МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»

Інститут комп’ютерних систем
Кафедра комп’ютеризовані системи та програмні технології

Бобок І.І.

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ПРАКТИЧНИХ ЗАНЯТЬ

з дисципліни
«МІЖНАРОДНА СТАНДАРТИЗАЦІЯ СФЕРИ БЕЗПЕКИ ОБ’ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ»
(9 семестр)
для здобувачів освітньо-кваліфікаційного рівня «Магістр»
за спеціальністю F5 Кібербезпека та захист інформації

Одеса – 2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»

Інститут комп'ютерних систем
Кафедра комп'ютеризовані системи та програмні технології

Бобок І.І.

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ПРАКТИЧНИХ ЗАНЯТЬ

з дисципліни
«МІЖНАРОДНА СТАНДАРТИЗАЦІЯ СФЕРИ БЕЗПЕКИ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ»
(9 семестр)
для здобувачів освітньо-кваліфікаційного рівня «Магістр»
за спеціальністю F5 Кібербезпека та захист інформації

Затверджено
на засіданні кафедри
комп'ютеризовані системи та
програмні технології
Протокол №__ від _____

Одеса – 2026

Методичні рекомендації до практичних занять з дисципліни «Міжнародна стандартизація сфери безпеки об’єктів інформаційної діяльності» (9 семестр) для здобувачів освітньо-кваліфікаційного рівня «Магістр» за спеціальністю F5 Кібербезпека та захист інформації / Укл.: І.І. Бобок. — Одеса: Національний університет «Одеська політехніка», 2026. — 66 с.

Укладач: Бобок І.І., д.т.н., професор

ЗМІСТ

АНОТАЦІЯ

Предметом вивчення дисципліни «Міжнародна стандартизація сфери безпеки об’єктів інформаційної діяльності» є методології, процеси та архітектурні рішення управління корпоративною інформаційною безпекою, а також механізми забезпечення технічного та правового комплаєнсу (відповідності) IT-інфраструктури міжнародним галузевим стандартам (NIST CSF, PCI DSS, SOC 2) і нормативним вимогам щодо захисту даних (GDPR).

Метою дисципліни є формування методологічного фундаменту для дослідження нормативного поля кібербезпеки як об'єкта наукового аналізу; набуття навичок не лише інтеграції і застосування міжнародних стандартів (ISO, NIST), а й критичного оцінювання їхньої ефективності, проведення порівняльних досліджень архітектур та розробки моделей оцінки відповідності вимогам захисту в умовах динамічних загроз. Дисципліна спрямована на розвиток спроможності до формалізації вимог безпеки та розробки алгоритмів автоматизованого комплаєнс-моніторингу з метою подальшого проведення системного аналізу регуляторних актів та розробки концептуальних пропозицій щодо адаптації та вдосконалення архітектур захисту інформації на національному та корпоративному рівнях.

Основними завданнями вивчення дисципліни є:

— Засвоєння теоретико-методологічних основ міжнародної стандартизації та нормативно-правового регулювання у сфері кібербезпеки;
— Формування системного розуміння архітектури сучасних безпекових та приватнісних фреймворків (NIST CSF, GDPR, PCI DSS, SOC 2);
— Набуття практичних навичок оцінювання зрілості систем кібербезпеки організацій та побудови цільових профілів захисту;
— Опанування методів інвентаризації, класифікації та картування потоків персональних даних відповідно до європейських вимог;
— Вивчення алгоритмів проведення технічного комплаєнс-аудиту, визначення меж перевірки та методології збору цифрових доказів;

— Розвиток спроможності до критичного аналізу регуляторних ризиків та розробки компенсаційних контролів у складних та гетерогенних IT-інфраструктурах;
— Навчання принципам автоматизації комплаєнс-моніторингу для безперервного контролю стану безпеки об'єктів.

Програмні результати навчання:

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.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

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.

МІСЦЕ ПРАКТИЧНИХ ЗАНЯТЬ В ПРОЦЕСІ ВИВЧЕННЯ ДИСЦИПЛІНИ

Практичне заняття в межах дисципліни «Міжнародна стандартизація сфери безпеки об’єктів інформаційної діяльності» є формою науково-орієнтованої навчальної роботи, що передбачає аналітичне опрацювання нормативних вимог, розв'язання прикладних ситуативних завдань (кейсів) та фахову дискусію.

Головною *метою* практичних занять є забезпечення глибокого та всебічного аналізу фундаментальних проблем курсу, формування у здобувачів вищої освіти системного мислення та навичок імплементації міжнародних стандартів у реальні процеси захисту інформації. Практикуми спрямовані на трансформацію теоретичних знань в управлінські та аналітичні компетенції, необхідні для подальшої науково-дослідної або експертної діяльності.

Залежно від специфіки теми, практичні заняття можуть проводитися у наступних *формах*:

— Захисту індивідуальних дослідницьких доповідей;

— Інтерактивних наукових дискусій та круглих столів;

— Моделювання процесів комплаєнс-аудиту;

— Розв'язання комплексних правових та технічних кейсів.

Заняття розпочинається вступним словом викладача (модератора), який концептуалізує проблематику теми, визначає фокус дискусії та методологію роботи.

Для забезпечення високого академічного рівня дискусії здобувач має попередньо опрацювати лекційний матеріал, першоджерела (тексти стандартів, директив, законодавчих актів) та рекомендовані наукові публікації. Під час самостійної роботи з джерелами здобувачам рекомендується формувати структуровані аналітичні виписки (конспекти, опорні тези) для аргументації своєї позиції під час виступу.

Активна участь у практичних заняттях формує навички ведення наукової полеміки. Здобувачі здійснюють критичну оцінку виступів колег, формулюють уточнюючі запитання, виявляють методологічні неточності та

пропонують альтернативні шляхи розв'язання проблем. Такий формат дозволяє кожному учаснику подолати прогалини в знаннях через синергію колективного обговорення та навчитися аргументовано відстоювати власні архітектурні чи управлінські рішення.

Окремий акцент робиться на розв'язанні ситуативних правових та нормативно-технічних задач з обраної тематики. Здобувачі самостійно, спираючись на чинне законодавство та глобальні фреймворки, генерують рішення та презентують їх аудиторії, після чого відбувається процес експертного рецензування (peer-review) з боку групи.

Під час доповідей викладач здійснює модерацію процесу: спрямовує обговорення на розкриття ключових питань, оптимізує використання часу (зокрема, корегуючи вектор виступу у разі суттєвих відхилень від теми) та залучає до активності всіх присутніх. Заняття завершується підсумковим резюме викладача, в якому верифікуються результати роботи, надається оцінка змістовності виступів та формулюються висновки щодо рівня розкриття винесеної на розгляд науково-практичної проблеми.

ПРАКТИЧНЕ ЗАНЯТТЯ 1: GAP-АНАЛІЗ СТАНУ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Мета заняття: опанування методологією порівняльного аналізу стану безпеки організації з вимогами стандарту для ідентифікації та формалізації критичних невідповідностей.

Суть теми полягає у дослідженні методології Gap-аналізу (аналізу розривів) як фундаментального аналітичного інструменту аудиту та стратегічного планування кібербезпеки. В межах заняття розглядається процес системного співставлення поточної архітектури безпеки та бізнес-процесів організації (стан «As-Is») з еталонними нормативними вимогами обраного стандарту (стан «To-Be» — наприклад, ISO/IEC 27001 або NIST CSF).

Здобувачі вивчають алгоритми збору аудиторських доказів, ідентифікації відсутності або неефективності захисних контролів, а також методи ранжування виявлених «розривів» за рівнем критичності. Акцент робиться на тому, що Gap-аналіз є не просто констатацією недоліків, а обґрунтованою базою для розробки стратегії розвитку інформаційної безпеки та оптимізації інвестицій у захист інфраструктури.

Очікувані результати опрацювання теми. Після успішного завершення цього практичного заняття здобувач:

Знає:

— методологічні принципи та етапи проведення первинного комплаєнс-аудиту;

— критерії оцінки зрілості процесів інформаційної безпеки;

— структуру та логіку побудови міжнародних стандартів ISO/IEC 27001 і NIST CSF як еталонних фреймворків для порівняльного аналізу.

Вміє:

— проводити декомпозицію вимог міжнародних стандартів на конкретні індикатори перевірки;

— здійснювати мапінг (mapping) існуючих організаційно-технічних заходів безпеки з нормативними вимогами;
— ідентифікувати та класифікувати невідповідності (Minor, Major, Observation) згідно з аудиторською практикою.

Володіє навичками:

— формалізації результатів дослідження у вигляді структурованої Матриці невідповідностей (Gap Analysis Matrix);
— розробки та обґрунтування Дорожньої карти усунення недоліків (Remediation Roadmap) з урахуванням пріоритезації ризиків та ресурсних обмежень організації.

Питання для обговорення:

1. Співвідношення Gap-аналізу та процедури оцінки ризиків при побудові системи управління інформаційною безпекою (СУІБ).
2. Значення формалізованих стандартів як еталону для Gap-аналізу та недоліки використання неформалізованих «кращих практик».
3. Класифікація невідповідностей: розмежування відсутності механізмів захисту (Design Gap) та їх неефективності (Effectiveness Gap).
4. Проблематика кількісного вимірювання комплаєнсу та межі застосування лінійних відсоткових показників за результатами Gap-аналізу.
5. Методи мінімізації суб'єктивного фактору аудитора під час збору доказів та оцінки організаційних процесів безпеки.
6. Принципи пріоритезації виявлених розривів та розробка дорожньої карти їх усунення (Remediation Roadmap) в умовах дефіциту ресурсів.
7. Особливості проведення Gap-аналізу в хмарних середовищах та розподіл зон відповідальності з IaaS/PaaS провайдером.
8. Етико-правовий алгоритм дій фахівця при виявленні критичних порушень законодавства під час проведення внутрішньої перевірки.
9. Трансформація традиційного Gap-аналізу в архітектуру безперервного комплаєнс-моніторингу (Continuous Compliance) на базі GRC-систем.

10. Специфіка Gap-аналізу для об'єктів критичної інфраструктури України з урахуванням національного регулювання та вимог євроінтеграції (NIS2).

Практичні завдання:

Завдання 1 (теоретико-аналітичне): Порівняльний аналіз методологічних підходів до Gap-аналізу.

Здобувачам пропонується проаналізувати та порівняти підходи до проведення Gap-аналізу в межах двох фреймворків – ISO/IEC 27001 та NIST CSF. На основі опрацьованих першоджерел необхідно:

— визначити спільні та відмінні методологічні принципи проведення оцінки відповідності в кожному з фреймворків;

— обґрунтувати, який із підходів є більш придатним для застосування в організаціях критичної інформаційної інфраструктури України з урахуванням вимог чинного законодавства;

— сформулювати не менше трьох критеріїв вибору еталонного стандарту залежно від типу та масштабу організації.

Форма подання результатів – усна аргументована доповідь (5–7 хв.) з подальшим обговоренням у групі.

Завдання 2 (ситуаційне): Побудова Gap Analysis Matrix для модельної організації.

Здобувачам надається картка-легенда модельної організації (наприклад, регіональний банк або державний реєстр), що містить короткий опис її IT-інфраструктури, наявних заходів захисту та організаційних процедур. На основі вимог ISO/IEC 27001 (Annex A) необхідно:

— провести мапінг задокументованих заходів організації з відповідними контролями стандарту;

— ідентифікувати невідповідності та класифікувати їх за типом (Minor / Major / Observation);

— заповнити структуровану матрицю невідповідностей за наступними колонками: контроль стандарту, поточний стан, тип невідповідності,

рівень ризику, рекомендований захід усунення;

— визначити топ-3 критичні розриви та обґрунтувати пріоритетність їх усунення.

Форма подання результатів – заповнена матриця у табличному вигляді з усним захистом прийнятих рішень перед групою.

Домашнє завдання: Міні-кейс «Gap-аналіз політики автентифікації».

Здобувачам пропонується виступити в ролі аудитора та проаналізувати один конкретний бізнес-процес вигаданої компанії, заповнивши базову матрицю розривів.

Вхідні дані («As-Is»):

1. Ви аналізуєте український IT-стартап, де співробітники працюють віддалено. Під час інтерв'ю з системним адміністратором ви з'ясували поточний стан автентифікації:
2. Співробітники входять до корпоративної пошти та CRM-системи лише за логіном та паролем.
3. Мінімальна довжина пароля налаштована на 8 символів.
4. Система змушує змінювати пароль кожні 30 днів.

