Міністерство освіти і науки України
Луцький національний технічний університет
Факультет комп'ютерних та інформаційних технологій
Кафедра кібербезпеки

ОЦІНКА ТА УПРАВЛІННЯ РИЗИКАМИ

Конспект лекцій
для здобувачів першого (бакалаврського) рівня вищої освіти
освітньої програми «Кібербезпека»
галузі знань 12 (F) Інформаційні технології
спеціальності F5 (125) Кібербезпека та захист інформації
денної та заочної форм навчання

Луцьк 2026

УДК 004.056

Рекомендовано до видання вченою радою факультету КІТ ЛНТУ,
протокол № _____ від «__» _____ 20 26 року.

Голова вченої ради факультету КІТ _____ Інна КОНДІУС

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ

Директор бібліотеки _____ Наталія ПОЛІЩУК

Розглянуто і схвалено на засіданні кафедри кібербезпеки
ЛНТУ, протокол № _____ від « _____» _____ 20 26 року.

Завідувач кафедри КБ _____ Сергій КОСТЮЧКО

Укладачі: _____ Сергій КОСТЮЧКО, кандидат технічних наук,
завідувач кафедри кібербезпеки ЛНТУ
_____Олег КУЛАКЕВИЧ, ас. кафедри кібербезпеки ЛНТУ

Рецензент: _____ Сергій ГРИНЮК, кандидат технічних наук,
доцент кафедри кібербезпеки ЛНТУ лін

Відповідальний за випуск: _____ Сергій КОСТЮЧКО, кандидат
технічних наук, завідувач кафедри кібербезпеки ЛНТУ

Оцінка та управління ризиками: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Кібербезпека» галузі знань 12 (F) Інформаційні технології спеціальності F5 (125) Кібербезпека та захист інформації денної та заочної форм навчання / уклад. С.М. Костючко, О.Р. Кулакевич. Луцьк: ЛНТУ, 2026. 62 с.

ЗМІСТ

ВСТУП 4
ЛЕКЦІЯ 1. ПОНЯТТЯ КІБЕРІНЦИДЕНТА/КІБЕРАТАКИ 6
ЛЕКЦІЯ 2. РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ/КІБЕРАТАК 12
ЛЕКЦІЯ 3. УПРАВЛІННЯ РИЗИКАМИ В ІНФОРМАЦІЙНІЙ ТА/АБО КІБЕРБЕЗПЕЦІ 18
ЛЕКЦІЯ 4. ЗАГАЛЬНА КОНЦЕПЦІЯ УПРАВЛІННЯ РИЗИКАМИ ІБ 24
ЛЕКЦІЯ 5. NIST SP 800x 29
ЛЕКЦІЯ 6. СИСТЕМИ КЛАСУ INCIDENT RESPONSE PLATFORM 36
ЛЕКЦІЯ 7. ЕТАПИ ПРОВЕДЕННЯ АУДИТУ. АУДИТ НА ОСНОВІ АНАЛІЗУ РИЗИКІВ 41
ЛЕКЦІЯ 8. АУДИТ НА ОСНОВІ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (ІБ). АУДИТ НА ОСНОВІ ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ ІНФОРМАЦІЙНИХ СИСТЕМ (ІС). ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕС-ПРОЦЕСІВ: ПОНЯТТЯ БІЗНЕС-ПРОЦЕСУ. МОДЕЛЬ БІЗНЕС-ПРОЦЕСУ 46
ЛЕКЦІЯ 9. РОЗРОБКА ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС ЗАБЕЗПЕЧЕННЯ БІЗНЕС-ПРОЦЕСІВ. ДОТРИМАННЯ ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС ЗАБЕЗПЕЧЕННЯ БІЗНЕС-ПРОЦЕСІВ 53
СПИСОК ЛІТЕРАТУРИ 59

ВСТУП

Конспект лекцій з освітнього компонента «Оцінка та управління ризиками» призначений для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Кібербезпека» спеціальності F5 (125) «Кібербезпека та захист інформації». Дисципліна є нормативною, викладається в сьомому семестрі в обсязі 5 кредитів ЄКТС і завершується екзаменом. Зміст конспекту повністю відповідає силабусу: дев’ять лекцій відтворюють назви та перелік питань тем двох змістових модулів – «Управління кіберінцидентами» та «Управління ризиками в інформаційній та/або кібербезпеці».

Метою дисципліни є формування у здобувачів системних знань про фундаментальні поняття та закономірності теорії ризиків, принципи побудови алгоритмів оцінювання ризиків у кібербезпеці, основні міжнародні стандарти оцінювання й оброблення ризиків та їх застосування в задачах захисту інформації, а також вмінь застосовувати програмні засоби, що реалізують ці алгоритми.

Методологічною основою конспекту є підручник C. Morales «Cyber Risk Management in Practice: A Guide to Real-World Solutions» (CRC Press, 2025) [1], у якому управління кіберризиками розглянуто як безперервний цикл із п’яти кроків: аналіз контексту та збирання інформації, оцінювання ризиків, вибір стратегій оброблення, комунікація та впровадження рішень, моніторинг і метрики. Положення підручника доповнено вимогами чинних редакцій міжнародних стандартів ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27005:2022, ISO/IEC 27035-1:2023, публікацій NIST (Cybersecurity Framework 2.0, SP 800-61 Rev. 3, SP 800-53 Release 5.2.0), а також нормативних актів України у сфері кіберзахисту.

Кожна лекція викладена як цілісний науковий текст без поділу на підпункти: послідовність викладу відповідає переліку питань теми в силабусі. Лекції містять визначення ключових понять, формалізовані моделі та розрахункові співвідношення, приклади застосування й контрольні питання

для самоперевірки. Окремі нормативні документи, які залишаються чинними, але видані до 2022 року (зокрема ISO 31000:2018, NIST SP 800-30 Rev. 1, NIST SP 800-37 Rev. 2, ISO/IEC 27007:2020), розглядаються в тексті як об’єкти вивчення з точним зазначенням редакції; список літератури сформовано з джерел 2022 року та новіших.

ЛЕКЦІЯ 1. ПОНЯТТЯ КІБЕРІНЦИДЕНТА/КІБЕРАТАКИ

Кібербезпека розглядається як стан захищеності життєво важливих інтересів людини, суспільства та держави в кіберпросторі, за якого забезпечуються сталий розвиток інформаційного суспільства й цифрового середовища, своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз. Об'єктом захисту є інформаційні активи та системи, що їх обробляють, а базовими властивостями, порушення яких становить зміст будь-якої загрози, є конфіденційність, цілісність і доступність інформації (тріада CIA), доповнені автентичністю, підзвітністю та неспростовністю. Відповідно до сучасного підходу, закріпленого в ISO/IEC 27001:2022 та NIST Cybersecurity Framework 2.0 [7; 15], забезпечення кібербезпеки є не набором окремих технічних заходів, а керованим процесом, центральним елементом якого виступає управління ризиками [1].

Закон України «Про основні засади забезпечення кібербезпеки України» розмежовує поняття кібератаки та кіберінциденту. Кібератака – це спрямовані (навмисні) дії в кіберпросторі, що здійснюються за допомогою засобів електронних комунікацій та мають на меті порушення конфіденційності, цілісності чи доступності електронних інформаційних ресурсів, отримання несанкціонованого доступу до них або порушення штатного функціонування систем. Кіберінцидент – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, зокрема внаслідок дії людського фактору) та/або таких, що мають ознаки можливої кібератаки, які становлять загрозу безпеці систем або спричинили порушення штатного режиму їх роботи. Отже, поняття кіберінциденту ширше: кожна успішна кібератака є кіберінцидентом, але не кожен кіберінцидент спричинений атакою. Стандарт ISO/IEC 27035-1:2023 використовує ще дві ступені деталізації: подія інформаційної безпеки – виявлений стан системи, служби чи мережі, що вказує на можливе порушення політики безпеки або збій заходів захисту, та інцидент інформаційної безпеки – одна чи кілька небажаних подій, які мають значну ймовірність скомпрометувати діяльність

організації та загрожують її інформаційній безпеці [12]. Розрізнення події та інциденту має практичне значення: потік подій у сучасній організації вимірюється мільйонами записів на добу, і лише незначна їх частка після аналізу кваліфікується як інцидент.

Класифікація кіберінцидентів виконується за кількома ознаками. За природою виникнення виокремлюють навмисні (зловмисні) та ненавмисні інциденти. За об'єктом впливу – інциденти, що порушують конфіденційність (витік, несанкціоноване розкриття даних), цілісність (несанкціонована модифікація, підміна, знищення) та доступність (відмова в обслуговуванні, шифрування даних програмою-вимагачем). За вектором реалізації розрізняють інциденти, пов'язані зі шкідливим програмним забезпеченням, соціальною інженерією, несанкціонованим доступом, атаками на вебзастосунки, компрометацією облікових записів, атаками на ланцюг постачання, зловживанням привілеями внутрішніми користувачами, фізичним доступом. За рівнем критичності інциденти поділяють, як правило, на чотири–п'ять рівнів (від низького до критичного) з урахуванням масштабу впливу на бізнес-процеси, кількості уражених систем, категорії скомпрометованих даних і регуляторних наслідків. Для об'єктів критичної інформаційної інфраструктури України порядок класифікації та повідомлення про кіберінциденти визначається нормативними актами Кабінету Міністрів України та Адміністрації Держспецзв'язку, а національним координатором реагування є CERT-UA.

До основних типів кібератак, що домінують у сучасному ландшафті загроз, належать такі:

– фішинг і цільовий фішинг (spear phishing), зокрема з використанням генеративного штучного інтелекту для створення переконливих повідомлень, голосових і відеодипфейків;

– атаки програм-вимагачів (ransomware) за моделлю подвійного вимагання, коли дані одночасно шифруються та викрадаються для подальшого шантажу;

– розподілені атаки на відмову в обслуговуванні (DDoS), що реалізуються з бот-мереж, зокрема з уражених IoT-пристроїв;

– експлуатація вразливостей загальнодоступних застосунків і периметрових пристроїв (VPN-шлюзів, міжмережевих екранів), у тому числі вразливостей нульового дня;

– атаки на ланцюг постачання програмного забезпечення та послуг, за яких зловмисник компрометує постачальника, щоб отримати доступ до його клієнтів;

– компрометація облікових даних (credential stuffing, підбір паролів, крадіжка сесійних токенів) та обхід багатофакторної автентифікації;

– атаки «людина посередині» (man-in-the-middle) та перехоплення трафіку;

– атаки на вебзастосунки (ін’єкції, міжсайтовий скриптинг, порушення контролю доступу).

За даними звіту ENISA Threat Landscape 2025, що охоплює період з липня 2024 до червня 2025 року, фішинг залишався основним вектором первинного проникнення, а найбільш руйнівною загрозою для організацій були програми-вимагачі; одночасно зросла роль зловмисного використання систем штучного інтелекту для соціальної інженерії [24].

Джерелом кіберзагрози є суб’єкт або чинник, здатний реалізувати загрозу. Прийнято виокремлювати такі категорії порушників: державні та спонсоровані державою угруповання (APT-групи), що мають найвищі ресурси й ведуть тривалі цілеспрямовані кампанії; кіберзлочинні угруповання з фінансовою мотивацією, зокрема ті, що працюють за моделлю «вимагач як послуга» (RaaS); хактивісти з ідеологічною мотивацією; внутрішні порушники (інсайдери) – як зловмисні, так і недбалі працівники; конкуренти, які здійснюють промислове шпигунство; а також ненавмисні джерела – збої обладнання, помилки персоналу, природні та техногенні явища. Для кожного джерела оцінюються мотивація, можливості (ресурси, кваліфікація, інструменти) та наміри щодо конкретної організації; саме ці характеристики

формують модель порушника, яку C. Morales розглядає як обов'язковий елемент моделювання загроз на початковому етапі управління ризиками [1].

Ключові для дисципліни поняття вразливості, загрози та ризику взаємопов'язані. Вразливість – це слабкість активу або заходу захисту, яку може використати одна чи кілька загроз (помилка в програмному коді, некоректна конфігурація, відсутність процедури, недостатня обізнаність персоналу). Публічно відомі вразливості програмного забезпечення реєструються в базі CVE та оцінюються за шкалою CVSS (актуальна версія 4.0), а ймовірність їх експлуатації прогнозується моделлю EPSS. Загроза – потенційна причина небажаного інциденту, який може завдати шкоди системі або організації. Ризик – вплив невизначеності на досягнення цілей; в інформаційній безпеці його виражають як поєднання ймовірності реалізації загрози через вразливість і величини наслідків для активу [11]. Узагальнено ці зв'язки описуються функціональною залежністю

$$R = f(T, V, I) \approx P(T, V) \times I,$$

де R – рівень ризику, T – характеристика загрози, V – вразливість, P – імовірність успішної реалізації загрози, I – величина наслідків (впливу). Відсутність будь-якого з компонентів (загрози, вразливості або цінного активу) означає відсутність ризику, що є теоретичним обґрунтуванням трьох груп заходів: усунення вразливостей, протидії джерелам загроз і зменшення наслідків.

Ознаки компрометації інформаційних систем поділяють на два класи. Передвісники (precursors) свідчать про можливий інцидент у майбутньому: сканування портів, розвідувальні запити до сервісів, публікація експлойта для вразливості, наявної в інфраструктурі, погрози з боку угруповань. Індикатори свідчать про інцидент, що вже відбувається або відбувся. Технічні індикатори компрометації (Indicators of Compromise, IoC) – це хеш-значення шкідливих файлів, IP-адреси та доменні імена командних серверів, URL-адреси, ключі реєстру, імена процесів, характерні рядки в мережевому трафіку. Поряд з ними застосовують індикатори атаки (Indicators of Attack, IoA), що описують не артефакти, а поведінку: запуск інтерпретатора команд офісним

застосунком, масове шифрування файлів, нетипове звернення до процесу LSASS, аномальні обсяги вихідного трафіку. Модель «піраміди болю» (Pyramid of Pain) показує, що блокування атомарних індикаторів (хешів, IP-адрес) мало впливає на порушника, тоді як виявлення його тактик, технік і процедур (TTP) змушує змінювати весь інструментарій, тому сучасні системи виявлення орієнтуються саме на поведінкові ознаки.

