937

76-12/121

**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ**
**СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ**
**Система забезпечення якості освітньої діяльності та якості вищої освіти**
*сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015*
**Кафедра інженерії програмного забезпечення та кібербезпеки**

**ЗАТВЕРДЖЕНО**
вченою радою КНТЕУ
(прот. п. 5 від «20» 01 2022 р.)
Ректор
_____ А. А. Мазаракі

# БЕЗПЕКА МЕРЕЖЕВОЇ ТА SMART ІНФРАСТРУКТУРИ /
# NETWORK AND SMART INFRASTRUCTURE SECURITY

## ПРОГРАМА /
## COURSE SUMMARY

**Київ 2022**

Автори: М.В. САШНЬОВА, кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Ю.В. КОСТЮК, асистент кафедри інженерії програмного забезпечення та кібербезпеки
А.М. ДЕСЯТКО, PhD, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Л.О. ВЛАСЕНКО, кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Т.В. САВЧЕНКО, кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Ю.В. САМОЙЛЕНКО, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «01» листопада 2021 р., протокол №10.

Рецензенти: Н.О. КОТЕНКО, кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Б.Т. БЕБЕШКО, Senior Software Engineer Softorino Inc.

# БЕЗПЕКА МЕРЕЖЕВОЇ ТА SMART ІНФРАСТРУКТУРИ /
# NETWORK AND SMART INFRASTRUCTURE SECURITY

## ПРОГРАМА /
## COURSE SUMMARY

# ВСТУП

Програма дисципліни «Безпека мережевої та SMART інфраструктури» призначена для студентів освітнього ступеня «магістр» галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека», спеціалізації «Безпека систем електронних комунікацій в економіці».

Програму підготовлено відповідно до Стандарту вищої освіти України за даною спеціальністю та відповідної освітньо-професійної програми підготовки магістрів КНТЕУ.

Програма складається з таких розділів:

1. Мета, завдання та предмет дисципліни.
2. Передумови вивчення дисципліни як вибіркової компоненти освітньої програми
3. Результати вивчення дисципліни.
4. Зміст дисципліни.
5. Список рекомендованих джерел.

## 1. МЕТА, ЗАВДАННЯ ТА ПРЕДМЕТ ДИСЦИПЛІНИ

*Метою* викладання дисципліни «Безпека мережевої та SMART інфраструктури» є формування у майбутніх спеціалістів умінь та компетенцій для забезпечення безпеки мережевої та SMART інфраструктури, підготовка до самостійного вирішення задач в процесі практичної діяльності.

*Завданням* вивчення дисципліни «Безпека мережевої та SMART інфраструктури» є освоєння принципів побудови безпеки комп'ютерних мереж для їх використання в сучасних інформаційних системах; дослідження різних механізмів захисту мереж даних, від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів; засвоєння основ розробки та програмування пристроїв, які працюють з використанням смарт-технологій та технологій Інтернету речей; отримання теоретичних знань та практичних вмінь в сфері впровадження, безпечної експлуатації та супроводження SMART інфраструктури.

*Предметом* вивчення дисципліни є основні поняття та методи для захисту від внутрішнього та зовнішнього втручання на різних рівнях у вузлах та комп'ютерних мережах; програмні засоби, які реалізують функції безпеки комп'ютерних мереж та SMART інфраструктури; засвоєння методики основ роботи з пристроями, датчиками та засобами комунікації Інтернету речей.

## 2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

*Знання з дисциплін:*

- Основи кібербезпеки;
- Безпека операційних систем;
- Безпека інформаційних систем та мереж;
- Організація комп'ютерних мереж.

*Вміння:*

- працювати з пошуковою системою Google;
- працювати з програмним додатком Cisco Packet Tracer v 8.0 або вище;
- працювати з Oracle VirtualBox.