Еталонна вимога («To-Be» — на основі NIST SP 800-63B):

1. Для будь-якого віддаленого доступу до корпоративних ресурсів є обов'язковим використання багатофакторної автентифікації (MFA).
2. Мінімальна довжина пароля має становити щонайменше 12 символів (бажано 15+).
3. Слід відмовитися від примусової періодичної зміни паролів (якщо немає підозри на їх компрометацію), оскільки це змушує користувачів створювати слабкі паролі.

Безпосереднє завдання: на основі цих даних заповнити таблицю Gap-аналізу (навести 2-3 ключові розриви) та запропонувати базові кроки для їх усунення.

Матриця розривів

Процес / Контроль	**Поточний стан (As-Is)**	**Вимога стандарту (To-Be)**	**Опис розриву (Gap)**	**Рекомендації щодо усунення (Remediation)**
Віддалений доступ	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)
Політика паролів	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)

Рекомендована література:

1. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT)
2. ДСТУ EN ISO/IEC 27002:2024 Інформаційна безпека, кібербезпека та захист конфіденційності. Заходи забезпечення інформаційної безпеки (EN ISO/IEC 27002:2022, IDT; ISO/IEC 27002:2022, IDT)
3. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. URL: https://doi.org/10.6028/NIST.CSWP.29
4. Center for Internet Security. CIS Critical Security Controls Version 8.1. URL: https://www.cisecurity.org/controls/v8-1
5. Information Systems Audit and Control Association (ISACA). COBIT 2019 Framework. URL: https://www.isaca.org/resources/cobit
6. Закон України «Про основні засади забезпечення кібербезпеки України»
7. Постанова НБУ «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України»

ПРАКТИЧНЕ ЗАНЯТТЯ 2: ПОБУДОВА МАТЕМАТИЧНОЇ МОДЕЛІ ТА МАТРИЦІ ОЦІНКИ РИЗИКІВ

Мета заняття: сформувати навички математичного моделювання кіберризиків та побудови ієрархічних матриць загроз для обґрунтування вибору засобів захисту.

Суть теми полягає у переході від евристичних (якісних) методів оцінки ризиків до строгого математичного та стохастичного моделювання. Оскільки традиційні ієрархічні матриці загроз мають значні обмеження через суб'єктивізм та неможливість точного фінансового прогнозування, фокус зміщується на кількісні моделі (Quantitative Risk Analysis).

Під час заняття здобувачі вивчають параметризацію ризику через імовірнісні показники: очікувану частоту виникнення події ARO (Annualized Rate of Occurrence) та фінансовий еквівалент одиничних втрат SLE (Single Loss Expectancy). Головний акцент робиться на побудові математичних функцій, які описують вплив впроваджених механізмів контролю на зниження базової ймовірності успішної атаки. Розглядається алгоритм розрахунку метрики повернення інвестицій у безпеку ROSI (Return on Security Investment), що є критичною навичкою для перекладу технічних загроз на мову фінансово-математичних обґрунтувань.

Очікувані результати опрацювання теми. Після успішного завершення цього практичного заняття здобувачі вищої освіти повинні:

Знати:

— фундаментальні відмінності між якісними, напівкількісними та кількісними математичними моделями оцінки кіберризиків;

— базові принципи стохастичного моделювання загроз (зокрема, елементи методології FAIR – Factor Analysis of Information Risk);

— обмеження кількісних моделей та умови їх коректного застосування залежно від доступності вхідних даних та зрілості процесів безпеки

організації.

Вміти:

— виконувати математичний розрахунок базових показників: SLE, ARO та ALE за класичною формулою:

$$ALE = SLE \times ARO;$$

— розраховувати економічну ефективність засобів контролю та обґрунтовувати бюджет на інформаційну безпеку, використовуючи математичну модель ROSI.

Володіти навичками:

— побудови формалізованих розрахункових моделей для оцінки залишкового ризику;

— трансформації технічних вразливостей систем в об'єктивні фінансові показники потенційних збитків для захисту архітектурних рішень перед керівництвом.

Питання для обговорення:

1. Криза якісних методів оцінки: математичні та логічні обмеження традиційних ієрархічних матриць ризиків при стратегічному плануванні.
2. Параметризація кіберзагроз: методологія розрахунку та математичний зміст базових показників очікуваних втрат (SLE, ARO, ALE).
3. Моделювання економічної ефективності: алгоритм розрахунку метрики ROSI для фінансового обґрунтування бюджету на інформаційну безпеку.
4. Проблема невизначеності вхідних даних: застосування методів теорії ймовірностей (зокрема, симуляцій Монте-Карло) для прогнозування частоти та наслідків кіберінцидентів.
5. Стохастичне моделювання за методологією FAIR: декомпозиція факторів інформаційного ризику та перехід до ймовірнісних діапазонів замість точкових оцінок.
6. Кількісна оцінка вартості активів: математична формалізація прямих

фінансових збитків та непрямих (репутаційних, юридичних) втрат від реалізації загрози.

7. Математичне моделювання багаторівневого захисту (Defense-in-Depth): розрахунок сукупної ймовірності успішної атаки при послідовному подоланні кількох незалежних контурів безпеки.
8. Формалізація «апетиту до ризику» (Risk Appetite): переклад якісних бізнес-вимог у точні математичні порогові значення допустимого залишкового ризику.
9. Кіберстрахування як математична задача: використання моделей кількісної оцінки (Quantitative Risk Analysis) для розрахунку страхових премій та лімітів відповідальності при передачі ризику (Risk Transfer).
10. Системні вразливості кількісного підходу: межі застосовності математичних моделей в умовах непередбачуваних загроз (Zero-day вразливості та концепція «Чорних лебедів»).

Практичні завдання:

Завдання 1 (теоретико-аналітичне): Порівняльний аналіз методологічних обмежень якісних та кількісних моделей оцінки кіберризиків.

Здобувачам пропонується здійснити критичний аналіз епістемологічних обмежень традиційних матричних підходів до оцінки ризиків (Heat Map, 5×5 Risk Matrix) та обґрунтувати методологічну перевагу кількісних моделей в контексті прийняття управлінських рішень. На основі опрацьованих першоджерел необхідно:

— виявити та систематизувати не менше чотирьох фундаментальних методологічних вад якісних матриць ризиків;
— обґрунтувати умови, за яких застосування методології FAIR є виправданим, а за яких – надмірно ресурсозатратним або неможливим через відсутність достатньої статистичної бази;
— сформулювати авторську позицію щодо оптимальної гібридної моделі оцінки ризиків для організацій із різним рівнем зрілості процесів

інформаційної безпеки (відповідно до шкали CMM[1]).

Форма подання результатів – аргументована доповідь (7–10 хвилин) з обов'язковим посиланням на першоджерела та подальшою дискусією у форматі «запитання → контраргумент → відповідь».

Завдання 2 (ситуаційне): Фінансове обґрунтування бюджету на кібербезпеку для модельної організації.

Здобувачам надається картка-легенда організації з наступними параметрами:

Регіональна логістична компанія. IT-інфраструктура: 3 сервери, 120 робочих станцій, ERP-система, зовнішній веб-портал. Відсутній WAF, антивірусне ПЗ застаріле (оновлення — раз на квартал), резервне копіювання — щотижневе. За останні 2 роки зафіксовано 1 успішну атаку типу ransomware зі збитками 180000 грн.

На основі наданих даних необхідно:

— розрахувати показники SLE, ARO та ALE для двох сценаріїв загроз – атаки ransomware та витоку персональних даних клієнтів – з обґрунтуванням прийнятих числових припущень;

— розрахувати ROSI для запропонованого комплексу засобів захисту (на вибір здобувача) та довести або спростувати економічну доцільність їх впровадження;

— підготувати коротке резюме для керівництва (*executive summary*) у форматі звернення до фінансового директора, в якому технічні показники перекладені мовою бізнес-ризиків та фінансових втрат.

Форма подання результатів – розрахункова таблиця з формулами, резюме для керівництва та усний захист із відповідями на запитання групи в режимі peer-review.

Домашнє завдання: Розробка повної кількісної моделі оцінки кіберризиків для реальної або модельної організації.

Здобувач самостійно обирає організацію для аналізу — реальну (з

[1] Capability Maturity Model — модель зрілості можливостей (модель повноти потенціалу) створення ПЗ: еволюційна модель розвитку здатності компанії розробляти програмне забезпечення.

відкритих джерел: річні звіти, публічні аудиторські висновки, новини про інциденти) або модельну, самостійно сконструйовану з обґрунтуванням її параметрів. На основі опрацьованого матеріалу необхідно виконати такі послідовні етапи:

Етап 1. Профілювання організації та загроз. Описати організацію: галузь, масштаб, критичні інформаційні активи, наявні заходи захисту. Ідентифікувати не менше трьох релевантних сценаріїв загроз з посиланням на актуальні джерела статистики кіберінцидентів (Verizon DBIR, ENISA Threat Landscape або аналогічні).

Етап 2. Кількісна оцінка ризиків. Для кожного сценарію загрози розрахувати SLE, ARO та ALE з детальним обґрунтуванням прийнятих числових значень. Джерела статистики та логіка припущень мають бути явно задокументовані – результати без обґрунтування не зараховуються.

Етап 3. Моделювання ефекту засобів контролю. Для найкритичнішого сценарію запропонувати комплекс технічних та організаційних заходів захисту, розрахувати скориговані показники залишкового ризику та обчислити ROSI для кожного запропонованого заходу окремо.

Етап 4. Аналітичний висновок. Підготувати структурований звіт (4–6 сторінок без урахування таблиць і додатків), який має містити: зведену таблицю розрахунків, критичну оцінку обмежень застосованої моделі та рекомендації щодо пріоритетності інвестицій у засоби захисту з урахуванням ресурсних обмежень організації.

Рекомендована література:

1. Hubbard D.W., Seiersen R. How to Measure Anything in Cybersecurity Risk (2nd Ed.). Wiley, 2023.
2. Freund J., Jones J. Measuring and Managing Information Risk: A FAIR Approach (2nd Ed.). Butterworth-Heinemann, 2025.
3. ДСТУ ISO/IEC 27005:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT)

4. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments.
5. Gordon L.A., Loeb M.P. The Economics of Information Security Investment. *ACM Transactions on Information and System Security*. 2002. 5. P. 438-457. https://doi.org/10.1145/581271.581274

ПРАКТИЧНЕ ЗАНЯТТЯ 3: ФОРМАЛІЗАЦІЯ ВИМОГ У ПОЛІТИКАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Мета заняття: опанування навичок трансформації високорівневих вимог стандартів у чітко структуровані внутрішні нормативні документи організації.

Суть теми полягає у вивченні методології побудови архітектури корпоративного управління інформаційною безпекою (Security Governance) через розробку ієрархічної системи внутрішніх нормативних документів. Здобувачі досліджують проблему розриву між абстрактними вимогами міжнародних стандартів (наприклад, вимогою ISO 27001 «необхідно керувати правами доступу») та їх практичною імплементацією в реальних бізнес-процесах організації.

Під час заняття розглядається класична багаторівнева модель документації: Політики (Policies) → Стандарти (Standards) → Процедури (Procedures) → Інструкції/Рекомендації (Guidelines). Головний акцент робиться на лінгвістичній та юридичній коректності формулювань: як уникати двозначностей, як визначати зону відповідальності (Roles and Responsibilities) та як забезпечити обов'язковість виконання норм (Enforceability). Окремо розглядається життєвий цикл політики: від ініціації та погодження з бізнес-підрозділами до комунікації персоналу та регулярного перегляду.

Очікувані результати опрацювання теми. Після успішного завершення цього практичного заняття здобувачі вищої освіти повинні:

Знати:

— структурну ієрархію внутрішньої нормативної бази системи управління інформаційною безпекою (СУІБ) та призначення кожного рівня документації;

— базові розділи комплексної політики безпеки (Purpose, Scope, Policy

Statements, Exceptions, Enforcement, Glossary) та вимоги до їх змісту;

— правові механізми легітимізації внутрішніх політик в межах українського трудового та господарського законодавства, зокрема вимоги щодо ознайомлення персоналу під розпис та встановлення відповідальності за порушення.

Вміти:

— здійснювати декомпозицію та трансформацію високорівневих контролів (наприклад, з Додатку А стандарту ISO/IEC 27001) у конкретні, зрозумілі для персоналу правила поведінки;

— розмежовувати директивні вимоги (що потрібно робити) від процедурних кроків (як саме це потрібно робити);

— адаптувати тональність та деталізацію документа залежно від цільової аудиторії (топ-менеджмент, IT-адміністратори, рядові користувачі);

— управляти життєвим циклом політики безпеки – від ініціації та погодження з бізнес-підрозділами до комунікації персоналу, моніторингу дотримання та регулярного перегляду документа.

