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

ОБРОБКА ІНЦИДЕНТІВ ТА РЕАГУВАННЯ

Конспект лекцій
для здобувачів першого (бакалаврського) рівня вищої освіти
освітньої програми «Кібербезпека»
галузь знань 12 Інформаційні технології
спеціальності 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
_____ Роман ВОЗНЮК, ас. кафедри кібербезпеки ЛНТУ

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

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

Обробка інцидентів та реагування: 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, Р.В. Вознюк. Луцьк: ЛНТУ, 2026. 60 с.

ЗМІСТ

ВСТУП..... 4
ТЕМА 1. ВСТУП ДО ОБРОБКИ ІНЦИДЕНТІВ ТА РЕАГУВАННЯ 6
ТЕМА 2. РІЗНОВИДИ ІНЦИДЕНТІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ..... 10
ТЕМА 3. МЕТОДИ ВИЯВЛЕННЯ ІНЦИДЕНТІВ 13
ТЕМА 4. МОНІТОРИНГ ТА ЛОГУВАННЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ..... 17
ТЕМА 5. АНАЛІЗ НАСЛІДКІВ ІНЦИДЕНТІВ ТА РОЗРОБКА СТРАТЕГІЙ РЕАГУВАННЯ..... 21
ТЕМА 6. КОМУНІКАЦІЯ ПІД ЧАС РЕАГУВАННЯ НА ІНЦИДЕНТИ..... 24
ТЕМА 7. УПРАВЛІННЯ ІНЦИДЕНТАМИ ТА СИСТЕМИ УПРАВЛІННЯ ІНЦИДЕНТАМИ 27
ТЕМА 8. КОМАНДНИЙ ПІДХІД ДО РЕАГУВАННЯ НА ІНЦИДЕНТИ 30
ТЕМА 9. СТАНДАРТИ ТА НОРМАТИВНО-ПРАВОВІ АКТИ В ГАЛУЗІ ОБРОБКИ ІНЦИДЕНТІВ 34
ТЕМА 10. ІНЦИДЕНТИ БЕЗПЕКИ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКА..... 38
ТЕМА 11. ВІДНОВЛЕННЯ ПІСЛЯ ІНЦИДЕНТУ ТА ПЛАНУВАННЯ ЗАХОДІВ У РАЗІ ВИНИКНЕННЯ ІНЦИДЕНТІВ..... 41
ТЕМА 12. РОБОТА З ВНУТРІШНІМИ ТА ЗОВНІШНІМИ СТЕЙКХОЛДЕРАМИ ПІД ЧАС РЕАГУВАННЯ НА ІНЦИДЕНТИ 44
ТЕМА 13. АУДИТ ТА ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМИ РЕАГУВАННЯ НА ІНЦИДЕНТИ..... 47
ТЕМА 14. ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ДЛЯ ЗБОРУ, АНАЛІЗУ ТА ВІЗУАЛІЗАЦІЇ ДАНИХ ВІДНОСНО ІНЦИДЕНТІВ 50
ТЕМА 15. ПОРІВНЯННЯ РІЗНИХ ПІДХОДІВ ДО РЕАГУВАННЯ НА ІНЦИДЕНТИ В РІЗНИХ СФЕРАХ ДІЯЛЬНОСТІ 53
СПИСОК ЛІТЕРАТУРИ..... 57

ВСТУП

Обробка інцидентів та реагування на них є однією з ключових практичних складових кібербезпеки: навіть найкраще спроєктована система захисту не гарантує, що атаку буде повністю запобігти, тому організація має вміти вчасно виявити подію, з'ясувати її суть, обмежити шкоду й повернутися до нормальної роботи. Сучасні настанови розглядають цю діяльність як невід'ємну частину управління кіберризиками, а не окремий технічний процес: остання редакція настанови NIST SP 800-61 Rev. 3 прямо пов'язує реагування з усіма функціями Рамки кібербезпеки NIST CSF 2.0 [2; 3]. Закони й директиви, зокрема NIS2 в ЄС та Закон № 4336-IX в Україні, встановлюють обов'язки повідомлення про інциденти й відповідальність керівництва за готовність до них [8; 17].

Методичний посібник підготовлено відповідно до силабуса освітнього компонента «Обробка інцидентів та реагування» і охоплює п'ятнадцять тем. Перший змістовий модуль (теми 1-8) присвячено основам: сутності інцидентів і життєвому циклу, їхній класифікації, методам виявлення, моніторингу й логуванню, аналізу наслідків і вибору стратегій, комунікації, системам управління інцидентами та командній організації реагування. Другий модуль (теми 9-15) розглядає стандарти й нормативно-правові акти, кіберзагрози та індикатори компрометації, відновлення й планування, роботу із зацікавленими сторонами, аудит ефективності, інструментальні засоби збору, аналізу та візуалізації даних і порівняння підходів у різних сферах діяльності.

Методологічною основою слугує підручник Дж. Латтгенса, М. Пепе та К. Мандіа «Incident Response & Computer Forensics» (3-тє видання), який послідовно описує процес реагування від підготовки до усунення наслідків і ґрунтується на великому практичному досвіді розслідувань [1]. Оскільки книга вийшла у 2014 році, її положення доповнено та, де необхідно, уточнено за сучасними джерелами: настановою NIST SP 800-61 Rev. 3 (2025), стандартами ISO/IEC 27035-1:2023 та 27035-2:2023, аналітичним звітом

ENISA Threat Landscape 2025, довідковою базою MITRE ATT&CK та українськими нормативними актами 2025-2026 років [2; 4; 5; 7; 12; 16].

Кожна тема викладена суцільним текстом без поділу на підпункти й завершується контрольними питаннями. Розташування матеріалу відповідає порядку питань у силабусі. Після опанування посібника здобувач має вміти пояснювати, як організовано процес реагування на інциденти, розрізняти типи інцидентів і оцінювати їхню критичність, обирати методи виявлення та налаштовувати джерела подій, розробляти стратегії локалізації та відновлення, організовувати комунікацію і взаємодію команди та зовнішніх сторін, використовувати стандарти й показники ефективності, застосовувати інструменти аналізу й візуалізації. Слід пам’ятати, що практика реагування й нормативна база змінюються швидко, тому перед застосуванням положень посібника в реальній організації їх необхідно звіряти з чинними версіями документів.

ТЕМА 1. ВСТУП ДО ОБРОБКИ ІНЦИДЕНТІВ ТА РЕАГУВАННЯ

Інцидент інформаційної безпеки – подія або сукупність подій, що порушують чи загрожують порушити конфіденційність, цілісність або доступність інформації та інформаційних систем, або суперечать політикам безпеки організації. Єдиного універсального визначення не існує, тому кожна організація має сформулювати власне, оскільки саме воно окреслює межі діяльності команди реагування. Автори підручника [1] виокремлюють три ознаки інциденту комп'ютерної безпеки: наявність наміру завдати шкоди, виконання дій людиною та залучення обчислювального ресурсу. Остання ознака відрізняє такий інцидент від звичайних подій на кшталт крадіжки чи підпалу. До обчислювальних ресурсів належать не лише сервери й робочі станції, а й телефони, принтери, носії інформації, картки доступу та хмарні сервіси.

Сутність інциденту виявляється через його наслідки: крадіжку даних, коштів чи інтелектуальної власності, вимагання, несанкціонований доступ, наявність шкідливого програмного забезпечення, використання ресурсів не за призначенням. Наслідки можуть бути різними – від перевстановлення кількох комп'ютерів до припинення діяльності організації. Показовими прикладами є зараження мережевим хробаком NotPetya в 2017 році, що паралізувало роботу великих корпорацій, атака на ланцюг постачання SolarWinds у 2020 році та масштабна відмова мільйонів систем Windows через помилкове оновлення засобу захисту в липні 2024 року: останній випадок не був атакою, проте за наслідками для доступності був інцидентом. Підозрілу подію слід вважати потенційним інцидентом, доки не доведено протилежне, а перше реагування може виявити, що це хибна тривога.

Основна мета реагування на інциденти полягає в тому, щоб ефективно усунути загрозу з обчислювального середовища організації, мінімізувати збитки й якнайшвидше відновити нормальну роботу [1]. Ця мета досягається двома видами діяльності. Розслідування встановлює початковий вектор атаки, використані зловмисником програми й інструменти, перелік уражених систем

і спосіб ураження, результат дій зловмисника, часові межі інциденту та те, чи триває він. Усунення наслідків використовує отримані відомості для розроблення й виконання плану, який видаляє загрозу та зменшує ймовірність повторення. Додатковими завданнями є збереження доказів для можливих судових процесів, виконання вимог щодо повідомлення регуляторів, документування й накопичення знань.

Життєвий цикл управління інцидентами в підручнику подано як три групи дій: первинне реагування, розслідування й усунення наслідків. Первинне реагування передбачає підтвердження факту інциденту, формування команди, огляд легкодоступних даних, визначення типу та оцінювання потенційного впливу. Розслідування й усунення після цього виконуються здебільшого паралельно. Сучасні стандарти пропонують дрібніший поділ. ISO/IEC 27035-1:2023 розрізняє планування й підготовку, виявлення та звітування, оцінювання й ухвалення рішення, реагування та винесення уроків [4]. Настанова NIST SP 800-61 Rev. 3 відмовилася від лінійної моделі й інтегрувала реагування в шість функцій CSF 2.0, показавши, що підготовка, виявлення, реагування й відновлення є безперервними й взаємозалежними процесами [2; 3].

Основні етапи виявлення, аналізу, локалізації та усунення становлять оперативне ядро циклу. Виявлення полягає в отриманні сигналу про подію з систем моніторингу, від користувачів, зовнішніх партнерів чи правоохоронців. Аналіз підтверджує, що подія є інцидентом, визначає її масштаб, критичність і вектор. Локалізація (стримування) зупиняє поширення шкоди, наприклад ізоляцією вузлів, блокуванням облікових записів чи відкликанням ключів; тут важливо врахувати, що передчасні дії можуть насторожити зловмисника, і тому момент локалізації часто узгоджують із завершенням збору даних про його присутність. Усунення видаляє першопричину, закриває вразливість і відновлює довіру до систем, а подальше відновлення повертає сервіси до роботи.

Для розуміння дій зловмисника корисна концепція життєвого циклу атаки, яку використовують у практиці розслідувань. Вона описує послідовність:

початкова розвідка, первинна компрометація, закріплення в мережі, підвищення привілеїв, внутрішня розвідка, бічне переміщення, підтримання присутності та виконання мети [1]. Кожен етап залишає сліди, і чим раніше їх виявлено, тим менших збитків завдасть атака. Сучасні зловмисники діють терпляче: вони можуть перебувати в мережі місяцями, вивчаючи її не гірше за IT-відділ, тому швидкість виявлення є критичним показником.

Роль реагування в системі забезпечення кібербезпеки організації подвійна. З одного боку, воно становить останню лінію захисту, коли превентивні заходи не спрацювали, і визначає, чи залишиться подія незначним епізодом, чи призведе до серйозної кризи. З іншого боку, воно є джерелом знань для всього циклу управління безпекою: висновки з інцидентів уточнюють оцінювання ризиків, змінюють вимоги політик, вдосконалюють навчання персоналу й закупівлі засобів захисту. Автори підручника наголошують, що більшість проблем реагування мають нетехнічний характер: це питання відповідальності, комунікації, юридичних вимог і взаємодії підрозділів [1].

Успішне реагування залежить від підготовки. До неї належать затвердження визначення інциденту та політики реагування, створення команди з чітко розподіленими ролями, налагодження джерел даних і журналювання, підготовка каналів комунікації й контактів зовнішніх сторін, а також регулярні навчання. Організації без власної команди можуть укладати договори із зовнішніми провайдерами реагування заздалегідь, бо під час кризи часу на переговори бракує. Українська практика додає до цього обов’язок повідомляти про значні інциденти національну команду CERT-UA відповідно до чинних порядків [16].

Контрольні питання

1. Які ознаки має інцидент комп’ютерної безпеки та чим він відрізняється від звичайної події?

2. У чому полягають основні цілі й завдання реагування на інциденти?

3. З яких етапів складається життєвий цикл управління інцидентами в підручнику, ISO/IEC 27035-1:2023 і NIST SP 800-61 Rev. 3?

