ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»

Факультет суспільних і прикладних наук

Кафедра права імені академіка УАН о. Івана Луцького

ЗАТВЕРДЖУЮ
Проректор з навчально-методичної роботи
_____ Ярослав ШТАНЬКО
«19» 02 2025 р.

КІБЕРБЕЗПЕКА І УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Галузь знань:	К Безпека та оборона
Спеціальність:	К 9 Правоохоронна діяльність
Освітньо-професійна програма:	«Правоохоронна діяльність»
Освітній рівень:	перший (бакалаврський)
Статус дисципліни:	обов'язкова
Мова викладання, навчання та оцінювання:	українська

Івано-Франківськ
2025

РОЗРОБНИК:
Професор кафедри права імені академіка УАН о. Івана Луцького
доктор юридичних наук,
професор Микола КАРЧЕВСЬКИЙ

ЗАТВЕРДЖЕНО:
на засіданні кафедри права імені академіка УАН о. Івана Луцького,
протокол № 4 від 18 листопада 2025 р.

в.о. завідувача кафедри Олександра ПТАШНИК

УЗГОДЖЕНО:
Гарант ОП Микола КАРЧЕВСЬКИЙ

СХВАЛЕНО:
на засіданні Науково-методичної ради, протокол № 4 від 28.11.2025 р.

E-mail	mykola.karchevskyi@ukd.edu.ua
Номер аудиторії чи кафедри	Кафедра права імені академіка УАН о. Івана Луцького, ауд. 201
Посилання на сайт	Микола Карчевський
Сторінка курсу в СДО	Кібербезпека і управління інформаційними ресурсами.

ВСТУП

У сучасних умовах цифровізації суспільства кібербезпека є невід'ємним елементом безпеки держави, суспільства, бізнесу та кожного громадянина. Для фахівців у сфері правоохоронної діяльності вивчення кібербезпеки та управління інформаційними ресурсами є особливо важливим, адже їхня професійна діяльність безпосередньо пов'язана із захистом інформації, реагуванням на кіберінциденти та забезпеченням інформаційної безпеки держави та громадян.

Злочинний світ активно використовує цифрові технології, застосовуючи складні методи кібератак, соціальної інженерії та використання штучного інтелекту для незаконних дій. Успішне протистояння таким загрозам потребує від правоохоронців не лише базових знань у сфері інформаційної безпеки, а й глибокого розуміння механізмів атак, сучасних технологічних рішень для їх виявлення, запобігання та реагування.

Дисципліна «Кібербезпека та управління інформаційними ресурсами» спрямована на формування у студентів необхідних знань та практичних навичок для ідентифікації кіберзагроз, управління інформаційними активами, розробки політик інформаційної безпеки, а також реагування на кіберінциденти. Опанування цієї дисципліни дозволить студентам ефективно працювати у правоохоронних органах, кіберпідрозділах, державних структурах та приватних компаніях, які займаються захистом інформаційних ресурсів.

ПІСЛЯ ВИВЧЕННЯ ДИСЦИПЛІНИ ПОВИННІ ЗНАТИ:

- Основні поняття кібербезпеки, зокрема активи, загрози, уразливості та ризики.
- Класифікацію та характерні риси кіберзагроз, методи атак та способи їх виявлення.
- Нормативно-правову базу України та міжнародні стандарти кібербезпеки (ISO/IEC 27001, NIST Cybersecurity Framework).
- Основні політики кібербезпеки, управління IT-активами та механізми захисту інформації.
- Технологічні рішення для забезпечення кібербезпеки: шифрування, міжмережеві екрани, системи виявлення та запобігання вторгненням (IDS/IPS), багатофакторну автентифікацію (MFA).
- Життєвий цикл кіберінцидентів та основні підходи до реагування на кіберзагрози.
- Використання штучного інтелекту та великих даних у сфері кібербезпеки.

ПІСЛЯ ВИВЧЕННЯ ДИСЦИПЛІНИ ПОВИННІ ВМІТИ:

- Ідентифікувати кіберзагрози та оцінювати їхній рівень ризику для інформаційних активів.
- Застосовувати методи аналізу загроз та інцидентів за допомогою сучасних інструментів кіберзахисту.

- Розробляти та впроваджувати політики інформаційної безпеки для організацій та установ.
- Використовувати механізми захисту даних, зокрема шифрування, контроль доступу, резервне копіювання.
- Аналізувати вразливості систем та застосовувати методи їх усунення.
- Здійснювати моніторинг та реагування на кіберінциденти, використовуючи сучасні технологічні засоби (SIEM-системи, антивірусне програмне забезпечення, аналіз мережевого трафіку).
- Інтерпретувати правові аспекти кібербезпеки та застосовувати їх у сфері правоохоронної діяльності.

Компетентності та результати навчання, яких набувають здобувачі вищої освіти внаслідок вивчення навчальної дисципліни	
Шифр та назва компетентності	**Шифр та назва програмних результатів навчання**
ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності.	**ПРН 3**. Розуміти та професійно застосовувати понятійний апарат права та правоохоронної діяльності.
СК 8. Здатність ефективно застосовувати сучасну техніку та інформаційні технології, використовувати технічні засоби, спеціалізовані інформаційно-пошукові системи, бази та банки даних, а також відповідне програмне забезпечення для захисту прав і свобод людини, власності, суспільних відносин від протиправних посягань	**ПРН 9**. Використовувати інформаційно-комунікаційні системи та інші інформаційні ресурси, у тому числі ті, що мають технічний та криптографічний захист, поштовий зв'язок спеціального призначення, фельд'єгерський зв'язок, системи цифрового зв'язку суб'єктів сектору безпеки і оборони з метою виконання професійних завдань у сфері правоохоронної діяльності.
СК 11. Здатність визначати особу правопорушника, аналізувати кількісні та якісні показники злочинності	**ПРН 21.** Організовувати та здійснювати заходи щодо дотримання режиму секретності та захисту інформації.
СК 16. Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об'єктів критичної інфраструктури	

