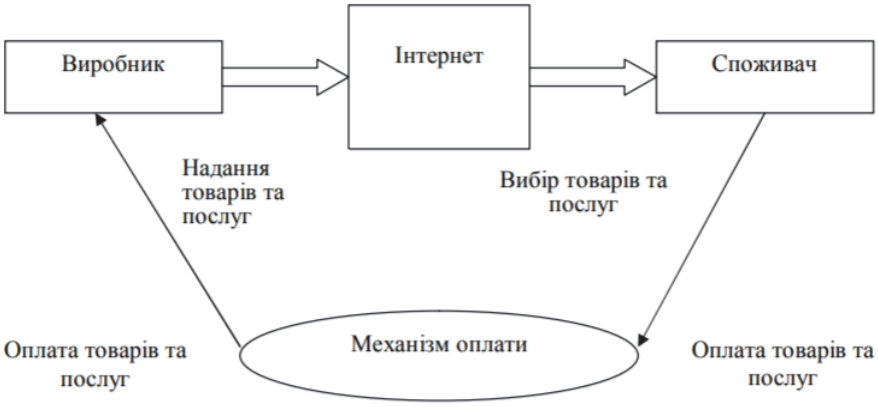


Рис. 1. Схема онлайн торгівлі

Крім того, програмна реалізація дозволяє підбирати комплектуючі на основі різних параметрів, таких як вартість, продуктивність, розмір, сумісність тощо. Це допомагає користувачеві знайти найбільш підходящу конфігурацію за його вимогами та можливостями.

Окрім цього, онлайн-сервіс може враховувати такі фактори, як технічні характеристики вже наявних комплектуючих та їх сумісність з іншими елементами комп'ютера. Таким чином, користувач може уникнути проблем зі сумісністю та зберегти кошти на зайвих покупках.

Крім цього, використання програмної реалізації дозволяє зменшити ймовірність помилок та неуважних дій, що можуть виникнути при ручному підборі комплектуючих. У загальному, використання онлайн-сервісу для підбору комплектуючих дозволяє значно спростити та оптимізувати процес вибору та покупки комп'ютерної техніки, що є важливим фактором у сучасному світі інформаційних технологій.

Сервіси онлайн-підбору комплектуючих для ПК є дуже важливими на ринку інформаційних технологій. За останні кілька років зростання інтересу до комп'ютерних ігор, відеомонтажу та інших завдань, які вимагають потужного комп'ютера, призвело до збільшення попиту на користувачів, які бажають зібрати свій власний ПК з оптимальними комплектуючими.

Сервіси онлайн-підбору комплектуючих для ПК дозволяють користувачам з легкістю зібрати свій власний ПК, відповідний їхнім потребам та бюджету. Це допомагає зменшити час, який потрібен для відбору компонентів, а також дозволяє користувачам уникнути помилок при виборі несумісних комплектуючих. Крім того, сервіси підбору комплектуючих для ПК можуть допомогти користувачам зменшити витрати на придбання компонентів, оскільки вони можуть порівняти ціни на різних платформах та виробниках.

На ринку сервісів онлайн-підбору комплектуючих для ПК є багато конкурентів, і тому компанії, які розробляють такі сервіси, повинні постійно покращувати свої продукти та додавати нові функції, щоб зберігати свою конкурентну перевагу. Від цього залежить їхній успіх на ринку та популярність сервісу серед користувачів.

Конкуренція сервісів з онлайн підбору комплектуючих для ПК є досить великою і динамічною. На ринку присутні багато компаній, що пропонують схожі послуги, тому важливо мати конкурентні переваги та додаткові функції, що привертають клієнтів.

Однією з основних конкурентних переваг є точність та повнота баз даних з комплектуючими. Клієнти часто вибирають сервіс, який надає найбільш повну та актуальну інформацію про наявні на ринку комплектуючі. Також важливо мати простий та зручний інтерфейс, щоб клієнти могли швидко та легко знайти потрібний компонент.

Іншим важливим аспектом є цінова конкуренція. Клієнти зазвичай шукають найкращу пропозицію за доступною ціною. Тому сервіси з онлайн підбору комплектуючих, що надають можливість порівнювати ціни на різних платформах, мають більші шанси на успіх. Також важливо мати додаткові функції, які можуть привернути клієнтів. Наприклад, деякі сервіси можуть пропонувати можливість складання власної конфігурації ПК з врахуванням потреб користувача, або надавати гарантію на придбані комплектуючі.

Окрім цього, важливо мати рекламну стратегію, яка допоможе залучити нових клієнтів. Такі сервіси можуть використовувати різні маркетингові інструменти, такі як контекстна реклама, соціальні мережі, пошукова оптимізація та інші.

Сервіс, який розробляється буде враховувати ці критерії, щоб конкурувати на ринку з подібними сервісами. В умовах проектування підтримки прийняття рішень при підбору комп'ютерної техніки, це пошук способу, якій задовольняє вимогам функціональності системи засобами наявних технологій з урахуванням заданих обмежень. Складність проектування проявляється в тому, що воно не є конструктивною задачею, як аналіз вимог чи реалізація проекту розв'язків. Проектування описується як окремий етап розробки проекту проміжний між аналізом та розробкою.

Для розробки сервісу з онлайн підбору комплектуючих для ПК потрібно використовувати різні технології, які допоможуть створити функціональний та ефективний продукт. Основними технологіями, які можна використовувати для розробки такого сервісу, є:

1. Бази даних: важливо мати точну та повну базу даних з комплектуючими, щоб користувачі могли швидко та легко знайти потрібні компоненти. Для зберігання даних можна використовувати реляційні або нереляційні бази даних, такі як MySQL, MongoDB, PostgreSQL тощо.

2. Front-end технології: для створення інтерфейсу користувача можна використовувати різні front-end технології, такі як HTML, CSS, JavaScript та фреймворки для них, наприклад, React, Angular, Vue.js тощо.

3. Back-end технології: для створення логіки та обробки запитів від користувачів можна використовувати різні back-end технології, такі як Python, PHP, Ruby, Node.js тощо. Також для розробки back-end можна використовувати фреймворки, такі як Django, Flask, Laravel, Express тощо.

4. API технології: для забезпечення взаємодії між front-end та back-end можна використовувати API технології, такі як REST або GraphQL.

5. Хмарні технології: для зберігання та обробки даних можна використовувати хмарні технології, такі як Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) тощо.

Для розробки сервісу з онлайн підбору комплектуючих для ПК можна використовувати різні моделі, наприклад Waterfall. Основна суть моделі Waterfall у тому, що етапи залежать один від одного і наступний починається, коли завершений попередній, утворюючи таким чином поступальний (каскадний) рух уперед.

Паралелізм етапів у каскадній моделі, хоч і обмежений, але можливий для абсолютно незалежних між собою робіт. При цьому інтеграція паралельних частин все одно відбувається на якомусь наступному етапі, а не в рамках одного. Команди різних етапів між собою не комунікують, кожна команда відповідає чітко за свій етап.

Недоліками цієї моделі є отримання результату по проходженню всіх етапів і складність виявлення помилок. Повертатися назад важко. Не зрозуміло що повертати: якщо стався збій на якомусь етапі, його наслідки видно тільки в кінці.

Дана модель зрозуміло і чисто вкладається в документи, наприклад в договори і роадмапи при наявності чітко визначених контрольних точок. У будь-який момент можна

легко зрозуміти чи була пройдена та чи інша точка контролю чи ні, і чи дотримані терміни. З цих причин довготривалі і особливо великі проекти, розраховані на десятиліття і залучення великої кількості організацій-учасників, керуються переважно waterfall.

Користувачі конфігуратора ПК можуть використовувати його для створення власних унікальних конфігурацій ПК, які відповідають їх потребам і бюджету. Основні кроки використання конфігуратора ПК включають наступне:

1. Вибір типу ПК: Користувач вибирає тип ПК, який йому потрібен, наприклад, робочий ПК, ігровий ПК або ноутбук.

2. Вибір компонентів: Користувач вибирає компоненти ПК, які йому потрібні, наприклад, процесор, материнську плату, оперативну пам’ять, жорсткий диск, відеокарту, блок живлення та інші. Кожен компонент має різні варіанти, які можуть бути вибрані в залежності від бюджету та потреб користувача.

3. Редагування конфігурації: Користувач може редагувати конфігурацію, змінюючи компоненти або додавати нові.

4. Збереження та завантаження конфігурації: Користувач може зберегти побудовану конфігурацію та завантажити її в майбутньому для використання.

5. Рекомендації щодо вибору оптимальної конфігурації: Конфігуратор ПК може надавати користувачам рекомендації щодо вибору оптимальної конфігурації на основі їх потреб та бюджету.

Ось схема схема структурного розгортання системи:

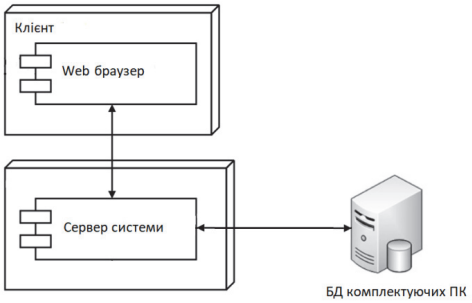


Рис. 3. Схема структурного розгортання системи програмної платформи

Схема структурного розгортання системи є важливою частиною проектування будь-якої складної інформаційної системи. Вона допомагає визначити потрібне обладнання та програмне забезпечення, необхідне для реалізації системи, а також дозволяє зрозуміти, як різні компоненти взаємодіють між собою та з іншими системами. Загалом, схема структурного розгортання системи дозволяє розробникам та інженерам зрозуміти фізичну реалізацію системи та забезпечити її ефективність та надійність.

Висновки. У результаті аналізу конкурентних сервісів та технологій, які можна використовувати для розробки сервісу з онлайн підбору комплектуючих для ПК, можна зробити висновок, що такий сервіс може бути дуже корисним для користувачів. Завдяки йому, користувач може зібрати оптимальний комп’ютер для своїх потреб, не витрачаючи багато часу та коштів на дослідження та вибір.

Важливим етапом розробки сервісу є використання відповідних моделей для підбору оптимальної конфігурації комп’ютера. Застосування таких моделей може зменшити кількість помилок при підборі комплектуючих та забезпечити вищу точність в роботі сервісу.

Однак, важливо також забезпечити зручний та інтуїтивно зрозумілий інтерфейс користувача, щоб зробити процес підбору комплектуючих максимально доступним та зрозумілим для широкого кола користувачів.

Отже, створення сервісу з онлайн підбору комплектуючих для ПК може бути вигідним та корисним для користувачів, що може допомогти вирішити проблему вибору оптимальної конфігурації комп'ютера.

Список використаних джерел

1. Блог Evergreen – методології розробки ПЗ. [Електронний ресурс]. – Режим доступу: https://evergreens.com.ua/ua/articles/software-development-metodologies.html
2. Роман Марченко, DAN IT Education. Електронний ресурс]. – Режим доступу: https://dan-it.com.ua/uk/blog/rozrobka-z-boku-front-end-shho-ce-take-i-chim-vidriznjaietsja-vid-back-end/
3. West Stream - Як створити свій сайт самостійно? Електронний ресурс]. – Режим доступу: https://wsart.com.ua/yak-stvoriti-sviy-sayt-samostiyno/

Робота виконана під науковим керівництвом канд. техн. наук, доцента
РЗАЄВОЇ С. Л.

UNITY ЯК ПЛАТФОРМА ДЛЯ РОЗРОБКИ ОСВІТЯНСЬКОГО ІГРОВОГО КОНТЕНТУ

ПАСЕШНИК О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто можливість використання платформи Unity в навчальних цілях, його функціонал, історію а також розглянуто його структуру і переваги які він може надати задля покращення освітнього процесу і збільшення зацікавленості учнів до навчання.

The article considers the possibility of using the Unity platform for educational purposes, its functionality, history, as well as its structure and advantages that it can provide to improve the educational process and increase students' interest in learning.

Актуальність. На Unity сьогодні розробляють багато різних проєктів які приносять великі прибутки своїм власникам, при цьому вона як платформа для розробки освітянського ігрового контенту є також досить актуальною в сучасному світі. За останні кілька років ігрові технології стали все більш популярними в освіті, і все більше навчальних закладів та компаній починають використовувати ігрові інтерактивні програми для покращення ефективності навчання та залучення учнів до процесу навчання. Завдяки широкому спектру інструментів та можливостей, які надає Unity, розробники можуть створювати навчальні ігри з використанням різних видів взаємодії та інтерактивності, що може забезпечити краще засвоєння матеріалу учнями.

Метою статті є вивчення можливостей платформи Unity, в тому числі для розробки освітянського ігрового контенту. Дослідження інструментів та технології які присутні в Unity, які можливості для інтерактивного навчання можна реалізувати на цій платформі, та які є приклади успішної реалізації ігрового контенту за допомогою рушія Unity. Результати

дослідження допоможуть зрозуміти, наскільки ефективно можна використовувати Unity для розробки навчальних ігор та як можна покращити якість освітнього контенту, щоб забезпечити кращі результати в процесі навчання.

Об'єктом дослідження є використання платформи Unity для створення освітянського контенту.

Предмет дослідження - Unity, як платформа для розробки освітянського ігрового контенту.