Життєвий цикл кібератаки описується формалізованими моделями. Модель Cyber Kill Chain включає сім послідовних стадій: розвідка, озброєння (підготовка шкідливого навантаження), доставка, експлуатація, встановлення, встановлення каналу управління (C2) та дії відповідно до цілей. Модель корисна тим, що переривання ланцюга на будь-якій стадії зриває атаку, а отже, заходи захисту доцільно розподіляти по всіх стадіях. Детальнішою є база знань MITRE ATT&CK, у матриці Enterprise якої виокремлено чотирнадцять тактик – від розвідки (Reconnaissance) і підготовки ресурсів (Resource Development) через первинний доступ, виконання, закріплення, підвищення привілеїв, ухилення від захисту, доступ до облікових даних, дослідження середовища, бокове переміщення, збирання даних і управління до ексфільтрації (Exfiltration) та деструктивного впливу (Impact). Кожна тактика деталізується техніками й підтехніками з описом процедур реальних угруповань, способів виявлення та протидії. ATT&CK використовується як спільна мова для аналітиків розвідки загроз, команд реагування та ризик-менеджерів: сценарій ризику, описаний послідовністю технік, піддається і кількісному оцінюванню, і перевірці покриття заходами захисту [1].

Основні принципи виявлення та запобігання кіберінцидентам випливають з наведених моделей. Принцип глибокого ешелонування (defense in depth) передбачає кілька незалежних рубежів захисту, так що відмова одного не призводить до компрометації. Принцип найменших привілеїв обмежує права користувачів і процесів мінімально необхідними. Архітектура нульової довіри (Zero Trust) відмовляється від неявної довіри до внутрішньої мережі й вимагає перевірки кожного запиту доступу. Безперервний моніторинг із централізованим збором журналів (SIEM), засобами виявлення та реагування

на кінцевих точках (EDR/XDR) і мережевим моніторингом забезпечує скорочення середнього часу виявлення (MTTD). Управління вразливостями з пріоритизацією за критичністю, імовірністю експлуатації та цінністю активу зменшує площу атаки. Нарешті, підвищення обізнаності персоналу знижує ефективність соціальної інженерії, яка залишається найпоширенішим вектором первинного доступу. CSF 2.0 узагальнює ці принципи в шести функціях – Govern, Identify, Protect, Detect, Respond, Recover, – де превентивні заходи (Protect) доповнюються здатністю швидко виявляти (Detect), реагувати (Respond) та відновлюватися (Recover) [15].

Контрольні питання

1. Чим відрізняються поняття «кібератака» та «кіберінцидент» за законодавством України?
2. Як співвідносяться поняття «подія інформаційної безпеки» та «інцидент інформаційної безпеки» за ISO/IEC 27035-1:2023?
3. За якими ознаками класифікують кіберінциденти?
4. Охарактеризуйте основні категорії джерел кіберзагроз та їх мотивацію.
5. Поясніть зв’язок між вразливістю, загрозою та ризиком.
6. Чим індикатори компрометації відрізняються від індикаторів атаки?
7. Порівняйте моделі Cyber Kill Chain та MITRE ATT&CK.
8. Які принципи лежать в основі виявлення та запобігання кіберінцидентам?

ЛЕКЦІЯ 2. РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ/КІБЕРАТАК

Розслідування кіберінциденту – це систематична діяльність зі встановлення фактичних обставин події: що сталося, коли, яким чином, які активи уражено, хто є ймовірним джерелом, яких наслідків завдано та яких заходів слід вжити для недопущення повторення. Основними завданнями розслідування є встановлення факту та масштабу компрометації, відновлення хронології дій порушника, визначення первинного вектора проникнення та використаних вразливостей, оцінювання збитків і порушених вимог законодавства, збирання доказів, придатних для внутрішніх процедур, страхових вимог або кримінального провадження, а також формування рекомендацій щодо вдосконалення системи захисту. Розслідування є складовою процесу управління інцидентами за ISO/IEC 27035-1:2023 та функції Respond у NIST CSF 2.0, зокрема категорії аналізу інцидентів (RS.AN), що охоплює встановлення першопричини, збереження цілісності даних розслідування та оцінювання масштабу [12; 17].

Етапи розслідування кібератак узгоджуються з фазами управління інцидентами. На етапі підготовки організація заздалегідь визначає склад команди реагування, повноваження, інструментарій, політику журналювання (які події, де і скільки часу зберігаються), процедури взаємодії з правоохоронними органами та CERT-UA. Етап виявлення та первинної оцінки починається з сигналу (спрацювання засобу захисту, повідомлення користувача, повідомлення від зовнішньої сторони) і завершується рішенням про кваліфікацію події як інциденту. Далі виконуються стримування з одночасним збиранням і збереженням доказів, поглиблений аналіз, усунення причин, відновлення та післяінцидентний аналіз. Принциповою вимогою є те, щоб дії зі стримування не знищували доказів: наприклад, вимкнення живлення ураженого сервера ліквідує вміст оперативної пам’яті, де можуть міститися ключі шифрування, мережеві з’єднання та код безфайлового шкідливого ПЗ.

Виявлення, реєстрація та класифікація інциденту є відправними точками розслідування. Кожен інцидент реєструється в журналі (реєстрі) інцидентів або в платформі реагування з присвоєнням унікального ідентифікатора; фіксуються час виявлення, джерело інформації, перелік уражених активів, первинні спостереження, особа, відповідальна за обробку. Класифікація визначає тип інциденту (шкідливе ПЗ, несанкціонований доступ, витік даних, відмова в обслуговуванні тощо) і рівень критичності, від якого залежать пріоритет, склад залучених ресурсів, строки реагування та обов'язки щодо зовнішнього повідомлення. Регламенти ЄС, зокрема директива NIS2, встановлюють для суттєвих інцидентів раннє попередження протягом 24 годин, повідомлення протягом 72 годин і фінальний звіт протягом місяця [22]; аналогічні процедури інформування CERT-UA діють для суб'єктів забезпечення кібербезпеки в Україні.

Збирання та збереження цифрових доказів підпорядковується принципам допустимості, достовірності, повноти та відтворюваності. Збирання ведеться в порядку зменшення мінливості даних: спочатку реєстри та кеш процесора, потім оперативна пам'ять, таблиці маршрутизації та ARP, перелік процесів і мережевих з'єднань, далі тимчасові файли, дані на дисках, віддалені журнали, архівні носії. Сучасна практика передбачає обов'язкове зняття образу оперативної пам'яті до вимкнення системи, оскільки повнодискове шифрування робить дані на диску недоступними після вимкнення, а частина шкідливих програм не залишає файлів на диску. Образи носіїв створюються побітово з використанням апаратних або програмних блокувальників запису, а їх цілісність підтверджується криптографічними хеш-функціями. Як допоміжні застосовуються функції сімейства SHA-2 (SHA-256 і вище); застарілі MD5 та SHA-1 через наявність практичних колізій не можуть бути єдиним засобом підтвердження цілісності. Кожне переміщення доказу документується в ланцюгу зберігання (chain of custody): хто, коли, з якою метою отримав доступ до носія і яким було хеш-значення. Для твердотільних накопичувачів слід ураховувати, що механізми TRIM і збирання сміття можуть безповоротно знищувати видалені дані вже після вилучення носія,

тому образ слід створювати якнайшвидше. Для хмарних середовищ докази збирають через інтерфейси провайдера (знімки віртуальних дисків, журнали аудиту API), а відповідні можливості мають бути передбачені договором заздалегідь.

Аналіз журналів подій операційних систем і мережевого обладнання є основним джерелом відновлення хронології. В ОС Windows ключовими є журнали Security, System, PowerShell та Sysmon. До подій, що найчастіше аналізуються, належать: 4624 і 4625 – успішний і невдалий вхід у систему (із зазначенням типу входу), 4672 – призначення спеціальних привілеїв, 4688 – створення процесу, 4720 – створення облікового запису, 4698 – створення запланованого завдання, 7045 – встановлення служби, 1102 – очищення журналу аудиту, що саме по собі є сильним індикатором зловмисної діяльності. Sysmon доповнює ці дані подіями створення процесу з хешем і командним рядком (подія 1), мережевими з'єднаннями (подія 3), завантаженням драйверів і модулів. У Linux аналізують журнали автентифікації (auth.log або secure), системний журнал journald, журнали аудиту auditd, історію командних оболонок, cron-завдання. Мережеве обладнання та засоби захисту (міжмережеві екрани, VPN-шлюзи, проксі-сервери, DNS-сервери) надають журнали з'єднань і запитів, що дозволяють встановити зовнішні адреси порушника, канали управління та обсяги переданих даних. Обов'язковою передумовою коректного аналізу є синхронізація часу всіх джерел (NTP) і зберігання журналів у централізованій системі, недоступній для модифікації порушником.

Аналіз мережевого трафіку виконується на двох рівнях. Аналіз метаданих потоків (NetFlow/IPFIX) дозволяє виявити аномалії обсягів, нетипові напрямки з'єднань, періодичні звернення шкідливої програми до командного сервера (beaconing) і ексфільтрацію даних без доступу до вмісту пакетів. Повний захоплений трафік (PCAP), що аналізується засобами Wireshark, Zeek, Suricata, дає змогу відновити сеанси, виокремити передані файли, виявити сигнатури експлойтів. Зростання частки зашифрованого трафіку (TLS 1.3, QUIC) обмежує аналіз вмісту, тому особливого значення набувають аналіз

DNS-запитів, сертифікатів, відбитків TLS-клієнтів (JA3/JA4) та статистичних характеристик потоків.

Визначення джерел і причин інциденту передбачає встановлення первинного вектора проникнення (фішинговий лист, експлуатація вразливості, скомпрометований обліковий запис постачальника), технік закріплення та переміщення, а також першопричини – того організаційного чи технічного недоліку, що уможливив атаку (відсутність оновлення, слабка автентифікація, надмірні привілеї, відсутність сегментації). Результати зіставляються з тактиками й техніками MITRE ATT&CK, що дозволяє оцінити повноту реконструкції атаки та порівняти її з відомими кампаніями. Атрибуція – встановлення конкретного угруповання – є складною задачею, що спирається на сукупність технічних і контекстних ознак, і в більшості корпоративних розслідувань обмежується віднесенням до кластера активності, а не до персоніфікованого виконавця.

Цифрова криміналістика (Digital Forensics) – прикладна наука про виявлення, збирання, дослідження та подання цифрових доказів. Її основними напрямами є криміналістика носіїв інформації, криміналістика оперативної пам’яті, мережева, мобільна та хмарна криміналістика. Методологічно вона спирається на принцип обміну Локара (будь-яка взаємодія залишає сліди), вимогу роботи лише з копіями доказів і відтворюваність результатів. Інструментальну базу становлять засоби створення образів (FTK Imager, dd/dc3dd), аналізу файлових систем і артефактів (Autopsy, The Sleuth Kit), аналізу пам’яті (Volatility 3), швидкого збирання артефактів і масштабного розслідування на багатьох вузлах (KAPE, Velociraptor), побудови суперхронології (plaso). Аналіз артефактів Windows включає реєстр, журнали, Prefetch, Amcache, ShimCache, LNK-файли, списки нещодавно відкритих документів, що разом дозволяють довести факт запуску програм і доступу до файлів. У кримінальному провадженні в Україні результати технічного дослідження набувають доказового значення через процедури, передбачені кримінальним процесуальним законодавством, зокрема через комп’ютерно-технічну експертизу.

Документування результатів розслідування здійснюється безперервно з першої хвилини: кожна дія фіксується з часом, виконавцем і результатом. Підсумковий звіт містить резюме для керівництва (суть інциденту, наслідки, ключові рішення), технічний опис із хронологією, перелік уражених активів і скомпрометованих даних, використані індикатори та техніки, оцінку збитків, опис вжитих заходів, висновки щодо першопричини та рекомендації. Звіт має бути зрозумілим для двох аудиторій: технічних фахівців, яким потрібна відтворюваність, і менеджменту, якому потрібна підстава для управлінських рішень.

Розроблення рекомендацій щодо запобігання повторним інцидентам є завершальним і найважливішим з погляду управління ризиками кроком. Рекомендації поділяються на негайні (закриття вразливості, зміна облікових даних, блокування індикаторів), середньострокові (посилення автентифікації, сегментація мережі, вдосконалення моніторингу) та стратегічні (зміни в політиках, навчанні персоналу, архітектурі). Кожна рекомендація пов’язується з відповідним ризиком у реєстрі ризиків, отримує відповідального й строк виконання. NIST SP 800-61 Rev. 3 підкреслює, що уроки інцидентів повинні надходити в категорію вдосконалення (ID.IM) функції Identify, тобто безпосередньо змінювати оцінку ризиків і план їх оброблення [17]. Так розслідування замикає цикл управління ризиками: фактичний інцидент є найбільш достовірним свідченням про реальні ймовірності та наслідки загроз [1].

Контрольні питання

1. Назвіть основні завдання розслідування кіберінцидентів.

2. Опишіть етапи розслідування кібератаки та їх зв’язок із фазами управління інцидентами.

3. Що включає реєстрація та класифікація інциденту?

4. Сформулюйте принцип порядку мінливості та поясніть, чому оперативну пам’ять слід збирати до вимкнення системи.

5. Що таке ланцюг зберігання доказів і як підтверджується цілісність образів носіїв?

6. Які події журналів Windows найважливіші для розслідування?

7. Які можливості та обмеження має аналіз зашифрованого мережевого трафіку?

8. Яку структуру має звіт за результатами розслідування?