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Курс	**Перший (1)**		
Семестр	**Семестр (ІІ)**		
Кількість кредитів ЄКТС	**3 (90 год)**		
Аудиторні навчальні заняття		**денна форма**	**заочна форма**
	лекції	14 год.	4 год.
	семінари, практичні	16 год.	4 год.
Самостійна робота		60 год.	82 год.
Форма підсумкового контролю	**Екзамен**		

Структурно-логічна схема вивчення навчальної дисципліни:

Пререквізити	**Постреквізити**
Кримінальне право України	Кримінальне право України
Кримінальне процесуальне право України	Криміналістика
Інформаційно-аналітичне забезпечення правоохоронної діяльності	Організація простору безпеки

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Перелік тем лекційного матеріалу

Тема 1. Вступ до кібербезпеки (2 години)

Кібербезпека та інформаційна безпека. Актуальність кібербезпеки в умовах цифровізації суспільства. Значення кібербезпеки для державних установ, бізнесу та громадян.

Основні поняття кібербезпеки: активи, загрози, уразливості, ризики. Активи: що потрібно захищати (дані, системи, люди, процеси). Загрози: що може завдати шкоди (зловмисники, природні катастрофи, помилки персоналу). Уразливості: слабкі місця системи (незахищені мережі, застаріле ПЗ). Ризики: імовірність втрати чи шкоди для активів. Оцінка ризиків

Розвиток кіберзагроз: історичний аспект та сучасні тренди. Історія перших вірусів і атак: від Morris Worm до сучасних APT-угруповань. Еволюція кіберзагроз: класичні віруси та черв'яки; мережеві атаки (DDoS, маніпуляція даними); сучасні виклики: ransomware, deepfake-атаки, використання штучного інтелекту зловмисниками.

Нормативне регулювання кібербезпеки. Міжнародні стандарти кібербезпеки: ISO/IEC 27001 (система управління інформаційною безпекою), NIST Cybersecurity Framework. Закон України "Про основні засади забезпечення кібербезпеки України". Діяльність CERT-UA.

Тема 2. IT активи та їх захист (2 години)

IT активи: поняття та види. Дані: персональні дані, корпоративна інформація, державні реєстри. Програмне забезпечення: системи управління базами даних, прикладні програми. Інфраструктура: сервери, мережі, системи зберігання даних.

Класифікація IT активів за критичністю. Критерії оцінки критичності. Значення для бізнесу чи організації. Потенційні наслідки втрати чи компрометації. Приклади класифікації: особисті дані користувачів як критичні, загальнодоступні ресурси як некритичні.

Політики управління IT активами. Документ, що регулює процеси доступу, використання та захисту активів. Елементи політики: розмежування прав доступу; регламент роботи з персональними даними (GDPR, Закон України "Про захист персональних даних"); резервне копіювання і відновлення даних. Ролі в управлінні: власники інформації, адміністратори ресурсів, користувачі (працівники, підрядники).

Тема 3. Кіберзагрози та методи атак (2 години)

Визначення кіберзагроз. Класифікація кіберзагроз. За джерелами загроз: внутрішні (недбалість працівників, зловмисні дії співробітників); зовнішні (хакери, кібершпигуни, організовані кіберзлочинні угруповання). За характером впливу (порушення конфіденційності, порушення цілісності, порушення доступності). За метою: економічні (шахрайство, крадіжка даних); політичні (кібершпигунство, пропаганда); соціальні (дезінформація, маніпуляція суспільною думкою).

Методи атак та їхні характеристики. Фішинг, підроблені електронні листи або сайти для крадіжки облікових даних. Шкідливе ПЗ: віруси, трояни. Соціальна інженерія, маніпуляція людьми для отримання доступу до інформації (дзвінки, фальшиві листи). DDoS-атаки (розподілені атаки на відмову в обслуговуванні). SQL-ін’єкції, впровадження шкідливого коду в запити до баз даних. Ransomware (програми-вимагачі), шифрування даних із вимогою викупу.

Атаки із застосуванням штучного інтелекту. Автоматизація фішингу, генерація deepfake-відео для маніпуляцій. IoT-атаки, злом "розумних" пристроїв (камери, термостати) для доступу до мереж. Zero-day атаки, використання невідомих вразливостей програмного забезпечення.

Відповідальність і етичні аспекти. Кримінальна відповідальність за правопорушення в сфері використання інформаційних технологій (ст.ст. 361 -363-1 Кримінального кодексу України). Використання кіберзасобів у військових та політичних цілях. Роль етичних хакерів у забезпеченні безпеки.

Тема 4. Базові технологічні рішення кібербезпеки (2 години)

Роль технологій у запобіганні, виявленні та реагуванні на кіберзагрози. Еволюція захисних рішень: від антивірусів до комплексних систем кіберзахисту.

Шифрування даних. Криптографічні стандарти та захист спеціальної інформації. Використання криптографічних засобів захисту інформації (КЗЗІ), що мають сертифікацію відповідно до вимог ДССЗЗІ України. Розгляд основних криптографічних протоколів, що використовуються у державному секторі та секторі безпеки. Криптографічні протоколи для захищеного зв'язку. Розгляд протоколів IPsec та OpenVPN як основи для побудови захищених каналів зв'язку (VPN-шлюзи) для віддаленого доступу та обміну інформацією між відомствами.

Інформаційно-комунікаційні системи (ІКС) з технічним та криптографічним захистом.

Спеціальний поштовий та фельд'єгерський зв'язок (короткий огляд). Регламентація та забезпечення конфіденційності та цілісності інформації, що передається.

Системи цифрового зв'язку суб'єктів сектору безпеки і оборони. Вимоги до їхньої стійкості та захисту від радіоелектронної розвідки.

Міжмережеві екрани. Типи міжмережевих екранів.

