Міністерство освіти і науки України
Луцький національний технічний університет

ОСНОВИ КІБЕРБЕЗПЕКИ

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

Луцьк 2026

УДК 004.056 (07)
О75

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

Завідувач кафедри КБ _____ Сергій КОСТЮЧКО

Укладач: _____ Оксана МІСКЕВИЧ, старший викладач кафедри кібербезпеки ЛНТУ

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

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

О75 Основи кібербезпеки : 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. І. Міскевич. Луцьк : ЛНТУ, 2026. 83 с.

Конспект лекцій з дисципліни «**Основи кібербезпеки**» складений відповідно до діючої програми курсу.

Призначений для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань F Інформаційні технології спеціальності 125 Кібербезпека та захист інформації

ЗМІСТ

ВСТУП 5
ТЕМА 1. ВСТУП ДО КІБЕРБЕЗПЕКИ: ОСНОВНІ ПОНЯТТЯ, ЦІЛІ ТА ПРИНЦИПИ 6
1.1 Предмет кібербезпеки та поняття кіберпростору 6
1.2 Основні поняття й терміни 7
1.3 Цілі кібербезпеки: тріада CIA та розширена модель 8
1.4 Базові принципи забезпечення кібербезпеки 9
1.5 Сучасний ландшафт кіберзагроз у цифрах 10
1.6 Складові кібербезпеки та професійні ролі 11
ТЕМА 2. НОРМАТИВНО-ПРАВОВА БАЗА ТА СТАНДАРТИ КІБЕРБЕЗПЕКИ 13
2.1 Рівні нормативно-правового регулювання кібербезпеки 13
2.2 Міжнародні та європейські правові акти 14
2.3 Законодавство України у сфері кібербезпеки 15
2.4 Національна система кібербезпеки та її суб'єкти 17
2.5 Міжнародні та національні стандарти й фреймворки 18
2.6 Відповідальність та практичне застосування вимог 19
ТЕМА 3. ІНФОРМАЦІЙНІ РЕСУРСИ ТА МОДЕЛЬ КУБА КІБЕРБЕЗПЕКИ МАККАМБЕРА 21
3.1 Інформація як ресурс і актив 21
3.2 Класифікація інформаційних ресурсів та їх цінність 21
3.3 Модель куба кібербезпеки Маккамбера 22
3.4 Три виміри моделі та 27 «комірок» 23
3.5 Застосування моделі на практиці 24
3.6 Модель Маккамбера, тріада CIA та сучасні підходи 26
ТЕМА 4. КІБЕРНАПАДНИКИ ТА КІБЕРВІЙНА: ТИПИ, МОТИВИ Й ЦІЛІ 28
4.1 Поняття кібернападника та їх загальна класифікація 28
4.2 Типи кібернападників 28
4.3 Мотиви та цілі 29
4.4 Кібервійна: поняття, ознаки й правові аспекти 30
4.5 Історія та уроки найвідоміших кібероперацій 31
4.6 Російсько-українська кібервійна 32
4.7 Захист від різних типів нападників 33
ТЕМА 5. КІБЕРАТАКИ: КЛАСИФІКАЦІЯ, КОНЦЕПЦІЇ ТА ЕТАПИ РЕАЛІЗАЦІЇ 35
5.1 Основні поняття: загроза, вразливість, атака, інцидент 35
5.2 Класифікація кібератак 35
5.3 Основні види кібератак 36
5.4 Етапи реалізації кібератаки: Cyber Kill Chain 37
5.5 Матриця MITRE ATT&CK 39
5.6 Приклад наскрізного сценарію атаки 39
5.7 Концепції протидії: глибокий захист та Zero Trust 40
ТЕМА 6. МЕТОДИ ПРОНИКНЕННЯ В ІНФОРМАЦІЙНІ СИСТЕМИ ТА ЕКСПЛУАТАЦІЯ ВРАЗЛИВОСТЕЙ 42
6.1 Вразливість: поняття, причини та життєвий цикл 42
6.2 Системи ідентифікації та оцінювання вразливостей (CVE, CWE, CVSS) 43
6.3 Основні класи вразливостей 44

6.4 Методи проникнення в інформаційні системи 44
6.5 Експлуатація вразливостей та дії після проникнення 46
6.6 Тестування на проникнення та управління вразливостями 46
6.7 Принципи захисту 47
ТЕМА 7. ЗАХИСТ КІНЦЕВИХ ПРИСТРОЇВ І МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ 49
7.1 Кінцеві пристрої як ціль атак 49
7.2 Захист кінцевих пристроїв 49
7.3 Мобільні пристрої та політика BYOD 51
7.4 Архітектура захищеної мережі 51
7.5 Засоби мережевого захисту 52
7.6 Безпека бездротових мереж, DNS та віддаленого доступу 53
7.7 Моніторинг та практичний чек-лист 53
ТЕМА 8. ЗБЕРЕЖЕННЯ ДАНИХ, ПРАВО ВЛАСНОСТІ НА ІНФОРМАЦІЮ ТА ЗАХИСТ ОНЛАЙН-ПРИВАТНОСТІ 55
8.1 Дані як об’єкт управління: життєвий цикл і збереження 55
8.2 Резервне копіювання та відновлення 55
8.3 Право власності на інформацію 56
8.4 Захист персональних даних: принципи та права суб’єктів 57
8.5 Інтелектуальна власність у цифровому середовищі 58
8.6 Онлайн-приватність: цифровий слід, відстеження, анонімність 58
8.7 Практичні засоби захисту приватності 59
ТЕМА 9. ТЕХНІЧНІ ЗАСОБИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ 61
9.1 Класифікація технічних засобів кібербезпеки 61
9.2 Криптографічні засоби 62
9.3 Ідентифікація, автентифікація та керування доступом 63
9.4 Засоби захисту вузлів і мережі 64
9.5 Захист даних та застосунків 64
9.6 Засоби моніторингу, реагування та керування вразливостями 65
9.7 Вибір і інтеграція засобів захисту 65
ТЕМА 10. ПОВЕДІНКОВІ АСПЕКТИ КІБЕРБЕЗПЕКИ ТА БЕЗПЕЧНА ПОВЕДІНКА КОРИСТУВАЧІВ 67
10.1 Людський фактор у кібербезпеці 67
10.2 Типові помилки та психологічні чинники 68
10.3 Правила безпечної поведінки користувача 68
10.4 Безпечна поведінка при віддаленій роботі та в соціальних мережах 69
10.5 Культура безпеки та навчання персоналу 70
10.6 Політики та організаційні заходи 71
10.7 Вимірювання та поліпшення поведінки 71
ТЕМА 11. ІНСТРУМЕНТИ ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ ТА ЗАПОБІГАННЯ КІБЕРЗАГРОЗАМ 73
11.1 Принципи виявлення та запобігання загрозам 73
11.2 Джерела даних і журналювання 74
11.3 Системи виявлення та запобігання вторгненням (IDS/IPS) 74
11.4 SIEM, SOAR та центр моніторингу (SOC) 75
11.5 EDR, XDR, NDR та аналіз поведінки 76
11.6 Кіберрозвідка (CTI) та пастки (honeypot) 76
11.7 Реагування на інциденти та показники ефективності 77
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 80

ВСТУП

Навчальна дисципліна «Основи кібербезпеки» формує у студентів базові знання і практичні навички у сфері кібербезпеки, розуміння основних кіберзагроз і вразливостей інформаційних систем, принципів забезпечення конфіденційності, цілісності та доступності інформації, а також опанування базових методів і засобів захисту інформаційних ресурсів, виявлення кіберзагроз та протидії кібератакам.

Програма курсу розподілена на два змістовні модулі, що забезпечують поступове поглиблення знань від основних кіберзагроз до заходів протидії кібератакам.

Змістовий модуль 1 «Основи кібербезпеки та концепції кібератак» охоплює: основні поняття, цілі та принципи кібербезпеки; нормативно-правову базу та стандарти кібербезпеки; інформаційні ресурси та модель куба кібербезпеки; класифікацію кібератак та методи проникнення в інформаційні системи та експлуатацію вразливостей.

Змістовий модуль 2 «Методи та засоби захисту пристроїв та даних» присвячений поглибленому вивченню захисту пристроїв та мережевої інфраструктури; виявленню кіберінцидентів та запобіганню кіберзагрозам.

Студентам необхідно знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

ТЕМА 1. ВСТУП ДО КІБЕРБЕЗПЕКИ: ОСНОВНІ ПОНЯТТЯ, ЦІЛІ ТА ПРИНЦИПИ

План лекції

1. Предмет кібербезпеки та поняття кіберпростору
2. Основні поняття й терміни
3. Цілі кібербезпеки: тріада CIA та розширена модель
4. Базові принципи забезпечення кібербезпеки
5. Сучасний ландшафт кіберзагроз у цифрах
6. Складові кібербезпеки та професійні ролі

1.1 Предмет кібербезпеки та поняття кіберпростору

Кібербезпека – прикладна міждисциплінарна галузь, що поєднує інформатику, мережеві технології, криптографію, право, управління ризиками та психологію. Її завдання – забезпечити можливість безпечно користуватися цифровими системами: банківськими застосунками, державними сервісами, промисловими контролерами, мобільним зв’язком. Якщо ще 30 років тому захист інформації зводився здебільшого до охорони приміщень, шифрування каналів зв’язку та контролю доступу до єдиного обчислювального центру, то сьогодні кожен смартфон, «розумний» лічильник чи камера спостереження є потенційною точкою входу для зловмисника.

Базовим для дисципліни є поняття кіберпростору – середовища, що виникає в результаті взаємодії сумісних комунікаційних систем, мережі Інтернет та інших глобальних мереж передачі даних і дає змогу здійснювати комунікації та реалізовувати суспільні відносини. На відміну від фізичного простору, кіберпростір не має державних кордонів, дозволяє діяти анонімно та масштабувати атаку майже без додаткових витрат: той самий шкідливий лист можна надіслати і десятьом, і десяти мільйонам адресатів.

Окремо розрізняють інформаційну безпеку та кібербезпеку. Інформаційна безпека охоплює захист інформації в будь-якому вигляді (паперовому, усному,

електронному), тоді як кібербезпека зосереджується на захисті цифрових систем, мереж, програм і даних, а також користувачів, що працюють із ними. Стандарт ISO/IEC 27001:2022 прямо поєднує ці поняття в назві («Інформаційна безпека, кібербезпека та захист приватності»), що відображає практичне зближення обох напрямів.

Приклад. Чому кіберпростір змінює правила. У 2017 році вірус-шифрувальник NotPetya, розповсюджений через оновлення української бухгалтерської програми, за лічені години вийшов за межі України та зупинив роботу транснаціональних корпорацій. Атака, розпочата в одній країні, мала глобальні наслідки, а збитки оцінювали в мільярди доларів. Це типовий приклад відсутності «кордонів» у кіберпросторі.

1.2 Основні поняття й терміни

Для коректного спілкування між фахівцями необхідно користуватися єдиною термінологією. Основні терміни, визначені Законом України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII та міжнародними стандартами серії ISO/IEC 27000, подано в таблиці 1.1.

Таблиця 1.1 – Основні терміни кібербезпеки

Термін	Зміст поняття	Приклад
Актив	Будь-що, що має цінність для організації: дані, програми, обладнання, репутація, персонал	База даних клієнтів; сервер електронної пошти
Вразливість	Слабкість активу або засобу захисту, яку може використати загроза	Незакрита помилка в програмі; простий пароль адміністратора
Загроза	Потенційна причина небажаного інциденту, що може завдати шкоди системі або організації	Шифрувальник-вимагач; помилка співробітника
Кібератака	Цілеспрямовані дії в кіберпросторі з метою порушити безпеку системи чи даних	DDoS-атака на сайт державного органу
Кіберінцидент	Подія, що порушила або створила загрозу порушення безпеки: зламаний акаунт, витік даних, збій через атаку	Виявлено несанкціонований вхід до пошти бухгалтера

Продовження таблиці 1.1.

Термін	Зміст поняття	Приклад
Ризик	Поєднання ймовірності події та розміру можливої шкоди від неї	Ймовірність фішингу високого рівня × збитки від втрати грошей
Кіберзахист	Сукупність організаційних, правових, інженерно-технічних і криптографічних заходів, спрямованих на запобігання інцидентам, виявлення атак і відновлення роботи систем	Міжмережеві екрани, резервні копії, політики доступу
Кіберстійкість	Здатність системи витримувати атаки, продовжувати роботу та швидко відновлюватися	Перемикання сервісу на резервний дата-центр

Взаємозв’язок термінів зручно уявити як ланцюг: загроза використовує вразливість активу, що створює ризик, а реалізація ризику приймає форму кібератаки чи кіберінциденту. Захисні заходи (контролі) спрямовані на розрив цього ланцюга на будь-якій ланці: зменшити цінність активу для зловмисника, усунути вразливість, знизити ймовірність загрози або пом’якшити наслідки.

1.3 Цілі кібербезпеки: тріада CIA та розширена модель

Класичною основою моделі безпеки є тріада CIA (Confidentiality – Integrity – Availability). Кожна атака, як правило, порушує одну чи кілька її властивостей.

– Конфіденційність – інформація доступна лише тим, хто має на це право. Порушується при витоку баз даних, перехопленні трафіку, перегляді чужих листів. Захисні заходи: шифрування, контроль доступу, багатофакторна автентифікація.

– Цілісність – дані та системи не змінені несанкціоновано й залишаються достовірними. Порушується при підміні платіжних реквізитів, зміні вмісту сайту, модифікації програмного коду. Захист: хеш-функції, цифрові підписи, журнали змін, контроль версій.

– Доступність – авторизовані користувачі отримують доступ до сервісів і даних тоді, коли це потрібно. Порушується при DDoS-атаках, ураженні шифрувальниками, збоях живлення. Захист: резервування, резервні копії, балансування навантаження, плани відновлення.

Стандарти доповнюють тріаду додатковими властивостями: автентичність (підтвердження, що суб'єкт чи об'єкт є тим, за кого себе видає), підзвітність (можливість простежити дії до конкретного користувача), неспростовність (неможливість відмовитися від виконаної дії, наприклад підпису) та надійність. Для персональних даних додається ще й приватність, нормована окремими законами та регламентами (зокрема GDPR у ЄС).

Приклад. Один інцидент – різні порушення. Шифрувальник на сервері лікарні порушує доступність (лікарі не можуть відкрити картки пацієнтів), а за схемою «подвійного вимагання» ще й конфіденційність (зловмисники копіюють дані перед шифруванням і погрожують їх оприлюднити). Якщо при цьому змінено записи про алергії, постраждає й цілісність, а значить – безпека пацієнтів.

Властивості CIA іноді конфліктують. Максимальна конфіденційність (суворі обмеження, багатоетапні перевірки) знижує зручність і доступність; максимальна доступність (відкриті сервіси, спрощений вхід) послаблює захист. Тому завдання фахівця – не «захистити все за будь-яку ціну», а знайти обґрунтований баланс залежно від цінності активів і бізнес-потреб.

1.4 Базові принципи забезпечення кібербезпеки

Безпека не зводиться до набору програм: це підхід до проєктування й експлуатації систем. Принципи, сформульовані у класичних роботах (Salzer & Schroeder, Kerckhoffs) і закріплені в сучасних стандартах та настановах NIST і ENISA, подано в таблиці 1.2.

Таблиця 1.2 – Базові принципи кібербезпеки

Принцип	Суть	Практичний вираз
Ешелонована оборона (defense in depth)	Кілька незалежних рівнів захисту: збій одного не веде до компрометації всієї системи	Периметр + сегментація мережі + захист кінцевих пристроїв + резервні копії
Мінімальні привілеї	Користувач і програма мають лише ті права, що потрібні для роботи	Звичайний обліковий запис для щоденної роботи; окремий адміністративний
Розподіл обов'язків	Критична дія потребує участі двох і більше осіб	Платіж понад ліміт підтверджують двоє співробітників

Продовження таблиці 1.2.

Принцип	Суть	Практичний вираз
Безпека за задумом та за замовчуванням (security by design / by default)	Захист закладають від початку проєктування; налаштування за замовчуванням є безпечними	Заводські паролі змінюються при першому вході; зайві порти закриті
Нульова довіра (zero trust)	«Ніколи не довіряй, завжди перевіряй»: довіра не надається автоматично за місцем у мережі	Перевірка особи та стану пристрою при кожному зверненні до ресурсу
Економія механізмів та відкритий дизайн	Простіші механізми легше перевірити; стійкість має ґрунтуватися на ключі, а не на секретності алгоритму	Використання відкритих перевірених криптографічних алгоритмів
Ризик-орієнтованість і безперервне вдосконалення	Витрати на захист співмірні з оцінкою ризиків; система захисту постійно оновлюється	Цикл «план – виконання – перевірка – удосконалення» (PDCA) у ISO/IEC 27001

На рівні всієї національної системи принципи кібербезпеки України, визначені законом, включають пріоритет захисту прав людини, державно-приватне партнерство, баланс між потребами безпеки та свободами, а також відкритість до міжнародної співпраці. Відповідальність за кібербезпеку поділена між державою, власниками об’єктів критичної інфраструктури та кожним користувачем.

1.5 Сучасний ландшафт кіберзагроз у цифрах

Актуальні дані допомагають зрозуміти, на чому слід фокусувати захист. За звітом Verizon Data Breach Investigations Report 2025, проаналізовано 22 052 інциденти, з яких 12 195 підтверджених витоків; людський фактор брав участь приблизно у 60 % витоків, експлуатація вразливостей була початковим вектором у 20 % випадків (на 34 % більше, ніж торік), а втручання третіх сторін (постачальників, підрядників) зросло з 15 до 30 %. Програми-вимагачі були присутні у 44 % витоків.