## 3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Безпека мережевої та SMART інфраструктури», як обов'язкова компонента освітньої програми, забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідною освітньо-професійною програмою:

✓ ***«Безпека систем електронних комунікацій в економіці»***
*(ОС магістр, ОП 2022 р.)*

| Номер в освітній програмі | Зміст компетентності | Номер теми, що розкриває зміст компетентності |
|---|---|---|
| *Загальні компетентності за освітньою програмою* | | |
| КЗ-1 | Здатність застосовувати знання у практичних ситуаціях. | 1-19 |
| КЗ-3 | Здатність до абстрактного мислення, аналізу та синтезу. | 1-19 |
| КЗ-4 | Здатність оцінювати та забезпечувати якість виконуваних робіт. | 1-19 |

| *Фахові компетентності за освітньою програмою* | | |
|---|---|---|
| КФ1 | Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. | 3-9, 12, 16-19 |
| КФ2 | Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. | 1-2, 10-11, 13-14 |
| КФ3 | Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. | 10-19 |
| КФ4 | Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. | 2, 15 |
| КФ5 | Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес / операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. | 13, 15, 19 |
| КФ8 | Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної без- | 10-19 |

| | | |
|---|---|---|
| | пеки та/або кібербезпеки організації. | |
| КФ9 | Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. | 3-5, 11 |
| *Програмні результати навчання за освітньою програмою* | | |
| РН2 | Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. | 1-19 |
| РН4 | Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. | 3-9, 12, 16-19 |
| РН5 | Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. | 3-9, 12, 16-19 |
| РН6 | Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. | 3-9, 12, 16-19 |
| РН7 | Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. | 2, 15 |
| РН8 | Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. | 10-19 |
| РН10 | Забезпечувати безперервність бізнес / операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. | 13, 15, 19 |

| | | |
|---|---|---|
| РН13 | Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес / операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. | 10-19 |
| РН14 | Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес \ операційних процесів у сфері інформаційної та \ або кібербезпеки в цілому. | 3-5, 11 |
| РН16 | Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. | 1-19 |
| РН17 | Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. | 1-19 |
| РН20 | Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. | 1-19 |
| РН21 | Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. | 1-19 |
| РН23 | Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. | 3-9, 12, 16-19 |

## 4. ЗМІСТ ДИСЦИПЛІНИ

## РОЗДІЛ 1. БЕЗПЕКА МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

### Тема 1. Необхідність безпеки мереж

Причини захисту мереж. Вектори мережевих атак. Найпоширеніші вектори втрати даних: електронна пошта/соціальні мережі; нешифровані пристрої; пристрої хмарного зберігання; знімні носії, паролі, тощо.

Огляд топології мережі: VPN, брандмауер ASA (Cisco Adaptive Security Appliance), пристрій системи запобігання вторгненням Cisco (IPS), комутатори рівня розподілу, комутатори рівня доступу, засоби захисту електронної пошти Cisco (ESA) та Web Security Appliance (WSA), сервер автентифікації, авторизації та бухгалтерського обліку (AAA). Офісні та домашні мережі. Широкомасштабні мережі (WAN). Мережі ЦОД (центрів обробки даних). Хмарні мережі та віртуалізація.

Загрози мережі. Категорії атак на мережі. Шкідливе програмне забезпечення, що уповільнює або зупиняє мережеву активність. Поширені мережеві атаки: розвідка, доступ та соціальна інженерія. Мережеві атаки: відмова в обслуговуванні, переповнення буфера та ухилення.

**Список рекомендованих джерел**

*Основний*: *1, 2*
*Додатковий*: *7, 8, 10*
*Інтернет-джерела*: *25, 26*

### Тема 2. Політичні аспекти безпеки мережі

Домени безпеки мережі, визначені Міжнародною організацією зі стандартизації (ISO)/Міжнародною електротехнічною комісією (IEC). Міжнародний консорціум сертифікації безпеки інформаційних систем ($ISC^2$). Центр безпеки в Інтернеті (СНД). Global Information Assurance Certification (GIAC). Асоціація аудиту та контролю інформаційних систем (ISACA). Бізнес-політика мережі: рекомендації, розроблені організацією для керування своїми діями. Інструменти тестування безпеки. Платформи безпеки даних (DSP). Алгоритми захисту мережі.