Системи виявлення та запобігання вторгненням (IDS/IPS). IDS (Intrusion Detection System): система виявляє підозрілу активність, але не блокує її. IPS (Intrusion Prevention System): виявляє та блокує загрози в режимі реального часу. Інструменти: Snort, Suricata. Приклади кейсів: атаки DDoS та їх нейтралізація за допомогою IDS/IPS.

Захист кінцевих пристроїв. Антивірусні системи: як працюють та чому важливі (ESET, Windows Defender). Можливості моніторингу та аналізу поведінки пристроїв. Багатофакторна автентифікація (MFA).

Практичний кейс: санкції США проти компанії Kaspersky Lab.

Захист хмарних сервісів. Доступ до ресурсів з різних пристроїв і локацій. Захист від атак на API.

Тема 5. Реагування на кіберінциденти (2 години)

Що таке кіберінцидент? Мета реагування на кіберінциденти. Аналіз практичних кейсів вдалого та невдалого реагування.

Життєвий цикл кіберінциденту. Етапи реагування на кіберінциденти. Підготовка: створення плану реагування, навчання персоналу, використання інструментів моніторингу. Виявлення: методи ідентифікації інцидентів, приклади ознак інцидентів. Аналіз: оцінка масштабу загрози, визначення впливу на системи та дані. Локалізація: ізоляція уражених систем, запобігання поширенню загрози. Усунення: видалення шкідливого програмного забезпечення, встановлення оновлень безпеки. Відновлення: перевірка систем після очищення, повернення систем до нормального стану. Підсумковий аналіз: висновки з інциденту, внесення змін до планів безпеки.

Інструменти моніторингу та аналізу. SIEM-системи (Security Information and Event Management). Популярні рішення: Splunk, ArcSight, IBM QRadar. Інструменти аналізу шкідливого ПЗ. Пісочниці (Sandbox): аналіз програм у безпечному середовищі. Аналітичні платформи: VirusTotal, Hybrid Analysis. Захист від DDoS: Cloudflare, Akamai. Відстеження атак: Wireshark для аналізу мережевого трафіку.

Взаємодія з CERT та іншими інституціями. CERT-UA: роль у забезпеченні кібербезпеки України. Співпраця з органами правопорядку (кіберполіція). Міжнародна взаємодія: FIRST, ENISA, Global Forum on Cyber Expertise.

Тема 6. Політика інформаційної безпека організації (2 години)

Захист даних як основа довіри між компанією, клієнтами та партнерами. Типові виклики в організації: людський фактор, невчасне оновлення ПЗ, відсутність чітких процедур і політик.

Політики інформаційної безпеки. Документ, що визначає правила, процедури та стандарти для забезпечення безпеки. Основні компоненти політики: розмежування доступу до даних; процедури резервного копіювання та відновлення даних; регламент реагування на інциденти; навчання працівників з питань безпеки. Регулярний аудит політик.

Управління доступом. Моделі доступу. DAC (Discretionary Access Control): власник даних визначає доступ. RBAC (Role-Based Access Control): доступ визначається роллю користувача в організації. ABAC (Attribute-Based Access Control): доступ базується на атрибутах (час, місце, рівень). Інструменти для управління доступом. Active Directory. Системи SSO (Single Sign-On). MFA (багатофакторна автентифікація).

Ролі та відповідальності в інформаційній безпеці. CISO (Chief Information Security Officer): стратегічне управління безпекою. IT-відділ: технічне забезпечення захисту. Користувачі: дотримання правил безпеки.

Резервне копіювання та відновлення. Політика "3-2-1".

Регламент реагування на інциденти кібербезпеки, як частина політики кібербезпеки.

Важливість навчання працівників. Проведення тренінгів з протидії фішинговим атакам. Інструкції щодо безпечної роботи з пристроями та системами.

Режим секретності та захист державної таємниці. Законодавча база (Закон України "Про державну таємницю"). Поняття таємної інформації та режиму секретності. Організація заходів захисту інформації з обмеженим доступом (державна таємниця, службова інформація). Роль та відповідальність режимно-секретного органу (РСО). Документообіг в умовах режиму секретності: правила роботи з матеріальними носіями секретної інформації.

Тема 7. Перспективи кібербезпеки: штучний інтелект і великі дані (2 години)

Зростання кількості пристроїв і даних у мережах (IoT, хмари) та ускладнення атак через використання нових технологій як передумови автоматизації процесів кібербезпеки.

ШІ у кібербезпеці. Використання машинного навчання для аналізу аномалій у трафіку. Поведінкова аналітика. Автоматизація реагування (Splunk, QRadar). Прогнозування атак.

Проблемні аспекти використання ШІ у кібербезпеці. Помилкові спрацьовування. Використання ШІ зловмисниками. Автоматизація фішингових

атак. Генерація deepfake для соціальної інженерії. Використання ШІ для автоматизації сканування вразливостей.

Великі дані: аналітика загроз і прогнозування атак. Джерела великих даних: логи систем, дані про трафік, інформація з соціальних мереж. Технології аналізу. Інструменти візуалізації (Tableau, GoogleLooker).

Кейси: Crystal – система аналізу блокчейнів віртуальних активів, її використання для розслідування несанкціонованих транзакцій. Як великі дані допомогли виявити складні APT-угруповання.

Етичні аспекти та кібербезпека майбутнього. Використання штучного інтелекту для масового спостереження. Генеративні моделі для атак. Баланс між безпекою та приватністю: як уникнути надмірного втручання у приватне життя громадян.

Zero Trust: концепція повної недовіри до будь-якої активності у мережі. Колективна безпека: важливість міжнародної співпраці для подолання глобальних загроз.

Перелік тем практичних занять

Тема 1. Вступ до кібербезпеки (2 години)

Доповнення наведених у лекції чинників значення кібербезпеки для держави, бізнесу та громадян на основі аналізу чинного законодавства України

Аналіз визначення поняття «актив інформаційної безпеки», що наводяться у глосарії National Institute of Standards and Technology.

Аналіз кіберінцидентів, що мали місце в Україніна основі Закону України "Про основні засади забезпечення кібербезпеки України" та ISO 27001.