За даними ENISA Threat Landscape 2025 (проаналізовано 4 875 інцидентів у ЄС за період з 1 липня 2024 до 30 червня 2025 року), фішинг залишається основним способом первинного проникнення (близько 60 %), на другому місці – експлуатація вразливостей (21,3 %). Більшість зареєстрованих інцидентів – DDoS-атаки

хактивістів (77 %), проте найбільш руйнівними для організацій лишаються програми-вимагачі. Звіт IBM Cost of a Data Breach 2026 фіксує, що середня вартість витоку у світі сягнула рекордних 4,99 млн доларів США, а кількість атак із використанням штучного інтелекту зросла на 56 % за рік.

В Україні, за даними CERT-UA, кількість зареєстрованих кіберінцидентів зросла з 2 541 у 2023 році до 4 315 у 2024-му та 5 927 у 2025 році. У той самий час, за оцінкою Держспецзв'язку, кількість найбільш серйозних інцидентів («помаранчевого», «червоного» та «чорного» рівнів) зменшилась на 75 %, що свідчить про зростання стійкості та ефективності реагування. Ключові показники стану кібербезпеки подано в таблиці 1.3.

Таблиця 1.3 – Ключові показники стану кібербезпеки

Показник	**Значення**	**Джерело**
Участь людського фактора у витоках	≈ 60 %	Verizon DBIR 2025
Експлуатація вразливостей як початковий вектор	20 % (+34 % за рік)	Verizon DBIR 2025
Фішинг як вектор проникнення в ЄС	≈ 60 %	ENISA ETL 2025
Середня вартість витоку даних у світі	4,99 млн USD	IBM, 2026
Інцидентів, опрацьованих CERT-UA у 2025 р.	5 927	CERT-UA / Держспецзв'язку

1.6 Складові кібербезпеки та професійні ролі

Практичну кібербезпеку зазвичай розглядають як взаємодію трьох складових: людей (навчання, культура безпеки), процесів (політики, управління ризиками, реагування на інциденти) та технологій (міжмережеві екрани, антивіруси, системи виявлення вторгнень, шифрування). Домінування лише однієї складової призводить до перекосів: найдорожче обладнання не допоможе, якщо співробітник передасть пароль шахраєві.

За напрямами виокремлюють: мережеву безпеку, безпеку кінцевих пристроїв, безпеку застосунків, хмарну безпеку, безпеку даних і криптографію, керування ідентифікацією та доступом, безпеку промислових (OT/ICS) систем, цифрову криміналістику та реагування на інциденти. Відповідно існують і професійні ролі: аналітик центру моніторингу (SOC), фахівець із реагування на інциденти,

тестувальник на проникнення (pentester), архітектор безпеки, аудитор, керівник з кіберзахисту (CISO). З 2025 року, після ухвалення Закону № 4336-IX, посада керівника з кіберзахисту стала обов'язковою у державних органах та на об'єктах критичної інфраструктури.

Висновки

Кібербезпека – це система заходів, спрямована на збереження конфіденційності, цілісності й доступності інформації та цифрових сервісів, а також на забезпечення кіберстійкості організацій і держави. Вона спирається на єдину термінологію, ризик-орієнтований підхід і базові принципи (ешелонована оборона, мінімальні привілеї, нульова довіра). Статистика останніх років свідчить: більшість успішних атак використовує людський фактор та вразливості, а отже, ефективний захист поєднує технології, процеси і навчання користувачів.

Контрольні питання

1. Чим кібербезпека відрізняється від інформаційної безпеки?

2. Поясніть зв'язок понять «актив – вразливість – загроза – ризик – кіберінцидент».

3. Які властивості входять до тріади CIA? Наведіть по одному прикладу порушення кожної з них.

4. У яких випадках вимоги конфіденційності та доступності вступають у конфлікт? Як шукати баланс?

5. Сформулюйте принципи мінімальних привілеїв та ешелонованої оборони та проілюструйте їх прикладами.

6. Які дані Verizon DBIR 2025 та ENISA ETL 2025 свідчать про значення людського фактора в кібератаках?

Література: [1], [2], [3], [4], [5], [6], [7], [8], [9].

ТЕМА 2. НОРМАТИВНО-ПРАВОВА БАЗА ТА СТАНДАРТИ КІБЕРБЕЗПЕКИ

План лекції

1. Рівні нормативно-правового регулювання кібербезпеки
2. Міжнародні та європейські правові акти
3. Законодавство України у сфері кібербезпеки
4. Національна система кібербезпеки та її суб'єкти
5. Міжнародні та національні стандарти й фреймворки
6. Відповідальність та практичне застосування вимог

2.1 Рівні нормативно-правового регулювання кібербезпеки

Кібербезпека – одна з небагатьох технічних галузей, де правила багато в чому визначаються правом. Закони встановлюють, хто відповідає за захист критичної інфраструктури, які інциденти необхідно повідомляти, яку відповідальність несе зловмисник чи недбалий власник системи. Стандарти, у свою чергу, пояснюють, як саме побудувати систему управління безпекою, і створюють спільну мову для організацій, регуляторів та аудиторів.

Регулювання має кілька рівнів. На міжнародному рівні діють конвенції та рекомендації (зокрема Конвенція Ради Європи про кіберзлочинність). На наднаціональному – регламенти й директиви Європейського Союзу. На національному – закони, укази, постанови уряду, накази профільних органів. На галузевому – вимоги регуляторів (наприклад, Національного банку України до фінансового сектору). Нарешті, на рівні організації – внутрішні політики, положення та інструкції, які конкретизують зовнішні вимоги. Рівні регулювання кібербезпеки подано в таблиці 2.1.

Таблиця 2.1 – Рівні регулювання кібербезпеки

Рівень	Приклади документів	Характер
Міжнародний	Будапештська конвенція про кіберзлочинність (2001); рекомендації ООН щодо відповідальної поведінки держав у кіберпросторі	Обов'язкові для держав-учасниць / рекомендаційні
Європейський	Директива NIS2 (2022/2555); Cybersecurity Act (2019/881); GDPR (2016/679); DORA (2022/2554); Cyber Resilience Act (2024/2847)	Обов'язкові в ЄС; для України – орієнтир гармонізації
Національний	Закон № 2163-VIII; Закон № 4336-IX; Закон «Про критичну інфраструктуру»; Кримінальний кодекс	Обов'язкові
Стандарти й фреймворки	ISO/IEC 27001:2022; NIST CSF 2.0; CIS Controls; PCI DSS	Добровільні, але можуть бути вимогою договору чи регулятора
Рівень організації	Політика інформаційної безпеки; план реагування на інциденти	Обов'язкові для працівників

2.2 Міжнародні та європейські правові акти

Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція, 2001) – перший міжнародний договір, що встановив спільні підходи до криміналізації правопорушень у кіберпросторі (несанкціонований доступ, перехоплення даних, втручання у систему, шахрайство з використанням комп'ютерів), порядку збирання електронних доказів та міжнародної співпраці правоохоронних органів. Україна ратифікувала Конвенцію у 2005 році, а її положення відображені в розділі XVI Кримінального кодексу України.

Для сучасної практики ключовою є Директива (ЄС) 2022/2555 (NIS2), що замінила попередню Директиву NIS. Вона поширюється на «суттєві» та «важливі» суб'єкти у секторах енергетики, транспорту, банківської справи, охорони здоров'я, цифрової інфраструктури, державного управління, космосу та ін. Основні вимоги NIS2:

– запровадити заходи управління кіберризиками (політики аналізу ризиків, реагування на інциденти, безперервність діяльності, безпека ланцюга постачання, шифрування, багатофакторна автентифікація, навчання);

– повідомляти про значні інциденти: раннє попередження – протягом 24 годин, повідомлення про інцидент – протягом 72 годин, остаточний звіт – протягом одного місяця;

– покласти відповідальність за кібербезпеку на керівництво організації (затвердження заходів, проходження навчання);

– за порушення передбачено штрафи: для суттєвих суб'єктів – до 10 млн євро або 2 % світового обороту, для важливих – до 7 млн євро або 1,4 %.

Cybersecurity Act (Регламент (ЄС) 2019/881) закріпив мандат Агентства ЄС з кібербезпеки (ENISA) і запровадив загальноєвропейську систему сертифікації ІКТ-продуктів, послуг та процесів. GDPR (Регламент 2016/679) регулює обробку персональних даних і вимагає «відповідних технічних та організаційних заходів» захисту, а також повідомлення наглядового органу про витік протягом 72 годин; штрафи сягають 20 млн євро або 4 % обороту. DORA (Регламент 2022/2554) встановлює вимоги до цифрової операційної стійкості фінансового сектору, а Cyber Resilience Act (Регламент 2024/2847) – до безпеки програмних та апаратних продуктів із цифровими елементами протягом усього життєвого циклу; його вимоги застосовуватимуться поетапно до 2027 року.

Приклад. Як NIS2 змінює бізнес. Виробник медичних пристроїв з ЄС, що використовує хмарні сервіси українського IT-підрядника, за NIS2 зобов'язаний оцінювати кіберризики ланцюга постачання. Тому європейські замовники дедалі частіше вимагають від українських компаній сертифікат ISO/IEC 27001, політики реагування на інциденти та регулярні тестування на проникнення – навіть якщо національне законодавство цього напряму не вимагає.

2.3 Законодавство України у сфері кібербезпеки

Фундамент правового регулювання становить Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року. Він визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини, суспільства і держави в кіберпросторі, основні принципи (законність, пріоритет прав людини, державно-приватне партнерство,

пропорційність заходів, міжнародна співпраця), а також повноваження суб'єктів національної системи кібербезпеки.

До основних правових актів належать також закони «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних», «Про електронні комунікації», «Про електронну ідентифікацію та електронні довірчі послуги», «Про критичну інфраструктуру» (№ 1882-IX від 2021 року). Кримінальний кодекс (розділ XVI) передбачає відповідальність за правопорушення у сфері використання комп'ютерів, систем та мереж: несанкціоноване втручання в роботу інформаційних систем (ст. 361), створення та розповсюдження шкідливих програм (ст. 361-1), несанкціоновані дії з інформацією (ст. 362), порушення правил експлуатації (ст. 363), перешкоджання роботі (ст. 363-1).

Стратегічним документом була Стратегія кібербезпеки України на 2021–2025 роки «Безпечний кіберпростір – запорука успішного розвитку країни» (введена Указом Президента від 26.08.2021 № 447/2021). Вона визначала три напрями: стримування (посилення спроможностей щодо протидії агресору), кіберстійкість (захист державних ресурсів та критичної інфраструктури) і взаємодію (співпраця з бізнесом, науковою спільнотою, міжнародними партнерами).

Закон № 4336-IX: курс на NIS2

Найважливішою новацією останніх років став Закон № 4336-IX від 27 березня 2025 року «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», який імплементує положення європейської директиви NIS2. Його ключові зміни:

– перехід від застарілої моделі комплексних систем захисту інформації (КСЗІ) до управління ризиками з урахуванням профілів безпеки;

– обов'язкова посада керівника з кіберзахисту (CISO) та підрозділів кіберзахисту в державних органах і на об'єктах критичної інфраструктури; для керівника встановлено вимоги до освіти (ІТ або кібербезпека) та стажу (не менше 3 років), а кандидатуру погоджують Держспецзв'язку та СБУ;

– створення національної системи реагування на кіберінциденти та системи обміну інформацією про них, механізми реагування в кризовій ситуації;

– система оцінювання стану кіберзахисту з використанням аудиту.

На виконання закону уряд оновив підзаконну базу: Загальні вимоги з кіберзахисту об’єктів критичної інфраструктури (постанова КМУ № 518 від 19.06.2019 у редакції постанови № 1470 від 13.11.2025), Національний план реагування на кіберінциденти, кібератаки та кіберзагрози (постанова № 1533 від 26.11.2025), порядок авторизації з безпеки ІС (постанова № 712 від 18.06.2025). Наказом Адміністрації Держспецзв’язку № 54 від 30.01.2025 затверджено базові заходи кіберзахисту. За повідомленням Держспецзв’язку (квітень 2026 р.), у 2026 році завершується розроблення решти нормативних актів, а основний акцент зміщується на практику застосування й створення регіональних центрів кіберзахисту.

2.4 Національна система кібербезпеки та її суб’єкти

Національна система кібербезпеки – сукупність суб’єктів, що забезпечують кіберзахист і координують зусилля держави. Координаційним органом при Раді національної безпеки і оборони України є Національний координаційний центр кібербезпеки (НКЦК). Основні суб’єкти та їх завдання подано в таблиці 2.2.

Таблиця 2.2 – Суб’єкти національної системи кібербезпеки

Суб’єкт	Основна роль
РНБО / НКЦК	Координація діяльності суб’єктів сектору безпеки й оборони, аналіз стану кібербезпеки, стратегічне планування
Держспецзв’язку (Державний центр кіберзахисту, CERT-UA)	Формування й реалізація політики кіберзахисту, захист державних ресурсів та критичної інфраструктури, реагування на інциденти
СБУ	Протидія кіберзлочинам проти основ національної безпеки, кібершпигунству, кібертероризму; контррозвідувальний захист
Кіберполіція Національної поліції	Боротьба з кіберзлочинністю: шахрайство, злочини у сфері платіжних систем

Продовження таблиці 2.2

Суб'єкт	Основна роль
Міноборони, Генштаб ЗСУ, розвідувальні органи	Кібероборона, військова розвідка в кіберпросторі
Національний банк України	Регулювання та нагляд у сфері кібербезпеки фінансового сектору
Оператори критичної інфраструктури та бізнес	Впровадження вимог кіберзахисту, інформування про інциденти

2.5 Міжнародні та національні стандарти й фреймворки

Стандарт відрізняється від закону добровільністю застосування, але в договорах, тендерах і вимогах регуляторів його дотримання часто стає обов'язковим. Основні стандарти та фреймворки подано в таблиці 2.3.

Таблиця 2.3 – Основні стандарти та фреймворки

Документ	Призначення	Ключові ознаки
ISO/IEC 27001:2022	Вимоги до системи управління інформаційною безпекою (СУІБ); можлива сертифікація	Розділи 4–10 (контекст, лідерство, планування, підтримка, функціонування, оцінка, вдосконалення); Додаток А – 93 заходи у 4 темах: організаційні (37), людські (8), фізичні (14), технологічні (34)
ISO/IEC 27002:2022	Настанови щодо впровадження заходів захисту	Каталог заходів із атрибутами; нові заходи: аналіз загроз (threat intelligence), безпека хмарних послуг та ін.
ISO/IEC 27005; ISO 31000	Управління ризиками	Процес: контекст, ідентифікація, аналіз, оцінка, обробка ризиків
NIST CSF 2.0 (2024)	Фреймворк управління кіберризиками (добровільний)	Шість функцій: Govern, Identify, Protect, Detect, Respond, Recover
NIST SP 800-53 Rev. 5	Каталог заходів безпеки для ІС	Понад 1 000 вимог, 20 сімейств заходів
CIS Controls v8.1	Пріоритизований перелік практичних заходів	18 контролів; групи впровадження IG1–IG3
PCI DSS v4.0.1	Захист даних платіжних карток	Обов'язковий для організацій, що приймають картки
ДСТУ ISO/IEC 27001:2023	Національне прийняття ISO/IEC 27001:2022	Використовується для сертифікації в Україні

Фреймворк NIST CSF 2.0, оприлюднений 26 лютого 2024 року, доповнив п'ять функцій попередньої версії новою – Govern (Управління), що ставить кібербезпеку в центр корпоративного управління ризиками. Функції утворюють безперервний цикл: Govern визначає стратегію, Identify – активи та ризики, Protect

– захисні заходи, Detect – виявлення подій, Respond – реагування, Recover – відновлення. Фреймворк не вимагає сертифікації і застосовується організаціями будь-якого розміру.

Приклад. ISO/IEC 27001 у малому підприємстві. IT-компанія зі 40 працівників перед виходом на європейський ринок проводить інвентаризацію активів, оцінює ризики (наприклад, втрата ноутбука з кодом), складає «Положення про застосовність» із переліком обраних заходів з Додатка А (шифрування дисків, багатофакторна автентифікація, навчання персоналу), після чого проходить зовнішній аудит та отримує сертифікат на три роки з щорічними наглядовими аудитами.

2.6 Відповідальність та практичне застосування вимог

Нормативні вимоги реалізуються через цикл «вимога – політика – процедура – доказ». Для кожної вимоги організація визначає відповідальну особу, запроваджує процедуру (наприклад, порядок скасування доступу при звільненні) і збирає докази виконання (журнали, звіти, протоколи навчання), які перевіряють аудитори. Типові помилки: формальна «паперова» відповідність без технічних заходів, відсутність регулярного оновлення політик, неврахування вимог до підрядників.

Відповідальність за порушення може бути кримінальною (для зловмисників – за статтями розділу XVI КК), адміністративною та цивільно-правовою (штрафи, відшкодування шкоди), а також договірною (штрафні санкції, втрата контракту). Для керівників державних органів та об’єктів критичної інфраструктури нові норми закріплюють персональну відповідальність за впровадження кіберзахисту, а для організацій у ЄС NIS2 прямо передбачає відповідальність менеджменту.

Висновки

Нормативно-правова база кібербезпеки багаторівнева: від конвенцій і директив ЄС до внутрішніх політик організації. Україна рухається до європейської моделі – Закон № 4336-IX запроваджує управління ризиками, посаду CISO та національну систему реагування. Стандарти ISO/IEC 27001 і NIST CSF 2.0 дають практичний інструментарій для побудови системи захисту і підтвердження її якості.

Знання нормативної бази – обов’язкова частина професійної підготовки фахівця з кібербезпеки.

Контрольні питання

1. Які рівні нормативно-правового регулювання кібербезпеки ви знаєте? Наведіть приклади для кожного.

2. Які основні вимоги Директиви NIS2 до суб’єктів та які терміни повідомлення про інциденти вона встановлює?

3. Які ключові зміни запровадив Закон України № 4336-IX?

4. Назвіть суб’єктів національної системи кібербезпеки та їхні основні функції.

5. У чому відмінність між законом, стандартом і фреймворком? Чому стандарт може стати обов’язковим?

6. Опишіть шість функцій NIST CSF 2.0. Що нового внесла функція Govern?