**Список рекомендованих джерел**

*Основний: 3*
*Додатковий*: *11*
*Інтернет-джерела*: *25, 26*

## Тема 3. Захист мережевої інфраструктури

Захист мережевої інфраструктури: маршрутизаторів, комутаторів, серверів, кінцевих точок та інших пристроїв. Три області безпеки маршрутизатора. Налаштування безпечного адміністративного доступу. Безпечний локальний та віддалений доступ. Налаштування SSH.

Моніторинг та управління пристроями. Блокування маршрутизатора за допомогою AutoSecure. Протоколи виявлення вразливостей CDP та LLDP. Аутентифікація протоколу маршрутизації. Безпека мережі за допомогою Syslog. Конфігурація та перевірка NTP (налаштування дати та часу на маршрутизаторі або комутаторі). Конфігурація SNMP.

Налаштування AAA (аутентифікація, авторизація та облік) для захисту мережі. Налаштування локальної автентифікації AAA. Характеристики та протоколи AAA на основі сервера. Налаштування авторизації та обліку на основі сервера.

### Список рекомендованих джерел

*Основний:1, 2*
*Додатковий*: *7, 8, 10*
*Інтернет-джерела*: *25, 26*

## Тема 4. Фільтрація трафіку та пом’якшення мережевих атак на мережу

Списки контролю доступу (ACL) для фільтрації трафіку та пом’якшення мережевих атак на мережу. Що таке ACL? Фільтрація пакетів. Огляд маски підстановки. Налаштування ACL. Огляд ACL IPv4. Протоколи та номери портів. Зменшення атак за допомогою ACL. Огляд ACL IPv6.

Безпечні мережі за допомогою брандмауерів. Брандмауер політики на основі зон (ZPF). Налаштування ZPF.

### Список рекомендованих джерел

*Основний*: *1, 2*
*Додатковий*: *7, 8, 10, 12*
*Інтернет-джерела*: *25, 26*

## Тема 5. Мережеві системи запобігання вторгненням для захисту мережі.

Характеристики IDS та IPS як . Доступні види IPS: хост-IPS (HIPS) та мережевий IPS. Методи моніторингу мережі: IDS, аналізатори пакетів, SNMP, NetFlow та інші інструменти. Відстеження мережевого трафіку Snort. Використання технології SPAN.

Атрибути підпису IPS. Налаштування Snort IPS.

### Список рекомендованих джерел

*Основний: 1, 2*
*Додатковий*: *7, 10*
*Інтернет-джерела*: *25, 26*

## Тема 6. Безпека кінцевих точок

Безпека кінцевих точок у мережі. Захист хостів на рівні мережі: оозширений захист від зловмисного програмного забезпечення (AMP), пристрій захисту електронної пошти (ESA), Web Security Appliance (WSA), контроль доступу до мережі (NAC). Апаратне та програмне шифрування локальних даних. Безпека за допомогою автентифікації на основі порту 802.1X.

### Список рекомендованих джерел

*Основний: 1, 2*
*Додатковий: 7, 10*
*Інтернет-джерела*: *25, 26*

## Тема 7. Загрози безпеки 2-го рівня моделі OSI

Атаки таблиці MAC. Заходи щодо зменшення атак на таблиці MAC. Захист невикористаних портів. Скористайтеся. Режими порушення безпеки порту комутатора. Реалізація безпеки портів. Зменшення атак VLAN. Приватні VLAN (PVLAN). Атаки DHCP. Етапи реалізації DHCP Snooping. Зменшення атак ARP. Атаки підробки ARP. Вказівки щодо впровадження DAI ( для зменшення ймовірності підробки ARP та отруєння ARP). Атаки підробки MAC–адреси. Захист від підробки MAC та IP-адреси. Протокол Spanning Tree Protocol (STP). STP атака. Механізми стабільності STP для підвищення загальної продуктивності комутаторів та скорочення часу, що втрачається під час зміни топології.