Дослідження інфографіки глобальних ризиків за матеріалами світового економічного форуму.

Практичне завдання 1. Наскрізний проєкт ч.1. Визначити групи для роботи над наскрізним проєктом та обрати установу, підприємство або організацію (реальну чи умовну), для якої буде створюватися політика кібербезпеки.

Вибір організації. Визначте установу, підприємство, державний орган, освітній заклад, стартап або інший тип організації, що буде об’єктом вашого проєкту. Обґрунтуйте, чому саме цю організацію ви обрали (актуальність, цікавість, доступність прикладів).

Характеристика організації. Опишіть сферу діяльності, цільові групи клієнтів чи користувачів, основні виробничі (бізнес) процеси. Сформулюйте мету кібербезпеки обраного об’єкта з урахуванням тріади CIA (Confidentiality, Integrity, Availability).

Результат представити у вигляді презентації, збереженої у хмарному сховищі університету. Як виконання завдання додати до СДО посилання на створену презентацію.

Тема 2. IT активи та їх захист (2 години)

Обговорення кейсів витоку даних у великих компаніях (наприклад, Facebook або Uber) у контексті питання класифікації IT-активів.

Діалог щодо політики доступу до IT активів університету на основі NIST Data Classification Guide.

Практичне завдання 2. Наскрізний проєкт ч.2. Визначити IT активи для вашого проєкту та запропонувати відповідні політики доступу.

Складіть перелік ключових IT-активів організації: дані (персональні, комерційна таємниця, навчальні матеріали, державні реєстри, резервні копії), програмне забезпечення (операційні системи, офісні пакети, прикладні програми, CRM/ERP-системи), комп'ютерне та мережеве обладнання (сервери, робочі станції, ноутбуки, мобільні пристрої, периферія, маршрутизатори, комутатори, Wi-Fi точки доступу, міжмережеві екрани).

Створіть таблицю-реєстр активів із зазначенням місцезнаходження, власників і статусу (критичний / некритичний).

Результат представити у вигляді презентації, збереженої у хмарному сховищі університету. Як виконання завдання додати до СДО посилання на створену презентацію.

Тема 3. Кіберзагрози та методи атак (2 години)

Обговорення повідомленнт про те, який метод атаки слухачі курсу вважають найбільш небезпечним і чому?

Дослідження реальних прикладів кібератак, що сталися в Україні чи світі, та коротке описання методів атак та наслідків. Для відповіді бажано скористатися ресурсами CERT-UA.

Практичне завдання 3. Наскрізний проєкт ч. 3. Визначення загроз, уразливостей, оцінка ризиків.

Виявлення потенційних загроз. Опишіть внутрішні та зовнішні загрози, які можуть вплинути на безпеку організації (технічні атаки, соціальна інженерія, людський фактор, фізичні ризики).

Ідентифікація уразливостей. Спробуйте визначити слабкі місця організації (наприклад: відсутність резервного копіювання, використання застарілого ПЗ, слабкі паролі, нестача політик безпеки).

Попередня оцінка ризиків. Опишіть можливі наслідки реалізації загроз через уразливості (втрата даних, репутаційні збитки, фінансові втрати, зупинка діяльності). Зробіть висновок, які ризики для цієї організації виглядають найбільш критичними.

Результат представити у вигляді презентації, збереженої у хмарному сховищі університету. Як виконання завдання додати до СДО посилання на створену презентацію.

Тема 4. Базові технологічні рішення кібербезпеки (2 години)

Перевірити сертифікат SSL/TLS на реальному сайті. Відкрити у браузері SSL Labs Server Test. Ввести доменне ім'я обраного сайту. Запропонувати інтерпретацію результатів роботи сервіси.

Описати, які технології кіберзахисту доцільно використовувати для захисту мережі в університеті.

Аналіз вимог до КЗЗІ. Дослідження та обговорення вимог до криптографічних засобів захисту інформації, що використовуються в державних установах відповідно до стандартів ДССЗЗІ. Студенти мають знайти приклади сертифікованих рішень (наприклад, для шифрування каналів чи електронного підпису).

Практичне завдання 4. Наскрізний проєкт ч. 4. Запропонуєте перелік технічних засобів (до семи позицій) кібербезпеки Вашого проєкту з описанням функціонального призначення по кожній позиції. На цьому етапі необхідно запропонувати конкретні технологічні рішення, які допоможуть мінімізувати критичні ризики та захистити ІТ-активи, визначені у попередніх частинах (ч. 2 та ч. 3).

Формування переліку засобів. Складіть деталізований перелік рекомендованих засобів кібербезпеки. Цей перелік повинен включати як програмне забезпечення, так і апаратні рішення. Міжмережеві екрани (Firewall - NGFW/UTM), системи виявлення/запобігання вторгнень (IDS/IPS), VPN-шлюзи, системи контролю доступу до мережі (NAC). Антивірусне/Антишкідливе ПЗ (Antivirus/Anti-Malware), рішення класу EDR (Endpoint Detection and Response), DLP-системи (Data Loss Prevention) для захисту даних на робочих станціях. Системи резервного копіювання та відновлення (Backup & Recovery), системи керування доступом та ідентифікацією (IAM/IdM), системи управління привілейованим доступом (PAM). Системи управління інформаційною безпекою та подіями безпеки (SIEM - Security Information and Event Management). Поштові шлюзи безпеки (Email Security Gateway), проксі-сервери з функціями фільтрації (Secure Web Gateway).

Опис функціонального призначення. Для кожної позиції у переліку чітко опишіть її основну функцію і поясніть, як саме вона вирішує визначену вами раніше загрозу або усуває критичну вразливість для вашої конкретної організації.

Пропозиція на ринку. Для кожної позиції знайдіть комерційну пропозицію, визначте ціну та можливість придбання.

Обґрунтування вибору. Стисло обґрунтуйте, чому саме ці технології є найбільш доцільними та економічно виправданими для обраної вами організації (наприклад, виходячи з її розміру, бюджету, сфери діяльності та найбільш критичних активів).

