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

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

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: _____ Олег КУЛАКЕВИЧ, ас. кафедри кібербезпеки ЛНТУ

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

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

Управління інформаційною безпекою: 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. О. Р. Кулакевич. Луцьк: ЛНТУ, 2026. 64 с.

ЗМІСТ

ЗМІСТ 3

ВСТУП 5

ЛЕКЦІЯ 1. ПЕРЕДУМОВИ ТА ОСНОВНІ НАПРЯМКИ РОЗВИТКУ МЕНЕДЖМЕНТУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. УПРАВЛІННЯ КІБЕРІНЦИДЕНТАМИ 7

ЛЕКЦІЯ 2. ДІЯЛЬНІСТЬ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 11

ЛЕКЦІЯ 3. СТАНДАРТИЗАЦІЯ В СФЕРІ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 15

ЛЕКЦІЯ 4. РОБОТИ СПЕЦІАЛІЗОВАНИХ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ ТА ОБ'ЄДНАНЬ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. УПРАВЛІННЯ РИЗИКАМИ В ІНФОРМАЦІЙНІЙ ТА КІБЕРБЕЗПЕЦІ 18

ЛЕКЦІЯ 5. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА РІВНІ ВЕЛИКИХ ПОСТАЧАЛЬНИКІВ ІНФОРМАЦІЙНИХ СИСТЕМ 22

ЛЕКЦІЯ 6. ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА США 26

ЛЕКЦІЯ 7. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ 29

ЛЕКЦІЯ 8. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ (КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ) 32

ЛЕКЦІЯ 9. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ (ТЕХНІЧНІ МЕТОДИ ЗАХИСТУ). ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИННОСТІ. СТАН КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ. БОРОТЬБА ІЗ КІБЕРЗЛОЧИНАМИ 36

ЛЕКЦІЯ 10. МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РІВНІ ПІДПРИЄМСТВА: ОСНОВНІ НАПРЯМКИ І СТРУКТУРА ПОЛІТИКИ БЕЗПЕКИ 40

ЛЕКЦІЯ 11. ЗМІСТ ДЕТАЛІЗОВАНОЇ ПОЛІТИКИ БЕЗПЕКИ 43

ЛЕКЦІЯ 12. ДЕПАРТАМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ І РОБОТА З ПЕРСОНАЛОМ 46

ЛЕКЦІЯ 13. ОРГАНІЗАЦІЯ РЕАГУВАННЯ НА НАДЗВИЧАЙНІ СИТУАЦІЇ (ІНЦИДЕНТИ) 49

ЛЕКЦІЯ 14. АУДИТ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ. НАДАННЯ ПОСЛУГ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (СТРАХУВАННЯ) 52

ЛЕКЦІЯ 15. МІЖНАРОДНИЙ СТАНДАРТ ISO/IEC 27001 ПЕРЕЛІК ЗАХИСНИХ ЗАХОДІВ ТА ЇХ ЦІЛЕЙ 56

СПИСОК ЛІТЕРАТУРИ 60

ВСТУП

Навчальна дисципліна «Управління інформаційною безпекою» формує в майбутніх фахівців із кібербезпеки управлінський рівень мислення: уміння розглядати захист інформації не як набір окремих технічних засобів, а як цілеспрямовану, плановану й контрольовану діяльність організації, підпорядковану її бізнес-цілям і регуляторним вимогам. Сучасна практика підтверджує, що більшість успішних атак пов’язана не з відсутністю певного засобу захисту, а з прогалинами в керуванні: неповним обліком активів, неузгодженими політиками, невизначеною відповідальністю, слабким контролем персоналу та постачальників. Саме тому міжнародні стандарти й нормативні акти останніх років, зокрема ISO/IEC 27001:2022, NIST Cybersecurity Framework 2.0 та Директива (ЄС) 2022/2555 (NIS2), ставлять вимоги до управління, лідерства та підзвітності вищого керівництва [1; 7; 11].

Конспект лекцій охоплює п’ятнадцять тем, що відповідають робочій програмі дисципліни. Перша половина курсу присвячена передумовам і міжнародному та державному рівням управління: основним поняттям і етапам розвитку менеджменту інформаційної безпеки, діяльності міжнародних організацій, стандартизації, управлінню ризиками, практикам великих постачальників інформаційних систем, а також організації безпеки на державному рівні в США та Україні, включно з криптографічними й технічними методами захисту та протидією кіберзлочинності. Друга половина курсу розкриває рівень підприємства: структуру політики безпеки, зміст детальних політик, роботу підрозділу безпеки з персоналом, реагування на надзвичайні ситуації, аудит і кіберстрахування та перелік захисних заходів, визначений стандартом ISO/IEC 27001:2022.

Основою для викладу є сучасні підручники та нормативні джерела. Методологічну канву задає підручник М. Уітмена і Г. Метторда «Management of Cybersecurity» (7-ме видання, 2026), що послідовно розглядає управління кібербезпекою як складову корпоративного менеджменту [6]. Положення стандартів і рамкових документів наведено за чинними редакціями: ISO/IEC

27001:2022 та 27002:2022, ISO/IEC 27005:2022, NIST CSF 2.0 (2024), NIST SP 800-61 Rev. 3 (2025), звітами ENISA 2025 року. Українське регулювання викладено з урахуванням Закону № 4336-IX, що імплементує підходи Директиви NIS2, та підзаконних актів, ухвалених у 2025–2026 роках [3; 4; 5; 19].

Кожна лекція викладена суцільним текстом без поділу на підпункти й завершується контрольними питаннями для самоперевірки. Матеріал побудовано від загального до часткового: від понять і принципів до конкретних механізмів та практичних регламентів. Після опанування курсу здобувач має вміти пояснювати структуру та взаємозв’язок складових системи управління інформаційною безпекою, застосовувати ризик-орієнтований підхід, орієнтуватися в системі міжнародних і національних стандартів, розробляти положення політик безпеки, організовувати реагування на кіберінциденти та готуватися до аудиту й сертифікації. Слід зважати, що нормативна база у сфері кібербезпеки змінюється швидко, тому перед практичним застосуванням положень конспекту необхідно звіряти їх із чинними редакціями документів.

ЛЕКЦІЯ 1. ПЕРЕДУМОВИ ТА ОСНОВНІ НАПРЯМКИ РОЗВИТКУ МЕНЕДЖМЕНТУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. УПРАВЛІННЯ КІБЕРІНЦИДЕНТАМИ

Управління інформаційною безпекою (УІБ) – це цілеспрямована діяльність з планування, організації, мотивації та контролю заходів, що забезпечують конфіденційність, цілісність і доступність інформації та підтримують досягнення цілей організації [6]. Менеджмент у цій сфері виник як відповідь на кілька взаємопов'язаних процесів. По-перше, бізнес-процеси, державне управління й повсякденне життя майже повністю залежать від інформаційних систем, тому збій або компрометація системи безпосередньо означає фінансові, репутаційні та правові втрати. По-друге, зросла кількість, складність і організованість загроз: від поодиноких зловмисників до злочинних угруповань і державно підтримуваних груп, що діють із використанням програм-вимагачів, атак на ланцюг постачання та соціальної інженерії [4]. По-третє, посилився регуляторний тиск: закони й директиви покладають на керівництво безпосередню відповідальність за стан кіберзахисту.

Історично захист інформації розпочинався як технічна задача. У 1970–1980-х роках у центрі уваги були моделі розмежування доступу, критерії оцінки захищених систем і засоби криптографії. Зі зростанням мережевої взаємодії стало очевидним, що навіть досконалі засоби не працюють без політик, процедур і дисциплінованого персоналу, тож акцент змістився з окремих механізмів на систему управління. Результатом стало формування менеджменту інформаційної безпеки як окремого напряму, у межах якого безпека розглядається як керований процес із визначеними цілями, ресурсами, відповідальними особами та показниками результативності.

До основних понять належать актив (будь-що, що має цінність для організації), загроза (потенційна причина небажаного інциденту), вразливість (слабкість активу чи заходу захисту), ризик (вплив невизначеності на цілі, що виявляється як можливість реалізації загрози через вразливість), захисний захід (засіб зміни ризику), політика безпеки (документ, що виражає наміри та

напрями керівництва) і система управління інформаційною безпекою (СУІБ) – сукупність політик, процесів і ресурсів, що спрямовують та контролюють безпеку. Базові принципи охоплюють забезпечення конфіденційності, цілісності й доступності, а також автентичності та спостережуваності; управлінські принципи включають лідерство вищого керівництва, пропорційність заходів ризикам, захист у глибину, мінімальні привілеї, розподіл обов'язків і постійне вдосконалення. Завданнями УІБ є визначення цілей і стратегії безпеки, розподіл повноважень, виявлення та оцінювання ризиків, вибір і впровадження заходів, контроль їх дієвості, навчання персоналу та реагування на інциденти.

Системний підхід вимагає розглядати інформаційну безпеку як властивість цілісної соціотехнічної системи, у якій взаємодіють люди, процеси, технології та зовнішнє середовище. Це означає, що локальне посилення одного елемента не гарантує підвищення безпеки загалом: надійний міжмережевий екран не компенсує слабких паролів чи відсутності контролю підрядників. Ризик-орієнтований підхід доповнює системний, пропонуючи розподіляти ресурси відповідно до величини ризиків. Замість прагнення до абсолютного захисту організація визначає прийнятний рівень ризику, порівнює з ним результати оцінювання й обирає заходи, вартість яких виправдана очікуваним зниженням втрат. Саме такий підхід покладено в основу ISO/IEC 27001:2022, ISO/IEC 27005:2022 і NIST CSF 2.0 [1; 7; 9].

Етапи розвитку систем менеджменту безпеки добре простежуються на історії стандартів. Британський стандарт BS 7799, що з'явився в середині 1990-х років, зафіксував перелік практичних заходів; на його основі виник міжнародний стандарт ISO/IEC 17799, а згодом, із введенням вимог до системи управління, – ISO/IEC 27001 (2005). Редакція 2013 року узгодила структуру з іншими стандартами систем менеджменту, а редакція 2022 року зорієнтувала вимоги на сучасні технологічні реалії та переглянула перелік заходів [7; 8]. Паралельно NIST у 2024 році випустив версію 2.0 Рамки кібербезпеки, додавши до п'яти функцій шосту – «Управління» (Govern), що підкреслює роль корпоративного менеджменту, стратегії, ролей і нагляду [1].

Ця еволюція виражає загальну тенденцію: від технічних контролів до організаційної зрілості й управління ризиками в ланцюгах постачання.

Кіберінцидент – подія або сукупність подій, що порушують чи загрожують порушити конфіденційність, цілісність або доступність інформації та інформаційних систем, або порушують політики безпеки. Інциденти класифікують за декількома ознаками. За типом розрізняють зараження шкідливим програмним забезпеченням, у тому числі програмами-вимагачами, несанкціонований доступ і компрометацію облікових записів, атаки на доступність (DDoS), витік або викрадення даних, соціальну інженерію та фішинг, внутрішні зловживання, фізичні інциденти. За наслідками їх поділяють за рівнями критичності: у практиці українського CERT-UA застосовується шкала від низького до критичного рівня, що залежить від масштабу, значущості уражених систем і впливу на послуги. За джерелом виокремлюють зовнішні й внутрішні, навмисні та ненавмисні інциденти.

Організація виявлення й обробки інцидентів передбачає створення відповідальної команди або функції, визначення каналів повідомлення про події, формування критеріїв пріоритезації та регламентів дій. Виявлення ґрунтується на моніторингу журналів подій, системах корелювання (SIEM), засобах захисту кінцевих точок, аналізі мережевого трафіку, розвідувальних даних про загрози та повідомленнях користувачів. Аналіз полягає в підтвердженні факту інциденту, визначенні його обсягу, вектора та впливу. Локалізація обмежує поширення шкоди, наприклад ізоляцією вузлів, блокуванням облікових записів чи відкликанням ключів. Усунення охоплює видалення причини, закриття вразливості та відновлення нормальної роботи з перевіркою цілісності даних.

Життєвий цикл управління інцидентами в сучасних документах трактується як безперервний процес, інтегрований у загальне управління ризиками. Остання редакція настанови NIST SP 800-61 Rev. 3 (2025) відмовилася від лінійної чотирифазної моделі та пов’язала реагування з функціями CSF 2.0: підготовка й управління належать до функцій

«Управління», «Ідентифікація» й «Захист», а безпосереднє реагування – до функцій «Виявлення», «Реагування» та «Відновлення» [2]. Стандарт ISO/IEC 27035-1:2023 описує схожу послідовність: планування й підготовка, виявлення та повідомлення, оцінювання й ухвалення рішення, реагування, винесення уроків [10]. Обидва підходи наголошують, що висновки після інциденту мають повертатися в політики, навчання та вибір заходів, а ефективність процесу вимірюється показниками на кшталт середнього часу виявлення та середнього часу відновлення.