Володіти навичками:

— проектування текстів внутрішніх політик (Drafting) із дотриманням принципів однозначності, вимірюваності та технологічної нейтральності;

— побудови матриці відповідальності (RACI) для процесів інформаційної безпеки, що закріплюються у нормативних документах організації.

Питання для обговорення:

1. Ієрархічна архітектура нормативної бази СУІБ: концептуальне та практичне розмежування функцій політик, стандартів, процедур та інструкцій.
2. Лінгвістичні принципи проектування політик: уникнення семантичної двозначності, використання імперативних конструкцій та дотримання принципу технологічної нейтральності.
3. Легітимізація політик безпеки в правовому полі України: механізми

синхронізації вимог інформаційної безпеки з трудовим законодавством та юридично правильна процедура ознайомлення персоналу.

4. Алгоритм декомпозиції міжнародних стандартів: перехід від високорівневих абстрактних контролів (на прикладі ISO/IEC 27001) до вимірюваних та однозначних внутрішніх корпоративних правил.
5. Процедура управління винятками (Policy Exceptions): формалізація процесу документування, компенсації ризиків та тимчасового затвердження легітимних відхилень від діючих політик.
6. Таргетування нормативної документації: адаптація рівня деталізації, термінології та тональності документів залежно від цільової аудиторії (топ-менеджмент, IT-підрозділи, нетехнічний персонал).
7. Інтеграція матриці RACI (Responsible, Accountable, Consulted, Informed): інструменти чіткого розмежування зон відповідальності для уникнення управлінського вакууму або дублювання функцій.
8. Життєвий цикл нормативного документа (Policy Lifecycle): етапи розробки, крос-функціонального погодження (з юристами, HR, бізнес-підрозділами), публікації, аудиту та регулярної актуалізації.
9. Проблема формалізму та «мертвих» політик: аналіз причин ігнорування нормативних вимог персоналом та організаційні методи трансформації політик у реальну корпоративну культуру (Security Awareness).
10. Формалізація санкційної політики: правове та організаційне закріплення дисциплінарної та матеріальної відповідальності працівників за порушення режиму інформаційної безпеки.

Практичні завдання:

Завдання 1 (теоретико-аналітичне): Критичний аналіз архітектурних моделей нормативної документації систем управління інформаційною безпекою.

Здобувачам пропонується здійснити порівняльний аналіз підходів до побудови ієрархії нормативної документації СУІБ у двох різних регуляторних контекстах – корпоративному (ISO/IEC 27001) та державному (вимоги НД ТЗІ

або галузеві стандарти критичної інфраструктури). На основі опрацьованих першоджерел необхідно:

— порівняти принципи структурування нормативної документації в обох контекстах: визначити, які рівні ієрархії є спільними, а які – унікальними для кожного підходу, та пояснити причини цих відмінностей;

— проаналізувати проблему «нормативного розриву» між рівнем Політики та рівнем Процедур: чому організації системно уникають деталізації на рівні процедур та які ризики це породжує з точки зору аудитора та з точки зору регулятора;

— сформулювати авторські критерії оцінки якості нормативного документа з інформаційної безпеки – не менше п'яти критеріїв з обґрунтуванням кожного та прикладами типових порушень.

Форма подання результатів – структурована доповідь (7–10 хв.) з обов'язковим посиланням на першоджерела. Після доповіді – дискусія у форматі «опонування»: двоє здобувачів з групи формулюють контраргументи, доповідач має їх спростувати або визнати та уточнити свою позицію.

Завдання 2 (ситуаційне): Розробка політики управління доступом для модельної організації.

Здобувачам надається картка-легенда організації з такими параметрами:

Державна установа – регіональне управління соціального захисту населення. Персонал: 85 осіб (керівництво, інспектори, архів, бухгалтерія, ІТ-відділ – 2 особи). ІТ-інфраструктура: локальна мережа, сервер бази даних з персональними даними громадян, веб-портал для подання заяв, хмарне сховище для архівних документів. Наявна документація: загальна інструкція з користування ПК (2017 р.), застаріла. Жодної чинної політики управління доступом немає. Нещодавно зафіксовано інцидент: звільнений співробітник протягом двох тижнів після звільнення зберігав активний доступ до бази даних.

На основі наданих даних необхідно:

— розробити повноцінний текст «Політики управління логічним доступом» відповідно до структури: Purpose → Scope → Policy Statements → Roles and Responsibilities → Exceptions → Enforcement → Review Schedule → Glossary;
— забезпечити відповідність документа вимогам контролю ISO/IEC 27001 (Annex A, розділи щодо управління доступом) та нормам законодавства України про захист персональних даних;
— побудувати матрицю RACI для процесу управління обліковими записами (створення, модифікація, блокування, видалення) із зазначенням конкретних посад організації;
— передбачити в тексті політики окремий розділ, що унеможливлює повторення зафіксованого інциденту, із зазначенням конкретних термінів і відповідальних осіб.

Форма подання результатів – повний текст розробленої політики (3–5 сторінок) та матриця RACI з усним захистом і рецензуванням у форматі peer-review.

Домашнє завдання: Міні-кейс «Аудит та рефакторинг Політики "Чистого столу та екрана"».

Здобувачам пропонується виступити в ролі аудитора з інформаційної безпеки, якому на рецензію потрапив фрагмент внутрішнього нормативного документа. Текст містить типові логічні, технічні та юридичні помилки, які роблять його нежиттєздатним.

Вхідні дані (фрагмент «поганої» політики):

«…Працівники повинні по можливості не залишати важливі документи на робочих столах, коли йдуть додому. Якщо ви відходите від комп'ютера на обід або покурити, екран треба вимкнути кнопкою на моніторі. Флешки, дискети та папірці з паролями краще ховати в шухляду. Системний адміністратор слідкує за цим і має право самостійно оштрафувати порушника на 1000 гривень».

Безпосереднє завдання:

1. Аудит (Ідентифікація недоліків): знайти у тексті та класифікувати мінімум 4 критичні помилки. Помилки слід шукати у трьох площинах:
   — лінгвістична / логічна: наявність розмитих формулювань (неоднозначність);
   — технічна: технологічна застарілість або неефективність описаного контролю;
   — юридична / організаційна: невідповідність трудовому законодавству України або неправильний розподіл ролей.
2. Рефакторинг (Переписування): спираючись на вимоги стандарту ISO/IEC 27001 (контроль щодо чистого столу та чистого екрана), переписати цей фрагмент академічною та імперативною мовою, прибравши всі знайдені недоліки.

Рекомендована література:

1. Peltier T.R. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Auerbach Publications, 2001.
2. Wood C.C. Information Security Policies Made Easy. Information Shield, 2008.
3. Johnson R. Security Policies and Implementation Issues (3rd Ed.). Jones & Bartlett Learning, 2022.

ПРАКТИЧНЕ ЗАНЯТТЯ 4: СТРАТЕГІЧНЕ ПРОФІЛЮВАННЯ ЗА NIST CYBERSECURITY FRAMEWORK

Мета заняття: сформувати навички стратегічного профілювання кібербезпеки організації на основі методології NIST CSF 2.0 та розробки пріоритезованого плану дій для досягнення цільового рівня кіберстійкості.

Суть теми полягає у вивченні NIST Cybersecurity Framework (CSF) не просто як технічного стандарту, а як високорівневого інструменту стратегічного менеджменту (Security Governance). Здобувачі досліджують три ключові компоненти фреймворку: Ядро (Core), Рівні впровадження (Tiers) та Профілі (Profiles). Особлива увага приділяється шістьом фундаментальним функціям Ядра: Govern (Керування), Identify (Ідентифікація), Protect (Захист), Detect (Виявлення), Respond (Реагування) та Recover (Відновлення).

Практична складова заняття сфокусована на методології профілювання. Здобувачі опановують методологію розробки «Поточного профілю» (Current Profile), який відображає реальний стан архітектури безпеки та рівень зрілості процесів організації на основі рівнів впровадження (Tiers 1–4). Наступним кроком є проектування «Цільового профілю» (Target Profile), який враховує унікальний ландшафт загроз, бізнес-цілі та прийнятний рівень ризику конкретного підприємства. Порівняння цих профілів дозволяє здобувачам сформувати об'єктивний, пріоритезований план дій для досягнення необхідного рівня кіберстійкості (Cyber Resilience).

Очікувані результати опрацювання теми. Після успішного завершення цього практичного заняття здобувачі вищої освіти повинні:

Знати:

— архітектурну структуру фреймворку NIST CSF 2.0 – зміст його функцій, категорій та підкатегорій – та логіку їх взаємозв'язку в системі управління кібербезпекою;

— критерії визначення та характеристики рівнів впровадження (Implementation Tiers) від часткового (Tier 1) до адаптивного (Tier 4) як індикаторів зрілості процесів кібербезпеки;
— призначення та відмінності між Поточним і Цільовим профілями кібербезпеки як інструментами стратегічного планування та комунікації з керівництвом організації.

Вміти:

— проводити декомпозицію бізнес-стратегії організації для визначення вимог до її цільового стану кібербезпеки;
— оцінювати поточний стан процесів безпеки організації та відносити їх до відповідних рівнів зрілості (Tiers) з обґрунтуванням прийнятих рішень;
— визначати пріоритети та послідовність кроків для ліквідації розривів між поточним та цільовим профілями з урахуванням ресурсних обмежень організації.

Володіти навичками:

— побудови інтегральних стратегічних профілів безпеки організації за методологією NIST CSF 2.0 з відображенням поточного та цільового стану за кожною функцією Ядра;
— розробки стратегічного плану дій (Action Plan / Transition Roadmap) для топ-менеджменту, що транслює технічні завдання кіберзахисту мовою бізнес-метрик та стратегічного розвитку організації.

Питання для обговорення:

1. NIST CSF як місток між IT та топ-менеджментом: чому цей фреймворк є найкращим інструментом для перекладу технічних загроз на зрозумілу для ради директорів мову бізнесу.
2. Еволюція стандарту та нова функція «Govern» (Керування): аналіз змін у NIST CSF 2.0 та причини, чому корпоративне управління тепер поставлене в самий центр архітектури безпеки.
3. Пастка максимального рівня (Tiers): чому досягнення 4-го рівня

зрілості (Adaptive) не завжди є фінансово виправданим і як визначити «достатній» рівень для конкретної компанії.

4. Практика побудови профілів (Profiles): алгоритм переходу від поточного стану (As-Is) до цільового (To-Be) без надмірної бюрократії та створення «документів заради документів».
5. NIST CSF для малого та середнього бізнесу (SMB): розвінчання міфу про те, що стандарт підходить лише для корпорацій, та методи його адаптації для стартапів з обмеженим бюджетом.
6. Кібербезпека ланцюга постачання (Supply Chain): використання фреймворку для оцінки надійності підрядників, хмарних провайдерів та партнерів.
7. Синергія фреймворків: як на практиці інтегрувати високорівневу стратегію NIST CSF з конкретними технічними вимогами ISO 27001 або CIS Controls.
8. Пріоритезація бюджету за допомогою профілювання: як результати Gap-аналізу між поточним та цільовим профілями допомагають обґрунтувати план закупівель перед фінансовим директором (CFO).
9. Профілювання в умовах геополітичних криз та воєнного стану: як адаптувати цільовий профіль організації (Target Profile) до вимог підвищеної стійкості (Cyber Resilience) та захисту від цілеспрямованих атак спонсорованих державою хакерів (APT-угруповань).
10. Штучний інтелект у функціях «Detect» та «Respond»: як поява генеративного ШІ змінює вимоги до сучасного профілю безпеки організації та які нові категорії контролів необхідно впроваджувати для моніторингу використання AI-інструментів працівниками.

Практичні завдання:

Завдання 1 (теоретико-аналітичне): Критичний аналіз еволюції NIST CSF: від версії 1.1 до 2.0 в контексті сучасного ландшафту кіберзагроз.

Здобувачам пропонується здійснити порівняльний аналіз концептуальних змін, внесених у NIST CSF 2.0 порівняно з версією 1.1, та

оцінити їх практичну значущість для організацій різних секторів. На основі опрацьованих першоджерел необхідно:

— проаналізувати додавання функції Govern як шостої функції Ядра: обґрунтувати, чому саме питання управління (governance) було виокремлено в самостійну функцію, які прогалини попередньої версії це усуває та які нові вимоги це ставить перед організаціями на рівні топ-менеджменту;
— порівняти концепцію Implementation Tiers у версіях 1.1 та 2.0: чи змінилася їх роль та як це впливає на методологію побудови профілів;
— сформулювати авторську позицію щодо придатності NIST CSF 2.0 для застосування українськими організаціями критичної інфраструктури з урахуванням специфіки воєнного стану, вимог законодавства про захист критичної інфраструктури та реального ландшафту кіберзагроз з боку державних акторів.