**Список рекомендованих джерел**

*Основний: 1, 2*
*Додатковий*: *7, 8, 10, 12*
*Інтернет-джерела*: *25, 26*

## Тема 8. Віртуальні приватні мережі (VPN) для створення наскрізних приватних мережевих з'єднань

Основні переваги VPN. VPN для захисту мережевого протоколу (IPsec) та VPN із захищеним сокетом (SSL) для захисту мережевого трафіку між сайтами. Топології VPN. VPN типу «сайт-сайт» і VPN з віддаленим доступом. VPN віддаленого доступу. Технології IPsec, і SSL VPN. VPN-сервіси IPsec типу Site-to-Site. Огляд IPsec: призначення, протоколи. Два основних протоколи IPsec: заголовок аутентифікації (AH) і протокол безпеки інкапсуляції (ESP). Шифрування та аутентифікація ESP. Протокол IKE – стандарт протоколу керування ключами, який використовується для автоматичного узгодження асоціацій безпеки IPsec та забезпечення безпечного зв’язку IPsec.

Впровадження VPN-мережі IPsec між сайтами за допомогою CLI. Топологія IPsec VPN між сайтами. IPsec VPN.

**Список рекомендованих джерел**

*Основний: 1, 2*
*Додатковий*: *7, 8, 10, 12*
*Інтернет-джерела*: *25, 26*

## Тема 9. Тестування безпеки мережі

Методи тестування безпеки мережі. Тестування та оцінка безпеки мережі (ST&E). Види мережевого тестування: тестування на проникнення, сканування мережі, сканування вразливостей, злом пароля, огляд журналу, перевірка цілісності, виявлення вірусів. Застосування результатів тестування мережі. Інструменти тестування безпеки мережі: Nmap/Zenmap, SuperScan, SIEM (Управління подіями інформації про безпеку), GFI LANguard, Tripwire, Hecc, L0phtCrack,

**Список рекомендованих джерел**

*Основний*: *1*
*Додатковий*: *7, 9, 13*
*Інтернет-джерела*: *25, 26*

## РОЗДІЛ 2. БЕЗПЕКА МЕРЕЖЕВОЇ ТА SMART ІНФРАСТРУКТУРИ

### Тема 10. Введення в SMART безпеку

SMART інфраструктура: головні характеристики та функції. Термін SMART інфраструктур. Цифрові технології, які застосовуються під час розбудови SMART інфраструктури (хмарні обчислення та IoT, інформаційне моделювання, геоінформаційні системи, ШІ та додаткові технології, як-то оптоволоконні системи, бездротові сенсорні мережі або мікроелектро-механічні системи, що полегшують у режимі реального часу збір та обробку даних. Цінність SMART інфраструктури. SWOT-аналіз розбудови SMART інфраструктури. Загрози SMART інфраструктури. Кібербезпека як ключовий елемент концепції «Розумного міста».

#### Список рекомендованих джерел

*Основний*: *4, 5*
*Додатковий*: *14, 15, 20, 23*
*Інтернет-джерела*: *27*

### Тема 11. Безпека SMART інфраструктури

Безпека як критичний чинник для будь-якої економіки цивілізованого світу. Цифрові технології в інфраструктурі міста: вплив на довкілля. «Розумне» використання водних ресурсів. «Розумне» управління відходами. «Розумне» енергоспоживання. «Розумна» мобільність. Процеси цифровізації у сфері туризму та дозвілля (соціальні медіа та GPS-трекери). Кібербезпека та нові виклики в енергетиці. Застосування технології блокчейн в енергетиці. Проблеми безпеки та конфіденційності розумного вимірювання. «Розумна» мережа, порівняно з традиційними електричними мережами. «Розумне» медичне обслуговування: Використання технології IoT, а також різних комп’ютерних технологій для отримання точних діагнозів та покращення надання медичних послуг в системі охорони здоров’я (вимірювання показників, підтримка лікаря через ШІ, робототехніка в лікуванні та догляді). «Розумна» освіта. «Розумний» дім: управління електронними пристроями, моніторинг та безпека будинку, контроль ландшафтної системи, тощо.