Контрольні питання

1. Дайте визначення управління інформаційною безпекою та назвіть його основні завдання.

2. У чому полягають відмінність і взаємодоповнюваність системного та ризик-орієнтованого підходів?

3. Які основні етапи розвитку систем менеджменту інформаційної безпеки?

4. Як класифікують кіберінциденти? Наведіть критерії класифікації.

5. З яких етапів складається життєвий цикл управління інцидентами за NIST SP 800-61 Rev. 3 та ISO/IEC 27035-1:2023?

ЛЕКЦІЯ 2. ДІЯЛЬНІСТЬ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кіберпростір не має державних кордонів, а атаки часто виконуються з однієї юрисдикції проти об'єктів в іншій, тому ефективність національних заходів безпеки залежить від міжнародного співробітництва. Воно потрібне для вироблення спільних правил поведінки держав, гармонізації кримінального законодавства, оперативного обміну даними про загрози, координації реагування та нарощування спроможностей менш підготовлених країн. Міжнародна діяльність у цій сфері поєднує юридично обов'язкові інструменти (конвенції, регламенти), політичні домовленості, технічні стандарти й неформальні мережі професійних спільнот.

Організація Об'єднаних Націй розглядає кібербезпеку на кількох рівнях. Питання відповідальної поведінки держав у інформаційному просторі впродовж двох десятиліть опрацьовували групи урядових експертів і відкрита робоча група, які сформулювали добровільні норми, зокрема щодо невтручання в роботу критичної інфраструктури, обміну інформацією та допомоги в розслідуваннях; на їх основі формується постійний механізм діалогу. Міжнародний союз електрозв'язку виконує технічну та рейтингову роль, зокрема публікує Глобальний індекс кібербезпеки. Найважливішим правовим досягненням останніх років стала Конвенція ООН проти кіберзлочинності, ухвалена Генеральною Асамблеєю у грудні 2024 року й відкрита для підписання в Ханої у жовтні 2025 року; вона набуде чинності на дев'яностий день після здачі на зберігання сорокового документа про ратифікацію [13].

Північноатлантичний альянс визнав кіберпростір окремою операційною сферою поряд із сушею, морем, повітрям і космосом, а серйозні кібератаки можуть бути підставою для консультацій і за певних умов – для застосування колективної оборони. Практичні спроможності Альянсу забезпечують Агентство НАТО з комунікацій та інформації, Центр кіберінцидентного реагування, а також Об'єднаний центр передової кібероборони НАТО в Таллінні, який готує дослідження, навчання та щорічні вправи на кшталт

Locked Shields. Україна співпрацює з Альянсом у межах цільових фондів і участі в роботі Таллінського центру.

Європейський Союз має найрозвиненішу систему наднаціонального регулювання. Основою є Директива (ЄС) 2022/2555 (NIS2), яка встановила єдині вимоги до управління ризиками, звітування про інциденти та нагляду для суб'єктів значущих секторів, а також створила інститути співпраці: Групу співробітництва, мережу CSIRT і мережу EU-CyCLONe для координації під час масштабних кібернадзвичайних подій [11]. Регламент DORA (ЄС) 2022/2554 визначає вимоги до цифрової операційної стійкості фінансового сектору [12]. Регламент про кіберстійкість (2024/2847) запроваджує обов'язкові вимоги безпеки до продуктів із цифровими елементами протягом їхнього життєвого циклу. Агентство ЄС з кібербезпеки ENISA підтримує державні та галузеві структури методичною допомогою, оцінками ландшафту загроз, звітами про інвестиції у безпеку, а також бере участь у європейській системі сертифікації [3; 4; 5].

Рада Європи є джерелом Конвенції про кіберзлочинність (Будапештської конвенції, 2001), яка досі залишається найпоширенішим міжнародним договором у цій сфері: вона визначає склад правопорушень, процесуальні інструменти збирання електронних доказів і механізми міжнародної допомоги, зокрема мережу контактних пунктів, що працюють цілодобово. Другий додатковий протокол (2022) розширив можливості прямої взаємодії з постачальниками послуг щодо даних абонентів та прискореного розкриття даних в екстрених випадках [14]. Україна є учасницею Будапештської конвенції з 2006 року.

Міжнародні ініціативи проти кіберзагроз охоплюють як державні, так і приватні майданчики. Прикладами є ініціатива «Counter Ransomware Initiative» за участю десятків держав, Паризький заклик до довіри й безпеки в кіберпросторі, Глобальний форум з кіберекспертизи, спільні операції правоохоронних органів за координації Європолу, Євроюсту та Інтерполу з ліквідації інфраструктури шкідливих мереж. Важливою складовою є розвиток

спроможностей: допомога у створенні CSIRT, навчання фахівців, поставки обладнання й програмних засобів країнам, що зазнають атак.

Механізми обміну інформацією про кіберінциденти будуються на поєднанні правових зобов'язань і добровільної довіри. Правові вимоги звітування в ЄС задає NIS2: рання попередня сповіщення без зайвих затримок, як правило, протягом 24 годин, повідомлення про інцидент протягом 72 годин і підсумковий звіт, що подається впродовж місяця. Добровільний обмін ґрунтується на секторальних центрах обміну інформацією (ISAC), платформах на кшталт MISP, форматах STIX і TAXII та протоколі маркування чутливості TLP. Для стимулювання обміну законодавство передбачає захист від відповідальності й конфіденційність даних, як-от Закон США про обмін інформацією про кіберзагрози 2015 року, дію якого неодноразово продовжували на короткі строки.

Захист критичної інформаційної інфраструктури є окремим напрямом співпраці, оскільки порушення роботи енергетики, транспорту, зв'язку, фінансів чи охорони здоров'я одразу має транскордонні наслідки. Міжнародні документи встановлюють вимоги до виявлення об'єктів критичної інфраструктури, до обов'язкових заходів безпеки, до спільних навчань і до перевірки ланцюгів постачання. Окрему увагу приділяють безпеці підводних кабелів, супутникового зв'язку та хмарних сервісів як спільних залежностей багатьох держав.

Участь України у міжнародних програмах і проєктах має кілька вимірів: співробітництво з ЄС у межах діалогу з питань кібербезпеки та участь у програмах цифрового розвитку, допомога держав-партнерів і приватних компаній у захисті мереж під час повномасштабної війни, обмін індикаторами компрометації з CSIRT інших країн, участь у вправах і в діяльності профільних об'єднань. Для набуття членства в ЄС Україна гармонізує законодавство з acquis, зокрема у сфері кібербезпеки, що відображено в Законі № 4336-IX і Національній програмі адаптації законодавства [18; 19].

Контрольні питання

1. Чому кібербезпека потребує міжнародного співробітництва?

2. Яку роль у сфері кібербезпеки відіграють ООН, НАТО, ЄС та Рада Європи?

3. Які основні вимоги Конвенції ООН проти кіберзлочинності та Будапештської конвенції?

4. Які механізми обміну інформацією про кіберінциденти застосовуються на міжнародному рівні?

5. Як Україна бере участь у міжнародних програмах із кібербезпеки?

ЛЕКЦІЯ 3. СТАНДАРТИЗАЦІЯ В СФЕРІ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Стандартизація у сфері менеджменту інформаційної безпеки покликана закріпити загальновизнані практики, зробити вимоги до безпеки порівнянними та перевірюваними, знизити витрати на розроблення власних методик і забезпечити взаємну довіру між організаціями, партнерами й регуляторами. Стандарт слугує мовою, якою замовник формулює вимоги, виконавець демонструє їх виконання, а аудитор підтверджує відповідність. Основними завданнями стандартизації є уніфікація термінології, визначення процесів і вимог до них, опис переліків заходів захисту, а також установлення правил оцінювання та сертифікації.

Стандарти поділяють на міжнародні, регіональні й національні. Міжнародні розробляють ISO та IEC, зокрема спільний технічний комітет, що опрацьовує сімейство стандартів інформаційної безпеки; до регіональних належать європейські документи ETSI, CEN і CENELEC; національні представлені стандартами національних органів стандартизації й нормативними документами регуляторів. Для України важливим є принцип прийняття міжнародних стандартів як національних методом підтвердження або перекладу: ДСТУ ISO/IEC 27001:2023 впроваджує чинну редакцію ISO/IEC 27001:2022. Окрему групу становлять рамкові документи, що не є стандартами в юридичному розумінні, але мають вплив, подібний до стандартів, як-от NIST Cybersecurity Framework 2.0 і серія NIST SP 800 [1; 15].

Сімейство ISO/IEC 27000 об’єднує десятки документів, що мають спільну логіку. Стандарт 27000 визначає терміни й загальний огляд. Стандарт 27001 містить вимоги до системи управління, за якими проводять сертифікацію. Стандарт 27002 – настанову із застосування заходів захисту. Стандарт 27003 пояснює впровадження системи, 27004 – вимірювання її результативності, 27005 – управління ризиками інформаційної безпеки. Стандарт 27006 встановлює вимоги до органів сертифікації, 27007 – настанову з аудиту, 27017 і 27018 стосуються хмарних сервісів і захисту персональних даних, 27035 – управління інцидентами, 27701 – управління приватністю. Така

будова дозволяє поєднувати обов'язкову частину (27001) з додатковими настановами [7; 8; 9; 10].

Вимоги ISO/IEC 27001:2022 до системи управління викладено в розділах 4–10 за єдиною структурою стандартів систем менеджменту. Розділ 4 вимагає визначити контекст організації, зацікавлені сторони та сферу застосування. Розділ 5 покладає на вище керівництво лідерство, затвердження політики безпеки й розподіл ролей. Розділ 6 описує планування: оцінювання ризиків і можливостей, оброблення ризиків, вибір заходів, складання декларації застосовності та встановлення цілей безпеки, а зміна 2024 року додала вимогу враховувати вплив кліматичних змін на систему. Розділ 7 стосується ресурсів, компетентності, обізнаності, комунікацій і документованої інформації. Розділ 8 регламентує виконання процесів оцінювання та оброблення ризиків. Розділ 9 вимагає моніторингу, вимірювання, внутрішнього аудиту й аналізу з боку керівництва, а розділ 10 – усунення невідповідностей і постійного вдосконалення. Додаток А містить перелік заходів із 93 позицій, структуру якого розглянуто в лекції 15.

Практичне застосування стандартів 27002 і 27005 демонструє поділ праці між ними. Стандарт 27005:2022 пропонує процес управління ризиками, який узгоджено з ISO 31000: встановлення контексту, ідентифікація, аналіз і оцінювання ризиків, оброблення, комунікація та моніторинг, і допускає як підхід на основі подій, так і на основі активів [9]. Стандарт 27002:2022 слугує каталогом заходів і містить настанови до кожного з них: мету, атрибути, рекомендації щодо впровадження [8]. У результаті організація проходить цикл: оцінює ризики за 27005, вибирає заходи з Додатка А та 27002, документує їх у декларації застосовності й контролює результативність за 27004.

Рамка кібербезпеки NIST CSF 2.0 орієнтована на результати й не є сертифікаційним стандартом. Вона містить шість функцій – «Управління», «Ідентифікація», «Захист», «Виявлення», «Реагування» та «Відновлення», які розділено на категорії та підкатегорії, а також інструменти: профілі, що описують поточний і цільовий стан, і рівні впровадження, що характеризують

зрілість процесів [1]. Рамку застосовують організації будь-якого розміру, а її довідкові відповідники пов’язують підкатегорії з ISO/IEC 27001, NIST SP 800-53 та іншими документами, що спрощує спільне використання. Каталог NIST SP 800-53 Rev. 5 (оновлення 5.2.0 від 2025 року) містить детальні вимоги до заходів і застосовується, насамперед, в урядових системах США та у суміжних секторах [15].

Сертифікація, аудит і оцінювання відповідності утворюють систему підтвердження. Сертифікацію системи управління проводять акредитовані органи за вимогами ISO/IEC 17021-1 та ISO/IEC 27006-1:2024. Процес складається із попередньої оцінки документації (аудит першого етапу), оцінки впровадження (аудит другого етапу), ухвалення рішення про видачу сертифіката та щорічних наглядових аудитів; сертифікат діє три роки, після чого проводять повторну сертифікацію. Внутрішній аудит і аналіз із боку керівництва передують зовнішньому. Для продуктів і послуг застосовують оцінювання за критеріями загальної оцінки (Common Criteria) та європейські схеми сертифікації, а для відповідності регуляторним вимогам – обов’язкові перевірки та декларування. У практичному вимірі сертифікація є не метою самою по собі, а доказом того, що система діє й постійно вдосконалюється.

Контрольні питання

1. Які мета й завдання стандартизації в менеджменті інформаційної безпеки?