Література: [1], [2], [3], [9], [10], [11], [12], [13], [14], [15], [16], [17].

ТЕМА 3. ІНФОРМАЦІЙНІ РЕСУРСИ ТА МОДЕЛЬ КУБА КІБЕРБЕЗПЕКИ МАККАМБЕРА

План лекції

1. Інформація як ресурс і актив
2. Класифікація інформаційних ресурсів та їх цінність
3. Модель куба кібербезпеки Маккамбера
4. Три виміри моделі та 27 «комірок»
5. Застосування моделі на практиці
6. Модель Маккамбера, тріада CIA та сучасні підходи

3.1 Інформація як ресурс і актив

Інформаційними ресурсами називають документовану інформацію, що зберігається в базах даних, файлах, архівах, інформаційно-комунікаційних системах, а також засоби її створення, обробки та передавання. Для організації вони є активом: мають вартість, можуть бути втрачені, викрадені чи спотворені, а їхня недоступність призводить до збитків. Тому першим кроком побудови захисту є розуміння того, що саме необхідно захищати.

Міжнародний стандарт ISO/IEC 27000 визначає актив як усе, що має цінність для організації. Інформаційна безпека оперує двома групами активів: первинними (інформація, бізнес-процеси) та допоміжними (апаратура, програмне забезпечення, мережі, персонал, приміщення, постачальники), які забезпечують існування первинних. Вразливість допоміжного активу робить вразливим і первинний: викрадений ноутбук – це загроза даним, що на ньому зберігаються.

3.2 Класифікація інформаційних ресурсів та їх цінність

За режимом доступу інформація поділяється на відкриту та інформацію з обмеженим доступом. До останньої в законодавстві України належать конфіденційна інформація (персональні дані, комерційна таємниця, службова

інформація) та таємна інформація (державна й інші передбачені законом таємниці). Класифікація за ступенем критичності для організації, як правило, містить чотири рівні (таблиця 3.1).

Таблиця 3.1 – Приклад схеми класифікації інформації

Рівень	**Опис**	**Приклади**	**Наслідки компрометації**
Публічна	Призначена для вільного поширення	Сайт, прес-релізи, відкриті набори даних	Мінімальні
Внутрішня	Для працівників організації	Регламенти, внутрішні телефонні довідники	Незначні, репутаційні
Конфіденційна	Обмежене коло осіб	Персональні дані, договори, фінансова звітність, вихідний код	Значні фінансові й правові збитки
Строго конфіденційна / таємна	Вкрай обмежене коло осіб	Криптографічні ключі, ноу-хау, державна таємниця	Критичні, можлива загроза існуванню організації

Цінність ресурсу оцінюють за наслідками порушення його конфіденційності, цілісності та доступності: прямі збитки, витрати на відновлення, штрафи, втрату довіри клієнтів, зупинку процесів. Оцінка є вхідними даними для аналізу ризиків і визначає, які заходи захисту економічно виправдані: захист не повинен коштувати дорожче за те, що захищається.

Приклад. Інвентаризація активів. Під час аудиту невелика лікарня склала реєстр активів: електронна медична карта (конфіденційна, висока критичність доступності), сервер реєстратури, комп’ютери лікарів, медичні пристрої з мережевим підключенням, бухгалтерські дані, сайт. З’ясувалося, що пристрої діагностики працюють на застарілій ОС і підключені до загальної мережі: допоміжний актив, про який раніше не згадували, створював ризик для життєво важливого первинного – доступності даних пацієнтів.

3.3 Модель куба кібербезпеки Маккамбера

Модель запропонував американський дослідник Джон Маккамбер (John McCumber) у 1991 році у праці «Information systems security: A comprehensive model». Її називають кубом Маккамбера (McCumber Cube) або структурою безпеки

інформаційних систем. Автор виходив з того, що безпеку неможливо звести до окремих технічних засобів: необхідно одночасно розглядати, які властивості інформації захищаються, де вона перебуває і якими засобами це досягається. Три відповіді утворюють три виміри куба (рис. 3.1).

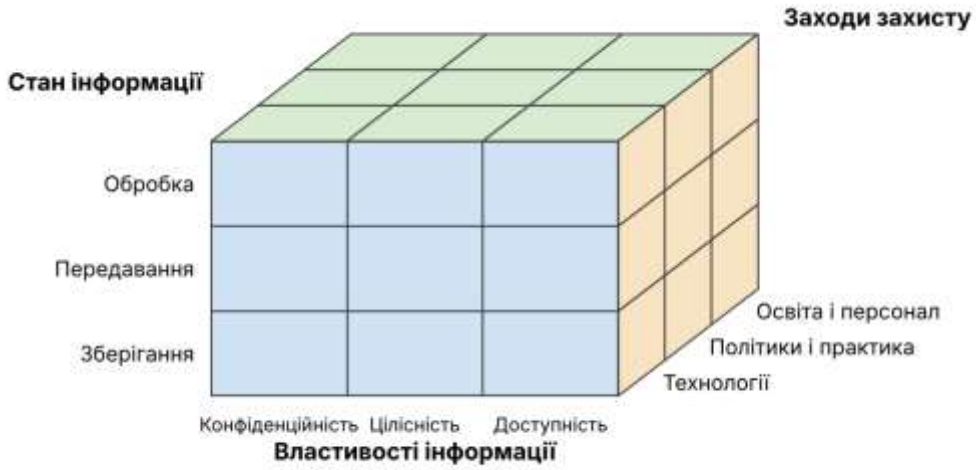


Рисунок 3.1 – Куб кібербезпеки Маккамбера

3.4 Три виміри моделі та 27 «комірок»

Вимір 1. Властивості (цілі) безпеки

Відповідає класичній тріаді CIA: конфіденційність – доступ до інформації мають лише уповноважені суб’єкти; цілісність – інформація не змінюється несанкціоновано та зберігає коректність; доступність – інформація й сервіси доступні тоді, коли потрібні. Саме ці цілі визначають, що вважати порушенням безпеки.

Вимір 2. Стан інформації

– Зберігання (storage, data at rest): диски, бази даних, хмарні сховища, резервні копії, USB-носії;

– Передавання (transmission, data in transit): мережі, електронна пошта, API, канали зв’язку;

– Обробка (processing, data in use): виконання програм, оперативна пам’ять, обчислення, відображення на екрані.

Одна й та сама інформація змінює стан протягом життєвого циклу й потребує різного захисту: для даних у спокої застосовують шифрування диска, для даних у русі – TLS, для даних під час обробки – контроль доступу, ізоляцію процесів, а в окремих випадках конфіденційні обчислення.

Вимір 3. Заходи захисту

– Технології – апаратні та програмні засоби: міжмережеві екрани, антивіруси, шифрування, системи виявлення вторгнень, резервне копіювання;

– Політики та практика – правила, процедури, регламенти, закони й стандарти, що визначають належну поведінку;

– Освіта та персонал (people) – навчання, підвищення обізнаності, тренування, культура безпеки.

Перетин трьох вимірів дає 3 × 3 × 3 = 27 комірок. Кожна комірка – окреме питання, на яке повинна відповісти система захисту. Наприклад, комірка «конфіденційність – передавання – технології» означає: чи використано шифрування каналу (TLS, VPN) для запобігання перехопленню даних? А комірка «доступність – зберігання – політики»: чи існують і чи виконуються політики резервного копіювання та відновлення?

3.5 Застосування моделі на практиці

Куб Маккамбера використовують як контрольний перелік (чек-лист) для перевірки повноти системи захисту: якщо для якоїсь комірки не передбачено жодних заходів, це «сліпа зона». Він допомагає уникнути типової помилки, коли організація купує дороге обладнання (технології), але нехтує політиками та навчанням персоналу. Приклади «комірок» куба Маккамбера подано в таблиці 3.2.

Таблиця 3.2 – Приклади «комірок» куба Маккамбера

Комірка моделі	**Загроза**	**Приклад заходу**
Конфіденційність – зберігання – технології	Викрадення ноутбука або диска	Повне шифрування диска (BitLocker, LUKS)
Конфіденційність – передавання – технології	Перехоплення трафіку в публічній Wi-Fi	VPN, TLS 1.3

Продовження таблиці 3.2

Комірка моделі	Загроза	Приклад заходу
Цілісність – обробка – технології	Підміна даних шкідливим ПЗ	Контроль цілісності, підписування коду, EDR
Цілісність – зберігання – політики	Несанкціоновані зміни в базах даних	Політика розмежування прав, журналювання змін
Доступність – передавання – технології	DDoS-атака на сервіс	Фільтрація трафіку, CDN, резервні канали
Доступність – зберігання – політики	Втрата даних через шифрувальник-вимагач	Правило резервного копіювання 3-2-1, регулярні перевірки відновлення
Конфіденційність – обробка – освіта	Фішинг, що виманює облікові дані	Навчання, імітаційні фішингові кампанії
Цілісність – передавання – освіта	Підроблене розпорядження про платіж (BEC)	Навчання перевірці запитів на платежі за другим каналом

Приклад. Аналіз інциденту за моделлю. Працівник бухгалтерії отримав лист нібито від директора з проханням терміново переказати кошти на новий рахунок. Через модель Маккамбера видно, що атакована цілісність інформації про платіж у стані передавання, а слабкою ланкою стали люди та політики: бракувало правила двофакторного підтвердження платежів та навчання. Додавання лише технічних засобів (спам-фільтра) проблему не вирішило б – потрібна комбінація заходів із кількох вимірів.

Життєвий цикл інформації та керування активами

Інформація проходить життєвий цикл: створення або збирання, класифікація, зберігання, використання, передавання, архівування та знищення. На кожному етапі змінюються стан інформації й відповідні ризики. Наприклад, на етапі знищення основною загрозою стає відновлення даних зі «видалених» носіїв, тому застосовують гарантоване стирання або фізичне знищення носіїв згідно зі стандартами (наприклад, NIST SP 800-88).

Практичне керування активами складається з кількох кроків: (1) виявлення та інвентаризація активів; (2) призначення власника кожного активу, який відповідає за його захист; (3) класифікація та маркування; (4) визначення правил поводження для кожного рівня класифікації (хто може читати, копіювати, пересилати, зберігати в хмарі); (5) регулярний перегляд реєстру. Без актуального реєстру неможливо захистити те, про що організація не знає, – так з’являється «тіньове IT» (shadow IT),

коли співробітники самостійно користуються неузгодженими сервісами. Ризики та заходи на етапах життєвого циклу інформації подано в таблиці 3.3.

Таблиця 3.3 – Ризики та заходи на етапах життєвого циклу інформації

Етап життєвого циклу	Типові ризики	Заходи
Створення / збирання	Збирання зайвих даних, відсутність підстав обробки	Принцип мінімізації даних, інформування суб'єктів
Зберігання	Витік, втрата носія, програма-вимагач	Шифрування, контроль доступу, резервні копії
Використання	Інсайдерські зловживання, помилки користувачів	Принцип найменших привілеїв, журналювання
Передавання	Перехоплення, підміна, неправильний адресат	TLS, VPN, електронний підпис, DLP
Архівування	Втрата читабельності, несанкціонований доступ до архіву	Контроль цілісності, політики зберігання
Знищення	Відновлення даних із носіїв	Гарантоване стирання, акти знищення

Приклад. Куб Маккамбера для хмарного сервісу. Українська компанія переносить облік клієнтів до SaaS-сервісу. Команда проходить 27 комірок: зберігання – де фізично розміщені дані, чи шифруються вони на стороні провайдера, хто володіє ключами; передавання – чи використовується TLS, чи обмежено доступ до API за IP-адресами; обробка – як розмежовано права адміністраторів провайдера; у вимірі політик – чи є угода про рівень сервісу (SLA) й договір обробки даних; у вимірі людей – чи пройшли навчання адміністратори облікових записів. Виявлено «порожню» комірку: відсутність політики регулярної перевірки журналів доступу, її додано до регламенту.

3.6 Модель Маккамбера, тріада CIA та сучасні підходи

Куб Маккамбера розширює тріаду CIA двома додатковими вимірами й тим самим перетворює перелік цілей на структуру для проєктування захисту. Водночас його варто розглядати як концептуальну модель, а не метод кількісної оцінки ризиків: він не вказує, який захід кращий і скільки ресурсів виділяти. Тому на практиці його поєднують із процесним підходом ISO/IEC 27001, аналізом ризиків та фреймворками на кшталт NIST CSF 2.0.

Сучасні обговорення пропонують розширювати перелік властивостей: автентичність, підзвітність (неспростовність), надійність. Іноді застосовують гексаду Паркера, що додає до CIA володіння (possession), автентичність і корисність (utility). Принцип залишається тим самим: кібербезпека – це сукупність цілей, станів інформації та засобів їх досягнення, які потрібно розглядати разом.

Висновки

Інформаційні ресурси – актив, цінність якого визначає необхідний рівень захисту. Класифікація інформації та інвентаризація активів – відправна точка управління безпекою. Куб Маккамбера описує безпеку у трьох вимірах (властивості, стани, заходи) і дає 27 комірок, що слугують чек-листом повноти захисту. Модель наочна й проста, її доцільно поєднувати зі стандартами та методами оцінки ризиків.

Контрольні питання

1. Що таке інформаційний ресурс? Чим відрізняються первинні та допоміжні активи?

2. Які рівні класифікації інформації за критичністю ви знаєте? Наведіть приклади.

3. Хто й коли запропонував куб кібербезпеки? Які три виміри він має?

4. Чому стан інформації (зберігання, передавання, обробка) впливає на вибір заходів захисту?

5. Скільки комірок містить куб Маккамбера? Поясніть зміст двох довільних комірок.

6. Проаналізуйте за допомогою моделі інцидент із фішинговим листом: які комірки порушено і які заходи слід застосувати?

7. Які обмеження має модель Маккамбера і чим її доцільно доповнювати?

Література: [1], [2], [3].

ТЕМА 4. КІБЕРНАПАДНИКИ ТА КІБЕРВІЙНА: ТИПИ, МОТИВИ Й ЦІЛІ

План лекції

1. Поняття кібернападника та їх загальна класифікація
2. Типи кібернападників
3. Мотиви та цілі
4. Кібервійна: поняття, ознаки й правові аспекти
5. Історія та уроки найвідоміших кібероперацій
6. Російсько-українська кібервійна
7. Захист від різних типів нападників

4.1 Поняття кібернападника та їх загальна класифікація

Кібернападник (threat actor) – особа або група осіб, що навмисно здійснює чи готує дії, спрямовані на порушення конфіденційності, цілісності чи доступності інформаційних систем та даних. Розуміння того, хто атакує, навіщо і з якими ресурсами, є основою моделювання загроз: захист від школяра-початківця і від державної розвідувальної служби вимагає принципово різних заходів.

Нападників класифікують за кількома ознаками: належністю (зовнішні та внутрішні), рівнем кваліфікації й ресурсів (від використання готових інструментів до розроблення власних експлойтів), організованістю (одинаки, групи, структури, що фінансуються державою), мотивацією (гроші, ідеологія, шпигунство, помста) та цілями (дані, гроші, репутація, руйнування інфраструктури).

4.2 Типи кібернападників

Основні типи кібернападників подано в таблиці 4.1.

Таблиця 4.1 – Основні типи кібернападників

Тип	Характеристика	Типові дії
Скрипт-кідді (script kiddies)	Початківці, що використовують чужі інструменти без глибокого розуміння	Масове сканування, DDoS-сервіси, проста зміна вмісту сайтів

Продовження таблиці 4.1.

Тип	Характеристика	Типові дії
Кіберзлочинці	Організовані групи, що діють заради прибутку; працюють за моделлю «злочинності як послуги» (CaaS)	Програми-вимагачі, шахрайство, викрадення платіжних даних, ботнети
Хактивісти	Ідеологічно вмотивовані; прагнуть привернути увагу до політичних чи соціальних питань	DDoS, дефейс сайтів, оприлюднення викрадених даних (hack-and-leak)
Державні (APT) групи	Добре фінансовані, мають кваліфікованих фахівців і тривалий горизонт планування	Кібершпигунство, прихований тривалий доступ, диверсії, інформаційні операції
Інсайдери	Працівники, підрядники, партнери з легітимним доступом; бувають зловмисні та необережні	Витік даних, саботаж, продаж доступу, помилки конфігурації
Брокери доступу (IAB)	Продають вже отриманий доступ до мереж іншим групам	Викрадення облікових даних, продаж доступу на форумах
Наймані групи (cyber mercenaries)	Виконують атаки на замовлення, у тому числі для держав; продають шпигунські інструменти	Цілеспрямована розвідка, злом облікових записів окремих осіб

Термін APT (Advanced Persistent Threat, «розвинена стійка загроза») позначає операцію, у якій нападник дістається мережі, довго залишається непоміченим і досягає стратегічних цілей. Для таких груп використовують ідентифікатори, що присвоюють дослідники й уряди: наприклад, MITRE ATT&CK веде каталог груп з описами їх інструментарію та тактик; CERT-UA позначає групи як UAC-XXXX, а Mandiant – APT/UNC.

Приклад. Модель «злочинність як послуга». Група-розробник шифрувальника здає програму в оренду «партнерам» (affiliates): партнери проникають у мережі та розгортають вимагач, а розробники забирають 20–30 % викупу, надають панель керування, переговорників і майданчик для оприлюднення даних. Окремі брокери доступу продають вже скомпрометовані VPN-облікові записи. Так організована злочинна діяльність набуває виробничого характеру з розподілом ролей, а поріг входу для виконавців знижується.

4.3 Мотиви та цілі

Мотиви нападників зручно описувати за допомогою моделей. Класичний мнемонічний перелік MICE охоплює Money (гроші), Ideology (ідеологію),

Compromise/Coercion (компрометацію або примус), Ego (его, прагнення визнання); його часто застосовують для аналізу інсайдерів. До цього додають шпигунство (політичне, економічне, військове) та помсту. Мотиви кібернападників подано в таблиці 4.2.