Аналіз попередніх досліджень. Unity була заснована в Копенгагені Ніколасом Френсісом, Йоахімом Анте та Девідом Хельгасоном. Її історія почалася на форумі OpenGL у травні 2002 року, де Френсіс розмістив оголошення про пошук співробітників для розробки шейдер-компілятора з відкритим вихідним кодом (графічного інструменту) для нішевої групи розробників ігор на базі Mac, таких як він сам. На нього відгукнувся Анте, на той час старшокласник з Берліна. Анте доповнив зосередженість Френсіса на графіці та геймплеї інтуїтивним розумінням внутрішньої архітектури. Оскільки гра, над якою він працював з іншою командою, нікуди не йшла, вони співпрацювали над шейдером неповний робочий день, поки кожен з них займався своїми власними проектами ігрового рушія, але вирішили об'єднати зусилля при особистій зустрічі. Щоб об'єднати кодові бази своїх рушіїв, вони розбили наметове містечко в квартирі Хельгасона на кілька днів, поки його не було в місті. План полягав у тому, щоб заснувати ігрову студію на базі потужної технічної інфраструктури, яку також можна було б ліцензувати.

Хельгасон і Френсіс працювали разом ще зі школи, працюючи над різними проектами з веб-розробки і навіть над короткочасними спробами кіновиробництва. Хельґасон навчався в Копенгагенському університеті, працюючи веб-розробником-фрілансером. Він допомагав, де міг, а через кілька місяців перейшов на повний робочий день, продавши свою невелику частку у фірмі з веб-розробки своїм партнерам [1].

Ігровий рушій Unity був випущений у 2005 році з початковою підтримкою ПК з Windows та веб-браузерів. З часом він став більш досконалим, що дозволило Unity розширити роботу до десятка чи близько того співробітників. Переломним моментом стала середина 2008 року, коли Apple представила iPhone App Store, що привело до появи ігрових додатків для iOS. Іншим великим прогресом став випуск MMORPG FusionFall від Cartoon Network, створеної на Unity3D із 8 мільйонами гравців. Unity також знайшла клієнтів серед великих компаній, таких як Electronic Arts, Microsoft і Ubisoft. У 2011 році Unity придбала анімаційну компанію під назвою Mecanim, покращивши основну технологію ігрового рушія. Сьогодні Unity та її 285 співробітників у всьому світі працюють над розробкою ігор для різних платформ, таких як iOS, Android, Windows, Mac, Linux, веб-браузери, PS3, Xbox 360 і Wii U. Unity3D використовують для створення складних ігор для iOS і Android. Незважаючи на гучні імена, які використовують Unity3D, засновник Unity - Helgason - пишається тим, що їх технологію можуть використовувати не тільки великі компанії, але і менші розробники. «Великі компанії завжди могли створювати ігри, вони б зрозуміли це і купили технологію або створили її самі» «Де ми дійсно досягли успіху, так це в тому, щоб ці маси людей могли не просто створювати ігри, а створювати ігри, використовуючи ті ж інструменти, що й великі хлопці» [2].

Також вивченням цього питання займались такі науковці як: Д.В. Мацокін, І.М. Пахомова та С.М. Цирульник.

Цирульник С.М., у своїй статті розглянув поняття доповненої реальності та акцентувався на застосуванні технології доповненої реальності в освітньому процесі підготовки студентів технічних спеціальностей. Вивчав актуальність та переваги використання даної технології в освітньому процесі [9].

Д.В. Мацокін та І.М. Пахомова в своїх дослідженнях пояснили актуальність такого підходу для учнів та студентів і на практиці показали як можна використовувати доповнену реальність. Вони створили додаток для учнів який допомагає вивчати фізику [10].

Виклад основного матеріалу. Ігровий рушій – це середовище розробки програмного забезпечення, яке також називають «архітектурою гри» або «ігровою структурою» з налаштуваннями та конфігураціями, які оптимізують і спрощують розробку відеоігор на різних мовах програмування. Ігровий движок може включати 2D- або 3D-графічний движок, який сумісний з різними форматами імпорту, фізичний рушій, який імітує дії в реальному світі, штучний інтелект (ШІ), який автоматично реагує на дії гравця, звуковий механізм, який керує звуковими ефектами, механізм анімації та безліч інших функцій [4].

Unity має дві основні переваги перед іншими передовими інструментами розроблення ігор: надзвичайно продуктивний візуальний робочий процес і потужна міжплатформна підтримка. Візуальний робочий процес є досить унікальною річчю, що виділяє цей інструмент із більшості інших середовищ розробки ігор. У той час як інші інструменти розроблення ігор найчастіше являють собою мішанину розрізнених частин, які потрібно контролювати, або, можливо, бібліотеку, для роботи з якою потрібно налаштовувати власне інтегроване середовище розробки (Integrated Development Environment, IDE), ланцюжок складання та інше в цьому роді, робочий процес в Unity прив'язаний до ретельно продуманого візуального редактора. У цьому редакторі ви будете компонувати сцени майбутньої гри, пов'язуючи ігрові ресурси і код в інтерактивні об'єкти. Саме він дає змогу швидко і раціонально створювати професійні ігри, забезпечуючи небачену продуктивність праці розробників і надаючи в їхнє розпорядження вичерпний перелік найсучасніших технологій у галузі відеоігор [5].

Рис. 1. Ігровий рушій [3]

Unity – це потужна технологія, яка має необмежені можливості для творчості і розвитку. Завдяки своїм інструментам та функціям, Unity може бути використана для створення різноманітних ігрових жанрів, анімаційних фільмів та навчальних проєктів. Unity дозволяє максимально реалізувати творчий потенціал та працювати над проектами в будь-якій галузі, тому можна сказати, що обмеження є лише уявою і продуктивністю [8].

Якщо ми говоримо про особливості Unity, то до таких можна віднести наступні пункти:

- Кросплатформеність: Unity дозволяє створювати ігри та додатки для різних платформах:
- Візуальний редактор: Unity має вбудований візуальний редактор, який дозволяє легко створювати і налаштовувати 3D та 2D об'єкти, освітлення, камери та інші складові ігрового світу без потреби в програмуванні.
- Система скриптів: Unity має вбудовану систему скриптів, яка дозволяє програмувати поведінку ігрових об'єктів на різних мовах програмування, таких як C#, JavaScript, Boo.
- Фізика: Unity має потужну систему фізики, яка дозволяє використовувати реалістичну фізику для руху об'єктів, колізій та ін.

- Інтеграція з іншими програмами: Unity дозволяє інтегрувати зовнішні програми та ресурси, такі як 3D-моделі, звукові доріжки, відео.
- Підтримка VR і AR.

Рис. 2. Підтримка платформ [6]

Unity - це важлива платформа для розробки VR та AR проектів, яка підтримує майже всі доступні гарнітури VR і надає численні пакети для розробки додатків на ARCore та ARKit. AR Foundation дозволяє розробникам Unity створювати додатки AR для Android та iOS одночасно, знижуючи складність розробки. Unity також пропонує XR Interaction Toolkit, щоб зробити процес розробки VR та AR ігор ще більш простим та доступним. Отже, Unity можна назвати одним з провідних підрядників у сфері розробки технологій XR [8].

Також Слід навести приклади одних з найбільш популярних ігор які були створенні за допомогою Unity:

- Valheim
- Genshin Impact
- Ori and the Blind Forest
- Cuphead
- Pokemon Go
- Hollow Knight
- The Forest

Так наприклад, якщо взяти Genshin Impact, відповідно до Sensor Tower за два роки з вересня 2020 року до вересня 2022 року вона стала третьої за доходами в Google Play та App Store, заробивши 3.7 млрд доларів. Слід сказати що цей результат йде без врахування прибутку з ПК [7].

Цей приклад демонструє що рушій Unity є досить конкурентоспроможним і прибутковим для створення ігор.

На сьогодні вивчення нових технологій та їх використання в навчанні стає все більш актуальним завданням в сучасному освітньому процесі, тому що використання таких технологій може допомогти підвищити якість освіти та забезпечити студентам зручний та цікавий спосіб здобуття знань. Враховуючи це, з'являється все більше програмних інструментів, спрямованих на полегшення процесу навчання та покращення ефективності навчання. Одним з таких інструментів може бути Unity, так як він має досить широкий функціонал.

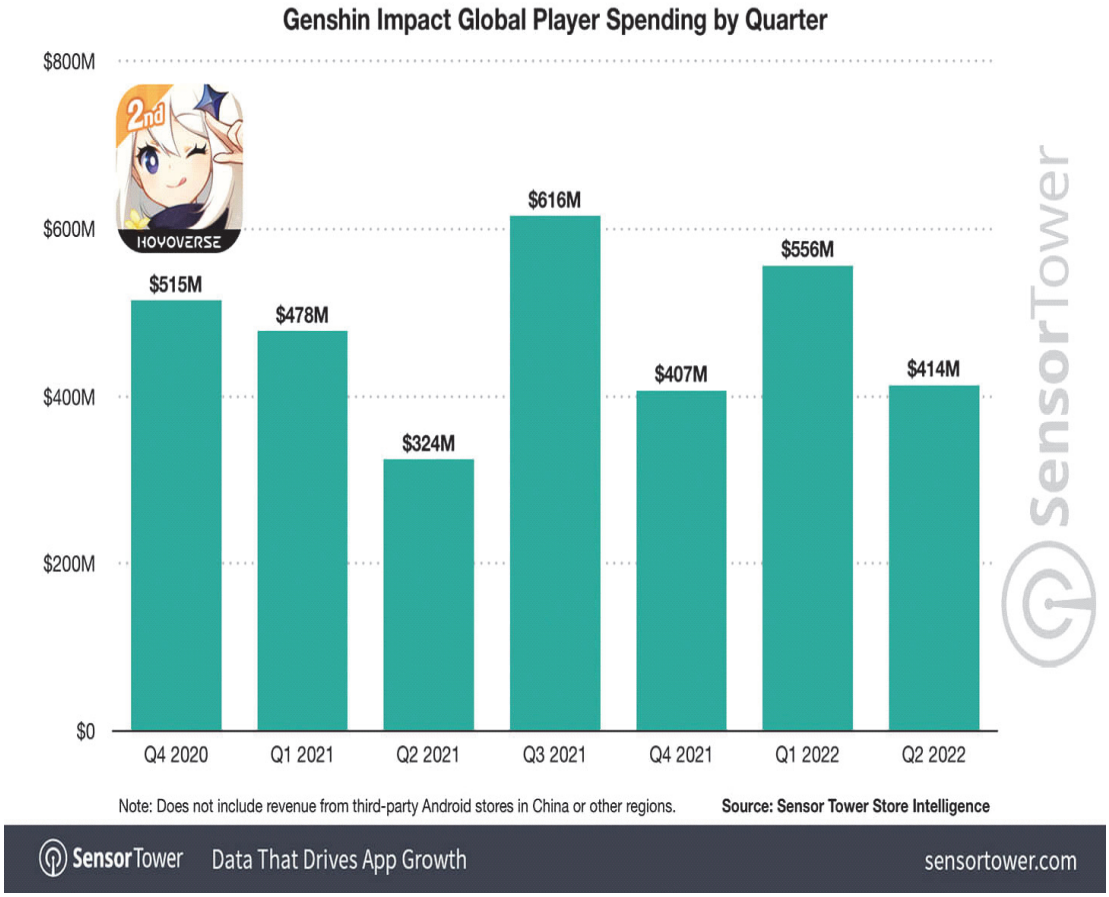


Рис. 3. Genshin Impact Global Spending by Quarter [7]

Unity надає можливість створювати інтерактивні візуалізації, симуляції та ігри, що можуть бути використані в різних навчальних аспектах. Наприклад, Unity можна використовувати для створення інтерактивних уроків з геометрії або фізики, де студенти можуть досліджувати різні сценарії і спостерігати за результатами. Також Unity має широкий вибір інструментів для створення анімацій та спеціальних ефектів, що можуть бути використані для створення технічних процесів, візуалізації даних тощо.

Однак, є певні недоліки використання Unity в навчальних цілях. Наприклад, навчання розробки в Unity може бути складним і потребувати від студентів вміння програмування та розуміння математичних концепцій. Крім того, використання Unity може вимагати потужних комп’ютерів для запуску складних ігор та симуляцій. Але можна сказати що позитивні аспекти у його використанні набагато більші.

У вищих навчальних закладах ми також можемо використовувати Unity, тому як приклад ми можемо взяти і розробити гру-тест за допомогою якої студенти могли б поліпшити свої знання в зручному для них форматі і практично будь де, адже таку гру можна буде використовувати як на комп’ютері так і на телефоні. На рисунку 4 дизайн-макет такої гри.