ЛЕКЦІЯ 3. УПРАВЛІННЯ РИЗИКАМИ В ІНФОРМАЦІЙНІЙ ТА/АБО КІБЕРБЕЗПЕЦІ

Поняття ризику в загальній теорії управління визначено стандартом ISO 31000:2018 як вплив невизначеності на цілі, причому вплив може бути як негативним, так і позитивним. В інформаційній безпеці розглядається переважно негативний аспект: ризик інформаційної безпеки – це можливість того, що певна загроза використає вразливість активу або групи активів і тим самим завдасть шкоди організації. ISO/IEC 27005:2022 наголошує, що ризик інформаційної безпеки пов’язаний з утратою конфіденційності, цілісності та доступності інформації в межах сфери застосування системи управління інформаційною безпекою та характеризується через ризикові сценарії, наслідки й імовірність [11]. C. Morales розглядає кіберризик як бізнес-ризик, що виникає внаслідок використання інформаційних технологій, і підкреслює, що управляти ним можна лише тоді, коли він описаний мовою наслідків для бізнес-цілей, а не мовою технічних недоліків [1].

Основними складовими ризику є актив (те, що має цінність для організації), загроза (потенційна причина небажаної події), вразливість (слабкість, через яку загроза може реалізуватися), існуючі заходи захисту (контролі, що знижують імовірність або наслідки), імовірність реалізації сценарію та наслідки. Структурною одиницею аналізу в сучасних стандартах є ризиковий сценарій – опис послідовності подій, у якій джерело загрози через певну вразливість впливає на актив і спричиняє визначені наслідки. Наприклад: «кіберзлочинна група через фішинговий лист отримує облікові дані працівника бухгалтерії, проникає в мережу, що не сегментована, і шифрує сервер фінансової системи, спричиняючи зупинку розрахунків на п’ять робочих днів». Сценарний опис робить оцінку відтворюваною і дозволяє пов’язати кожен ризик із конкретними заходами.

Класифікація ризиків інформаційної та кібербезпеки здійснюється за низкою ознак. За джерелом розрізняють ризики, пов’язані з навмисними діями зовнішніх порушників, з діями внутрішніх порушників, з помилками

персоналу, з технічними збоями, з природними і техногенними подіями, з діяльністю третіх сторін і постачальників. За порушеною властивістю – ризики конфіденційності, цілісності та доступності. За характером наслідків – фінансові, операційні, юридичні (регуляторні), репутаційні, стратегічні, ризики для безпеки життєдіяльності. За рівнем управління – стратегічні (рівень організації), процесні (рівень бізнес-процесів) та системні (рівень інформаційних систем). Окремо виокремлюють ризики ланцюга постачання, ризики хмарних сервісів і ризики нових технологій, зокрема систем штучного інтелекту, яким C. Morales присвячує окремий розділ підручника [1; 20].

Ідентифікація інформаційних активів є першим практичним кроком оцінювання. Розрізняють первинні активи – інформацію та бізнес-процеси, що мають безпосередню цінність, – і допоміжні (підтримувальні) активи, від яких залежать первинні: апаратне та програмне забезпечення, мережі, персонал, приміщення, постачальники послуг. Для кожного активу визначають власника, місце розташування, залежності та цінність, що виражається через наслідки порушення конфіденційності, цілісності й доступності. Результатом є реєстр (інвентар) активів, ведення якого прямо вимагається ISO/IEC 27001:2022 (захід 5.9). Ідентифікація загроз спирається на каталоги загроз (додатки ISO/IEC 27005:2022, каталог ENISA), дані розвідки загроз, звіти про інциденти в галузі та модель порушника; для кожного активу визначаються релевантні джерела загроз і їх можливі дії.

Виявлення вразливостей інформаційних систем здійснюється комбінацією методів: автоматизованим скануванням вразливостей мереж і застосунків, аналізом конфігурацій щодо еталонних профілів безпеки (наприклад, CIS Benchmarks), тестуванням на проникнення, аналізом вихідного коду, аудитом процесів і опитуванням персоналу. Для технічних вразливостей застосовується шкала CVSS v4.0, яка оцінює базову критичність, а для пріоритизації додатково враховують імовірність експлуатації (EPSS), наявність у каталозі активно експлуатованих вразливостей (CISA KEV) та критичність ураженого активу. Організаційні вразливості – відсутність

процедур, нечіткий розподіл відповідальності, недостатнє навчання – виявляються переважно методами аудиту.

Методи оцінювання ризиків поділяються на якісні, кількісні та напівкількісні. Якісні методи використовують порядкові шкали («низький», «середній», «високий») для ймовірності та наслідків; вони швидкі, не потребують статистичних даних і зрозумілі керівництву, але суб'єктивні та погано придатні для порівняння ризиків з вартістю заходів. Напівкількісні методи приписують рівням шкал числові бали (наприклад, від 1 до 5) і обчислюють рівень ризику як добуток балів. Кількісні методи виражають імовірність через частоту або розподіл імовірностей, а наслідки – у грошових одиницях. Класичною кількісною моделлю є модель очікуваних річних втрат:

$$SLE = AV \times EF; \quad ALE = SLE \times ARO,$$

де AV (Asset Value) – вартість активу; EF (Exposure Factor) – частка вартості, що втрачається при одиничному інциденті (від 0 до 1); SLE (Single Loss Expectancy) – очікувані втрати від одиничного інциденту; ARO (Annualized Rate of Occurrence) – очікувана кількість інцидентів за рік; ALE (Annualized Loss Expectancy) – очікувані річні втрати. Нехай вартість бази даних клієнтів AV = 2 000 000 грн, EF = 0,4, ARO = 0,5. Тоді SLE = 800 000 грн, ALE = 400 000 грн. Якщо запровадження заходу вартістю 120 000 грн на рік зменшує ARO до 0,1, то ALE після заходу дорівнює 80 000 грн, а чиста річна вигода становить 400 000 − 80 000 − 120 000 = 200 000 грн. Показник повернення інвестицій у безпеку обчислюється як

$$ROSI = (ALE_0 - ALE_1 - C) / C,$$

де C – річна вартість заходу; у прикладі ROSI ≈ 1,67, тобто захід економічно виправданий.

Модель ALE має обмеження: вона оперує точковими оцінками й не відображає невизначеності. Сучасним розвитком кількісного підходу є модель FAIR (Factor Analysis of Information Risk), у якій ризик визначається як імовірнісно розподілена величина майбутніх втрат:

$$Risk = LEF \times LM; \quad LEF = TEF \times Vuln,$$

де LEF – частота подій втрат, TEF – частота подій загрози, Vuln – імовірність того, що подія загрози перетвориться на подію втрат, LM – величина втрат (первинних і вторинних). Кожен параметр задається діапазоном (мінімум, найбільш імовірне значення, максимум), а розподіл річних втрат отримується методом Монте-Карло. Результат подається кривою перевищення втрат (loss exceedance curve), що показує ймовірність перевищення будь-якої суми збитків за рік. D. Hubbard і R. Seiersen доводять, що навіть калібровані експертні оцінки, оброблені статистично, дають кращі рішення, ніж порядкові шкали [4]; C. Morales розглядає перехід до кількісної оцінки як етап зрілості, до якого організація рухається після запровадження стабільного якісного процесу [1].

Визначення ймовірності реалізації загроз ґрунтується на статистиці власних інцидентів, галузевих даних, характеристиках порушника (мотивація, можливості), доступності вразливості (експлуатованість, наявність публічного експлойта) та ефективності наявних заходів. Можливі наслідки оцінюються за кількома вимірами: прямі фінансові втрати, витрати на відновлення та розслідування, втрачений дохід від простою, штрафи та компенсації, втрата репутації та клієнтів, вплив на безпеку людей. Для кожного виміру організація визначає критерії, що пов’язують якісні рівні з кількісними межами: наприклад, «критичні наслідки» – збитки понад 5 % річного бюджету або простій ключового процесу понад 72 години.

Матриця ризиків є інструментом візуалізації та ранжування ризиків у координатах «імовірність – наслідки». У напівкількісній матриці 5×5 рівень ризику обчислюється як добуток балів імовірності та наслідків і відноситься до одного з рівнів, наприклад: 1–4 – низький, 5–9 – середній, 10–16 – високий, 20–25 – критичний. Приклад шкал наведено в таблиці 3.1.

Таблиця 3.1 – Напівкількісна матриця ризиків 5×5

Імовірність \ Наслідки	**1 Незначні**	**2 Помірні**	**3 Суттєві**	**4 Значні**	**5 Критичні**
5 Майже напевно	5	10	15	20	25
4 Імовірно	4	8	12	16	20
3 Можливо	3	6	9	12	15
2 Малоймовірно	2	4	6	8	10

Імовірність \ Наслідки	**1 Незначні**	**2 Помірні**	**3 Суттєві**	**4 Значні**	**5 Критичні**
1 Рідко	1	2	3	4	5

Матриці ризиків поширені завдяки наочності, проте мають відомі вади: обмежену роздільну здатність, ефект стиснення діапазону (ризики з різницею в збитках на порядки потрапляють в одну клітинку), неоднозначність при негативно корельованих оцінках. Тому для рішень щодо значних інвестицій матрицю доповнюють кількісними розрахунками [4].

Пріоритизація ризиків полягає в упорядкуванні їх за рівнем і порівнянні з критеріями прийнятності. Ризики, що перевищують ризик-апетит організації, підлягають обов'язковому обробленню; серед них першочергово обробляються ті, що мають найвищий рівень і найбільший вплив на критичні бізнес-процеси. Додатковими критеріями пріоритету є швидкість настання (velocity) ризику, взаємозалежність ризиків і наявність регуляторних вимог.

Основними способами оброблення ризиків за ISO/IEC 27005:2022 є модифікація ризику (запровадження або вдосконалення заходів, що зменшують імовірність чи наслідки), збереження (свідоме прийняття ризику за умови відповідності критеріям прийнятності), уникнення (відмова від діяльності чи технології, що породжує ризик) і розподіл (передача частини наслідків третій стороні через страхування кіберризиків, аутсорсинг, договірні зобов'язання) [11]. Для кожного ризику може застосовуватися комбінація способів; при цьому відповідальність за результат не може бути повністю передана третій стороні.

Моніторинг та перегляд ризиків забезпечують актуальність оцінок у динамічному середовищі. Ризики переглядаються планово (щонайменше щороку та за графіком, визначеним критеріями), а також позапланово – у разі значних змін у бізнесі, інфраструктурі, ландшафті загроз, після серйозних інцидентів і змін законодавства. Для моніторингу використовують ключові індикатори ризику (KRI), які сигналізують про зростання ризику до його реалізації: частка систем без критичних оновлень, середній час усунення критичних вразливостей, кількість облікових записів із надмірними

привілеями, частка працівників, що відкрили тестовий фішинговий лист. C. Morales виокремлює моніторинг і метрики як самостійний п’ятий крок циклу, що замикає процес і повертає його до перегляду контексту [1].

Контрольні питання

1. Дайте визначення ризику інформаційної безпеки та назвіть його складові.

2. Що таке ризиковий сценарій і чому він є одиницею аналізу в ISO/IEC 27005:2022?

3. За якими ознаками класифікують ризики інформаційної та кібербезпеки?

4. Чим первинні активи відрізняються від допоміжних?

5. Порівняйте якісні, напівкількісні та кількісні методи оцінювання ризиків.

6. Розрахуйте SLE, ALE і ROSI для власного прикладу.

7. Опишіть модель FAIR та роль методу Монте-Карло в кількісному оцінюванні.

8. Які обмеження має матриця ризиків?

9. Назвіть способи оброблення ризиків і наведіть приклади.

ЛЕКЦІЯ 4. ЗАГАЛЬНА КОНЦЕПЦІЯ УПРАВЛІННЯ РИЗИКАМИ ІБ

Управління ризиками інформаційної безпеки – це скоординована діяльність зі спрямування та контролю організації щодо ризиків, пов’язаних з інформацією та інформаційними системами. Його метою є не усунення всіх ризиків, що неможливо й економічно недоцільно, а утримання їх у межах, визначених ризик-апетитом організації, за оптимальних витрат. Основні завдання управління ризиками полягають у створенні обґрунтованої основи для рішень щодо інвестицій у безпеку, забезпеченні відповідності вимогам законодавства й стандартів, захисті цінності організації, підвищенні її стійкості до інцидентів та формуванні спільного розуміння ризиків між технічними фахівцями й керівництвом.

Загальні принципи управління ризиками сформульовано в ISO 31000:2018, який є методологічною основою для всіх галузевих стандартів, зокрема ISO/IEC 27005:2022. Стандарт визначає вісім принципів: управління ризиками має бути інтегрованим у всі види діяльності організації; структурованим і всеосяжним; адаптованим до зовнішнього та внутрішнього контексту; інклюзивним, тобто враховувати погляди зацікавлених сторін; динамічним, реагуючи на зміни; спиратися на найкращу доступну інформацію; враховувати людські та культурні чинники; забезпечувати постійне вдосконалення. Ці принципи реалізуються через структуру (framework), ядром якої є лідерство та зобов’язання керівництва, а складовими – інтеграція, проєктування, впровадження, оцінювання та вдосконалення. C. Morales окремо наголошує на ролі управління (governance) та культури кібербезпеки: формальний процес без підтримки керівництва та без культури, в якій працівники повідомляють про ризики, вироджується в паперову процедуру [1].

Життєвий цикл управління ризиками інформаційної безпеки за ISO/IEC 27005:2022 включає встановлення контексту, оцінювання ризиків (ідентифікація, аналіз, оцінювання), оброблення ризиків, а також процеси, що супроводжують цикл безперервно, – комунікацію та консультування,

документування та звітування, моніторинг і перегляд. Стандарт підкреслює ітеративний характер процесу: якщо результати оцінювання недостатні для рішень, проводиться повторна, більш детальна ітерація; якщо після оброблення залишковий ризик неприйнятний, цикл повторюється з іншими варіантами оброблення [11]. Стандарт також розмежовує стратегічний цикл, що охоплює організацію в цілому, і операційні цикли для окремих систем і проєктів. У підручнику C. Morales цей самий цикл подано як п’ять практичних кроків: аналіз контекстів і збирання інформації; оцінювання ризиків від ідентифікації до характеристики; стратегії оброблення; комунікація та впровадження; моніторинг і метрики [1].