Форма подання результатів – структурована доповідь (7–10 хв.) з обов'язковим посиланням на офіційний текст NIST CSF 2.0 та супутні публікації NIST. Після доповіді – дискусія у форматі «опонування»: двоє здобувачів формулюють контраргументи або уточнюючі запитання, доповідач має їх спростувати або визнати та скоригувати свою позицію.

Завдання 2 (ситуаційне): Розробка Поточного та Цільового профілів кібербезпеки для модельної організації.

Здобувачам надається картка-легенда організації з такими параметрами:

Обласна лікарня швидкої медичної допомоги. Персонал: 650 осіб. IT-інфраструктура: медична інформаційна система (MIC) з базою даних пацієнтів, підключена до національного реєстру eHealth; мережа медичного обладнання з частковою цифровою інтеграцією (IoMT); адміністративна мережа; зовнішній портал для запису пацієнтів. IT-відділ: 4 особи, окремої функції кібербезпеки немає. Інцидентів за останні 3 роки: дві успішні фішингові атаки з компрометацією облікових записів адміністративного персоналу, одна спроба несанкціонованого доступу до MIC (відбита). Бюджет

на кібербезпеку: не виділений окремим рядком.

На основі наданих даних необхідно:

— побудувати Поточний профіль організації за всіма шістьма функціями NIST CSF 2.0 із присвоєнням рівня зрілості для кожної функції та детальним обґрунтуванням кожної оцінки на основі параметрів картки-легенди;

— визначити Цільовий профіль з урахуванням специфіки організації як суб'єкта критичної інфраструктури у сфері охорони здоров'я, вимог законодавства про захист персональних даних та медичної таємниці, а також реального ландшафту загроз для медичного сектору;

— ідентифікувати топ-3 критичні розриви між профілями та розробити для кожного з них конкретний, пріоритезований захід усунення з обґрунтуванням послідовності впровадження та орієнтовними ресурсними витратами;

— підготувати одну сторінку резюме для керівництва у форматі доповідної записки головному лікарю: без технічного жаргону, мовою операційних ризиків для діяльності лікарні та репутаційних наслідків для керівництва.

Форма подання результатів – зведена таблиця профілів, перелік пріоритезованих заходів та резюме для керівництва з усним захистом і рецензуванням у форматі peer-review.

Домашнє завдання: Міні-кейс «Розробка Цільового профілю та підготовка резюме для керівництва».

Здобувачам пропонується виступити в ролі незалежного консультанта з кібербезпеки, який проводить стратегічний аудит української логістичної компанії. Мета – розробити фрагмент Цільового профілю за NIST CSF 2.0 та написати стисле обґрунтування для генерального директора.

Вхідні дані: деяка логістична компанія має власний автопарк, склади та онлайн-систему трекінгу вантажів. Нещодавно компанія підписала контракт із великим європейським партнером, який вимагає високого рівня

кіберстійкості ланцюга постачань (Supply Chain). Ви провели інтерв'ю з IT-відділом та з'ясували поточний стан (As-Is) для двох ключових категорій:

— Інвентаризація активів (ID.AM): IT-відділ має таблицю в Excel з переліком серверів, але вона оновлюється вручну раз на півроку. Тіньове IT (Shadow IT) не контролюється.

— Управління ідентифікаційною інформацією та доступом (PR.AA): Парольна політика існує, але багатофакторна автентифікація (MFA) налаштована лише для адміністраторів. Рядові менеджери працюють віддалено зі звичайними паролями.

Безпосереднє завдання:

1. Профілювання: заповнити матрицю поточного (Current) та цільового (Target) профілю для двох вказаних категорій, визначивши їхній рівень зрілості (Tier) від 1 до 4.
2. План дій: сформулювати конкретні кроки для переходу від поточного стану до цільового.
3. Економічне / Стратегічне обґрунтування: написати резюме для керівництва обсягом до 5 речень, де мовою бізнесу пояснити, чому компанія повинна проінвестувати в усунення цих розривів.

Матриця профілювання

Функція та категорія NIST CSF 2.0	**Поточний стан (Current Profile)**	**Оцінка Tier**	**Цільовий стан (Target Profile)**	**Очікуваний Tier**	**План дій (Action Plan)**
IDENTIFY (ID) **Asset Management (ID.AM)**	(*описано в умові*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)
PROTECT (PR) **Identity Management, Authentication and Access Control (PR.AA)**	(*описано в умові*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)

Рекомендована література:

1. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. URL: https://doi.org/10.6028/NIST.CSWP.29
2. National Institute of Standards and Technology. NIST Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View. URL: https://doi.org/10.6028/NIST.SP.800-39
3. Sharp M.K., Lambros K. The CISO Evolution: Business Knowledge for Cybersecurity Executives. Wiley, 2022.
4. Arnold R. Cybersecurity: A Business Solution. An Executive Perspective on Managing Cyber Risk. Threat Sketch LLC, 2017.

ПРАКТИЧНЕ ЗАНЯТТЯ 5: КАРТУВАННЯ ДАНИХ (DATA MAPPING) ТА АНАЛІЗ КОНФІДЕНЦІЙНОСТІ (GDPR)

Мета заняття: засвоїти методологію інвентаризації та візуалізації потоків персональних даних в IT-інфраструктурі організації, а також опанувати інструментарій оцінки впливу на захист даних (DPIA) для забезпечення комплаєнсу з вимогами GDPR.

Суть теми полягає у розмежуванні та одночасній інтеграції концепцій «Кібербезпеки» (захист систем) та «Приватності» (захист прав суб'єктів даних). Головна парадигма заняття: організація не може захистити дані, якщо не знає, де саме вони зберігаються, як обробляються та куди передаються.

Основним практичним інструментом виступає Data Mapping – процес побудови карти потоків даних та створення Реєстру діяльності з обробки RoPA (Record of Processing Activities), що є прямою вимогою статті 30 GDPR. Здобувачі вивчають життєвий цикл персональних даних: від збору (через веб-форми, API, контрагентів) до зберігання, передачі третім особам (Data Processors) та безпечного знищення.

Окрема увага приділяється концепції *Privacy by Design and by Default* (вбудована конфіденційність). На практичних прикладах розглядається алгоритм проведення DPIA (Data Protection Impact Assessment) – оцінки впливу на конфіденційність при впровадженні нових технологій чи бізнес-процесів. Здобувачі набувають навичок трансформації абстрактних юридичних вимог європейського регламенту в конкретні технічні контроли: криптографічний захист, псевдонімізацію, анонімізацію та контроль доступу.

Очікувані результати опрацювання теми. Після успішного завершення цього практичного заняття здобувачі вищої освіти повинні:

Знати:

— ключові принципи GDPR (мінімізація даних, обмеження мети, точність, обмеження зберігання) та права суб'єктів даних, зокрема право на видалення (*right to erasure*);
— відмінності між ролями Data Controller (Контролер) та Data Processor (Обробник), їхні зони відповідальності та договірні зобов'язання між ними;
— юридичні та технічні тригери, які роблять проведення DPIA обов'язковим відповідно до статті 35 GDPR.

Вміти:

— ідентифікувати та класифікувати персональні дані (PII) та чутливі категорії даних (Sensitive Data) у складних інформаційних системах;
— заповнювати реєстр діяльності з обробки, фіксуючи мету обробки, категорії суб'єктів, терміни зберігання та транскордонні передачі даних;
— проводити базову оцінку DPIA для виявлення ризиків порушення конфіденційності та формулювання заходів їх мінімізації.

Володіти навичками:

— візуалізації та картування складних інформаційних потоків (Data Flow Diagrams) між внутрішніми базами даних та зовнішніми хмарними сервісами із зазначенням правових підстав обробки для кожного потоку;
— проектування архітектури IT-рішень з урахуванням принципів *Privacy by Design* – вибору методів маскування даних, хешування, шифрування баз даних та мінімізації обсягу зібраних даних;
— підготовки структурованої документації з питань захисту персональних даних – RoPA, звіту DPIA та внутрішніх повідомлень для керівництва – відповідно до вимог GDPR.

Питання для обговорення:

1. Тіньове IT (Shadow IT) як головна перешкода для Data Mapping: організаційні методи виявлення несанкціонованих хмарних сервісів, месенджерів та особистих пристроїв працівників, через які

відбувається неконтрольований потік персональних даних.

2. Ілюзія анонімізації та псевдонімізація в епоху Big Data: межі можливостей технічного знеособлення даних та сучасні ризики швидкої деанонімізації за допомогою алгоритмів машинного навчання.
3. Конфлікт «Права на забуття» (Right to be Forgotten) та резервного копіювання: архітектурні виклики та технічні компроміси при видаленні персональних даних клієнтів із незмінних бекапів, системних логів та розподілених баз даних.
4. Privacy by Design в умовах Agile-розробки: практичні кроки інтеграції вимог щодо вбудованої конфіденційності у швидкі спринти розробників (DevSecOps) без гальмування виходу продукту на ринок (Time-to-Market).
5. DPIA як захист бізнесу, а не бюрократія: критерії обов'язковості проведення оцінки впливу та її роль у мінімізації ризиків багатомільйонних штрафів від європейських регуляторів.
6. Реєстр діяльності з обробки як фундамент кібербезпеки: трансформація юридичної вимоги (ст. 30 GDPR) у зручну карту IT-активів, яка допомагає CISO налаштовувати системи захисту від витоків (DLP).
7. Пастка «Згоди» (Consent) та «Законний інтерес» (Legitimate Interest): як правильно обирати правові підстави для обробки даних (на прикладі маркетингової аналітики, трекінгу поведінки та файлів cookie), щоб не порушити архітектуру системи.
8. Розподіл відповідальності в Cloud-інфраструктурі: юридичне та технічне розмежування обов'язків із захисту даних між організацією-власником (Data Controller) та хмарним провайдером послуг (Data Processor).
9. Транскордонна передача даних та локалізація серверів: технічні вимоги та правові механізми (зокрема, *Standard Contractual Clauses*) легального зберігання та обробки персональних даних громадян ЄС на серверах в Україні.

10. Реагування на інциденти та правило «72 годин» (*Data Breach Notification*): організаційна готовність компанії оперативно виявити витік, класифікувати ризик для суб'єктів даних та подати звіт наглядовому органу (DPA) в умовах стресу.

Практичні завдання:

Завдання 1 (теоретико-аналітичне): Порівняльний аналіз правових режимів захисту персональних даних: GDPR та законодавство України.

Здобувачам пропонується здійснити системний порівняльний аналіз регуляторних підходів до захисту персональних даних в ЄС (GDPR) та Україні (Закон України «Про захист персональних даних», вимоги Уповноваженого Верховної Ради з прав людини). На основі опрацьованих першоджерел необхідно:

— порівняти правові підстави обробки персональних даних за GDPR та українським законодавством: визначити, де підходи є конвергентними, а де – суттєво відрізняються, та обґрунтувати практичні наслідки цих відмінностей для організацій, що працюють в обох юрисдикціях одночасно;

— проаналізувати механізми реалізації прав суб'єктів даних в обох системах та оцінити, наскільки українське законодавство відповідає стандарту *adequacy decision* ЄС, необхідному для легітимної транскордонної передачі даних;

— сформулювати авторську позицію щодо ключових законодавчих змін, які Україна має імплементувати в межах євроінтеграційного процесу для досягнення повної відповідності стандартам GDPR, із зазначенням пріоритетності кожної зміни.

Форма подання результатів – структурована доповідь (7–10 хв.) з обов'язковим посиланням на тексти нормативних актів обох юрисдикцій. Після доповіді – дискусія у форматі «опонування»: двоє здобувачів формулюють контраргументи або уточнюючі запитання, доповідач має їх спростувати або визнати та скоригувати свою позицію.

Завдання 2 (ситуаційне): Комплексний GDPR-аудит модельної організації: від Data Mapping до DPIA.

