**ДЕРЖАВНИЙ ТОГРОВЕЛЬНО-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
(пост. п. 12 від «10» 03 2024 р.)
Ректор
_____ Анатолій МАЗАРАКІ

# АНАЛІЗ ЗАГРОЗ ТА ЕКСПЛУАТАЦІЇ УРАЗЛИВОСТЕЙ /
# ANALYSIS OF THREATS AND EXPLOITATION OF VULNERABILITIES

## ПРОГРАМА /
## COURSE SUMMARY

**Київ 2024**

Автори: Ю.Є. ХОХЛАЧОВА, кандидат технічних наук, професор . кафедри безпеки інформаційних технологій Національного авіаційного університету ,
Д.Д. ЧЕРНИШОВА, асистент кафедри інженерії програмного забезпечення та кібербезпеки

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «22» січня 2024р., протокол № 20.

Рецензенти: Н.О. КОТЕНКО, канд. пед. наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
В.П. ЗВЄРЄВ, кандидат технічних наук, заступник керівника служби з питань інформаційної безпеки та кібербезпеки – керівник управління інформаційної безпеки Апарату Ради Національної безпеки і оборони України

**АНАЛІЗ ЗАГРОЗ ТА ЕКСПЛУАТАЦІЇ УРАЗЛИВОСТЕЙ /**
ANALYSIS OF THREATS AND EXPLOITATION OF VULNERABILITIES

# ПРОГРАМА /
# COURSE SUMMARY

## ВСТУП

Дисципліна «Аналіз загроз та експлуатації уразливостей» є обов'язковою компонентою навчального плану підготовки студентів денної та заочної форм навчання другого (магістерського) рівня вищої освіти галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека та захист інформації», освітньої програми «Безпека систем електронних комунікацій в економіці».

Програму підготовлено відповідно до Стандарту вищої освіти України із зазначеної спеціальності та відповідної освітньо-професійної програми підготовки магістрів ДТЕУ.

Програма складається з таких частин:

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 навчальної дисципліни «Аналіз загроз та експлуатації уразливостей» є формування у майбутніх спеціалістів системи теоретичних знань та практичних умінь про сучасні наукові концепції, поняття, принципи і методики аналізу та опрацювання консолідованих інформаційних ресурсів та інженерії знань, що є практичною основою для фахівця в галузі кібербезпеки.

**Завданням** дисципліни є: оволодіння технологіями моделювання інформаційних систем в умовах невизначеності; моделювання кіберресурсів; оволодіння механізмами кіберресурів із забезпеченням безпеки

**Предметом** вивчення дисципліни є технології моделювання інформаційних систем в умовах невизначеності та моделювання кіберресурсів.

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

*знання:*

- інформаційних технологій;
- безпека інформаційних систем та мереж;
- іноземної мови за професійним спрямуванням;
- організації комп'ютерних мереж.

*вміння:* вільно працювати:

- з офісними додатками Microsoft;
- з хмарними сервісами Office 365;
- з пошуковою системою Google.

## *3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ*

Дисципліна «Аналіз загроз та експлуатації уразливостей» 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»)***

| 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. | 1-14 |
| КЗ-2. | Здатність проводити дослідження на відповідному рівні. | 1-14 |
| КЗ-3. | Здатність до абстрактного мислення, аналізу та синтезу. | 1-14 |
| КЗ-4. | Здатність оцінювати та забезпечувати якість виконуваних робіт. | 1-14 |
| КЗ-5. | Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). | 1-14 |
| *Спеціальні (фахові, предметні) 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. | 1-14 |
| КФ3. | Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. | 1-14 |
| 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. | 1-14 |
| *Програмні результати навчання за освітньою програмою* | | |
| РН5 | Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі | 1-14 |

| Номер в освітній програмі | Зміст компетентності | Номер теми, що розкриває зміст компетентності |
|---|---|---|
| | розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. | |
| РН6 | Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. | 1-14 |
| 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. | 1-14 |
| РН15 | Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. | 1-14 |
| 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. | 1-14 |

## *4. ЗМІСТ ДИСЦИПЛІНИ*

### Тема 1. Національна база даних уразливостей (National Vulnerability Database)

Поняття та історія виникнення Національной бази даних уразливостей (National Vulnerability Database). Зміст та склад бази даних. Протокол автоматизації контенту безпеки – Security Content Automation Protocol (SCAP), Складові компоненти, опис та призначення.

***Список рекомендованих джерел:***

*Основний: 3, 4.*
*Додатковий: 3, 4*
*Інтернет-ресурси: 1, 2, 3, 4*

### Тема 2. Протоколи документування, відстеження та спільного використання інформації про інциденти

Протоколи документування та спільного використання структурної інформації про загрози. Threat Analysis Automation Protocol (TAAP), основні компоненти. Event Management Automation Protocol (EMAP) – протокол для звітів про події безпеки, основні складові. Incident Tracking and Assessment Protocol (ITAP) – протокол для відстеження, документування, управління та спільного використання інформації про інциденти, основні компоненти.