Визначення контексту та критеріїв ризику є фундаментом усього процесу. Зовнішній контекст охоплює законодавче та регуляторне середовище, галузеві вимоги, ландшафт загроз, очікування клієнтів і партнерів. Внутрішній контекст – цілі та стратегію організації, бізнес-процеси, організаційну структуру, інформаційну архітектуру, культуру, наявні ресурси та зобов’язання. Визначається також сфера застосування процесу – межі організації, процесів і систем, які він охоплює. Критерії ризику включають критерії наслідків (шкали з описом рівнів шкоди), критерії імовірності, метод визначення рівня ризику, критерії оцінювання (порівняння з прийнятним рівнем) та критерії прийняття ризику. Критерії затверджуються керівництвом і мають бути стабільними, оскільки саме вони забезпечують порівнюваність результатів повторних оцінювань.

Формування реєстру ризиків є способом документування та контролю всього процесу. Реєстр ризиків – це структурований перелік ризиків, що для кожного містить ідентифікатор, опис ризикового сценарію, уражені активи та процеси, джерело загрози і вразливість, власника ризику, наявні заходи, оцінки імовірності, наслідків і рівня властивого (inherent) ризику, рішення щодо оброблення, заплановані заходи з відповідальними та строками, оцінку залишкового ризику, дату останнього перегляду та статус. C. Morales розглядає реєстр ризиків як центральний робочий інструмент методології, що

пов’язує оцінювання, оброблення та звітування, і рекомендує вести його в єдиному форматі для всієї організації [1].

Поняття прийнятного та залишкового ризику пов’язані з ризик-апетитом і ризик-толерантністю. Ризик-апетит – це обсяг і тип ризику, який організація готова прийняти для досягнення своїх цілей; ризик-толерантність – допустиме відхилення від цього рівня для конкретних цілей чи категорій ризику. Прийнятний ризик – ризик, рівень якого не перевищує встановлених критеріїв прийняття. Залишковий ризик – ризик, що залишається після оброблення. Його величину можна наближено подати як

$$Rзал = Rвл \times (1 - Ек),$$

де Rвл – властивий ризик (без урахування заходів), Ек – сукупна ефективність заходів захисту (від 0 до 1). Залишковий ризик ніколи не дорівнює нулю; ISO/IEC 27001:2022 (п. 6.1.3) вимагає, щоб план оброблення ризиків і прийняття залишкових ризиків були затверджені власниками ризиків [7].

Розроблення плану оброблення ризиків передбачає вибір для кожного ризику, що перевищує критерії, способу оброблення та конкретних заходів. План містить перелік заходів, пріоритети, відповідальних, необхідні ресурси, строки, очікуваний рівень залишкового ризику та показники, за якими перевірятиметься результат. Для організацій, що впроваджують ISO/IEC 27001, складовою результату є Заява про застосовність (Statement of Applicability), яка містить перелік необхідних заходів, обґрунтування їх включення чи виключення та статус упровадження. Обов’язковою є звірка обраних заходів із переліком додатка A ISO/IEC 27001:2022, щоб жоден необхідний захід не був пропущений.

Вибір організаційних і технічних заходів захисту здійснюється з урахуванням їх ефективності щодо конкретних сценаріїв, вартості впровадження та супроводження, впливу на бізнес-процеси та сумісності з наявною інфраструктурою. ISO/IEC 27002:2022 групує 93 заходи в чотири теми: організаційні (37), людські (8), фізичні (14) та технологічні (34), і для кожного вказує атрибути – тип заходу (запобіжний, виявляючий, коригувальний), властивості безпеки, концепції кібербезпеки за функціями

Identify–Protect–Detect–Respond–Recover, операційні можливості та домени безпеки [10]. Атрибути дозволяють перевірити, чи збалансований набір заходів: наприклад, чи не обмежується захист лише запобіжними засобами без можливостей виявлення та відновлення. До організаційних заходів належать політики, процедури, розподіл обов'язків, управління постачальниками, навчання; до технічних – засоби автентифікації та контролю доступу, шифрування, сегментація мереж, резервне копіювання, засоби моніторингу та виявлення.

Розподіл відповідальності за управління ризиками ґрунтується на принципі, що кожен ризик має власника – особу з повноваженнями та підзвітністю за управління ним, як правило, керівника відповідного бізнес-процесу. Поширеною є модель трьох ліній: перша лінія (операційні підрозділи) володіє ризиками та управляє ними; друга (функції ризик-менеджменту, інформаційної безпеки, комплаєнсу) розробляє методологію, здійснює нагляд і консультування; третя (внутрішній аудит) надає незалежне підтвердження ефективності. Для деталізації ролей у конкретних процесах застосовують матрицю RACI (Responsible – виконує, Accountable – відповідає за результат, Consulted – консультує, Informed – інформується). Загальну підзвітність за кіберризики несе вище керівництво; CSF 2.0 закріплює це окремою функцією Govern, що охоплює контекст організації, стратегію управління ризиками, ролі та повноваження, політику, нагляд і управління ризиками ланцюга постачання [15].

Документування та контроль ризиків забезпечують відтворюваність і підзвітність процесу. Документуються методологія та критерії, результати кожного оцінювання, реєстр ризиків, план оброблення, рішення про прийняття ризиків, звіти для керівництва. Контроль здійснюється через регулярне звітування власників ризиків, моніторинг ключових індикаторів ризику, внутрішні аудити та аналіз з боку керівництва. Звіт про ризики для вищого керівництва має бути стислим: перелік найсуттєвіших ризиків, їх динаміка, стан виконання плану оброблення, ризики, що потребують рішення.

Основні положення ISO/IEC 27005:2022 та ISO 31000 узагальнюються так. ISO 31000:2018 є загальним стандартом настанов щодо управління будь-якими ризиками й визначає принципи, структуру та процес. ISO/IEC 27005:2022 (четверта редакція, жовтень 2022 р.) адаптує ці настанови до інформаційної безпеки й призначений для підтримки вимог ISO/IEC 27001:2022 щодо оцінювання та оброблення ризиків. У редакції 2022 року термінологію та структуру узгоджено з ISO 31000 і ISO/IEC 27001:2022, запроваджено поняття ризикового сценарію, описано два підходи до ідентифікації ризиків – на основі подій (event-based), що аналізує сценарії на стратегічному рівні, та на основі активів (asset-based), що деталізує загрози та вразливості окремих активів, – а також розширено додатки прикладами критеріїв, шкал і каталогів загроз [11]. Стандарт не встановлює єдиної методики, а надає настанови, що дозволяють організації обрати методику, адекватну її розміру та зрілості. Сертифікація на відповідність ISO/IEC 27005 не передбачена; вона застосовується як методична основа для виконання вимог п. 6.1.2, 6.1.3, 8.2 та 8.3 ISO/IEC 27001:2022.

Контрольні питання

1. Сформулюйте мету та завдання управління ризиками інформаційної безпеки.

2. Назвіть принципи управління ризиками за ISO 31000:2018.

3. Опишіть життєвий цикл управління ризиками за ISO/IEC 27005:2022.

4. Що входить до зовнішнього та внутрішнього контексту, які критерії ризику визначаються?

5. Які поля має містити реєстр ризиків?

6. Розмежуйте поняття ризик-апетиту, прийнятного й залишкового ризику.

7. Що містить план оброблення ризиків і Заява про застосовність?

8. Як групуються заходи в ISO/IEC 27002:2022 і для чого використовуються атрибути заходів?

9. Поясніть модель трьох ліній і матрицю RACI.

10. Які зміни внесено в ISO/IEC 27005 у редакції 2022 року?

ЛЕКЦІЯ 5. NIST SP 800x

Національний інститут стандартів і технологій США (NIST) розробляє документи з кібербезпеки у двох основних серіях: федеральні стандарти обробки інформації FIPS, обов'язкові для федеральних органів США, та спеціальні публікації серії SP 800 (Special Publications 800), що мають характер рекомендацій. Призначення серії SP 800 полягає в наданні узгодженого, детального та технологічно нейтрального методичного апарату для управління безпекою інформаційних систем. Обов'язковість цих документів для федеральних агентств випливає із закону FISMA (Federal Information Security Modernization Act, 2014), однак завдяки відкритості, безкоштовній доступності, єдиній термінології та регулярному оновленню вони стали фактичним міжнародним еталоном і широко застосовуються приватними організаціями та державними структурами інших країн, зокрема України. Зв'язок між документами серії утворює цілісну систему: SP 800-39 визначає організаційний рівень управління ризиками, SP 800-37 – процес (Risk Management Framework), SP 800-30 – методику оцінювання ризиків, SP 800-53 і SP 800-53B – каталог заходів та базові набори, SP 800-53A – процедури оцінювання заходів, SP 800-137 – безперервний моніторинг, SP 800-61 – реагування на інциденти, SP 800-161 – управління ризиками ланцюга постачання [18–20]. Над ними як рамковий документ для організацій будь-якого типу стоїть Cybersecurity Framework 2.0 (лютий 2024 р.) [15; 16].

Основні положення NIST SP 800-30 Rev. 1 «Guide for Conducting Risk Assessments» (2012) стосуються методики оцінювання ризиків, яка застосовується на всіх трьох рівнях управління – організації, місії (бізнес-процесів) та інформаційних систем. Документ визначає модель ризику, що містить фактори ризику та зв'язки між ними: джерело загрози з характеристиками можливостей, намірів і цілеспрямованості ініціює подію загрози; подія використовує вразливість з урахуванням передумов (predisposing conditions); у разі успіху вона спричиняє негативний вплив; ризик визначається як поєднання ймовірності та впливу. Імовірність

оцінюється в три кроки: імовірність ініціювання (для навмисних загроз) або виникнення (для ненавмисних) події загрози; імовірність того, що ініційована подія спричинить негативний вплив з урахуванням вразливостей і наявних заходів; загальна імовірність як поєднання обох оцінок. SP 800-30 описує три аналітичні підходи – орієнтований на загрози, орієнтований на активи (наслідки) та орієнтований на вразливості, – а також підходи до оцінювання: кількісний, якісний і напівкількісний. Для напівкількісного оцінювання використовуються п’ятирівневі шкали з числовими діапазонами: дуже високий (96–100), високий (80–95), помірний (21–79), низький (5–20), дуже низький (0–4). Процес оцінювання складається з чотирьох кроків: підготовка до оцінювання (мета, обсяг, припущення та обмеження, джерела інформації, модель ризику й аналітичний підхід); проведення оцінювання (ідентифікація джерел і подій загроз, вразливостей і передумов, визначення ймовірності, величини впливу та ризику); повідомлення результатів; підтримання оцінювання в актуальному стані. Документ також привертає увагу до явища зсуву загроз (threat shifting) – зміни порушником тактики чи цілі у відповідь на запроваджені заходи – та до агрегування ризиків, коли кілька прийнятних поодинці ризиків нижчого рівня утворюють неприйнятний сукупний ризик для організації.

NIST SP 800-37 Rev. 2 «Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy» (2018) визначає концепцію Risk Management Framework (RMF) – дисциплінований, структурований і гнучкий процес управління ризиками безпеки та приватності, інтегрований у життєвий цикл систем. RMF складається з семи кроків. На кроці підготовки (Prepare) на рівні організації визначаються ролі, стратегія управління ризиками та ризик-толерантність, проводиться оцінювання ризиків організаційного рівня, визначаються загальні (успадковувані) заходи та стратегія безперервного моніторингу; на рівні системи – бізнес-функції, зацікавлені сторони, активи, межа авторизації, типи інформації та вимоги безпеки. На кроці категоризації (Categorize) система та інформація категоризуються за потенційним впливом утрати

конфіденційності, цілісності й доступності; федеральні системи категоризуються за FIPS 199 з рівнями низький, помірний або високий за принципом максимуму (high water mark). На кроці вибору (Select) обирається базовий набір заходів із SP 800-53B відповідно до категорії та адаптується (tailoring) з урахуванням оцінки ризику. На кроці впровадження (Implement) заходи реалізуються й документуються в плані безпеки. На кроці оцінювання (Assess) незалежний оцінювач за процедурами SP 800-53A перевіряє, чи правильно реалізовано заходи, чи функціонують вони як задумано і чи забезпечують бажаний результат; недоліки фіксуються в плані дій і контрольних точок (POA&M). На кроці авторизації (Authorize) уповноважена посадова особа на основі пакета авторизації ухвалює рішення про прийнятність ризику експлуатації системи. На кроці моніторингу (Monitor) здійснюється безперервне спостереження за змінами в системі та середовищі, повторне оцінювання заходів, звітування про стан безпеки й, зрештою, виведення системи з експлуатації. Ревізія 2 інтегрувала в RMF управління приватністю й ризиками ланцюга постачання та встановила відповідність між завданнями RMF і категоріями Cybersecurity Framework. В Україні аналогічну логіку допуску системи до експлуатації за результатами оцінювання залишкових ризиків реалізує Порядок авторизації з безпеки, затверджений постановою Кабінету Міністрів України від 18.06.2025 № 712 [25].