#### Список рекомендованих джерел

*Основний*: *4, 5*
*Додатковий*: *14, 15, 19, 20, 21, 22*
*Інтернет-джерела*: *28, 29,30, 31, 32, 33, 34, 35, 36*

## Тема 12. Апаратні засоби та технології SMART інфраструктури

Датчики і пристрої збору даних: Термопари та температурні датчики, Резистивні датчики температури, Термістори, Фотоелектричні датчики, LiDAR і активні датчики, Датчики MEMS, Датчики тиску та мікрофони MEMS, «Інтелектуальні» точки IoT, Пристрої введення - виведення. Поєднання, «злиття» датчиків. Технологія LTE. Загальні поняття, архітектура базової мережі, Категорії LTE для IoT, Інші безпроводові технології для IoT.

Сценарії застосування технології LTE для «Розумного міста». Перспективи розвитку мереж мобільного зв'язку в напрямку 4G/5G. Особливості міжмашинної взаємодії в мережах LTE. Географічні області 4G LTE, потоки даних і процедури передачі обслуговування для сфери «розумного транспорту» та логістики. Сценарії та можливості застосування eMTC (LTE-M, LTE Cat.M1)

### Список рекомендованих джерел

*Основний*: *4, 5*
*Додатковий*: *14, 15, 16, 17*
*Інтернет-джерела*: *37, 38, 39*

## Тема 13. Ризики цифрової безпеки для соціально-економічної діяльності SMART інфраструктури

Перешкоди, притаманні етапам впровадження SMART рішень. Відсутність загальнодержавної політики розбудови SMART інфраструктури. Проблеми відкритості даних. Невідповідність інфраструктури: у більшості міст доступними є мобільні системи покриття, недостатньо ефективні для швидкої передачі даних. Низький рівень е-вмінь населення. Технічні неполадки в роботі пристроїв. Неналежний стан програмного забезпечення. Порушення конфіденційності: три найбільші загрози приватному життю – технології IoT, Big Data та хмарні обчислення.

Небезпека та вразливість систем «розумних» міст: відсутність безпеки та надійності IoT. Кіберзлочинність, кібертероризм і кібершпигунство. Розробка стратегії управління ризиками цифрової безпеки. Системи захисту SMART систем (технологій кібербезпеки).

### Список рекомендованих джерел

*Основний*: *4, 5*
*Додатковий*: *14, 15, 24*
*Інтернет-джерела*: *40, 41, 42, 43, 44*

## Тема 14. Стан і головні небезпеки цифровізації на шляху розбудови SMART інфраструктури в містах України

Інструменти управління та контролю розбудови SMART інфраструктури. Пріоритетність SMART інфраструктури в містах України. Головні небезпеки цифровізації та перешкоди до розбудови SMART інфраструктури в містах України.

SMART мережі для SMART міст. Типова схема «SMART мережі».

### Список рекомендованих джерел

*Основний*: *4, 5*
*Додатковий*: *14, 15*
*Інтернет-джерела*: *45*

## Тема 15. Необхідність безпеки Інтернету речей у SMART інфраструктурі

Використання IoT на прикладі: розумного дому, у сфері охорони здоров'я. Оцінка ризику безпеки Інтернету речей у промисловому секторі.

Моделі систем IoT. Безпека в еталонній моделі IoT. Стандартизована архітектура ETSI M2M. Модель Purdue Enterprise (PERA) для ієрархії управління. Промислова еталонна архітектура Інтернету (IIRA). Архітектурна еталонна модель (ARM) для Інтернету речей.