2. Як співвідносяться міжнародні та національні стандарти? Наведіть приклади.

3. Яка структура сімейства ISO/IEC 27000 і призначення його основних документів?

4. Які вимоги ISO/IEC 27001:2022 висувають до системи управління?

5. У чому полягають особливості NIST CSF 2.0 порівняно з ISO/IEC 27001?

6. Як відбувається сертифікація системи управління інформаційною безпекою?

ЛЕКЦІЯ 4. РОБОТИ СПЕЦІАЛІЗОВАНИХ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ ТА ОБ'ЄДНАНЬ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. УПРАВЛІННЯ РИЗИКАМИ В ІНФОРМАЦІЙНІЙ ТА КІБЕРБЕЗПЕЦІ

Поряд з міждержавними інституціями вагому роль у сфері кібербезпеки відіграють спеціалізовані організації та професійні об'єднання, які безпосередньо забезпечують оперативну взаємодію команд реагування й поширення знань про загрози. Агентство ЄС з кібербезпеки ENISA сприяє виконанню політики Союзу: готує рекомендації з впровадження Директиви NIS2, щорічні оцінки ландшафту загроз, огляди інвестицій у безпеку, підтримує мережу CSIRT і навчання, а також бере участь у розвитку європейської сертифікації та реєстру вразливостей [3; 4; 5]. Форум команд реагування та безпеки FIRST, що працює з 1990 року, об'єднує сотні CSIRT і підрозділів безпеки з різних країн, підтримує протокол TLP, систему оцінювання вразливостей CVSS і сучасні моделі пріоритезації на кшталт EPSS.

Координаційний центр CERT/CC при Університеті Карнегі–Меллона виник у 1988 році після інциденту із мережевим хробаком Морріса й став прообразом національних команд реагування. Сьогодні терміни CERT і CSIRT вживають як близькі: перший історично є захищеним товарним знаком, другий – узагальнена назва команди з реагування на інциденти. Українська урядова команда CERT-UA діє в складі Держспецзв'язку й акредитована в мережі довіри TF-CSIRT і FIRST. Міжнародна координація реагування здійснюється як через двосторонні канали обміну між командами, так і через мультилатеральні мережі: мережу CSIRT ЄС, регіональні асоціації та глобальну спільноту FIRST.

Обмін інформацією про вразливості, загрози та індикатори компрометації (IoC) спирається на стандартизовані формати й ідентифікатори. Вразливості реєструються в програмі CVE, що присвоює їм унікальні ідентифікатори, а їхню важкість описують за системою CVSS (версія 4.0 з 2023 року); бази на кшталт NVD і європейського реєстру EUVD збирають відомості про

ураження. Скоординоване розкриття вразливостей передбачає, що дослідник повідомляє постачальника, надає час для усунення дефекту й лише потім оприлюднює подробиці. Загрози й IoC (хеші файлів, IP-адреси, домени, правила виявлення) обмінюють у структурованих форматах STIX і TAXII, через платформи MISP та спільноти ISAC, застосовуючи маркування TLP для визначення допустимого кола поширення.

Ризик у сфері інформаційної та кібербезпеки – це поєднання ймовірності реалізації загрози та величини наслідків для цілей організації. Ризики класифікують за джерелом (зовнішні й внутрішні, природні, технічні, людські), за об'єктом (ризики активів, процесів, ланцюга постачання, третіх сторін), за природою наслідків (втрата конфіденційності, цілісності, доступності; фінансові, репутаційні, правові, операційні втрати) та за рівнем (стратегічні, тактичні, операційні). Відмінність кіберризику від інших ризиків полягає в наявності цілеспрямованого супротивника, який змінює свою поведінку, у швидкому розвитку вразливостей і в системних залежностях між активами [6].

Процес управління ризиками, відповідно до ISO/IEC 27005:2022, містить кілька взаємопов'язаних етапів. Ідентифікація полягає у визначенні активів, власників, загроз, вразливостей, наявних заходів і ризикових сценаріїв. Аналіз встановлює ймовірність і наслідки кожного сценарію. Оцінювання порівнює отримані рівні з критеріями прийнятності та визначає пріоритети. Далі йдуть оброблення, повідомлення й консультування зі стейкхолдерами, а також безперервний моніторинг і перегляд [9]. Кожен етап документують у реєстрі ризиків, який є робочим інструментом власників ризиків і керівництва.

Методи аналізу поділяють на якісні, кількісні та напівкількісні. Якісні використовують шкали на кшталт «низький – середній – високий» і матриці «ймовірність × наслідки»; вони прості, швидкі й придатні для широкої оцінки, однак суб'єктивні. Кількісні виражають ризик у грошових одиницях. Класична модель оперує вартістю активу AV, коефіцієнтом впливу EF, одноразовими очікуваними втратами SLE та річною частотою ARO, звідки визначають річні очікувані втрати ALE:

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

Більш сучасні підходи, наприклад модель FAIR, розкладають ризик на частоту втратних подій і величину втрат із застосуванням розподілів імовірностей і методів Монте-Карло [6]. Вибір методу залежить від доступних даних, зрілості організації та мети оцінювання, а на практиці часто поєднують якісний скринінг із кількісним аналізом найкритичніших сценаріїв.

Стратегії оброблення ризиків, за ISO/IEC 27005:2022, охоплюють такі варіанти: зміна ризику (упровадження заходів, що знижують ймовірність або наслідки), утримання (свідоме прийняття ризику в межах допустимого рівня), уникнення (відмова від діяльності, що створює ризик) і поділ (передача частини ризику іншій стороні, наприклад через страхування або аутсорсинг). Вибір ґрунтується на порівнянні вартості заходу й зниження очікуваних втрат, а рішення про прийняття залишкового ризику ухвалює його власник у межах повноважень, визначених керівництвом. Результатом є план оброблення ризиків, що вказує відповідальних, строки, ресурси та очікуваний залишковий ризик.

Моніторинг ефективності управління ризиками здійснюють за допомогою ключових індикаторів ризику та результативності, зокрема часткою активів із актуальною оцінкою, середнім часом усунення критичних вразливостей, кількістю інцидентів за типами, часткою ризиків, які перевищують допустимий рівень. Перегляд проводять за графіком і після значних змін: впровадження нових систем, зміни постачальників, виявлення нових загроз чи інцидентів. Звіти про стан ризиків надходять керівництву, що, відповідно до сучасних вимог, несе відповідальність за затвердження підходу та нагляд за його виконанням [1; 7].

Контрольні питання

1. Яку роль виконують ENISA, FIRST, CERT і CSIRT?

2. Як відбувається обмін інформацією про вразливості та індикатори компрометації?

3. Як визначають і класифікують ризики в кібербезпеці?

4. Які етапи процесу управління ризиками за ISO/IEC 27005:2022?

5. Порівняйте якісні та кількісні методи оцінювання ризиків.

6. Які існують стратегії оброблення ризиків і як контролюють їх ефективність?

ЛЕКЦІЯ 5. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА РІВНІ ВЕЛИКИХ ПОСТАЧАЛЬНИКІВ ІНФОРМАЦІЙНИХ СИСТЕМ

Великі постачальники інформаційних систем і хмарних послуг мають особливе значення для кібербезпеки, оскільки їхні платформи є спільною основою для тисяч організацій, а компрометація постачальника спричиняє ланцюгові наслідки. Для таких компаній безпека – одночасно умова існування бізнесу й конкурентна перевага, тож вони формують власні корпоративні політики, моделі управління й технічні архітектури, які згодом стають галузевими орієнтирами. Вивчення їхнього досвіду корисне тим, що дозволяє побачити, як стандарти й рамки втілюються в масштабованій практиці.

Корпоративна політика безпеки великого постачальника зазвичай має багаторівневу структуру: загальні принципи, затверджені вищим керівництвом, тематичні політики та технічні стандарти, а також робочі процедури. Управління здійснюють через виділену посаду керівника безпеки, незалежний від IT-підрозділів комітет із ризиків, програми управління вразливостями й зовнішні аудити. Типовим доказом відповідності є сертифікати ISO/IEC 27001, звіти SOC 2, відповідність схемам на кшталт FedRAMP та участь у реєстрі CSA STAR, що дозволяє клієнтам перевіряти заходи постачальника без власного аудиту [6; 16].

Корпорація Microsoft організовує безпеку навколо моделі «нульової довіри» (Zero Trust) і життєвого циклу розроблення Security Development Lifecycle. У 2023 році вона оголосила програму Secure Future Initiative, що передбачає безпеку за проєктом, безпеку за замовчуванням і безпечні операції, а також посилення захисту ідентичностей, ізоляцію середовищ і скорочення часу усунення вразливостей. Компанія Google довела до практики модель BeyondCorp, у якій доступ визначається ідентичністю користувача та станом пристрою, а не розташуванням у мережі, а також запровадила рамку SLSA для безпеки ланцюга постачання програмного забезпечення та концепцію SAIF для безпечного розроблення систем штучного інтелекту. Компанія Amazon Web Services побудувала безпеку навколо моделі

розподіленої відповідальності, детального керування ідентичністю та доступом, шифрування за замовчуванням і структури Well-Architected Framework, що містить окремий стовп безпеки.

Керування ідентичністю та доступом (IAM) є центральним елементом хмарної безпеки. Воно охоплює централізовану автентифікацію з багатофакторним підтвердженням, федерацію ідентичностей, модель ролей і політик із мінімально необхідними правами, тимчасові облікові дані замість довготривалих секретів, привілейований доступ з обмеженим часом дії та безперервний аудит дій. Практика показує, що більшість хмарних компрометацій пов'язана з помилками конфігурації та викраденими обліковими даними, а не з вразливостями платформи, тому належне налаштування IAM має пріоритет перед іншими заходами [6].

Безпека хмарної інфраструктури ґрунтується на моделі розподіленої відповідальності: постачальник відповідає за безпеку самої хмари (фізичні центри обробки даних, обладнання, віртуалізацію), а клієнт – за безпеку у хмарі (дані, ідентичності, конфігурацію, програми). Межа відповідальності зсувається залежно від моделі послуги, як показано в таблиці.

Таблиця 5.1 – Розподіл відповідальності в хмарних моделях

Рівень	**IaaS**	**PaaS**	**SaaS**
Дані й доступ користувачів	Клієнт	Клієнт	Клієнт
Застосунки	Клієнт	Клієнт	Постачальник
Операційна система й середовище виконання	Клієнт	Постачальник	Постачальник
Віртуалізація, мережа, обладнання	Постачальник	Постачальник	Постачальник

Додатково застосовують сегментацію мереж, шифрування даних у спокої й під час передавання з керуванням ключами (KMS, HSM), безперервний моніторинг конфігурацій і засоби виявлення загроз на рівні хмарних сервісів. Для зменшення ризиків, пов'язаних із постачальником, клієнти використовують кілька регіонів або кілька хмар, а також перевіряють умови виходу з послуги.

Безпека життєвого циклу програмного забезпечення охоплює вимоги до безпеки на етапі проєктування, моделювання загроз, безпечне програмування, статичний і динамічний аналіз коду, перевірку залежностей, підписання артефактів, захищене розгортання й моніторинг у експлуатації. Основою служить рамка NIST SP 800-218 (SSDF), що описує практики для виробників програмного забезпечення; вона поєднана з вимогою складання переліку компонентів SBOM, який дозволяє швидко виявляти уражені залежності під час нових вразливостей [30]. Європейський Регламент про кіберстійкість закріплює подібні вимоги юридично для продуктів із цифровими елементами.

Управління вразливостями й інцидентами в постачальників будується на безперервному процесі: власні команди дослідників, програми винагород за виявлення помилок, скоординоване розкриття, швидке випускання виправлень і публічні бюлетені безпеки. Для інцидентів діють цілодобові команди реагування, чіткі вимоги до сповіщення клієнтів і регуляторів, а також післяінцидентні розбори, результати яких публікують у вигляді звітів. Така відкритість підвищує довіру й сприяє розвитку галузевих практик.

Безперервність послуг забезпечують розподілені центри обробки даних, резервування на рівні регіонів і зон доступності, автоматичне перемикання, регулярне тестування відновлення й хаос-інжиніринг, що перевіряє стійкість до відмов. Клієнтам надають угоди про рівень обслуговування (SLA), у яких зафіксовано доступність та умови компенсації. Оскільки навіть найбільші постачальники зазнають збоїв, організація має самостійно визначати прийнятні час і обсяг втрат даних (RTO і RPO) та узгоджувати з ними архітектуру рішень, а також враховувати залежність від кількох постачальників як окремий ризик ланцюга постачання.

Контрольні питання

1. Чим особливі вимоги до безпеки великих постачальників інформаційних систем?

2. Які принципи покладено в основу підходів Microsoft, Google та Amazon до безпеки?