Таблиця 4.2 – Мотиви кібернападників

Мотив	Хто типово діє	Кінцева мета	Приклад
Фінансова вигода	Кіберзлочинці	Викуп, продаж даних, крадіжка коштів	Вимагач у лікарні, шахрайство BEC
Шпигунство	Державні групи, наймані групи	Секретна, комерційна й особиста інформація	Тривала присутність у мережі міністерства
Ідеологія/ політика	Хактивісти, державні групи	Вплив на суспільну думку, дискредитація	DDoS проти урядових сайтів, hack-and-leak
Деструкція/ диверсія	Державні групи	Руйнування систем, зупинка інфраструктури	Атаки на енергосистеми й оператора зв’язку
Помста/ незадоволення	Інсайдери	Збитки роботодавцю	Видалення даних звільненим адміністратором
Репутація/ самоствердження	Скрипт-кідді, окремі хакери	Визнання в спільноті	Дефейс сайту

Цілі нападників залежать від мотивів і охоплюють: гроші й цифрові активи (облікові записи, криптовалюту); персональні та комерційні дані; інтелектуальну власність; критичну інфраструктуру (енергетика, зв’язок, транспорт, охорона здоров’я); репутацію організації; інформаційний простір (дезінформація, маніпуляція). Для державних груп важливою ціллю є й ланцюг постачання – компрометація постачальника програмного забезпечення дозволяє дістатися тисячам клієнтів одночасно.

4.4 Кібервійна: поняття, ознаки й правові аспекти

Кібервійна – використання кібероперацій державами або від їхнього імені для досягнення політичних і військових цілей, зокрема у складі збройного конфлікту. Єдиного загальноприйнятого визначення не існує, а більшість кіберінцидентів між державами залишаються нижче порогу збройного нападу, тому дослідники

говорять про «сіру зону» між миром і війною та про гібридну війну, що поєднує кібероперації, дезінформацію, економічний тиск і військову силу.

Ключовим експертним документом є Таллінський посібник 2.0 (Tallinn Manual 2.0, 2017), підготовлений міжнародною групою експертів за ініціативи Центру передового досвіду НАТО з кібероборони (CCDCOE). Він підтверджує, що міжнародне право, зокрема суверенітет, заборона застосування сили та міжнародне гуманітарне право, поширюється й на кіберпростір. Відповідно, кібероперація може становити застосування сили чи збройний напад, якщо її масштаби й наслідки подібні до кінетичних, а напад на цивільні об'єкти й критичну інфраструктуру обмежений нормами гуманітарного права.

Ознаки кібервійни: державна підтримка або керівництво; політичні чи військові цілі; значні масштаби й наслідки (руйнування, відключення інфраструктури); поєднання з традиційними бойовими діями; використання складних спеціалізованих засобів. Складність полягає в атрибуції: встановити, хто саме стоїть за атакою, технічно і юридично важко, оскільки нападники використовують посередників, чужу інфраструктуру й хибні сліди.

4.5 Історія та уроки найвідоміших кібероперацій

Показові кібероперації подано в таблиці 4.3.

Таблиця 4.3 – Показові кібероперації

Рік	Подія	Суть та наслідки
2007	Атаки на Естонію	Тривалі DDoS-атаки на державні, банківські й медійні ресурси після суперечки навколо пам'ятника; привернули увагу НАТО до кіберзахисту, у Таллінні створено CCDCOE
2010	Stuxnet	Складний хробак вразив центрифуги збагачення урану в Ірані; перший відомий приклад кіберзброї, що спричинила фізичне руйнування
2015–2016	Атаки на енергосистему України	Відключення електропостачання кількох областей (грудень 2015) за допомогою BlackEnergy та віддаленого керування; у 2016 – шкідливе ПЗ Industroyer. Група Sandworm
2017	NotPetya	Руйнівний вайпер, замаскований під вимагач, поширений через оновлення бухгалтерського ПЗ M.E.Doc; зачепив сотні компаній у світі, збитки – мільярди доларів

Продовженння таблиці 4.3

Рік	Подія	Суть та наслідки
2020	SolarWinds	Компрометація оновлень платформи Orion; прихований доступ до мереж тисяч організацій, у тому числі державних органів США
2022	Атака на Viasat (KA-SAT)	У день початку повномасштабного вторгнення виведено з ладу тисячі супутникових модемів в Україні та Європі

4.6 Російсько-українська кібервійна

Україна є одним із найбільш інтенсивних полів кіберконфлікту: ще з 2014 року країна зазнавала атак на виборчу інфраструктуру, енергетику, державні реєстри, медіа. З лютого 2022 року кібероперації стали складовою повномасштабної війни. За оцінками CERT-UA та Держспецзв'язку, кількість зафіксованих кіберінцидентів у країні зросла в рази порівняно з довоєнним періодом; значна частка атак спрямована на державний сектор, енергетику й сектор безпеки й оборони. Атаки включають вайпери (WhisperGate, HermeticWiper, CaddyWiper), фішинг і шпигунське ПЗ, атаки на постачальників послуг, DDoS та інформаційні операції.

Показовим став інцидент 12 грудня 2023 року – масштабна атака на найбільшого мобільного оператора «Київстар», що залишила без зв'язку і мобільного інтернету близько 24 мільйонів абонентів та вплинула на роботу систем безпеки (зокрема повітряної тривоги в окремих регіонах). За даними СБУ та заявою оператора, зловмисники тривалий час перебували в системі, а відновлення тривало кілька днів; відповідальність за атаку приписують структурі, пов'язаній з російською групою Sandworm (військова розвідка ГРУ). Інцидент ілюструє як деструктивну мету, так і важливість стійкості критичної інфраструктури та сегментації мереж.

Паралельно в Україні сформувалися кібероборонні спроможності: Сили кібербезпеки СБУ, Командування сил зв'язку та кібербезпеки ЗСУ, CERT-UA, а також волонтерська «ІТ-армія України», яка проводила DDoS-акції та кібероперації проти російських об'єктів. Співпраця з міжнародними партнерами і приватними

компаніями (Microsoft, Google, ESET та ін.) дозволила швидко виявляти кампанії та поширювати індикатори компрометації.

Приклад. Аналіз за ознаками. Інцидент: вайпер, замаскований під програму-вимагач, розгорнутий одночасно на сотнях комп'ютерів державної установи напередодні військових дій. Ознаки кібервійни: деструктивна мета (немає вимоги викупу), синхронізація з військовими подіями, складні інструменти, ймовірна державна підтримка. Мотив – підрив управління й дестабілізація. Кваліфікація за правом: питання, чи досягнуто порогу застосування сили, залежить від масштабів наслідків; атрибуція виконується спільно технічними (аналіз шкідливого ПЗ, інфраструктури) і розвідувальними даними.

4.7 Захист від різних типів нападників

Підхід до захисту визначається моделлю загроз. Для масових кіберзлочинців достатньо базової гігієни: оновлення, багатофакторна автентифікація, резервні копії, навчання від фішингу. Для цілеспрямованих атак потрібні сегментація мереж, моніторинг, реагування на інциденти та аналіз кіберрозвідувальних даних (CTI). Для державних груп важливі також безпека ланцюга постачання, перевірка постачальників, зменшення площини атаки, а для критичної інфраструктури – відокремлення технологічних мереж (OT) від офісних і плани безперервності. Від інсайдерів захищають принцип найменших привілеїв, розподіл обов'язків, моніторинг поведінки та культура безпеки.

Висновки

Кібернападники відрізняються рівнем ресурсів, організованістю та мотивами – від наживи й ідеології до шпигунства та деструкції. Кібервійна є частиною гібридного конфлікту; міжнародне право застосовується до кіберпростору, але атрибуція залишається складною. Досвід Естонії, Stuxnet, NotPetya та атак на Україну демонструє, що кібератаки здатні завдавати фізичної та економічної шкоди, а тому адекватний захист починається з моделювання загроз.

Контрольні питання

1. Хто такий кібернападник? За якими ознаками їх класифікують?

2. Охарактеризуйте основні типи нападників та їхні типові дії.

3. Що означає термін APT? Чим такі групи відрізняються від кіберзлочинців?

4. Поясніть модель MICE. Які мотиви характерні для інсайдерів?

5. Що таке кібервійна? Чому атрибуція є складною проблемою?

6. Яку роль відіграє Таллінський посібник у регулюванні кібервійни?

7. Порівняйте інциденти Stuxnet, NotPetya і атаку на «Київстар»: мета, засоби, наслідки.

8. Як змінюються заходи захисту залежно від типу нападника?

Література: [5], [7], [8], [17], [18].

ТЕМА 5. КІБЕРАТАКИ: КЛАСИФІКАЦІЯ, КОНЦЕПЦІЇ ТА ЕТАПИ РЕАЛІЗАЦІЇ

План лекції

1. Основні поняття: загроза, вразливість, атака, інцидент
2. Класифікація кібератак
3. Основні види кібератак
4. Етапи реалізації кібератаки: Cyber Kill Chain
5. Матриця MITRE ATT&CK
6. Приклад наскрізного сценарію атаки
7. Концепції протидії: глибокий захист та Zero Trust

5.1 Основні поняття: загроза, вразливість, атака, інцидент

Загроза – потенційна причина небажаного інциденту, що може завдати шкоди системі чи організації. Вразливість – слабкість активу чи заходу захисту, яку може використати загроза. Кібератака – навмисна дія, спрямована на порушення конфіденційності, цілісності чи доступності інформації або систем шляхом використання вразливостей. Інцидент – подія, що фактично порушила чи загрожує порушити безпеку. Ризик – поєднання ймовірності й наслідків реалізації загрози.

Поверхня атаки (attack surface) – сукупність усіх точок, через які нападник може вплинути на систему: відкриті порти й сервіси, веб-застосунки, облікові записи, електронна пошта, пристрої користувачів, хмарні конфігурації, постачальники. Зменшення поверхні атаки – один із найефективніших засобів захисту. Вектор атаки – шлях, яким нападник досягає цілі (фішинговий лист, скомпрометований VPN-обліковий запис, вразливе ПЗ).

5.2 Класифікація кібератак

Атаки класифікують за різними ознаками, що допомагає обирати заходи захисту (таблиця 5.1).

Таблиця 5.1 – Ознаки класифікації кібератак

Ознака	Види	Пояснення
За впливом на властивості безпеки	Порушення конфіденційності, цілісності, доступності	Перехоплення й витік; підміна даних; DDoS та вимагачі
За характером впливу	Пасивні та активні	Пасивні – спостереження, перехоплення без змін; активні – змінюють дані чи працездатність системи
За розташуванням нападника	Зовнішні та внутрішні	Внутрішні здійснюють користувачі з легітимним доступом
За метою	Масові та цілеспрямовані	Масові – широка розсилка; цілеспрямовані – проти конкретної організації (у т. ч. APT)
За рівнем стека	Фізичні, мережеві, на рівні ОС, застосунків, людей	Напр.: підключення пристрою, MITM, експлуатація ПЗ, SQL-ін’єкція, фішинг
За ступенем автоматизації	Автоматизовані й ручні	Боти сканують Інтернет; операторський «hands-on-keyboard» вторгнення

5.3 Основні види кібератак

Шкідливе програмне забезпечення

Malware об’єднує віруси, хробаків, трояни, шпигунське ПЗ, руткіти, ботів, програми-вимагачі (ransomware) та вайпери. Сучасні вимагачі застосовують подвійне здирництво: шифрують дані та загрожують оприлюднити викрадену копію. За даними звіту Verizon DBIR 2025, вимагачі були присутні у 44 % порушень проти 32 % роком раніше.

Соціальна інженерія та фішинг

Методи психологічного впливу, що змушують людину розкрити облікові дані чи виконати небезпечну дію: фішинг (масові листи), spear-phishing (цілеспрямований), вішинг (телефон), смішинг (SMS), BEC (шахрайство з підміною листування керівника чи постачальника). Людський фактор присутній у переважній більшості порушень, а штучний інтелект дозволяє генерувати переконливі листи, голос і відео (діпфейки).

Атаки на доступність

DoS/DDoS – перевантаження сервісу запитами з багатьох пристроїв (ботнетів). Розрізняють об’ємні (UDP/ICMP flood), протокольні (SYN flood) та

атаки на рівні застосунку (HTTP flood). Захист: фільтрація та розподіл трафіку (CDN, scrubbing-центри), обмеження швидкості запитів, горизонтальне масштабування.

Атаки на мережу та канали зв’язку

MITM («людина посередині»), ARP/DNS spoofing, перехоплення сеансів, атаки на Wi-Fi (rogue AP, evil twin), підміна маршрутів. Захист: шифрування (TLS, VPN), автентифікація вузлів, DNSSEC, моніторинг.

Атаки на веб-застосунки та облікові дані

SQL-ін’єкції, міжсайтовий скриптинг (XSS), підробка запитів (CSRF), порушення контролю доступу – типові пункти переліку OWASP Top 10. Атаки на облікові дані: brute force, credential stuffing (використання витоків паролів), password spraying, викрадення токенів сеансів. Захист: валідація вхідних даних, параметризовані запити, MFA, обмеження спроб входу.

Атаки на ланцюг постачання

Нападник компрометує постачальника ПЗ, бібліотеку чи сервіс, щоб дістатися багатьох клієнтів одночасно (SolarWinds, NotPetya через M.E.Doc, зловмисні пакети в репозиторіях npm та PyPI). Звіти ENISA та Verizon відзначають зростання частки порушень через третіх осіб.

Приклад. Credential stuffing. Нападник купує на форумі базу з мільйонів пар «логін – пароль» з витоку одного сервісу й автоматично перевіряє їх на інших сайтах (банківських, поштових, корпоративних порталах). Оскільки багато людей повторно використовують паролі, частина облікових записів скомпрометована без жодної вразливості в самому сервісі. Заходи: унікальні паролі та менеджер паролів, MFA, виявлення аномальної кількості входів, перевірка паролів за базами витоків.

5.4 Етапи реалізації кібератаки: Cyber Kill Chain

Модель Cyber Kill Chain розробили фахівці компанії Lockheed Martin (Hutchins, Cloppert, Amin, 2011) за аналогією з військовим «ланцюгом ураження цілі». Вона розглядає атаку як послідовність семи етапів (рис. 5.1); перерваний на будь-якому етапі ланцюг означає, що атака не досягла мети.



Рисунок 5.1 – Етапи моделі Cyber Kill Chain

Етапи Cyber Kill Chain, приклади та контрзаходи подано в таблиці 5.2.

Таблиця 5.2 – Етапи Cyber Kill Chain, приклади та контрзаходи

Етап	**Що робить нападник**	**Приклад**	**Захист**
1. Розвідка	Збирає інформацію про ціль: домени, працівників, технології, відкриті сервіси	OSINT, соцмережі, сканування портів	Мінімізація публічної інформації, моніторинг сканувань
2. Озброєння	Створює шкідливий вміст і поєднує його з експлойтом	Документ Office із макросом, троян	Аналіз загроз (CTI), пісочниці
3. Доставка	Передає вміст жертві	Фішинговий лист, USB, скомпрометований сайт	Фільтрація пошти, навчання персоналу
4. Експлуатація	Використовує вразливість чи довіру користувача	Запуск вкладення, експлойт вразливості	Патч-менеджмент, обмеження виконання коду
5. Встановлення	Закріплюється в системі	Бекдор, завдання планувальника, запис у реєстрі	EDR, контроль списку дозволених програм
6. Керування (C2)	Встановлює канал для віддаленого керування	HTTPS-з'єднання з сервером керування, DNS-тунелювання	Фільтрація вихідного трафіку, DNS-захист
7. Дії для досягнення мети	Викрадає дані, шифрує, руйнує, рухається мережею	Ексфільтрація, вимагач, вайпер	Сегментація, DLP, резервні копії, виявлення аномалій

Модель Kill Chain добре описує зовнішні вторгнення, проте менше підходить для інсайдерів і атак без шкідливого ПЗ (living-off-the-land), коли нападник

використовує легітимні інструменти системи. Тому її доповнюють моделями Unified Kill Chain і матрицею MITRE ATT&CK.

5.5 Матриця MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – відкрита база знань про поведінку нападників, побудована на реальних спостереженнях. Тактики відповідають на запитання «навіщо» (мета на певному етапі), техніки – «як», підтехніки уточнюють спосіб, а процедури описують конкретну реалізацію групою. Матриця Enterprise містить 14 тактик: розвідка, розроблення ресурсів, первинний доступ, виконання, закріплення, підвищення привілеїв, ухилення від захисту, отримання облікових даних, дослідження, горизонтальне переміщення, збирання, керування й контроль, ексфільтрація, вплив. Окремі матриці охоплюють мобільні пристрої та промислові системи керування (ICS). Базу застосовують для емуляції атак, оцінки покриття засобів виявлення й обміну розвідданими. Приклади тактик і технік MITRE ATT&CK подано в таблиці 5.3.

Таблиця 5.3 – Приклади тактик і технік MITRE ATT&CK

Тактика ATT&CK	Приклади технік
Первинний доступ (Initial Access)	Фішингове вкладення, експлуатація публічного застосунку, дійсні облікові записи
Виконання (Execution)	PowerShell, скрипти, виконання користувачем
Закріплення (Persistence)	Заплановані завдання, ключі автозапуску, створення облікових записів
Отримання облікових даних (Credential Access)	Дамп LSASS, brute force, перехоплення вводу
Горизонтальне переміщення (Lateral Movement)	Віддалені служби (RDP, SMB), pass-the-hash
Ексфільтрація (Exfiltration)	Передавання через C2-канал, у хмарні сховища
Вплив (Impact)	Шифрування даних, знищення даних, відмова в обслуговуванні

5.6 Приклад наскрізного сценарію атаки

Приклад. Атака вимагача на виробничу компанію. Розвідка: нападники знаходять у соцмережах працівників бухгалтерії та структуру пошти. Озброєння й

доставка: розсилають лист із рахунком, що містить завантажувач. Експлуатація: працівник відкриває вкладення й вмикає макрос. Встановлення: на ПК розгортається троян, створюється завдання автозапуску. C2: з'єднання з сервером керування по HTTPS. Дії: викрадення облікових даних адміністратора, горизонтальне переміщення до сервера файлів, ексфільтрація сотень гігабайтів даних, а потім шифрування систем у вихідні. Де можна було зупинити: фільтрація пошти й відключення макросів (етапи 3–4), EDR (5), контроль вихідного трафіку (6), сегментація й MFA для адміністраторів, офлайн-копії (7).