4. Охарактеризуйте етапи виявлення, аналізу, локалізації та усунення інциденту.

5. Яка роль реагування на інциденти в системі забезпечення кібербезпеки організації?

ТЕМА 2. РІЗНОВИДИ ІНЦИДЕНТІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Класифікація інцидентів потрібна для того, щоб однаково називати схожі події, вибирати типові сценарії реагування, порівнювати статистику й визначати пріоритети. Універсальної класифікації немає, тому організації використовують кілька ознак одночасно. За типом події розрізняють несанкціонований доступ і компрометацію облікових записів, зараження шкідливим програмним забезпеченням, витік або викрадення даних, мережеві атаки, атаки на доступність, соціальну інженерію, зловживання ресурсами та фізичні інциденти. За джерелом виокремлюють зовнішні й внутрішні, навмисні та ненавмисні. За наслідками інциденти поділяють за порушеною властивістю інформації (конфіденційність, цілісність, доступність) і за ступенем критичності. Українські команди реагування застосовують також шкалу від низького до критичного рівня, що залежить від масштабу й значущості уражених об’єктів [4; 16].

Інциденти, пов’язані з несанкціонованим доступом, охоплюють використання вкрадених чи підібраних облікових даних, експлуатацію вразливостей публічних сервісів, обхід автентифікації та зловживання привілеями. Типовий сценарій виглядає так: зловмисник купує або отримує через фішинг облікові дані користувача, входить через віддалений доступ без багатофакторної автентифікації, підвищує привілеї, переміщується мережею й дістається цінних даних. Ознаками є входи з незвичних місць і в незвичний час, нові облікові записи з високими правами, створення запланованих завдань чи служб, використання засобів адміністрування не за призначенням [1; 7].

Інциденти зі шкідливим програмним забезпеченням охоплюють віруси, троянські програми, засоби віддаленого доступу, шпигунські програми, злодії облікових даних, завантажувачі та програми-вимагачі. Вимагачі з’явилися в кінці 2010-х як основна фінансова загроза: вони шифрують дані й нерідко викрадають їх для подвійного вимагання, а доступ до мережі нерідко продають спеціалізовані «брокери доступу». Звіти ENISA констатують стійке

зростання ролі вимагачів і атак на ланцюг постачання серед найважливіших загроз у Європі [7]. Ознаками слугують масові зміни розширень файлів, зупинка служб резервного копіювання, видалення тіньових копій, незвичне навантаження на диски.

Витік інформації може бути наслідком зовнішнього проникнення, помилкової конфігурації (відкриті сховища хмарних даних), дій внутрішнього порушника чи втрати носіїв. Особливістю є те, що організація нерідко дізнається про витік від третіх осіб: клієнтів, правоохоронців, журналістів або з публікації даних на форумах. Такі інциденти тягнуть юридичні наслідки, зокрема обов'язок повідомити регулятора й постраждалих осіб; в ЄС за Загальним регламентом захисту даних строк повідомлення становить 72 години з моменту виявлення, а за директивою NIS2 діють власні етапи звітування [8].

Мережеві атаки включають сканування, перехоплення трафіку, підміну адрес і імен, атаки на протоколи маршрутизації та бездротові мережі. Фішинг – розсилання повідомлень, що імітують довірене джерело, щоб виманити облікові дані, спонукати до відкриття шкідливого вкладення чи виконання платежу; його різновиди – вішинг (голосові дзвінки), смішинг (повідомлення) та цільовий фішинг, спрямований на конкретних осіб. Атаки типу DoS і DDoS перевантажують ресурси систем і мережі, роблячи сервіс недоступним, і діють на рівні мережі (затоплення пакетами), транспорту (SYN-атаки) та застосунків (запити до дорогих операцій). Важливо враховувати, що DDoS може слугувати димовою завісою для іншої атаки.

Внутрішні та зовнішні загрози відрізняються мотивами й можливостями. Зовнішні суб'єкти – кіберзлочинці, державні групи, хактивісти – не мають легітимного доступу й проникають через вразливості або обман. Внутрішні – працівники, підрядники, партнери – мають доступ і знання процесів, тому можуть завдати значної шкоди як навмисно (помста, вигода), так і через помилку чи недбалість. Практика показує, що жорстка межа часто стирається: зловмисник, укравши облікові дані працівника, стає для систем «внутрішнім» користувачем, і виявляти його можна лише за поведінкою [1].

Для порівняльного огляду типових інцидентів зручно скористатися таблицею, що зіставляє їх ознаки та характерний вплив.

Таблиця 2.1 – Типові інциденти, їхні ознаки та вплив

Тип інциденту	**Типові ознаки**	**Основний вплив**
Несанкціонований доступ	Незвичні входи, нові привілейовані облікові записи	Конфіденційність, цілісність
Шкідливе ПЗ	Незвичні процеси, зв’язок із керівними серверами	Усі три властивості
Програма-вимагач	Масове шифрування, видалення резервних копій	Доступність, конфіденційність
Витік даних	Великі вихідні передавання, повідомлення від третіх осіб	Конфіденційність
DDoS	Різке зростання трафіку, відмови сервісу	Доступність

Визначення критичності й оцінювання впливу на інформаційні системи спираються на кілька чинників: цінність і чутливість уражених даних, значущість систем для бізнес-процесів, кількість уражених вузлів і користувачів, наявність доказів активності зловмисника, юридичні й репутаційні наслідки та потенційна швидкість поширення. Результат подають у вигляді рівня (наприклад, низький, середній, високий, критичний) із чітко описаними критеріями, щоб команда однаково розуміла пріоритети. Критичність не є сталою: вона переоцінюється, коли з’являються нові факти, а рівень впливу залежить також від часу доби й ритму діяльності організації. Для узгодженості рівнів із вимогами до повідомлення в Україні діють критерії значного кіберінциденту, затверджені наказом Адміністрації Держспецзв’язку від 14 травня 2026 року № 351 [16].

Контрольні питання

1. За якими ознаками класифікують інциденти інформаційної безпеки?

2. Які ознаки мають інциденти несанкціонованого доступу та зараження шкідливим ПЗ?

3. Як відбуваються витік інформації та атаки на доступність? Назвіть їхні ознаки.

4. Чим відрізняються внутрішні й зовнішні загрози?

5. Як визначають критичність інциденту та оцінюють його вплив?

ТЕМА 3. МЕТОДИ ВИЯВЛЕННЯ ІНЦИДЕНТІВ

Виявлення інцидентів є вирішальним етапом, оскільки від часу між початком атаки та її виявленням залежить обсяг збитків. Джерелами виявлення є автоматизовані засоби моніторингу, повідомлення користувачів, звернення клієнтів, інформація від зовнішніх партнерів і правоохоронців, а також результати цілеспрямованого пошуку загроз. Практика розслідувань свідчить, що значну частку інцидентів організація виявляє не власними засобами, а за повідомленнями третіх осіб, що вказує на недостатній рівень видимості [1; 7]. Основні підходи до автоматичного виявлення поділяють на сигнатурні, аномальні та поведінкові, і ефективна система комбінує їх.

Сигнатурні методи порівнюють події, файли чи мережевий трафік із відомими шаблонами шкідливої активності: хешами файлів, байтовими послідовностями, правилами для мережевих пакетів, індикаторами компрометації. Вони забезпечують високу точність для вже відомих загроз і просто інтерпретуються, проте не виявляють нових чи модифікованих атак і вимагають постійного оновлення баз. Аномальні методи спочатку будують профіль нормальної роботи (трафіку, входів, використання ресурсів), а потім сигналізують про відхилення. Вони теоретично здатні виявляти раніше невідомі атаки, але дають багато хибних спрацьовувань, оскільки нормальна поведінка змінюється, а відхилення не завжди зловмисне. Поведінкові методи аналізують послідовності дій і зв’язки між подіями, наприклад поєднання відкриття документа, запуску командного інтерпретатора й нетипового мережевого з’єднання, і порівнюють їх з відомими тактиками та техніками зловмисників, що описані у довідковій базі MITRE ATT&CK [12].

Таблиця 3.1 – Порівняння підходів до виявлення

Підхід	**Переваги**	**Обмеження**
Сигнатурний	Висока точність для відомих загроз	Не виявляє нових атак
Аномальний	Може виявити невідомі загрози	Багато хибних спрацьовувань
Поведінковий	Стійкий до зміни інструментів	Потребує якісних даних і налаштування

Системи виявлення та запобігання вторгненням (IDS і IPS) аналізують мережевий трафік або події на вузлах. Мережеві системи розміщують у ключових точках, вони перевіряють пакети й потоки за сигнатурами та протокольними аномаліями; системи запобігання, на відміну від систем виявлення, здатні блокувати підозрілі з'єднання, проте їх неправильне налаштування ризикує зупинити легітимну роботу. Розв'язання для кінцевих точок (EDR) постійно збирають телеметрію про процеси, файли, реєстр, мережеві з'єднання й дії користувачів, виявляють шкідливу поведінку та надають можливості віддаленого реагування: ізоляцію хоста, завершення процесу, збирання артефактів. Системи управління подіями та інформацією безпеки (SIEM) централізовано збирають журнали з багатьох джерел, нормалізують їх, корелюють події за правилами й формують сповіщення; сучасні платформи доповнюють їх аналітикою поведінки та автоматизацією реагування.

Аналіз мережевого трафіку виконують на кількох рівнях деталізації. Повне захоплення пакетів дає найбільше відомостей, проте потребує значних ресурсів зберігання. Потоковий облік (NetFlow, IPFIX) фіксує лише метадані про з'єднання – адреси, порти, обсяги, час – і дозволяє довго зберігати історію. Журнали застосунків і мережевих служб, наприклад DNS, проксі та міжмережевих екранів, надають контекст щодо запитів і дозволів. Для виявлення типових ознак компрометації застосовують пошук з'єднань із відомими шкідливими адресами, незвичних запитів до імен, періодичних «маяків» до керівних серверів, передавання великих обсягів даних назовні та використання нестандартних протоколів [1].

Аналіз подій безпеки охоплює кореляцію записів із різних систем, побудову часових ліній і пошук закономірностей. Правила кореляції описують сценарії на кшталт «багато невдалих входів, за якими йде успішний вхід», «створення нової служби на сервері після віддаленого запуску», «доступ до великої кількості файлів за короткий час». Для обміну правилами виявлення використовують формат Sigma, для опису шкідливих файлів –

правила YARA, для мережевих сигнатур – правила Suricata і Snort. Регулярно виконують також цілеспрямований пошук загроз (threat hunting), коли аналітик за гіпотезою шукає ознаки активності, що не викликали автоматичних сповіщень.

Машинне навчання застосовують для виявлення підозрілої активності у вигляді класифікації (відрізнення шкідливих файлів чи доменів від легітимних), виявлення аномалій у поведінці користувачів і мереж, групування подій і зменшення кількості сповіщень. Навчання з учителем потребує розмічених даних, яких у галузі небагато й які швидко застарівають; навчання без вчителя виявляє відхилення, проте не пояснює їхню природу. Типовими проблемами є зміщення даних, дрейф поведінки, штучні атаки на моделі та складність інтерпретації. Якість виявлення оцінюють точністю й повнотою:

$$Precision = TP / (TP + FP); \quad Recall = TP / (TP + FN)$$

де TP – правильні спрацьовування, FP – хибні, FN – пропущені. Через значну перевагу нормальних подій над атаками навіть невелика частка хибних спрацьовувань породжує сотні сповіщень, тому моделі розглядають як допомогу аналітику, а не заміну.

Ефективність виявлення залежить не лише від технологій. Команда має визначити, які тактики зловмисників вона здатна виявити, і покрити прогалини; перевіряти правила на практиці, зокрема за допомогою тестових атак; зменшувати шум, видаляючи неактуальні сповіщення; налагоджувати зворотний зв’язок між аналітиками й інженерами правил. Показниками якості є частка інцидентів, виявлених власними засобами, середній час виявлення та кількість хибних спрацьовувань на аналітика за зміну [2; 6].

Контрольні питання

1. Які джерела й основні підходи застосовують для виявлення інцидентів?

2. У чому полягають відмінності сигнатурних, аномальних і поведінкових методів?

3. Яке призначення систем IDS/IPS, EDR та SIEM?