Модель безпеки IoT. Рівні безпеки IoT. Моделювання загроз IoT. Система NICE Cybersecurity Workforce Framework. Аналіз моделі загроз для системи Інтернету речей. Оцінка загроз IoT

### Список рекомендованих джерел

*Основний*: *4, 5*
*Додатковий*: *14, 15, 24*
*Інтернет-джерела*: *25, 26, 46*

## Тема 16. Безпека обладнання та заходи щодо зменшення загроз пристроям IoT

Огляд пристроїв Інтернету речей. Апаратні компоненти пристрою IoT. Компоненти вразливості апаратного забезпечення OWASP. Основні типи процесорів, що використовуються в IoT – ARM, MIPS та x86. Обчислення з обмеженим набором інструкцій (RISC) та Комплексне обчислення набору інструкцій (CISC). Поширені типи пам'яті, що використовуються для зберігання даних в пристроях IoT. Поширені операційні системи Інтернету речей.

Вразливості та атаки на рівні обладнання. Вразливості прошивки. Проблеми з оновленням прошивки. Базові моделі контролю доступу до мережі. Заходи щодо зменшення загроз пристроям IoT Структура авторизації OAuth 2.0. Управління ідентифікацією пристроїв IoT. Безпека даних і паролів пристроїв IoT. Криптографія з відкритим ключем. Інфраструктура відкритих ключів (PKI) та Центр сертифікації (CA).

**Список рекомендованих джерел**

*Основний*: *1*
*Додатковий*: 6, *18*
*Інтернет-джерела*: *25, 26, 46, 47*

## Тема 17. Атаки на комунікаційному рівні IoT

Комунікаційний рівень IoT. Функції комунікаційного рівня IoT. Вразливості комунікаційного рівня OWASP. Огляд бездротового протоколу (IEEE 802.15.4, Bluetooth Low Energy (BLE), IEEE 802.11, NFC, Стільниковий зв'язок – 3GPP, 4G, LTE та 5G). Вразливості комунікаційного рівня IoT. Вразливості IP. Вразливості TCP і UDP. Безпека комунікаційних протоколів IoT.

**Список рекомендованих джерел**

*Основний*: *1*
*Додатковий*: 6, *18*
*Інтернет-джерела*: *25, 26*

## Тема 18. Атаки рівня додатків IoT

Мобільні програми. Вразливості веб- та хмарних програм OWASP. Програми керування пристроями та даними. Настанови щодо безпечних веб -та хмарних програм. Вразливості веб-інтерфейсу. Моделювання загроз на рівні програми. Протоколи прикладного рівня IoT. Протоколи обміну повідомленнями Інтернету речей. Забезпечення захисту в протоколах обміну повідомленнями.

**Список рекомендованих джерел**

*Основний*: *1*
*Додатковий*: 6, *18*
*Інтернет-джерела*: *25, 26*

## Тема 19. Оцінка вразливості та тестування на проникнення систем IoT

Процес оцінки вразливості. Види оцінки вразливості. Типи та інструменти перевірки вразливості. Інструменти відображення портів. Інструменти для виявлення вразливості паролів. Інструменти для виявлення вразливостей веб-додатків. Служби оцінки вразливості.

Концепції та підходи оцінки ризиків. Оцінка ризику IoT. Загальна система оцінки вразливостей. Моделювання загроз для оцінки ризику в системі IoT.

Інновації в галузі безпеки Інтернету речей. Введення в блокчейн. IoT та блокчейн.

### Список рекомендованих джерел

*Основний*: *1*
*Додатковий*: 6, *18*
*Інтернет-джерела*: *25, 26*

## 5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

*Основний*

1. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В.Л. Бурячок, А.О. Аносов, В.В. Семко, В.Ю. Соколов, П.М. Складанний. – К.: КУБГ, 2019. – 218 с.

2. Mark Ciampa, Ph.D. CompTIA® Security+ Guide to Network Security Fundamentals, Fifth Edition. Cengage Learning Customer & Sales Support, 2015. – 724p. Book Only ISBN: 978-1-305-09394-2.

3. Mike, Chapple, Gibson, Darril, Stewart, James Michael. (ISC)² CISSP certified information systems security professional: official study guide. Published simultaneously in Canada, 2018. – 1107 Pages.

4. Smart Cities Cybersecurity and Privacy, 1st Edition. Elsevier, 2018. – 303 Pages. eBook ISBN: 9780128150337.

5. Катерина Маркевич. SMART інфраструктура у сталому розвитку міст: світовий досвід та перспективи України. Видавництво “Заповіт”, 2021. – 400 с.