5.7 Концепції протидії: глибокий захист та Zero Trust

Глибокий захист (defense in depth) – багаторівневий підхід, за якого ефективність захисту не залежить від одного засобу: периметр, мережа, вузол, застосунок, дані, люди й процеси. Якщо один рівень пробито, наступний зменшує шкоду. Це перегукується з моделлю Kill Chain: чим більше етапів перекрито незалежними засобами, тим нижча ймовірність успіху атаки.

Zero Trust (нульова довіра) виходить з припущення, що периметр уже порушено: жодному користувачу чи пристрою не довіряють лише через їхнє розташування в мережі. Основні принципи: явна перевірка кожного запиту (автентифікація, стан пристрою), мінімальні привілеї, мікросегментація та постійний моніторинг. Архітектуру описує NIST SP 800-207. Додатково застосовують принцип «assume breach» – планування діяльності з припущенням, що компрометація вже відбулася.

Висновки

Кібератака – це керований процес, що складається з послідовних етапів, а не одиничний технічний акт. Класифікація атак і знання основних видів (malware, соціальна інженерія, DDoS, атаки на веб-застосунки, облікові дані, ланцюг постачання) дають змогу вибирати доречні заходи. Моделі Cyber Kill Chain та MITRE ATT&CK надають спільну мову для опису поведінки нападників, пошуку прогалин у захисті й планування реагування, а принципи глибокого захисту й Zero Trust – архітектурну основу протидії.

Контрольні питання

1. Дайте визначення загрози, вразливості, атаки та інциденту. Як вони пов’язані між собою?

2. Що таке поверхня атаки та вектор атаки? Наведіть приклади.

3. За якими ознаками класифікують кібератаки? Наведіть приклади для кожної ознаки.

4. Що таке подвійне здирництво? Чим відрізняються phishing, spear-phishing, BEC?

5. Опишіть сім етапів Cyber Kill Chain і заходи протидії для кожного етапу.

6. У чому різниця між тактикою, технікою та процедурою в MITRE ATT&CK?

7. Поясніть ідею «глибокого захисту» й принципи Zero Trust.

8. Складіть сценарій атаки на університет за етапами Kill Chain та запропонуйте контрзаходи.

Література: [4], [5], [18].

ТЕМА 6. МЕТОДИ ПРОНИКНЕННЯ В ІНФОРМАЦІЙНІ СИСТЕМИ ТА ЕКСПЛУАТАЦІЯ ВРАЗЛИВОСТЕЙ

План лекції

1. Вразливість: поняття, причини та життєвий цикл
2. Системи ідентифікації та оцінювання вразливостей (CVE, CWE, CVSS)
3. Основні класи вразливостей
4. Методи проникнення в інформаційні системи
5. Експлуатація вразливостей та дії після проникнення
6. Тестування на проникнення та управління вразливостями
7. Принципи захисту

Матеріал має освітній характер: розглядаються принципи та класи методів проникнення з метою формування розуміння захисту. Перевірка захищеності реальних систем допустима лише за письмовою згодою власника та в межах узгодженого обсягу робіт.

6.1 Вразливість: поняття, причини та життєвий цикл

Вразливість – слабкість у програмному чи апаратному забезпеченні, конфігурації, процесах або діях людей, яку можна використати для порушення безпеки. Експлойт – код або методика, що використовує вразливість; payload (корисне навантаження) – дії, які виконуються після успішної експлуатації. Причини вразливостей: помилки проєктування й програмування, небезпечні налаштування за замовчуванням, відсутність оновлень, слабка автентифікація, надмірні права, помилки персоналу.

Життєвий цикл вразливості: введення помилки під час розроблення → виявлення (дослідником, вендором чи нападником) → оприлюднення й присвоєння ідентифікатора → випуск виправлення (патча) → встановлення виправлення користувачами.

Небезпечним є проміжок між оприлюдненням чи першою експлуатацією та встановленням патча. Вразливість нульового дня (zero-day) – така, про яку вендор ще не знає або для якої немає виправлення; нападник має перевагу, бо захисних сигнатур не існує. N-day – вразливість, відома й виправлена, але не усунена в конкретній організації: саме вони становлять основну масу успішних атак.

6.2 Системи ідентифікації та оцінювання вразливостей (CVE, CWE, CVSS)

Системи ідентифікації й оцінювання вразливостей подано в таблиці 6.1.

Таблиця 6.1 – Системи ідентифікації й оцінювання вразливостей

Система	Призначення	Приклад / особливості
CVE (Common Vulnerabilities and Exposures)	Унікальні ідентифікатори конкретних вразливостей	CVE-2021-44228 (Log4Shell)
CWE (Common Weakness Enumeration)	Каталог типів слабкостей у ПЗ та апаратурі	CWE-79 (XSS), CWE-89 (SQL-ін’єкція); щорічний перелік CWE Top 25
CVSS 4.0	Стандартизована оцінка критичності від 0 до 10	Групи метрик: Base, Threat, Environmental, Supplemental; рівні: None, Low, Medium, High, Critical
EPSS	Імовірність експлуатації вразливості найближчими 30 днями	Допомагає пріоритизувати патчі
CISA KEV	Каталог вразливостей, що реально експлуатуються	Містить терміни усунення для федеральних органів США; корисний орієнтир для всіх
NVD / БДУ ФСТЕК / бази вендорів	Бази даних вразливостей із описами, оцінками, посиланнями	Джерела для сканерів вразливостей

Оцінка CVSS показує технічну серйозність, але не завжди – реальний ризик для організації. Тому пріоритетність усунення визначають, ураховуючи: чи експлуатується вразливість у реальності (KEV, EPSS), чи доступна система ззовні, наскільки критичним є актив і які компенсуючі заходи вже діють.

6.3 Основні класи вразливостей

Основні класи вразливостей подано в таблиці 6.2.

Таблиця 6.2 – Основні класи вразливостей

Клас	Суть	Типові наслідки	Захист
Ін’єкції (SQL, команд ОС)	Недовірені дані потрапляють в інтерпретатор як частина команди	Читання/зміна БД, виконання команд	Параметризовані запити, валідація, найменші привілеї
Порушення контролю доступу	Користувач виконує дії, на які не має прав (IDOR, обхід перевірок)	Доступ до чужих даних, підвищення привілеїв	Перевірка прав на сервері, принцип «за замовчуванням заборонено»
Помилки роботи з пам’яттю	Переповнення буфера, використання після звільнення	Виконання довільного коду, збій	Безпечні мови (Rust, Go), ASLR/DEP, перевірки меж
Криптографічні помилки	Слабкі алгоритми, неправильне керування ключами	Витік даних, підробка	Сучасні алгоритми, перевірені бібліотеки, TLS 1.2+
Небезпечна конфігурація	Паролі за замовчуванням, відкриті сховища, зайві сервіси	Несанкціонований доступ, витоки	Базові конфігурації (CIS Benchmarks), аудит, IaC-перевірки
Вразливі та застарілі компоненти	Використання бібліотек зі відомими вразливостями	Експлуатація n-day вразливостей	SBOM, інвентаризація залежностей, автооновлення
Слабка автентифікація	Прості паролі, відсутність MFA, повторне використання	Захоплення облікових записів	MFA, менеджери паролів, FIDO2/passkeys
Помилки логіки та проєктування	Порушення бізнес-логіки, довіра до клієнта	Шахрайство, обхід обмежень	Моделювання загроз, огляд архітектури

Збірники OWASP Top 10 і CWE Top 25 щороку узагальнюють найпоширеніші класи слабкостей і використовуються як відправні точки для навчання розробників та тестувальників.

6.4 Методи проникнення в інформаційні системи

Проникнення починається з розвідки. Пасивна (OSINT) не взаємодіє з ціллю: пошук публічних даних про домени, співробітників, технології, витоки облікових

даних. Активна – це сканування мережі, виявлення відкритих портів, версій сервісів, перевірка веб-застосунків. Результатом є карта поверхні атаки.

Основні категорії методів первинного доступу (за даними DBIR 2025, найчастішими були зловживання обліковими даними, експлуатація вразливостей та фішинг, кожен – у межах 16–22 % порушень):

– використання облікових даних**:** підбір, повторне використання витоків, перехоплення токенів, обхід MFA через соціальну інженерію («втома від запитів»);

– експлуатація вразливостей зовнішніх сервісів: особливо пристроїв на периметрі (VPN-шлюзи, міжмережеві екрани, поштові сервери, веб-застосунки);

– соціальна інженерія: фішинг, телефонний обман, підкидання носіїв, інсценування службових запитів;

– зловживання довіреними зв’язками: компрометація постачальника, підрядника чи програмного пакета;

– помилки конфігурації: відкриті бази даних, публічні хмарні сховища, відкриті служби віддаленого доступу;

– фізичне проникнення: доступ до приміщень, підключення пристроїв до мережі, викрадення носіїв;

– атаки на бездротові мережі: слабке шифрування, підроблені точки доступу, зловмисні портали.

Приклад. Експлуатація вразливості периметрового пристрою. Виробник мережевого обладнання виявляє критичну вразливість у веб-інтерфейсі VPN-шлюзу, що дозволяє виконати команди без автентифікації. Протягом кількох днів після оприлюднення сканери в Інтернеті знаходять тисячі вразливих шлюзів, з’являються публічні експлойти, а вразливість потрапляє до каталогу CISA KEV. Організації, які оновили пристрої в перші дні, уникнули компрометації; ті, що відклали патч, виявили на шлюзі бекдор. Урок: для зовнішніх сервісів терміни усунення критичних вразливостей мають вимірюватися днями, а не тижнями.

6.5 Експлуатація вразливостей та дії після проникнення

Після первинного доступу нападник, як правило, прагне: закріпитися (створити додатковий доступ, що переживе перезавантаження); підвищити привілеї (від звичайного користувача до адміністратора); отримати облікові дані інших користувачів; дослідити середовище та рухатися мережею горизонтально до цінних систем; приховати сліди (видалення журналів, використання легітимних засобів – підхід living-off-the-land); зрештою досягти мети – ексфільтрації, шифрування чи руйнування. Саме на цих етапах ефективні сегментація, моніторинг та реагування: час між проникненням і виявленням (dwell time) визначає масштаб шкоди. Дії після проникнення та контрзаходи подано в таблиці 6.3.

Таблиця 6.3 – Дії після проникнення та контрзаходи

Дія нападника	Що спостерігається	Контрзахід
Підвищення привілеїв	Нетипові запуски адміністративних інструментів, зміни прав	Принцип найменших привілеїв, PAM, моніторинг подій безпеки
Отримання облікових даних	Звернення до сховищ облікових даних ОС, масові невдалі входи	Захист пам’яті процесів, MFA, розподіл адміністративних рівнів
Горизонтальне переміщення	Віддалені підключення між робочими станціями, використання RDP/SMB	Сегментація мережі, блокування зайвих протоколів, EDR
Ексфільтрація	Незвично великий вихідний трафік, з’єднання з невідомими хостами	DLP, фільтрація вихідного трафіку, оповіщення про аномалії

6.6 Тестування на проникнення та управління вразливостями

Тестування на проникнення (penetration testing) – санкціонована імітація атаки для виявлення вразливостей і оцінювання ефективності захисту. Відрізняється від сканування вразливостей (автоматизованого виявлення відомих слабкостей) тим, що включає ручний аналіз, ланцюжки експлуатації й оцінку реального впливу. Види тестування: «чорна», «сіра» та «біла» скриньки (залежно від обсягу відомої інформації), зовнішнє й внутрішнє, веб-застосунків, бездротових мереж, соціальної інженерії, фізичне. Методології: NIST SP 800-115, PTES, OWASP Web Security Testing Guide, OSSTMM.

Типовий процес: (1) узгодження обсягу й правил проведення робіт (Rules of Engagement) та письмовий дозвіл; (2) розвідка; (3) пошук вразливостей; (4) контрольована експлуатація; (5) аналіз та підтвердження впливу; (6) звіт із ризиками та рекомендаціями; (7) повторна перевірка після усунення. Окремий формат – Red Team (імітація цілеспрямованого супротивника з перевіркою виявлення й реагування), що виконується разом із захисниками (Blue Team), а їх спільна робота зветься Purple Team. Програми bug bounty дозволяють залучати незалежних дослідників, які повідомляють про вразливості за винагороду за відповідальним розкриттям (coordinated disclosure).

Управління вразливостями – безперервний цикл: інвентаризація активів → сканування → оцінювання та пріоритизація → усунення (патч, зміна конфігурації, компенсуючий захід) → перевірка → звітність. Показники: середній час усунення (MTTR), частка своєчасно усунених критичних вразливостей, охоплення сканування. Якщо патч неможливо встановити відразу, застосовують віртуальні патчі (правила WAF/IPS), відключення вразливої функції, сегментацію.

Приклад. Пріоритизація вразливостей. Сканер знайшов 3 500 вразливостей. Керувати такою кількістю неможливо одночасно, тому спочатку усувають ті, що (1) присутні в KEV або мають високий EPSS; (2) стосуються доступних з Інтернету систем; (3) належать до критичних активів. Результат: 120 вразливостей виправляють протягом 72 годин, ще кілька сотень – за плановими вікнами, решта потрапляє до реєстру прийнятих ризиків із компенсуючими заходами.

6.7 Принципи захисту

– скорочувати поверхню атаки: вимикати зайві сервіси, закривати порти, видаляти невикористовувані облікові записи;

– підтримувати інвентаризацію активів та SBOM;

– своєчасно оновлювати ПЗ, насамперед на периметрі;

– застосовувати MFA (бажано стійку до фішингу – FIDO2/passkeys) та принцип найменших привілеїв;

– впроваджувати безпечну розробку (SSDLC): моделювання загроз, огляд коду, статичний і динамічний аналіз, перевірка залежностей;

– сегментувати мережу й моніторити події (SIEM/EDR), готувати плани реагування на інциденти;

– регулярно проводити пентести й навчання персоналу.

Висновки

Проникнення в інформаційні системи здебільшого відбувається не через екзотичні нульові дні, а через відомі вразливості, слабкі облікові дані, помилки конфігурації та соціальну інженерію. Знання класів вразливостей, систем їх оцінювання (CVE, CWE, CVSS, KEV, EPSS) і етапів дій нападника дозволяє будувати ефективні процеси управління вразливостями, правильно пріоритизувати усунення та перевіряти захист легітимними тестами на проникнення.

Контрольні питання

1. Чим відрізняються вразливість, експлойт і payload? Що таке zero-day та n-day?

2. Для чого призначені CVE, CWE, CVSS, EPSS і CISA KEV?

3. Чому оцінки CVSS недостатньо для пріоритизації усунення вразливостей?

4. Назвіть основні класи вразливостей і способи захисту від них.

5. Які методи первинного доступу найчастіше використовують нападники?

6. Опишіть дії нападника після проникнення та відповідні заходи виявлення.

7. У чому різниця між скануванням вразливостей і тестуванням на проникнення? Що таке Red, Blue, Purple Team?

8. Які елементи має містити письмова угода (Rules of Engagement) на пентест?

9. Складіть план пріоритизації для сканування, що виявило 2 000 вразливостей.

Література: [4], [18], [19], [20], [21], [22].

ТЕМА 7. ЗАХИСТ КІНЦЕВИХ ПРИСТРОЇВ І МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

План лекції

1. Кінцеві пристрої як ціль атак
2. Захист кінцевих пристроїв
3. Мобільні пристрої та політика BYOD
4. Архітектура захищеної мережі
5. Засоби мережевого захисту
6. Безпека бездротових мереж, DNS та віддаленого доступу
7. Моніторинг та практичний чек-лист

7.1 Кінцеві пристрої як ціль атак

Кінцевий пристрій (endpoint) – комп'ютер, ноутбук, смартфон, планшет, сервер, а також IoT-пристрій, що підключається до мережі та обробляє дані. Саме кінцеві пристрої перебувають найближче до користувача, тому вони є основною точкою проникнення: фішингове вкладення відкривається на робочій станції, зламаний пароль використовується з ноутбука, а загублений смартфон містить корпоративну пошту. Кількість і різноманітність пристроїв зростає (віддалена робота, власні пристрої, «розумні» речі), а отже зростає й поверхня атаки.

Мережева інфраструктура – комутатори, маршрутизатори, міжмережеві екрани, точки доступу, VPN-шлюзи, DNS- та DHCP-сервери, а також хмарні та віртуальні мережі. Її компрометація дає нападникові контроль над трафіком усіх підключених пристроїв. Тому захист будують на двох рівнях одночасно: на самому пристрої та у мережі, відповідно до принципу глибокого захисту.

7.2 Захист кінцевих пристроїв

Основні заходи захисту кінцевих пристроїв подано в таблиці 7.1.

Таблиця 7.1 – Основні заходи захисту кінцевих пристроїв

Захід	Суть	Що запобігає
Своєчасне оновлення	Автоматичне встановлення патчів ОС, браузерів і застосунків	Експлуатація відомих вразливостей
Антивірус / EDR	Виявлення шкідливого коду та підозрілої поведінки, ізоляція вузла, збір телеметрії	Шкідливе ПЗ, вимагачі, безфайлові атаки
Шифрування диска	BitLocker, FileVault, LUKS; ключі з TPM	Витік даних при втраті чи крадіжці пристрою
Принцип найменших привілеїв	Робота під звичайним обліковим записом; адміністративні права тільки за потреби	Підвищення привілеїв, поширення шкідливого ПЗ
Багатофакторна автентифікація	Пароль + додатковий чинник (застосунок, ключ FIDO2)	Захоплення облікових записів
Локальний міжмережевий екран	Фільтрація вхідних і вихідних з’єднань на вузлі	Несанкціоновані підключення
Контроль запуску програм	Списки дозволених програм (allowlisting), блокування макросів із Інтернету	Запуск небажаного коду
Захищене завантаження	Secure Boot, UEFI, захист мікропрограм	Руткіти, bootkit
Резервне копіювання	Правило 3-2-1, офлайн-копії, перевірка відновлення	Втрата даних через вимагач чи збій

Hardening (зміцнення конфігурації) – зменшення поверхні атаки шляхом вимкнення зайвих служб, видалення невикористовуваних програм і облікових записів, зміни паролів за замовчуванням, застосування безпечних налаштувань. Орієнтиром є CIS Benchmarks та Microsoft Security Baselines; їх застосування автоматизують через групові політики, засоби керування конфігурацією (Ansible, Intune) та перевіряють сканерами відповідності.