4. Які методи аналізу мережевого трафіку та подій безпеки використовують?

5. Як застосовують машинне навчання для виявлення підозрілої активності та які його обмеження?

ТЕМА 4. МОНІТОРИНГ ТА ЛОГУВАННЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Моніторинг – безперервне спостереження за станом інформаційної інфраструктури з метою своєчасного виявлення подій, що вказують на загрозу, збій чи порушення політик; логування – реєстрація подій у журналах для подальшого аналізу. Моніторинг вирішує три завдання: оперативне виявлення атак, забезпечення даних для розслідування та підтвердження відповідності вимогам. Автори підручника наголошують, що ключова проблема більшості розслідувань – не брак інструментів, а відсутність потрібних даних на момент інциденту: якщо події не фіксувалися або журнали встигли перезаписатися, відновити картину неможливо [1]. Тому організація моніторингу є частиною підготовки до реагування, а не реакцією на подію. Каталог заходів NIST SP 800-53 виділяє для цього окрему родину вимог щодо аудиту й журналювання [11].

Організація моніторингу починається з визначення цілей і переліку активів, які необхідно охопити: критичних серверів, служб автентифікації, периметра мережі, хмарних сервісів, кінцевих пристроїв, баз даних, систем резервного копіювання. Для кожного джерела визначають, які події підлягають реєстрації, у якому форматі, з яким рівнем деталізації й як довго зберігатимуться. Слід знайти баланс між повнотою й вартістю: надмірні журнали збільшують витрати та шум, а недостатні унеможливлюють розслідування. Окремої уваги потребують вимоги законодавства про персональні дані, адже журнали можуть містити відомості про особу, тому доступ і строки зберігання мають бути обґрунтовані.

Джерела подій безпеки охоплюють операційні системи (журнали подій Windows, системні журнали й підсистему аудиту Linux), служби автентифікації та каталогу, мережеве обладнання (маршрутизатори, комутатори, міжмережеві екрани), системи виявлення вторгнень, проксі- та поштові шлюзи, DNS і DHCP, веб-сервери й застосунки, бази даних, засоби захисту кінцевих точок, хмарні платформи, а також фізичні системи доступу. Автори підручника окремо розглядають корпоративні служби як цінне

джерело доказів: журнали DHCP зіставляють IP-адреси з вузлами, журнали DNS показують звернення до шкідливих доменів, журнали антивірусних систем відображають виявлені й видалені файли, журнали веб-серверів фіксують експлуатацію вразливостей застосунків [1].

Типи журналів різняться за призначенням: журнали автентифікації й авторизації, журнали системних і прикладних подій, мережеві журнали й потокові дані, журнали змін конфігурації та аудиту, журнали безпеки засобів захисту. Для Windows важливими є події успішного й невдалого входу, створення облікових записів і служб, запуску процесів (за наявності розширеного аудиту або системного монітора Sysmon), очищення журналу. Для Linux – записи автентифікації, виконання привілейованих команд, зміни файлів за правилами аудиту. Окрему категорію становлять журнали хмарних сервісів, які фіксують дії в консолі керування та API й нерідко є єдиним доказом доступу до хмарних ресурсів.

Централізований збір, зберігання й обробка логів вирішують кілька проблем. Локальні журнали легко змінити або видалити, а зловмисники нерідко роблять це, щоб приховати сліди; передавання записів на окремий захищений сервер зменшує цей ризик. Для збору застосовують протокол syslog, агентів на вузлах, інтерфейси хмарних провайдерів і платформи на кшталт Wazuh, Elastic Stack, Graylog чи комерційних SIEM [13]. Критично важливі єдиний час (синхронізація за NTP), нормалізація полів до спільної схеми, захист цілісності (хешування, запис без можливості зміни), контроль доступу до сховища та резервування. Строки зберігання задають із урахуванням того, що зловмисники можуть бути в мережі місяцями, тому для гарячого пошуку тримають короткий період, а архіви – значно довше.

Кореляція подій і виявлення аномалій перетворюють потік записів на корисні сигнали. Правила кореляції поєднують події з різних джерел, як-от вхід користувача з нової країни, подальше створення правила пересилання пошти й обмін великими обсягами даних. Статистичні та поведінкові методи виявляють відхилення від базового рівня: незвичний обсяг трафіку, нетипові години роботи, раптове збільшення кількості автентифікацій. Важливо вести

контекст про активи й користувачів, адже без нього будь-яка аномалія залишається незрозумілою. Результатом кореляції є сповіщення з пріоритетом, яке потрапляє до аналітика й, за необхідності, відкриває інцидент [6].

Інструменти моніторингу й аналізу журналів охоплюють кілька класів. Платформи SIEM і системи на основі відкритого коду зберігають журнали та надають пошук. Засоби моніторингу мережевого трафіку (Zeek, Suricata, Wireshark) допомагають перевіряти протоколи й вилучати артефакти. Платформа Wazuh поєднує функції збору журналів, контролю цілісності файлів, виявлення вразливостей і виявлення вторгнень на вузлах, а також дозволяє приймати журнали мережевих пристроїв [13]. Для оперативного опитування вузлів і збору артефактів використовують відкриті засоби на кшталт Velociraptor [14]. Вибір залежить від масштабу, бюджету та кваліфікації команди, але навіть скромна інфраструктура з правильно налаштованим збором журналів перевершує дорогу платформу без якісних даних.

Контроль якості моніторингу виконують регулярними перевірками. Потрібно переконатися, що всі критичні джерела надсилають дані й жодне не «замовкло», що правила виявлення працюють, а журнали придатні для судового використання, тобто мають достовірний час, захист від змін і документований ланцюг володіння. Корисним є вимірювання покриття за тактиками ATT&CK, що показує, які техніки зловмисників команда здатна побачити [12]. Моніторинг має бути підтриманий процесами: розподіленими ролями аналітиків, графіками перегляду сповіщень, регламентами ескалації й навчанням.

Контрольні питання

1. Що таке моніторинг і логування та які завдання вони вирішують?
2. Які основні джерела подій безпеки та типи журналів існують?
3. Чому важливий централізований збір логів і які умови його коректної організації?

4. Як працюють кореляція подій та виявлення аномалій?

5. Які інструменти використовують для моніторингу й аналізу журналів безпеки?

ТЕМА 5. АНАЛІЗ НАСЛІДКІВ ІНЦИДЕНТІВ ТА РОЗРОБКА СТРАТЕГІЙ РЕАГУВАННЯ

Після підтвердження факту інциденту команда має відповісти на два принципові питання: наскільки серйозна подія та що робити далі. Відповідь на перше дає аналіз наслідків, на друге – стратегія реагування. Автори підручника наголошують, що початкова розробка зачіпок і визначення масштабу інциденту є окремими завданнями розслідування, які мають передувати рішенням про усунення: без розуміння, які системи та облікові записи вражені, будь-яка спроба локалізації виявиться неповною й насторожить зловмисника [1]. Ця тема розглядає оцінювання масштабів, аналіз впливу на властивості безпеки, визначення пріоритетів, вибір стратегій і заходів на основі ризиків.

Методи оцінювання масштабів і наслідків ґрунтуються на збиранні й зіставленні свідчень. Спочатку формують початкові факти: хто й коли виявив подію, які системи залучені, що відомо про часові межі, які бізнес-процеси можуть бути зачеплені, та ведуть журнал справи з усіма діями й доказами. Потім виокремлюють «зачіпки» – конкретні відомості, що дозволяють шукати далі: імена файлів і хеші шкідливих програм, адреси й домени керівних серверів, облікові записи, що використовувалися, часові мітки. Кожна зачіпка перетворюється на пошукові запити по всій інфраструктурі, а результати розширюють перелік уражених вузлів і дають нові зачіпки; цей ітеративний процес продовжується, доки нові знахідки не припиняться [1]. Паралельно оцінюють, чи тривають дії зловмисника, які дані могли бути доступні й що він, імовірно, зробив із ними.

Аналіз впливу на конфіденційність, цілісність і доступність виконують для кожного активу. Для конфіденційності визначають, які відомості могли бути переглянуті або вилучені, їхню чутливість та обсяг, а також кількість осіб, чиї дані зачеплено. Для цілісності – чи змінювалися дані, програми, конфігурації та чи можна довіряти їхньому стану; найскладніші випадки пов’язані з прихованими змінами, коли необхідно перевіряти еталонні копії. Для доступності – які сервіси недоступні, як довго й яких втрат це завдає.

Додатково оцінюють юридичні наслідки (обов’язок повідомлення, регуляторні штрафи, позови), репутаційні й фінансові збитки, зокрема вартість розслідування, відновлення та втраченого прибутку.

Пріоритети реагування визначають комбінацією критичності інциденту й терміновості. Чинниками є значущість уражених систем для основних процесів, швидкість поширення шкоди, наявність активного зловмисника, ризик втрати доказів, залежність інших систем. Для узгодженості рішень зручно користуватися матрицею, де за рівнем впливу й терміновістю призначають пріоритет, від якого залежать склад задіяних ресурсів та час реакції.

Таблиця 5.1 – Приклад матриці пріоритетів реагування

Вплив / терміновість	**Низька**	**Висока**
Низький	Пріоритет 4: планова обробка	Пріоритет 3: швидка обробка
Високий	Пріоритет 2: залучення керівництва	Пріоритет 1: кризовий режим

Розроблення стратегій локалізації, стримування та усунення починається з вибору між двома підходами. Негайна локалізація зупиняє поширення шкоди, проте повідомляє зловмисника про виявлення, і він може змінити тактику, знищити сліди або запустити деструктивні дії. Спостереження дозволяє краще зрозуміти його засоби та охопити всі точки присутності, проте ризикує поглибленням шкоди. Настанови пропонують розглядати потенційну шкоду й викрадення ресурсів, потребу збереження доказів, доступність сервісів, час і ресурси, потрібні для стратегії, її ефективність і тривалість [2]. У підручнику рекомендовано не виконувати окремих локальних дій заздалегідь, а узгодити єдиний план, який здійснюється одномоментно проти всіх відомих точок присутності, щоб зловмисник не встиг перегруповатися [1].

Стратегічні рішення охоплюють такі групи заходів. Короткострокова локалізація: ізоляція вузлів від мережі, блокування облікових записів і адрес, відключення вразливих сервісів, відкликання ключів і токенів. Довгострокова локалізація: сегментація, тимчасове посилення контролю, заміна облікових даних. Усунення: видалення шкідливих засобів, виправлення вразливостей,

перебудова скомпрометованих систем із довірених носіїв, зміна всіх облікових даних, що могли бути викрадені. Відновлення: повернення сервісів у порядку пріоритетів із перевіркою чистоти. Для кожного заходу заздалегідь оцінюють побічні наслідки для бізнесу.

Оцінювання ризиків і вибір оптимальних заходів виконують порівнянням очікуваного зниження шкоди з вартістю й побічним впливом кожного варіанта. Приклад: відключення критичної виробничої системи може завдати більших збитків, ніж саме вторгнення, тому спочатку розглядають компенсаційні заходи, як-от посилений моніторинг і блокування на периметрі. Рішення, що суттєво впливають на бізнес, погоджує менеджер інциденту з керівництвом, і їх документують. Підготовка альтернатив і заздалегідь описані сценарії для типових інцидентів скорочують час прийняття рішень [2; 6].

Типовими помилками є передчасні дії без повного розуміння масштабу, обмеження стратегії лише тими системами, де знайдено сліди, відсутність плану щодо облікових даних, ігнорування бізнес-контексту й відсутність чіткого критерію завершення. Остаточним критерієм вважають не відсутність сповіщень, а підтвердження, що вектор проникнення закрито, всі відомі зачіпки перевірено, а скомпрометовані засоби й облікові дані замінено [1; 20].

Контрольні питання

1. Як оцінюють масштаб і наслідки інциденту?

2. Як аналізують вплив інциденту на конфіденційність, цілісність і доступність?

3. Як визначають пріоритети реагування?

4. Які стратегії локалізації, стримування та усунення застосовують і як вибирають між ними?

5. Як оцінюють ризики під час вибору заходів реагування?