Здобувачам надається картка-легенда організації з такими параметрами:

Приватна мережа медичних лабораторій (12 відділень по Україні). Сервіси: онлайн-запис на аналізи через веб-портал та мобільний застосунок, передача результатів аналізів пацієнтам через особистий кабінет та на електронну пошту, передача даних лікарям-партнерам через API-інтеграцію, зберігання архіву результатів у хмарному сховищі AWS (Ірландія). Категорії даних: ПІБ, дата народження, контактні дані, дані медичного страхування, результати аналізів (біометричні та медичні дані – чутлива категорія за статтею 9 GDPR). Наявна документація: політика конфіденційності на сайті (остання редакція – 2019 р.), окремого RoPA немає, угоди з Data Processors не укладалися. Нещодавня подія: організація планує впровадити модуль AI-діагностики, що аналізує результати аналізів та надає попередні висновки пацієнтам автоматично.

На основі наданих даних необхідно:

— побудувати повну карту потоків персональних даних із зазначенням для кожного потоку: категорії даних, правової підстави обробки, ролі сторін (controller / processor), наявності транскордонної передачі та механізму її легітимізації;

— заповнити реєстр діяльності з обробки для двох ключових процесів – онлайн-запису пацієнтів та передачі результатів лікарям-партнерам – з усіма обов'язковими полями відповідно до статті 30 GDPR;

— провести DPIA для запланованого модуля AI-діагностики: ідентифікувати не менше п'яти ризиків для прав суб'єктів даних, оцінити їх за матрицею імовірність × вплив та запропонувати конкретні технічні й організаційні заходи мінімізації для кожного ризику;

— підготувати перелік невідповідностей (*compliance gap list*) між поточним станом організації та вимогами GDPR із зазначенням пріоритетності усунення кожної з них.

Форма подання результатів – карта потоків персональних даних, заповнений RoPA, таблиця DPIA та перелік невідповідностей з усним захистом і рецензуванням у форматі peer-review.

Домашнє завдання: Міні-кейс «Розробка реєстру обробки (RoPA) та базова оцінка впливу (DPIA)».

Здобувачам пропонується виступити в ролі DPO (Data Protection Officer) або Privacy Engineer в українському HealthTech стартапі, який готується до виходу на європейський ринок. Завдання полягає у картуванні потоків даних та оцінці ризиків для нового мобільного застосунку.

Вхідні дані: компанія розробляє застосунок «SmartFit», який поєднує трекінг фізичної активності з рекомендаціями щодо ментального здоров'я. Застосунок збирає під час реєстрації: ім'я, email, вік. Під час використання: геолокацію (для трекінгу пробіжок), пульс (через смарт-годинник), а також користувач щодня вказує свій рівень стресу та настрій. Основна база даних розгорнута на AWS (Німеччина). Для аналітики поведінки користувачів інтегровано Google Analytics. Для розсилки маркетингових матеріалів та дайджестів використовується сервіс Mailchimp (США).

Безпосереднє завдання:

1. Картування даних: заповнити реєстр обробки для двох бізнес-процесів: «Трекінг пробіжок» та «Маркетингові email-розсилки».

Фрагмент реєстру обробки

Бізнес-процес	**Категорії персональних даних**	**Правова підстава (ст. 6 або ст. 9 GDPR)**	**Сторонні обробники (Processors)**	**Транскордонна передача**	**Термін зберігання (Retention)**
Трекінг пробіжок	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*Так* / *Ні, куди*)	(*заповнює здобувач*)
Маркетингові email-розсилки	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*Так* / *Ні, куди*)	(*заповнює здобувач*)

2. Аналіз ризиків (міні-DPIA): ідентифікувати щонайменше 2 критичні

ризики для конфіденційності в описаній архітектурі та запропонувати конкретні технічні або організаційні заходи для їхнього зниження.

Оцінка впливу на конфіденційність

Опис виявленого ризику	**Наслідки для суб'єкта даних**	**Запропоновані заходи захисту (Mitigation Controls)**
Зберігання даних про пульс та рівень стресу у відкритому вигляді в базі AWS	Витік медичних/чутливих даних, дискримінація, репутаційна шкода	Впровадження шифрування на рівні бази даних (AES-256), розділення ідентифікаторів користувачів (псевдонімізація)
(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)

*Примітка: *здобувачі мають обов'язково звернути увагу на те, що дані про здоров'я (пульс, рівень стресу) належать до чутливих даних, а використання Mailchimp передбачає передачу даних до США, що потребує додаткових юридичних механізмів.*

Рекомендована література:

1. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)
2. ДСТУ ISO/IEC 27701:2022 Методи безпеки. Розширення до ISO/IEC 27001 та ISO/IEC 27002 для керування конфіденційною інформацією. Вимоги та настанови (ISO/IEC 27701:2019, IDT)
3. The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. Version 1.0 (January 2020). URL: https://www.nist.gov/privacy-framework/privacy-framework
4. Bhajaria N. Data Privacy: A Runbook for Engineers. Manning Publications, 2022.
5. Dennedy M.F., Fox J., Finneran T.R. The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value. Apress, 2014.

ПРАКТИЧНЕ ЗАНЯТТЯ 6: ТЕХНІЧНИЙ КОМПЛАЄНС-АУДИТ (НА ПРИКЛАДІ PCI DSS АБО SOC 2)

Мета заняття: відпрацювання алгоритмів перевірки відповідності технічної інфраструктури жорстким галузевим вимогам, опанування методів збору аудиторських доказів (Evidence Collection) та верифікації цілісності систем.

Суть теми полягає у переході від теоретичного менеджменту безпеки до практичної інженерії комплаєнсу (Compliance Engineering). Головний фокус заняття зроблено на двох найбільш затребуваних у міжнародному бізнесі стандартах: PCI DSS (індустрія платіжних карток) та SOC 2 (критерії довірчих послуг для хмарних та сервісних організацій).

Під час заняття здобувачі вивчають критично важливу концепцію визначення меж аудиту (Scoping). На прикладі PCI DSS розглядається, як правильно ізолювати середовище даних власників карток CDE (Cardholder Data Environment) за допомогою сегментації мережі, щоб зменшити витрати на аудит та знизити ризики.

У контексті SOC 2 здобувачі розбирають різницю між звітами Type I (оцінка дизайну контролів на певний момент часу) та Type II (перевірка операційної ефективності контролів протягом тривалого періоду, зазвичай 6 місяців). Особлива увага приділяється методології технічного аудиту: як перевірити налаштування бездротових мереж, конфігурації серверів за hardening-гайдами (наприклад, CIS Benchmarks), процеси патч-менеджменту та цілісність критичних файлів FIM (File Integrity Monitoring). Таким чином здобувачі набувають навичок аудиторів (QSA / CPA), розуміючи, які саме технічні артефакти (логи, скріншоти конфігурацій, вивантаження з баз даних) є валідними доказами відповідності.

Очікувані результати опрацювання теми. Після успішного завершення цього практичного заняття здобувачі вищої освіти повинні:

Знати:

— архітектуру та 12 базових вимог актуальної версії стандарту PCI DSS, а також 5 критеріїв довірчих послуг (Trust Services Criteria) SOC 2 (Security, Availability, Processing Integrity, Confidentiality, Privacy);

— правила та критерії визначення меж технічного аудиту та методи захисту цих меж;

— види аудиторських доказів та вимоги до їхньої зрілості (автоматизовані логи vs. мануальні звіти).

Вміти:

— проводити технічний Gap-аналіз інфраструктури на відповідність обраному стандарту (PCI DSS або SOC 2);

— перевіряти технічні конфігурації операційних систем та мережевого обладнання на відповідність базовим рівням безпеки (Security Baselines);

— формувати «пакет доказів» (Audit Evidence Pack) для зовнішнього аудитора, мінімізуючи суб'єктивні трактування.

Володіти навичками:

— застосування автоматизованих інструментів для безперервного комплаєнс-моніторингу та аналізу технічних невідповідностей;

— розробки компенсаційних контролів (Compensating Controls) у випадках, коли пряме виконання технічної вимоги стандарту є неможливим через архітектурні обмеження системи.

Питання для обговорення:

1. Визначення меж аудиту у мікросервісній архітектурі: як контейнеризація та безсерверні обчислення ускладнюють або, навпаки, спрощують ізоляцію середовища даних платіжних карток.
2. SOC 2 Type I проти Type II: чому сучасний бізнес дедалі менше вірить «миттєвим знімкам» безпеки (Type I) і вимагає тривалого тестування операційної ефективності контролів (Type II).
3. Гнучкість PCI DSS 4.0 та кастомізований підхід (Customized Approach):

як новий ризик-орієнтований підхід дозволяє компаніям відходити від жорстких бінарних вимог стандарту та самостійно проектувати контроли безпеки.

4. Тотальна двофакторна автентифікація (MFA) за вимогами PCI DSS 4.0: технічні виклики впровадження MFA для будь-якого доступу до CDE, включаючи системні облікові записи та внутрішні комунікації.
5. Концепція Compliance-as-Code: інтеграція перевірок відповідності (наприклад, CIS Benchmarks) безпосередньо в CI/CD пайплайни розробки інфраструктури (Terraform, Ansible).
6. Еволюція збору доказів: від ручних скріншотів до API-платформ автоматизації: аналіз роботи сучасних GRC-платформ (Vanta, Drata, Secureframe) для безперервного збору аудиторських артефактів.
7. Мистецтво захисту компенсаційних контролів (Compensating Controls): як логічно та технічно обґрунтувати перед аудитором безпеку legacy-системи, яку неможливо оновити під прямі вимоги стандарту.
8. Менеджмент логів та моніторинг цілісності файлів (FIM) у хмарі: пошук балансу між вартістю зберігання терабайтів лог-файлів у SIEM-системах та суворими вимогами стандартів щодо термінів їхнього утримання (Retention Period).
9. Безперервне сканування вразливостей проти щорічного пентесту: як вимоги до тестування на проникнення в PCI DSS та SOC 2 адаптуються до умов, коли код продукту оновлюється кілька разів на день.
10. Мультихмарний комплаєнс (Multi-cloud Compliance): архітектурні складнощі побудови єдиної системи технічного контролю, якщо частина інфраструктури компанії розгорнута в AWS, частина в Azure, а ядро системи знаходиться на on-premise серверах.

Практичні завдання:

Завдання 1 (теоретико-аналітичне): Хмарний Gap-аналіз та мапінг контролів SOC 2.

Здобувачі об'єднуються в міні-групи. Їм надається опис типової хмарної

інфраструктури B2B SaaS-стартапу (розгорнутого в AWS або Azure), який готується до отримання звіту SOC 2 Type I за критеріями Security (Безпека) та Availability (Доступність).

Архітектура стартапу має наступний вигляд. Усі сервери працюють на віртуальних машинах AWS EC2. База даних клієнтів (PostgreSQL) розгорнута на AWS RDS в одній зоні доступності (Single-AZ). Доступ розробників до серверів відбувається через SSH-ключі, які зберігаються локально на їхніх ноутбуках. Резервні копії бази даних створюються щоночі та зберігаються у хмарному сховищі (AWS S3).

На основі наданих даних необхідно:

1. Мапінг: здобувачі отримують 3 абстрактні вимоги SOC 2. Для кожної з них вони мають вказати, який саме технічний інструмент або конфігурацію в цій архітектурі вони використають як доказ для аудитора:

   вимога 1: компанія використовує логічний контроль доступу для захисту систем.

   вимога 2: компанія моніторить систему на наявність аномалій та інцидентів безпеки;

   вимога 3: компанія забезпечує доступність системи для відновлення роботи після збоїв.
2. Gap-аналіз: здобувачі повинні знайти в описаній архітектурі щонайменше дві критичні невідповідності, через які аудитор відмовить у видачі сертифіката SOC 2.
3. План виправлення: здобувачі повинні запропонувати технічне рішення для усунення знайдених прогалин до початку аудиту.

Форма подання результатів – заповнена матриця відповідності та технічний звіт про знайдені архітектурні недоліки з рекомендаціями щодо їх усунення.

Завдання 2 (ситуаційне): Проведення технічного комплаєнс-аудиту платіжної інфраструктури відповідно до PCI DSS.

Компанія «PayCloud Services» надає послуги онлайн-еквайрингу та обробляє дані платіжних карток клієнтів. Інфраструктура компанії включає: веб-сервер із платіжним порталом; сервер застосунків; сервер бази даних із даними власників карток; корпоративну мережу співробітників; Wi-Fi мережу для відвідувачів офісу; VPN-доступ адміністраторів.

Під час попереднього обстеження було встановлено:

— сегментація між CDE та корпоративною мережею відсутня;

— патчі на сервері баз даних не встановлювались протягом 8 місяців;

— моніторинг цілісності критичних файлів не використовується;

— журнали подій зберігаються лише 14 днів;

— частина серверів використовує стандартні облікові записи виробника.