3. Яку роль відіграє IAM у хмарній безпеці?

4. Як розподіляється відповідальність між постачальником і клієнтом хмарних послуг?

5. Які практики забезпечують безпеку життєвого циклу програмного забезпечення?

6. Як постачальники управляють вразливостями, інцидентами та безперервністю послуг?

ЛЕКЦІЯ 6. ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА США

Державна політика Сполучених Штатів у сфері кібербезпеки формується стратегічними документами президентської адміністрації, законами Конгресу, виконавчими указами й директивами відомств. Особливість американської моделі полягає в децентралізації: єдиного відомства, що відповідало б за все, немає, а координація досягається розподілом ролей і спільними рамками. Через це політика помітно змінюється з приходом нових адміністрацій, і конкретні акценти (регулювання чи добровільна співпраця, наступальні чи оборонні операції) варто звіряти з чинними документами. Національна стратегія кібербезпеки 2023 року, наприклад, ґрунтувалася на п’яти напрямах: захист критичної інфраструктури, порушення діяльності загроз, формування ринкових стимулів до безпеки, інвестиції в стійке майбутнє та міжнародне партнерство.

Структура органів управління включає кілька рівнів. На рівні Білого дому діє Офіс національного директора з кібербезпеки (ONCD), що координує стратегію та бюджетні пріоритети, поряд із Радою національної безпеки. Міністерство внутрішньої безпеки відповідає за цивільну кібербезпеку через Агентство з кібербезпеки та безпеки інфраструктури (CISA). Міністерство торгівлі через Національний інститут стандартів і технологій (NIST) розробляє стандарти й настанови. Міністерство оборони реалізує відповідні функції через Кіберкомандування США та Агентство національної безпеки (NSA). Федеральне бюро розслідувань і Секретна служба відповідають за розслідування кіберзлочинів; Управління з питань управління та бюджету (OMB) контролює виконання вимог безпеки у федеральних відомствах.

Агентство CISA створене законом 2018 року як операційна структура для захисту цивільної федеральної мережі та підтримки власників критичної інфраструктури: воно оприлюднює попередження й вказівки, веде каталог відомих експлуатованих вразливостей, надає послуги оцінювання та вправи, координує обмін даними та реагування. Інститут NIST розробляє Рамку кібербезпеки (редакція 2.0 вийшла у 2024 році), серію публікацій SP 800,

зокрема каталог заходів SP 800-53 і настанову з реагування на інциденти SP 800-61 Rev. 3, а також програму криптографічної стандартизації, у межах якої у 2024 році затверджено перші постквантові стандарти [1; 2; 15; 29]. Агентство NSA забезпечує безпеку систем національної безпеки, надає технічні рекомендації та аналітику загроз, в тому числі для оборонно-промислової бази.

Нормативне регулювання спирається на кілька ключових актів. Закон про управління інформаційною безпекою федеральних органів (FISMA) зобов'язує відомства впроваджувати програми безпеки на основі стандартів NIST та щорічно звітувати. Виконавчий указ 14028 (2021) запровадив вимоги щодо принципу нульової довіри, безпеки ланцюга постачання програмного забезпечення та переліків компонентів, а наступні укази коригували ці вимоги. Закон про обмін інформацією про кіберзагрози 2015 року надає компаніям правові гарантії для добровільного обміну даними з урядом і між собою; його дію неодноразово подовжували на короткі терміни, а долю довгострокового продовження визначає Конгрес, тому поточний статус слід перевіряти за офіційними джерелами. Закон про звітування про кіберінциденти в критичній інфраструктурі (CIRCIA, 2022) уповноважує CISA запровадити обов'язкове повідомлення про значні інциденти протягом 72 годин і про виплату викупу протягом 24 годин, а остаточні правила для нього неодноразово переносили. Для підрядників Міністерства оборони застосовується програма сертифікації CMMC.

Захист критичної інфраструктури визначено як спільна відповідальність держави й власників. Директива національної безпеки NSM-22 (2024) встановила шістнадцять секторів критичної інфраструктури й призначила для кожного профільне відомство з управління ризиками. Для підтримки співпраці створено секторальні координаційні ради, центри обміну інформацією ISAC та ISAO, а також спільну структуру взаємодії уряду й приватного сектору при CISA (JCDC). Цивільні об'єкти критичної інфраструктури здебільшого належать приватним компаніям, тому держава

спирається більше на стимули, добровільні рамки й вибіркове регулювання (енергетика, транспорт, фінанси, охорона здоров'я), ніж на єдиний закон.

Національне реагування організовано на основі Національного плану реагування на кіберінциденти, який розподіляє ролі між відомствами: CISA координує захист і відновлення, ФБР – розслідування та атрибуцію, а відомства розвідувального співтовариства – аналіз загроз. Під час значних подій створюється Єдина координаційна група, що поєднує урядові та приватні структури. Рівень реагування залежить від масштабу, а особливу увагу приділено розслідуванню після інцидентів, зокрема роботі Ради з огляду кіберінцидентів, яка за прикладом авіаційних розслідувань публікує висновки та рекомендації.

Державно-приватне партнерство є визначальною рисою американської моделі, оскільки найбільші технологічні й виробничі активи перебувають у приватних руках. Воно виявляється в спільних центрах аналізу загроз, програмах добровільної сертифікації, обміні даними через AIS, участі приватних дослідників у розкритті вразливостей, а також в державних закупівлях, які використовують вимоги безпеки як важіль впливу на ринок. Недоліками такої моделі вважають фрагментарність, залежність від добровільності та нестабільність законодавчих рамок, що підтверджується повторними короткими продовженнями дії Закону 2015 року. Для України американський досвід цінний як приклад розподілу ролей, використання стандартів як регуляторного інструменту й побудови довіри між державою та бізнесом.

Контрольні питання

1. Які основні принципи державної політики США у сфері кібербезпеки?
2. Які органи входять до системи кібербезпеки США та які їхні функції?
3. Яку роль відіграють CISA, NIST і NSA?
4. Які закони та виконавчі акти регулюють кібербезпеку в США?
5. Як організовано захист критичної інфраструктури й національне реагування?

ЛЕКЦІЯ 7. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ

Засади державної політики України у сфері кібербезпеки визначає Закон «Про основні засади забезпечення кібербезпеки України» 2017 року та Стратегія кібербезпеки України, що затверджена 2021 року. Вони встановлюють мету – створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства й держави, а також принципи: верховенство права, пропорційність заходів, державно-приватне партнерство, міжнародне співробітництво, відкритість до змін. Повномасштабне вторгнення 2022 року перетворило кіберпростір на безпосередню арену збройного протистояння й прискорило оновлення підходів: від формальних вимог до управління ризиками та спроможності швидко реагувати.

Нормативне забезпечення має кілька рівнів. Базові закони охоплюють кібербезпеку, захист інформації в інформаційно-телекомунікаційних системах, електронні довірчі послуги, захист персональних даних та критичну інфраструктуру. Найсуттєвіше оновлення пов’язане із Законом № 4336-IX, який імплементує підходи Директиви NIS2: він запровадив обов’язкову посаду керівника з кіберзахисту (CISO), змістив акцент в оцінюванні із «паперових» вимог на управління ризиками й створив систему національних, секторальних та регіональних команд реагування [19]. Для виконання закону Держспецзв’язку розробляє пакет підзаконних актів; серед них постанова Кабінету Міністрів від 18 червня 2025 року № 712 про авторизацію з безпеки та наказ Адміністрації Держспецзв’язку від 14 травня 2026 року № 351, що затвердив порядок обміну інформацією про кіберінциденти й критерії визначення значного кіберінциденту [20; 21]. За оцінкою Держспецзв’язку, станом на початок 2026 року рівень імплементації NIS2 становив 76 %, а до кінця року планують досягти 90 % [27].

Суб’єктами забезпечення кібербезпеки є Державна служба спеціального зв’язку та захисту інформації, Служба безпеки України, Національна поліція, Міністерство оборони й Генеральний штаб Збройних сил, розвідувальні

органи, Національний банк України. Координацію здійснює Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України. Держспецзв'язку відповідає за формування й реалізацію державної політики в галузі кіберзахисту, нагляд, захист державних інформаційних ресурсів і критичної інформаційної інфраструктури, а також за функціонування урядової команди CERT-UA. Служба безпеки України протидіє кібератакам і кіберрозвідці, що загрожують державній безпеці; Національна поліція (департамент кіберполіції) розслідує кіберзлочини; Міністерство оборони й Генштаб розвивають кібервійська та захист військових систем.

Команда CERT-UA виконує функції національного центру реагування: приймає повідомлення про інциденти, проводить аналіз і допомагає в усуненні наслідків, готує попередження та рекомендації, обмінюється даними з міжнародними партнерами. За даними Держспецзв'язку, у першому півріччі 2026 року CERT-UA опрацювала 3 137 кіберінцидентів, що на 8 % більше, ніж у другому півріччі 2025 року; найчастіше мішенями ставали органи місцевої влади (37 % інцидентів), урядові організації (22 %), сектор безпеки й оборони (9 %) та енергетика (8 %), а чотири основні типи – розповсюдження та зараження шкідливим програмним забезпеченням, соціальна інженерія й компрометація систем – склали близько 84 % [22]. Такі цифри свідчать, що основний тягар припадає на органи, які мають найменші ресурси, тому розвиток регіональних центрів кіберзахисту та регіональних команд реагування за принципом «єдиного вікна» є пріоритетом 2026 року.

Захист державних інформаційних ресурсів і критичної інфраструктури ґрунтується на комбінації вимог і контролю. Державні інформаційні системи, що обробляють інформацію з обмеженим доступом, мають комплексну систему захисту інформації з підтвердженою відповідністю; інші державні ресурси та об'єкти критичної інфраструктури підпадають під вимоги Закону «Про критичну інфраструктуру», за яким об'єкти категоризують за значущістю та вносять до реєстру. Нова модель оцінювання базується на ризикоріентованому підході: суб'єкт самостійно оцінює ризики, обирає

заходи з каталогу кіберзахисту, що затверджується Держспецзв'язку, проходить аудит і подає звітність. Каталог заходів, затверджений наказом № 75 від 30 січня 2026 року, слугує посібником для цього вибору. Окремий інструмент – авторизація з безпеки, що підтверджує здатність системи або послуги забезпечувати визначений рівень захищеності.

Координація здійснюється як на рівні державних органів, так і між державою, бізнесом та міжнародними партнерами. Під час масштабних кіберкриз створюється Об'єднана група при НКЦК, яка координує дії суб'єктів; якщо атака загрожує системам країн ЄС, CERT-UA як національний контактний центр за NIS2 оперативно інформує зарубіжні організації [23]. Практичними механізмами є обмін індикаторами компрометації, спільні розслідування, вправи, а також взаємодія з великими технологічними компаніями, що допомагають перенести критичні сервіси в хмару й посилити захист мереж.

Подальший розвиток державної системи кібербезпеки пов'язаний з кількома напрямами. Першим є завершення нормативної бази Закону № 4336-IX: у 2026 році Держспецзв'язку планувало фіналізувати ухвалення ще близько двадцяти актів. Другим є кадрове забезпечення – підготовка CISO, аудиторів і фахівців команд реагування. Третім – перехід до активного кіберзахисту, що поєднує моніторинг, проактивний пошук загроз і швидку взаємодію. Четвертим – подальша інтеграція в європейський правовий і технічний простір у межах процесу вступу до ЄС, зокрема адаптація законодавства до acquis. Ефективність цих кроків залежить від бюджетного забезпечення, довіри бізнесу та сталого міжнародного партнерства.

Контрольні питання

1. Які засади державної політики України у сфері кібербезпеки?
2. Які основні нормативні акти регулюють кібербезпеку в Україні?
3. Які повноваження мають Держспецзв'язку, СБУ, Національна поліція та CERT-UA?
4. Як забезпечується захист державних ІС і критичної інфраструктури?

ЛЕКЦІЯ 8. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ (КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ)

Криптографічний захист інформації – це застосування математичних перетворень для забезпечення конфіденційності, цілісності, автентичності та неспростовності даних. Його принципи включають відкритість алгоритмів за секретності ключів (принцип Керкгоффса), доведену або практично підтверджену стійкість, правильну реалізацію й належне управління ключами; слабкою ланкою зазвичай виявляється не алгоритм, а його використання. У державних системах криптографія забезпечує захист інформації з обмеженим доступом, юридичну значущість електронних документів та довіру до цифрових послуг.

Правове регулювання криптографічного захисту в Україні спирається на Закон «Про захист інформації в інформаційно-телекомунікаційних системах», Закон «Про державну таємницю» та Закон «Про електронну ідентифікацію та електронні довірчі послуги». Державну політику у сфері криптографічного захисту інформації реалізує Держспецзв’язку. Засоби криптографічного захисту для державних інформаційних ресурсів і інформації з обмеженим доступом підлягають обов’язковій державній експертизі й сертифікації; експертні дослідження виконує Державний науково-дослідний інститут технологій кібербезпеки, який у 2026 році оновив систему власних стандартів і порядок експертних досліджень засобів криптографічного та технічного захисту [24].