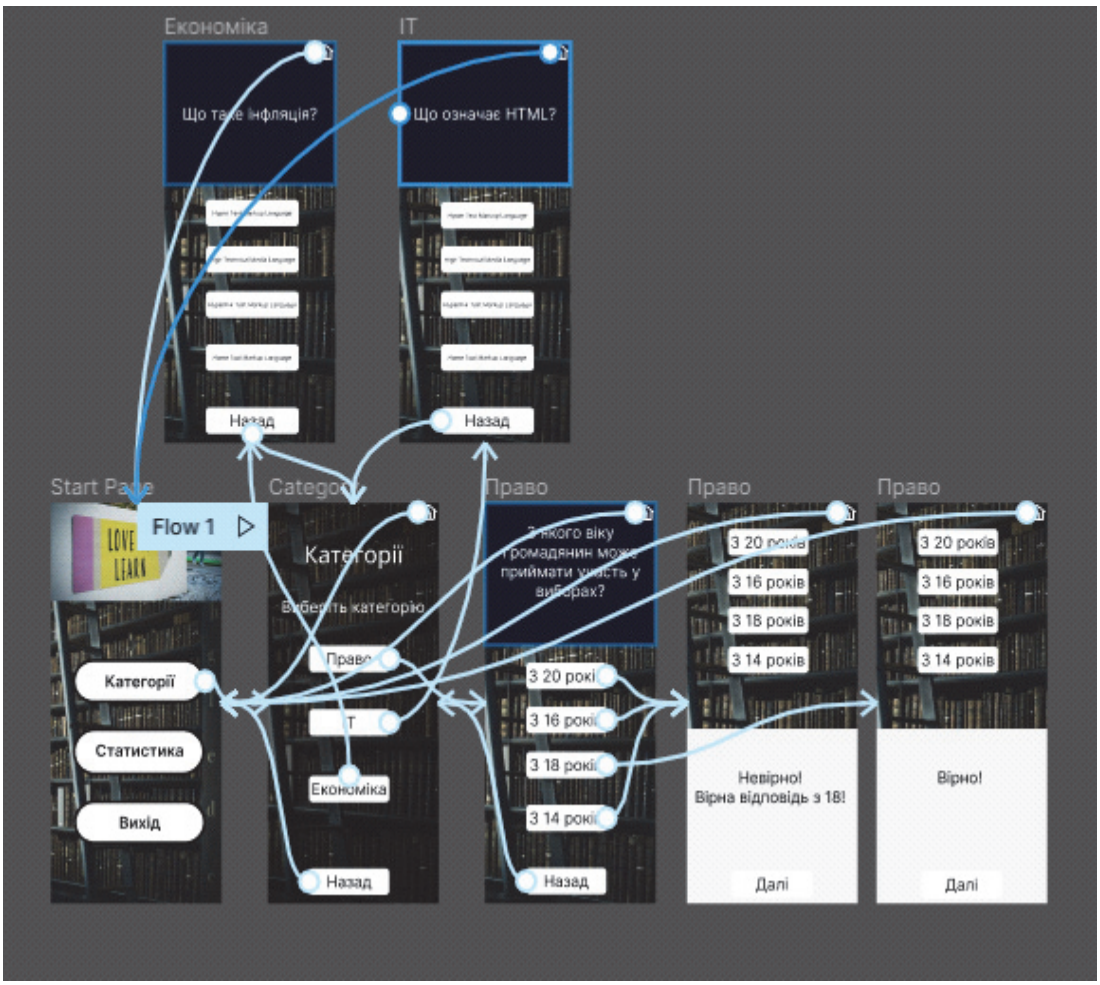


Рис. 4. Приклад гри-тесту

Джерело: Розроблено автором в середовищі Figma (Скріншот екрану)

Висновки. У статті досліджено потребу в освітянському ігровому контенті в закладах вищої освіти та його значення для покращення навчального процесу. Розглянуто можливість використання платформи Unity в навчальних цілях, а також її функціонал, історію та структуру. Досліджено переваги, які Unity може надати у збільшенні зацікавленості учнів до навчання, зокрема забезпечення візуалізації складних понять, сприяння інтерактивному навчанню та стимулювання творчого мислення. Також висвітлено можливість застосування платформи для вивчення різноманітних галузей знань, таких як право, інформаційні технології та інші. Застосування платформи Unity дозволяє створювати інтерактивні симуляції та візуалізації складних процесів, що може допомогти в засвоєнні теорії та практики в цих галузях знань. Загалом, використання цієї платформи в навчальних закладах може сприяти покращенню якості освіти та підвищенню мотивації учнів до навчання.

Список використаних джерел

1. Eric Peckham. How Unity built the world's most popular game engine. URL: https://techcrunch.com/2019/10/17/how-unity-built-the-worlds-most-popular-game-engine/ (дата звернення 28.03.2023)
2. Jon Brodkin How Unity3D Became a Game-Development Beast. URL: https://www.dice.com/career-advice/how-unity3d-become-a-game-development-beast (дата звернення 28.03.2023)

3. Ілля Сафронов. Що таке Unity? Курс для митців. URL: https://gamedev.dou.ua/ forums/ topic/38048/ (дата звернення 28.03.2023)
4. Glossary Gaming Engines. URL: https://www.arm.com/glossary/gaming-engines (дата звернення 28.03.2023)
5. Joe Hocking. Unity in Action: Multiplatform Game Development in C# with Unity 5. Publisher: Manning. 2018. 400p.
6. Офіційний сайт Unity. URL: https://unity.com/solutions/multiplatform (дата звернення 29.03.2023)
7. Офіційний сайт Sensor Tower. URL https://sensortower.com/blog/genshin-impact-mobile-two-years-analysis (дата звернення 30.03.2023)
8. Lindsay Schardon What is Unity? – A Guide for One of the Top Game Engines. URL: https://gamedevacademy.org/what-is-unity/#What_is_Unity (дата звернення 30.03.2023)
9. Tsyrulnyk, S. (2019). Застосування технології доповненої реальності у процесі підготовки фахівців з радіоелектроніки. Електронне наукове фахове видання «відкрите освітнє е-середовище сучасного університету», 355-362. URL: https://doi.org/10.28925/2414-0325.2019s32 (дата звернення 04.04.2023)
10. Мацокін, Д. В., & Пахомова, І. М. (2020). Платформи й мобільні додатки для створення та використання контенту із технологією доповненої реальності в освітньому процесі. *Проблеми сучасної освіти*, (11), 153-160. URL: https://periodicals.karazin.ua/issuesedu/article/view/17672 (дата звернення 06.04.2023)

Робота виконана під науковим керівництвом PhD, доцента
ДЕСЯТКО А. М.

ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ПЕРСОНАЛЬНИХ ДАНИХ У ВЕБСИСТЕМАХ

ПІХМАНЕЦЬ А., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

Стаття присвячена технологіям виявлення вразливостей персональних даних у веб-системах. У ній досліджуються загальні питання захисту персональних даних, такі як їх визначення, властивості, рівні захисту та забезпечення безпеки. Розглянуті різні види вразливостей персональних даних, що можуть виникати у вебсистемах, а також рекомендації щодо їх виявлення та виправлення. Автори наголошують на необхідності регулярного аудиту та тестування веб-систем з метою виявлення та виправлення вразливостей персональних даних та забезпечення їх безпеки.

The article is devoted to the technologies of detecting vulnerabilities of personal data in web systems. It explores the general issues of personal data protection, such as their definition, properties, levels of protection, and security. Various types of vulnerabilities of personal data that may arise in web systems are considered, as well as recommendations for their detection and correction. The authors emphasize the need for regular auditing and testing of web systems to detect and correct vulnerabilities of personal data and ensure their security.

Актуальність статті полягає в тому, що персональні дані стали надзвичайно цінними для кіберзлочинців, що призвело до зростання кількості кібератак на веб-системи з метою викрадення персональних даних користувачів. Тому виявлення та виправлення

вразливостей персональних даних у вебсистемах є надзвичайно важливим завданням для забезпечення їх безпеки та захисту користувачів від можливих кібератак. Дана стаття містить детальний огляд загальних питань захисту персональних даних та різні види вразливостей персональних даних, що можуть виникати у веб-системах, а також рекомендації щодо їх виявлення та виправлення. Отже, ця стаття має велике значення для розуміння проблеми захисту персональних даних та допоможе фахівцям забезпечити безпеку веб-систем та користувачів.

Метою статті є дослідження технологій виявлення вразливостей персональних даних у веб-системах. У статті будуть проаналізовані загальні питання захисту персональних даних, види вразливостей персональних даних, що можуть виникати у веб-системах, та методи їх виявлення та виправлення. Метою статті є також надання рекомендацій фахівцям з області кібербезпеки щодо захисту веб-систем та персональних даних користувачів від можливих кібератак.

Завданнями статті є:

- Дослідження загальних питань захисту персональних даних та їх важливості для користувачів веб-систем.
- Аналіз видів вразливостей персональних даних, що можуть виникати у веб-системах, та їх характеристик.
- Вивчення технологій виявлення вразливостей персональних даних у веб-системах та методів їх виправлення.
- Надання рекомендацій фахівцям з області кібербезпеки щодо захисту веб-систем та персональних даних користувачів від можливих кібератак.

Результатом статті буде поглиблене розуміння проблем захисту персональних даних у веб-системах, а також навичок виявлення та виправлення вразливостей персональних даних.

Об'єктом статті є технології виявлення вразливостей персональних даних у веб-системах.

Результатом дослідження є опис видів вразливостей персональних даних, що можуть виникати у веб-системах, та методів їх виявлення та виправлення.

Було визначено, що вразливості персональних даних можуть виникати через недостатні заходи безпеки, недостатню аутентифікацію користувачів, недостатню захист мережевого трафіку та інші фактори. В статті було описано типи вразливостей, такі як SQL-ін'єкції, Cross-Site Scripting (XSS), CSRF (Cross-Site Request Forgery) та інші.

Для виявлення вразливостей персональних даних веб-систем було проаналізовано методи, такі як сканування портів, сканування веб-додатків, аналіз коду, тестування з використанням зломника (penetration testing) та інші. Було наголошено на важливості постійного моніторингу веб-систем та забезпечення безпеки в режимі реального часу.

У статті було описано також методи виправлення вразливостей персональних даних, такі як патчі, оновлення програмного забезпечення, внесення змін у налаштування серверів та інші.

Результатом дослідження є набір рекомендацій для фахівців з кібербезпеки щодо захисту веб-систем та персональних даних користувачів. В статті було наголошено на важливості захисту персональних даних та розглянуто кроки, які можуть бути прийняті для запобігання можливих кібератак.

Зв'язок людей через Інтернет стає все більш популярним і важливим у сучасному світі. Інтернет-сервіси і веб-сайти пропонують користувачам широкий спектр послуг і можливостей, від соціальних мереж до онлайн-банкінгу і електронної комерції. Однак, збільшення обсягу зберігання та обробки персональних даних у веб-системах призводить до збільшення ризику витоку даних і порушення приватності. У зв'язку з цим, забезпечення безпеки та конфіденційності персональних даних стає все важливішим завданням для розробників веб-систем та користувачів.

Один з способів захисту персональних даних - це виявлення вразливостей веб-систем, які можуть бути використані зловмисниками для зламування безпеки даних. Виявлення

вразливостей дозволяє розробникам веб-систем вчасно виявляти та виправляти потенційні проблеми безпеки, тим самим зменшуючи ризик порушення безпеки даних. Водночас, це також дозволяє користувачам забезпечити свої дані веб-системи вищим рівнем захисту.

Отже, розробка технологій виявлення вразливостей персональних даних у веб-системах - це важлива проблема для забезпечення безпеки та конфіденційності персональних даних. Ця стаття присвячена дослідженню різних технологій виявлення вразливостей та їхнього застосування у практиці.

Поняття технології виявлення вразливостей персональних даних у веб-системах.

Технологія виявлення вразливостей персональних даних у веб-системах - це процес виявлення слабких місць у системі збору та обробки персональних даних, що можуть бути використані зловмисниками для незаконного доступу до цих даних або їх крадіжки. Ця технологія дозволяє підвищити рівень безпеки персональних даних, які збираються та обробляються веб-системами, і зменшити ризик втрати цих даних [1, 11].

Веб-системи є джерелом значної кількості персональних даних, таких як імена користувачів, адреси електронної пошти, паролі, кредитні картки, медичні записи та інші. Ці дані є дуже цінними для зловмисників, які можуть використовувати їх для зловживань, крадіжки особистості та шахрайства [2].

Один з ключових факторів, що забезпечують безпеку персональних даних у веб-системах, є виявлення та усунення вразливостей. Вразливості - це слабкі місця в системі, які можуть бути використані для отримання несанкціонованого доступу до даних. Виявлення та усунення вразливостей є важливими процесами, що допомагають зменшити ризик порушення безпеки даних у веб-системах [3, 12].

Один з типів вразливостей, що можуть бути знайдені у веб-системах, - це SQL-ін’єкція. Ця вразливість відбувається тоді, коли зловмисник може ввести SQL-запит у форму на веб-сайті, що призводить до виконання несанкціонованого запиту до бази даних. Це може дозволити зловмиснику отримати доступ до конфіденційних даних, які зберігаються у базі даних [10].

Ще одна вразливість, що можна знайти в веб-системах - це кросс-сайт скриптінг (XSS). Ця вразливість дозволяє зловмисникам вставляти скрипти на веб-сторінки, які відвідують інші користувачі. Це може призвести до крадіжки даних, таких як паролі та кредитні картки [9].

Одним із способів виявлення уразливостей є підходи, що базуються на побудові або аналізі моделей загроз. Моделі загроз відображають сценарії або послідовності дій, які можуть призвести до порушення конфіденційності, цілісності або доступності даних. Для побудови моделей загроз часто використовуються уразливості, що вже були виявлені та вивчені, а також типові сценарії атак [4].

Іншим підходом є використання технологій аналізу коду програмного забезпечення, які можуть допомогти виявити уразливості на рівні джерела. Наприклад, статичний аналізатор коду може знайти ділянки коду, які можуть призвести до SQL-ін’єкції або переповнення буфера. Динамічні інструменти аналізу виконання програм можуть виявляти уразливості на основі взаємодії програми з оточенням [10].

З врахуванням того, що веб-системи містять багато персональної інформації, включаючи ім’я, електронну пошту, паролі, фінансову інформацію та інше, важливо забезпечити безпеку даних у веб-системах. Для цього можуть бути використані різні технології та підходи. Зараз на ринку існує багато технологій та підходів до виявлення вразливостей персональних даних у веб-системах. Ось деякі з них:

- Сканування портів: ця технологія дозволяє виявляти вразливості, пов’язані з портами веб-серверів, на яких розміщені веб-системи.
- Тестування на проникнення: ця технологія дозволяє виявляти вразливості, пов’язані зі зломом системи, з використанням спеціальних програм для тестування на проникнення.

- Відслідковування атак: цей підхід полягає в використанні спеціальних програм, які відслідковують вразливості в режимі реального часу та надсилають повідомлення про спроби злому.
- Використання SSL-шифрування: ця технологія дозволяє захистити персональні дані, передані між користувачем та веб-системою, від прослуховування.
- Використання різноманітних методів аутентифікації: цей підхід дозволяє забезпечити захист від несанкціонованого доступу до персональних даних за допомогою використання різноманітних методів аутентифікації, таких як паролі, коди підтвердження та інші.