Результат представити у вигляді презентації, збереженої у хмарному сховищі університету. Як виконання завдання додати до СДО посилання на створену презентацію.

Тема 5. Реагування на кіберінциденти (2 години)

Сценарій: у мережі інтернет магазину зафіксовано аномальний сплеск трафіку. Студенти повинні: обґрунтувати висновок щодо можливого інциденту, визначити можливу причину, запропонувати кроки для локалізації та усунення проблеми. Бажано використовувати: посібник NIST "Computer Security Incident Handling Guide" (SP 800-61); огляд інструментів аналізу інцидентів від CERT-UA.

Практичне завдання 5. Наскрізний проєкт ч. 5. Запропонуй описання циклу реагування на інцидент, пов’язаний з одним з визначених Вами ризиком (практичне завдання 3).

Сформулюйте у чому в ситуації реалізації цього ризику полягає:

- підготовка (план, навчання персоналу, використання інструментів моніторингу);
- виявлення (методи ідентифікації інцидентів, приклади ознак інцидентів);
- аналіз (оцінка масштабу, визначення впливу на системи та дані);
- локалізація (ізоляція уражених систем, запобігання поширенню загрози);
- усунення (видалення шкідливого програмного забезпечення, встановлення оновлень безпеки);
- відновлення (перевірка систем після очищення, повернення систем до нормального стану);
- підсумковий аналіз (висновки з інциденту, внесення змін до планів безпеки).

Результат представити у вигляді презентації, збереженої у хмарному сховищі університету. Як виконання завдання додати до СДО посилання на створену презентацію.

Тема 6. Перспективи кібербезпеки: штучний інтелект і великі дані

Знайти реальний приклад використання ШІ або великих даних для забезпечення кібербезпеки та підготувати короткий звіт.

Приклади напрямків для дослідження: Використання машинного навчання (ML) у системах EDR (виявлення аномальної поведінки), застосування Big Data для аналізу логів SIEM (кореляція мільйонів подій), ШІ для автоматизованого полювання на загрози (Threat Hunting) або для класифікації фішингових листів.

Обговорення етичних та безпекових викликів, пов'язаних із впровадженням ШІ в кібербезпеку (наприклад, Deepfake атаки, використання ШІ зловмисниками, проблема "чорного ящика" в ML-моделях).

Концепція Zero Trust. Дослідження та обговорення основних принципів архітектури Zero Trust (Нульової Довіри) та її зв'язку з необхідністю обробки великих обсягів даних.

Практичне завдання 6. Наскрізний проєкт ч. 6. Інтеграція сучасних трендів. Ціль: оцінити потенціал використання сучасних технологій (Штучний Інтелект, Великі Дані, Zero Trust) для посилення політики кібербезпеки обраної організації.

Визначте 1-2 конкретні проблеми або ризики у вашій організації (визначені в ч. 3), які можна потенційно вирішити або мінімізувати за допомогою ШІ (Machine Learning) або аналізу Великих Даних (Big Data Analytics).

Наприклад: якщо критичною загрозою є соціальна інженерія, запропонуйте використання ШІ-фільтра для пошти, який аналізує поведінку користувача та контент листів. Якщо це несанкціонований доступ, запропонуйте ML-систему моніторингу поведінки користувачів.

Концепція Zero Trust. Поясніть, як принципи Zero Trust ("Нікому не довіряти, завжди перевіряти") можуть бути застосовані до вашої організації.

Сформулюйте 2-3 ключові зміни у політиці доступу (ч. 2) або технічних рішеннях (ч. 4), які б відповідали філософії Zero Trust.

Сформулюйте висновок про те, як впровадження цих трендів (ШІ, Big Data, Zero Trust) підвищить захищеність, швидкість реагування та ефективність кібербезпеки вашого об'єкта.

Результат представити у вигляді презентації, збереженої у хмарному сховищі університету. Як виконання завдання додати до СДО посилання на створену презентацію.

Тема 7. Політика інформаційної безпека в організації (4 години)

Аналіз кейсу співробітник отримує фальшивий лист із запитом на доступ до конфіденційної інформації. Як діяти?

Скласти коротку політику доступу до корпоративної Wi-Fi мережі.

Запропонувати вдосконалення до політики інформаційної безпеки університету.

Практичне завдання 7. Наскрізний проєкт ч. 7. На підставі попередніх завдань підготувати презентацію політики кібербезпеки Вашого проєкту. Закріпити знання з основ кібербезпеки шляхом практичного моделювання політики безпеки для реального або умовного об’єкта (банк, університет, кав’ярня, інтернет-магазин, державна установа тощо).

Завдання поєднує ключові теми курсу - активи, загрози, уразливості, ризики, політики безпеки, реагування на інциденти та перспективи розвитку.

Кожна команда готує презентацію до 10 слайдів відповідно до наведеної структури.

Структура презентації:

1. Назва команди та обраного об’єкта.

(Напр.: “Team CyberShield – CoffeeHouse IF”)

2. Характеристика об’єкта.

“Я працюю фахівцем з кібербезпеки у… (короткий опис діяльності, масштаб, кількість працівників, тип даних, які обробляються)”

3. ІТ-активи.

Перелік даних, ПЗ, технічного обладнання.

4. Можливі загрози для виявлених активів.

Класифікація за видами активів. Окремо вітається додатковий рівень класифікації: технічні, людські, природні, організаційні.

5. Уразливості об’єкта.

Типові недоліки (незахищені порти, слабкі паролі, відсутність оновлень, людський фактор).

6. Ризики.

загроза – уразливість – наслідки – імовірність – рівень ризику.

7. Структура політики безпеки.

Ключові положення:

- контроль доступу до даних;
- резервне копіювання;
- реагування на інциденти;
- навчання персоналу;
- аудит політики безпеки.

8. Можливі технічні рішення.

(антивірус, IDS/IPS, міжмережеві екрани, SIEM, MFA, резервні системи, хмарні сервіси).