EDR (Endpoint Detection and Response) – клас рішень, що безперервно збирають події на вузлі (процеси, мережеві з’єднання, зміни реєстру, файлові операції), аналізують їх поведінково, дозволяють аналітику швидко дослідити інцидент і дистанційно ізолювати пристрій. На відміну від класичного антивіруса на основі сигнатур, EDR виявляє й невідомі загрози за поведінковими ознаками. Розширенням є XDR, що корелює дані з пошти, мережі, хмари та ідентифікаційних систем.

Приклад. Ланцюжок, перерваний на кінцевому пристрої. Працівник відкриває документ із макросом. Політика блокує макроси з Інтернету – запуск не

відбувається. Якби макрос запустився, EDR помітив би нетиповий ланцюжок «Word → PowerShell → з'єднання із зовнішнім хостом», завершив би процес і ізолював вузол. А завдяки політиці найменших привілеїв шкідливий код не зміг би змінити системні налаштування, а завдяки резервним копіям втрата даних була б мінімальною. Кожен захід перекриває різні етапи атаки.

7.3 Мобільні пристрої та політика BYOD

Смартфони й планшети зберігають пошту, документи, токени MFA та доступ до хмарних сервісів. Типові загрози: втрата чи крадіжка, шкідливі застосунки з неофіційних джерел, небезпечні Wi-Fi, застарілі ОС, фішинг через SMS та месенджери. Заходи: блокування екрана та біометрія, шифрування (увімкнено за замовчуванням у сучасних ОС), оновлення, встановлення застосунків тільки з офіційних магазинів, MDM/UEM (системи керування мобільними пристроями) із можливістю віддаленого стирання, розділення особистого й робочого профілів.

BYOD (Bring Your Own Device) – використання працівниками власних пристроїв для роботи. Це знижує витрати, але ускладнює контроль. Політика BYOD визначає допустимі пристрої та версії ОС, обов'язкові заходи захисту (шифрування, PIN, MFA), порядок реєстрації в MDM, межі моніторингу, правила на випадок втрати та звільнення працівника, а також поділ даних на корпоративні й особисті контейнери.

7.4 Архітектура захищеної мережі

Ключовий принцип – сегментація: поділ мережі на ізольовані зони за рівнем довіри та функціями, між якими трафік дозволений лише за явними правилами. Це обмежує горизонтальне переміщення нападника: компрометація однієї зони не відкриває автоматично доступ до інших. Типові зони: користувацька, серверна, DMZ (демілітаризована зона для публічних сервісів), гостьова, керування, технологічна (OT), а також ізольована зона резервних копій. Підходи до побудови захищеної мережі подано в таблиці 7.2.

Таблиця 7.2 – Підходи до побудови захищеної мережі

Підхід	Реалізація	Переваги / обмеження
VLAN	Логічний поділ комутованої мережі на широкомовні домени	Дешево й просто; потребує коректного налаштування маршрутизації та фільтрації між VLAN
Міжмережеві екрани між зонами	Правила за принципом «заборонено все, що явно не дозволено»	Основа контролю трафіку; потребує регулярного перегляду правил
Мікросегментація	Політики на рівні окремих робочих навантажень (віртуалізація, хмара)	Дуже точний контроль; складність адміністрування
NAC (802.1X)	Допуск до мережі лише автентифікованих і відповідних політиці пристроїв	Блокує сторонні пристрої; потребує інфраструктури автентифікації
Zero Trust	Перевірка кожного запиту незалежно від розташування	Сучасна модель; поступове впровадження

7.5 Засоби мережевого захисту

– Міжмережевий екран (firewall) фільтрує трафік за адресами, портами й протоколами. NGFW (міжмережевий екран нового покоління) додатково розпізнає застосунки, користувачів, виконує перевірку TLS-трафіку та інтегрує IPS.

– IDS/IPS – системи виявлення та запобігання вторгненням: аналізують трафік за сигнатурами й аномаліями (приклади: Suricata, Snort, Zeek). IDS лише сповіщає, IPS може блокувати.

– WAF захищає веб-застосунки від ін’єкцій, XSS та інших атак рівня L7.

– Проксі-сервери та шлюзи безпечного доступу до Інтернету фільтрують веб-трафік і блокують шкідливі ресурси.

– VPN створює шифрований канал для віддаленого доступу (IPsec, WireGuard, OpenVPN); для окремих застосунків дедалі частіше використовують ZTNA.

– Захист пошти – перевірка вкладень і посилань, SPF, DKIM, DMARC для запобігання підробці відправника.

– Захист від DDoS – фільтрація й розподіл трафіку на стороні провайдера або CDN.

7.6 Безпека бездротових мереж, DNS та віддаленого доступу

Для Wi-Fi рекомендовано WPA3 (або принаймні WPA2-AES); застарілі WEP і WPA з TKIP вразливі й не повинні застосовуватися. У корпоративних мережах використовують WPA2/WPA3-Enterprise з автентифікацією 802.1X (RADIUS), окрему гостьову мережу, вимкнення WPS та контроль несанкціонованих точок доступу. Вдома достатньо складної парольної фрази, оновлення прошивки роутера й зміни паролів адміністратора за замовчуванням.

DNS – частий вектор атак (підміна відповідей, тунелювання, перенаправлення на шкідливі ресурси). Захист: надійні резолвери з фільтрацією шкідливих доменів, DNSSEC, шифрування запитів (DoT/DoH), моніторинг аномальних запитів. Віддалений доступ має вимагати MFA, перевіряти стан пристрою, використовувати найменші привілеї та журналювання. Пристрої на периметрі (VPN-шлюзи, міжмережеві екрани) потребують пріоритетного оновлення: за даними Verizon DBIR 2025 саме вразливості таких пристроїв дедалі частіше стають вектором первинного доступу.

7.7 Моніторинг та практичний чек-лист

Без видимості захист неефективний. Мережеві пристрої й вузли мають надсилати журнали до централізованої системи (SIEM), ведеться інвентаризація активів, автоматизується виявлення нових пристроїв. Розглянемо мінімальний набір дій для малої організації:

– скласти реєстр пристроїв і ПЗ; видалити невикористовуване;

– увімкнути автоматичні оновлення; терміново усувати критичні вразливості на периметрі;

– увімкнути шифрування дисків і MFA для всіх облікових записів;

– розділити мережу на користувацьку, серверну та гостьову зони; закрити зайві порти;

– змінити паролі за замовчуванням, відключити застарілі протоколи (Telnet, SMBv1);

– налаштувати централізоване журналювання та сповіщення;

– регулярно робити резервні копії за правилом 3-2-1 та перевіряти відновлення.

Приклад. Мала юридична фірма. Фірма з 15 працівників має один плоский сегмент мережі, спільний пароль до Wi-Fi та ноутбуки без шифрування. Після аудиту вона впроваджує: окрему гостьову мережу, WPA3-Personal із довгою парольною фразою для гостей та WPA2/3-Enterprise для працівників, шифрування ноутбуків, MFA, централізоване керування оновленнями та хмарні резервні копії з офлайн-копією. Загальна вартість – значно нижча за потенційні збитки від витоку клієнтських даних.

Висновки

Захист кінцевих пристроїв і мережі будується за принципом глибокого захисту: актуальні оновлення, зміцнена конфігурація, EDR, шифрування й MFA на вузлах; сегментація, міжмережеві екрани, IDS/IPS, захищений Wi-Fi та VPN у мережі. Ключові управлінські елементи – інвентаризація, політика BYOD, централізований моніторинг і регулярна перевірка резервних копій.

Контрольні питання

1. Чому кінцеві пристрої є основною точкою проникнення?
2. Перелічіть основні заходи захисту робочої станції.
3. Чим EDR відрізняється від класичного антивіруса?
4. Що таке hardening і які стандарти конфігурацій ви знаєте?
5. Які ризики несе BYOD і як їх зменшують?
6. Що таке сегментація мережі та DMZ? Для чого вони потрібні?
7. Порівняйте міжмережевий екран, NGFW, IDS та IPS.
8. Які вимоги до безпеки Wi-Fi у домашній і корпоративній мережі?

Література: [3], [4], [15].

ТЕМА 8. ЗБЕРЕЖЕННЯ ДАНИХ, ПРАВО ВЛАСНОСТІ НА ІНФОРМАЦІЮ ТА ЗАХИСТ ОНЛАЙН-ПРИВАТНОСТІ

План лекції

1. Дані як об’єкт управління: життєвий цикл і збереження
2. Резервне копіювання та відновлення
3. Право власності на інформацію
4. Захист персональних даних: принципи та права суб’єктів
5. Інтелектуальна власність у цифровому середовищі
6. Онлайн-приватність: цифровий слід, відстеження, анонімність
7. Практичні засоби захисту приватності

8.1 Дані як об’єкт управління: життєвий цикл і збереження

Дані мають не лише технічну, а й правову та економічну цінність. Організація повинна знати, які дані вона збирає, навіщо, де вони зберігаються, хто має доступ, як довго вони потрібні і як будуть знищені. Цей підхід називають управлінням даними (data governance). Базові елементи: інвентаризація й класифікація даних, призначення власників, політики зберігання (retention), доступу, резервного копіювання й знищення.

Політика зберігання визначає строки, після яких дані видаляють. Мінімізація зберігання зменшує ризики: дані, яких немає, не можна викрасти. Водночас закони можуть вимагати мінімальних строків (бухгалтерські документи, журнали доступу, медичні записи). Типові способи збереження: локальні диски, мережеві сховища (NAS/SAN), хмарні сервіси, знімні носії, архіви. Для кожного вибирають засоби захисту: шифрування, контроль доступу, журналювання, перевірку цілісності.

8.2 Резервне копіювання та відновлення

Резервна копія – головний захист від втрати даних через збої, помилки, вима-

гачі чи катастрофи. Широко відоме правило 3-2-1: мати щонайменше 3 копії даних, на 2 різних типах носіїв, з яких 1 копія розташована окремо (в іншому місці чи хмарі). Сучасні рекомендації розширюють його: одна копія має бути офлайн або незмінною (immutable), щоб вимагач не міг її зашифрувати, а відновлення необхідно регулярно перевіряти – копія, що не відновлюється, марна. Типи резервних копій подано в таблиці 8.1.

Таблиця 8.1 – Типи резервних копій

Тип копії	Що копіюється	Переваги	Недоліки
Повна	Усі дані	Просте відновлення	Великий обсяг і час
Інкрементна	Зміни з останньої копії будь-якого типу	Швидка, мало місця	Відновлення потребує всього ланцюжка
Диференціальна	Зміни з останньої повної копії	Компроміс швидкості та обсягу	Зростає з часом

Для планування застосовують показники: RPO (Recovery Point Objective) – допустима втрата даних у часі (наприклад, 4 години), та RTO (Recovery Time Objective) – допустимий час відновлення сервісу. Вони визначають частоту копіювання та вибір технологій (реплікація, кластеризація, хмарні сервіси відновлення).

Приклад. RPO та RTO. Інтернет-магазин визначив RPO = 15 хв, RTO = 2 год для бази замовлень, а для архіву старих звітів – RPO = 24 год, RTO = 3 доби. Для першого застосовують безперервну реплікацію та автоматичне перемикання, для другого – нічне копіювання в дешеве хмарне сховище. Витрати на захист відповідають цінності даних.

8.3 Право власності на інформацію

Інформація як нематеріальний об’єкт має особливості: її можна копіювати без втрати оригіналу, одночасно використовувати багатьма суб’єктами, вона легко передається. Тому право розрізняє інформацію і носій (матеріальний об’єкт). Закон України «Про інформацію» (ст. 38) визнає право власності на інформацію: власник інформації може вільно розпоряджатися нею – володіти, користуватися, передавати, обмежувати доступ, якщо інше не передбачено законом; обмеження для

інформації з обмеженим доступом, персональних даних, державної таємниці тощо визначаються окремими законами.

Практичні питання власності: хто є власником даних, створених працівником в межах трудових обов'язків (як правило, роботодавець); чи може клієнт вимагати копію власних даних; кому належать дані користувача в хмарному сервісі (за договором і умовами сервісу, а персональні дані – суб'єкту). Тому в політиках і договорах закріплюють: власника даних, розпорядника, правила обробки, відповідальність за порушення, умови повернення та видалення даних після припинення співпраці.

8.4 Захист персональних даних: принципи та права суб'єктів

Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована: ПІБ, адреса, телефон, e-mail, ідентифікатори пристроїв, IP-адреса в окремих випадках, біометричні дані. В Україні діє Закон «Про захист персональних даних» № 2297-VI, а в ЄС – GDPR (Регламент 2016/679). Реформування національного законодавства спрямоване на його наближення до GDPR. Принципи обробки персональних даних (GDPR, ст. 5) подано в таблиці 8.2.

Таблиця 8.2 – Принципи обробки персональних даних (GDPR, ст. 5)

Принцип GDPR	Зміст
Законність, справедливість, прозорість	Обробка має правову підставу й зрозуміла суб'єкту
Обмеження мети	Дані збирають для визначених, чітких цілей
Мінімізація даних	Збирають лише те, що необхідно
Точність	Дані актуальні, неточні виправляють
Обмеження зберігання	Зберігають не довше, ніж потрібно
Цілісність і конфіденційність	Захист технічними й організаційними заходами
Підзвітність	Контролер може довести відповідність

Суб'єкт даних має права: на доступ, виправлення, видалення («право бути забутим»), обмеження обробки, перенесення даних, заперечення проти обробки та проти автоматизованого ухвалення рішень. У разі витоку контролер зобов'язаний повідомити наглядовий орган (за GDPR – протягом 72 годин) і, за високого ризику,

самих суб’єктів. Технічні заходи: псевдонімізація (заміна прямих ідентифікаторів кодами, зі збереженням можливості зворотного зв’язку) та анонімізація (незворотне позбавлення зв’язку з особою), шифрування, контроль доступу, DLP.

Приклад. Мінімізація та псевдонімізація. Навчальний заклад аналізує успішність студентів. Замість повних даних аналітик отримує набір, де ПІБ замінено ідентифікаторами, дата народження – віковою групою, а адресу видалено. Таблицю відповідності ідентифікаторів зберігає окремий відповідальний. Ризик витоку з аналітичної системи значно нижчий, а мету дослідження досягнуто.

8.5 Інтелектуальна власність у цифровому середовищі

Цифрові об’єкти – програми, бази даних, тексти, зображення, відео – охороняються авторським правом. В Україні діє Закон «Про авторське право і суміжні права» (№ 2811-IX від 01.12.2022). Для програмного забезпечення важливі ліцензії: комерційні (EULA) і відкриті (MIT, Apache 2.0, GPL), що встановлюють права на використання, зміну та поширення. Порушенням є піратське копіювання, використання коду з порушенням умов ліцензії та обхід технічних засобів захисту. Для текстів і зображень застосовують Creative Commons (CC BY, CC BY-SA, CC BY-NC тощо). Нові питання виникають із контентом, створеним штучним інтелектом, і використанням захищених творів для навчання моделей: правила активно розробляються, тому під час роботи слід перевіряти умови сервісів.

8.6 Онлайн-приватність: цифровий слід, відстеження, анонімність

Цифровий слід – сукупність даних, які особа залишає в Інтернеті: активний (публікації, коментарі, форми) та пасивний (IP-адреса, історія переглядів, метадані, відбиток браузера). Дані збирають сайти, рекламні мережі, застосунки, соціальні мережі, оператори та провайдери. Агрегування розрізнених даних дозволяє складати детальний профіль людини, що використовують у таргетованій рекламі, а також у фішингу й шахрайстві.

– Cookie та трекери: сторонні cookie, піксельні теги, SDK у застосунках стежать за поведінкою між сайтами;

– Відбиток браузера (fingerprinting): унікальна комбінація налаштувань, шрифтів, роздільної здатності ідентифікує без cookie;

– Метадані: геолокація в фото (EXIF), автор документа, час створення;

– Соціальні мережі: відкриті профілі, геотеги, зв'язки – джерело для OSINT і соціальної інженерії;

– Витоки даних: пов'язані з вашою поштою акаунти в скомпрометованих сервісах.

Анонімність і приватність – не те саме. Приватність – контроль над тим, хто й які відомості про вас бачить; анонімність – неможливість ідентифікувати особу. Мережа Tor забезпечує високий рівень анонімності, VPN переносить довіру з провайдера на VPN-сервіс і приховує IP-адресу від сайтів, але не робить користувача анонімним: сервіс бачить трафік, а облікові дані й відбиток браузера залишаються. Наскрізне шифрування (E2EE) в месенджерах захищає зміст повідомлень, але не метадані.

8.7 Практичні засоби захисту приватності

– перевірити й обмежити налаштування приватності в соціальних мережах та акаунтах Google/Apple/Microsoft;

– використовувати браузери й розширення, що блокують трекери; вимикати сторонні cookie; періодично видаляти дані сайтів;

– вибирати месенджери з E2EE, увімкнути автоматичне видалення повідомлень там, де це доцільно;

– обмежувати дозволи застосунків (геолокація, мікрофон, контакти);

– використовувати окремі адреси електронної пошти (псевдоніми) для реєстрації на сервісах;

– перевіряти витоки (Have I Been Pwned), змінювати пароль після витоку, вмикати MFA;

– видаляти метадані з документів і зображень перед публікацією;

– користуватися VPN у публічних мережах, але розуміти його межі.