Симетричні алгоритми використовують один ключ для шифрування й розшифрування та характеризуються високою швидкістю. Асиметричні застосовують пару ключів – відкритий і закритий – і слугують для узгодження ключів, цифрового підпису та шифрування малих обсягів даних. Практика поєднує обидва типи: асиметричний механізм узгоджує сеансовий ключ, яким симетричний шифр захищає основний обсяг даних. Порівняння типів наведено в таблиці.

Таблиця 8.1 – Порівняння симетричних та асиметричних алгоритмів

Ознака	**Симетричні**	**Асиметричні**
Кількість ключів	Один спільний	Пара: відкритий і закритий
Швидкість	Висока	Нижча
Основне призначення	Шифрування великих обсягів даних	Узгодження ключів, цифровий підпис
Головна проблема	Безпечний розподіл ключа	Автентичність відкритого ключа

Національні стандарти України охоплюють весь комплекс примітивів. Блоковий шифр «Калина» визначено в ДСТУ 7624:2014; він підтримує розмір блока й довжину ключа від 128 до 512 біт та десять режимів роботи, включно з автентифікованим шифруванням. Хеш-функція «Купина» описана в ДСТУ 7564:2014 і формує значення довжиною 256, 384 або 512 біт. Цифровий підпис на еліптичних кривих визначає ДСТУ 4145-2002. Для коротких повідомлень на еліптичних кривих призначено ДСТУ 9041:2020, а потоковий шифр «Струмок» описано в ДСТУ 8845:2019. До переліку стандартів, чинних у сфері криптографічного захисту, входять також міжнародні, прийняті як національні, зокрема ДСТУ ISO/IEC 19772:2022 про автентифіковане шифрування [25]. У практиці сертифікації електронних довірчих послуг відбувся перехід від старої хеш-функції ГОСТ 34.311-95 до «Купини», що відповідає завданню відмови від застарілих алгоритмів.

Електронний підпис, сертифікати й інфраструктура відкритих ключів (PKI) становлять основу юридично значущого електронного документообігу. Кваліфікований електронний підпис за правовою дією прирівнюється до власноручного й створюється із застосуванням кваліфікованого засобу на основі кваліфікованого сертифіката, виданого кваліфікованим надавачем електронних довірчих послуг. Центральний засвідчувальний орган видає сертифікати надавачам і веде довірчий список; надавачі видають сертифікати користувачам та підтримують перелік відкликаних сертифікатів і службу перевірки статусу в реальному часі. Сертифікат формату X.509 пов’язує відкритий ключ із ідентифікаційними даними власника та містить строк дії й опис алгоритмів.

Властивості безпеки забезпечуються різними механізмами. Конфіденційність досягається шифруванням; цілісність – хеш-функціями, кодами автентифікації повідомлень і підписом; автентичність – підписом та протоколами автентифікації; неспростовність – кваліфікованим підписом із часовою позначкою, що не дозволяє автору заперечити авторство. Використання протоколів TLS для каналів, захищених дисків і сховищ, підписаних журналів та захищених резервних копій є типовою практикою. Складніші завдання, як-от безпечні обчислення чи анонімна автентифікація, вимагають спеціальних протоколів і зазвичай не належать до базового рівня.

Управління ключами охоплює повний життєвий цикл: генерацію з надійного джерела випадковості, безпечне зберігання (у захищених носіях чи апаратних модулях безпеки HSM), розподіл, використання за призначенням, періодичну заміну, резервування, відкликання у разі компрометації та гарантоване знищення. Критичні операції виконують за принципом двох осіб і розподілу обов’язків, а доступ до ключового матеріалу журналюють. Окремої уваги потребує криптографічна гнучкість – готовність швидко замінити алгоритм: у 2024 році NIST затвердив перші постквантові стандарти (ML-KEM, ML-DSA, SLH-DSA), а це спонукає організації вести інвентар криптографічних активів і планувати перехід [29].

Державний контроль і оцінювання відповідності включають сертифікацію засобів криптографічного захисту, державну експертизу комплексних систем захисту інформації, атестацію й нагляд за надавачами електронних довірчих послуг та перевірку виконання вимог до зберігання ключів і використання сертифікованих засобів. Для суб’єктів, що не обробляють державні секрети, використання національних алгоритмів і сертифікованих засобів стає обов’язковим у випадках, прямо визначених законом, а в інших – оцінюється з позиції ризиків. Тому фахівець повинен розуміти, які вимоги чинні для конкретної інформаційної системи, і документувати рішення в політиці криптографічного захисту.

Контрольні питання

1. Які принципи покладено в основу криптографічного захисту інформації?

2. У чому полягає відмінність симетричних і асиметричних алгоритмів?

3. Охарактеризуйте національні криптографічні стандарти України.

4. Як функціонують електронний підпис, сертифікати та PKI?

5. Які основні етапи управління криптографічними ключами?

6. Як здійснюється державний контроль у сфері криптографічного захисту?

ЛЕКЦІЯ 9. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ (ТЕХНІЧНІ МЕТОДИ ЗАХИСТУ). ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИННОСТІ. СТАН КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ. БОРОТЬБА ІЗ КІБЕРЗЛОЧИНАМИ

Технічний захист інформації (ТЗІ) – діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації, а також на запобігання її витоку технічними каналами. Принципами ТЗІ є комплексність, обґрунтованість, безперервність, економічна доцільність, відповідність вимогам нормативних документів і розмежування відповідальності. Правове підґрунтя становлять Закон «Про захист інформації в інформаційно-телекомунікаційних системах», Положення про технічний захист інформації в Україні та система нормативних документів ТЗІ, які визначають вимоги до побудови комплексних систем захисту інформації, критерії оцінювання захищеності й порядок створення систем, зокрема НД ТЗІ 1.1-002-99, 2.5-004-99 та 3.7-003-2005.

Організаційні методи ТЗІ охоплюють формування політики безпеки, розподіл повноважень, режимні обмеження, інструктування, контроль доступу до приміщень та документообіг із носіями, а інженерно-технічні – фізичні перешкоди, сигналізацію, відеоспостереження, екранування приміщень, заземлення, фільтрацію живлення, зонування території й засоби активного протидіяння. Вибір комплексу заходів ґрунтується на моделі загроз і порушника, яку розробляють на початку проєкту, та на категорії захищеної інформації й класі автоматизованої системи.

Витік інформації технічними каналами можливий різними фізичними шляхами. До них належать побічні електромагнітні випромінювання та наведення, що виникають під час роботи обладнання; акустичні й віброакустичні канали, через які мова з приміщення переходить у конструкції, трубопроводи та вікна; оптичні канали спостереження; канали, пов’язані з несанкціонованим підключенням і закладними пристроями. Протидія полягає у зменшенні рівня сигналу, збільшенні рівня перешкод, фільтрації й екрануванні, а також у виявленні закладних пристроїв методом

спеціальних обстежень. Відповідні вимоги особливо жорсткі для приміщень, де циркулює державна таємниця, і для систем із високим класом захищеності.

Контроль доступу, мережевий захист і виявлення вторгнень становлять технічний складник кіберзахисту. Контроль доступу реалізують автентифікацією, розмежуванням прав за ролями та атрибутами, ізоляцією сегментів. Мережевий захист охоплює міжмережеві екрани нового покоління, сегментацію, віртуальні приватні мережі, системи запобігання вторгненням та фільтрацію вмісту; на кінцевих точках працюють засоби EDR, антивірусного захисту й контролю пристроїв, а у складі центру моніторингу – SIEM і засоби реагування. Системи запобігання витоку даних (DLP) контролюють канали виходу конфіденційної інформації. Усі ці засоби мають бути інтегровані в єдину систему моніторингу, інакше їхня ефективність значно знижується [6; 8].

Оцінювання відповідності в системі ТЗІ складається з державної експертизи комплексної системи захисту інформації, атестації об’єктів і сертифікації засобів. Експертизу виконують акредитовані організації: вони перевіряють документацію, фактичну реалізацію функцій безпеки й дотримання критеріїв. За позитивного результату видають експертний висновок, що є підставою для експлуатації системи. Сучасні вимоги поступово поєднують традиційні підходи з ризикорієнтованими, зокрема каталог заходів кіберзахисту, і потребують відповідної перекваліфікації фахівців.

Кіберзлочинність – сукупність кримінально караних діянь, що вчиняються з використанням комп’ютерних систем і мереж або спрямовані проти них. Міжнародна практика, зокрема Будапештська конвенція, виокремлює кілька груп: правопорушення проти конфіденційності, цілісності й доступності комп’ютерних даних і систем (несанкціонований доступ, перехоплення даних, втручання в дані та системи, зловживання пристроями); правопорушення, пов’язані з комп’ютерами (шахрайство, підробка); правопорушення, пов’язані зі змістом (насамперед матеріали сексуальної експлуатації дітей); правопорушення проти авторського права [14]. У

Кримінальному кодексі України кіберзлочини зосереджено переважно в розділі XVI, статті 361–363-1: несанкціоноване втручання в роботу електронно-обчислювальних машин і мереж, створення та розповсюдження шкідливих програмних засобів, несанкціоновані дії з інформацією, порушення правил експлуатації, перешкоджання роботі систем.

Особливості кіберзлочинності в Україні визначаються воєнним станом і високим рівнем цифровізації. З одного боку, країна перебуває під безперервним тиском державних акторів, чия мета – руйнування критичних сервісів, розвідка та інформаційно-психологічний вплив; з іншого, зростає соціальна інженерія, фішинг, вішинг, шахрайства із підробленими інтернет-магазинами та виманюванням реквізитів банківських карток. За даними аналітики Opendatabot, кількість відкритих кримінальних проваджень про шахрайство загалом (не лише кібершахрайство) становила 82 609 у 2023 році, 64 978 у 2024-му та 48 871 у 2025 році; частка спрямованих до суду справ залишається невисокою, що відображає складність доказування [26]. Вимагання за допомогою програм-вимагачів, DDoS-атаки, крадіжка криптовалют і втручання у системи дистанційного банківського обслуговування також належать до поширених явищ.

Боротьбу з кіберзлочинами здійснюють кілька державних органів. Департамент кіберполіції Національної поліції розслідує більшість злочинів у цій сфері, виконує оперативні й слідчі дії, блокує шахрайські ресурси й співпрацює з банками та провайдерами; Служба безпеки України протидіє злочинам, що загрожують державній безпеці, зокрема атакам на критичну інфраструктуру; прокуратура здійснює процесуальне керівництво; Держспецзв’язку та CERT-UA надають технічну експертизу й оперативну інформацію. Збирання електронних доказів потребує дотримання процесуальних вимог до цілісності й походження цифрових слідів, тому розвивається цифрова криміналістика.

Міжнародне співробітництво необхідне, оскільки значна частина злочинців, інфраструктури й коштів перебуває за межами України. Його правовою основою є Будапештська конвенція, угоди про взаємну правову

допомогу, а в перспективі – Конвенція ООН проти кіберзлочинності [13; 14]. На практиці розслідування проводять через Європол, Євроюст та Інтерпол, спільні слідчі групи й міжнародні операції, спрямовані на ліквідацію інфраструктури шкідливих мереж, а також через цілодобові контактні пункти для термінового збереження даних. Українські правоохоронці регулярно беруть участь у таких операціях і діляться досвідом протидії атакам у воєнних умовах.

Контрольні питання

1. Які принципи й методи технічного захисту інформації?
2. Як відбувається витік інформації технічними каналами і як з ним боротися?
3. Які технічні засоби контролю доступу, мережевого захисту й виявлення вторгнень застосовують?
4. Як класифікують кіберзлочини та які статті Кримінального кодексу України їх стосуються?
5. Які особливості кіберзлочинності в Україні?
6. Які органи й механізми протидіють кіберзлочинності на національному та міжнародному рівнях?

ЛЕКЦІЯ 10. МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РІВНІ ПІДПРИЄМСТВА: ОСНОВНІ НАПРЯМКИ І СТРУКТУРА ПОЛІТИКИ БЕЗПЕКИ

Менеджмент інформаційної безпеки на рівні підприємства спрямований на те, щоб захист інформації став керованою складовою бізнесу, а не набором розрізнених технічних рішень. Його мета – забезпечити захищеність інформаційних активів до рівня, що відповідає цілям організації, ризик-апетиту й вимогам законодавства. До завдань належать визначення вимог до безпеки, оцінювання та оброблення ризиків, розроблення політик і процедур, розподіл відповідальності, навчання персоналу, контроль дотримання вимог і вдосконалення системи. Принципами є лідерство керівництва, інтеграція безпеки в бізнес-процеси, пропорційність ризикам, відповідальність, безперервність і доказовість, тобто здатність підтвердити виконання вимог документами та записами [6; 7].