Ще одним підходом є використання технологій тестування на проникнення, що дозволяють виявити уразливості шляхом спроб використання вразливостей програми з метою отримання доступу до конфіденційної інформації або злому системи.

Крім того, важливо пам'ятати про регулярне виконання аудиту безпеки системи, що дозволяє виявляти уразливості та проводити профілактичні заходи для їх запобігання. Аудит безпеки включає перевірку параметрів системи, конфігурацію мережі, аналіз журналів подій та інших системних параметрів [6].

Однак, незважаючи на наявність різних методів виявлення уразливостей, цей процес завжди залишається складним та вимагає великої уваги.

Методи виявлення вразливостей персональних даних у веб-системах. Існує кілька методів виявлення вразливостей персональних даних у веб-системах, такі як:

1. Аналіз коду програми. Цей метод використовується для виявлення слабких місць у коді програми, що можуть бути використані для незаконного доступу до персональних даних. Цей метод зазвичай використовується на етапі розробки програмного забезпечення [3–4, 5].

2. Тестування на проникнення. Цей метод використовується для симуляції атак на веб-систему з метою виявлення слабких місць, які можуть бути використані зловмисниками. Під час тестування на проникнення використовуються різні інструменти, які дозволяють виявляти вразливості веб-системи та проводити тестування безпеки [4, 5].

3. Аналіз безпеки мережі. Цей метод використовується для виявлення вразливостей в мережі, яка забезпечує доступ до веб-системи. Під час аналізу безпеки мережі досліджуються різні аспекти, такі як налаштування мережевих пристроїв, наявність захисних механізмів та інші параметри, які впливають на безпеку веб-системи [6, 5].

4. Моніторинг системи. Цей метод використовується для постійного відслідковування подій у веб-системі з метою виявлення незвичайної поведінки та потенційних загроз безпеці персональних даних. Моніторинг системи зазвичай проводиться за допомогою спеціальних програмних засобів, які дозволяють аналізувати журнали подій та виявляти потенційні загрози [9, 5].

Інструменти виявлення вразливостей персональних даних у веб-системах.

Існує багато інструментів, які дозволяють виявляти вразливості персональних даних у веб-системах. Деякі з них наведені нижче:

1. Nessus. Цей інструмент дозволяє проводити тестування на проникнення та виявляти вразливості веб-системи. Він містить базу даних з вразливостями та дозволяє виконувати різноманітні сканування, щоб виявляти потенційні загрози безпеці [9, 7].
2. Metasploit. Цей інструмент є потужним інструментом тестування на проникнення, який дозволяє використовувати різні експлойти для злому веб-системи. Він має велику базу даних з вразливостями та дозволяє проводити автоматизовані тестування на проникнення [1, 6, 7].
3. Burp Suite. Цей інструмент є одним з найпопулярніших інструментів для тестування на проникнення. Він має багато різноманітних функцій, таких як перехоплення трафіку, модифікація запитів та відповідей, аналіз вразливостей та інші [7].

4. OpenVAS. Цей інструмент є відкритим інструментом тестування на проникнення та виявлення вразливостей. Він має базу даних з вразливостями та дозволяє проводити сканування веб-систем для виявлення потенційних загроз безпеці [7].
5. Wireshark. Цей інструмент є програмою для аналізу мережевого трафіку. Він дозволяє перехоплювати трафік, аналізувати його та виявляти потенційні загрози безпеці [2, 7].

Заходи для запобігання вразливостей персональних даних у веб-системах

Щоб запобігти вразливостям персональних даних у веб-системах, необхідно вживати певні заходи безпеки. Нижче наведено деякі з них:

1. Шифрування даних. Важливо застосовувати шифрування для захисту персональних даних під час їх передачі через мережу. Це можна зробити за допомогою протоколів шифрування, таких як SSL або TLS.
2. Регулярні оновлення програмного забезпечення. Регулярні оновлення програмного забезпечення дозволяють виправляти виявлені вразливості та підвищувати загальний рівень безпеки веб-системи [8].
3. Використання складних паролів. Важливо використовувати складні паролі для доступу до веб-систем. Це дозволяє зменшити ризик злому пароля та неправомірного доступу до персональних даних.
4. Автентифікація та авторизація. Важливо реалізувати механізми автентифікації та авторизації для забезпечення захисту персональних даних веб-системи від неправомірного доступу.
5. Захист від SQL-ін’єкцій та інших атак. Важливо використовувати заходи для запобігання SQL-ін’єкціям та іншим типам атак, таким як валідація даних та коректна обробка введених даних [10].
6. Захист від Cross-Site Scripting (XSS). Важливо використовувати заходи для запобігання атакам XSS, таким як екранування спецсимволів та фільтрація введених даних [9].

Висновки.

Виявлення вразливостей персональних даних у веб-системах є надзвичайно важливим для забезпечення безпеки та захисту персональних даних. Існує багато інструментів для виявлення вразливостей, які дозволяють проводити тестування на проникнення та аналіз веб-систем. Однак, на практиці, найбільш ефективним є комплексний підхід, що включає в себе використання різних інструментів та заходів безпеки.

Захист персональних даних є важливою складовою сучасного світу, оскільки захист даних є основою для захисту особистої свободи та приватності людини. Тому, забезпечення захисту персональних даних у веб-системах має важливе значення для бізнесу та суспільства в цілому.

Висновки, які можна зробити, полягають у тому, що необхідності регулярного аудиту та тестування веб-систем з метою виявлення та виправлення вразливостей персональних даних. Також важливо враховувати рекомендації та заходи безпеки при розробці та експлуатації веб-систем.

Отже, виявлення вразливостей персональних даних у веб-системах є актуальною темою, оскільки персональні дані є важливим ресурсом для бізнесу та суспільства в цілому. Для захисту персональних даних веб-систем необхідно використовувати комплексний підхід, який включає в себе використання різних інструментів та заходів безпеки. Регулярне тестування та аудит веб-систем дозволить виявляти та виправляти вразливості персональних даних та забезпечити захист цих даних від неправомірного доступу.

Список використаних джерел

1. OWASP. (2021). Top Ten Project. Retrieved from https://owasp.org/Top10/
2. NIST. (2020). Guide to Privacy Risk Assessment. Retrieved from https://www.nist.gov/publications/guide-privacy-risk-assessment
3. European Commission. (2018). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX: 32016R0679 &from=EN
4. Zhang, Y., Han, J., & Cheng, J. (2020). Security vulnerabilities and protection of personal information in web applications: A review. Journal of Ambient Intelligence and Humanized Computing, 11(8), 3475-3490. https://doi.org/10.1007/s12652-019-01314-6
5. Acunetix. (2021). The ultimate guide to web application security. Retrieved from https://www.acunetix.com/blog/docs/the-ultimate-guide-to-web-application-security/
6. SANS Institute. (2021). SANS Top 20 Critical Security Controls. Retrieved from https://www.sans.org/sans-top-20-critical-security-controls/
7. Zawoad, S., Hasan, R., & Hasan, M. (2019). Detecting and preventing web application security vulnerabilities: A survey. Journal of Network and Computer Applications, 138, 1-23. https://doi.org/10.1016/j.jnca.2019.04.019
8. Microsoft. (2021). Best practices for preventing information leaks. Retrieved from https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/best-practices-for-preventing-information-leaks
9. IBM Security. (2021). Data privacy and protection. Retrieved from https://www.ibm.com/security/data-privacy
10. Veracode. (2021). Web Application Security: What You Need to Know. Retrieved from https://www.veracode.com/security/web-application-security.
11. Bebeshko, B., Khorolska, K., Kotenko, N., Kharchenko, O., & Zhyrova, T. (2021). Use of neural networks for predicting cyberattacks. Paper presented at the CEUR Workshop Proceedings, , 2923 213-223. http://ceur-ws.org/Vol-2923/paper23.pdf
12. Lakhno V., Akhmetov B., Ydyryshbayeva M., Bebeshko B., Desiatko A., Khorolska K. (2021) Models for Forming Knowledge Databases for Decision Support Systems for Recognizing Cyberattacks. In: Vasant P., Zelinka I., Weber GW. (eds) Intelligent Computing and Optimization. ICO 2020. Advances in Intelligent Systems and Computing, vol 1324. Springer, Cham. https://doi.org/10.1007/978-3-030-68154-8_42

Робота виконана під науковим керівництвом старшого викладача
БЕБЕШКО Б. Т.

ЗАХИСТ ДАНИХ ПРИ ПЕРЕДАЧІ ІНФОРМАЦІЇ В КАНАЛАХ БЕЗДРОТОВОГО ЗВ'ЯЗКУ В УКРАЇНІ

ПЛОХИЙ М., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто канали бездротового зв'язку в Україні, а також описано основні проблеми захисту передачі інформації. Розглянуто різні типи зловмисних атак, що можуть бути спрямовані на бездротові мережі, а також запропоновані різні методи захисту даних при передачі інформації в бездротових мережах в Україні.

This article examines wireless communication channels in Ukraine, and also describes the main problems of information transmission protection. Different types of malicious attacks that can be aimed at wireless networks are considered, as well as different methods of data protection during information transmission in wireless networks in Ukraine are proposed.

Актуальність. Тема захисту даних при передачі інформації в каналах бездротового зв'язку є дуже актуальною в Україні, так само як і в інших країнах світу. Зростаюча популярність бездротових технологій та зростаюча кількість пристроїв, які використовують бездротовий зв'язок, робить цю тему надзвичайно важливою. Україна, як і багато інших країн світу, залежить від бездротових мереж для забезпечення зв'язку в багатьох сферах, включаючи бізнес, медицину, громадський транспорт та інші. Проте, бездротові мережі можуть бути дуже вразливими до різних видів кібератак, таких як перехоплення даних, віруси та зловмисний код. Це може призвести до крадіжки конфіденційної інформації, в тому числі фінансових даних, медичної інформації, персональних даних та інших.

Таким чином, захист даних при передачі інформації в каналах бездротового зв'язку є надзвичайно важливою проблемою в Україні, яка потребує серйозної уваги та заходів щодо її вирішення.

Метою статті є дослідження проблем захисту даних при передачі інформації в каналах бездротового зв'язку є дуже актуальною в Україні. Також метою є спонукання до свідомого використання бездротових мереж та до виконання правил безпеки в процесі передачі даних через ці мережі.

Об'єктом дослідження є процес передачі даних через бездротові мережі і проблеми, які виникають у зв'язку з недостатнім захистом цих даних.

Предметом дослідження є способи забезпечення безпеки і захисту даних, які передаються через бездротові мережі в Україні.

Аналіз попередніх досліджень. Дослідження на тему захисту даних при передачі інформації в каналах бездротового зв'язку в Україні ведуться вже протягом кількох років. Серед українських вчених, які займалися цією темою, можна відзначити таких: Калашникова Ірина Валентинівна – доктор технічних наук, професор, провідний науковий співробітник Інституту телекомунікацій та глобальної інформації при НАН України; Губаренко Сергій Олександрович – доктор технічних наук, професор, головний науковий співробітник Інституту телекомунікацій та глобальної інформації при НАН України; Лисенко Андрій Вікторович – доктор технічних наук, професор, завідувач кафедри інформаційної безпеки та комп'ютерних технологій в Національному технічному університеті України «Київський політехнічний інститут». Деякі з них були присвячені загальним питанням захисту даних в бездротових мережах, тоді як інші були спрямовані на вивчення конкретних аспектів цієї теми. Наприклад, в дослідженні «Аналіз методів захисту бездротових мереж в Україні» автори проаналізували різні методи захисту бездротових мереж, які використовуються в Україні. У дослідженні було встановлено, що більшість бездротових мереж в Україні використовують метод WPA2 для захисту даних, але також було виявлено проблеми з безпекою деяких мереж. Інше дослідження, «Аналіз методів криптографічного захисту даних в бездротових мережах» було спрямоване на вивчення методів криптографічного захисту даних в бездротових мережах. У дослідженні було досліджено такі методи захисту даних, як AES, DES і RSA, і було встановлено, що захист даних, які передаються через бездротові мережі, може бути підвищений, якщо використовувати сучасні методи криптографічного захисту.

Загалом, попередні дослідження підтверджують необхідність ретельного аналізу протоколів зв'язку і методів захисту для забезпечення безпеки при передачі даних в каналах бездротового зв'язку. Також дослідження підкреслюють важливість постійного вдосконалення заходів захисту даних для забезпечення безпеки від нових загроз.

Виклад основного матеріалу. Захист даних при передачі інформації в каналах бездротового зв'язку є важливою проблемою в сучасному світі, де бездротові мережі використовуються в різних сферах діяльності, включаючи бізнес, освіту, медицину та інше.

За даними Державної служби статистики України, станом на 2021 рік, понад 50 % населення України користується бездротовим інтернетом. Крім того, кількість підключень до мобільного інтернету в Україні зростає щороку. За даними Асоціації операторів зв'язку України (АОЗТ), станом на кінець 2020 року, в Україні налічувалося понад 51 мільйонів підключень до мобільного інтернету, що є на 9 % більше порівняно з 2019 роком.

Також, за даними Всесвітнього інтернет-ресурсу Speedtest.net, середня швидкість інтернет-з'єднання в Україні зросла в 2020 році на 23,9 %, до 54,21 Мбіт/сек. З цим показником Україна займає 63 місце у світовому рейтингу.

Україна має законодавчу базу, що регулює захист персональних даних, включаючи дані, що передаються в каналах бездротового зв'язку. Основним законом в цій сфері є Закон України «Про захист персональних даних», прийнятий у 2010 році [4].