ТЕМА 6. КОМУНІКАЦІЯ ПІД ЧАС РЕАГУВАННЯ НА ІНЦИДЕНТИ

Реагування на інцидент є командною та міжфункціональною діяльністю, тому якість комунікації значною мірою визначає її результат. Автори підручника зазначають, що більшість проблем реагування мають нетехнічний характер, і серед них найчастіші – неузгоджені очікування, запізніле залучення юристів, нечіткі ролі та неконтрольований обмін інформацією [1]. Хаотична комунікація призводить до дублювання роботи, суперечливих рішень, витоку відомостей про інцидент і юридичних ризиків, тоді як налагоджена дозволяє швидко ухвалювати рішення та зберігати довіру зацікавлених сторін.

Організація інформаційної взаємодії починається в межах підготовки. Політика реагування визначає, хто має право оголошувати інцидент, хто керує комунікацією, які відомості та кому надаються. Менеджер інциденту координує дії команди, узгоджує пріоритети й виступає єдиною точкою контакту для керівництва. Для масштабних подій створюють допоміжні групи: юридичну, комунікаційну, кадрову та бізнес-представників. Під час кризи вводять режим штабу з визначеним ритмом нарад і розподілом завдань, а всі рішення записують у журнал справи.

Внутрішні канали охоплюють спеціалізовану систему обліку інцидентів, захищені чати, телефонні мости, електронну пошту й регулярні зведення для керівництва. Зовнішні канали – зв’язок із клієнтами й партнерами, регуляторами, національною командою реагування, правоохоронцями, страховиком, постачальниками послуг і засобами масової інформації. Для кожної аудиторії визначають зміст і форму повідомлення: технічні подробиці потрібні команді, тоді як керівництву важливі масштаби впливу, прийняті рішення та потреби в ресурсах, а клієнтам – чітка інформація про вплив на них і рекомендовані дії.

Таблиця 6.1 – Аудиторії та зміст комунікації

Аудиторія	**Зміст повідомлення**	**Канал**
Команда реагування	Технічні факти, завдання, статус	Захищений чат, система обліку

Аудиторія	Зміст повідомлення	Канал
Керівництво	Масштаб, ризики, рішення, ресурси	Зведення, нарада
Регулятор і CERT-UA	Дані за встановленою формою та строками	Офіційний канал
Клієнти й партнери	Вплив, рекомендовані дії	Розсилка, сайт

Порядок повідомлення про інциденти й ескалації подій ґрунтується на заздалегідь визначених порогах. Працівник, що помітив підозрілу подію, негайно повідомляє визначений контакт (службу підтримки, команду безпеки), не намагаючись самостійно її «лагодити». Аналітик оцінює критичність і, перевищивши поріг, ескалює подію до менеджера інциденту, а той – до керівництва та юристів. Окремий порядок встановлюють для зовнішніх повідомлень. За директивою NIS2 суттєвий інцидент потребує раннього попередження без зайвих затримок, як правило, протягом 24 годин, повідомлення про інцидент протягом 72 годин і підсумкового звіту протягом місяця; регламент DORA встановлює для фінансового сектору власні, ще стисліші строки [8; 9]. В Україні порядок обміну інформацією про кіберінциденти та критерії значного кіберінциденту затверджено наказом Адміністрації Держспецзв'язку № 351 від 14 травня 2026 року [16].

Документування процесу реагування є одночасно робочим інструментом і юридичною вимогою. Журнал справи фіксує час, виконавця, виконані дії, джерела даних, висновки та рішення, а також збережені докази й ланцюг їх передачі. Автори підручника радять записувати факти окремо від припущень, використовувати єдину часову зону та вказувати джерело кожної інформації [1]. Підсумковий звіт має бути зрозумілим різним читачам: короткий виклад для керівництва та технічні додатки для спеціалістів; питання, що стосуються стандартів і якості звітності, розглянуто в розділі підручника про написання звітів.

Забезпечення конфіденційності інформації під час комунікації передбачає кілька правил. Принцип «необхідності знати» обмежує коло осіб, а відомості маркують за рівнем чутливості, наприклад за протоколом TLP. Комунікації під час інциденту ведуть через канали, які не залежать від потенційно скомпрометованої інфраструктури, оскільки зловмисник може читати пошту

й корпоративні чати; у цьому випадку використовують окремі пристрої, зовнішні сервіси або телефонний зв’язок. Залучення зовнішніх консультантів часто здійснюють через юридичних радників, щоб розслідування й листування могли бути захищені правилами про професійну таємницю [1]. Слід уникати спекуляцій у публічних заявах і узгоджувати всі офіційні повідомлення з юристами та відповідальними за комунікацію.

Практика показує типові помилки: надто пізнє залучення юристів і керівників, надмірна кількість учасників у каналах, відсутність єдиного джерела істини, непослідовність повідомлень різним аудиторіям, змішування фактів і припущень. Профілактикою є шаблони повідомлень, довідник контактів із резервними варіантами, регулярні командні навчання із відпрацюванням комунікаційних сценаріїв і постінцидентні розбори, що оцінюють роботу каналів [2; 20].

Контрольні питання

1. Чому комунікація є критичною для реагування на інциденти?
2. Які внутрішні та зовнішні канали комунікації застосовують?
3. Як організовано повідомлення про інциденти й ескалацію?
4. Що та як документують під час реагування?
5. Як забезпечується конфіденційність інформації під час комунікації?

ТЕМА 7. УПРАВЛІННЯ ІНЦИДЕНТАМИ ТА СИСТЕМИ УПРАВЛІННЯ ІНЦИДЕНТАМИ

Управління інцидентами – це організований процес, який забезпечує систематичну обробку подій безпеки від їх виявлення до закриття й винесення уроків. Принципи його побудови спираються на стандарти ISO/IEC 27035 і настанови NIST: чітка політика й сфера дії, визначені ролі, єдина класифікація, документовані процедури, вимірювані показники, зв’язок із управлінням ризиками й безперервністю діяльності, а також постійне вдосконалення [2; 4; 5]. Процес має бути придатним до масштабування: від одиничних подій, які обробляє черговий аналітик, до криз, що потребують штабу.

Організація реєстрації, класифікації та супроводу інцидентів передбачає послідовність кроків. Кожна подія, що відповідає критеріям, реєструється в системі обліку з унікальним ідентифікатором, часом, джерелом, описом і першою оцінкою. Класифікація присвоює тип, критичність і пріоритет за затвердженою схемою. Далі призначаються відповідальний, строки реакції та план дій, фіксуються всі виконані кроки, залучені системи й докази. Закриття виконують після підтвердження усунення причин і відновлення, а після нього проводять аналіз і оновлення знань. Єдина схема дозволяє збирати статистику, виявляти повторювані проблеми та вимірювати показники, наприклад середній час виявлення й відновлення [2].

Системи обліку й управління інцидентами охоплюють кілька класів засобів. Загальні системи обслуговування (ITSM) використовують для реєстрації й маршрутизації запитів та інцидентів, вони добре інтегруються з IT-процесами, але потребують доналаштування для потреб безпеки. Спеціалізовані платформи управління реагуванням призначені для роботи команди безпеки: вони підтримують справи, завдання, спостережувані дані (адреси, файли, домени), шаблони, роботу в команді й інтеграцію з аналітичними сервісами. Серед відомих рішень – відкриті системи на кшталт RTIR, а також платформа TheHive, п’ята версія якої є комерційною з безкоштовною ліцензією для спільноти, та комерційні продукти великих

постачальників; перед вибором слід перевіряти актуальні умови ліцензування й підтримки. Для документування й керування завданнями часто застосовують і універсальні інструменти командної роботи [6].

Автоматизація реагування спирається на платформи оркестрації, автоматизації й реагування (SOAR). Вони виконують сценарії (плейбуки), які поєднують дії різних систем: збагачення сповіщення відомостями з розвідувальних джерел, перевірку репутації файлів і адрес, запит додаткових даних із вузлів, створення справи, сповіщення відповідальних, ізоляцію вузла, блокування облікового запису чи адреси. Правильне автоматичне реагування скорочує час відповіді з годин до хвилин і розвантажує аналітиків від рутини. Водночас автоматизація має ризики: хибне спрацювання може зупинити легітимну роботу, а помилковий сценарій – завдати масових збоїв. Тому небезпечні дії зазвичай виконують із підтвердженням людини, а плейбуки тестують і версіонують.

Інтеграція засобів моніторингу, аналізу й управління створює наскрізний конвеєр. Джерела журналів надходять до SIEM, де правила генерують сповіщення; SOAR збагачує їх і відкриває справи в системі обліку; аналітики працюють із даними через EDR та інструменти криміналістики; результати повертаються в систему обліку, а нові індикатори – у правила виявлення та засоби блокування. Відкриті інтерфейси й стандарти обміну, такі як STIX і TAXII, спрощують підключення зовнішніх джерел розвідувальної інформації. Ключова вимога – єдина модель даних і ідентифікаторів, щоб подію можна було відстежити від першого сигналу до закриття [12].

Процеси управління інцидентами потребують метрик і контролю якості. Показниками слугують кількість і типи інцидентів, їхня критичність, час виявлення, локалізації, усунення та відновлення, частка інцидентів, виявлених власними засобами, кількість повторних, частка інцидентів, закритих у встановлені строки, і задоволеність зацікавлених сторін. Дані використовують для планування ресурсів, аналізу причин і обґрунтування змін. Регулярні огляди черги виявляють «завислі» справи, а вибіркові перевірки якості записів – неповну документацію.

Практичними вимогами до системи обліку є захист даних (записи містять чутливі відомості), розмежування доступу, журналювання дій, резервне копіювання й можливість роботи під час кризи, у тому числі в автономному режимі, якщо корпоративна інфраструктура недоступна. Для організацій, на які поширюються регуляторні вимоги, система має підтримувати формування звітів і передавання даних регуляторам та національним командам у встановлених форматах. Це особливо актуально в Україні, де нові порядки обміну інформацією про кіберінциденти зобов'язують суб'єктів передавати відомості про інциденти відповідним командам реагування за визначеними правилами [16; 18].

Контрольні питання

1. На яких принципах будують процеси управління інцидентами?
2. Як організовано реєстрацію, класифікацію та супровід інцидентів?
3. Які системи обліку й управління інцидентами існують і чим вони відрізняються?
4. Що таке SOAR та які переваги і ризики автоматизації реагування?
5. Як інтегрують засоби моніторингу, аналізу та управління інцидентами?

ТЕМА 8. КОМАНДНИЙ ПІДХІД ДО РЕАГУВАННЯ НА ІНЦИДЕНТИ

Реагування на складні інциденти неможливе силами одного фахівця: воно потребує поєднання технічних, юридичних, управлінських та комунікаційних компетенцій. Автори підручника характеризують реагування як багатогранну дисципліну, у якій беруть участь IT-працівники, фахівці з безпеки, юристи, кадрові працівники, фахівці зі зв'язків із громадськістю, бізнес-менеджери та співробітники корпоративної служби безпеки [1]. Командний підхід означає, що ролі, повноваження й процедури визначено заздалегідь, а під час інциденту команда діє злагоджено під керівництвом уповноваженого менеджера.

Організаційна структура команд реагування зазвичай має три шари. Ядро становить постійна або оперативно сформована команда, яка проводить розслідування й організовує усунення наслідків. Його очолює менеджер інциденту, який має повноваження залучати ресурси інших підрозділів і ухвалювати рішення за вищого керівництва; без такої можливості ефективність реагування різко падає. До ядра входять аналітики з виявлення й аналізу журналів, фахівці з цифрової криміналістики, з аналізу мережевого трафіку, з первинного аналізу шкідливих програм, з розвідки про загрози. Другий шар – допоміжні команди, що залучаються за запитом: юристи, фахівці з відповідності, IT-підтримка, мережеві адміністратори, представники бізнесу, кадрів і комунікацій. Третій – зовнішні консультанти, правоохоронці та національні команди реагування [1].