*Додатковий*

6. Hanes D. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things. 1st ed. Cisco Press, 2017. 576 p.

7. Eric Maiwald. Network Security: A Beginner’s Guide, Second Edition. The McGraw-Hill Companies, 2003. – 497 p.

8. Harris Andrea. Cisco ASA Firewall Fundamentals, 3rd Edition, 2014 – 233 Pages.

9. Gordon "Fyodor" Lyon. Nmap Network Scanning Official Nmap Project Guide to Network Discovery and Security Scanning, 2013 – 465 Pages.

10. Eric D. Knapp, Joel Thomas Langil. Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems Second Edition. Book. – Syngress is an imprint of Elsevier 225 Wyman Street, Waltham, MA 02451, USA, 2015. – 438 p.

11. ISO/IEC 27002:2007(E). Information technology – Security techniques – Code of practice for information security management. 128 Pages.

12. Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., ОсиповаТ.Ю., Савицька Я.А. Комп’ютерні мережі[навчальний посібник] / А.І. Блозва, Ю.В. Матус, В.В. Смолій, Б.С. Гусєв, Д.Ю. Касаткін, Т.Ю. Осипова, Я.А. Савицька // - К.: Компрінт, 2017. – 821 с.

13. Gordon Fyodor Lyon. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, 2009. – 467 Pages.

14. Smart Living Handbook, 4th Edition. Published by the City of Cape Town, 2011. – 166 Pages.

15. OgieR., PerezP., Dignum V. Smart infrastructure: an emerging frontier for multidisciplinary research. – Smart Infrastructure and Construction, Vol.170, Issue SC1, March 2017

16. Проектування без проводових стільникових мереж зв'язку: навчальний посібник для виконання курсової роботи з дисципліни «Телекомунікаційні безпроводові системи» для студентів усіх форм навчання за напрямом підготовки 6.050903 «Телекомунікації» / НТУУ «КПІ»; уклад.: В.В. Пілінський, П.В. Попович, С.М. Веретюк. – Київ : НТУУ «КПІ», 2014. – 69 с. – Режим доступу: http://ela.kpi.ua/handle/123456789/211773.

17. Навчальний практикум з кредитного модуля «Безпроводові телекомунікаційні системи – 2. Системи та засоби зв'язку з рухомими об'єктами»: методичні рекомендації до проведення практичних занять та виконання лабораторних робіт для студентів усіх форм навчання за напрямом підготовки 6.050903 «Телекомунікації»/ НТУУ «КПІ»; уклад.: В. Г. Абакумов, П. В. Попович, К. О. Трапезон. – Київ: НТУУ «КПІ», 2013. – 146с. – Режим доступу: http://ela.kpi.ua/handle/123456789/211804

18. AWS IoT – Developer Guide. Amazon Web Services, 2020. – 262 Pages.

19. В.В. Ткаченко, М.Ю. Комаров, С.М. Сергєєв «Основні підходи до оцінки кібербезпеки SMART GRID систем» Європейський університет, Національний авіаційний університет: Актуальні питання забезпечення кібербезпеки та захисту інформації: VI Міжнародна наук-практ. конф., Київ 2020, С. 99 –104.

20. Закон України «Про основні засади забезпечення кібербезпеки України».

21. Постанова Кабінету Міністрів України від 19 червня 2019 року No 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури».

22. Постанова Кабінету Міністрів України від 11 листопада 2020 року No1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

23. С.Ф. Гончар. Алгоритм визначення актуальних загроз безпеці інформації на об'єктах критичної інфраструктури/ Гончар С.Ф., Юдін О.Ю., Леоненко Г.П. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2016. – No2(32). –С. 40-48.

24. С.Ф. Гончар. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури. Монографія. – К.: «Альфа Реклама», 2019. – 176 с.