Згідно з цим законом, оператори мереж зв'язку повинні забезпечувати захист персональних даних під час їх збору, обробки та передачі. Оператори мереж повинні також забезпечувати конфіденційність та цілісність даних, що передаються в каналах бездротового зв'язку.

Національний регуляторний орган - Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ) - має право встановлювати вимоги щодо захисту персональних даних в мережах зв'язку.

Захист даних в каналах бездротового зв'язку є критичним завданням, оскільки такі мережі набувають все більшої популярності і застосовуються в багатьох галузях [5, с. 75].

Захист даних має здійснюватися, насамперед, шляхом проведення виваженої та збалансованої політики держави в електронній сфері, яка має три основні вектори:

- захист інформаційних прав і свобод людини, захист державної безпеки в електронній сфері та захист національного
- інформаційного ринку, економічних інтересів держави в електронній сфері, національних виробників інформаційної продукції [1].

Інформаційна політика інформаційного забезпечення важлива в Україні з кількох причин. По-перше, в умовах росту кількості інформації, яку ми передаємо та обробляємо, важливо мати політику, яка допоможе забезпечити належний захист цієї інформації. Захист персональних даних, конфіденційності комерційної інформації, та іншої важливої інформації є ключовим елементом інформаційної політики. По-друге, інформаційна політика допомагає управляти ризиками, пов'язаними зі зберіганням та обробкою інформації. Вона включає в себе планування заходів безпеки, оцінку ризиків, розробку політики доступу, використання технологій захисту даних, та інші заходи для забезпечення безпеки інформації. По-третє, інформаційна політика допомагає забезпечити дотримання вимог законодавства в галузі захисту інформації. Зокрема, в Україні існують закони та правила, які встановлюють вимоги щодо захисту персональних даних, конфіденційності інформації, та інших аспектів безпеки інформації. Інформаційна політика допомагає забезпечити дотримання цих вимог.

Така політика допомагає забезпечити належний захист персональних даних, управляти ризиками, та дотримуватись вимог законодавства.

Україна має основні цілі інформаційної політики інформаційного забезпечення. Основними з них є:

- захист інформаційного суверенітету держави (особливо захист національного інформаційного простору з інформаційним ресурсом і систем формування масової суспільної свідомості) в сучасних умовах глобалізації та інтернаціоналізації процесів в електронній сфері;
- рівня інформаційної достатності для прийняття рішень державними органами, підприємствами та громадянами;

- реалізацію конституційних прав і свобод громадян, суспільства і держави на інформацію [3 с. 384].

Україна має декілька типів каналів бездротового зв'язку, які використовуються для передачі інформації.

Таблиця 1

Канали бездротового зв'язку та методи передачі інформації

Тип каналу	Метод передачі інформації
GSM (2G)	Частотна модуляція з фазовим зсувом (GMSK)
UMTS (3G)	Квадратурна фазова модуляція (QPSK) та 16-кувантова амплітудна модуляція (16QAM)
LTE (4G)	Квадратурна фазова модуляція (QPSK, 16QAM, 64QAM)
5G	Квадратурна фазова модуляція (QPSK, 16QAM, 64QAM) та 256QAM
Wi-Fi	Квадратурна амплітудна модуляція (QAM) та фазова модуляція (PM)
Bluetooth	Частотна гопперова модуляція (FHSS) та широкосмугова частотна модуляція (WBFM)
NFC (ближньодіапазонна комунікація)	Амплітудна модуляція (AM)
Zigbee	Частотна модуляція з фазовим зсувом (FSK) та квадратурна амплітудна модуляція (QAM)
LoRa	Розширення спектру частоти (FSK) та розширення спектру частоти з фазовим зсувом (FSK + PSK)

Wi-Fi використовує радіохвилі для передачі даних між різними пристроями. Wi-Fi є широко поширеною технологією в Україні і використовується для бездротового доступу до Інтернету, а також для бездротової мережі у побутових та офісних приміщеннях.

Bluetooth використовує радіохвилі для передачі даних між різними пристроями на невеликій відстані. Bluetooth використовується для передачі даних між мобільними пристроями, такими як смартфони, планшети, навушники, та інші пристрої.

NFC використовується для безконтактної передачі даних між двома пристроями. NFC використовується для безконтактної оплати, обміну даними між пристроями, інтерактивних рекламних кампаній та інших сценаріїв.

Zigbee використовується для передачі даних на коротких відстанях між різними пристроями. Zigbee використовується в інтернеті речей, смарт-домах, системах безпеки та інших промислових застосуваннях.

LTE використовується для передачі даних у мережах мобільного зв'язку. LTE є стандартом 4G та використовується для передачі даних на великій відстані у діапазонах частот, що належать операторам мобільного зв'язку.

5G передбачає значні покращення швидкості передачі даних, зниження затримок мережі та підвищення пропускної здатності. 5G також використовує діапазони частот, які належать операторам мобільного зв'язку, але знаходиться у процесі розгортання.

LoRaWAN використовується для підключення різних пристроїв до Інтернету речей на великі відстані. Ця технологія використовується для збір даних з датчиків віддалених пристроїв у міських та сільських областях, де інші технології можуть бути неефективними.

Важливо зазначити, що кожна з цих технологій має свої власні вимоги до захисту даних та протоколи безпеки, які повинні бути дотримані при передачі інформації в каналах бездротового зв'язку.

Згідно статистики (Рис.1) можна зробити висновок, що з кожним роком користувачів бездротової мережі стає все більше. Отже, збільшується необхідність посилювати захист передачі даних.

Рис. 1. Динаміка користування Інтернетом в Україні

Найбільш поширеною проблемою безпеки в бездротових мережах є недостатня захист від несанкціонованого доступу до мережі та передаваної інформації [8, с. 217].

Існує кілька ризиків та викликів, пов'язаних із захистом даних при передачі інформації в каналах бездротового зв'язку в Україні. Основні з них:

1. Небезпека перехоплення даних. При передачі інформації в каналах бездротового зв'язку, дані можуть бути перехоплені зловмисниками, які можуть використовувати ці дані для своїх злочинних цілей.
2. Недостатня захищеність мережі. Часто мережі бездротового зв'язку можуть бути недостатньо захищеними від зловмисників, які можуть використовувати ці мережі для атак на комп'ютери та інші пристрої користувачів.
3. Відсутність шифрування. Якщо передача даних не зашифрована, зловмисники можуть легко зрозуміти та використовувати ці дані.
4. Відсутність обмежень доступу. У разі відсутності обмежень доступу до бездротових мереж можуть використовуватися незаконними користувачами для зловживання.
5. Недостатній захист пристроїв. Якщо пристрої не мають достатньої захищеності, зловмисники можуть здійснювати атаки на ці пристрої та отримувати доступ до важливої інформації.

Для забезпечення захисту даних в каналах бездротового зв'язку необхідно застосовувати комплексний підхід, який включає в себе технічні та організаційні заходи [7, с. 41].

Загалом, захист даних при передачі інформації в каналах бездротового зв'язку є важливою задачею, яку необхідно вирішувати з урахуванням законодавчих вимог та використанням сучасних технічних засобів захисту даних.

Законодавчі вимоги регулюються Міністерством інформаційної політики України. Основними завданнями Міністерства інформаційної політики України є:

- забезпечення формування державної політики щодо діяльності засобів масової комунікації;
- формування стратегії інформаційної політики держави та забезпечення її дотримання;
- реалізація державної політики у сферах поширення інформації, просвітницької діяльності і використання національних інформаційних ресурсів;
- створення умов для розвитку інформаційного суспільства, а також у сфері здійснення державного нагляду (контролю) за діяльністю засобів масової комунікації незалежно від їх підпорядкування і форми власності [3].

Один із способів захисту даних в каналах бездротового зв'язку - це шифрування, яке дозволяє забезпечити конфіденційність інформації та запобігти її неправомірному доступу [6].

Існує кілька методів захисту даних при передачі інформації в каналах бездротового зв'язку в Україні:

- Використання методів ідентифікації користувачів, таких як аутентифікація по сертифікату, паролю або відбитку пальця.
- Використання фаєрволів та інших засобів захисту мережі від несанкціонованого доступу.
- Використання методів фізичного захисту, таких як зберігання пристроїв з підключенням до бездротової мережі в захищених приміщеннях або використання замків та інших засобів захисту.

Для забезпечення безпеки передачі даних в каналах бездротового зв'язку можна використовувати різні методи шифрування, такі як WPA2, WPA3, або інші стандарти шифрування даних, які відповідають вимогам безпеки. Для аутентифікації користувачів можуть використовуватись такі методи, як паролі, сертифікати, біометричні дані.

Протокол WPA2 залишається одним з найбільш популярних та ефективних методів захисту бездротових мереж. Він забезпечує високий рівень безпеки, використовуючи сильне шифрування трафіку та слабкі ключі шифрування на основі протоколу WPA2 були покращені за останні роки, але все ще існують деякі вразливості, які можуть бути використані зловмисниками для отримання доступу до бездротової мережі [11].

Протокол WPA2 (Wi-Fi Protected Access II) є одним з найбільш поширених протоколів для захисту бездротового зв'язку. Цей протокол був розроблений з метою покращення безпеки бездротових мереж Wi-Fi, що використовують стандарт 802.11. Протокол WPA2 використовує алгоритми шифрування AES (Advanced Encryption Standard) і TKIP (Temporal Key Integrity Protocol), що дозволяє забезпечити високий рівень захисту даних в бездротових мережах. Крім того, WPA2 включає в себе механізм аутентифікації IEEE 802.1X, який дозволяє перевіряти ідентифікацію користувача та дозволяти доступ до мережі тільки авторизованим користувачам. WPA2 також має певні недоліки, що можуть бути використані для атак на бездротову мережу. Наприклад, атака на перехоплення WPA2-PSK ключа, яка полягає у вилученні пароля для доступу до мережі, може бути успішною в разі використання слабкого пароля.

Однак, навіть з використанням таких протоколів, існують можливості для атак на бездротові мережі, такі як атака «чоловік-у-середині» (Man-in-the-Middle) або атака «зміни довіри» (Trust Hijacking). Тому, для забезпечення ефективного захисту даних у каналах

бездротового зв'язку, необхідно використовувати додаткові заходи захисту, такі як захист від DDoS атак, захист від зловмисних програм, захист від перехоплення сигналу та інші. Крім того, важливо дотримуватись правильної конфігурації мережі та використовувати сильні паролі для доступу до мережі.

Оператори мереж зв'язку повинні також забезпечувати захист від несанкціонованого доступу до мережі, зокрема, використовуючи мережеві протоколи, такі як MAC-адреса, які обмежують доступ до мережі лише для авторизованих користувачів.

MAC-адреса є унікальним ідентифікатором мережевої карти, який використовується для передачі даних в мережах з локальним доступом. Кожна мережева карта має свій власний MAC-адрес, що дозволяє ідентифікувати її в мережі та передавати дані [10].

MAC-адреса (Media Access Control address) - це унікальний ідентифікатор, який призначений для кожного мережевого пристрою, такого як комп'ютер, смартфон, роутер або інший пристрій, який може бути підключений до мережі. MAC-адреса може бути відображена у вигляді шістнадцяткового числа, яке складається з шести пар цифр і літер, розділених двокрапкою. Кожний виробник мережевих пристроїв призначає унікальний MAC-адрес своїм пристроям. Це дозволяє мережевому обладнанню ідентифікувати та взаємодіяти з іншими пристроями у мережі. Крім того, MAC-адреса використовується для контролю доступу до мережі, наприклад, при налаштуванні списку дозволених пристроїв для підключення до Wi-Fi.

MAC-адреса працює на другому рівні моделі OSI (Data Link Layer). Вона використовується для передачі даних між двома пристроями в мережі, що знаходяться на одному рівні мережевої моделі. Наприклад, коли комп'ютер надсилає запит до сервера, він включає MAC-адресу свого мережевого адаптера, щоб інші пристрої в мережі могли відправити відповідь.

Окрім того, користувачі бездротових мереж повинні дотримуватись певних правил безпеки, таких як використання складних паролів, не використовувати мережі без авторизації, встановлення програмного забезпечення для захисту від шкідливих програм.

Дуже важливо ретельно перевіряти налаштування бездротової мережі та використовувати надійні паролі для забезпечення безпеки під час передачі даних в бездротовому режимі [9, с. 117].

Україна має національний регуляторний орган, який відповідає за розвиток та нагляд за забезпеченням ефективної та безпечної роботи телекомунікаційних послуг. Цим органом є Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ).

Національний регуляторний орган має право проводити перевірки операторів мереж зв'язку на дотримання вимог щодо захисту персональних даних, включаючи дані, що передаються в каналах бездротового зв'язку. В разі порушення вимог щодо захисту даних можуть бути застосовані адміністративні, грошові та кримінальні санкції. Проведення перевірок з боку НКРЗІ є важливим елементом забезпечення захисту персональних даних в Україні, оскільки це забезпечує виконання законодавчих вимог та відповідність міжнародним стандартам у цій сфері.

Висновки. Захист даних при передачі інформації в каналах бездротового зв'язку в Україні є важливою задачею, яка вимагає використання різноманітних технічних та організаційних заходів, включаючи дотримання законодавчих вимог та правил безпеки операторами мереж та користувачами.

Забезпечення безпеки при передачі даних в каналах бездротового зв'язку в Україні є необхідним завданням для захисту особистих даних користувачів та запобігання можливим кібератакам. Для досягнення цієї мети потрібні спільні зусилля операторів мереж та користувачів. Незахищені мережі можуть бути легко підмінені та скомпрометовані зловмисниками, що може призвести до витоку конфіденційної інформації, викрадення особистих даних та ідентифікаційної інформації. Це може призвести до серйозних проблем з безпекою та фінансовими збитками.