Функції та завдання SOC, CSIRT і CERT різняться за акцентами, хоча на практиці перетинаються. Центр операцій безпеки (SOC) здійснює безперервний моніторинг, виявлення та первинне опрацювання подій: його працівники чергують у режимі 24/7, аналізують сповіщення й за потреби передають інциденти далі. Команда реагування на інциденти (CSIRT) спеціалізується на обробці підтверджених інцидентів – розслідуванні, локалізації, усуненні, відновленні, а також на координації та наданні рекомендацій. Термін CERT історично пов'язаний із координаційним

центром при Університеті Карнегі–Меллона й часто вживається для національних або секторальних команд, як-от CERT-UA, які поєднують реагування з координацією, інформуванням та обміном даними [15]. Перелік послуг, які можуть надавати такі команди, описано в Рамці послуг CSIRT, розробленій форумом FIRST.

Таблиця 8.1 – Порівняння SOC, CSIRT і CERT

Структура	**Основний фокус**	**Типові функції**
SOC	Моніторинг і виявлення	Нагляд за сповіщеннями, тріаж, первинне реагування
CSIRT	Обробка інцидентів	Розслідування, локалізація, усунення, відновлення
CERT	Координація та обмін	Попередження, довідки, співпраця, підтримка суб’єктів

Розподіл ролей і відповідальності між учасниками команди має бути задокументований. Типові ролі: менеджер інциденту, що керує процесом і ухвалює рішення; керівники напрямів – розслідування, усунення й комунікації; аналітики різних рівнів (перший рівень виконує тріаж, другий – поглиблений аналіз, третій – складні розслідування та пошук загроз); криміналісти, які збирають і зберігають докази; аналітики шкідливого коду; фахівці з розвідки; зв’язковий із юристами; відповідальний за зв’язки із зовнішніми сторонами. Для чіткості застосовують матрицю RACI та описи посад. Окрему увагу приділяють взаємозамінності, оскільки під час тривалого інциденту виникає втома, і потрібні ротації.

Координація дій під час розслідування й ліквідації ґрунтується на єдиному плані, спільному журналі справи та регулярному ритмі нарад. Менеджер інциденту розподіляє завдання між потоками роботи: розслідування й усунення виконують паралельно, але з обміном відомостями, оскільки результати першого визначають зміст другого. Для великих інцидентів створюють штаб із чітким порядком звітності й вимогою фіксувати всі рішення. Важливо, щоб технічні дії виконувались за узгодженим планом, а не

ініціативно, інакше можна випадково знищити докази чи насторожити зловмисника [1; 2].

Нарощування спроможностей команди вимагає навчань. Настільні вправи перевіряють процеси та комунікацію на уявному сценарії без технічних дій. Технічні симуляції відтворюють атаки на тестовому середовищі, щоб аналітики відпрацьовували виявлення та реагування. Командні навчання «червоних» і «синіх» команд, зокрема у формі спільних вправ, дають змогу оцінити покриття виявлення. На міжнародному рівні проводять великі кібервправи, наприклад Locked Shields, у яких беруть участь і українські фахівці. Результати навчань записують і перетворюють на завдання для вдосконалення планів, правил виявлення та програм підготовки [6].

Моделювання кіберінцидентів як навчальний інструмент має певні вимоги: реалістичний сценарій, спираючись на тактики з бази ATT&CK, чіткі цілі навчання, ролі учасників, спостерігачі й обов'язкова розмова після вправи [12]. Наприклад, сценарій атаки з викраденням облікових даних перевіряє виявлення нетипових входів, ескалацію, локалізацію та комунікацію з юристами. Навчання без наступного аналізу залишається розвагою; навпаки, регулярні, змістовні вправи формують «м'язову пам'ять» команди й скорочують час реакції під час справжнього інциденту.

Вибір моделі команди залежить від масштабу організації та ризиків. Невеликі установи часто мають лише кількох IT-фахівців і залучають зовнішніх партнерів за договором із гарантованим часом реакції, а великі формують власні SOC і CSIRT. Автори підручника відзначають, що навіть неформально створена власна команда підвищує шанси на успішне розслідування, адже вона знає середовище; зовнішні провайдери доцільно залучати для складних випадків і для додаткових спроможностей [1]. У будь-якому випадку відносини з постачальниками й порядок залучення мають бути узгоджені до інциденту.

Контрольні питання

1. Яка організаційна структура команд реагування на інциденти?

2. Чим відрізняються функції SOC, CSIRT і CERT?

3. Як розподіляють ролі й відповідальність у команді реагування?

4. Як координують дії під час розслідування й ліквідації інциденту?

5. Для чого проводять командні навчання та моделювання інцидентів?

ТЕМА 9. СТАНДАРТИ ТА НОРМАТИВНО-ПРАВОВІ АКТИ В ГАЛУЗІ ОБРОБКИ ІНЦИДЕНТІВ

Стандарти й нормативно-правові акти задають єдині вимоги до організації реагування, визначають терміни, відповідальність і строки звітування, а також дозволяють перевіряти відповідність процесів. Для фахівця важливо розрізняти документи, які мають обов'язкову силу (закони, директиви, регламенти, нормативні акти регуляторів), і документи рекомендаційного характеру (стандарти й настанови), які стають обов'язковими лише через договір чи рішення організації. Правильна практика поєднує обидва види, використовуючи стандарти як спосіб виконання нормативних вимог.

Міжнародні стандарти та рекомендації щодо управління інцидентами інформаційної безпеки представлені, насамперед, серією ISO/IEC 27035. Частина 1 (редакція 2023 року) визначає принципи й процес управління інцидентами: планування та підготовку, виявлення й звітування, оцінювання й ухвалення рішення, реагування, винесення уроків. Частина 2 (2023) містить настанови щодо планування та підготовки, зокрема створення політики, структури команди, технічної й організаційної підтримки, а також навчань. Раніше діяли ДСТУ, що ввели попередні редакції цієї серії; для навчальних цілей слід користуватися чинними версіями [4; 5]. Вимоги до управління інцидентами містяться й у ISO/IEC 27001:2022 у вигляді заходів Додатка A: планування та підготовка, оцінювання подій і ухвалення рішень, реагування, винесення уроків і збирання доказів.

Рекомендації NIST щодо реагування на інциденти найповніше викладені в SP 800-61 Rev. 3 (2025), яка адаптує реагування до функцій Рамки CSF 2.0 і підкреслює, що підготовка та вдосконалення є частиною загального управління кіберризиками, а не окремою діяльністю [2; 3]. Каталог заходів NIST SP 800-53 містить родину вимог до реагування на інциденти та пов'язані з нею вимоги щодо аудиту, моніторингу й безперервності [11]. Для роботи з цифровими доказами застосовують настанови стандарту ISO/IEC 27037 про ідентифікацію, збирання, отримання й збереження цифрових

доказів, а також пов’язані стандарти. Узагальнення практики наведено й у підручнику, який описує процес розслідування та роботу з доказами [1].

Правове регулювання на рівні ЄС задає директива NIS2: суб’єкти значущих і важливих секторів зобов’язані впроваджувати заходи управління ризиками, мати процеси обробки інцидентів і повідомляти про суттєві інциденти національну команду реагування або компетентний орган за етапами: раннє попередження, як правило, протягом 24 годин, повідомлення про інцидент протягом 72 годин і підсумковий звіт протягом місяця [8; 21]. Регламент DORA встановлює вимоги до класифікації та звітування про великі інциденти у сфері інформаційно-комунікаційних технологій у фінансових установах [9]. Загальний регламент захисту даних вимагає повідомляти наглядовий орган про порушення захисту персональних даних, як правило, протягом 72 годин.

Нормативно-правове регулювання кібербезпеки в Україні спирається на Закон «Про основні засади забезпечення кібербезпеки України» та Закон № 4336-IX, що імплементує підходи NIS2: він запровадив обов’язкову посаду керівника з кіберзахисту, змінив підхід до аудиту й сформував мережу національних, секторальних і регіональних команд реагування [17]. Державна команда CERT-UA діє при Держспецзв’язку; вона приймає повідомлення про інциденти, надає допомогу й виконує функцію національного контактного центру за NIS2 для взаємодії із закордонними партнерами [15; 18]. Наказом Адміністрації Держспецзв’язку від 14 травня 2026 року № 351 затверджено Порядок обміну інформацією про кіберінциденти та Критерії визначення значного кіберінциденту [16]. Під час масштабних кіберкриз діє Об’єднана група при Національному координаційному центрі кібербезпеки, що координує дії суб’єктів [18]. Крім того, для сектору діють галузеві вимоги регуляторів, наприклад Національного банку України.

Вимоги до повідомлення про кіберінциденти та їх документування зводяться до кількох положень. Суб’єкт має визначити критерії значного інциденту, мати процедуру внутрішньої оцінки, дотримуватися встановлених строків і форм, зазначати відомості про природу, масштаби, вплив, вжиті

заходи та, за можливості, індикатори компрометації. Документування охоплює реєстрацію, хронологію, докази, ухвалені рішення, повідомлення, звіт про усунення та уроки. Зберігання документів має відповідати вимогам законодавства й захищати чутливі відомості, а доступ до них – бути обмеженим і журналюваним [16].

Відповідність процедур реагування нормативним вимогам перевіряють через зіставлення вимог із процесами (картування), внутрішній аудит, навчання й незалежне оцінювання. Корисним інструментом є матриця відповідності, у якій кожна вимога закону чи стандарту пов'язана з процедурою, відповідальним і доказом виконання. Для організацій, що працюють у кількох юрисдикціях, ускладненням є різні строки й порядок повідомлення, тому процедури реагування мають передбачати декілька паралельних потоків звітності, які запускаються одночасно під час інциденту. Автори підручника наголошують, що вимоги юристів і регуляторів слід з'ясувати заздалегідь, бо середина розслідування – найгірший час для цього [1].

Таблиця 9.1 – Основні документи для обробки інцидентів

Документ	**Тип**	**Основний зміст**
ISO/IEC 27035-1, -2:2023	Міжнародний стандарт	Процес і підготовка до управління інцидентами
NIST SP 800-61 Rev. 3	Настанова	Реагування у складі CSF 2.0
Директива NIS2 (2022/2555)	Правовий акт ЄС	Управління ризиками, звітування в 24/72 години
Наказ Держспецзв'язку № 351	Український нормативний акт	Обмін інформацією, значний інцидент

Контрольні питання

1. Які міжнародні стандарти й рекомендації регулюють управління інцидентами?

2. Що містять ISO/IEC 27035 і NIST SP 800-61 Rev. 3?

3. Які вимоги до повідомлення про інциденти встановлює NIS2?

4. Як регулюється реагування на кіберінциденти в Україні?

5. Як перевіряють відповідність процедур реагування нормативним вимогам?

ТЕМА 10. ІНЦИДЕНТИ БЕЗПЕКИ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКА

Інформаційна безпека та кібербезпека тісно пов’язані, але не тотожні. Інформаційна безпека охоплює захист інформації в будь-якій формі – електронній, паперовій, усній – незалежно від того, де вона зберігається й передається. Кібербезпека зосереджена на захисті інформації та систем у кіберпросторі, тобто в середовищі, що утворюється взаємодією людей, програмного забезпечення та послуг у мережах. Кібербезпека входить до сфери інформаційної безпеки, але додає специфічні проблеми: цілеспрямовані віддалені атаки, глобальну досяжність зловмисників, взаємозалежність систем і ланцюгів постачання. Для реагування на інциденти важливо, що й паперовий документ, залишений без нагляду, і мережева атака є інцидентами інформаційної безпеки, але методи й інструменти їх опрацювання різні [4].

Основними джерелами кіберзагроз є кіберзлочинці, що мотивовані фінансовою вигодою; державно підтримувані групи, які займаються шпигунством і руйнівними операціями; хактивісти; внутрішні порушники; недбалість і помилки персоналу; природні й техногенні чинники. За оцінкою ENISA, у ландшафті загроз Європи домінують програми-вимагачі, атаки на ланцюги постачання, використання вразливостей, фішинг і соціальна інженерія, відмова в обслуговуванні за участю хактивістів, а також дії державних груп [7]. Українська практика додатково характеризується інтенсивною діяльністю країни-агресора проти цивільної та критичної інфраструктури, що підтверджують дані CERT-UA: у першому півріччі 2026 року опрацьовано 3 137 кіберінцидентів, найчастіше мішенями ставали органи місцевої влади й урядові організації, а переважну більшість становили розповсюдження й зараження шкідливим програмним забезпеченням та соціальна інженерія [19].