Каталог заходів безпеки NIST SP 800-53 Rev. 5 «Security and Privacy Controls for Information Systems and Organizations» є найповнішим відкритим переліком заходів захисту. Заходи згруповано у 20 сімейств: управління доступом (AC), обізнаність і навчання (AT), аудит і підзвітність (AU), оцінювання, авторизація та моніторинг (CA), управління конфігурацією (CM), планування безперервності (CP), ідентифікація та автентифікація (IA), реагування на інциденти (IR), обслуговування (MA), захист носіїв (MP), фізичний захист і захист середовища (PE), планування (PL), управління програмою (PM), безпека персоналу (PS), обробка персональних даних і прозорість (PT), оцінювання ризиків (RA), придбання систем і послуг (SA), захист систем і комунікацій (SC), цілісність систем та інформації (SI),

управління ризиками ланцюга постачання (SR). Кожен захід містить формулювання вимоги, настанови, посилання та, за потреби, посилення (control enhancements). Принциповими особливостями п’ятої ревізії є орієнтація на результат (заходи сформульовано без прив’язки до суб’єкта виконання, що дозволяє застосовувати їх до будь-яких організацій), інтеграція заходів приватності та винесення базових наборів у окремий документ SP 800-53B. У серпні 2025 року NIST випустив оновлення Release 5.2.0, яке посилило вимоги до безпечного й надійного розгортання оновлень і виправлень програмного забезпечення, зокрема додавши нові заходи SA-15(13), SA-24 і SI-02(07) та відповідні процедури оцінювання в SP 800-53A [18; 19]. Каталог має офіційні відповідності (mappings) з ISO/IEC 27001:2022 і CSF 2.0 і доступний у машиночитаному форматі OSCAL, що дозволяє автоматизувати перевірку відповідності. Українським аналогом каталогу є Каталог заходів із кіберзахисту, затверджений наказом Адміністрації Держспецзв’язку від 30.01.2026 № 75 [26].

Управління кіберінцидентами відповідно до NIST SP 800-61 зазнало принципових змін. Попередня редакція Rev. 2 (2012) описувала життєвий цикл реагування з чотирьох фаз: підготовка; виявлення та аналіз; стримування, усунення та відновлення; післяінцидентна діяльність. У квітні 2025 року її замінено редакцією Rev. 3 «Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile» [17]. Нова редакція розглядає реагування на інциденти як невід’ємну частину управління кіберризиками й описує його через шість функцій CSF 2.0. Функції Govern, Identify та Protect відповідають за підготовку: політики та ролі реагування, управління активами й ризиками, захисні заходи, що зменшують імовірність і вплив інцидентів. Функція Detect охоплює виявлення та аналіз аномалій і подій; Respond – управління інцидентом, аналіз, звітування й комунікацію, стримування та усунення; Recover – виконання плану відновлення та комунікацію щодо відновлення. Уроки інцидентів спрямовуються до категорії вдосконалення (ID.IM) функції

Identify. Документ подано як профіль спільноти CSF 2.0, тобто як набір пріоритетних результатів для організацій, а не як жорстку процедуру.

Основи реагування на кіберінциденти, сформульовані в SP 800-61 Rev. 3 та ISO/IEC 27035-1:2023, зводяться до кількох положень. Організація повинна мати затверджену політику й план реагування з чітко визначеними ролями та повноваженнями, зокрема правом ухвалювати рішення про відключення систем. Команда реагування (CSIRT) має бути забезпечена інструментами, доступом до журналів і контактами внутрішніх і зовнішніх сторін. Події мають бути класифіковані за пріоритетом з урахуванням функціонального впливу, впливу на інформацію та складності відновлення. Стратегія стримування обирається з урахуванням потреби у збереженні доказів, доступності сервісів, необхідних ресурсів і тривалості дії. Комунікація з керівництвом, працівниками, клієнтами, регуляторами та правоохоронними органами здійснюється за заздалегідь визначеними правилами. Після інциденту обов’язково проводиться аналіз уроків з оновленням оцінки ризиків і заходів.

Визначення рівнів ризику та вибір заходів захисту в логіці NIST поєднують результати SP 800-30 і каталог SP 800-53. Рівень ризику, отриманий для кожного сценарію, порівнюється з ризик-толерантністю, визначеною на кроці Prepare. Для систем, ризики яких перевищують толерантність, базовий набір заходів адаптується: додаються посилення заходів, що протидіють найбільш імовірним технікам порушника, або компенсувальні заходи там, де базовий захід неможливо реалізувати. Пріоритизація заходів враховує їх внесок у зниження ризику на одиницю витрат. Наприклад, для сценарію компрометації облікових записів адміністраторів доцільними є посилення IA-2(1) (багатофакторна автентифікація для привілейованих облікових записів), AC-6 (мінімальні привілеї), AU-6 (аналіз журналів аудиту) та SI-4 (моніторинг системи), що разом зменшують і ймовірність, і наслідки сценарію.

Практичне застосування рекомендацій NIST для забезпечення кібербезпеки інформаційних систем доцільно будувати через профілі CSF 2.0.

Організація формує поточний профіль (Current Profile) – опис фактично досягнутих результатів за 22 категоріями і 106 підкатегоріями CSF – та цільовий профіль (Target Profile), що відображає бажаний стан з урахуванням ризиків і вимог. Різниця між профілями є переліком прогалин, для закриття яких з каталогу SP 800-53 обираються заходи, а план дій формується з урахуванням пріоритету ризиків. Рівні (Tiers) CSF – частковий, поінформований про ризики, повторюваний, адаптивний – характеризують зрілість управління ризиками в організації. Для невеликих організацій NIST підготував короткі посібники швидкого старту, а для оцінювання програм безперервного моніторингу – SP 800-137A. C. Morales наводить NIST CSF і RMF серед ключових фреймворків, які практик має вміти поєднувати з ISO/IEC 27001 і ISO 31000, використовуючи кожен за його сильною стороною: ISO – для побудови системи управління та сертифікації, NIST – для детального каталогу заходів і процедур їх оцінювання [1].

Таблиця 5.1 – Взаємозв'язок основних публікацій NIST з управління ризиками

Документ	**Призначення**	**Актуальна редакція**
CSF 2.0 (CSWP 29)	Рамковий опис результатів кібербезпеки (6 функцій)	2024
SP 800-39	Управління ризиками на рівні організації	2011
SP 800-37	Risk Management Framework, 7 кроків	Rev. 2, 2018
SP 800-30	Методика оцінювання ризиків	Rev. 1, 2012
SP 800-53 / 53B	Каталог заходів і базові набори	Rev. 5, Release 5.2.0, 2025
SP 800-53A	Процедури оцінювання заходів	Rev. 5, 2022 (Release 5.2.0, 2025)
SP 800-61	Реагування на інциденти	Rev. 3, 2025
SP 800-137 / 137A	Безперервний моніторинг та його оцінювання	2011 / 2020
SP 800-161	Ризики ланцюга постачання	Rev. 1, 2022

Контрольні питання

1. Яке призначення серії NIST SP 800 і як пов'язані між собою її основні документи?

2. Опишіть модель ризику та чотири кроки оцінювання за SP 800-30 Rev. 1.

3. Що таке зсув загроз і агрегування ризиків?

4. Назвіть сім кроків RMF за SP 800-37 Rev. 2 та результат кожного.

5. Як здійснюється категоризація систем за FIPS 199?

6. Які сімейства заходів містить SP 800-53 Rev. 5? Що змінено в Release 5.2.0?

7. Чим SP 800-61 Rev. 3 відрізняється від Rev. 2?

8. Як використовуються поточний і цільовий профілі CSF 2.0 для вибору заходів?

ЛЕКЦІЯ 6. СИСТЕМИ КЛАСУ INCIDENT RESPONSE PLATFORM

Зростання кількості подій безпеки та складності атак зробило ручне реагування на інциденти за допомогою електронної пошти, таблиць і текстових документів неефективним: інформація розпорошується, втрачається хронологія дій, неможливо контролювати строки й відтворювати рішення. Платформа реагування на інциденти (Incident Response Platform, IRP) – це програмний комплекс, що забезпечує централізоване управління інцидентами інформаційної безпеки протягом усього їх життєвого циклу, спільну роботу аналітиків, накопичення знань та автоматизацію рутинних операцій. Призначення IRP полягає в скороченні часу реагування, підвищенні відтворюваності та якості обробки інцидентів, забезпеченні доказовості дій і формуванні даних для управління ризиками. У термінах CSF 2.0 IRP підтримує функцію Respond (управління інцидентами, аналіз, звітування та комунікація, стримування) і частково Detect [15; 17].

Основні функції IRP охоплюють приймання та агрегацію сповіщень (alerts) від засобів виявлення; створення інцидентів (кейсів) на основі сповіщень чи вручну; управління спостережуваними об’єктами (observables) – IP-адресами, доменами, хешами, обліковими записами – з автоматичним збагаченням даними розвідки загроз; управління завданнями, призначенням виконавців і строками; ведення хронології та журналу дій; зберігання артефактів і доказів; шаблони обробки типових інцидентів; базу знань; звітність і метрики; розмежування доступу та роботу з кількома організаціями (для провайдерів послуг безпеки); інтеграцію з зовнішніми системами через програмний інтерфейс. Ключовими метриками ефективності, які обчислює IRP, є середній час виявлення (MTTD), середній час підтвердження (MTTA), середній час стримування (MTTC) та середній час усунення або відновлення (MTTR), а також кількість інцидентів за типами й рівнями критичності та частка хибних спрацювань.

Реєстрація, класифікація та пріоритизація інцидентів в IRP формалізуються. Під час реєстрації кожному кейсу присвоюються

ідентифікатор, назва, опис, джерело, час виявлення, перелік спостережуваних об’єктів та уражених активів. Класифікація здійснюється за таксономією, прийнятою в організації (наприклад, за типами шкідливого ПЗ, фішингу, несанкціонованого доступу, витоку даних), та за тактиками і техніками MITRE ATT&CK. Пріоритет визначається як функція критичності загрози та критичності ураженого активу; поширеним є підхід, коли пріоритет P обчислюється за матрицею «серйозність × критичність активу» з кількома рівнями (від P1 – критичний, реагування негайно, до P4 – низький). Для обміну інформацією про інцидент із зовнішніми сторонами застосовують протокол Traffic Light Protocol 2.0 (TLP:CLEAR, TLP:GREEN, TLP:AMBER, TLP:AMBER+STRICT, TLP:RED), що визначає межі поширення відомостей, та протокол PAP, що регламентує допустимі дії з індикаторами.

Управління життєвим циклом інцидентів в IRP реалізується через статуси кейсу: новий, у роботі (розслідування), стримування, усунення, відновлення, закритий – з фіксацією результату закриття (підтверджений інцидент, хибне спрацювання, дублікат, інцидент без наслідків). Перехід між статусами контролюється правилами, а для кожного статусу визначаються обов’язкові завдання. Так забезпечується відповідність фактичного процесу фазам ISO/IEC 27035-1:2023: планування й підготовка, виявлення та звітування, оцінювання й рішення, реагування, отримання уроків [12]. Закриття кейсу вимагає заповнення підсумкових полів – першопричини, уражених активів, ужитих заходів, рекомендацій, – які потім використовуються для оновлення реєстру ризиків.

Інтеграція IRP із системами SIEM, EDR та засобами моніторингу є необхідною умовою ефективності. Система управління інформацією та подіями безпеки (SIEM) збирає й корелює журнали подій з усієї інфраструктури та генерує сповіщення, які передаються до IRP; засоби виявлення й реагування на кінцевих точках (EDR/XDR) надають детальну телеметрію про процеси, файли й мережеві з’єднання та дозволяють віддалено ізолювати вузол, завершити процес чи зібрати артефакти; мережеві системи виявлення вторгнень і засоби аналізу трафіку надають мережевий

контекст. Платформи розвідки загроз (зокрема MISP) збагачують спостережувані об’єкти відомостями про їх належність до відомих кампаній. Інтеграція забезпечує двосторонній обмін: IRP не лише приймає сповіщення, а й ініціює дії в зовнішніх системах – блокування адреси на міжмережевому екрані, вимкнення облікового запису в службі каталогів, ізоляцію вузла засобом EDR.

Автоматизація процесів реагування спрямована на зменшення навантаження на аналітиків і скорочення часу реагування. Автоматизуються насамперед повторювані дії з низьким ризиком помилки: дедуплікація та групування сповіщень, збагачення спостережуваних об’єктів (перевірка репутації в зовнішніх сервісах, геолокація, запити до систем управління активами), первинна класифікація, сповіщення відповідальних, збирання артефактів з кінцевих точок. Дії, що можуть порушити роботу бізнес-процесів (ізоляція критичного сервера, блокування облікового запису керівника), як правило, виконуються напівавтоматично – після підтвердження аналітиком. Рівень автоматизації має визначатися ризиком: помилкове автоматичне блокування також є ризиковою подією.

Поняття SOAR (Security Orchestration, Automation and Response) об’єднує три групи можливостей: оркестрацію – узгоджену взаємодію різнорідних засобів безпеки через інтеграції; автоматизацію – виконання сценаріїв без участі людини; реагування – управління інцидентами та координацію дій команди. Сучасні IRP і SOAR конвергують: платформи реагування набувають засобів автоматизації, а SOAR-платформи – функцій управління кейсами. Відмінність полягає в акценті: IRP орієнтовані на процес і управління інцидентом, SOAR – на автоматизацію та інтеграцію. До поширених рішень належать комерційні платформи великих виробників засобів захисту та рішення з відкритим кодом або безкоштовними редакціями, зокрема Shuffle як засіб автоматизації робочих процесів.

Використання TheHive та аналогічних платформ розглянемо на прикладі TheHive – однієї з найпоширеніших платформ реагування на інциденти, що розробляється компанією StrangeBee. Поточна п’ята версія поширюється за

комерційною моделлю з безкоштовною ліцензією Community з обмеженою кількістю користувачів і функцій та платними ліцензіями Gold і Platinum; попередні версії 3 і 4 з відкритим кодом більше не підтримуються [27]. TheHive оперує сповіщеннями (alerts), які надходять з SIEM чи інших джерел і можуть бути перетворені на кейси; кейсами з завданнями (tasks) і журналами виконання; спостережуваними об’єктами з позначками IoC; зіставленням з техніками MITRE ATT&CK; шаблонами кейсів. Аналіз спостережуваних об’єктів виконується через рушій Cortex, що містить аналізатори (перевірка репутації, аналіз файлів у пісочниці, запити до сервісів розвідки) і респондери (активні дії: блокування, сповіщення). Інтеграція з MISP забезпечує обмін індикаторами з галузевими спільнотами. Аналогічні функції надають інші платформи управління інцидентами та модулі реагування в складі SIEM-систем. Під час вибору платформи враховують модель ліцензування, підтримку інтеграцій з наявними засобами, можливість розгортання у власній інфраструктурі (важливо для обробки чутливих даних), масштабованість і вимоги законодавства щодо місця зберігання даних.