Тому, щоб забезпечити безпеку та захист конфіденційної інформації, необхідно використовувати ефективні заходи безпеки в мережах Wi-Fi та інших каналах бездротового

зв’язку. Це включає в себе використання протоколів шифрування, встановлення файрволів та систем ідентифікації користувачів, регулярне оновлення програмного забезпечення та інші заходи безпеки.

Важливою є розробка та впровадження нових технологій та стандартів бездротового зв’язку, які забезпечують високий рівень безпеки при передачі даних. Наприклад, розробка нових протоколів шифрування та аутентифікації, які відповідають вимогам безпеки та можуть бути використані для захисту даних під час їх передачі в каналах бездротового зв’язку. Необхідно проводити регулярні навчання та тренінги для операторів мереж зв’язку та користувачів, щоб підвищити рівень обізнаності щодо правил безпеки при використанні бездротового зв’язку та запобігти можливим кібератакам.

Захист даних при передачі інформації в каналах бездротового зв’язку в Україні є важливою та актуальною темою, яка потребує уваги та дій з боку всіх зацікавлених сторін. Тільки за спільних зусиль можна забезпечити високий рівень безпеки при використанні бездротового зв’язку та запобігти можливим кібератакам.

Список використаних джерел

1. Корупційні ризики в діяльності державних службовців: роз’яснення міністерства юстиції України від 12.04.2011 р. [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/n0026323-11].
2. Дзьобань О.П., Ставицька О.В. Депривaційний стан суспільства і питання національної безпеки // О.П. Дзьобань, О.В. Ставицька / Психологічні аспекти національної безпеки: Тези Другої Міжнародної науково-практичної конференції. – Львів : Львівський державний університет внутрішніх справ, 2008. – С. 70–75.
3. Правове забезпечення інформаційної діяльності в Україні / за заг. ред. Ю.С. Шемшученка, І.С. Чижа. – К.: ТОВ «Юридична думка», 2006. – 384 с.
4. Закону України від 1 червня 2010 року № 2297-VI «Про захист персональних даних» - Стаття 10.
5. Карпенко В.І., Захист інформації в комп’ютерних системах та мережах, Київ, 2014. 75–75 с.
6. Баклан О.Ю., «Безпека інформації в комп’ютерних системах», Київ, 2013.
7. Яковенко Ю.О., «Інформаційна безпека: навчальний посібник», Київ, 2012. 41 с.
8. Козачок О.М., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. / «Безпека комп’ютерних систем: підручник» / Київ, 2015. 217 с.
9. Матяш О.В. Комп’ютерна безпека. Захист інформації. - К.: Навчальна книга, 2018. 117–120 с.
10. Джеймс Ф. Куроуз і Кіт В. Росс. Комп’ютерні мережі: підхід «зверху вниз. 7-ме видання. 2019 р. 70–75 с.
11. Абдала А.С. «Безпека бездротової локальної мережі: Огляд протоколів WEP, WPA та WPA2». 2021 рік. 311–316 с.

Робота виконана під науковим керівництвом д-ра екон. наук, професора
ТОКАРЯ В. В.

РІЗНОВИДИ ГЕНЕРАТИВНИХ МОДЕЛЕЙ У ГРАФІЧНИХ ПРОГРАМАХ ДЛЯ РОБОТИ З ТРИВИМІРНОЮ ГРАФІКОЮ

ПОБЕРЕЖНИЙ В., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто певні різновиди генеративних моделей у програмі для роботи з тривимірною графікою, Blender. Зазначено переваги та недоліки використаних підходів в ході створення та стилізації 3D-об'єктів.

The article considers certain types of generative models in the software program for working with 3D-graphics, Blender. The advantages and disadvantages of the approaches used in the creation and stylization of 3D-objects are noted.

Актуальність генеративних моделей в різних сферах людської діяльності, попри очевидний попит використання в ігровій індустрії, підтверджується масштабністю у використанні даного методу для вирішення різноманітних задач. Цей підхід шириться від генеративно створених, художніх одиниць із розмаїттям візерунків у візуальному мистецтві, до додатку IKEA Place із алгоритмом створення 3D-меблів, а також вкрай актуальних на сьогодні генеративних моделей для автоматизованого розпізнавання й ідентифікації ворожої техніки. Ми маємо потребу в швидкому та ефективному створенні складних тривимірних моделей, що могли б відображати реальні об'єкти та процеси для вдалого відтворення нами віртуальних світів, відповідних до наших бажань, цілей та запитів. Як наслідок - отримуємо технологічні пропозиції в якості різновидів генеративних моделей-шаблонів для роботи з тривимірною графікою.

Традиційні методи створення 3D-моделей вимагають значних зусиль та часу. У цьому контексті можливість генеративності контенту через певні патерни стала необхідним інструментом для ефективного та швидкого створення моделей, що задовольняють високі стандарти якості. Це надає можливість автоматично генерувати складні моделі з витратою ресурсу спеціаліста лише на налаштування шаблону, що в свою чергу дозволяє зосередитися на творчому процесі та оптимізувати часові затрати.

Метою даної статті є дослідження різновидів генеративних моделей у графічній програмі для роботи з тривимірною графікою. В статті будуть розглянуті можливості програми Blender, її модифікатора Array, інтеграції бібліотеки PyTorch3D, що дають змогу зрозуміти, яким чином генеративні моделі можуть бути використані для створення 3D-моделей.

Об'єктом дослідження є різновиди генеративних моделей у графічній програмі для роботи з тривимірною графікою.

Предмет дослідження - графічна програма Blender.

Аналіз попередніх досліджень. Дослідженням генеративних моделей займались у своїх працях такі іноземні науковці: Jiajun Wu, Chengkai Zhang, Tianfan Xue, William T. Freeman, Joshua B. Tenenbaum, Lyle Regenwetter, Amin Heyrani Nobari, Faez Ahmed, Haisheng Li1, Yanping Zheng, Xiaoqun Wu, Qiang Cai1, Tianyu Zhou, Weidan Xiong, Yuki Obata, Carlos Lange, Yongsheng Ma.

Виклад основного матеріалу. Генеративні моделі можна описати як клас алгоритмів, які використовуються для створення нових даних, які вони ніколи не бачили раніше, але які можуть здатися реальними або достатньо правдоподібними для їх відтворення. Принцип роботи генеративних моделей полягає в тому, що вони використовують створені алгоритми здатні продукувати на основі існуючих даних нові. Ці алгоритми можуть включати в себе випадкові числа, математичні формули, генеративні сітки та інші техніки для створення даних.

Що робить генеративну модель об’єктів у тривимірному просторі привабливою? Вважається, що хороша генеративна модель повинна здатна створювати тривимірні об’єкти, які є одночасно різноманітними та реалістичними. Зокрема, для того, щоб тривимірні об’єкти мали варіації, генеративна модель повинна здатна виходити за рамки запам’ятовування та перекомбінування частин або елементів з попередньо визначеного репозиторію для створення нових форм; а для того, щоб об’єкти були реалістичними, у згенерованих прикладах повинні бути дрібні деталі [1].

Один з підходів, який певним чином задовольняє характеристику унікальності створених об’єктів та містить в собі частку випадковості це процедурна генерація. Концепт вдало існує та часто застосовується в іграх для вирішення проблем великих світів, майже нескінченних масштабів та відтворення унікального ігрового досвіду для гравців у таких продуктах як «No Man’s Sky», «Minecraft», «Don’t Starve» і багатьох інших, менш популярних ігрових одиницях.

Принцип процедурної генерації полягає в створенні певного алгоритму, який автоматично створює об’єкти що виходять із заданих раніше або випадкових параметрів [2]. У Blender відтворення алгоритму здійснюється за допомогою використання Blender’s Python API. Із використанням розділу «Scripting», в Blender розширюються функціональні можливості створення об’єктів та їх генерації.

Створимо генеративну модель що буде абстракцією невеликого поля кубів із сіткою(7x7), алгоритм якої буде працювати перебираючи вказану розмірність(комірки), моделювати на певній відстані можливу кількість об’єктів, спираючись на вказані нами дані: розмір, перепади висоти, візуальні матеріали(колір). Створивши новий скрипт «cube.py» дамо дозвіл на викликання функцій програми за допомогою мови «Python».

```
import bpy
import random
```

Додамо відстань що буде дозволяти генерування кубів без появи їх всередині один одного та переберемо кожне місце сітки, де міг бути створений куб.

```
spacing = 2.2
for x in range(7):
        for y in range(7):
```

Також надамо обчислення розташування поточного місця створення з генеруванням випадкової висоти.

```
location = (x * spacing, y * spacing, random.random() * 2)
```

Оголосимо куб та визначимо правило використання ним кольорів в залежності від згенерованого значення висоти(попередньо створених матеріалів жовтого та фіолетового кольорів).

```
bpy.ops.mesh.primitive_cube_add(
        size = 2,
        enter_editmode = False,
        align = ‘WORLD’,
        location = location,
        scale = (0.5, 0.5, 0.5))

item = bpy.context.object
if random.random() < 0.2:        item.data.materials.append(bpy.data.materials[‘Material.Purple’])
else: item.data.materials.append(bpy.data.materials[‘Material.Yellow’])
```

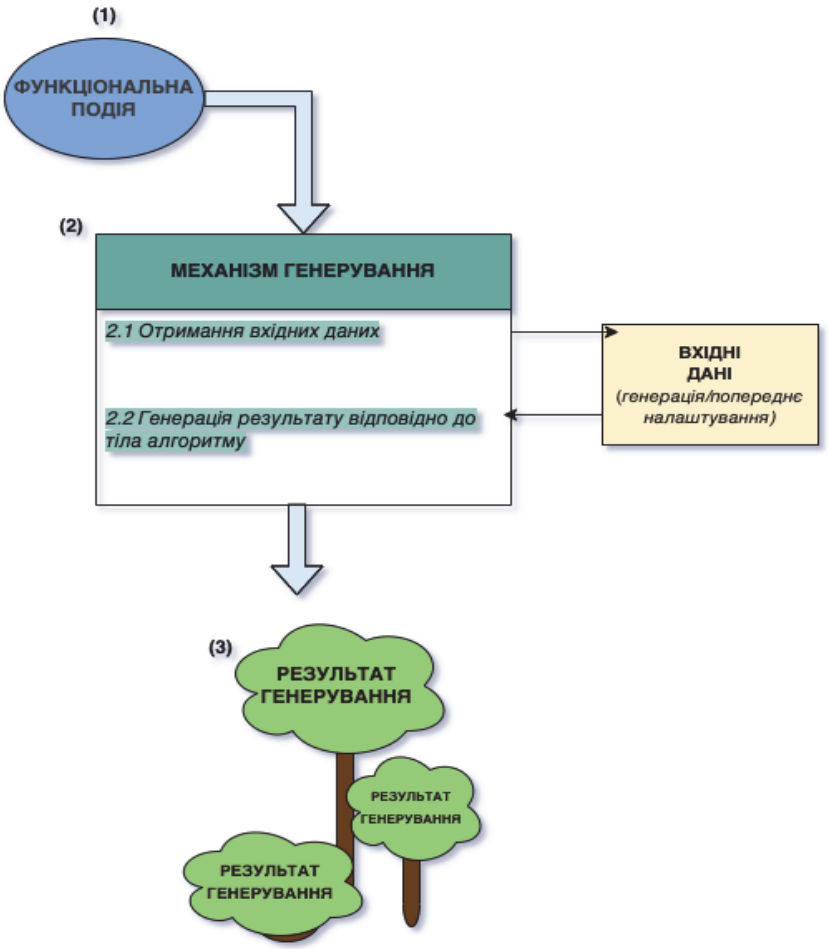
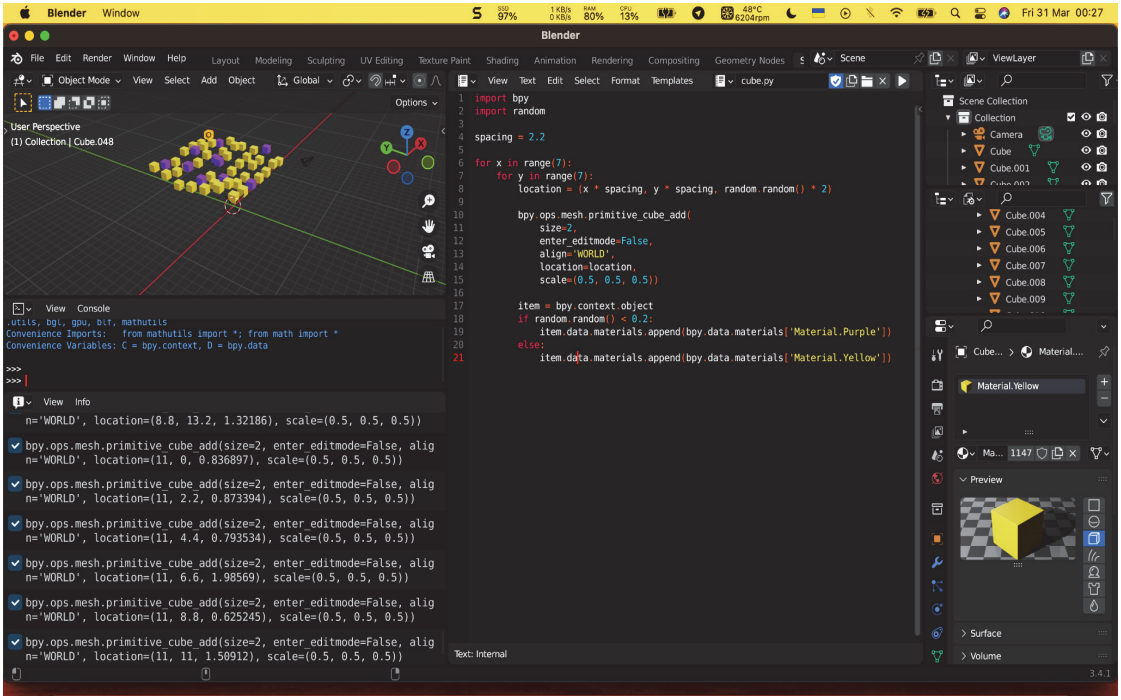


Рис. 1. Схема відпрацювання процедурної генерації




```
import bpy
import random

spacing = 2.2

for x in range(7):
    for y in range(7):
        location = (x * spacing, y * spacing, random.random() * 2)

        bpy.ops.mesh.primitive_cube_add(
            size=2,
            enter_editmode=False,
            align='WORLD',
            location=location,
            scale=(0.5, 0.5, 0.5))

        item = bpy.context.object
        if random.random() < 0.2:
            item.data.materials.append(bpy.data.materials['Material.Purple'])
        else:
            item.data.materials.append(bpy.data.materials['Material.Yellow'])
```

Рис. 2. Результат відпрацювання процедурної генерації

Джерело: розроблено автором в середовищі Blender(скрін з екрану)

Дана операція дозволила згенерувати абстракцію поля кубів з певними унікальними характеристиками та параметрами, які були, в деякій мірі, попередньо визначеними. В більш змістовній, не абстрактній генеративній моделі що організована алгоритмом, повністю випадкова вибірка вхідних даних може спричинити руйнацію початкової задумки та відхилення від цілей спеціаліста який її використовує.