Вразливості інформаційних систем виникають через помилки в програмах, конфігураціях і процесах: непатчене програмне забезпечення, стандартні чи слабкі паролі, відсутність багатофакторної автентифікації,

надмірні привілеї, незахищені API та хмарні сховища, застарілі протоколи. Вразливості реєструються в системі CVE, їхню серйозність оцінюють за CVSS, а перелік уразливостей, що вже використовуються в реальних атаках, веде, зокрема, американське агентство CISA у каталозі відомих експлуатованих уразливостей. Для пріоритезації корисно враховувати не лише оцінку серйозності, а й факт експлуатації, доступність виправлення та значущість актива.

Типові сценарії реалізації кіберінцидентів мають спільну структуру, яку описує життєвий цикл атаки [1]. У сценарії із програмою-вимагачем зловмисник отримує доступ через фішинг або вразливий сервіс на периметрі, закріплюється, розвідує мережу, викрадає облікові дані адміністраторів, переміщується до серверів, знищує резервні копії, викрадає дані й нарешті шифрує системи. У сценарії атаки на ланцюг постачання шкідливий код потрапляє через довірене оновлення чи постачальника. У сценарії експлуатації вразливості веб-застосунку зловмисник отримує виконання коду, встановлює веб-оболонку й рухається вглиб. Знання сценаріїв дозволяє шукати сліди на кожному етапі та планувати розірвання ланцюга.

Аналіз кіберзагроз і індикаторів компрометації (IoC) охоплює збір, перевірку, контекстуалізацію й застосування відомостей про загрози. Індикатори є технічними слідами активності: хеші файлів, адреси, домени, URL, імена процесів і служб, ключі реєстру, правила для журналів. Вони мають різну цінність, що описує «піраміда болю»: зміна хешу чи адреси майже безкоштовна для зловмисника, а зміна тактик і методів обходиться дуже дорого, тому виявлення за поведінкою стійкіше за виявлення за індикаторами.

Таблиця 10.1 – Піраміда болю: типи індикаторів

Тип індикатора	**Складність зміни для зловмисника**	**Цінність для виявлення**
Хеші файлів	Тривіальна	Низька, коротка
Адреси та домени	Низька – помірна	Помірна
Артефакти й інструменти	Висока	Висока
Тактики, техніки,	Дуже висока	Найвища

Тип індикатора	Складність зміни для зловмисника	Цінність для виявлення
процедури		

Для опису тактик і технік зловмисників використовують базу MITRE ATT&CK – глобально доступну базу знань, що ґрунтується на реальних спостереженнях. Корпоративна матриця містить чотирнадцять тактик: розвідка, підготовка ресурсів, початковий доступ, виконання, закріплення, підвищення привілеїв, обхід захисту, отримання облікових даних, дослідження середовища, бічне переміщення, збирання, керування й контроль, ексфільтрація та вплив; кожна тактика поділяється на техніки й підтехніки [12]. ATT&CK застосовують, щоб структурувати розслідування, зіставляти спостережувані дії з відомими групами, оцінювати покриття виявлення, планувати навчання й формулювати звіти спільною мовою.

Практичне використання результатів аналізу охоплює оновлення правил виявлення, блокування індикаторів на периметрі та кінцевих точках, пошук загроз у середовищі, інформування керівництва й партнерів. Обмін індикаторами в стандартних форматах (STIX, TAXII) і через довірені спільноти дозволяє іншим учасникам виявити ту саму кампанію. Водночас індикаторам властиве старіння: потрібен термін придатності й перевірка на хибні спрацьовування, а під час публічного обміну слід дотримуватися маркування TLP [6; 12].

Контрольні питання

1. Як співвідносяться інформаційна безпека та кібербезпека?

2. Які основні джерела кіберзагроз і типові вразливості інформаційних систем?

3. Опишіть типові сценарії кіберінцидентів.

4. Що таке індикатори компрометації та піраміда болю?

5. Як використовують MITRE ATT&CK для дослідження тактик і технік зловмисників?

ТЕМА 11. ВІДНОВЛЕННЯ ПІСЛЯ ІНЦИДЕНТУ ТА ПЛАНУВАННЯ ЗАХОДІВ У РАЗІ ВИНИКНЕННЯ ІНЦИДЕНТІВ

Відновлення є завершальною частиною реагування й водночас початком наступного циклу підготовки. Його метою є повернення інформаційних систем і бізнес-процесів до нормального стану з гарантією, що причину усунено, а системи не містять залишкових шкідливих засобів. У підручнику відновленню присвячено цілу частину: розглянуто, як сформувати команду з усунення, вибрати час, розробити підготовчі заходи, заходи зі стримування й план ліквідації, а потім задокументувати отримані уроки [1].

Основні етапи відновлення інформаційних систем зазвичай такі. Спершу підтверджують, що локалізацію виконано й подальше розширення шкоди припинено. Далі відновлюють або перебудовують уражені системи з довірених образів і носіїв, а не «лікують» їх на місці, якщо ступінь компрометації не дозволяє довіряти системі. Змінюють облікові дані, що могли бути викрадені, відкликають ключі й сертифікати, виправляють вразливості, які використав зловмисник. Відновлюють дані з перевірених резервних копій, перевіряють їхню цілісність і чистоту, а потім послідовно вводять сервіси в роботу в порядку пріоритетів, посилено контролюючи їх. Завершальний етап – період підвищеного моніторингу, під час якого шукають ознаки повернення зловмисника.

Розроблення планів реагування та відновлення після кіберінцидентів виконують до того, як інцидент трапиться. План реагування на інциденти описує класифікацію, ролі, процедури, шаблони та контакти. План аварійного відновлення визначає, як відновити системи й дані, а план безперервності діяльності – як підтримувати критичні процеси під час збою. Основою для них слугує аналіз впливу на бізнес, у якому для кожного процесу встановлюють допустимий час простою (RTO), допустимий обсяг втрат даних (RPO) та максимально допустимий період порушення (MTPD). Між показниками діє співвідношення:

$$RTO + WRT \leq MTPD$$

де WRT – час відновлення роботи після технічного відновлення систем, наприклад на перевірку даних і повернення процесу. Плани мають бути конкретними, мають актуальні контакти й залежності та регулярно перевірятися [2; 5].

Резервне копіювання та відновлення даних належать до найкритичніших заходів, особливо в разі програм-вимагачів, які цілеспрямовано знищують резервні копії. Загальне правило «3-2-1» вимагає зберігати щонайменше три копії на двох різних типах носіїв, одну з яких – за межами основного майданчика; сучасна його версія додає одну копію, ізольовану або незмінну, та нуль помилок під час перевірки відновлення. Копії слід захищати від змін і окремо керувати доступом до них, а головне – регулярно тестувати відновлення: копія, яку не перевіряли, залишається припущенням. Для критичних систем слід також враховувати час, потрібний для відновлення великих обсягів, і залежності між службами, адже без каталогу автентифікації більшість сервісів не запуститься [6].

Забезпечення безперервності бізнес-процесів і відновлення працездатності критичних сервісів потребує узгодженості IT-планів із потребами бізнесу. Для сервісів, що не можуть чекати відновлення, будують резервні майданчики, кластери та резервування каналів; для менш критичних допускають ручні процедури на час збою. Організація має знати порядок запуску сервісів, мінімальний склад систем, необхідний для роботи, альтернативні способи роботи працівників і порядок інформування клієнтів. Практичним орієнтиром слугує стандарт ISO 22301 із системами управління безперервністю діяльності, а українська практика воєнного часу додала до планів питання перенесення сервісів у хмару й географічне розподілення даних.

Аналіз причин інцидентів і формування коригувальних та превентивних заходів завершують цикл. Аналіз першопричин відповідає на питання, чому подія стала можливою: яка вразливість чи прогалина в процесах дозволила атаці відбутися, чому її не було виявлено раніше, що завадило швидшому реагуванню. Методи включають хронологічний розбір, дерево причин,

питання «чому» кілька разів поспіль. Результатом є коригувальні заходи (усунути виявлену проблему) та превентивні заходи (запобігти подібним проблемам у майбутньому), кожен із відповідальним і строком. Розбір проводять у форматі без пошуку винних, інакше учасники приховуватимуть помилки [1; 2].

Типовими помилками відновлення, за спостереженнями авторів підручника, є недостатнє планування, час виконання, не узгоджений із зацікавленими сторонами, неповне усунення точок присутності зловмисника, забуті облікові дані та сервісні облікові записи, а також відсутність пізнішого моніторингу [1]. Тому відновлення розглядають як проєкт із планом, відповідальними, контрольними точками та критеріями завершення, а його результатом є не лише працюючі системи, а й оновлені плани, правила виявлення та програма навчання.

Контрольні питання

1. Які основні етапи відновлення інформаційних систем після інцидентів?
2. Як розробляють плани реагування та відновлення і які показники (RTO, RPO, MTPD) використовують?
3. Яких правил дотримуються під час резервного копіювання та відновлення даних?
4. Як забезпечують безперервність бізнес-процесів і відновлення критичних сервісів?
5. Як аналізують причини інцидентів і формують коригувальні та превентивні заходи?

ТЕМА 12. РОБОТА З ВНУТРІШНІМИ ТА ЗОВНІШНІМИ СТЕЙКХОЛДЕРАМИ ПІД ЧАС РЕАГУВАННЯ НА ІНЦИДЕНТИ

Зацікавлені сторони (стейкхолдери) процесу реагування – це особи та організації, на яких інцидент впливає або від яких залежить його успішне вирішення. Їх визначають заздалегідь на етапі підготовки, а не під час кризи. До внутрішніх належать вище керівництво, власники бізнес-процесів, IT-підрозділи (системні, мережеві, адміністратори застосунків), підрозділ інформаційної безпеки, юристи й відповідальні за відповідність, кадрова служба, фахівці зі зв’язків із громадськістю, служба фізичної безпеки та користувачі. До зовнішніх – національні команди реагування, регулятори, правоохоронні органи, постачальники й партнери, клієнти, страховики, зовнішні консультанти й експерти з криміналістики, ЗМІ [1].

Організація взаємодії між технічними підрозділами, керівництвом і користувачами ґрунтується на розподілі ролей та узгоджених очікуваннях. Технічні підрозділи надають дані, виконують завдання локалізації й відновлення, але потребують від команди безпеки чітких і виконуваних інструкцій. Керівництво очікує інформацію про масштаб, ризики й рішення, які потребують його затвердження, зокрема зупинення бізнес-сервісів, виплату викупу, публічні повідомлення. Користувачам повідомляють, що робити й чого не робити (наприклад, не вимикати комп’ютери без вказівки, не відкривати підозрілі листи), а також куди звертатися. Автори підручника підкреслюють, що очікування юристів і спеціалістів із дотримання вимог необхідно з’ясувати заздалегідь, бо з ними пов’язані пороги звітності й обмеження на збирання даних [1].

Особливе значення має співпраця з національними командами реагування. В Україні таку функцію виконує CERT-UA при Держспецзв’язку: вона приймає повідомлення, допомагає в аналізі й усуненні, поширює попередження та рекомендації, а як національний контактний центр за директивою NIS2 – інформує закордонні та міжнародні організації, якщо атака загрожує системам країн ЄС [15; 18]. Наказ Адміністрації Держспецзв’язку № 351 встановлює порядок передавання відомостей про

кіберінциденти та критерії значного інциденту, тому з ним мають бути узгоджені внутрішні процедури суб'єктів [16]. Держспецзв'язку також розвиває регіональні центри кіберзахисту й секторальні команди, що розширює коло партнерів для організацій різного рівня [17].

Взаємодія з правоохоронними органами потрібна в разі кримінальних проявів: викрадення даних і коштів, вимагання, втручання в роботу систем. В Україні це Департамент кіберполіції Національної поліції, Служба безпеки України в справах, що стосуються державної безпеки, та прокуратура. Звернення до правоохоронців слід готувати: узгодити з юристами, зберегти докази з дотриманням ланцюга відповідальності, підготувати стислу хронологію. Автори підручника радять визначити заздалегідь, коли залучати правоохоронні органи, адже розслідування встановлення причетних осіб комерційна команда здебільшого виконати не може [1]. Слід враховувати, що участь правоохоронців може вплинути на хід усунення, наприклад на вимогу зберегти активність зловмисника для збору даних.