Формування сценаріїв реагування (Playbooks) є методичною основою як ручного, так і автоматизованого реагування. Плейбук – це формалізований опис дій для певного типу інциденту, що містить умови запуску (тригери), ролі та відповідальних, послідовність кроків із точками ухвалення рішень, критерії ескалації, вимоги до збирання доказів, комунікації та документування, а також критерії закриття. Розрізняють плейбуки високого рівня (процедурні, для людей) і ранбуки (технічні послідовності команд, придатні до автоматизації). Наприклад, плейбук обробки повідомлення про фішинг передбачає: отримання листа та його заголовків; вилучення URL-адрес, вкладень і адрес відправника як спостережуваних об’єктів; автоматичну перевірку їх репутації та аналіз вкладень у пісочниці; пошук аналогічних листів у поштових скриньках організації; за підтвердження зловмисності – видалення листів, блокування індикаторів, перевірку факту переходу користувачів за посиланням і, за необхідності, скидання їх облікових даних; сповіщення користувачів; закриття кейсу з фіксацією

результату. Плейбуки розробляються на основі ризикових сценаріїв з реєстру ризиків, перевіряються під час навчань (table-top exercises) і переглядаються після кожного значного інциденту [1; 17].

Документування та аналіз результатів реагування на інциденти завершують цикл. Платформа зберігає повну хронологію дій із зазначенням виконавців і часу, що забезпечує доказовість і можливість зовнішнього аудиту. На основі закритих кейсів формуються звіти для керівництва, аналіз тенденцій (найчастіші типи інцидентів, уражені активи, вектори проникнення), оцінка ефективності заходів і процесу реагування за метриками MTTD/MTTR. Ці дані є найбільш достовірним джерелом інформації про фактичну частоту подій загроз і величину втрат, тому вони безпосередньо використовуються для калібрування оцінок імовірності та наслідків у реєстрі ризиків і для обґрунтування інвестицій у засоби захисту [4].

Контрольні питання

1. Що таке Incident Response Platform і яке її призначення?
2. Назвіть основні функції IRP та метрики, які вона обчислює.
3. Як здійснюється пріоритизація інцидентів? Для чого використовується TLP 2.0?
4. Опишіть статуси життєвого циклу інциденту в IRP.
5. Яка роль SIEM, EDR і MISP у роботі платформи реагування?
6. Які дії доцільно автоматизувати, а які залишати під контролем аналітика?
7. Чим відрізняються IRP та SOAR?
8. Опишіть архітектуру TheHive та роль Cortex.
9. Які елементи має містити плейбук? Наведіть приклад.

ЛЕКЦІЯ 7. ЕТАПИ ПРОВЕДЕННЯ АУДИТУ. АУДИТ НА ОСНОВІ АНАЛІЗУ РИЗИКІВ

Аудит інформаційної безпеки – це систематичний, незалежний і документований процес отримання аудиторських доказів та їх об’єктивного оцінювання з метою визначення ступеня виконання критеріїв аудиту. Критеріями виступають вимоги законодавства, міжнародних і національних стандартів, договірні зобов’язання, внутрішні політики та процедури організації. Призначення аудиту полягає в наданні зацікавленим сторонам – керівництву, власникам, регуляторам, клієнтам – обґрунтованої впевненості в тому, що система захисту інформації відповідає вимогам і ефективно управляє ризиками, а також у виявленні недоліків до того, як ними скористається порушник. Загальні принципи аудиту систем управління встановлено стандартом ISO 19011:2018, а їх застосування до систем управління інформаційною безпекою – стандартом ISO/IEC 27007:2020; вимоги до органів, що здійснюють сертифікаційний аудит, визначає ISO/IEC 27006-1:2024 [13].

Основними цілями аудиту є оцінювання відповідності системи захисту встановленим критеріям, оцінювання ефективності заходів захисту щодо актуальних ризиків, виявлення вразливостей і невідповідностей, перевірка виконання раніше наданих рекомендацій, а також підготовка до сертифікації чи регуляторної перевірки. Завданнями аудиту є визначення обсягу та критеріїв перевірки, збирання доказів, їх аналіз і порівняння з критеріями, формулювання висновків щодо відповідності й ефективності та надання рекомендацій. Аудит ґрунтується на принципах доброчесності, об’єктивного подання результатів, належної професійної ретельності, конфіденційності, незалежності аудиторів від перевірюваної діяльності та підходу, заснованого на доказах і ризиках.

Види аудиту інформаційних систем розрізняють за кількома ознаками. За суб’єктом проведення виокремлюють аудит першої сторони (внутрішній, який організація проводить сама або доручає зовнішнім фахівцям від свого

імені), другої сторони (аудит постачальника замовником) і третьої сторони (незалежний, зокрема сертифікаційний). Слід наголосити, що внутрішній аудит є обов'язковою вимогою ISO/IEC 27001:2022 (п. 9.2), а умовою його достовірності є об'єктивність і неупередженість аудиторів, а не їх зовнішність щодо організації [7]. За предметом розрізняють аудит відповідності (compliance audit), що перевіряє виконання вимог, аудит ефективності, що оцінює досягнення результатів, технічний аудит (аналіз захищеності, сканування вразливостей, тестування на проникнення, аналіз конфігурацій) та аудит процесів управління. За періодичністю – плановий і позаплановий (після інциденту, суттєвих змін, на вимогу регулятора). За методологією – аудит на основі стандартів, аудит на основі аналізу ризиків і аудит на основі експертних досліджень.

Планування та підготовка аудиту починаються з формування програми аудитів – сукупності перевірок на певний період, спрямованих на досягнення визначеної мети. Для кожного конкретного аудиту визначаються мета, обсяг (організаційні підрозділи, процеси, локації, системи, період), критерії, склад аудиторської групи з урахуванням компетентності та незалежності, ресурси, графік і план аудиту. Планування включає попередній аналіз документації (політик, реєстру ризиків, Заяви про застосовність, звітів попередніх аудитів, статистики інцидентів), що дозволяє зосередити увагу на найбільш ризикованих сферах. На етапі підготовки розробляються робочі документи – контрольні переліки, опитувальники, плани вибірки, – погоджується доступ до систем і персоналу та порядок проведення технічних перевірок, щоб вони не порушили роботу виробничих систем.

Визначення об'єктів і критеріїв аудиту має забезпечити однозначність висновків. Об'єктами аудиту можуть бути система управління інформаційною безпекою в цілому, окремі процеси (управління доступом, управління змінами, реагування на інциденти, резервне копіювання), інформаційні системи та інфраструктура, постачальники послуг. Критерії мають бути перевірюваними: формулювання на кшталт «доступ надається належним чином» замінюється вимогою «права доступу надаються лише на

підставі погодженої заявки власника ресурсу та переглядаються щонайменше раз на квартал».

Збирання та аналіз аудиторських доказів здійснюються методами вивчення документів, інтерв'ювання, спостереження за виконанням процедур, повторного виконання (reperformance) контрольних операцій, технічного тестування та аналізу даних. Аудиторські докази мають бути достатніми (за кількістю) і належними (за якістю – релевантними та достовірними). Достовірність доказів зростає, якщо вони отримані з незалежного джерела, безпосередньо аудитором, у документальній формі та з автоматизованих систем, а не лише з усних пояснень. Оскільки перевірити всю сукупність операцій неможливо, застосовується вибірка – статистична або на основі судження, – і висновок поширюється на сукупність з урахуванням ризику вибірки. Сучасною практикою є застосування аналітики даних до повних масивів журналів (наприклад, перевірка всіх облікових записів на відповідність кадровим даним), що зменшує залежність від вибірки.

Оцінювання ризиків інформаційної безпеки в аудиті відіграє подвійну роль. По-перше, аудитор перевіряє, чи організація сама належним чином оцінює й обробляє ризики: чи визначено критерії, чи є реєстр ризиків, чи узгоджено план оброблення з результатами оцінювання, чи затверджено залишкові ризики власниками. По-друге, аудитор використовує власне оцінювання ризиків для планування перевірки. Аудит на основі аналізу ризиків (risk-based audit) розподіляє аудиторські ресурси пропорційно до рівня ризику: спочатку формується «аудиторський всесвіт» – перелік усіх потенційних об'єктів аудиту, – кожен об'єкт оцінюється за властивим ризиком і якістю заходів контролю, після чого найбільш ризиковані об'єкти перевіряються частіше та глибше. Модель аудиторського ризику, поширена в практиці ISACA та фінансового аудиту, подає ризик хибного висновку як добуток:

$$AR = IR \times CR \times DR,$$

де AR – аудиторський ризик (імовірність того, що аудитор не виявить суттєвого недоліку), IR – властивий ризик об'єкта, CR – ризик того, що

контролі організації не запобіжать недоліку й не виявлять його, DR – ризик невиявлення аудиторськими процедурами. За заданого прийнятного AR чим вищі IR і CR, тим нижчим має бути DR, тобто тим більш обсяжними й детальними мають бути процедури перевірки. Глобальні стандарти внутрішнього аудиту IIA, що набули чинності в 2025 році, також вимагають ризик-орієнтованого планування діяльності внутрішнього аудиту.

Визначення критичних інформаційних активів є складовою ризик-орієнтованого підходу. Критичними вважаються активи, порушення безпеки яких призводить до неприйнятних наслідків для ключових бізнес-процесів, а також активи, що підлягають особливому правовому режиму (персональні дані, інформація з обмеженим доступом, об'єкти критичної інфраструктури). Аудитор перевіряє повноту реєстру активів, коректність визначення їх власників і цінності, а також відповідність рівня захисту критичності: наприклад, чи застосовано до найкритичніших систем посилену автентифікацію, сегментацію, резервування та моніторинг.

Виявлення недоліків системи захисту ґрунтується на порівнянні фактичного стану (умови) з критерієм. Кожна знахідка описується за структурою: критерій (що мало бути), умова (що встановлено), причина (чому виникла розбіжність), наслідок (який ризик це створює) і рекомендація. Знахідки класифікують за значущістю – відповідно до рівня ризику, який вони створюють, – що дозволяє керівництву визначити пріоритети. Типовими недоліками є відсутність або неактуальність оцінки ризиків, невідповідність прав доступу посадовим обов'язкам, неусунені критичні вразливості, відсутність перевірки відновлення з резервних копій, недостатнє журналювання та моніторинг, відсутність контролю постачальників.

Формування аудиторського звіту завершує основний етап аудиту. Звіт містить резюме для керівництва з загальним висновком, мету, обсяг, критерії та період аудиту, методологію та обмеження, опис знахідок із класифікацією за значущістю, висновки щодо відповідності та ефективності, рекомендації, а також, як правило, відповіді керівництва перевірюваного підрозділу з планом коригувальних дій. Висновки мають бути обґрунтовані доказами, а

формулювання – однозначними. Звіт обговорюється з перевірюваною стороною на заключній нараді до його затвердження.

Розроблення рекомендацій щодо зменшення ризиків є найціннішим для організації результатом аудиту. Рекомендації мають бути конкретними, реалістичними, спрямованими на першопричину, а не на симптом, і пов'язаними з ризиками з реєстру. Для кожної рекомендації визначається відповідальний, строк і очікуваний ефект у вигляді зниження рівня ризику. Аудитор не впроваджує рекомендації сам, щоб зберегти незалежність; натомість на етапі подальшого контролю (follow-up) він перевіряє виконання коригувальних дій і їх результативність. C. Morales підкреслює, що результати аудиту повинні надходити безпосередньо в цикл управління ризиками як нова інформація для переоцінювання, а не залишатися окремим документом [1].

Контрольні питання

1. Дайте визначення аудиту інформаційної безпеки та назвіть його принципи.

2. Які стандарти регламентують аудит систем управління інформаційною безпекою?

3. Класифікуйте види аудиту інформаційних систем.

4. Що включає планування та підготовка аудиту?

5. Які вимоги висуваються до аудиторських доказів? Як застосовується вибірка?

6. У чому полягає аудит на основі аналізу ризиків? Поясніть модель аудиторського ризику.

7. Опишіть структуру аудиторської знахідки.

8. Що містить аудиторський звіт і як контролюється виконання рекомендацій?

ЛЕКЦІЯ 8. АУДИТ НА ОСНОВІ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (ІБ). АУДИТ НА ОСНОВІ ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ ІНФОРМАЦІЙНИХ СИСТЕМ (ІС). ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕС-ПРОЦЕСІВ: ПОНЯТТЯ БІЗНЕС-ПРОЦЕСУ. МОДЕЛЬ БІЗНЕС-ПРОЦЕСУ

Стандартизований аудит інформаційної безпеки – це аудит, критеріями якого є вимоги визнаних міжнародних або національних стандартів, а процедури проведення також регламентовані стандартами. Його перевагами є об’єктивність і відтворюваність результатів, порівнюваність між організаціями й у часі, зрозумілість для зовнішніх сторін і можливість сертифікації. Обмеженням є те, що відповідність стандарту не гарантує достатньої захищеності від конкретних загроз: стандарт задає мінімально необхідну структуру, а її наповнення має визначатися ризиками організації. Тому стандартизований аудит доцільно поєднувати з ризик-орієнтованим підходом і технічними перевірками [5; 6].