***Список рекомендованих джерел:***

*Основний: 3, 4*
*Додатковий: 1, 5*
*Інтернет-ресурси: 1, 2, 8*

### Тема 3. Банк даних загроз безпеки інформації.

Відомості про загрози ІБ та уразливості ПЗ. Види загроз інформаційній безпеці. Джерела загроз інформаційної безпеки. Основні параметри загроз та уразливостей. Інформаційна безпека та захист персональних даних.

***Список рекомендованих джерел:***

*Основний: 1, 4*
*Додатковий: 1, 3*
*Інтернет-ресурси: 1, 2, 9, 10*

### Тема 4. Калькулятор CVSS v2.0.

Аналіз на сайті бази даних безпеки інформації калькулятора CVSS v2.0. Історія та основні моменти. Формули для розрахунку калькулятора CVSS v2.0. Приклади та застосування. Критика та порівняння версій

стандарту. Приклади уразливостей з рахунком 10,0.

***Список рекомендованих джерел:***

*Основний: 3, 4*
*Додатковий: 1, 3*
*Інтернет-ресурси: 1, 2*

## Тема 5. База даних уразливостей від відкритих джерел (Open Sourced Vulnerability Database).

Історія виникнення та мета проєкту. Основні відомості про базу уразливостей від відкритих джерел. Опис уразливості, що заноситься в OSVDB. Інтерфейс OSVDB.

***Список рекомендованих джерел:***

*Основний: 2, 3, 4*
*Додатковий: 1, 3*
*Інтернет-ресурси: 1, 2, 3, 6*

## Тема 6. Сучасні бази даних атак та їх використання в системах виявлення вторгнень.

Бази даних атак та їх структура. Набір даних NSL-KDD. База даних All.Net Security. Набір даних UNSW-NB15. Набори даних ADFA-LD та ADFA-WD.

***Список рекомендованих джерел:***

*Основний: 2, 3, 4*
*Додатковий: 1, 3, 5*
*Інтернет-ресурси: 1, 2*

## Тема 7. База даних інцидентів веб-хакерства

Основні питання щодо баз даних інцидентів веб-хакерства. Приклади та можливі варіанти захисту від злому. База даних інцидентів веб-хакерства The Web Hacking Incident Database (WHID).

***Список рекомендованих джерел:***

*Основний: 2, 3, 4*
*Додатковий: 1, 3*
*Інтернет-ресурси: 1, 2*

## Тема 8. Бази даних атак, сформовані при проведенні конкурсів з кібербезпеки.

Основні відмінності та особливості баз даних атак. Складові частини. Переваги та недоліки. Особливості баз даних атак та їх використання в сучасних системах виявлення вторгнень.

***Список рекомендованих джерел:***

*Основний: 1, 2, 3, 4*
*Додатковий: 1, 2, 3, 4, 5*
*Інтернет-ресурси: 1, 2*

## Тема 9. База даних уразливостей IBM X-Force.

Історія виникнення. Складові частини. Основні відомості про базу даних уразливостей IBM X-Force. Процес доступу. Приклад опису уразливості Microsoft Excel Remote Code Execution.

***Список рекомендованих джерел:***

*Основний: 1, 2, 3, 4*
*Додатковий: 1, 2, 3*
*Інтернет-ресурси: 1, 2, 5*

## Тема 10. База даних записів уразливостей US-CERT

Основні відомості про базу даних записів уразливостей US-CERT. Історія виникнення та розробки. Ідентифікатор «VU #». Основні пункти опису уразливостей. Відмінності від інших баз даних. Переваги та недоліки.

***Список рекомендованих джерел:***

*Основний: 1, 2, 3, 4*
*Додатковий: 1, 2, 3, 4, 5*
*Інтернет-ресурси: 1, 2, 6, 7*

## Тема 11. Бази даних уразливостей в VND.

Основні пункти опису уразливості в VND. Приклад опису уразливостей. Вільні дані оцінок CVSS. Історія, термінологія. Базові показники: вектор доступу, складність доступу, автентифікація. Методи впливу: конфіденційність, цілісність, доступність. Розрахунки, приклади. Темпоральні метрики та метрики середовища. Порівняння та критика версії 2 та версії 3.

***Список рекомендованих джерел:***

*Основний: 1, 2, 3, 4*
*Додатковий: 1, 2, 3, 4, 5*
*Інтернет-ресурси: 1, 2, 9, 10*

## Тема 12. База даних уразливостей SecurityFocus.

Історія виникнення та основні відомості. Вміст та особливості. Дослідження бази даних уразливостей SecurityFocus. Візуалізація та огляд інтерфейсу. Приклад опису уразливості Bugtraq 77270.