Корпоративна система управління інформаційною безпекою (СУІБ) становить сукупність політик, процесів, ролей і ресурсів, що діють за циклом «плануй – виконуй – перевіряй – удосконалюй». На етапі планування визначають контекст, сферу застосування, ризики й цілі; на етапі виконання впроваджують заходи й навчають персонал; на етапі перевірки здійснюють моніторинг, внутрішній аудит і аналіз керівництвом; на етапі вдосконалення усувають невідповідності та оновлюють систему. Система повинна мати документоване підтвердження, але її цінність визначається не наявністю документів, а реальним впливом на ризики [7].

Структура та відповідальність у СУІБ мають кілька рівнів. Вище керівництво затверджує політику, виділяє ресурси й несе кінцеву відповідальність. Керівник із питань безпеки (CISO) організовує роботу системи, звітує перед керівництвом і координує підрозділи. Власники активів і процесів відповідають за оцінювання ризиків і прийняття залишкових ризиків. ІТ-підрозділи реалізують технічні заходи, а кожен працівник виконує вимоги політик у повсякденній діяльності. Для розподілу ролей застосовують матрицю RACI, яка визначає, хто відповідає, хто затверджує, кого

консультують і кого інформують. Незалежність функції безпеки від IT-операцій дозволяє уникнути конфлікту інтересів, коли той самий підрозділ і будує, і контролює систему.

Політика інформаційної безпеки – документ, що формулює наміри та напрями організації у сфері безпеки, затверджений керівництвом. Її складовими є мета й сфера застосування, основні принципи, ролі та відповідальність, зобов'язання щодо виконання вимог законодавства та постійного вдосконалення, а також порядок перегляду й санкції за порушення. Розроблення політики включає аналіз бізнес-цілей і вимог, консультації зі стейкхолдерами, підготовку проєкту, погодження, затвердження, доведення до відома персоналу та періодичний перегляд. Політика має бути стислою й зрозумілою, а деталізація переноситься в тематичні політики, стандарти та процедури, що формують ієрархію документів від стратегічного до оперативного рівня [17].

Активи, ризики та доступ утворюють змістовне ядро політики. Організація веде реєстр інформаційних активів (дані, системи, програми, носії, сервіси, люди, постачальники), призначає власників і класифікує активи за цінністю та чутливістю. Ризики визначають за процесом, описаним у лекції 4, а політика встановлює принципи їх оброблення й критерії прийнятності. Положення про доступ закріплюють принципи мінімальних прав, розподілу обов'язків, необхідності знати й періодичного перегляду прав, а також вимоги до автентифікації й керування привілейованими обліковими записами [8].

Окремі положення політики стосуються персональних даних і комерційної таємниці. Обробка персональних даних регулюється українським Законом «Про захист персональних даних» і, якщо діяльність стосується громадян ЄС, Регламентом GDPR (ЄС) 2016/679; вимоги включають законні підстави, мінімізацію й обмеження мети, інформування суб'єктів, забезпечення безпеки обробки, повідомлення про порушення та реалізацію прав суб'єктів. Комерційну таємницю захищають режимом, який передбачає визначення переліку відомостей, обмеження доступу, укладення угод про нерозголошення, маркування та контроль. Політика має встановлювати, хто

відповідає за дотримання таких режимів, і пов’язувати їх із трудовими й цивільно-правовими договорами.

Безперервність діяльності й реагування включають аналіз впливу на бізнес (BIA), визначення критичних процесів, допустимих часу простою й обсягу втрат даних, розроблення планів безперервності й відновлення, резервування та регулярні навчання. Політика закріплює вимоги до створення команди реагування, порядку повідомлення про інциденти й оповіщення регуляторів та клієнтів. Узгодженість цих планів із загальним управлінням ризиками вимагає, щоб вони переглядалися після змін і інцидентів та відповідали вимогам стандартів, наприклад ISO 22301 і ISO/IEC 27035 [10].

Контроль, внутрішній аудит і оцінювання ефективності замикають цикл. Контроль здійснюють безперервно – через моніторинг, перевірки конфігурацій, сканування вразливостей, огляди прав доступу. Внутрішній аудит проводять за планом незалежні особи, а його результатом є звіт із висновками та коригувальними діями. Ефективність оцінюють за показниками: часткою працівників, які пройшли навчання, часом виявлення й усунення інцидентів, часткою усунених критичних вразливостей, кількістю порушень політик, результатами тестових фішингових кампаній. Результати розглядає керівництво, ухвалює рішення про ресурси й корективи, а ці рішення фіксуються як вхідні дані для наступного циклу [6; 7].

Контрольні питання

1. Які мета, завдання й принципи менеджменту безпеки на рівні підприємства?

2. З яких елементів складається корпоративна СУІБ та як розподілено відповідальність?

3. З яких складових складається політика інформаційної безпеки і як її розробляють?

4. Які положення політики стосуються активів, ризиків і доступу?

5. Як політика регулює захист персональних даних і комерційної таємниці?

ЛЕКЦІЯ 11. ЗМІСТ ДЕТАЛІЗОВАНОЇ ПОЛІТИКИ БЕЗПЕКИ

Детальна політика безпеки конкретизує загальні положення, переводячи їх у чіткі правила для певних областей: від класифікації активів до користування електронною поштою. Її призначення – зробити вимоги однозначними, перевірюваними й придатними до виконання працівниками різних рівнів підготовки. Типова структура документа включає мету й сферу застосування, нормативні посилання, терміни, ролі та відповідальність, власне положення, порядок виявлення порушень і санкцій, винятки та порядок їх затвердження, пов’язані документи, а також інформацію про версії та періодичність перегляду. Тематичні політики доцільно складати окремо й узгоджувати між собою, щоб уникнути суперечностей [17; 8].

Принципи побудови деталізованої політики охоплюють орієнтацію на ризики, відповідність законодавству, простоту та однозначність формулювань, обов’язковість для всіх категорій користувачів, практичну здійсненність і вимірюваність. Вимоги формулюють у вигляді правил, що мають однозначні критерії виконання: «обов’язковий багатофакторний вхід для віддаленого доступу» перевірити легко, а «посилити автентифікацію» – ні. Кожне правило має власника, строк дії та спосіб контролю, а винятки допускаються лише письмово, із зазначенням ризику й компенсаційних заходів.

Класифікація активів є відправною точкою для всіх інших політик. Інформацію зазвичай поділяють на рівні за чутливістю: публічна, внутрішня, конфіденційна й особливо конфіденційна (для державних організацій додаються категорії інформації з обмеженим доступом і державної таємниці). Для кожного рівня встановлюють вимоги до маркування, зберігання, передавання, копіювання та знищення. Власник активу відповідає за визначення рівня й періодичний перегляд класифікації, а політика вказує, як відповідні вимоги поширюються на носії, хмарні сервіси й паперові документи.

Управління доступом та ідентифікація визначають, хто і до чого може мати доступ. Політика закріплює процес надання прав (запит, погодження власником, фіксація), модель на основі ролей, принцип мінімальних прав, регулярний перегляд (як правило, не рідше одного разу на рік, для привілейованих облікових записів – частіше), негайне відкликання прав під час звільнення та переведення. Для кожного працівника використовують персональний обліковий запис, спільне використання облікових записів забороняється, а привілейований доступ виконується через окремі облікові записи й журналюється. Багатофакторна автентифікація є базовою вимогою для віддаленого доступу, привілейованих користувачів і критичних систем.

Парольний захист за сучасними настановами базується на довжині та унікальності, а не на складності й частій зміні. Настанова NIST SP 800-63B-4 щодо автентифікації рекомендує довгі парольні фрази, перевірку пароля за списками скомпрометованих значень, відмову від примусової періодичної зміни без підстав та заохочення до використання менеджерів паролів і стійких до фішингу методів, таких як ключі доступу (passkeys) [28]. Політика має відображати ці положення, а також визначати порядок зберігання службових секретів і заборону передавати пароль іншим особам.

Положення щодо корпоративних мереж охоплюють сегментацію, правила підключення пристроїв, використання міжмережевих екранів, безпеку бездротових мереж, порядок віддаленого доступу через захищені канали й моніторинг мережевого трафіку. Політика користування електронною поштою встановлює дозволені цілі, вимоги до шифрування чутливих вміщень, заборону автоматичного пересилання на зовнішні адреси, порядок обробки підозрілих листів і засоби захисту від фішингу й підміни відправника. Політика мобільних пристроїв регулює використання службових і особистих (BYOD) пристроїв, вимоги до шифрування, блокування, віддаленого стирання, обов’язкову реєстрацію у системі керування й заборону на модифіковані пристрої.

Захист персональних даних і конфіденційної інформації втілюється в конкретних правилах: хто має доступ, де зберігаються дані, як довго, як

передаються за межі організації, коли шифруються, а також як відбувається їх знищення. До політики включають вимоги до оцінки впливу на захист даних, договорів з обробниками, порядку інформування про порушення та реагування на запити суб'єктів. Для конфіденційної інформації застосовують маркування, шифрування носіїв, обмеження друку та копіювання, засоби запобігання витоку даних. Порушення правил, як-от відправлення даних на особисту пошту, мають чіткі наслідки, закріплені у внутрішніх документах і трудових договорах.

Контроль, перегляд і актуалізація політик утворюють завершальний елемент. Політики переглядають за графіком (як правило, щорічно) і позачергово – після інцидентів, зміни бізнесу, технологій чи законодавства. Виконання контролюють через автоматичні перевірки конфігурацій, аудити, тестові кампанії й аналіз порушень. Новим працівникам політики доводять під підпис, а чинні редакції доступні в єдиному сховищі з історією змін. Показником зрілості є не обсяг документів, а те, наскільки вони відповідають практиці й підтримуються в актуальному стані [7; 16].

Контрольні питання

1. Яке призначення та структура деталізованої політики безпеки?
2. Які принципи розроблення такої політики?
3. Як класифікують інформаційні активи та які вимоги застосовують до кожного рівня?
4. Які положення політик стосуються управління доступом та ідентифікації?
5. Яких вимог до парольного захисту, мереж, електронної пошти й мобільних пристроїв дотримуються сьогодні?
6. Як контролюють і актуалізують політики безпеки?

ЛЕКЦІЯ 12. ДЕПАРТАМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ І РОБОТА З ПЕРСОНАЛОМ

Підрозділ інформаційної безпеки в сучасній організації виконує організаційну, методичну, технічну й контрольну функції. До його структури залежно від масштабу входять напрями управління ризиками й відповідністю (GRC), архітектури безпеки, управління ідентичностями та доступом, управління вразливостями, центр моніторингу й реагування (SOC), безпека застосунків і хмари, управління безпекою постачальників, а також навчання й підвищення обізнаності. У малих організаціях ці функції поєднує одна особа або їх частково делегують зовнішнім провайдерам. Головною вимогою є чітка відповідальність і наявність ресурсів відповідно до обсягу ризиків [6].

Повноваження підрозділу визначає політика безпеки: він розробляє методичні документи, погоджує проєкти нових систем, веде реєстр ризиків, здійснює моніторинг подій, проводить розслідування, організовує навчання й веде звітність перед керівництвом. Підрозділ має право доступу до необхідної інформації, права вето або ескалації у випадку неприйнятних ризиків і право ініціювати перевірки. Обмеженням є незалежність від IT-операцій: підрозділ безпеки не має самостійно адмініструвати системи, які контролює, інакше втрачається незалежність оцінки.

Керівник із кіберзахисту (CISO) очолює підрозділ і відповідає за стратегію безпеки, управління ризиками, узгодження з регуляторними вимогами, взаємодію з керівництвом і радою, реагування на інциденти. Згідно із Законом № 4336-IX наявність такої посади стала обов’язковою для визначених категорій суб’єктів, а відповідальність за стан кіберзахисту покладається і на керівника організації [19]. Підпорядкування CISO залежить від моделі: прямий звіт генеральному директору або раді забезпечує незалежність і вагу рішень, підпорядкування директору з інформаційних технологій потенційно створює конфлікт інтересів. Компетенції CISO поєднують технічне розуміння, управління ризиками, комунікацію з керівництвом та знання нормативних вимог.

Взаємодія з іншими підрозділами будується на чітких процесах. Із IT-підрозділом погоджують зміни, патчі й конфігурації; з юридичним – договори, регуляторні питання й повідомлення про інциденти; з кадровою службою – прийняття, переведення й звільнення персоналу; із закупівлями – вимоги до постачальників; з комунікаціями – зовнішнє інформування під час криз; з внутрішнім аудитом – незалежну перевірку. Для підтримки цієї взаємодії створюють комітети з безпеки, мережу відповідальних у підрозділах (security champions) і спільні регламенти.