*Інтернет-джерела*

25. Cisco -Україна. URL: https://www.cisco.com/c/uk_ua/index.html
26. Cisco академія. URL: https://www.netacad.com/ru
27. Smart-інфраструктура: головні характеристики та функції. URL: https://razumkov.org.ua/uploads/other/2021-SMART-%D0%A1YTI-SITE.pdf
28. Huang Y. When the U.S. and China Fight, It Is the Environment That Suffers. – The New YorkTimes, 12 October 2020. URL: https://www.nytimes.com/2020/10/12/opinion/china-us-environment.html.15
29. Make or break for green economy. – SDG Pulse, United Nations,. URL: https://sdgpulse.unctad.org/green-economy/#9-4-1
30. Global Energy Review 2020. The impacts of the COVID-19 crisison global energy demand and CO2 emissions. – IEA, April 2020. URL: https://www.iea.org/reports/global-energy-review-2020.
31. Huang Y. When the U.S. and China Fight, It Is the Environment That Suffers. – The New YorkTimes, 12 October 2020. URL: https://www.nytimes.com/2020/10/12/opinion/china-us-environment.html.15
32. Make or break for green economy. – SDG Pulse, United Nations. URL: https://sdgpulse.unctad.org/green-economy/#9-4-1.
33. GlobalEnergyReview 2020. TheimpactsoftheCOVID-19 crisisonglobalenergydemandandCO2emissions. – IEA, April 2020. URL: https://www.iea.org/reports/global-energy-review-2020.)
34. Smart city spending share worldwide in 2019, by use case. – Statista, 22 April 2020. URL: https://www.statista.com/statistics/884130/worldwide-smart-city-investment-initiatives-use-case.33
35.Третяк Я. Галузі майбутнього: "розумні" міста та будинки. – Mind, 11 вересня 2018р. URL: https://mind.ua/publications/20188390-galuzi-majbutnogo-rozumni-mista-ta-budinki.
36. Tushar W., Yuen C., Mohsenian-Rad H., Saha T., Poor H.V., Wood K.L. Transforming Energy Networks via Peer-to-Peer Energy Trading. – IEEE Signal Processing Magazine. July 2018. URL: https://escholarship.org/content/qt8zw4735s/qt8zw4735s_noSplash_528854980c8cc6f006ab3c68be3f932c.pdf.32
37. 4G. – URL: http://forbes.net.ua/opinions/1390343–skolko–ukraincam–eshche–zhdat–vnedreniya–4g 2
38. LTE — це не стільки швидкість, скільки нові можливості. – URL: https://www.imena.ua/blog/lte-lifecell-report/.

39 . 4G ВІД VODAFON. URL:http://4g.vodafone.ua/uk10

40. Соснін О. Цифровізація як нова реальність України. – LexInform. Юридичні новини України, 18 січня 2020р. URL: https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny

41. The impact of technological change on future infrastructure supply and demand. – National Infrastructure Commission. URL: https://www.nic.org.uk/wp-content/uploads/2905991-NIC-TECHNICAL-v0_5-ACCESSIBLE.pdf

42. Allianz Risk Barometer. Identifying The Major Business Risks for 2021. – Allianz Group. URL: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2021.pdf.

43. The Global Risks Report 2021, 16th Edition. Insight Report. – World Economic Forum, 2021. URL: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf)

44. Chalimov A. Smart Cities: Challenges & Opportunities for a Sustainable Environment. – Eastern Peak, 19 August 2019. URL: https://easternpeak.com/blog/smart-cities-challenges-opportunities-for-a-sustainable-environment

45. Top 8 Benefits of Technology Parks. – Percento Technologies International, 16 February 2019. URL: https://percentotech.com/top-8-benefits-of-technology-parks

46. Лекція 1 з навчальної дисципліни «Архітектура і технології IoT» [Електронний ресурс] – Режим доступу: https://learn.ztu.edu.ua/mod/folder/view.php?id=26748

47. Проектування Інтернет речей (IoT) [Електронний ресурс] – Режим доступу: https://www.slideshare.net/ssuserf405bc/iot-7960856315.