10. Перспективи розвитку кібербезпеки об’єкта. Використання ШІ, великих даних, Zero Trust, автоматизації.

Результат представити у вигляді презентації, збереженої у хмарному сховищі університету. Як виконання завдання додати до СДО посилання на створену презентацію.

Кібербезпека та управління інформаційними ресурсами:

Найменування видів робіт	Розподіл годин за формами навчання	
	денна	заочна
Самостійна робота, год, зокрема:	60	82
Опрацювання матеріалу, викладеного на лекціях	10	10
Підготовка до практичних занять та контрольних заходів	10	15
Виконання індивідуальних практичних робіт	10	15
Підготовка до поточного контролю	15	17
Опрацювання матеріалу, винесеного на самостійне вивчення	15	25

ПОЛІТИКА КУРСУ

1) щодо системи поточного і підсумкового контролю

Організація поточного та підсумкового семестрового контролю знань студентів, проведення практик та атестації, переведення показників академічної успішності за 100-бальною шкалою в систему оцінок за національною шкалою здійснюється згідно з "Положенням про систему поточного і підсумкового контролю, оцінювання знань та визначення рейтингу здобувачів освіти". Ознайомитись з документом можна за покликанням.

2) щодо оскарження результатів контрольних заходів

Здобувачі вищої освіти мають право на оскарження оцінки з дисципліни отриманої під час контрольних заходів. Апеляція здійснюється відповідно до «Положення про політику та врегулювання конфліктних ситуацій». Ознайомитись з документом можна за покликанням.

3) щодо відпрацювання пропущених занять

Згідно "Положення про організацію освітнього процесу" здобувач допускається до семестрового контролю з конкретної навчальної дисципліни (семестрового екзамену, диференційованого заліку), якщо він виконав усі види робіт, передбачені на семестр навчальним планом та силабусом / робочою програмою навчальної дисципліни, підтвердив опанування на мінімальному рівні результатів навчання (отримав ≥35 бали), відпрацював визначені індивідуальним навчальним планом всі лекційні, практичні, семінарські та лабораторні заняття, на яких він був відсутній. Ознайомитись з документом можна за покликанням.

4) щодо дотримання академічної доброчесності

"Положення про академічну доброчесність" закріплює моральні принципи, норми та правила етичної поведінки, позитивного, сприятливого, доброчесного освітнього і наукового середовища, професійної діяльності та професійного спілкування спільноти Університету, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання. Ознайомитись з документом можна за покликанням.

5) щодо використання штучного інтелекту

"Положення про академічну доброчесність" визначає політику щодо використання технічних засобів на основі штучного інтелекту в освітньому процесі. Ознайомитись з документом можна за покликанням.
"Положення про систему запобігання та виявлення академічного плагіату, самоплагіату, фабрикації та фальсифікації академічних творів" містить рекомендації щодо використання в академічних текстах генераторів на основі штучного інтелекту. Ознайомитись з документом можна за покликанням.

6) щодо використання технічних засобів в аудиторії та правила комунікації

Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та практичних занять дозволяється виключно у навчальних цілях (для уточнення певних даних, перевірки правопису, отримання довідкової інформації тощо). На гаджетах повинен бути активований режим «без звуку» до початку заняття. Під час занять заборонено надсилання текстових повідомлень, прослуховування музики, перевірка електронної пошти, соціальних мереж тощо. Під час виконання заходів контролю використання гаджетів заборонено (за винятком, коли це передбачено умовами його проведення). У разі порушення цієї заборони результат анульовується без права перескладання.
Ознайомитись з відповідним документом можна за посиланням.
Комунікація відбувається через електронну пошту і сторінку дисципліни в Moodle.

7) щодо зарахування результатів навчання, здобутих шляхом формальної/інформальної освіти

Процедури визнання результатів навчання, здобутих шляхом формальної/інформальної освіти визначаються «Положенням про порядок визнання результатів навчання, здобутих шляхом неформальної та / або інформальної освіти». Ознайомитись з документом можна за покликанням.

МЕТОДИ НАВЧАННЯ

При вивченні дисципліни застосовується комплекс методів для організації навчання студентів з метою розвитку їх логічного та абстрактного мислення, творчих здібностей, підвищення мотивації до навчання та формування особистості майбутнього фахівця.

Програмний результат навчання	Метод навчання	Метод оцінювання
Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію до фахівців і нефахівців; зокрема, під час публічних виступів, дискусій, проведення занять.	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний методи, метод самостійної роботи вдома, робота під керівництвом викладача	іспит, поточний контроль, усний контроль, письмовий контроль, тестовий контроль
Узагальнювати практичні результати роботи і пропонувати нові рішення, з урахуванням цілей, обмежень, правових, соціальних, економічних та етичних аспектів.	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний методи, метод самостійної роботи вдома, робота під керівництвом викладача	іспит, поточний контроль, усний контроль, письмовий контроль, тестовий контроль
Аналізувати умови і причини вчинення правопорушень, визначати шляхи їх усунення.	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний	іспит, поточний контроль, усний контроль,

	методи, метод самостійної роботи вдома, робота під керівництвом викладача	письмовий контроль, тестовий контроль
Оцінювати та забезпечувати якість виконуваних робіт у процесі управління правоохоронним підрозділом в різних умовах обстановки, а також розробляти відповідні аналітичні та інформаційні матеріали, робити усні та письмові звіти та доповіді.	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний методи, метод самостійної роботи вдома, робота під керівництвом викладача	іспит, поточний контроль, усний контроль, письмовий контроль, тестовий контроль
Забезпечувати законність та правопорядок, захист прав та інтересів особистості, суспільства, держави з використанням ефективних методів й засобів забезпечення публічної безпеки і порядку в межах виконання своїх посадових обов'язків.	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний методи, метод самостійної роботи вдома, робота під керівництвом викладача	іспит, поточний контроль, усний контроль, письмовий контроль, тестовий контроль
Розробляти та кваліфіковано застосовувати нормативно-правові акти в різних сферах юридичної діяльності, реалізовувати норми матеріального й процесуального	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний методи, метод самостійної роботи вдома, робота під керівництвом викладача	іспит, поточний контроль, усний контроль, письмовий контроль, тестовий контроль