Отже, повна унікальність такого графічного шаблону остаточно досягається за допомогою сторонніх маніпуляцій над новоствореними об'єктами. Використання даного методу підходить для масивних даних, одноманітних скупчень об'єктів, які можуть формувати на загальному тлі навколишнього середовища. Процедурна генерація вдало застосовується для створення оточення ігрових світів, що все ж таки мають обмеження та визначені правила автоматичного генерування як по обсягу (в ролі оптимізаційних рішень відносно зменшення загального навантаження на систему, яка запускає програму в якій об'єкти моделюються), так і в законах формування самого ігрового рівня(для збереження змісту генеративної моделі).

Отримання відмінностей можливе в процесі генерування об'єктів методом параметричного моделювання. Параметричне моделювання являє собою процес з можливістю зміни форми геометрії моделі, щойно змінено значення розміру. Параметричне моделювання реалізується за допомогою коду комп'ютерного програмування, такого як сценарій для визначення розмірів і форми моделі. Такі моделі також візуалізуються в програмах для 3D-креслень, щоб нагадувати атрибути реальної поведінки оригінального проекту. Досить часто параметрична генеративна модель використовує інструменти моделювання на основі функцій для маніпулювання її атрибутами. Параметричне моделювання є альтернативою для створення точної моделі за допомогою редагування параметрів, що могло б полегшити процеси 3D-дизайнерів, наприклад, створення циліндру, застосувавши мінімальне редагування декількох параметрів (верхній діаметр, нижній діаметр і висоту), замість того, щоб вручну додавати примітиви з нуля або перетягувати їх із основної форми.

В розмаїтті інших корисних модифікатор, Blender впроваджує «Array», що дозволяє створювати масив копій базового об'єкта, де кожна копія зсувається відносно попередньої будь-яким із кількох можливих способів. Вершини в суміжних копіях можуть бути об'єднані, якщо вони знаходяться поруч, що дозволяє генерувати гладкий subdivision surface. Базові опції модифікатора дозволяють створити достатню кількість копій для розміщення в межах довжини об'єкта кривої, зазначеного в параметрі Curve, створити достатню кількість копій для розміщення в межах фіксованої довжини, заданої параметром Length та згенерувати визначену кількість копій, вказану в параметрі Count [3].

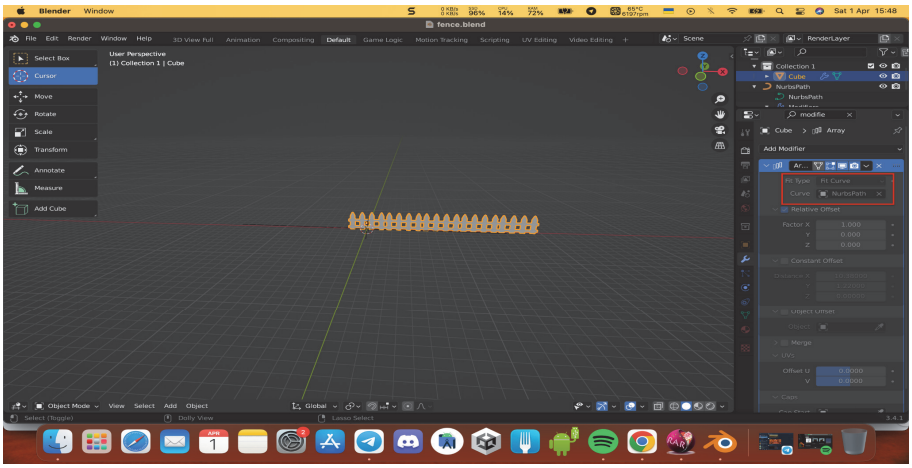


Рис. 3. Результат застосування опції «Fit Curve» в параметрі Fit Type

Джерело: розроблено автором в середовищі Blender(скрін з екрану)

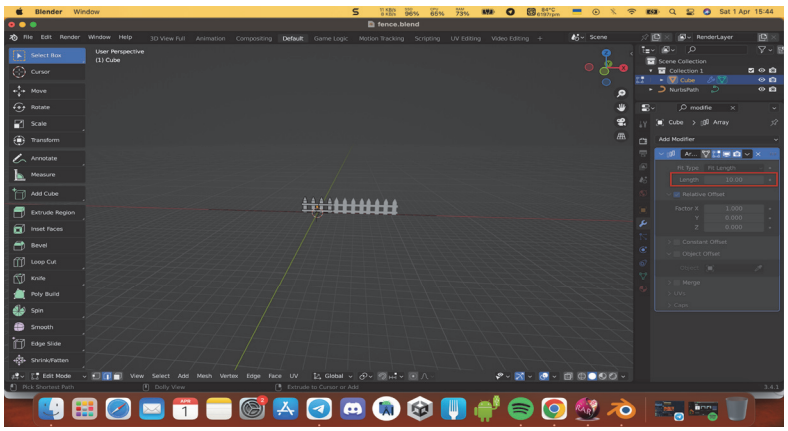


Рис. 4. Результат застосування опції «Fit Length» в параметрі Fit Type

Джерело: розроблено автором в середовищі Blender(скрін з екрану)

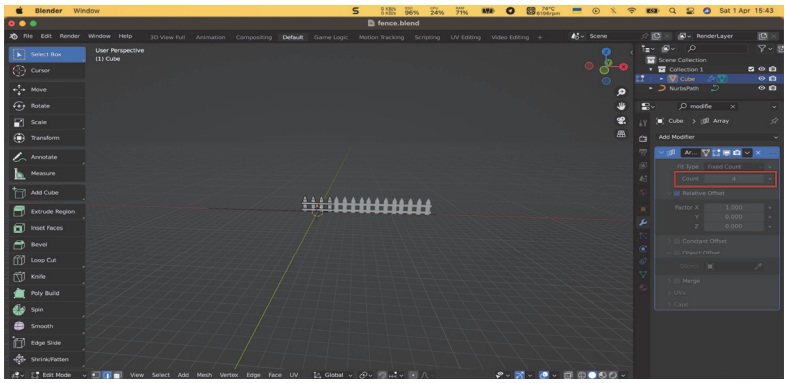


Рис. 5. Результат застосування опції «Fixed Count» в параметрі «Fit Type»

Джерело: розроблено автором в середовищі Blender(скрін з екрану)

Цей модифікатор може бути корисним у поєднанні з плитковими сітками для швидкого створення великих сцен, зручний для створення складних повторюваних форм. За допомогою поєднання базових опцій та реалізованих у модифікаторі параметрів зміщення(відносного, постійного та орієнтованого на інший об'єкт), така генеративна модель може слугувати альтернативою процедурному моделюванню і є більш дружньою для використання, оскільки не залучає спеціаліста до роботи з алгоритмом та відтворенням окремих правил генерації у коді. Перевагою цього методу також є ефективне використання пам'яті, оскільки цей модифікатор зберігає кількість об'єктів у пам'яті як один елемент, що зменшує обсяг виділення самої пам'яті, який використовується для збереження об'єктів.

Інший глобальний підхід, що задовольняє низку потреб відмінності та, в більшій мірі, реалістичності згенерованих моделей є генерація об'єктів за допомогою навчання глибоких нейронних мереж(GANs). GAN – це структура для генерації об'єктів за допомогою змагальної оцінки процесу, яка має глибокий вплив на розробку методів генерації в глобальному розумінні.

GAN реалізується шляхом поєднання генератора G і дискримінатор D. D класифікує, чи його вхідні дані створені чи взяті з «реальних» даних. G. фіксує розподіл даних і намагається фальсифікувати «реальні» дані, щоб змусити дискримінатора зробити неправильне судження. G і D можна розглядати як двох гравців у міні-максимальній грі, які тренуються одночасно, мета формулюється наступним чином:

$$(minG)(maxD)V(D,G) = E_{p_r}[log\ log\ D(x)] + E_{p_z}\left[log\ log\ \left(1 - D(G(z))\right)\right] \quad (1)$$

де p_r є розподілом даних навчального набору, і z є випадковим вектором із попереднього розподілу шуму p_z , $D(x)$ є вихідним скаляром D що вказує на можливість що x взятий з навчального набору. І G навчений будувати карту z між простором даних $G(z)$, знижує ймовірність того, що D відрізняє $G(z)$ прийшовшого з p_g а не p_r . Навчання стандартних GAN вимагає лише анотаційної інформації (правдивої чи хибної) джерела даних і оптимізовано відповідно до вихідних даних дискримінатора. Умовний GAN відноситься до додавання умов c в реальних даних, G і D . Функція c , яка може бути інформацією про клас або іншою додатковою інформацією, використовується для контролю навчання мережі. А функцію втрат можна визначити як:

$$L_D^{CGAN} = E_{p_r}[log\ log\ D(x|c) + E_{p_z}\left[log\ log\left(1 - D\left(G(c)\right)\right)\right] \quad (2)$$

Щоб вирішити проблему зникнення градієнта, яка може виникнути під час навчання, і уникнути нестабільності процесу навчання, WGAN-GP використовується для навчання всієї моделі. Наша цільова функція полягає в наступному:

$$: L_D = -E_{p_r}[D(c)] + E_{p_z}[D(G(z|c)] + \alpha E_{p_{\hat{x}}}[(\|\|\nabla_{\hat{x}} D(\hat{x})\|\|_2 - 1)^2] \quad (3)$$

де $p_{\hat{x}}$ позначає розподіл, який рівномірно відбирається на прямій лінії між p_r і p_g . Тут p_z визначається рівномірним розподілом по [0, 1], а втрата дискримінатора додається градієнтним штрафом з α = 10 як запропоновано в WGAN-GP.

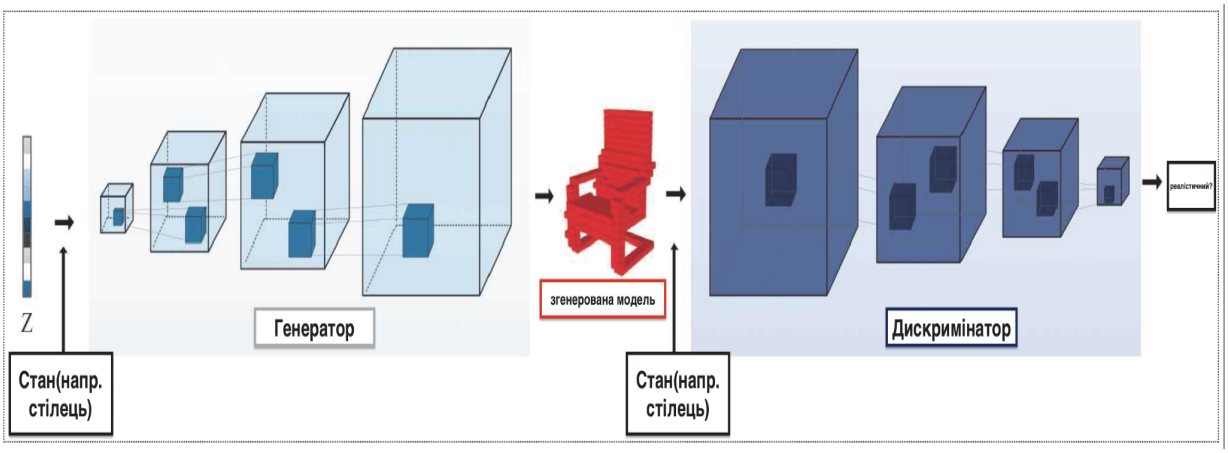


Рис. 6. Архітектура мережі генерації тривимірної моделі

Джерело: [4]

Генератор навчений відображати низьковимірний ймовірнисний простір у 3D-моделях, щоб досліджувати тривимірне розмаїття. Моделі генеруються на основі заданих умов без довідкових зображень і моделей CAD. Дискримінатор відрізняє згенеровані 3D-моделі від «реальних» даних і повертає результат генератору для керування його навчанням [5].

У Blender можна використовувати GANs для генерації 3D-об'єктів за допомогою бібліотеки PyTorch3D. Один з прикладів застосування реалізований в навчальних матеріалах сервісу(за застосування Google Colab), що дозволяє деформувати вихідну сітку, щоб сформувати цільову сітку за допомогою функцій втрат.