Міжнародні та національні стандарти у сфері захисту інформації утворюють кілька груп. Серію ISO/IEC 27000 становлять ISO/IEC 27000 (огляд і словник), ISO/IEC 27001:2022 (вимоги до системи управління інформаційною безпекою, СУІБ), ISO/IEC 27002:2022 (настанови щодо заходів), ISO/IEC 27005:2022 (управління ризиками), ISO/IEC 27007:2020 (настанови з аудиту СУІБ), ISO/IEC 27006-1:2024 (вимоги до органів аудиту та сертифікації), ISO/IEC 27035 (управління інцидентами), галузеві стандарти для хмарних сервісів (27017, 27018) і приватності (27701). Із системою управління безперервністю пов’язаний ISO 22301:2019 зі змінами 2024 року [14]. Окрему групу становлять фреймворки NIST (CSF 2.0, SP 800-53), галузеві стандарти (PCI DSS v4.0.1 для платіжних карток) та регуляторні акти ЄС – директива NIS2 і регламент DORA для фінансового сектору [22; 23]. В Україні ISO/IEC 27001:2022 прийнято як національний стандарт ДСТУ ISO/IEC 27001:2023 [9]; вимоги до захисту державних інформаційних ресурсів і об’єктів критичної інфраструктури визначаються законодавством

про кіберзахист і нормативними документами системи технічного захисту інформації.

Основні положення ISO/IEC 27001 та ISO/IEC 27002 є головним змістом стандартизованого аудиту. ISO/IEC 27001:2022 побудований за гармонізованою структурою стандартів систем управління й містить обов'язкові вимоги в розділах 4–10: контекст організації (зовнішні й внутрішні чинники, зацікавлені сторони, сфера застосування СУІБ), лідерство (зобов'язання керівництва, політика, ролі), планування (дії щодо ризиків і можливостей, оцінювання та оброблення ризиків, цілі інформаційної безпеки, планування змін), підтримка (ресурси, компетентність, обізнаність, комунікація, документована інформація), функціонування (операційне планування, оцінювання та оброблення ризиків), оцінювання результативності (моніторинг і вимірювання, внутрішній аудит, аналіз з боку керівництва) та вдосконалення (невідповідності, коригувальні дії, постійне вдосконалення). Додаток А містить 93 заходи, згруповані в чотири теми; зміна 1:2024 доповнила стандарт вимогою враховувати зміну клімату як чинник контексту [7; 8]. ISO/IEC 27002:2022 розкриває кожен захід додатка А: мету, настанови з упровадження та атрибути. Порівняно з редакцією 2013 року додано 11 нових заходів, зокрема розвідку загроз, безпеку використання хмарних сервісів, готовність ІКТ до забезпечення безперервності бізнесу, моніторинг фізичної безпеки, управління конфігурацією, видалення інформації, маскування даних, запобігання витоку даних, моніторинг діяльності, вебфільтрацію та безпечне кодування [10].

Рекомендації ISO/IEC 27007:2020 щодо аудиту систем управління інформаційною безпекою деталізують загальні положення ISO 19011 з урахуванням специфіки СУІБ. Стандарт висуває вимоги до компетентності аудиторів (знання ISO/IEC 27001, методів оцінювання ризиків, технологій і заходів захисту), рекомендує під час планування враховувати результати оцінювання ризиків організації, наголошує на перевірці зв'язку між оцінюванням ризиків, планом оброблення, Заявою про застосовність і фактично впровадженими заходами. Сертифікаційний аудит за ISO/IEC

27006-1:2024 проводиться у два етапи: на першому етапі (stage 1) оцінюються документація і готовність організації, на другому (stage 2) – фактичне впровадження та результативність СУІБ; надалі проводяться щорічні наглядові аудити і повторна сертифікація кожні три роки [13].

Використання NIST Cybersecurity Framework в аудиті доповнює ISO-орієнтований підхід. CSF 2.0 дозволяє оцінити досягнення 106 результатів (підкатегорій) у шести функціях і зрілість управління за чотирма рівнями (Tiers). Аудитор порівнює поточний профіль організації з цільовим або з профілем спільноти для відповідної галузі, а прогалини перетворює на рекомендації. Офіційні відповідності між підкатегоріями CSF, заходами SP 800-53 і ISO/IEC 27001:2022 дають змогу провести один аудит за кількома рамками одночасно [15; 16].

Перевірка відповідності політик і процедур вимогам стандартів виконується на трьох рівнях. На рівні проєктування перевіряється, чи містять документи всі обов’язкові положення: наприклад, чи визначає політика інформаційної безпеки зобов’язання щодо виконання застосовних вимог і постійного вдосконалення, як того вимагає п. 5.2 ISO/IEC 27001:2022. На рівні впровадження – чи виконуються процедури фактично (наявність записів, журналів, підписаних заявок). На рівні результативності – чи досягають процедури своєї мети за визначений період (наприклад, чи всі критичні вразливості усунуто в установлені строки).

Формування контрольних списків аудиту (checklists) є основним методичним інструментом стандартизованого аудиту. Контрольний список містить перелік вимог або заходів, для кожного з яких зазначено посилання на пункт стандарту, питання для перевірки, очікувані докази, метод перевірки та поле для результату. Добре складений контрольний список не обмежується питаннями «так/ні», а спонукає аудитора отримати докази впровадження й результативності. Водночас контрольний список не повинен підміняти професійного судження: аудитор зобов’язаний розглядати й ризики, не охоплені переліком.

Аналіз невідповідностей здійснюється за їх класифікацією. Значна невідповідність – відсутність або системна невиконуваність вимоги стандарту, що ставить під сумнів здатність СУІБ досягати цілей (наприклад, відсутність оцінювання ризиків). Незначна невідповідність – поодиноке або часткове невиконання вимоги, що не порушує системи в цілому. Окремо фіксуються спостереження (потенційні проблеми) та можливості для вдосконалення. Для кожної невідповідності організація проводить аналіз першопричини (методами «5 чому», діаграми Ісікави) та розробляє коригувальні дії, а не лише виправлення наслідку. Методику аналізу прогалин (gap analysis) застосовують під час підготовки до сертифікації: поточний стан порівнюється з кожною вимогою стандарту, а прогалини ранжуються за ризиком і трудомісткістю усунення.

Документування результатів перевірки здійснюється у звіті, що містить сферу та критерії аудиту, перелік перевірених процесів і вибірок, знахідки з посиланнями на докази та пункти стандарту, класифікацію невідповідностей і загальний висновок про відповідність і результативність СУІБ. Підготовка рекомендацій щодо вдосконалення системи інформаційної безпеки спрямована на усунення першопричин невідповідностей, підвищення зрілості процесів і приведення заходів у відповідність до актуальних ризиків; рекомендації пріоритизуються за значущістю.

Аудит на основі експертних досліджень інформаційних систем застосовується тоді, коли формальних критеріїв недостатньо або коли об’єкт є унікальним: нестандартні архітектури, промислові системи керування, нові технології, оцінювання ймовірностей рідкісних подій. Його основою є судження групи кваліфікованих експертів, отримане за формалізованою процедурою, що зменшує суб’єктивність. Застосовуються методи індивідуального оцінювання (інтерв’ю, анкетування), колективні методи (мозковий штурм, метод номінальної групи) та ітеративні методи з анонімним зворотним зв’язком, зокрема метод Дельфі, за яким експерти в кілька раундів надають оцінки, отримують узагальнені результати й аргументи інших учасників та уточнюють свої оцінки до досягнення узгодженості.

Узгодженість ранжувань m експертів щодо n об’єктів оцінюється коефіцієнтом конкордації Кендалла:

$$W = 12S / (m^2(n^3 - n)),$$

де S – сума квадратів відхилень сум рангів кожного об’єкта від середньої суми рангів. Значення W змінюється від 0 (повна неузгодженість) до 1 (повна узгодженість); як правило, при $W \geq 0,7$ узгодженість вважається високою, а результати – придатними для використання. Для підвищення точності експертних оцінок D. Hubbard і R. Seiersen рекомендують калібрування експертів – тренування оцінювати діапазони так, щоб вони з заданою ймовірністю містили істинне значення [4]. Експертний аудит часто доповнюється технічними дослідженнями: аналізом архітектури, моделюванням загроз за методиками STRIDE чи PASTA, тестуванням на проникнення.

Забезпечення безперервності бізнес-процесів є завданням, у якому управління ризиками інформаційної безпеки поєднується з управлінням операційною стійкістю. C. Morales розглядає побудову кіберстійкості (cyber resilience) як наступний рівень зрілості після впровадження базового процесу управління ризиками: організація має не лише запобігати інцидентам, а й зберігати здатність виконувати критичні функції під час атаки та швидко відновлюватися після неї [1]. ISO/IEC 27001:2022 містить заходи щодо безпеки інформації під час порушень (5.29) та готовності ІКТ до забезпечення безперервності бізнесу (5.30), а ISO 22301 встановлює вимоги до системи управління безперервністю [7; 14].

Поняття бізнес-процесу є вихідним для планування безперервності. Бізнес-процес – це сукупність взаємопов’язаних видів діяльності, що перетворює входи на виходи, які мають цінність для споживача, і виконується з використанням ресурсів під управлінням певних правил. Кожен процес має власника, межі (початкову й кінцеву події), входи та виходи, ресурси (персонал, інформаційні системи, обладнання, приміщення), регламенти та показники результативності. За роллю в організації розрізняють основні процеси, що створюють цінність для зовнішніх споживачів, допоміжні, що

забезпечують основні ресурсами (зокрема IT-процеси), та процеси управління. Залежність бізнес-процесу від інформаційних систем визначає, яким чином кіберінцидент трансформується у бізнес-наслідки.

Модель бізнес-процесу – це формалізований опис процесу, що відображає його структуру, послідовність дій, учасників, інформаційні потоки та ресурси. Формально процес можна подати кортежем

$$BP = \langle I, O, A, R, C, M \rangle,$$

де I – множина входів, O – множина виходів, A – множина дій (функцій) і відношення порядку на ній, R – ресурси, C – керуючі впливи (правила, регламенти), M – механізми виконання (виконавці та системи). Ця структура відповідає нотації функціонального моделювання IDEF0 з її чотирма типами зв'язків (входи, виходи, управління, механізми). Найпоширенішою нотацією моделювання процесів є BPMN 2.0 (стандартизована як ISO/IEC 19510), що використовує події, дії (задачі та підпроцеси), шлюзи для розгалуження й злиття потоків, потоки керування й повідомлень, а також пули й доріжки для позначення учасників. Для IT-систем застосовують також UML-діаграми діяльності, для високорівневого опису – схему SIPOC (постачальники, входи, процес, виходи, споживачі). Модель процесу дозволяє виявити його залежності від інформаційних активів і постачальників, єдині точки відмови та критичні ланки.

На основі моделей бізнес-процесів проводиться аналіз впливу на бізнес (Business Impact Analysis, BIA), який визначає для кожного процесу наслідки його переривання в часі та ключові параметри відновлення: максимально допустимий період порушення (MTPD) – час, після якого наслідки стають неприйнятними; цільовий час відновлення (RTO) – час, за який процес або система мають бути відновлені, причому RTO < MTPD; цільову точку відновлення (RPO) – максимально допустимий обсяг утрати даних, виражений у часі між останньою резервною копією та моментом збою; мінімальний рівень функціонування (MBCO). Ці параметри визначають вимоги до резервного копіювання, резервування інфраструктури, планів відновлення та їх тестування. Так модель бізнес-процесу, аналіз впливу та

оцінювання ризиків утворюють єдину основу для рішень щодо забезпечення безперервності.

Контрольні питання

1. Які переваги та обмеження має стандартизований аудит інформаційної безпеки?

2. Назвіть основні стандарти серії ISO/IEC 27000 та їх призначення.

3. Опишіть структуру вимог ISO/IEC 27001:2022 і додатка А. Які заходи додано в ISO/IEC 27002:2022?

4. Що регламентують ISO/IEC 27007:2020 та ISO/IEC 27006-1:2024?

5. Як використовується CSF 2.0 під час аудиту?

6. Як формуються контрольні списки аудиту та класифікуються невідповідності?

7. Опишіть метод Дельфі та розрахунок коефіцієнта конкордації Кендалла.

8. Дайте визначення бізнес-процесу та назвіть його елементи.

9. Які нотації використовуються для моделювання бізнес-процесів?

10. Поясніть параметри MTPD, RTO, RPO та MBCO.

ЛЕКЦІЯ 9. РОЗРОБКА ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС ЗАБЕЗПЕЧЕННЯ БІЗНЕС-ПРОЦЕСІВ. ДОТРИМАННЯ ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС ЗАБЕЗПЕЧЕННЯ БІЗНЕС-ПРОЦЕСІВ

Політика інформаційної безпеки – це документ, у якому вище керівництво організації формально висловлює свої наміри та напрям діяльності щодо захисту інформації. Призначення політики полягає у визначенні цілей і принципів захисту, встановленні обов'язкових правил поведінки для персоналу й третіх сторін, розподілі відповідальності, створенні основи для вибору заходів і для оцінювання їх виконання. Політика є першим із заходів додатка А ISO/IEC 27001:2022 (захід 5.1 «Політики інформаційної безпеки»), а пункт 5.2 стандарту вимагає, щоб вище керівництво встановило політику, яка відповідає призначенню організації, містить цілі інформаційної безпеки або основу для їх встановлення, зобов'язання виконувати застосовні вимоги та постійно вдосконалювати СУІБ, була доведена до працівників і доступна зацікавленим сторонам [7]. У CSF 2.0 політика належить до функції Govern (категорія GV.PO) [15].

Основні принципи розроблення політик безпеки полягають у такому. Політика має ґрунтуватися на ризиках, тобто відображати результати їх оцінювання й рішення щодо оброблення, а не копіювати шаблон. Вона повинна підтримувати бізнес-цілі, а не перешкоджати їм, тому розробляється за участю власників бізнес-процесів. Політика повинна бути зрозумілою, стислою та однозначною, а вимоги – вимірюваними й перевірюваними. Вона має бути узгодженою з законодавством, договірними зобов'язаннями та іншими внутрішніми документами. Принцип ієрархічності передбачає, що загальні положення закріплюються в політиці верхнього рівня, а деталі – у підпорядкованих документах. Нарешті, політика має бути реалістичною: вимога, яку неможливо виконати наявними ресурсами, руйнує довіру до всієї системи документів. C. Morales наголошує, що ефективність політик визначається культурою кібербезпеки: правила, які персонал вважає

безглуздими, обходять, тоді як пояснені й підтримані керівництвом правила стають частиною повсякденної практики [1].