права в професійній діяльності.		
Надавати кваліфіковані юридичні висновки й консультації в конкретних сферах юридичної діяльності.	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний методи, метод самостійної роботи вдома, робота під керівництвом викладача	іспит, поточний контроль, усний контроль, письмовий контроль, тестовий контроль
Відшуковувати необхідну інформацію в спеціальній літературі, базах даних, інших джерелах інформації, аналізувати та об'єктивно оцінювати інформацію.	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний методи, метод самостійної роботи вдома, робота під керівництвом викладача	іспит, поточний контроль, усний контроль, письмовий контроль, тестовий контроль

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Вид контрольного заходу	***Зміст***	***% від загальної оцінки***	***Бал***	
			min	***max***
Поточні контрольні заходи	опитування, поточні контрольні роботи, практичні завдання, результати виконання індивідуальної роботи	**60**	**35**	**60**
Підсумкові контрольні заходи	екзамен	**40**	**24**	**40**
Усього:		**100**	**60**	**100**

Процедура проведення контрольних заходів, а саме поточного контролю знань протягом семестру та підсумкового семестрового контролю, регулюється Положенням про систему поточного та підсумкового контролю оцінювання знань та визначення рейтингу студентів.

Фіксація **поточного** контролю здійснюється в електронному журналі обліку успішності академічної групи на підставі чотирибальної шкали («2»; «3»; «4»; «5»). У разі відсутності студента на занятті виставляється «н». За результатами поточного контролю у Журналі, автоматично визначається підсумкова оцінка, здійснюється підрахунок пропущених занять.

Усі пропущені заняття, а також негативні оцінки здобувачі зобов'язані відпрацювати впродовж трьох наступних тижнів. У разі недотримання цієї норми, замість «н» у журналі виставляється «0» (нуль балів), без права перескладання. Відпрацьоване лекційне заняття в електронному журналі позначається літерою «в».

Порядок оцінювання. До **підсумкового** контролю допускаються студенти, які за результатами поточного контролю отримали не менше 35 балів. Усі студенти, що отримали 34 балів і менше, не допускаються до складання підсумкового контролю і на підставі укладання додаткового договору, здійснюють повторне вивчення дисципліни впродовж наступного навчального семестру. За результатами підсумкового контролю (екзамен) студент може отримати 40 балів. Студенти, які під час підсумкового контролю отримали 24 бали і менше, вважаються такими, що не здали екзамен / диференційований залік і повинні йти на перездачу.

Підсумковий (семестровий) контроль проводиться для встановлення рівня досягнення здобувачами освіти програмних результатів навчання з навчальної дисципліни (освітнього компонента), після завершення вивчення дисципліни.

Підсумковий контроль знань проводиться у формі захисту наскрізного проєкту. Наскрізний проєкт є обов'язковим елементом роботи студентів у межах вивчення дисципліни «Кібербезпека і управління інформаційними ресурсами».

Проєкт виконується поетапно: під час опрацювання кожної теми студенти розробляють окремі розділи політики кібербезпеки для обраної організації, установи, підприємства чи стартапу. У ході роботи студенти визначають інформаційні активи, ідентифікують кіберзагрози, аналізують уразливості, формують політики доступу, пропонують технічні та організаційні засоби захисту, а також описують процедури реагування на кіберінциденти.

Підсумковим результатом є презентація політики кібербезпеки об'єкта дослідження, що відображає знання та навички, набуті упродовж курсу.

Форма підсумкового контролю - захист наскрізного проєкту.

Студенти презентують результати роботи, аргументують обрані рішення, демонструють практичні навички оцінювання ризиків та планування заходів інформаційної кібербезпеки. Оцінювання здійснюється за критеріями:

- повнота та логічність представлення матеріалу (10 балів);
- обґрунтованість запропонованих заходів (10 балів);
- врахування правових та етичних аспектів (10 балів);

- уміння відповідати на запитання та захищати власні висновки (10 балів).

Таким чином, наскрізний проєкт поєднує всі теми ОК та виступає інтегрованим підсумковим завданням.

Загальна семестрова оцінка з дисципліни, яка виставляється в екзаменаційних відомостях оцінюється в балах (згідно зі Шкалою оцінювання знань за ЄКТС) і є сумою балів отриманих під час поточного та підсумкового контролю.

Шкала оцінювання знань за ЄКТС

Оцінка за національною шкалою	**Рівень досягнень, %**	**Шкала ECTS**
Національна диференційована шкала		
Відмінно	90 – 100	A
Добре	83 – 89	B
	75 – 82	C
Задовільно	67 – 74	D
	60 – 66	E
Незадовільно	35 – 59	FX
	0 – 34	F
Національна недиференційована шкала		
Зараховано	60 – 100	-
Не зараховано	0 – 59	-

Студенти, які не з’явилися на заліки / екзамени без поважних причин, вважаються такими, що одержали незадовільну оцінку.