На основі наданих даних необхідно:

— визначити межі аудиту та перелік систем, що входять до CDE;

— встановити, які вимоги PCI DSS порушені;

— провести Gap-аналіз поточного стану інфраструктури;

— запропонувати технічні заходи щодо усунення невідповідностей;

— визначити перелік аудиторських доказів, які необхідно надати зовнішньому аудитору;

— запропонувати можливі компенсаційні контролі для випадків, коли окремі вимоги неможливо реалізувати негайно.

Форма подання результатів – короткий звіт аудитора, який містить: опис меж аудиту; перелік невідповідностей; матрицю ризиків; перелік необхідних доказів відповідності; рекомендації щодо досягнення комплаєнсу.

Домашнє завдання: Міні-кейс «Scoping та підготовка доказів для аудиту PCI DSS».

Здобувачам пропонується виступити в ролі інженер з внутрішнього комплаєнсу у стартапі «PayStream». За місяць компанію чекає сертифікаційний аудит за стандартом PCI DSS 4.0, який проводитиме зовнішній QSA-аудитор. Ваше завдання – визначити межі середовища даних

платіжних карток, підготувати матрицю доказів та розробити один компенсаційний контроль.

Вхідні дані (архітектура «PayStream» в AWS):

— сервіс A (Payment Gateway): мікросервіс, який безпосередньо приймає, токенізує та передає номери платіжних карток (PAN) у банк;

— сервіс B (Web Frontend): вітрина сайту та каталог товарів, не обробляє картки напряму (картки вводяться через iframe, що веде на сервіс A);

— сервіс C (Admin Panel): внутрішня панель управління, яка доступна для служби підтримки через корпоративний VPN. Дозволяє бачити лише масковані номери карток (перші 6, останні 4 цифри) для вирішення проблем клієнтів;

— Legacy Server (Система звітності): старий локальний сервер в офісі, який генерує фінансові звіти. Сервер підключений до тієї ж мережі, що й корпоративний VPN.

Безпосереднє завдання:

1. Визначення меж аудиту (Scoping): проаналізувати 4 компоненти системи та визначити, чи входять вони до середовища даних платіжних карток CDE, чи до підключених систем (Connected-to), чи є поза межами аудиту (Out of Scope).

Визначення меж аудиту

Компонент інфраструктури	**Статус (CDE / Connected-to / Out of Scope)**	**Обґрунтування (Чому саме цей статус?)**
Сервіс A	(*заповнює здобувач*)	(*заповнює здобувач*)
Сервіс B	(*заповнює здобувач*)	(*заповнює здобувач*)
Сервіс C	(*заповнює здобувач*)	(*заповнює здобувач*)
Legacy Server	(*заповнює здобувач*)	(*заповнює здобувач*)

2. Побудова матриці доказів (Evidence Matrix): сформувати перелік конкретних технічних артефактів (доказів), які необхідно надати аудитору для підтвердження виконання трьох специфічних вимог стандарту.

Матриця збору доказів

Вимога PCI DSS 4.0 / SOC 2	**Який документ підтверджує дизайн контролю? (Policy / Procedure)**	**Який технічний артефакт підтверджує роботу контролю? (Technical Evidence)**
Регулярне сканування на вразливості внутрішньої мережі (Vulnerability Scanning)	Затверджена Політика управління вразливостями	Звіт з Nessus / Qualys за останні 4 квартали з відсутністю High / Critical вразливостей
Багатофакторна автентифікація (MFA) для всього неконсольного доступу до CDE	(*заповнює здобувач*)	(*заповнює здобувач*)
Моніторинг цілісності критичних системних файлів (FIM)	(*заповнює здобувач*)	(*заповнює здобувач*)
Зберігання логів аудиту (Audit Trails) щонайменше 1 рік	(*заповнює здобувач*)	(*заповнює здобувач*)

3. Компенсаційний контроль (Compensating Control): уявити, що для доступу до Legacy Server неможливо технічно налаштувати багатофакторну автентифікацію, як того вимагає стандарт. Запропонувати технічне або організаційне рішення, яке компенсує цей ризик.

Рекомендована література:

1. PCI SSC. PCI DSS v4.0.1 Standard and Self-Assessment Questionnaire (SAQ).
2. American Institute of CPAs. Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (SOC 2).
3. CIS Benchmarks (Center for Internet Security). URL: https://www.cisecurity.org/cis-benchmarks
4. NIST Special Publication 800-53a: Assessing Security and Privacy Controls in Information Systems and Organizations. URL: https://doi.org/10.6028/NIST.SP.800-53Ar5

ПРАКТИЧНЕ ЗАНЯТТЯ 7: МОДЕЛЮВАННЯ ПРОЦЕСІВ РЕАГУВАННЯ НА ІНЦИДЕНТИ

Мета заняття: розробка та верифікація алгоритмічної моделі реагування на кіберінциденти, спрямованої на забезпечення стійкості бізнес-процесів у кризових умовах.

Суть теми полягає в опануванні методології побудови та алгоритмізації процесів реагування на інциденти кібербезпеки (Incident Response Lifecycle) на основі міжнародних індустріальних стандартів NIST SP 800-61 та SANS (PICERL). Головний фокус заняття зміщено з хаотичного «гасіння пожеж» на створення чітких, математично та логічно обґрунтованих моделей інструкцій (Playbooks) для різних типів загроз (Ransomware, DDoS, APT, витік даних).

Під час заняття здобувачі вивчають архітектуру крос-функціональної взаємодії команди реагування (CSIRT/CERT) з іншими вузлами бізнесу (IT, Legal, PR, HR, C-Suite). Особлива увага приділяється фундаментальній дилемі реагування на інциденти: локалізація загрози (Containment) проти збереження цифрових доказів (Forensics). Здобувачі вчаться моделювати процеси тріажу (первинного оцінювання та класифікації), розраховувати метрики ефективності реагування (середній час виявлення MTTD, середній час ліквідації MTTR) та інтегрувати технічні дії з планами забезпечення безперервності бізнесу (BCP) та аварійного відновлення (DRP). Верифікація розроблених моделей відбувається за допомогою симуляційних методів та настільних тренувань (Tabletop Exercises).

Очікувані результати опрацювання теми. Після успішного завершення цього практичного заняття здобувачі вищої освіти повинні:

Знати:

— фази життєвого циклу інциденту за стандартами NIST та SANS, а також критерії класифікації інцидентів за рівнями критичності для бізнесу;

— ключові метрики ефективності SOC/CSIRT (MTTD, MTTR) та параметри відновлення бізнес-процесів (цільовий час відновлення RTO, цільова точка відновлення RPO);
— юридичні та регуляторні вимоги щодо сповіщення про інциденти, зокрема таймлайни повідомлення за GDPR та директивою NIS 2.

Вміти:

— розробляти алгоритмічні моделі реагування (IR Playbooks) у вигляді блок-схем або нотацій (наприклад, елементів BPMN) для специфічних векторів атак на основі фреймворку MITRE ATT&CK;
— проводити швидкий технічний тріаж інциденту (Incident Triage), визначати масштаб компрометації інфраструктури та ізолювати уражені сегменти без зупинки критичних сервісів;
— формулювати технічно та юридично коректні звіти про інцидент (Incident Reports) для регуляторів, клієнтів та внутрішнього менеджменту.

Володіти навичками:

— проектування компенсаційних та тимчасових технічних рішень для підтримки працездатності бізнесу в умовах активної атаки на основі динамічного аналізу впливу на бізнес-процеси BIA (Business Impact Analysis);
— проведення аналізу «уроків на майбутнє» (Lessons Learned) після інциденту для детектування системних прогалин в архітектурі захисту та реконфігурації політик безпеки.

Питання для обговорення:

1. Порівняльний аналіз класичних методологій життєвого циклу інциденту NIST SP 800-61 і SANS (PICERL): Як адаптувати ці стандарти до динамічних хмарних (Cloud-Native) та мікросервісних інфраструктур?
2. Автоматизація тріажу та боротьба з «втомою від сповіщень» (Alert Fatigue): Де проходить межа між автоматичним блокуванням загрози за

допомогою SOAR-систем та ризиком випадково зупинити критичний бізнес-процес через помилку алгоритму?

3. Критична дилема «Локалізація проти Криміналістики» (Containment vs Forensics): Як архітектору безпеки прийняти рішення між негайним ізолюванням (або вимкненням) скомпрометованого сервера та збереженням артефактів в оперативній пам'яті?
4. Узгодження технічних метрик безпеки з бізнес-метриками: У яких кейсах керівник безпеки (CISO) має свідомо дозволити атаці продовжуватися, якщо миттєва ізоляція системи завдасть збитків, що перевищують допустимий час простою бізнесу RTO?
5. Моделювання дій під час Ransomware-атак із потрійним шантажем (Triple Extortion): Особливості побудови сценаріїв реагування, коли хакери не лише шифрують дані, а й викрадають їх для шантажу та паралельно запускають DDoS-атаку на клієнтів компанії.
6. Кризова крос-функціональна комунікація: Як виконати вимогу суворого таймлайну сповіщення регуляторів (наприклад, 72 години за GDPR або директивою NIS 2) і не знищити репутацію бренду?
7. Інциденти у ланцюжку поставок (Supply Chain Incidents): Алгоритм дій команди безпеки, якщо джерелом компрометації є не власна інфраструктура, а комерційне ПЗ третьої сторони або підрядник із легітимним доступом.
8. Штучний інтелект на службі Incident Response: Потенціал та ризики залучення ШІ-асистентів для швидкої інтерпретації складних логів під час тріажу та генерації коду для закриття вразливостей «на льоту».
9. Методология верифікації моделей: Як організувати симуляцію кібератаки для топ-менеджменту компанії, щоб перевірити реальну життєздатність паперових інструкцій без шкоди для продуктивного середовища?
10. Культура «Безвинних розслідувань» (Blameless Post-Mortem): Як правильно моделювати етап аналізу «уроків на майбутнє», щоб

фокусуватися на виправленні системних архітектурних прогалин, а не на пошуку та покаранні «винного» адміністратора чи розробника?

Практичні завдання:

Завдання 1 (теоретико-аналітичне): Критичний аналіз застосовності фреймворку MITRE ATT&CK для побудови проактивних IR Playbooks.

Здобувачам пропонується дослідити, наскільки систематичне використання матриці MITRE ATT&CK при розробці алгоритмів реагування на інциденти дозволяє організації перейти від реактивної до проактивної моделі кібербезпеки. На основі опрацьованих першоджерел необхідно:

— проаналізувати, як декомпозиція атаки на тактики та техніки за MITRE ATT&CK (наприклад, Initial Access, Lateral Movement, Exfiltration) дозволяє формалізувати Playbook не як універсальну інструкцію, а як набір тригерних точок реагування, прив'язаних до конкретних поведінкових індикаторів атакуючого;

— дослідити обмеження цього підходу: чи здатна статична матриця технік встигати за швидкою еволюцією тактик реальних APT-груп, та які механізми (наприклад, ATT&CK Navigator, Threat Intelligence Feeds) дозволяють підтримувати Playbooks в актуальному стані;

— порівняти ефективність побудови IR Playbooks на основі MITRE ATT&CK з альтернативним підходом – Kill Chain моделлю Lockheed Martin – та обґрунтувати, в яких організаційних контекстах кожен із підходів є більш доцільним.

Форма подання результатів – структурована доповідь (7–10 хв.) з обов'язковим посиланням на офіційну документацію MITRE ATT&CK та релевантні дослідження ефективності Threat-Informed Defense. Після доповіді – дискусія у форматі «опонування»: двоє здобувачів формулюють контраргументи або наводять контрприклади з реальних інцидентів, доповідач має їх спростувати або скоригувати свою позицію.

Завдання 2 (ситуаційне): Розробка IR Playbook та симуляція реагування на інцидент типу Ransomware.

Здобувачам надається картка-легенда інциденту:

Виробнича компанія (250 співробітників, власна логістична мережа). О 03:14 ночі система моніторингу фіксує аномальну активність шифрування файлів на файловому сервері відділу бухгалтерії. До 06:00 ранку шифрування поширюється на 40% робочих станцій мережі через незахищений RDP-доступ адміністратора, що залишився відкритим після технічних робіт. О 07:30 на екранах уражених станцій з'являється повідомлення про викуп у криптовалюті з вимогою 50 BTC та погрозою публікації викрадених даних клієнтів. ERP-система, що містить персональні дані 15000 клієнтів, перебуває в тому самому сегменті мережі. Бекапи останній раз перевірялись 4 місяці тому.