Структура та зміст політики інформаційної безпеки організації визначаються ієрархією документів. На верхньому рівні знаходиться загальна політика інформаційної безпеки, що містить мету та сферу застосування, цілі, принципи, ролі та відповідальність, посилання на тематичні політики, порядок контролю виконання та відповідальність за порушення, порядок перегляду. Середній рівень становлять тематичні політики (topic-specific policies), які ISO/IEC 27002:2022 рекомендує розробляти для управління доступом, фізичної безпеки, управління активами, передавання інформації, безпечної конфігурації та обробки кінцевих пристроїв, мережевої безпеки, управління інцидентами, резервного копіювання, криптографії та управління ключами, класифікації та обробки інформації, управління технічними вразливостями, безпечної розробки [10]. Нижній рівень утворюють стандарти (обов'язкові технічні вимоги, наприклад параметри паролів чи конфігурацій), процедури (покрокові інструкції) та настанови (рекомендаційні документи). Така структура дозволяє змінювати технічні деталі без перезатвердження політики верхнього рівня.

Визначення вимог до захисту інформаційних активів здійснюється на основі їх класифікації. Схема класифікації встановлює рівні конфіденційності (наприклад, публічна, внутрішня, конфіденційна, з обмеженим доступом), а також вимоги до цілісності й доступності. Для кожного рівня політика визначає правила маркування, зберігання, передавання, копіювання, знищення та допустимі способи обробки. Вимоги до захисту також випливають із законодавства (захист персональних даних, службової інформації, вимоги до об'єктів критичної інфраструктури), договорів і результатів оцінювання ризиків.

Розроблення політики управління доступом спирається на принципи службової необхідності (need-to-know), мінімальних привілеїв і розділення обов'язків. Політика визначає модель розмежування доступу: рольову (RBAC), за якої права надаються ролям відповідно до посадових обов'язків;

атрибутну (ABAC), за якої рішення ухвалюються на основі атрибутів суб'єкта, ресурсу й контексту (час, місце, стан пристрою); мандатну (MAC) для інформації з обмеженим доступом. Вона встановлює процедури надання, зміни та відкликання доступу, періодичного перегляду прав, управління привілейованими обліковими записами, вимоги до автентифікації (зокрема обов'язкову багатофакторну автентифікацію для віддаленого й привілейованого доступу), а також принципи архітектури нульової довіри. Ризик-орієнтований контроль доступу передбачає, що строгість вимог зростає з критичністю ресурсу та ризиковістю контексту запиту.

Політика резервного копіювання визначає перелік даних і систем, що підлягають копіюванню, періодичність і тип копій, строки зберігання, місця зберігання та захист копій (шифрування, ізоляція), а також регулярне тестування відновлення. Параметри політики виводяться з результатів аналізу впливу на бізнес: періодичність копіювання визначається цільовою точкою відновлення RPO, а технологія відновлення – цільовим часом RTO. Поширеним орієнтиром є правило «3-2-1-1-0»: три копії даних, на двох різних типах носіїв, одна поза основним майданчиком, одна незмінна або ізольована від мережі (захист від програм-вимагачів), нуль помилок під час перевірки відновлення.

Політика використання інформаційних ресурсів (правила прийнятного використання) встановлює для працівників правила роботи з корпоративними пристроями, електронною поштою, інтернетом, хмарними сервісами, знімними носіями, особистими пристроями (BYOD), а також із загальнодоступними сервісами генеративного штучного інтелекту, зокрема заборону передавання до них конфіденційної інформації. Політика реагування на інциденти визначає обов'язок кожного працівника повідомляти про підозрілі події, канали повідомлення, повноваження команди реагування, порядок взаємодії з керівництвом, регуляторами, CERT-UA і правоохоронними органами, вимоги до збереження доказів і післяінцидентного аналізу [12; 17].

Врахування ризиків і критичності бізнес-процесів є тим, що відрізняє дієву політику від формальної. Строгість вимог має бути пропорційною ризику: для критичних процесів із низьким RTO встановлюються вимоги до резервування, посиленого моніторингу та частішого перегляду доступу, тоді як для некритичних процесів вимоги можуть бути спрощені. Політика передбачає процедуру винятків: якщо бізнес-процес не може виконати певну вимогу, власник процесу обґрунтовує виняток, оцінюється пов'язаний ризик, визначаються компенсувальні заходи, а рішення про прийняття ризику ухвалює уповноважена особа на обмежений строк із занесенням до реєстру ризиків.

Розподіл ролей і відповідальності закріплюється в політиці явно. Вище керівництво затверджує політику й несе загальну відповідальність за управління ризиками; керівник служби інформаційної безпеки (CISO) розробляє політики, координує їх впровадження та контролює виконання; власники бізнес-процесів і активів відповідають за класифікацію інформації та прийняття ризиків у своїй сфері; IT-підрозділи реалізують технічні вимоги; працівники зобов'язані дотримуватися політики й повідомляти про порушення; внутрішній аудит незалежно оцінює виконання. Відповідальність третіх сторін закріплюється в договорах відповідно до вимог ISO/IEC 27001:2022 щодо відносин із постачальниками.

Погодження, затвердження та впровадження політик здійснюються за встановленою процедурою. Проєкт політики погоджується з юридичним підрозділом (відповідність законодавству та трудовим відносинам), підрозділом кадрів, власниками ключових бізнес-процесів та IT. Затвердження здійснює вище керівництво, що демонструє його зобов'язання. Впровадження включає доведення політики до персоналу з підтвердженням ознайомлення, навчання та програми підвищення обізнаності (захід 6.3 ISO/IEC 27001:2022), технічне впровадження вимог (налаштування систем відповідно до стандартів конфігурацій), а також інтеграцію вимог у процеси – прийом на роботу, закупівлі, управління змінами, розробку.

Дотримання політик інформаційної безпеки під час забезпечення бізнес-процесів контролюється кількома механізмами. Технічний контроль здійснюється засобами, що автоматично забезпечують виконання вимог (групові політики, системи управління мобільними пристроями, засоби запобігання витоку даних) і фіксують порушення. Моніторинг відповідності ведеться за метриками: частка систем, конфігурація яких відповідає стандарту; частка працівників, що пройшли навчання; середній час усунення критичних вразливостей; частка своєчасно переглянутих прав доступу; кількість зареєстрованих порушень і винятків. Періодичні внутрішні аудити та самооцінювання перевіряють фактичне виконання, а дисциплінарний процес (захід 6.4 ISO/IEC 27001:2022) забезпечує відповідальність за порушення. Ефективна практика розглядає порушення насамперед як сигнал про невідповідність політики реальним бізнес-процесам: якщо правило систематично порушують, слід з'ясувати причину й або змінити процес, або змінити правило.

Періодичний перегляд та актуалізація документів з інформаційної безпеки є обов'язковою вимогою: політики переглядаються в заплановані строки (як правило, щорічно) та позапланово – у разі суттєвих змін у бізнесі, організаційній структурі, інфраструктурі, законодавстві, ландшафті загроз, а також за результатами серйозних інцидентів і аудитів. Перегляд включає оцінювання актуальності, достатності та результативності політики з урахуванням метрик дотримання. Документи підлягають управлінню версіями: кожна версія має номер, дату затвердження, власника документа та історію змін, а застарілі версії вилучаються з обігу. Тим самим політики інформаційної безпеки стають живою частиною циклу управління ризиками, що постійно адаптується до змін середовища [1; 7].

Контрольні питання

1. Дайте визначення політики інформаційної безпеки та назвіть вимоги ISO/IEC 27001:2022 до неї.

2. Сформулюйте основні принципи розроблення політик безпеки.

3. Опишіть ієрархію документів з інформаційної безпеки.

4. Які тематичні політики рекомендує ISO/IEC 27002:2022?

5. Порівняйте моделі RBAC, ABAC та MAC.

6. Як пов’язані параметри політики резервного копіювання з RPO і RTO? Поясніть правило «3-2-1-1-0».

7. Як ураховуються ризики та критичність бізнес-процесів у політиках? Що таке процедура винятків?

8. Опишіть розподіл ролей і відповідальності за політики безпеки.

9. Якими механізмами контролюється дотримання політик?

10. Коли і як переглядаються документи з інформаційної безпеки?

СПИСОК ЛІТЕРАТУРИ

1. Morales C. Cyber Risk Management in Practice : A Guide to Real-World Solutions. Boca Raton : CRC Press, 2025. 360 p.

2. Whitman M. E., Mattord H. J. Management of Cybersecurity. 7th ed. Boston : Cengage Learning, 2025. 546 p.

3. Bayuk J. L. Stepping Through Cybersecurity Risk Management : A Systems Thinking Approach. Hoboken : John Wiley & Sons, 2024. 336 p.

4. Hubbard D. W., Seiersen R. How to Measure Anything in Cybersecurity Risk. 2nd ed. Hoboken : John Wiley & Sons, 2023. 368 p.

5. Calder A., Watkins S. IT Governance : An International Guide to Data Security and ISO 27001/ISO 27002. 8th ed. Ely : IT Governance Publishing, 2024. 486 p.

6. Nair A., Greeshma M. R. Mastering Information Security Compliance Management : A comprehensive handbook on ISO/IEC 27001:2022 compliance. Birmingham : Packt Publishing, 2023. 236 p.

7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. Geneva : ISO, 2022. 19 p.

8. ISO/IEC 27001:2022/Amd 1:2024. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. Amendment 1 : Climate action changes. Geneva : ISO, 2024. 2 p.

9. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). Вид. офіц. Київ : ДП «УкрНДНЦ», 2023.

10. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection. Information security controls. Geneva : ISO, 2022. 152 p.

11. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection. Guidance on managing information security risks. Geneva : ISO, 2022. 62 p.

12. ISO/IEC 27035-1:2023. Information technology. Information security incident management. Part 1 : Principles and process. Geneva : ISO, 2023.

13. ISO/IEC 27006-1:2024. Information security, cybersecurity and privacy protection. Requirements for bodies providing audit and certification of information security management systems. Part 1 : General. Geneva : ISO, 2024. 47 p. URL: https://www.iso.org/standard/82908.html (дата звернення: 14.11.2026).

14. ISO 22301:2019/Amd 1:2024. Security and resilience. Business continuity management systems. Requirements. Amendment 1 : Climate action changes. Geneva : ISO, 2024. URL: https://www.iso.org/standard/88412.html (дата звернення: 14.11.2026).

15. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0 : NIST Cybersecurity White Paper 29. Gaithersburg : National Institute of Standards and Technology, 2024. 32 p. DOI: https://doi.org/10.6028/NIST.CSWP.29.

16. NIST Cybersecurity Framework 2.0 : Resource and Overview Guide : NIST Special Publication 1299 / National Institute of Standards and Technology. Gaithersburg : NIST, 2024. DOI: https://doi.org/10.6028/NIST.SP.1299.

17. Incident Response Recommendations and Considerations for Cybersecurity Risk Management : A CSF 2.0 Community Profile : NIST Special Publication 800-61 Rev. 3 / A. Nelson, S. Rekhi, M. Souppaya, K. Scarfone. Gaithersburg : National Institute of Standards and Technology, 2025. DOI: https://doi.org/10.6028/NIST.SP.800-61r3.

18. Security and Privacy Controls for Information Systems and Organizations : NIST Special Publication 800-53 Rev. 5, Release 5.2.0 / Joint Task Force. Gaithersburg : National Institute of Standards and Technology, 2025. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (дата звернення: 14.11.2026).

19. Assessing Security and Privacy Controls in Information Systems and Organizations : NIST Special Publication 800-53A Rev. 5 / Joint Task Force. Gaithersburg : National Institute of Standards and Technology, 2022. DOI: https://doi.org/10.6028/NIST.SP.800-53Ar5.

20. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations : NIST Special Publication 800-161 Rev. 1 / J. Boyens et al. Gaithersburg : National Institute of Standards and Technology, 2022. DOI: https://doi.org/10.6028/NIST.SP.800-161r1.

21. Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems : NIST Special Publication 800-18 Rev. 2 / National Institute of Standards and Technology. Gaithersburg : NIST, 2026. URL: https://csrc.nist.gov/projects/risk-management (дата звернення: 14.11.2026).

22. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union. 2022. L 333. P. 80–152.

23. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union. 2022. L 333. P. 1–79.

24. ENISA Threat Landscape 2025 / European Union Agency for Cybersecurity. Athens : ENISA, 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (дата звернення: 14.11.2026).

25. Про затвердження Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем : постанова Каб. Міністрів України від 18.06.2025 р. № 712. URL: https://zakon.rada.gov.ua/laws/show/712-2025-п (дата звернення: 14.11.2026).

26. Про затвердження Каталогу заходів із кіберзахисту : наказ Адміністрації Держ. служби спец. зв'язку та захисту інформації України від 30.01.2026 р. № 75. URL: https://zakon.rada.gov.ua (дата звернення: 14.11.2026).

27. TheHive Documentation : Licenses and Installation / StrangeBee. 2025. URL: https://docs.strangebee.com/thehive/ (дата звернення: 14.11.2026).

Оцінка та управління ризиками: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Кібербезпека» галузі знань 12 (F) Інформаційні технології спеціальності F5 (125) Кібербезпека та захист інформації денної та заочної форм навчання / уклад. С.М. Костючко, О.Р. Кулакевич. Луцьк: ЛНТУ, 2026. 62 с.

Комп’ютерний набір С.М. Костючко

Редактор С.М. Костючко

Підп. до друку «___» _____ 2026р.
Формат 60х84/16. Папір офс. Гарнітура Таймс.
Ум. друк. арк. ____. Тираж 10 прим. Зам. ____

Відділ іміджу та промоцій
Луцького національного технічного університету
43018, м. Луцьк, вул. Львівська, 75
ВІП ЛНТУ