Приклад. Фото з метаданими. Користувач публікує фото домашнього кабінету з робочим комп'ютером. У файлі збереглися GPS-координати та модель камери, а на екрані видно частину внутрішніх даних. Зловмисник за метаданими визначає адресу, а за екраном – використовувані системи, і готує цілеспрямований фішинговий лист. Правильні дії: видалити EXIF, перевірити фон фотографії, обмежити аудиторію публікації.

Висновки

Безпечне зберігання даних вимагає політик, класифікації й перевірених резервних копій (3-2-1, RPO/RTO). Право власності на інформацію та вимоги до персональних даних визначають, ким і як можна обробляти дані; GDPR та українське законодавство встановлюють принципи й права суб'єктів. Онлайн-приватність потребує усвідомленого управління цифровим слідом, налаштувань сервісів та технічних засобів (E2EE, блокувальники трекерів, VPN) за розуміння їхніх обмежень.

Контрольні питання

1. Що включає управління даними та політика зберігання?

2. Поясніть правило 3-2-1 та значення незмінних (immutable) копій. Що таке RPO і RTO?

3. Чим відрізняються інформація та її носій з погляду права власності?

4. Що вважається персональними даними? Назвіть принципи їх обробки за GDPR.

5. Які права має суб'єкт персональних даних? У чому різниця між псевдонімізацією й анонімізацією?

6. Які види ліцензій на ПЗ та контент ви знаєте?

7. Що таке цифровий слід і відбиток браузера? Чим приватність відрізняється від анонімності?

8. Які можливості та обмеження має VPN?

Література: [1], [2], [23].

ТЕМА 9. ТЕХНІЧНІ ЗАСОБИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

План лекції

1. Класифікація технічних засобів кібербезпеки
2. Криптографічні засоби
3. Ідентифікація, автентифікація та керування доступом
4. Засоби захисту вузлів і мережі
5. Захист даних та застосунків
6. Засоби моніторингу, реагування та керування вразливостями
7. Вибір і інтеграція засобів захисту

9.1 Класифікація технічних засобів кібербезпеки

Технічні засоби кібербезпеки – програмні, апаратні та програмно-апаратні рішення, що реалізують заходи захисту. Їх зручно класифікувати за функціями, що збігаються з функціями NIST CSF 2.0: ідентифікувати (інвентаризація, сканери), захищати (криптографія, міжмережеві екрани, IAM, EDR), виявляти (SIEM, IDS), реагувати (SOAR, ізоляція) та відновлювати (резервні копії). За моделлю Маккамбера, розглянутою в темі 3, технологічні заходи – лише один із трьох вимірів, тому їх завжди доповнюють політиками й навчанням. Класифікація технічних засобів кібербезпеки подано в таблиці 9.1.

Таблиця 9.1 – Класифікація технічних засобів кібербезпеки

Функція	Класи засобів	Приклади
Криптографічний захист	Шифрування, хешування, електронний підпис, PKI, керування ключами	TLS, BitLocker, GPG, HSM
Керування ідентичністю і доступом	IAM, MFA, PAM, SSO	Active Directory/Entra ID, FIDO2-ключі, менеджери паролів
Захист вузлів	Антивірус, EDR, контроль пристроїв, шифрування дисків	Microsoft Defender, CrowdStrike, ESET
Захист мережі	NGFW, IDS/IPS, WAF, VPN, NAC, ZTNA	Fortinet, Palo Alto, Suricata, WireGuard

Продовження таблиці 9.1

Функція	Класи засобів	Приклади
Захист даних	DLP, резервне копіювання, шифрування баз, маскування	Veeam, Purview DLP
Захист застосунків	SAST/DAST, SCA, WAF, захист API	SonarQube, OWASP ZAP, Dependabot
Моніторинг і реагування	SIEM, SOAR, NDR, UEBA, honeypot	Splunk, Wazuh, Elastic Security
Керування вразливостями	Сканери, інвентаризація, патч-менеджмент	Nessus, OpenVAS, WSUS

Приклади продуктів подано для ілюстрації класів засобів; вибір конкретного рішення залежить від вимог, бюджету й сумісності.

9.2 Криптографічні засоби

Симетричне шифрування використовує один ключ для шифрування й розшифрування; швидке, придатне для великих обсягів даних. Сучасний стандарт – AES (128, 192, 256 біт), режими GCM або CBC із додатковою перевіркою цілісності; в Україні діє національний стандарт ДСТУ 7624:2014 «Калина». Асиметричне шифрування застосовує пару ключів (відкритий і закритий): RSA, еліптичні криві (ECDH, ECDSA, Ed25519); застосовується для обміну ключами й підписів. Геш-функції (SHA-256, SHA-3, в Україні – ДСТУ 7564:2014 «Купина») формують «відбиток» даних фіксованої довжини й використовуються для контролю цілісності та зберігання паролів (із сіллю й повільними функціями – Argon2id, bcrypt, scrypt).

Електронний підпис забезпечує цілісність, автентичність і неспростовність; в Україні регулюється Законом «Про електронну ідентифікацію та електронні довірчі послуги»; кваліфікований електронний підпис має юридичну силу власноручного. Інфраструктура відкритих ключів (PKI) пов’язує відкритий ключ із суб’єктом за допомогою сертифікатів, виданих довіреними центрами сертифікації. TLS – протокол, що забезпечує шифрування й автентифікацію в HTTPS: клієнт перевіряє сертифікат сервера, сторони узгоджують ключі (ECDHE), після чого обмінюються даними, зашифрованими симетричним алгоритмом. Рекомендовано TLS 1.2 і 1.3,

застарілі SSL і TLS 1.0/1.1 слід вимкнути. Криптографічні засоби за задачами подано в таблиці 9.2.

Таблиця 9.2 – Криптографічні засоби за задачами

Задача	Засіб	Приклад використання
Конфіденційність даних у спокої	Симетричне шифрування (AES)	Шифрування диска, баз даних, резервних копій
Конфіденційність у русі	TLS, IPsec, WireGuard	HTTPS, VPN
Цілісність	Геш-функції, HMAC, цифровий підпис	Контрольні суми, підписані оновлення
Автентичність і неспростовність	Електронний підпис, сертифікати	Підписання документів, SSH-ключі
Зберігання паролів	Argon2id, bcrypt + сіль	Бази облікових записів

Приклад. Що відбувається при відкритті https-сайту. Браузер надсилає запит на з'єднання; сервер передає сертифікат; браузер перевіряє підпис довіреного ЦС, ім'я домену та термін дії. Сторони узгоджують сеансовий ключ за алгоритмом ECDHE (забезпечує прямою секретність: компрометація довгострокового ключа не розкриває минулі сеанси). Далі трафік шифрується симетрично (наприклад, AES-GCM). Якщо сертифікат підроблений чи прострочений, браузер показує попередження – і це перша лінія захисту від атаки «людина посередині».

Окрему увагу привертає постквантова криптографія: потужні **к**вантові комп'ютери теоретично здатні зламати RSA та еліптичні криві. NIST у 2024 році затвердив перші стандарти постквантових алгоритмів (ML-KEM, ML-DSA, SLH-DSA – FIPS 203, 204, 205), тому організації починають готувати міграцію («крипто-гнучкість»), особливо для даних із тривалим строком конфіденційності.

9.3 Ідентифікація, автентифікація та керування доступом

Ідентифікація – заявлення особи («я – користувач X»); автентифікація – підтвердження; авторизація – надання прав; облік (accounting) – журналювання дій. Чинники автентифікації: знання (пароль, PIN), володіння (токен, смартфон, ключ FIDO2), властивість (біометрія). Багатофакторна автентифікація (MFA) поєднує щонайменше два різні чинники та суттєво знижує ризик захоплення облікових записів. Найстійкіші до фішингу методи – апаратні ключі та passkeys (стандарти

FIDO2/WebAuthn): секрет не передається, а автентифікація прив’язана до домену сайту. Слабкі методи – SMS-коди (можливість перехоплення чи SIM-swap) та push-підтвердження без перевірки (атаки «втоми від запитів»).

– Менеджер паролів дозволяє мати унікальні складні паролі для кожного сервісу;

– SSO (єдиний вхід) зменшує кількість паролів і дозволяє централізовано керувати доступом;

– RBAC/ABAC – керування доступом на основі ролей або атрибутів; реалізація принципу найменших привілеїв;

– PAM – керування привілейованими обліковими записами: сховище паролів, тимчасовий доступ, запис сеансів;

– IGA/процедури життєвого циклу: своєчасне створення, зміна й відкликання прав при прийнятті, переведенні та звільненні.

9.4 Засоби захисту вузлів і мережі

Засоби захисту вузлів (антивірус, EDR, контроль пристроїв, шифрування дисків) та мережі (NGFW, IDS/IPS, WAF, VPN, NAC, ZTNA) розглянуто в темі 7. З погляду вибору технологій важливо розуміти їх **межі**: антивірус із сигнатурами не виявить нову загрозу; міжмережевий екран не зупинить атаку, що використовує дозволений порт із легітимним обліковим записом; VPN не захищає від шкідливого ПЗ на пристрої. Тому засоби поєднують у багаторівневу архітектуру.

9.5 Захист даних та застосунків

DLP (Data Loss Prevention) – системи запобігання витокам: аналізують вміст і контекст (електронна пошта, USB, хмарні завантаження, друк) і блокують чи маркують передавання конфіденційних даних за політиками (наприклад, не допускати відправлення файла із номерами карток на зовнішній e-mail). Маскування й токенізація замінюють чутливі значення у тестових і аналітичних

середовищах. Шифрування баз даних (TDE, шифрування полів) та керування ключами (KMS, HSM) завершують захист даних у сховищах.

Захист застосунків забезпечують на етапах розроблення (SSDLC): моделювання загроз; SAST – статичний аналіз коду; SCA – перевірка залежностей на відомі вразливості, генерація SBOM; DAST – динамічне тестування працюючого застосунку; IAST/RASP – аналіз під час виконання; захист API (автентифікація, обмеження швидкості); WAF – шар захисту від типових веб-атак.

9.6 Засоби моніторингу, реагування та керування вразливостями

SIEM збирає й корелює журнали з різних джерел, формує сповіщення та підтримує розслідування. SOAR автоматизує типові дії реагування (блокування IP, ізоляція вузла, створення тікета). NDR аналізує мережевий трафік на аномалії. UEBA виявляє відхилення від нормальної поведінки користувачів. Honeypot – приманка для виявлення й вивчення дій нападника. Сканери вразливостей і системи патч-менеджменту підтримують цикл керування вразливостями.

9.7 Вибір і інтеграція засобів захисту

Вибір будують на аналізі ризиків: спершу з’ясовують, які активи й загрози найважливіші, а потім підбирають засоби, що знижують ризик найефективніше за прийнятних витрат (ROSI – повернення інвестицій у безпеку; TCO – загальна вартість володіння, що враховує ліцензії, впровадження, супровід та навчання персоналу). Критерії вибору: відповідність вимогам законодавства та стандартів (включно з вимогами до криптографічних засобів і сертифікацією в Україні), інтеграція з існуючою інфраструктурою, масштабованість, якість виявлення (за незалежними тестами), простота керування, підтримка вендора, відкритий або закритий код.

Приклад. Мінімальний стек для малого університетського підрозділу. MFA (ключі FIDO2 або застосунок) для пошти та хмарних сервісів; менеджер паролів; EDR/антивірус із централізованим керуванням; шифрування ноутбуків; фільтрація

пошти з DMARC; NGFW із сегментацією (користувачі, лабораторії, сервери, гості); автоматичне оновлення та сканування вразливостей; централізований збір журналів (наприклад, Wazuh) і резервне копіювання за правилом 3-2-1. Для більшості типових атак цього достатньо, а складніші засоби додають за результатами оцінки ризиків.

Висновки

Технічні засоби кібербезпеки охоплюють криптографію, керування доступом, захист вузлів, мережі, даних і застосунків, а також моніторинг і реагування. Жоден засіб не є універсальним, тому їх поєднують в архітектуру глибокого захисту, обираючи за результатами оцінки ризиків і з урахуванням вимог законодавства, вартості та можливостей експлуатації.

Контрольні питання

1. За якими функціями класифікують технічні засоби кібербезпеки?

2. Порівняйте симетричне й асиметричне шифрування. Для яких задач застосовують геш-функції?

3. Опишіть основні кроки встановлення TLS-з’єднання. Що таке пряма секретність?

4. Що таке PKI і електронний підпис? Яку юридичну силу має кваліфікований електронний підпис в Україні?

5. Які чинники автентифікації існують? Чому passkeys і FIDO2 стійкі до фішингу?

6. Що таке DLP, SAST, SCA і DAST?

7. Які функції виконують SIEM і SOAR?

8. За якими критеріями вибирають засоби захисту для організації?

Література: [3], [13], [24], [25], [26].

ТЕМА 10. ПОВЕДІНКОВІ АСПЕКТИ КІБЕРБЕЗПЕКИ ТА БЕЗПЕЧНА ПОВЕДІНКА КОРИСТУВАЧІВ

План лекції

1. Людський фактор у кібербезпеці
2. Типові помилки та психологічні чинники
3. Правила безпечної поведінки користувача
4. Безпечна поведінка при віддаленій роботі та в соціальних мережах
5. Культура безпеки та навчання персоналу
6. Політики та організаційні заходи
7. Вимірювання та поліпшення поведінки

10.1 Людський фактор у кібербезпеці

Технічні засоби можуть бути ідеально налаштованими, проте найчастіше успіху досягають атаки, спрямовані на людей. За даними звіту Verizon DBIR 2025, людський елемент (помилки, фішинг, зловживання привілеями, використання викрадених облікових даних) бере участь приблизно у 60 % порушень. Тому поведінка користувачів вважається одним із трьох вимірів моделі Маккамбера (освіта й персонал) і окремим доменом у стандартах (у ISO/IEC 27001:2022 – 8 «людських» заходів, серед них перевірка кандидатів, навчання, дисциплінарний процес, віддалена робота, повідомлення про події).

Важливо дивитися на людину не як на «слабку ланку», а як на частину системи: правильно побудовані процеси та інтерфейси роблять безпечну поведінку найлегшою. Якщо для виконання роботи користувач змушений обходити правила, система спроєктована неправильно. Тому управління поведінкою поєднує навчання, мотивацію, зручні засоби захисту й чіткі політики.

10.2 Типові помилки та психологічні чинники

Типові помилки користувачів подано в таблиці 10.1.

Таблиця 10.1 – Типові помилки користувачів

Помилка	**Причина**	**Наслідок**
Повторне використання паролів	Складність запам’ятовування багатьох паролів	Credential stuffing, захоплення облікових записів
Перехід за посиланнями у листах і SMS	Терміновість, довіра до відправника	Фішинг, шкідливе ПЗ
Відкладення оновлень	«Потім», страх зламати робочі процеси	Експлуатація відомих вразливостей
Передавання даних неперевіреним особам	Бажання допомогти, тиск авторитету	BEC, соціальна інженерія
Використання особистих хмар і месенджерів для робочих даних	Зручність	Витік, втрата контролю
Підключення до публічного Wi-Fi без захисту	Економія трафіку	Перехоплення даних
Нехтування повідомленням про інцидент	Страх покарання	Зростання шкоди через затримку

Нападники використовують когнітивні упередження й принципи впливу (Р. Чалдіні): авторитет (лист «від директора»), терміновість і дефіцит («рахунок буде заблоковано через годину»), соціальний доказ, взаємність, симпатія, послідовність. Додаткові чинники: втома від безпеки (security fatigue) – коли надмірні й складні вимоги призводять до їх ігнорування; звикання до попереджень; перевантаженість і поспіх; оптимістичне упередження («зі мною такого не станеться»).

Приклад. Втома від MFA-запитів. Нападник, дізнавшись пароль працівника, надсилає десятки push-запитів на підтвердження вночі. Утомлений користувач зрештою натискає «Підтвердити». Захист: застосунки з вводом коду (number matching), ліміти запитів, ключі FIDO2, навчання повідомляти про незапитані підтвердження.

10.3 Правила безпечної поведінки користувача

– Паролі: унікальні для кожного сервісу, довгі (парольні фрази від 12–16 символів), зберігання в менеджері паролів; ніколи не передавати іншим;

– MFA: увімкнути скрізь, де можливо; віддавати перевагу passkeys/ключам, а не SMS;

– Пошта та повідомлення: перевіряти відправника, домен і посилання; не відкривати несподівані вкладення; при сумніві перевіряти запит іншим каналом;

– Оновлення: встановлювати оновлення ОС і застосунків; не використовувати непідтримуване ПЗ;

– Джерела ПЗ: тільки офіційні магазини й сайти; не встановлювати «зламані» програми;

– Пристрої: блокувати екран, шифрувати диск, не залишати без нагляду; не підключати невідомі USB;

– Дані: не публікувати зайвого; не пересилати конфіденційні файли через особисті сервіси;

– Резервні копії: регулярно та за правилом 3-2-1;

– Повідомлення про інциденти: швидко повідомляти про підозрілі події, не боятися помилок.

Корисне правило: «Зупинись – подумай – перевір». Перед виконанням терміново-емоційної дії (переказ коштів, надання пароля, відкриття вкладення) варто зупинитися, оцінити правдоподібність і перевірити запит через незалежний канал (дзвінок на відомий номер, окрема розмова з колегою).

10.4 Безпечна поведінка при віддаленій роботі та в соціальних мережах

Під час віддаленої роботи користувач сам відповідає за частину IT-інфраструктури: домашній роутер, пристрої, мережу. Рекомендації: змінити пароль адміністратора роутера, оновити прошивку, вимкнути WPS, використовувати WPA3/WPA2-AES; працювати через корпоративний VPN або ZTNA; не залишати відкритими екрани й документи (екран видно через вікно, у кав’ярні); не використовувати публічні комп’ютери для входу в робочі облікові записи; розділяти робоче й особисте.