Починаючи з мешу сфери, ми вивчаємо зсув до кожної вершини сітки таким чином, щоб прогнозована сітка була ближчою до цільової сітки на кожному кроці оптимізації. Щоб

досягти цього, ми мінімізуємо: відстань між прогнозованою (деформованою) і цільовою сіткою(chamfer_distance). Однак лише ця мінімізація між прогнозованою та цільовою сіткою призведе до негладкої форми, в залежності від параметрів що будуть вказані(від 1.0 до 0.0). Ми забезпечуємо плавність, додаючи регуляризатори форми до цілі. А саме додаємо: mesh_edge_length, який мінімізує довжину країв у прогнозованій сітці; mesh_normal_ consistency, який забезпечує узгодженість між нормалями сусідніх граней; mesh_laplacian_smoothing, який є регуляризатором. Після встановлення та імпортування в середовище Blender необхідних модулів torch, torchvision та pytorch3d. Завантажуємо файл розширення obj(примітив дельфіна) і створюємо сітку об'єкту та читаємо її(за допомогою load_obj). Далі ми нормалізуємо масштаб і центруємо цільову сітку, щоб вона помістилася в сфері радіуса 1 з центром (0,0,0). Також масштабування по центру буде використано, щоб привести прогнозовану сітку до початкового центру та масштабу. Потрібно зауважити, що нормалізація цільової сітки прискорює оптимізацію, але не є обов'язковою саме в цьому процесі, тож ми лише створюємо структуру сітки для цільової сітки та ініціалізуємо вихідну форму як сферу радіуса 1. При візуалізації вихідної та цільової сітки необхідно відбирати зразки рівномірно з поверхні сітки, яку ми використовуємо. Наступним етапом є цикл оптимізації в якому ми деформуємо вихідну сітку, зміщуючи його вершини. В ньому форма параметрів деформації дорівнює загальній кількості вершин у src_mesh. В оптимізаторі, ми будемо мати параметри кількості кроків оптимізації, вагу для chamfer loss, mesh edge loss, mesh normal consistency та mesh laplacian smoothing, сума якої пізніше надасть нам графічне розуміння загальних втрат. Вкажемо період побудови для загальних втрат та ініціалізуємо оптимізатор, після чого приступаємо до деформування сітки, де нам необхідно вибрати 5 тисяч точок із поверхні кожної сітки та порівняти два набори точок, обчислюючи chamfer loss. Друкуємо та зберігаємо витрати, проводимо побудову сітки та запускаємо раніше організований оптимізаційний процес. Відобразимо наші втрати.

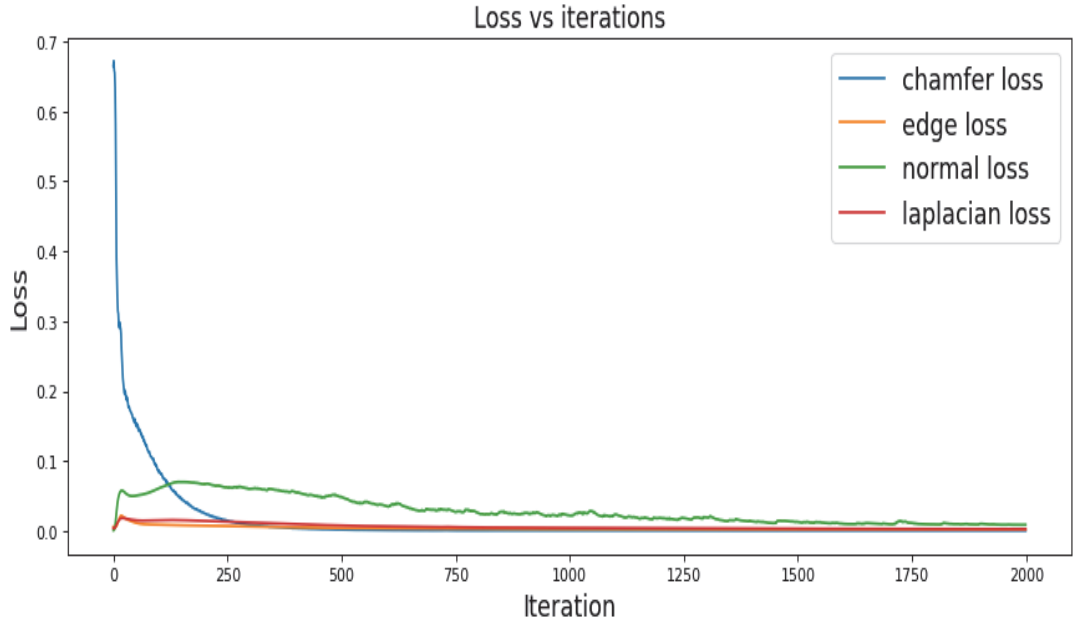


Рис. 7. Загальні ітераційні втрати

Джерело: скрін з екрану

Збережемо нашу створену сітку, де виберемо вершини і грані остаточної прогнозованої сітки, нормалізуємо масштаб до вихідного цільового розміру та кінцево фіксуємо спрогнозований меш(знову за допомогою save_obj) [6]. Отримаємо наступний результат в якому видно мінімальну розбіжність відносно заданого оригіналу.

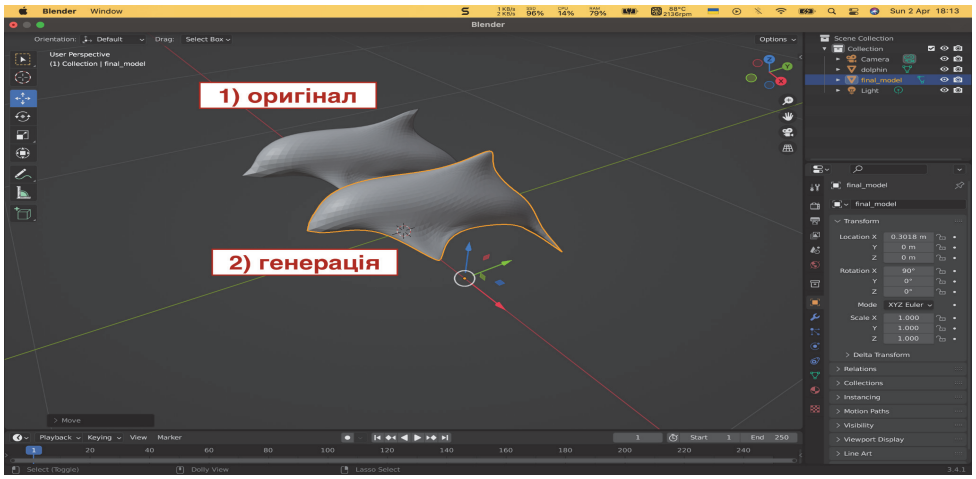


Рис. 8. Вхідний та вихідний результати

Джерело: розроблено автором в середовищі Blender(скрін з екрану)

Якщо поекспериментувати із вказанням значень втрат, та мінімізувати їх(w_edge = 0.0, w_normal = 0.00, w_laplacian = 0.0) згенерований об'єкт буде менш відповідним до більш реалістичного оригіналу, та матиме явні пошкодження генерації, що не зовсім задовольняє початкову ціль.

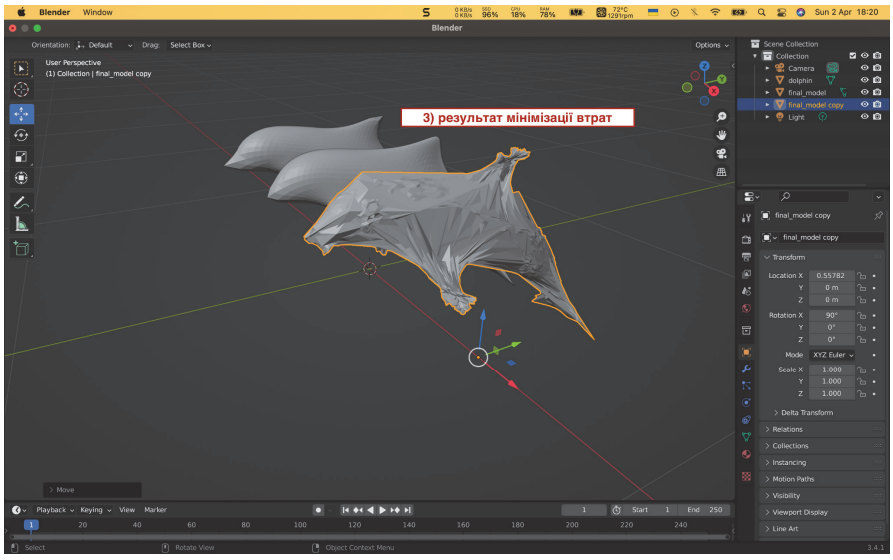


Рис. 9. Результат генерації з мінімізацією втрат

Джерело: розроблено автором в середовищі Blender(скрін з екрану)

Отже, за допомогою навчальних матеріалів PyTorch можемо завантажувати сітку з файлу розширення obj, ініціалізувати структуру даних під назвою «Сітки», налаштувати цикл оптимізації та використовувати чотири різні функції втрати сітки для корекції генерування об'єкту з наявною можливістю інтегрування бібліотеки в робочий процес програми Blender.

Деформування вихідної сітки для створення цільової сітки за допомогою функцій втрат в є важливим кроком у генерації нових 3D-об'єктів. Цей процес дозволяє створити моделі з більш складною формою та більш точною геометрією. PyTorch3D надає функції втрат, які дозволяють точно порівняти дві сітки та визначити, наскільки вони відрізняються. Це важливо при генерації нових сіток, оскільки нейронна мережа повинна навчатися генерувати нові об'єкти, які якомога більше схожі на зразок. Використання функцій втрат дозволяє зменшити відстань між зразком та сгенерованою моделлю, що покращує якість генерації. Отже, використання даної бібліотеки в Blender для деформування вихідної сітки за

допомогою функцій втрат допомагає в створенні та використанні генеративних моделей, оскільки дозволяє точніше генерувати нові 3D-об’єкти з більш складною формою та більш точною геометрією, що може вирішити низку специфічних задач в яких загальні рішення процедурної та параметричної генерації не підходять.

Висновки. Процедурна генерація дозволяє швидко створювати багато різних варіантів об’єктів, проте, деталізація та відтворення складних форм може бути обмеженою. Параметричне генерування дає більшу свободу у створенні складних форм та деталізації об’єктів. Однак, процес налаштування параметрів може бути трудомістким. 3D GANs є найбільш складною генеративною моделлю для використання, але вона може створювати найбільш подібні до натренованих об’єкти, допомагаючи у вирішенні проблем, де є вкрай важливо отримати максимальну реалістичність та деталізацію. Такі моделі здебільшого доцільно використовувати у візуалізації архітектурних проектів, інтерактивних додатків, на виробництві та промисловості, технологіях доповненої чи віртуальної реальності. Дана генеративна модель може бути дорогим процесом, що потребує великої кількості ресурсів, обчислювальної потужності та є менш гнучкою у порівнянні з іншими методами генерації. У загальному, використання різних видів генеративних моделей в Blender вимагає певної кількості досвіду, технічної компетентності та має свої переваги, а їх недоліки реально мінімізувати правильно визначивши цілі та задачі проєкту, де вони беруться у використання.

Список використаних джерел

1. Jiajun Wu, Chengkai Zhang, Tianfan Xue, William T. Freeman, Joshua B. Tenenbaum. (2017). Learning a Probabilistic Latent Space of Object Shapes via 3D Generative-Adversarial Modeling \\ Режим доступу: https://arxiv.org/pdf/1610.07584.pdf (останнє звернення 05.04.2023)
2. Tianyu Zhou, Weidan Xiong, Yuki Obata, Carlos Lange, Yongsheng Ma. (2022). Digital Manufacturing: Chapter 2. Digital product design and engineering analysis techniques \\ Режим доступу: http://surl.li/gqykf (останнє звернення 05.04.2023)
3. Матеріали некомерційної організації Blender Foundation. (2023). Offical Blender Documentation. Generative Modeling: Array Modifier \\ Режим доступу: http://surl.li/gqyko (останнє звернення 05.04.2023)
4. Haisheng Li1, Yanping Zheng, Xiaoqun Wu, Qiang Cai1. (2019). 3D Model Generation and Reconstruction Using Conditional Generative Adversarial Network: «Figure 1» \\ Режим доступу: http://surl.li/gqykx (останнє звернення 05.04.2023)
5. Haisheng Li1, Yanping Zheng, Xiaoqun Wu, Qiang Cai1. (2019). 3D Model Generation and Reconstruction Using Conditional Generative Adversarial Network \\ Режим доступу: https://www.atlantis-press.com/journals/ijcis/125911591/view#bibr-R9 (останнє звернення 05.04.2023)
6. Матеріали компанії Meta Platform Inc. (2023). Deform a source mesh to form a target mesh using 3D loss functions \\ Режим доступу: https://pytorch3d.org/tutorials/deform_ source_mesh_to_target_mesh (останнє звернення 05.04.2023)
7. Lyle Regenwetter, Amin Heyrani Nobari, Faez Ahmed. (2022). Deep Generative Models in Engineering Design: A Review \\ Режим доступу: https://decode. mit.edu/ assets/papers/2022_regenwetter_review.pdf (останнє звернення 05.04.2023)

Робота виконана під науковим керівництвом доцента ДЕСЯТКО А. М.

Наукове електронне видання

ПРОГРАМУВАННЯ ТА ЗАХИСТ ІНФОРМАЦІЇ

**Збірник наукових статей студентів,
які здобувають освітній ступінь «магістр»
за спеціальностями
«Інженерія програмного забезпечення»,
«Кібербезпека та захист інформації»**

Частина 2

Видавець і виготовлювач
Державний торговельно-економічний університет
вул. Кіото, 19, м. Київ-156, Україна, 02156
Тел. (044) 513 74 18
Електронна пошта knute@knute.edu.ua
280-2Е-2023