Зовнішні експерти додають спроможності, яких бракує організації: глибокий аналіз шкідливого коду, цифрова криміналістика, досвід розслідування складних проникнень, масштабування команди. Їх залучають за договорами, які визначають склад послуг, строки реагування, відповідальність і порядок обміну даними. Практично корисно підписувати договір заздалегідь (так звана «передоплачена» послуга реагування), а під час інциденту виконувати залучення через юристів, щоб листування й результати були захищені правилами про професійну таємницю [1; 6]. Страховик у разі кіберстрахування часто має власний перелік схвалених постачальників, і про подію його необхідно повідомити за умовами договору.

Порядок обміну інформацією про інциденти повинен забезпечувати баланс між потребою ділитися й захистом чутливих відомостей. Правила визначають, який обсяг даних і кому передають, у якому форматі, з якими маркуваннями (протокол TLP), за яких умов. Технічні індикатори обмінюють у стандартних форматах STIX і TAXII, а також за допомогою платформ на кшталт MISP; персональні дані й комерційну таємницю передають лише за

наявності правових підстав та угод про нерозголошення. Для довіри між партнерами важливі взаємність і дотримання домовленостей про поширення отриманих відомостей [12].

Координація спільних заходів із локалізації й усунення кіберзагроз вимагає єдиного плану. Якщо атака зачіпає кілька організацій, наприклад постачальника та його клієнтів, дії мають бути синхронізовані за часом, щоб зловмисник не скористався розривом. Для цього призначають координатора, узгоджують спільні канали, ведуть спільну хронологію та погоджують повідомлення. Під час масштабних подій в Україні діє Об'єднана група при НКЦК, яка координує дії суб'єктів кіберзахисту [18]. Після завершення проводять спільний розбір, а його результати передають учасникам для вдосконалення процедур.

Таблиця 12.1 – Основні зацікавлені сторони та їхня роль

Сторона	**Роль у реагуванні**	**Коли залучати**
Керівництво	Рішення, ресурси, зовнішні заяви	Від підтвердження значного інциденту
Юристи	Вимоги до повідомлення, захист листування	З початку розслідування
CERT-UA, регулятори	Звітування, допомога, координація	За критеріями значного інциденту
Правоохоронці	Розслідування, збирання доказів	За ознак злочину
Зовнішні експерти	Криміналістика, аналіз ШПЗ, ресурси	За браку власних спроможностей

Контрольні питання

1. Хто є внутрішніми та зовнішніми зацікавленими сторонами під час реагування?

2. Як організувати взаємодію технічних підрозділів, керівництва й користувачів?

3. Як співпрацюють із національними командами реагування й правоохоронними органами?

4. Коли й як залучати зовнішніх експертів?

5. Як організовано обмін інформацією про інциденти та координацію спільних заходів?

ТЕМА 13. АУДИТ ТА ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМИ РЕАГУВАННЯ НА ІНЦИДЕНТИ

Аудит процесів реагування на інциденти – незалежна систематична перевірка того, наскільки спроможність організації виявляти інциденти й реагувати на них відповідає цілям, політикам, нормативним вимогам і реальним загрозам. Його **мета** полягає в оцінюванні того, чи працюють процеси на практиці, а не лише на папері, у виявленні прогалин та формуванні рекомендацій для вдосконалення. Завдання включають перевірку наявності й актуальності політик і планів, оцінювання ролей, ресурсів і компетенцій, перевірку технічних можливостей виявлення й збереження доказів, аналіз досвіду минулих інцидентів і перевірку виконання нормативних вимог щодо повідомлення. Методологічною основою є настанови зі стандартів аудиту систем управління, зокрема ISO/IEC 27007, і вимоги ISO/IEC 27035 щодо вдосконалення процесу [4; 5].

Методи оцінювання ефективності систем виявлення та реагування поєднують кілька підходів. Огляд документації й інтерв'ю дозволяють оцінити формальну основу й розуміння процедур персоналом. Аналіз записів про минулі інциденти показує, як процеси застосовуються: чи дотримано строки, чи повні записи, чи враховано уроки. Спостереження за навчаннями й настільними вправами виявляє слабкі місця в комунікації та прийнятті рішень. Технічні перевірки охоплюють тестування правил виявлення за допомогою імітації тактик зловмисників (відображених у базі ATT&CK), перевірку наявності й якості журналів, перевірку відновлення з резервних копій і тестування засобів реагування [12]. Спільні вправи команд нападу та захисту дають найреалістичнішу оцінку: вони показують, які дії супротивника не було виявлено і як довго це тривало.

Ключові показники ефективності реагування вимірюють швидкість і якість. Найвідоміші з них – середній час виявлення (MTTD) та середній час відновлення чи реагування (MTTR). Їх обчислюють за зареєстрованими інцидентами:

$$MTTD = (\Sigma(t_{виявл} - t_{початку})) / N; \quad MTTR = (\Sigma(t_{відновл} - t_{виявл})) / N$$

де tпочатку – оцінений момент початку інциденту, tвиявл – момент виявлення, tвідновл – момент відновлення, N – кількість інцидентів. Важливо чітко визначити, що вважати початком і кінцем, інакше значення не можна порівнювати. Крім середніх, корисні медіани й верхні процентилі, оскільки поодинокі тривалі інциденти спотворюють середнє. Доповнюють їх середній час до підтвердження та до локалізації, частка інцидентів, виявлених власними засобами, частка закритих у строк, кількість повторних інцидентів і хибних спрацьовувань на аналітика.

Таблиця 13.1 – Приклади показників ефективності

Показник	**Що вимірює**	**Як інтерпретувати**
MTTD	Швидкість виявлення	Менше – краще; залежить від покриття
MTTR	Швидкість відновлення	Менше – краще; враховувати критичність
Частка власного виявлення	Зрілість моніторингу	Зростання свідчить про покращення видимості
Повторні інциденти	Якість усунення причин	Зниження – ознака ефективних коригувань

Аналіз відповідності процедур реагування встановленим політикам і стандартам виконують порівнянням вимог (політик, ISO/IEC 27001 і 27035, NIST SP 800-61 Rev. 3, нормативних актів) із фактичними практиками, шукаючи відхилення, їх причини й наслідки [2; 4]. Відхилення класифікують за суттєвістю, а для кожного встановлюють першопричину й коригувальний захід. Для оцінювання зрілості застосовують моделі зрілості: наприклад, рівні впровадження Рамки кібербезпеки NIST та модель зрілості управління інцидентами для команд реагування (SIM3), що дозволяють порівнювати поточний і цільовий стан [3].

Розроблення рекомендацій щодо вдосконалення системи управління інцидентами завершує аудит. Рекомендації мають бути конкретними, обґрунтованими результатами перевірок, пріоритезованими за ризиками, мати відповідальних і строки. Типові рекомендації стосуються розширення джерел

журналів, скорочення часу переходу від сповіщення до дії, автоматизації рутинних операцій, оновлення планів, посилення навчання, підготовки контактів зовнішніх сторін і тестування відновлення. Звіт аудиту подають керівництву, а виконання рекомендацій відстежують до закриття, після чого перевіряють їхню результативність.

Аудит доцільно проводити регулярно й поєднувати з постійним самоконтролем. Внутрішній аудит виконують за річним планом, зовнішній – за потреби підтвердження для регуляторів, партнерів чи страховиків. Автори підручника наголошують на ролі контролю якості та аналізу уроків після кожного інциденту, що є найдешевшим способом удосконалення [1]. Нормативні вимоги в Україні й ЄС дедалі більше зміщують акцент із формальних перевірок на оцінювання реального стану кіберзахисту й спроможності реагувати, тому показники та докази ефективності стають частиною звітності перед регуляторами [8; 17].

Контрольні питання

1. Які мета й завдання аудиту процесів реагування на інциденти?
2. Які методи оцінювання ефективності виявлення та реагування існують?
3. Як обчислюють MTTD та MTTR і які обмеження цих показників?
4. Як аналізують відповідність процедур реагування політикам і стандартам?
5. Як формують рекомендації щодо вдосконалення системи управління інцидентами?

ТЕМА 14. ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ДЛЯ ЗБОРУ, АНАЛІЗУ ТА ВІЗУАЛІЗАЦІЇ ДАНИХ ВІДНОСНО ІНЦИДЕНТІВ

Інструментальні засоби реагування охоплюють весь ланцюг обробки даних: збір артефактів із вузлів і мереж, їх зберігання та обробку, аналіз, візуалізацію й подання результатів. Автори підручника наголошують, що вибір інструмента має підпорядковуватися меті, а не навпаки: перед збиранням слід визначити, які питання треба з'ясувати, і лише потім обрати, що та як збирати. Інструмент, який змінює стан системи або знищує докази, може зашкодити розслідуванню, тому кожен засіб слід перевіряти й документувати його використання [1]. Відомі приклади різних класів засобів наведено в таблиці.

Таблиця 14.1 – Класи інструментів для роботи з інцидентами

Клас	**Приклади**	**Призначення**
Збір з вузлів	Velociraptor, osquery, KAPE, агенти EDR і Wazuh	Збір артефактів, опитування вузлів
Пам'ять і диски	Volatility 3, FTK Imager, Autopsy, Sleuth Kit	Криміналістика пам'яті й носіїв
Мережа	Wireshark, Zeek, Suricata, Arkime	Аналіз трафіку, виявлення, зберігання пакетів
Журнали й SIEM	Elastic, Splunk, Graylog, Wazuh	Збір, пошук, кореляція
Розвідка й обмін	MISP, OpenCTI	Індикатори, кампанії, обмін

Програмні засоби збору та обробки інформації про події безпеки поділяють за способом роботи. Збирання живих даних із працюючої системи фіксує нестійкі відомості – запущені процеси, мережеві з'єднання, відкриті файли, вміст пам'яті, – які зникнуть після вимкнення; автори підручника радять виконувати його, коли ці дані мають значення, застосовуючи перевірені засоби, що мінімально змінюють систему [1]. Для масового опитування вузлів використовують платформи збору артефактів на кшталт Velociraptor, що виконують запити до сотень і тисяч вузлів і повертають результати в центральне сховище [14]. Криміналістичне дублювання створює побітову копію диска із застосуванням блокувальників запису та перевіркою

цілісності хешем, а зображення зберігають у відомих форматах і працюють лише з копіями. Для аналізу пам’яті застосовують фреймворк Volatility, для файлових систем – набір Sleuth Kit й оболонку Autopsy.

Використання SIEM-платформ для аналізу інцидентів дозволяє швидко знаходити пов’язані події в усьому середовищі: за ідентифікатором користувача, адресою вузла, хешем файлу чи доменом. Аналітик будує запити, групує результати, формує часову лінію, збагачує дані даними про активи й розвідувальною інформацією, зберігає запити як шаблони для повторного використання. Для побудови часових ліній із різнорідних артефактів застосовують засоби обробки на кшталт Plaso та систему спільного аналізу Timesketch. Платформу слід налаштовувати так, щоб ключові поля були нормалізовані, а часові мітки – узгоджені, інакше кореляція стане складною [6; 13].

Інструменти аналізу мережевого трафіку та системних журналів відповідають різним завданням. Wireshark дає змогу детально вивчати окремі пакети й потоки; Zeek перетворює трафік на структуровані журнали про з’єднання, DNS, HTTP, TLS, які зручні для пошуку; Suricata поєднує виявлення за сигнатурами з вилученням метаданих; Arkime зберігає повні пакети й індексує їх для пошуку. Системні журнали Windows аналізують спеціальними засобами обробки подій, а Linux – засобами командного рядка й журналами аудиту. Для вилучення артефактів Windows (журнали подій, реєстр, файлова таблиця, заплановані завдання, артефакти запуску програм) використовують набори інструментів, описаних у розділах підручника про дослідження систем Windows [1].

Візуалізація подій безпеки за допомогою інформаційних панелей допомагає швидко зрозуміти стан і виявити відхилення. Панель оперативного чергового містить кількість відкритих інцидентів за пріоритетами, час реакції, хід обробки, джерела сповіщень; панель керівника – тенденції, ключові показники й ризики; панель аналітика – карту з’єднань, найактивніші вузли, розподіл подій за часом. Принципи якісної візуалізації: одне питання – один показник, зрозумілі масштаби, обережність із кольорами та відсутність

надмірного шуму. Для побудови панелей використовують модулі SIEM, інструменти на кшталт Kibana та Grafana.