На основі наданих даних необхідно:

— розробити покроковий IR Playbook реагування на цей конкретний інцидент у вигляді блок-схеми, що охоплює фази Identification → Containment → Eradication → Recovery → Lessons Learned, з прив'язкою кожної дії до конкретної ролі в команді CSIRT (технічний аналітик, керівник IR, Legal, PR);
— провести технічний тріаж: визначити пріоритетність ізоляції сегментів мережі з обґрунтуванням послідовності дій, враховуючи компроміс між зупинкою поширення атаки та збереженням доказів для подальшого розслідування;
— розрахувати орієнтовні MTTD та MTTR для цього сценарію на основі наданого таймлайну та запропонувати конкретні технічні заходи, які скоротили б ці показники;
— визначити юридичні зобов'язання організації щодо сповіщення – кого, у які терміни та з яким обсягом інформації необхідно повідомити відповідно до GDPR та законодавства України, з огляду на компрометацію персональних даних клієнтів;
— підготувати короткий проєкт публічної заяви для клієнтів (executive communication) – без технічного жаргону, з балансом між прозорістю та

юридичною обачністю.

Форма подання результатів – блок-схема Playbook, розрахунок метрик, перелік регуляторних зобов'язань та проєкт заяви з усним захистом і рецензуванням групи у форматі настільного тренування.

Домашнє завдання: Проєктування та верифікація IR Playbook для атаки типу Ransomware.

Здобувачам пропонується виступи у ролі керівника команди реагування на інциденти (Incident Response Lead) у логістичній компанії «FastCargo».

Вхідні дані (контекст організації):

— інфраструктура: 80% сервісів розгорнуто в хмарі AWS, але ядро системи трекінгу працює на локальних серверах у центральному дата-центрі;

— бізнес-критичність: зупинка системи трекінгу понад 4 години (RTO = 4 години) призводить до колапсу логістичних терміналів та збитків у розмірі $50000 за кожну наступну годину простою. Максимально допустимий час відновлення становить 1 годину (RPO = 1 година).

Сценарій інциденту:

— понеділок, 09:15 – системний адміністратор помічає аномально високе навантаження на процесор головного сервера бази даних трекінгу;

— 09:20 – користувачі починають скаржитися, що файли внутрішньої документації на спільних дисках мають дивне розширення .locked;

— 09:25 – на робочих столах серверів з'являється текстовий файл від угруповання BlackCat із вимогою викупу в $300000 за ключ дешифрування. Хакер стверджує, що 100 Гб конфіденційних даних клієнтів (включаючи адреси та фінансові звіти) вже завантажено на їхній сервер шантажу.

Безпосереднє завдання:

1. Побудувати детальну схему процесу реагування (IR Playbook) у будь-якому графічному редакторі (Draw.io, Lucidchart, Miro). Схема

повинна базуватися на фазах NIST:

Identification (Ідентифікація): які технічні логи/метрики підтверджують, що це саме Ransomware, а не технічний збій? Опишіть критерії тріажу.

Containment (Локалізація): опишіть алгоритм ізоляції. Важлива дилема: чи вимикати живлення серверів (що знищить дампи оперативної пам'яті), чи відключати їх від мережі на рівні комутаторів?

Eradication & Recovery (Ліквідація та Відновлення): покроковий план очищення та відновлення з бекапів з урахуванням обмежень RTO та RPO.

2. Побудувати матрицю відповідальності (RACI), відповівши таким чином на питання "Хто за що відповідає в момент кризи?".

Матриця відповідальності

Етапи реагування	**IR Team (Безпека)**	**IT-відділ (Адміни)**	**Legal (Юристи)**	**PR**	**CEO (Директор)**
Технічна ізоляція мережі	A / R (приклад)	R (приклад)	I (приклад)	I (приклад)	I (приклад)
Прийняття рішення про перехід на паперовий документообіг	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)
Повідомлення Уповноваженого з прав людини / Держспецзв'язку	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)
Комунікація зі ЗМІ щодо витоку даних	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)
Прийняття рішення про (не)виплату викупу	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)	(*заповнює здобувач*)

*Примітка: R – Responsible (Виконує), A – Accountable (Затверджує / Несе відповідальність), C – Consulted (Консультує), I – Informed (Інформується).

3. Провести аналіз «уроків на майбутнє». Дати письмові розгорнуті відповіді (по 1-2 абзаци) на наступні пост-кризові запитання:

Аналіз KPI: Якщо відновлення системи з бекапів тривало 6 годин замість задекларованих 4, які технічні чи організаційні чинники стали причиною порушення RTO? Як автоматизувати процес, щоб вкластися в ліміт наступного разу?

Регуляторний комплаєнс: Оскільки зловмисники заявили про викрадення персональних даних клієнтів, які ваші юридичні зобов'язання щодо термінів сповіщення національних та / або міжнародних регуляторів (якщо серед клієнтів були громадяни ЄС)?

Рекомендована література:

1. National Institute of Standards and Technology. NIST Special Publication 800-61 Revision 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management. URL: https://doi.org/10.6028/NIST.SP.800-61r3
2. ДСТУ ISO/IEC 27035-1:2024 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи та процес (ISO/IEC 27035-1:2023, IDT).
3. ДСТУ ISO/IEC 27035-2:2024 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2023, IDT).
4. ДСТУ ISO/IEC 27035-3:2024 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 3. Настанова щодо реагування на інциденти у сфері ІКТ (ISO/IEC 27035-3:2020, IDT).
5. SANS Institute. Incident Handler's Handbook. URL: https://www.sans.org/white-papers/33901
6. National Institute of Standards and Technology. NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response. URL: https://doi.org/10.6028/NIST.SP.800-86

ПРАКТИЧНЕ ЗАНЯТТЯ 8: ЗАХИСТ РЕЗУЛЬТАТІВ АУДИТУ ТА ВЕРИФІКАЦІЯ ДОКАЗІВ

Мета заняття: удосконалити навички збору, аналізу та представлення об'єктивних доказів у процесі науково-технічної експертизи систем захисту інформації.

Суть теми полягає в опануванні фінальної стадії аудиторського циклу (згідно зі стандартами ISO 19011 та ISACA ITAF) – валідації зібраних артефактів та формуванні експертного висновку. Заняття фокусується на принципі «професійного скептицизму»: здобувачі вчаться відрізняти декларативні заяви (політики на папері) від технічно верифікованих доказів (логування конфігурацій, хеш-суми, результати автоматизованого сканування).

Особлива увага приділяється концепції безперервності доказів (Chain of Custody) та методам захисту аудиторського сліду (Audit Trail) від маніпуляцій з боку адміністраторів систем, що перевіряються. Під час заняття здобувачі відпрацьовують навички складання фінальних звітів (Executive Summary та Technical Report) і моделюють процес публічного захисту результатів аудиту перед стейкхолдерами та зовнішніми регуляторами. Розглядається психологія комунікації в умовах конфлікту інтересів, коли аудитор змушений фіксувати критичні невідповідності (Non-Conformities), що можуть зупинити реліз продукту або призвести до штрафів.

Очікувані результати опрацювання теми. Після успішного завершення цього практичного заняття здобувачі вищої освіти повинні:

Знати:

— міжнародні критерії якості аудиторських доказів (достатність, достовірність, релевантність) за стандартами ISACA;

— методологію забезпечення цілісності цифрових доказів під час їх збору та зберігання (хешування, криптографічні мітки часу);

— структуру та правила оформлення фінального звіту про аудит інформаційної безпеки відповідно до вимог PCI DSS RoC (Report on Compliance) або SOC 2 Type II Report.

Вміти:

— проводити крос-валідацію доказів – порівнювати заявлену архітектуру з реальними вивантаженнями з систем моніторингу та конфігураційних файлів;

— формулювати чіткі, юридично та технічно обґрунтовані висновки щодо знайдених вразливостей або порушень комплаєнсу;

— транслювати глибокі технічні метрики (наприклад, відсутність шифрування на рівні бази даних) у зрозумілі бізнес-ризики – репутаційні втрати, фінансові штрафи за GDPR.

Володіти навичками:

— публічної та аргументованої комунікації зі стейкхолдерами компанії (управлінським складом, розробниками, IT-відділом) для захисту висновків експертизи;

— конструктивного вирішення суперечок під час узгодження результатів аудиту – вміння відстоювати свою професійну позицію під тиском;

— розробки плану усунення недоліків (Remediation Plan) та оцінки залишкових ризиків (Residual Risks) після впровадження компенсаційних контролів.

Питання для обговорення:

1. Принцип «професійного скептицизму» в IT-аудиті: Як аудитору відрізнити декларативні заяви (політики та процедури на папері) від реальних, технічно верифікованих доказів (логів, конфігурацій, правил брандмауерів)?
2. Автоматизований комплаєнс-моніторинг проти ручних скріншотів: Переваги та ризики використання інструментів автоматизації (на кшталт Chef InSpec чи AWS Audit Manager).
3. Забезпечення цілісності цифрових артефактів: Які криптографічні

методи (хешування, блокчейн-реєстри логів, криптографічні мітки часу) гарантують, що технічні докази не були змінені адміністраторами системи під час або після проведення перевірки?

4. Порівняльний аналіз доказової бази для різних типів звітів (на прикладі SOC 2 Type I vs Type II): Чому довести відповідність контролю безпеки в конкретний момент часу (*point-in-time*) значно легше, ніж довести його безперервну роботу протягом 6–12 місяців (*period-of-time*)? Які артефакти потрібні для другого варіанту?
5. Написання фінальних звітів для топ-менеджменту: Як правильно транслювати складні технічні невідповідності (наприклад, слабкі алгоритми шифрування в базі даних) мовою бізнес-ризиків (фінансові збитки, репутаційні втрати, відкликання ліцензії)?
6. Управління конфліктами та супротив під час аудиту (Pushback): Як діяти внутрішньому або зовнішньому аудитору, якщо власник системи чи керівник IT-відділу категорично не погоджується з виявленою невідповідністю і чинить професійний тиск?
7. Оцінка залишкових ризиків після аудиту: Як методологічно визначити, чи розроблений компанією план усунення недоліків та впроваджені компенсаційні контроли дійсно знижують ризик до прийнятного для бізнесу рівня?
8. Проблема вибірки (Sampling) у динамічних середовищах: Як аудитору сформувати репрезентативну та об'єктивну вибірку хостів, логів чи облікових записів для перевірки у великих хмарних інфраструктурах, де щодня автоматично створюються та видаляються тисячі мікросервісів?
9. Генеративний ШІ як асистент аудитора та інженера з комплаєнсу: Потенціал та приховані загрози використання LLM-моделей для аналізу тисяч сторінок технічних логів та конфігураційних файлів на предмет відповідності стандартам. Як боротися з ШІ-галюцинаціями в експертних висновках?

10. Юридична сила результатів технічного аудиту: Як результати внутрішньої науково-технічної експертизи безпеки об'єкта можуть бути використані як доказова база в судовому процесі (наприклад, під час розслідування масштабного витоку даних чи корпоративного шпигунства)?

Практичні завдання:

Завдання 1 (теоретико-аналітичне): Професійний скептицизм аудитора: межі довіри до автоматизованих доказів.

Здобувачам пропонується здійснити критичний аналіз принципу «професійного скептицизму» в контексті зростаючої автоматизації аудиторського процесу. На основі опрацьованих першоджерел необхідно:

— дослідити парадокс довіри до автоматизованих доказів: чи знижує використання інструментів безперервного комплаєнс-моніторингу пильність аудитора щодо можливості маніпуляції цими ж інструментами з боку адміністраторів системи, що перевіряється;

— проаналізувати щонайменше три технічні сценарії, в яких формально валідний цифровий доказ (лог, хеш-сума, звіт сканера) може вводити аудитора в оману (через підміну часових міток, селективне логування або компрометацію самого моніторингового агента) та визначити контрзаходи для виявлення таких маніпуляцій;

— обґрунтувати, де проходить межа між обґрунтованою недовірою аудитора та надмірним скептицизмом, що паралізує ефективність аудиторського процесу й шкодить робочим відносинам зі стейкхолдерами.

Форма подання результатів – структурована доповідь (7–10 хв.) з обов'язковим посиланням на стандарти ISACA ITAF та ISO 19011. Після доповіді – дискусія у форматі «опонування»: двоє здобувачів наводять контрприклади або альтернативні інтерпретації, доповідач має їх спростувати або скоригувати свою позицію.

Завдання 2 (ситуаційне): Захист звіту про критичну невідповідність

перед радою директорів.