***Список рекомендованих джерел:***

*Основний: 1, 2, 3, 4*
*Додатковий: 1, 2, 3, 4*
*Інтернет-ресурси: 1, 2*

## Тема 13. Бази шаблонів атак KDD-99.

Категорування баз даних на основі принципів теорії подібності. Опис параметрів мережевого з'єднання за базою шаблонів атак KDD-99. Структура шаблонів нормальної поведінки та кібератак за базою KDD Cup 1999.

***Список рекомендованих джерел:***

*Основний: 1, 2, 3, 4*
*Додатковий: 1, 2, 3, 4*
*Інтернет-ресурси: 1, 2, 8, 9, 10*

## Тема 14. Бази шаблонів атак CAPEC.

Структура бази CAPEC. Загальний перелік та класифікація комп'ютерних атак бази шаблонів атак CAPEC. Порівняльний аналіз баз шаблонів. Узагальнена схема формування джерел первинних даних для розроблення шаблонів потенційно небезпечних КбА.

***Список рекомендованих джерел:***

*Основний: 1, 2, 3, 4*
*Додатковий: 1, 2, 3, 4*
*Інтернет-ресурси; 1, 2, 8, 9*

## *5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ*

### *Основний*

1. Луцький М.Г., Хорошко В.О., Хохлачова Ю.Є., Козловський В.В., Баланюк Ю.В., Прав Ю.Г. Новітні технології захисту інформації: підручник. К.: НАУ, 2023 312 с.

2. М.М. Браіловський, Н.С. Вишневська, В.Д. Козюра, Ю.В. Пепа, В.О. Хорошко, Ю.Є. Хохлачова. Комп'ютерні технології: навчальний посібник. К.: ФОП Ямчинський О.В., 2023. 200 с.

3. Браіловський М.М., Зибін С.В., Кобозєва А.А., Хорошко В.О., Хохлачова Ю.Є. Аналіз кіберзахищеності інформаційних систем Київ: ФОП Ямчинський О.В. 2021. 360 с.

*4. Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с.*

### *Додатковий*

*1. Хорошко О.В. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.*

2. Браіловський М.М., Зибін С.В., Пискун І.В., Хорошко В.О., Хохлачова Ю.Є. Технології захисту інформації. К.: ЦП «Компринт», 2021. 296 стр.

3. Технології виявлення уразливостей інформаційних систем: лабораторний практикум / Ю.Є. Хохлачова , В.М. Кінзерявий, В.В. Погорелов та ін. К.: НАУ, 2022. 68 с.

4. М.М. Браіловський, В.Д. Козюра, В.В. Кузавков, Ю.В. Пепа, Ю.М. Ткач, В.О. Хорошко. Спеціалізовані програмні засоби наукових досліджень: навчальний посібник. К.: ФОП Ямчинський О.В., 2022. 204 с.

5. Остапов С. Е., Євсеєв С. П., Король О.Г. Кібербезпека : сучасні технології захисту: навчальний посібник. Львів: Новий Світ-2000, 2020.

### *Інтернет-ресурси*

1. www.rada.gov.ua – офіційний сайт Верховної Ради України.

2. www.dstszi.gov.ua/dstszi - офіційний сайт ДСТЗІ.

3. «National Vulnerability Database» [Electronic resource], National Institute of Standards and Technology, Gaithersburg, 2016, [Online]. Access mode: https://nvd.nist.gov/home.cfm.

4. «Open Sourced Vulnerability Database» [Electronic resource], Open Security Foundation, Lafayette, 2016, [Online]. Access mode: https:// http://osvdb.org/

5. «IBM X-Force Exchange» [Electronic resource], IBM Corporation, New York, 2016, [Online]. Access mode: https:// exchange. xforce. ibmcloud.com/ vulnerabilities/109429.

6. «Vulnerability Notes Database» [Electronic resource], United States Computer Emergency Readiness Team, Murray Lane, 2016, [Online]. Access mode: https://www.kb.cert.org/vuls/#

7. «Vulnerabilities» [Electronic resource], SecurityFocus, Mountain View, 2016 [Online]. Access mode: http://www.securityfocus.com/ -53r4 – Falls Church: Natl. Inst. Stand. Technol, 2013, p. 462.

8. «A Complete Guide to the Common Vulnerability Scoring System. Version 2.0», [Electronic resource], Forum of Incident Re-sponse and Security Teams, Morrisville, 2016, [Online]. Access mode: http://www.first.org/cvss/v2/guide.

9. «Common Vulnerability Scoring System v3.0: User Guide» [Electronic resource], Forum of Incident Response and Security Teams, Morrisville, 2016, [Online]. Access mode: http://www.first.org/cvss /user-guide.

10. «CWE™ International in scope and free for public use», [Electronic resource], MITRE, Bedford, 2016, [Online]. Access mode: http://cwe.mitre.org/index.html.

**Курсивом зазначені джерела, що є в наявності в бібліотеці ДТЕУ*