Побудова звітів, графіків і часових діаграм інцидентів перетворює дані на знання. Часова діаграма показує послідовність подій від початкового доступу до виявлення та відновлення, виявляючи «сліпі зони» й затримки. Граф зв'язків демонструє переміщення зловмисника між вузлами та облікові записи, що використовувалися. Діаграма розподілу за тактиками ATT&CK показує, на яких етапах атаку було зупинено чи пропущено [12]. Звіт має відповідати вимогам: чіткі висновки, докази для кожного твердження, окремі розділи для керівництва й техніків; автори підручника окремо підкреслюють значення якості звітності та її відповідності стандартам [1].

Автоматизація аналізу та формування сповіщень про загрози зменшує час реакції. Правила виявлення описують у переносних форматах (Sigma, YARA), збагачення виконують автоматично через інтеграції з сервісами розвідки, а типові дії – за плейбуками SOAR. Важливо підтримувати якість: тестувати правила, відстежувати хибні спрацьовування, переглядати застарілі та документувати зміни. Автоматизація не знімає потреби в аналітику, а розвантажує його, залишаючи час для складних випадків [6].

Контрольні питання

1. Які програмні засоби збору й обробки інформації про події безпеки існують?

2. Як застосовують SIEM-платформи для аналізу інцидентів?

3. Які інструменти використовують для аналізу мережевого трафіку та журналів?

4. Як візуалізують події безпеки за допомогою інформаційних панелей?

5. Як будують звіти, графіки та часові діаграми інцидентів і автоматизують сповіщення?

ТЕМА 15. ПОРІВНЯННЯ РІЗНИХ ПІДХОДІВ ДО РЕАГУВАННЯ НА ІНЦИДЕНТИ В РІЗНИХ СФЕРАХ ДІЯЛЬНОСТІ

Принципи реагування на інциденти однакові для всіх організацій, проте пріоритети, регуляторні вимоги, обмеження й ризики істотно відрізняються залежно від сфери діяльності. Те, що виправдано для офісної мережі компанії, може бути неприйнятним для лікарні чи заводу, де вимкнення системи загрожує життю людей або безпеці виробництва. Тому в кожній сфері процес реагування адаптують, зберігаючи спільну структуру: підготовку, виявлення, аналіз, локалізацію, усунення, відновлення й винесення уроків [2; 4].

Державні установи мають особливості, пов'язані з обробкою інформації з обмеженим доступом і державних реєстрів, суворими вимогами до захисту та підзвітності, а також із різним рівнем ресурсів: центральні органи мають власні підрозділи, а органи місцевої влади нерідко залежать від зовнішньої підтримки. Статистика CERT-UA свідчить, що саме місцеві органи влади становлять найбільшу частку цілей: 37 % інцидентів у першому півріччі 2026 року [19]. Тому державна політика розвиває регіональні центри кіберзахисту й регіональні команди реагування, що працюватимуть за принципом «єдиного вікна» [17].

Фінансові організації працюють у середовищі жорсткого регулювання, високої залежності від доступності сервісів і постійної мотивації зловмисників до фінансової вигоди. Для них характерні вимоги швидкого повідомлення регуляторів (у ЄС – регламент DORA), широке використання засобів моніторингу шахрайства, тісна взаємодія з платіжними системами, банками-партнерами та правоохоронцями, відпрацьована безперервність і відновлення [9]. Критичними є цілісність транзакцій і довіра клієнтів, тож комунікації з клієнтами посідають одне з перших місць.

Медичні заклади поєднують великі обсяги чутливих персональних даних з обов'язковою безперервністю надання допомоги. Програма-вимагач у лікарні може зупинити діагностику й планові операції, тому пріоритетом є безпека пацієнтів і швидке відновлення, а не повне розслідування. Складнощами є застаріле обладнання, яке не можна швидко оновити, велика кількість

підключених медичних пристроїв, обмежені ресурси. Яскравим прикладом став інцидент 2021 року в ірландській системі охорони здоров'я, коли атака вимагача змусила перейти на паперові процеси на тривалий час. Для українських закладів існують власні вимоги електронної системи охорони здоров'я та захисту персональних даних.

Промислові підприємства та критична інфраструктура використовують системи керування технологічними процесами (OT/ICS), для яких доступність і безпека людей важливіші за конфіденційність. Систему не можна легко перезавантажити чи оновити, традиційні засоби виявлення можуть порушити її роботу, мережі часто слабо сегментовані, а протоколи не мають автентифікації. Реагування потребує тісної співпраці з технологічним персоналом, пасивного моніторингу, чіткої сегментації між корпоративною мережею та технологічною, здатності працювати в ручному режимі та планів відновлення, узгоджених із вимогами безпеки; застосовують серію стандартів IEC 62443. Приклад: у квітні 2022 року українські та міжнародні фахівці зупинили спробу атаки на енергетичну інфраструктуру з використанням модифікованого шкідливого програмного забезпечення Industroyer2.

Таблиця 15.1 – Особливості реагування за сферами

Сфера	**Головний пріоритет**	**Ключова особливість**
Державні установи	Захист державних даних і сервісів	Нерівномірні ресурси, регуляторна підзвітність
Фінансові організації	Цілісність і доступність транзакцій	Строгі строки звітування, робота з клієнтами
Медичні заклади	Безпека пацієнтів	Безперервність допомоги, застаріле обладнання
Промислові підприємства	Безпека й доступність процесів	Обмежені можливості патчингу, OT/IT-сегментація

Порівняння централізованих і децентралізованих моделей реагування показує компроміс між єдністю підходів і гнучкістю. Централізована модель

має єдину команду, що обробляє інциденти для всієї організації: вона накопичує досвід, забезпечує єдину політику й зручна для контролю, але може бути повільною та віддаленою від бізнесу. Децентралізована модель розподіляє функції між підрозділами чи філіями: рішення ухвалюють швидше й ближче до систем, але виникає ризик розбіжностей у якості та дублювання. Поширена гібридна модель, у якій центральна команда задає політику, інструменти й координує складні інциденти, а локальні групи виконують первинне реагування. Така логіка відображена й у національних системах: державна команда координує, а регіональні та секторальні виконують оперативні завдання [17; 18].

Особливості реагування в хмарних, корпоративних і промислових системах визначаються тим, хто керує інфраструктурою. У хмарі діє модель розподіленої відповідальності: клієнт не має доступу до фізичних носіїв і низькорівневих даних, тому розслідування спирається на журнали платформи, ідентичності та знімки систем; ресурси можуть бути короткочасними й зникати разом із доказами, а тому журналювання слід увімкнути заздалегідь. У корпоративних мережах більше можливостей контролю, але вища складність і наявність застарілих систем. У промислових середовищах діють обмеження, описані вище [1; 10].

Аналіз практичних сценаріїв допомагає закріпити розуміння. Атака на американського оператора трубопроводу Colonial Pipeline в 2021 році показала, що компанія зупинила операції через неможливість гарантувати безпеку, хоча шифрування торкнулося лише IT-систем. Руйнівна атака на мобільного оператора «Київстар» у грудні 2023 року наочно продемонструвала вплив на доступність послуг для мільйонів абонентів і значення відновлення критичних сервісів. Атака на ланцюг постачання SolarWinds показала складність виявлення прихованих, терплячих кампаній. Аналізуючи такі випадки, слід розглядати вектор, виявлення, рішення з локалізації, комунікацію та відновлення.

Критерії вибору ефективних стратегій реагування відповідно до специфіки діяльності організації охоплюють такі питання: що найкритичніше

(безпека людей, доступність, цілісність, конфіденційність), які нормативні вимоги та строки діють, які технічні обмеження є в системах, якими ресурсами й компетенціями володіє організація, який рівень ризику прийнятний, і як взаємодіяти із зовнішніми партнерами. Відповіді задають вибір між негайним відключенням і спостереженням, між самостійним відновленням і залученням зовнішніх експертів, між централізованим і розподіленим управлінням. Найкращою стратегією є та, що заздалегідь описана, перевірена на навчаннях і відповідає специфіці організації [2; 6; 20].

Контрольні питання

1. Чим відрізняється реагування на інциденти в державних установах, фінансових організаціях, медичних закладах і промислових підприємствах?

2. Порівняйте централізовані та децентралізовані моделі реагування.

3. Які особливості реагування в хмарних, корпоративних і промислових системах?

4. Які уроки можна винести з практичних сценаріїв кіберінцидентів?

5. За якими критеріями обирають стратегію реагування для конкретної організації?

СПИСОК ЛІТЕРАТУРИ

1. Luttgens J. T., Pepe M., Mandia K. Incident Response & Computer Forensics. 3rd ed. New York : McGraw-Hill Education, 2014. (використано український переклад, наданий кафедрою).

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

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

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

5. ISO/IEC 27035-2:2023. Information technology. Information security incident management. Part 2: Guidelines to plan and prepare for incident response. Geneva : ISO, 2023.

6. Johansen G. Digital Forensics and Incident Response. 3rd ed. Birmingham : Packt Publishing, 2022. URL: https://www.oreilly.com/library/view/digital-forensics-and/9781803238678/ (дата звернення: 14.11.2026).

7. ENISA Threat Landscape 2025. Heraklion : ENISA, 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (дата звернення: 14.11.2026).

8. 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.

9. 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.

10. Whitman M. E., Mattord H. J. Management of Cybersecurity. 7th ed. Boston : Cengage Learning, 2026. 546 p.

11. NIST SP 800-53 Rev. 5 (Release 5.2.0). Security and Privacy Controls for Information Systems and Organizations. Gaithersburg : National Institute of Standards and Technology, 2025. DOI: https://doi.org/10.6028/NIST.SP.800-53r5.

12. MITRE ATT&CK. MITRE Corporation. URL: https://attack.mitre.org/ (дата звернення: 14.11.2026).

13. Monitoring Network Devices with Wazuh. Wazuh. URL: https://wazuh.com/blog/monitoring-network-devices/ (дата звернення: 14.11.2026).

14. Velociraptor: Digging Deeper. GitHub. URL: https://github.com/Velocidex/velociraptor (дата звернення: 14.11.2026).

15. CERT-UA. Урядова команда реагування на комп'ютерні надзвичайні події України. URL: https://cert.gov.ua/ (дата звернення: 14.11.2026).

16. Про затвердження Порядку обміну інформацією про кіберінциденти та Критеріїв визначення значного кіберінциденту : наказ Адміністрації Держспецзв'язку від 14 трав. 2026 р. № 351. Урядовий портал. URL: https://www.kmu.gov.ua/news/derzhspetszviazku-vyznachyla-poriadok-obminu-informatsiieiu-pro-kiberintsydenty-ta-kryterii-vyznachennia-znachnoho-kiberintsydentu (дата звернення: 14.11.2026).

17. Держспецзв'язку: Україна трансформує систему кібербезпеки за європейськими стандартами (до Закону України № 4336-IX). Урядовий портал. URL: https://www.kmu.gov.ua/news/derzhspetszviazku-ukraina-transformuie-systemu-kiberbezpeky-za-ievropeiskymy-standartamy (дата звернення: 14.11.2026).

18. Затвердили порядок дій у кіберкризі: координуватиме Об'єднана група при НКЦК. ЛІГА:ЗАКОН. URL: https://biz.ligazakon.net/news/246644_zatverdili-poryadok-dy-u-kberkriz-koordinuvatime-grupa-pri-nktsk (дата звернення: 14.11.2026).

19. У першому півріччі 2026 року кількість кіберінцидентів в Україні зросла на 8 %. DEV.UA. URL: https://dev.ua/news/u-pershomu-pivrichchi-2026-

roku-kilkist-kiberintsydentiv-v-ukraini-zrosla-na-8-1790769498 (дата звернення: 14.11.2026).

20. Santos O. Developing Cybersecurity Programs and Policies in an AI-Driven World. 4th ed. Hoboken : Pearson, 2025.

21. NIS2 Technical Implementation Guidance. Heraklion : ENISA, 2025. URL: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance (дата звернення: 14.11.2026).

Обробка інцидентів та реагування: 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, Р.В. Вознюк. Луцьк: ЛНТУ, 2026. 60 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