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основні джерела

1. Бурячок В. Л., Киричок Р. В., Складанний П. М. Основи інформаційної та кібернетичної безпеки: навч. посібник. – Київ: Київ. ун-т ім. Б. Грінченка, 2019. – 320 с. Доступ: https://elibrary.kubg.edu.ua/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf
2. Бурячок В.Л., Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки, підручник, - К.; ПВП «Задруга», 2014. - 222 с
3. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібер-оборони: підручник. – 2-ге вид., перероб. і доп. – Одеса: ОНАЗ ім. О. С. Попова, 2019. – 320 с.
4. Інформаційна безпека та кібербезпека держави [Текст] : навчальний посібник / Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська ; під заг. ред. Н. М. Титова. – Київ : Ліра-К, 2024. – 224 с.
5. Лісовська, Ю. П. Кібербезпека: ризики та заходи [Текст] : навчальний посібник / Ю. П. Лісовська. – Київ : Кондор, 2021. – 268 с.
6. Основи кіберпростору, кібербезпеки та кіберзахисту [Текст] : навчальний посібник / [автори: В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін]. -Київ : Ліра-К, 2022. - 553 с.
7. Сілін Є.С., Кадубовський О.А. Основи кібербезпеки : навчальний посібник [електронний ресурс]. Дніпро, 2023. – 200 с.Доступ: https://ddpu.edu.ua/fmk/publications/manuals/manual_18.pdf
8. Технології захисту інформації [Текст] : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король ; під заг. ред. С. Е. Остапова. – Київ : Новий світ-2000, 2020. – 500 с.
9. Користін О.Є., Швець Д.В., Бутко Б.О. та ін. Реалізація філософії “Intelligence-Led Policing” в системі кримінального аналізу Національної поліції України: монографія / за заг. ред. О.Є. Користіна. – Київ: BAITE, 2024. – 444 с. – ISBN 978-966-2310-66-5. – DOI: 10.36486/978-966-2310-66-5. – URL: https://vaite.kiev.ua/doi/ilp/INTELLIGENCE-LED_POLICING_sfs.pdf (дата звернення: 22.09.2025).

Додаткова література

1. Перлрос, Н. Ось таким, як мені кажуть, буде кінець світу: перегони кіберозброєнь [Текст]: [монографія] / Н. Перлрос – Харків : Фоліо, 2024. – 576с.

2. Ромашко, І. Правила з кібербезпеки [Текст] / І. Ромашко // Управління освітою. – 2020. – № 2, лютий. - С. 50-56.
3. Когут, Ю. Кібервійна та безпека об’єктів критичної інфраструктури [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2021. – 332с.
4. Когут, Ю. Кібервійни, кібертероризм, кіберзлочинність. Концепції, стратегії, технології [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2022. – 284с.
5. Когут, Ю. Кібертероризм. Історія, цілі, об’єкти [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2021. – 304с.
6. Когут, Ю. Цифрова трансформація економіки та проблеми кібербезпеки [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2021. – 368с.
7. Когут, Ю. Штучний інтелект і безпека [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2024. – 294с.
8. Ланде, Д. OSINT у кібербезпеці [Текст] : навчальний посібник / Д. Ланде – Київ : ТОВ «Інжиніринг», 2024. – 552с.
9. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ – Київ : Видавництво НА СБ України, 2020. 256 с.
10. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. – Київ: НІСД, 2014. – 328 с.
11. Іванюк, К. Обережність та обачність [Текст] : соціалізація і кіберсоціалізація підлітків як соціально-педагогічне явище / К. Іванюк // Соціальний педагог. – 2020. – № 6, червень. – С. 10-15.
12. Богуш В.М., Довидьков О.А. Проектування захищених комп’ютерних систем та мереж, навчальний посібник, -К.; ДУІКТ, 2008. – 500 с.
13. Бугайчук, А. Кіберсоціалізація [Текст] : життя в новій віртуальній реальності / А. Бугайчук // Управління освітою. – 2020. – № 2, лютий. – С. 24-44.
14. Alam, Shahid. Cybersecurity: Past, Present and Future. – arXiv preprint, 2022. https://arxiv.org/abs/2207.01227
15. Cyber Security. Simply. Make it Happen. : Monograph / edit. Abolhassan. – Springer International Publishing, 2017. – ISBN 978- 3-319-46528-9 (print) ; 978-3-319-46529-6 (online). 127 p.
16. Cyber-Physical Security : Monograph / edit. Clark. – Springer International Publishing, 2017. – ISBN 978-3-319-32822-5 (print) ; 978-3-319-32824-9 (online). 299 p.
17. Enterprise Security : Monograph / edit. Chang. – Springer International Publishing, 2017. – ISBN 978-3-319-54379-6 (print) ; 978-3-319-54380-2 (online). 277 p.

18. Mashima, D., Chen, Y., Roomi, M. M., Lakshminarayana, S., Chen, D. Cybersecurity for Modern Smart Grid against Emerging Threats. – arXiv monograph, 2024. https://arxiv.org/abs/2404.04466

19. Pavlovic, D., Seidel, P.-M. Security Science (SecSci), Basic Concepts and Mathematical Foundations. – Open-access lecture notes/textbook (Oxford, Royal Holloway, Hawaii), 2025. https://arxiv.org/abs/2504.16617v1

Електронні інформаційні ресурси

1. Офіційний веб-сайт Президента України – http://www.president.gov.ua.
2. Офіційний веб-сайт Верховної Ради України – http://www.portal.rada.gov.ua.
3. Офіційний веб-сайт Кабінету Міністрів України – http://www.kmu.gov.ua.
4. Офіційний веб-сайт Міністерства внутрішніх справ України – http://www.mvs.gov.ua.
5. Офіційний веб-сайт Офісу Генерального прокурора – http://www.gp.gov.ua.
6. Офіційний веб-сайт Міністерства юстиції України – http://www.minjust.gov.ua.
7. Єдиний реєстр судових рішень в Україні – http://www.reyestr.court.gov.ua.
8. Національна бібліотека України ім. В. І. Вернадського – http://www.nbuv.gov.ua.
9. Національна парламентська бібліотека України – http://www.catalogue.nplu.org.
10. Журнал "Кібербезпека", аналітичний дайджест — щомісячне видання від НАН України та НБУВ, охоплює актуальні погляди й новини сфери. https://ippi.org.ua/kiberbezpeka-v-informatsiinomu-suspilstvi
11. CERT-UA, офіційний сайт Державного центру кібербезпеки України (CERT-UA) — нормативна база, кейси реагування, аналітика. https://cert.gov.ua/
12. Journal of Cybersecurity (Oxford University Press) — відкритий академічний журнал із міждисциплінарним підходом до кібербезпеки. https://academic.oup.com/cybersecurity/issue?login=false