Кадрові ризики пов’язані з тим, що персонал є і першою лінією захисту, і найвразливішою ланкою. Вони охоплюють помилки, недбалість, зловмисні дії, залежність від ключових фахівців, звільнення й конфлікти. Управління кадровими ризиками складається із перевірки кандидатів у межах закону, укладення угод про нерозголошення, чіткого визначення обов’язків у сфері безпеки, програми адаптації, регулярного підтвердження обізнаності, процедур зміни ролей і гарантованого відкликання прав і повернення активів під час звільнення [8]. За даними щорічного звіту Verizon про порушення даних, людський фактор бере участь у переважній більшості компрометацій, тому спрямування зусиль на персонал є виправданим.

Навчання, інструктажі й підвищення обізнаності мають бути безперервними, диференційованими й практичними. Вступний інструктаж знайомить з політиками, а щорічні курси оновлюють знання. Спеціальні програми призначають привілейованим користувачам, розробникам, керівникам та персоналу, що працює з персональними даними. Ефективність підвищується, коли навчання поєднується з імітованими атаками (тестовими фішинговими розсилками), короткими нагадуваннями й позитивною мотивацією замість покарань. Результати вимірюють частками працівників, що повідомляють про підозрілі листи, й часом реагування.

Протидія соціальній інженерії та внутрішнім загрозам потребує поєднання навчання й технічних заходів. Соціальна інженерія охоплює фішинг, його телефонний варіант (вішинг), повідомлення (смішинг), претекстинг, підкидання носіїв і дедалі частіше підроблення голосу та відео за допомогою

штучного інтелекту. Протидіють їй спільним навчанням, перевіркою запитів на платежі й зміну реквізитів каналом зворотного зв’язку, багатофакторною автентифікацією, стійкою до фішингу, і культурою, в якій повідомлення про підозру вітається. Внутрішні загрози, навмисні й ненавмисні, виявляють за допомогою моніторингу доступу й поведінкової аналітики, розподілу обов’язків, обмеження привілеїв і запровадження процедур звільнення. Контроль дотримання здійснюється через аудити, перевірки журналів і оцінку порушень, а дисциплінарні заходи мають бути пропорційними й задокументованими.

Контрольні питання

1. Яка структура і які функції департаменту інформаційної безпеки?
2. Які повноваження він має та як забезпечується його незалежність?
3. Яку роль виконує CISO і як організовано його підпорядкування?
4. Як організується взаємодія підрозділу безпеки з іншими підрозділами?
5. Які кадрові ризики існують і як ними керують?
6. Як організувати навчання персоналу та протидію соціальній інженерії й внутрішнім загрозам?

ЛЕКЦІЯ 13. ОРГАНІЗАЦІЯ РЕАГУВАННЯ НА НАДЗВИЧАЙНІ СИТУАЦІЇ (ІНЦИДЕНТИ)

Надзвичайна ситуація в інформаційній безпеці – стан, за якого подія або сукупність подій порушує нормальне функціонування критично важливих процесів організації або створює загрозу значних втрат, і для подолання якого недостатньо звичайних операційних процедур. Інцидент є вужчим поняттям: це подія, що порушує або загрожує порушити безпеку; більшість інцидентів обробляють у штатному режимі, а надзвичайною ситуація стає тоді, коли масштаб наслідків потребує кризового управління, залучення вищого керівництва, регуляторів і зовнішніх партнерів. Класифікація ґрунтується на типі події, її впливі на активи, терміновості та рівні критичності. Українська практика використовує шкалу від низького до критичного рівня, а Закон № 4336-IX і наказ № 351 запроваджують поняття значного кіберінциденту з відповідними критеріями та обов’язком повідомлення [19; 20].

Принципами реагування є готовність (дії тренуються заздалегідь), швидкість, пропорційність, чіткість відповідальності, збереження доказів, регулярна комунікація й навчання на помилках. Реагування розглядають як частину управління ризиками й безперервністю діяльності, а не як ізольований технічний процес. Сучасні настанови, зокрема NIST SP 800-61 Rev. 3, пов’язують підготовку з управлінням і ідентифікацією ризиків та вимагають безперервного вдосконалення на підставі отриманого досвіду [2].

Команда реагування (CSIRT) складається з керівника інциденту, аналітиків з виявлення та розслідування, технічних фахівців із локалізації та відновлення, представників юридичної служби, комунікацій, кадрів та бізнесових підрозділів. Роботу команди забезпечують контакти зовнішніх сторін: регуляторів, національної команди CERT-UA, правоохоронців, постачальників послуг, страховика. Під час кризи вводять режим штабу з визначеним ритмом нарад і ведуть журнал рішень. Для менших організацій розв’язанням є угоди з зовнішніми провайдерами послуг реагування, які діють за заздалегідь узгодженими процедурами.

Плани реагування та безперервності діяльності зв’язують між собою три документи. План реагування на інциденти описує класифікацію, ролі, процедури й шаблони комунікацій. План безперервності діяльності визначає, як підтримувати критичні процеси під час збою, а план аварійного відновлення – як відновити системи та дані. Основою є аналіз впливу на бізнес, у якому встановлюють допустимий час простою, цільову точку відновлення даних та мінімальний рівень послуг. Плани перевіряють навчаннями трьох видів: настільними вправами, технічними симуляціями і повномасштабними тестами.

Реагування проходить послідовно від виявлення до усунення. Виявлення надходить із систем моніторингу, звітів користувачів, зовнішніх повідомлень та розвідувальних даних. Аналіз підтверджує факт інциденту, визначає масштаб і пріоритет. Локалізація зупиняє поширення шкоди: ізоляцією уражених вузлів, блокуванням облікових записів, відкликанням ключів і токенів, відключенням каналів. Усунення видаляє першопричину, закриває вразливість, відновлює довіру до систем і перевіряє їх чистоту. На кожному етапі зберігають докази з дотриманням ланцюга відповідальності, що дозволяє використати їх у розслідуванні й судовому розгляді [10].

Резервне копіювання та відновлення належать до критичних заходів, особливо за атак із програмами-вимагачами. Практика рекомендує правило «3-2-1», доповнене незмінюваною та ізольованою копією, а також регулярну перевірку відновлення, адже необроблена резервна копія без перевірки фактично не є копією. Відновлення здійснюють у порядку пріоритету критичних сервісів, із попередньою перевіркою чистоти середовища та зміною облікових даних. Рішення про виплату викупу ухвалюють на рівні вищого керівництва за участі юристів, враховуючи ризики санкцій і відсутність гарантій відновлення, а правоохоронців інформують.

Документування й післяінцидентний аналіз перетворюють подію на джерело знань. Запис про інцидент містить хронологію, вплив, прийняті рішення, використані ресурси й відомі індикатори. Аналіз проводять у формі розбору без пошуку винних: встановлюють першопричини, оцінюють, що

спрацювало, а що ні, формулюють коригувальні заходи з відповідальними та строками. Нормативні вимоги встановлюють терміни повідомлення: за NIS2 – попереднє сповіщення, як правило, протягом 24 годин, повідомлення протягом 72 годин і підсумковий звіт протягом місяця; за українським порядком обміну інформацією суб’єкти передають відомості про інциденти відповідним командам реагування в установлені строки [11; 20].

Оцінювання ефективності та вдосконалення реагування здійснюють за кількісними показниками: середнім часом виявлення, середнім часом локалізації й відновлення, часткою інцидентів, виявлених власними засобами, кількістю повторних інцидентів, результатами навчань. Отримані дані порівнюють із цілями й використовують для коригування планів, програм навчання та інвестицій. Зрілість процесу виявляється у здатності швидко ухвалювати рішення за невизначеності, підтримувати комунікацію й повертати організацію до нормальної роботи з мінімальними втратами [2; 6].

Контрольні питання

1. У чому відмінність між інцидентом і надзвичайною ситуацією?
2. Які принципи організації реагування?
3. З кого складається команда реагування і які її функції?
4. Як співвідносяться плани реагування, безперервності й аварійного відновлення?
5. Як організувати резервне копіювання та відновлення після атак?
6. Як документують інциденти та оцінюють ефективність реагування?

ЛЕКЦІЯ 14. АУДИТ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ. НАДАННЯ ПОСЛУГ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (СТРАХУВАННЯ)

Аудит інформаційної безпеки – систематичний, незалежний і документований процес отримання об’єктивних свідчень та їх оцінювання для визначення ступеня відповідності системи захисту встановленим критеріям. Мета аудиту полягає в підтвердженні відповідності вимогам стандартів, законодавства й політик, виявленні слабких місць, оцінюванні ефективності заходів і формуванні рекомендацій щодо вдосконалення. Принципами аудиту є доброчесність, об’єктивне подання результатів, професійна ретельність, конфіденційність, незалежність і підхід, заснований на доказах і ризиках; їх сформульовано в настанові ISO 19011, яку для систем управління безпекою конкретизує ISO/IEC 27007 [6].

Аудит поділяють на внутрішній, який проводять працівники організації або залучені особи для власних потреб і підготовки до зовнішньої перевірки, і зовнішній, що виконують замовники (аудит другої сторони) чи незалежні органи (аудит третьої сторони, зокрема сертифікаційний). За предметом розрізняють аудит відповідності, технічний аудит (перевірка захищеності систем), аудит процесів і аудит постачальників. Новий український підхід до державних систем і критичної інфраструктури відходить від формальної перевірки документів до оцінювання реального стану кіберзахисту й управління ризиками, що збільшує вагу кваліфікованих аудиторів [19].

Етапи аудиту охоплюють планування, збирання доказів, аналіз, звітування і подальший контроль. На етапі планування визначають цілі, сферу, критерії, склад групи, графік та вибірку. Під час збирання доказів застосовують огляд документації, інтерв’ювання, спостереження за процесами, вибіркову перевірку записів і технічні тести. Аналіз порівнює отримані факти із критеріями, класифікує невідповідності за суттєвістю та визначає першопричини. Звіт містить сферу й методологію, результати, класифіковані висновки, оцінку ризиків і рекомендації з пріоритетами. На останньому етапі відстежують виконання коригувальних дій і перевіряють їх результативність.

Методи оцінювання поєднують опитування й перевірку документів з інструментальними засобами. До технічних належать сканування вразливостей, перевірка конфігурацій на відповідність еталонним профілям, тестування на проникнення із різним рівнем попередньої інформації, оцінювання безпеки застосунків та хмарних середовищ, аналіз архітектури та перевірка стійкості до соціальної інженерії. Вибір методів визначається ризиками, а їх застосування потребує письмового дозволу, розподілу відповідальності і правил поводження з даними. Результати подаються у вигляді кількісних і якісних оцінок, наприклад рівня зрілості за шкалою процесів.

Аналіз вразливостей, загроз і ризиків в аудиті зводиться до трьох взаємопов’язаних елементів. Вразливості виявляють технічними й організаційними методами та пріоритезують за критичністю й експлуатованістю. Загрози оцінюють за актуальними даними про дії супротивників у відповідному секторі, спираючись, зокрема, на звіти ENISA й національних команд реагування [4]. Ризики визначають як поєднання вразливостей, загроз і цінності активів, а результат порівнюють з рівнем прийнятного ризику. Це дозволяє розрахувати пріоритети виправлень і обґрунтувати витрати, що є ключовим для рішень керівництва.

Послуги у сфері інформаційної безпеки утворюють окремий ринок. До нього належать консалтинг (розроблення політик, підготовка до сертифікації), аудит і оцінювання відповідності, тестування на проникнення та вправи на кшталт «червоної команди», керовані послуги моніторингу й реагування (MDR, SOC як послуга), послуги віртуального CISO, цифрова криміналістика й реагування на інциденти за договорами з гарантованим часом реакції, навчання персоналу. Використання зовнішніх провайдерів знижує вартість і допомагає отримати компетенції, проте створює залежність і додаткові ризики, тому договори мають містити вимоги до безпеки, конфіденційності, права на перевірку та порядку припинення співпраці.

Кіберстрахування – вид страхування, що покриває фінансові наслідки кіберінцидентів. Його принципи тотожні загальним принципам страхування:

передавання частини ризику страховику за плату (премію), страховий інтерес, добросовісність і розкриття суттєвої інформації. Страхове покриття, як правило, поділяють на власні втрати (витрати на розслідування й відновлення систем та даних, перерва в діяльності, викуп і вимагання, повідомлення постраждалих, кризові комунікації) та відповідальність перед третіми сторонами (позови, судові витрати, а в окремих юрисдикціях – штрафи, якщо їх допускає закон). Типовими винятками є вже відомі до укладення договору порушення, зношення обладнання, внутрішні дії керівництва, а також, відповідно до прийнятих у Ллойдсі вимог 2023 року, дії, що трактуються як державно підтримувані кібероперації, чи наслідки війни. Для українських підприємств це суттєво обмежує доступність покриття, а ринок кіберстрахування в країні залишається початковим.