Здобувачам надається картка-легенда ситуації:

Здобувач виступає в ролі зовнішнього аудитора SOC 2 Type II для SaaS-компанії, що обслуговує понад 200 корпоративних клієнтів. У ході аудиту виявлено критичну невідповідність: база даних клієнтів не має шифрування на рівні зберігання (*encryption at rest*), хоча в офіційній політиці безпеки компанії, наданій клієнтам як частина договірних зобов'язань, прямо зазначено, що «всі дані клієнтів шифруються відповідно до галузевих стандартів». Технічний директор компанії заперечує критичність знахідки, аргументуючи це тим, що мережевий периметр добре захищений, а шифрування на рівні диска створить додаткове навантаження на продуктивність системи. Звіт SOC 2 має бути завершений за 5 робочих днів, а CEO компанії вже повідомив трьом великим клієнтам очікувану дату отримання чистого звіту.

На основі наданих даних необхідно:

— сформулювати технічно та юридично коректний опис виявленої невідповідності для включення у фінальний звіт, з чітким посиланням на порушений критерій Trust Services Criteria;

— підготувати аргументацію для захисту критичності цієї знахідки в розмові з технічним директором – перевести технічний ризик (відсутність шифрування) на мову бізнес-наслідків (договірна відповідальність, потенційні штрафи, втрата довіри клієнтів);

— розробити план дій для трьох можливих сценаріїв розвитку ситуації: компанія погоджується усунути недолік до фіналізації звіту; компанія просить відстрочку та пропонує компенсаційний контроль; компанія наполягає на видаленні знахідки зі звіту;

— підготувати коротку структуровану позицію (Executive Summary) для представлення на засіданні ради директорів, що пояснює суть проблеми, ризики бездіяльності та рекомендовані наступні кроки.

Форма подання результатів – письмовий опис невідповідності,

аргументація для кожного сценарію та коротка структурована позиція з рольовою грою перед групою, де частина здобувачів виконує роль ради директорів і ставить уточнюючі або провокативні запитання.

Домашнє завдання: Експертиза доказової бази та захист аудиторського висновку в умовах конфлікту інтересів.

Вхідні дані: здобувачі виступають в ролі провідного внутрішнього аудитора (Lead Compliance Engineer) у компанії «PayStream» (FinTech-платформа). Компанія готується до фінального зовнішнього аудиту SOC 2 Type II (критерій Security).

Команда DevOps та системні адміністратори надали пакет доказів (артефактів), стверджуючи, що всі вимоги стандарту виконано на 100%. Однак під час крос-валідації були виявлені серйозні розбіжності між тим, що написано «на папері», і тим, що відбувається в реальності.

Технічні артефакти для аналізу:

1. Захист адміністративного доступу (Вимога CC6.1 – MFA).
   - — Заява команди DevOps та адміністраторів: «Усі облікові записи з правами адміністратора в хмарі AWS захищені багатофакторною автентифікацією (MFA)».
   - — Наданий доказ: скріншот із панелі AWS IAM Identity Center, де видно увімкнену політику MFA, яка датована першим числом звітного періоду.
   - — Результат детальної перевірки: проаналізувавши «сирі» логи AWS CloudTrail за останній місяць, ви виявили, що три адміністратори систематично підключалися до інфраструктури через CLI (інтерфейс командного рядка) за допомогою постійних API-ключів (Access Keys), де MFA взагалі не було налаштовано або воно було обійдене для «зручності автоматизації скриптів».
2. Цілісність логів безпеки (Вимога CC7.2 – Log Integrity).
   - — Заява команди DevOps та адміністраторів: «Логи з усіх серверів автоматично та безперервно відправляються у централізоване

сховище AWS S3, доступ до якого суворо обмежений. Модифікація чи видалення логів неможливі».

— Наданий доказ: копія тексту офіційної «Політики логування та моніторингу».

— Результат детальної перевірки: проаналізувавши реальну конфігурацію політики доступу (S3 Bucket Policy), виявилося, що обліковий запис root, пароль від якого зберігається у спільному менеджері паролів IT-відділу (і до якого мають доступ 4 людини), має повні права (S3:PutBucketPolicy та S3:DeleteObject). Тобто, у разі компрометації будь-якого з цих адмінів, зловмисник може повністю стерти сліди своєї присутності.

Безпосереднє завдання:

1. Підготувати картку невідповідності (Non-Conformity Report). Для кожного з двох кейсів здобувачі мають скласти офіційний аудиторський висновок за класичною міжнародною структурою 5C:
   — стан речей (Condition): Що реального виявлено в системі? (Опис технічної прогалини з посиланням на логи CloudTrail / конфігурацію S3);
   — критерій (Criteria): Чому саме це є порушенням? (Посилання на конкретну вимогу SOC 2 або PCI DSS);
   — причина (Cause): Чому, на вашу думку, це сталося? (Наприклад, людський фактор, брак автоматизації, намагання спростити роботу);
   — наслідки / ризик (Consequence / Risk): Чим це загрожує бізнесу? (Опис вектора можливої атаки через цю вразливість);
   — рекомендація (Corrective Action): Що конкретно технічно потрібно зробити IT-відділу для виправлення ситуації?
2. Підготовка Executive Summary на ім'я CEO компанії.

Уявіть, що керівник IT-відділу чинить на вас тиск і каже: «Ці зауваження – дрібниці, ми покажемо зовнішньому аудитору скріншоти, і все

буде ОК. Не зривай нам терміни релізу!».

Перекладіть технічну проблему (API-ключі без MFA та права на видалення S3) мовою бізнес-ризиків. Поясніть директору, чому спроба «сховати» ці проблеми від зовнішнього аудитора загрожує провалом сертифікації SOC 2, фінансовими втратами та репутаційним колапсом у разі реального хакерського зламу.

Рекомендована література:

1. ДСТУ EN ISO/IEC 27007:2022 Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою (EN ISO/IEC 27007:2022, IDT; ISO/IEC 27007:2020, IDT).
2. ДСТУ ISO 19011:2019 Настанови щодо проведення аудитів систем управління (ISO 19011:2018, IDT).
3. ISACA. ITAF: A Professional Practices Framework for IT Assurance (4th Edition). URL: https://www.famu.edu/administration/audit/pdf/standards/ITAF-4th-Edition.pdf

КРИТЕРІЇ ОЦІНЮВАННЯ ПРАКТИЧНИХ ЗАНЯТЬ

Поточний контроль здійснюється в усній та письмовій формах і передбачає оцінювання результатів фронтального та індивідуального опитування, виконання практичних завдань, а також моделювання ситуаційних кейсів. Максимальний обсяг балів, який здобувач вищої освіти може набрати за поточну успішність, становить 40 балів.

В якості індивідуальної роботи передбачено виконання розрахунково-графічної роботи. Максимальна оцінка за бездоганне виконання розрахунково-графічної роботи становить 10 балів.

Модульний контроль охоплює дві модульні контрольні роботи, що проводяться у форматі комп'ютерного тестування та містять теоретичний і практичний блоки. Максимальна оцінка за бездоганне виконання кожної модульної роботи становить 25 балів.

Підсумковий контроль реалізується у формі заліку, який має накопичувальний характер. Максимальний підсумковий рейтинг здобувача становить 100 балів, а мінімальний пороговий рівень, що дозволяє отримати оцінку «зараховано», – 60 балів.

Диференційовані критерії оцінювання результатів навчання наведено у таблицях нижче.

Таблиця 1 – Критерії оцінювання за різними видами робіт

Види роботи	Бали	Критерії оцінювання
Усні відповіді на практичних заняттях	0	**Незадовільна відповідь або її відсутність.** Здобувач відмовився від відповіді, надав повністю хибну інформацію або припустився критичних помилок, що свідчать про відсутність розуміння базових концептів теми.
	1	**Часткова або неточна відповідь.** Матеріал засвоєно на базовому рівні, проте виклад є неповним, містить несуттєві помилки чи термінологічні шорсткості. Здобувач потребує навідних запитань викладача для деталізації.
	2	**Повна та обґрунтована відповідь.** Здобувач виявляє глибоке розуміння матеріалу, логічно й послідовно викладає думку, вільно та правильно використовує професійну термінологію, наводить чіткі аргументи чи прикладні кейси.
Практичні завдання	0	**Завдання не виконано.** Роботу не представлено у визначений термін, або надані результати повністю не відповідають умовам завдання (плагіат, хибні технічні рішення, відсутність розрахунків чи моделей).
	1	**Часткове (поверхневе) виконання.** Завдання виконано менш ніж наполовину або містить серйозні концептуальні помилки. Робота має суто формальний характер, аналіз ризиків чи обґрунтування рішень практично відсутні.
	3	**Виконання з незначними недоліками.** Завдання виконано загалом правильно, але припущено окремі несуттєві помилки, термінологічні неточності або частково пропущено другорядні елементи аналізу, які суттєво не впливають на кінцевий результат.
	5	**Повне та бездоганне виконання.** Завдання виконано в повному обсязі з дотриманням усіх вимог стандартів. Здобувач продемонстрував глибокий аналіз, технічну/юридичну грамотність, обґрунтував вибір рішень та безпомилково сформулював висновки.

Таблиця 2 – Критерії оцінювання модульних контрольних робіт

Види роботи	Бали	Критерії оцінювання
Теоретичні питання	0	**Неправильна відповідь.** Здобувач виявив повне незнання теоретичного матеріалу, припустився грубих концептуальних помилок, що спотворюють суть питання, або взагалі залишив питання без відповіді.
	1	**Частково правильна відповідь.** Теорію загалом засвоєно, але відповідь є невидною, містить неточності у формулюваннях або частково пропущені важливі елементи класифікацій/процесів. Було допущено незначні термінологічні помилки.
	2	**Повна та правильна відповідь.** Здобувач продемонстрував точне знання теоретичного матеріалу (нормативних вимог, положень стандартів). Термінологію використано безпомилково, відповідь логічно структурована та містить вичерпні аргументи.
Практичне питання	0	**Завдання не розв'язано.** Відповідь повністю відсутня, або надане рішення абсолютно не відповідає змісту завдання (присутні сліди плагіату, або технічні рішення є критично хибними й загрожують безпеці об'єкта).
	1	**Поверхневе / хаотичне виконання.** Зроблено лише спробу підходу до завдання. Продемонстровано слабке розуміння практичного інструментарію; запропоновані рішення є безсистемними, містять грубі концептуальні помилки та не вирішують поставлену проблему.
	2	**Фрагментарне розв'язання.** Здобувач розуміє суть завдання і базовий алгоритм його вирішення, але спроможний виконати лише окремі елементи (наприклад, правильно вказано формули чи критерії, але розрахунки або побудова моделі Playbook не завершені).
	3	**Виконання з частковими помилками в логіці або розрахунках.** Завдання виконано переважно правильно, але припущено помилку на одному з ключових етапів (наприклад, невірно визначено пріоритет інциденту чи межі скоупінгу), що частково спотворило фінальний результат. Висновки потребують доопрацювання.
	4	**Правильне розв'язання з несуттєвими графічними та / або текстовими похибками.** Завдання виконано в повному обсязі, логіка вирішення є правильною. Проте допущено поодинокі дрібні неточності, які не впливають на загальну коректність архітектури чи фінальний результат оцінки ризиків/комплаєнсу.
	5	**Бездоганне розв'язання.** Завдання виконано повністю, обрано оптимальну методологію (алгоритм). Продемонстровано бездоганний аналіз технічного контексту, розрахунки або моделі є абсолютно точними, висновки логічні та повністю обґрунтовані.

Таблиця 3 – Розподіл балів, які отримують здобувачі за результатами поточного контролю

<table>
<tr><th colspan="3">Поточний контроль (практичні заняття, самостійна робота)</th><th>РГР (бали)</th><th>МК (бали)</th><th>Залік (бали)</th></tr>
<tr><td>ПЗ</td><td colspan="2">Бали</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>ПЗ 1</td><td>5</td><td rowspan="4">20</td><td rowspan="8">10</td><td rowspan="4">25</td><td rowspan="8"></td></tr>
<tr><td>ПЗ 2</td><td>5</td></tr>
<tr><td>ПЗ 3</td><td>5</td></tr>
<tr><td>ПЗ 4</td><td>5</td></tr>
<tr><td>ПЗ 5</td><td>5</td><td rowspan="4">20</td><td rowspan="4">25</td></tr>
<tr><td>ПЗ 6</td><td>5</td></tr>
<tr><td>ПЗ 7</td><td>5</td></tr>
<tr><td>ПЗ 8</td><td>5</td></tr>
<tr><td>Всього</td><td colspan="2">40</td><td>10</td><td>50</td><td>100</td></tr>
</table>