Оцінювання ризиків для умов страхування спирається на анкети й технічну перевірку. Андеррайтер аналізує рівень зрілості кіберзахисту: наявність багатофакторної автентифікації, захисту кінцевих точок, ізольованих і перевірених резервних копій, управління патчами, плану реагування та навчання персоналу. Страхова премія приблизно відповідає очікуваним втратам із надбавками на витрати, прибуток і невизначеність, а наявність сильних заходів знижує її та підвищує шанси на покриття. Таким чином страхування стимулює розвиток безпеки, проте не замінює її: страховик відшкодовує фінансові наслідки, але не відновлює репутацію й не гарантує безперервності [6].

Покриття фінансових наслідків забезпечується обмеженням (лімітом) відповідальності, франшизою та сублімітами за видами збитків. Організація, обираючи ліміти, виходить із результатів кількісного оцінювання ризиків, максимальних правдоподібних втрат та інших засобів зниження ризику. Страхова подія вимагає швидкого повідомлення страховика, залучення схвалених ним постачальників послуг реагування та збереження доказів, а невиконання цих умов може призвести до відмови у виплаті. Тому страховий договір слід узгодити з планом реагування на інциденти й включити страховика до списку зовнішніх контактів.

Контрольні питання

1. Які мета, завдання й принципи аудиту інформаційної безпеки?

2. Чим відрізняються внутрішній і зовнішній аудит? Охарактеризуйте етапи аудиту.

3. Які методи застосовують для оцінювання стану безпеки?

4. Як в аудиті аналізують вразливості, загрози й ризики? Що містить аудиторський звіт?

5. Які види послуг у сфері інформаційної безпеки існують?

6. Що таке кіберстрахування, які ризики воно покриває й за яких умов діє?

ЛЕКЦІЯ 15. МІЖНАРОДНИЙ СТАНДАРТ ISO/IEC 27001 ПЕРЕЛІК ЗАХИСНИХ ЗАХОДІВ ТА ЇХ ЦІЛЕЙ

Міжнародний стандарт ISO/IEC 27001:2022 «Інформаційна безпека, кібербезпека та захист приватності. Системи управління інформаційною безпекою. Вимоги» призначений для створення, впровадження, підтримки й постійного вдосконалення системи управління інформаційною безпекою. Його сфера охоплює організації будь-якого розміру та галузі, а сертифікація підтверджує, що система відповідає вимогам. Структуру документа складають вступні розділи 1–3 (сфера, нормативні посилання, терміни), основні вимоги розділів 4–10 та нормативний додаток А із переліком заходів захисту. У 2024 році було прийнято зміну 1, що вимагає враховувати у розділах 4.1 та 4.2 вплив кліматичних змін на систему. Українським еквівалентом є ДСТУ ISO/IEC 27001:2023 [7].

Вимоги до системи управління викладено так, щоб їх можна було перевірити під час аудиту: визначення контексту та зацікавлених сторін, сфери застосування, лідерство й політика, ролі, планування заходів щодо ризиків, цілі безпеки, ресурси, компетентність, обізнаність, комунікації, документована інформація, оперативне планування й контроль, моніторинг і вимірювання, внутрішній аудит, аналіз з боку керівництва, реагування на невідповідності й вдосконалення. Особливістю стандарту є вимога, щоб набір заходів визначався результатами оцінювання ризиків, а не механічним застосуванням переліку.

Ризик-орієнтований вибір заходів реалізовано в пункті 6.1.3. Організація встановлює процес оброблення ризиків, визначає всі заходи, необхідні для реалізації обраних варіантів оброблення, порівнює їх із заходами Додатка А, щоб перевірити, чи не пропущено необхідних, формує декларацію застосовності, розробляє план оброблення ризиків і погоджує його та залишкові ризики з власниками. Додаток А не є вичерпним: організація може додавати власні заходи або використовувати інші джерела, і навпаки, виключати ті, що не стосуються її ризиків, обґрунтувавши виключення [7; 9].

Структура та призначення Додатка А у редакції 2022 року відображає узгодження зі стандартом ISO/IEC 27002:2022. Замість чотирнадцяти розділів і 114 заходів стандарт тепер містить 93 заходи, згруповані в чотири теми. Кожен захід у ISO/IEC 27002 має назву, мету, атрибути (тип заходу, властивості безпеки, концепції кібербезпеки, оперативні можливості, домени безпеки) і настанови із впровадження, що дозволяє фільтрувати перелік за різними ракурсами. Нові заходи, додані у 2022 році, охоплюють розвідку про загрози, безпеку при використанні хмарних послуг, готовність ІКТ до забезпечення безперервності діяльності, моніторинг фізичної безпеки, управління конфігурацією, видалення інформації, маскування даних, запобігання витоку даних, моніторинг діяльності, веб-фільтрацію та безпечне кодування [7; 8].

Таблиця 15.1 – Теми Додатка А ISO/IEC 27001:2022

Тема	**Кількість заходів**	**Приклади заходів**
Організаційні	37	Політики, ролі, класифікація інформації, управління доступом, постачальники, інциденти, безперервність
Кадрові	8	Перевірка кандидатів, умови найму, обізнаність і навчання, процедура звільнення, дистанційна робота
Фізичні	14	Периметри, фізичний вхід, захист обладнання, чистий стіл і екран, безпечне видалення
Технологічні	34	Кінцеві пристрої, привілейований доступ, криптографія, мережі, журналювання, безпечна розробка

Організаційні заходи формулюють правила й процеси: політики, розподіл ролей, поділ обов’язків, контакти з органами влади, розвідка про загрози, безпека в управлінні проєктами, інвентаризація й класифікація активів, правила допустимого використання, управління доступом та ідентичностями, безпека відносин із постачальниками та хмарними послугами, управління інцидентами, безперервність, дотримання вимог законодавства, незалежний огляд. Кадрові заходи регулюють життєвий цикл працівника: перевірку, умови, навчання, дисциплінарний процес, обов’язки після звільнення, угоди про нерозголошення, дистанційну роботу та повідомлення про події. Фізичні

заходи охоплюють периметри й приміщення, моніторинг, захист від зовнішніх загроз, роботу в захищених зонах, безпеку обладнання, комунікаційних кабелів та обслуговування. Технологічні заходи – захист кінцевих пристроїв, керування привілейованим доступом, обмеження доступу до інформації, захист від шкідливого коду, управління вразливостями й конфігураціями, резервне копіювання, журналювання, мережеву безпеку, криптографію, безпечну розробку, тестування й управління змінами.

Цілі заходів сформульовано як результати, які необхідно досягти, а не як технічні вимоги. Наприклад, ціль заходу з управління привілейованим доступом – забезпечити, щоб підвищені права мали лише уповноважені користувачі, у необхідний час і для визначених завдань; ціль заходу з резервного копіювання – забезпечити можливість відновлення даних після втрати. Така побудова дає організації свободу вибору способу реалізації, але вимагає обґрунтування достатності. Сукупність цілей дозволяє оцінити, чи покриває набір заходів сценарії ризиків, визначені під час аналізу.

Вибір, обґрунтування та впровадження заходів фіксуються в декларації застосовності (SoA). Для кожного заходу вона містить рішення про застосування, обґрунтування включення чи виключення, стан впровадження та посилання на документи. Це ключовий документ під час сертифікації, адже аудитор перевіряє відповідність між результатами оцінювання ризиків, планом їх оброблення та SoA. Впровадження супроводжується розподілом відповідальності, складанням політик і процедур, технічними роботами, навчанням і збиранням свідчень роботи заходу, наприклад журналів, звітів і записів перевірок.

Моніторинг, результативність і вдосконалення забезпечують життєздатність системи. Організація визначає, що вимірювати, як і коли, використовуючи показники виконання заходів і результативності системи; проводить внутрішній аудит за планом, аналіз керівництвом із розглядом результатів аудитів, змін контексту, рівня виконання цілей та можливостей поліпшення; виправляє невідповідності й усуває їхні причини. Сертифікати за редакцією 2013 року діяли до кінця жовтня 2025 року, тож чинними нині є

сертифікати відповідності редакції 2022 року. Системи, що поєднують ISO/IEC 27001 з іншими стандартами систем управління й з рамками на кшталт NIST CSF 2.0 та вимогами NIS2, демонструють зрілу та інтегровану модель безпеки [1; 3; 7].

Контрольні питання

1. Яке призначення, структура й сфера дії ISO/IEC 27001:2022?
2. Які основні вимоги до системи управління містять розділи 4–10?
3. Як ризик-орієнтований підхід визначає вибір заходів?
4. Яка структура Додатка А і які нові заходи з’явилися в редакції 2022 року?
5. Охарактеризуйте організаційні, кадрові, фізичні й технологічні заходи.
6. Що таке декларація застосовності та яку роль вона відіграє?

СПИСОК ЛІТЕРАТУРИ

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

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

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

5. NIS Investments 2025. Heraklion: ENISA, 2025. URL: https://www.enisa.europa.eu/publications/nis-investments-2025 (дата звернення: 14.11.2026).

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

7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements (with Amd 1:2024). Geneva: ISO, 2022.

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

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

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

11. 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.

12. 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.

13. United Nations Convention against Cybercrime. United Nations Office on Drugs and Crime. URL: https://unodc.org/unodc/en/cybercrime/convention/home.html (дата звернення: 14.11.2026).

14. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Strasbourg: Council of Europe, 2022. (CETS; No. 224).

15. 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.

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

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

18. Про схвалення Національної програми адаптації законодавства України до права Європейського Союзу (acquis ЄС): постанова Кабінету Міністрів України від 1 квіт. 2026 р. № 438. Урядовий портал. URL: https://www.kmu.gov.ua/news/uriad-skhvalyv-prohramu-adaptatsii-zakonodavstva-ukrainy-do-norm-ies-derzhspetszviazku-vidpovidatyme-za-nyzku-kliuchovykh-napriamiv (дата звернення: 14.11.2026).

19. Держспецзв'язку: Україна трансформує систему кібербезпеки за європейськими стандартами. Урядовий портал. URL:

https://www.kmu.gov.ua/news/derzhspetszviazku-ukraina-transformuie-systemu-kiberbezpeky-za-ievropeiskymy-standartamy (дата звернення: 14.11.2026).

20. 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).

21. Порядок авторизації з безпеки: постанова Кабінету Міністрів України від 18 черв. 2025 р. № 712.

22. 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).

23. 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).

24. Державний НДІ технологій кібербезпеки ввів у дію нові стандарти захисту інформації у 2026 році. Дебет-Кредит. URL: https://news.dtkt.ua/society/community/114167-derzavnii-institut-kiberbezpeki-vviv-u-diiu-novi-standarti-zaxistu-informaciyi-u-2026-roci (дата звернення: 14.11.2026).

25. Перелік стандартів, що визначають вимоги до криптографічних алгоритмів і протоколів : затв. наказом Адміністрації Держспецзв'язку від 27 жовт. 2020 р. № 687 (у чинній редакції). URL: https://www.cip.gov.ua/services/cm/api/attachment/download?id=54312 (дата звернення: 14.11.2026).

26. Шахрайство в Україні у 2025 році. Opendatabot. URL: https://opendatabot.ua/en/analytics/fraud-2025-12 (дата звернення: 14.11.2026).

27. Олександр Потій: 2026 рік стане роком переходу до активного кіберзахисту та розбудови цілісної екосистеми кібербезпеки. Урядовий портал. URL: https://www.kmu.gov.ua/news/oleksandr-potii-2026-rik-stane-rokom-perekhodu-do-aktyvnoho-kiberzakhystu-ta-rozbudovy-tsilisnoi-ekosystemy-kiberbezpeky (дата звернення: 14.11.2026).

28. NIST SP 800-63B-4. Digital Identity Guidelines: Authentication and Authenticator Management. Gaithersburg: National Institute of Standards and Technology, 2025.

29. FIPS 203, 204, 205. Module-Lattice-Based Key-Encapsulation Mechanism Standard; Module-Lattice-Based Digital Signature Standard; Stateless Hash-Based Digital Signature Standard. Gaithersburg: National Institute of Standards and Technology, 2024.

30. NIST SP 800-218. Secure Software Development Framework (SSDF) Version 1.1. Gaithersburg: National Institute of Standards and Technology, 2022. DOI: https://doi.org/10.6028/NIST.SP.800-218.

Управління інформаційною безпекою: 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. О.Р. Кулакевич. Луцьк: ЛНТУ, 2026. 64 с.

Комп’ютерний набір О.Р. Кулакевич

Редактор О.Р. Кулакевич

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