У соціальних мережах слід обмежувати відкритість профілю, не публікувати документи, квитки, геолокацію в реальному часі, інформацію про роботу та режим

дня; перевіряти запити «у друзі» (клонування профілів); критично ставитися до «опитувань», що збирають відповіді на типові секретні питання (ім'я домашнього улюбленця, школа**).** Дипфейки та генеративний ШІ дозволяють створювати переконливі голос і відео: прохання, що надходять голосом чи відео від «керівника» чи «родича», особливо щодо грошей, перевіряють за домовленим кодовим словом чи окремим каналом.

Приклад. Дзвінок від «керівника». Бухгалтер отримує відеодзвінок, де «фінансовий директор» просить терміново провести конфіденційний переказ. Правильна поведінка: не виконувати прохання під тиском, завершити розмову й зателефонувати за відомим номером або подати запит через затверджену систему з двоособовим підтвердженням. У відомому випадку 2024 року компанія в Гонконзі втратила близько 25 млн доларів США після відеоконференції з діпфейками «керівників» (за повідомленнями поліції Гонконгу).

10.5 Культура безпеки та навчання персоналу

Культура безпеки – спільні цінності, переконання та звички, що визначають ставлення співробітників до безпеки. Сильна культура означає, що люди розуміють ризики, не бояться повідомляти про помилки, а керівники подають приклад. Основні елементи програми обізнаності: (1) вступний інструктаж; (2) регулярні короткі навчання (мікронавчання) замість одного щорічного; (3) імітаційні фішингові кампанії з негайним зворотним зв'язком; (4) рольове навчання (для керівників, адміністраторів, розробників, бухгалтерів); (5) кампанії обізнаності й тематичні дні; (6) прості канали повідомлення про інциденти («кнопка "повідомити про фішинг"»). Принципи ефективної програми обізнаності подано в таблиці 10.2.

Таблиця 10.2 – Принципи ефективної програми обізнаності

Принцип програми навчання	**Що це означає на практиці**
Релевантність	Приклади з реальної роботи й актуальних атак (BEC, діпфейки, QR-фішинг)

Продовження таблиці 10.2

Принцип програми навчання	Що це означає на практиці
Короткі та регулярні заняття	5–10-хвилинні модулі щомісяця
Позитивне підкріплення	Заохочення за повідомлення; без публічного осуду за помилки
Практика, а не лише лекції	Симуляції, тренування реагування, настільні вправи
Підтримка керівництва	Керівники проходять навчання й дотримуються правил
Вимірюваність	Показники змін поведінки, а не лише відвідуваність

10.6 Політики та організаційні заходи

Поведінку закріплюють у документах: політика інформаційної безпеки, політика прийнятного використання (Acceptable Use Policy), політики паролів і MFA, BYOD, віддаленої роботи, роботи з даними, реагування на інциденти. Політики мають бути стислими, зрозумілими й виконуваними; користувачі ознайомлюються з ними під підпис. Організаційні заходи включають перевірку кандидатів, угоди про нерозголошення, розмежування обов’язків, процедуру звільнення (негайне відкликання доступу), дисциплінарну відповідальність за навмисні порушення та політику «без обвинувачення» (just culture) для ненавмисних помилок і своєчасних повідомлень.

Стосовно інсайдерських загроз розрізняють: зловмисних (мотиви – гроші, образа), необережних (помилки, недбалість) і скомпрометованих (облікові дані викрадено ззовні). Заходи: принцип найменших привілеїв, розподіл обов’язків, моніторинг аномальної поведінки, процедури при звільненні, а також відкрита комунікація та підтримка працівників.

10.7 Вимірювання та поліпшення поведінки

Ефективність програм вимірюють показниками: частка користувачів, що клікнули в імітаційному фішингу, і, що важливіше, частка тих, хто повідомив про нього; середній час між отриманням підозрілого листа та повідомленням; частка користувачів із MFA; кількість порушень політик; кількість повідомлених

інцидентів; результати тестів знань. Тривала динаміка показує, чи змінюється поведінка. Поліпшення досягають, спрощуючи безпечний шлях (за замовчуванням безпечні налаштування, SSO, менеджер паролів), застосовуючи «підштовхування» (nudges) – підказки в момент ризикової дії, та вдосконалюючи процеси на основі аналізу інцидентів.

Приклад. Щомісячна фішингова кампанія. У компанії початковий показник кліків – 22 %, а повідомлень про підозрілі листи – 5 %. Після шести місяців мікронавчання й додавання кнопки «Повідомити про фішинг» кліки знизилися до 7 %, повідомлення зросли до 38 %. Значення умовні, але демонструють логіку: важливіше за зниження кліків, зростання кількості повідомлень, бо кожен повідомлений лист дає службі безпеки час відреагувати.

Висновки

Людський фактор присутній у більшості кіберінцидентів, але люди можуть стати найефективнішим рубежем захисту за умови грамотної програми навчання, зрозумілих політик, зручних безпечних інструментів та культури, що заохочує повідомляти про проблеми. Основні правила – унікальні паролі й MFA, критичне ставлення до повідомлень, оновлення, обережність у соціальних мережах і своєчасне повідомлення про інциденти.

Контрольні питання

1. Чому людський фактор вважають одним з найважливіших у кібербезпеці?
2. Які психологічні прийоми використовують соціальні інженери? Наведіть приклади.
3. Що таке втома від безпеки й як з нею боротися?
4. Сформулюйте основні правила безпечної поведінки користувача.
5. Як перевірити підозріле прохання, що надійшло голосом чи відео?
6. Які елементи має ефективна програма підвищення обізнаності?
7. Що таке політика прийнятного використання й політика «без обвинувачення»?

Література: [2], [4], [6], [13].

ТЕМА 11. ІНСТРУМЕНТИ ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ ТА ЗАПОБІГАННЯ КІБЕРЗАГРОЗАМ

План лекції

1. Принципи виявлення та запобігання загрозам
2. Джерела даних і журналювання
3. Системи виявлення та запобігання вторгненням (IDS/IPS)
4. SIEM, SOAR та центр моніторингу (SOC)
5. EDR, XDR, NDR та аналіз поведінки
6. Кіберрозвідка (CTI) та пастки (honeypot)
7. Реагування на інциденти та показники ефективності

11.1 Принципи виявлення та запобігання загрозам

Запобіжні заходи (антивіруси, міжмережеві екрани, MFA) не можуть зупинити всі атаки. Тому сучасна модель кібербезпеки виходить із принципу «припустимо компрометацію» (assume breach): поряд із запобіганням необхідно швидко виявляти атаку та реагувати. Ключові показники – MTTD (середній час виявлення) та MTTR (середній час реагування або відновлення): чим вони менші, тим менша шкода. У NIST CSF 2.0 цим цілям відповідають функції Detect та Respond.

Підходи до виявлення: сигнатурний – порівняння з відомими ознаками (хеші файлів, шаблони трафіку, правила); евристичний і поведінковий – аналіз підозрілих дій (запуск PowerShell із Word); аномальний (статистичний, на основі машинного навчання) – відхилення від нормального профілю; за індикаторами компрометації (IoC) – відомі IP-адреси, домени, хеші; за тактиками й техніками (TTP) – ознаки поведінки за MITRE ATT&CK, стійкіші до зміни інфраструктури нападника. Кожен підхід має хибні спрацьовування (false positive) та пропуски (false negative), тому їх поєднують. Підходи до виявлення загроз подано в таблиці 11.1.

Таблиця 11.1 – Підходи до виявлення загроз

Підхід	**Сильні сторони**	**Слабкі сторони**
Сигнатурний	Точний для відомих загроз, швидкий	Не бачить нових і змінених загроз
Поведінковий / евристичний	Виявляє невідомі загрози та безфайлові атаки	Хибні спрацьовування, потребує налаштування
Аномальний (ML)	Виявляє невідомі схеми, адаптується	Потребує даних і тренування; складний для пояснення
На основі IoC	Простота, швидка реакція на відомі кампанії	Інфраструктуру нападник легко змінює
На основі TTP	Стійкий до змін інструментів	Потребує експертизи й якісних даних

11.2 Джерела даних і журналювання

Виявлення неможливе без даних. Основні джерела: журнали операційних систем (події входу, створення процесів, зміни прав), мережевих пристроїв і міжмережевих екранів, DNS і проксі, електронної пошти, хмарних сервісів і систем ідентифікації, веб-застосунків та баз даних, засобів захисту вузлів, мережевий трафік (NetFlow, дзеркалювання, PCAP). Журнали мають бути повними (охоплення ключових джерел), надійними (захист від зміни – пересилання на окремий сервер), синхронізованими за часом (NTP) і зберігатися достатньо довго (практично – від 90 днів у швидкому доступі до року й більше в архіві, залежно від вимог).

– Windows: події 4624/4625 (успішний і невдалий вхід), 4688 (створення процесу), Sysmon для розширеної телеметрії;

– Linux: auth.log, journald, auditd;

– Мережа: журнали NGFW, NetFlow, DNS-запити, Zeek-журнали;

– Хмара: журнали активності (аудит дій адміністраторів і API);

– Автентифікація: невдалі входи, MFA-події, «неможливі переміщення» між країнами.

11.3 Системи виявлення та запобігання вторгненням (IDS/IPS)

IDS аналізує трафік чи події й сповіщає про підозрілу активність; IPS розташовується «в розріз» каналу й може автоматично блокувати. За місцем

встановлення розрізняють NIDS/NIPS (мережеві) та HIDS/HIPS (на вузлах). Широко використовуються відкриті рішення Snort, Suricata (правила на основі сигнатур) і Zeek (детальний аналіз протоколів і журналювання). Wazuh/OSSEC поєднують HIDS, контроль цілісності файлів та збір журналів.

Приклад. Правило Suricata (концептуально). Адміністратор додає правило: якщо з внутрішньої мережі встановлюється з'єднання HTTP із підозрілим рядком User-Agent, що характерний для відомого шкідливого завантажувача, – сформувати сповіщення високого пріоритету. Правило складається із заголовка (дія, протокол, адреси, порти) та опцій (повідомлення, умови пошуку в вмісті, класифікація). Сповіщення надходить у SIEM, де аналітик перевіряє, який вузол і користувач ініціювали з'єднання.

11.4 SIEM, SOAR та центр моніторингу (SOC)

SIEM (Security Information and Event Management) збирає журнали з багатьох джерел, нормалізує їх, зберігає, корелює події за правилами й формує сповіщення, а також надає інструменти пошуку та розслідування й звітність для аудиту. Приклади: Splunk, Microsoft Sentinel, IBM QRadar, Elastic Security, Wazuh. Ефективність SIEM залежить від якості джерел, правил кореляції та їх постійного налаштування. Приклади правил кореляції подано в таблиці 11.2.

Таблиця 11.2 – Приклади правил кореляції

Приклад правила кореляції	**Логіка**	**Що виявляє**
Підбір пароля з наступним успіхом	≥ 10 невдалих входів за 5 хв до успішного входу з тієї ж IP-адреси	Brute force, password spraying
Неможливе переміщення	Входи одного користувача з двох країн за короткий час	Захоплення облікового запису
Підозрілий ланцюжок процесів	Word → PowerShell → мережеве з'єднання	Макровірус, доставка шкідливого ПЗ
Масове шифрування файлів	Різке зростання змін/перейменувань файлів на вузлі	Вимагач
Нетиповий вихідний трафік	Великий обсяг даних на невідомий зовнішній хост уночі	Ексфільтрація даних

SOAR (Security Orchestration, Automation and Response) автоматизує типові дії за сценаріями (playbooks): збагачення сповіщення даними розвідки, блокування IP

в міжмережевому екрані, ізоляція вузла, скидання пароля, створення тікета. SOC (Security Operations Center) – підрозділ, що забезпечує безперервний моніторинг та реагування: аналітики першого рівня (тріаж сповіщень), другого (розслідування), третього (полювання на загрози, форензика), а також інженери виявлення й керівник. Малі організації можуть використовувати зовнішній SOC (MDR-послуги). В Україні функції національного рівня виконують НКЦК та CERT-UA.

11.5 EDR, XDR, NDR та аналіз поведінки

EDR забезпечує глибоку телеметрію вузлів, виявлення за поведінкою та реагування. NDR (Network Detection and Response) аналізує мережевий трафік, в тому числі зашифрований (за метаданими й поведінкою), виявляючи горизонтальне переміщення, C2-канали й ексфільтрацію. XDR об'єднує дані EDR, NDR, пошти, хмари та ідентичності для кореляції в єдиній платформі. UEBA будує профілі нормальної поведінки користувачів і сутностей (час роботи, ресурси, обсяги даних) й виявляє відхилення: наприклад, бухгалтер раптом завантажує гігабайти даних з репозиторію коду.

Ефективним доповненням є полювання на загрози (threat hunting) – проактивний пошук ознак компрометації за гіпотезами, а не за сповіщеннями. Гіпотезу формулюють на основі TTP з ATT&CK (наприклад: «нападники можуть використовувати заплановані завдання для закріплення»), перевіряють запитами до журналів і за результатами створюють нові правила виявлення. Для портативного опису правил використовують формати Sigma (для журналів), YARA (для файлів та пам'яті) і Suricata/Snort (для мережі).

11.6 Кіберрозвідка (CTI) та пастки (honeypot)

Cyber Threat Intelligence (CTI) – оброблена інформація про загрози, що допомагає ухвалювати рішення. Рівні: стратегічна (тенденції, мотиви – для керівництва), оперативна (кампанії та TTP груп), тактична (поведінка, правила), технічна (IoC: хеші, IP, домени). Джерела: відкриті (OSINT), спільноти обміну

інформацією (ISAC), платформи MISP, OpenCTI, звіти вендорів, CERT-UA. Для автоматичного обміну застосовують формати STIX і протокол TAXII. Важливо оцінювати достовірність, актуальність і релевантність даних – застарілі IoC дають хибні спрацьовування.

Honeypot (приманка) – навмисно вразливий або імітований ресурс, будь-яка взаємодія з яким підозріла за визначенням. Він дає раннє попередження й дані про інструменти нападників. Honeytoken – фальшиві облікові записи, ключі чи файли, використання яких викликає сповіщення. Такі засоби мають мало хибних спрацьовувань, але вимагають ізоляції від виробничого середовища.

Приклад. Honeytoken у хмарі. Адміністратор розміщує в репозиторії фальшивий ключ доступу до хмарного акаунта без прав. Через кілька тижнів SIEM отримує сповіщення: цей ключ використовується з невідомої IP-адреси. Це свідчить, що репозиторій скомпрометовано або код витік; команда ініціює розслідування, замінює справжні ключі й виявляє, що внутрішній розробник зберігав копію репозиторію на особистому пристрої.

11.7 Реагування на інциденти та показники ефективності

Виявлення має продовжуватися процесом реагування. Згідно з NIST SP 800-61 Rev. 3 (2025), узгодженим із CSF 2.0, реагування інтегроване в загальне управління кіберризиками. Традиційно цикл містить такі фази: підготовка (плани, команда, інструменти), виявлення й аналіз (класифікація, пріоритезація, визначення масштабу), стримування, усунення та відновлення (ізоляція, видалення загрози, відновлення з копій, закриття вразливості), післяінцидентний аналіз (уроки, поліпшення). Для кожного типу інцидентів створюють плейбуки і регулярно проводять навчання (tabletop-вправи).

Для держави в Україні обов’язкове повідомлення про інциденти на об’єктах критичної інфраструктури та державних органах до НКЦК/CERT-UA передбачене законодавством та підзаконними актами (див. тему 2). Приватні організації, що працюють з ЄС, враховують вимоги NIS2 (24 години/72 години) і GDPR (72 години

щодо персональних даних). Показники ефективності виявлення й реагування подано в таблиці 11.3.

Таблиця 11.3 – Показники ефективності виявлення й реагування

Показник	Що вимірює	Мета
MTTD	Середній час від початку інциденту до його виявлення	Зменшувати
MTTR	Середній час від виявлення до усунення чи відновлення	Зменшувати
Частка хибних спрацьовувань	Відсоток сповіщень без реальної загрози	Зменшувати, зберігаючи покриття
Покриття джерел журналів	Частка критичних систем, що передають журнали	Збільшувати
Покриття ATT&CK	Частка технік, для яких є правила виявлення	Збільшувати за пріоритетами
Час тріажу	Час від сповіщення до рішення аналітика	Зменшувати

Приклад. Повний цикл. Сповіщення EDR: з бухгалтерського ПК запущено PowerShell із Word. Автоматичний сценарій SOAR збагачує його: хеш файла відомий як шкідливий. Вузол ізолюється, SIEM перевіряє інші пристрої на той самий хеш і знаходить ще один. Аналітик підтверджує інцидент, скидає облікові дані користувача, усуває загрозу, перевіряє резервні копії. Після інциденту команда додає правило блокування макросів із Інтернету та проводить тренінг. MTTD склав 6 хвилин, MTTR – 2 години.

Висновки

Ефективний захист поєднує запобігання та виявлення. Основою виявлення є якісні журнали, а головні інструменти – IDS/IPS, EDR/NDR/XDR, SIEM і SOAR, що працюють у межах SOC. Кіберрозвідка, honeypot і полювання на загрози підвищують проактивність. Процеси реагування, відпрацьовані навчаннями, і показники MTTD/MTTR дозволяють вимірювати та поліпшувати захист.

Контрольні питання

1. Чому виявлення й реагування так само важливі, як і запобігання?

2. Охарактеризуйте сигнатурний, поведінковий та аномальний підходи до виявлення загроз.

3. Які джерела журналів необхідні для моніторингу та які вимоги до журналювання?

4. Чим відрізняються IDS та IPS? Які відкриті рішення вам відомі?

5. Для чого призначені SIEM і SOAR? Наведіть приклади правил кореляції.

6. Яка структура та функції SOC?

7. Що таке CTI, IoC і TTP? Для чого використовують STIX і TAXII?

8. Що таке honeypot і honeytoken? Які в них переваги?

9. Опишіть фази реагування на інцидент та основні показники ефективності.

Література: [3], [7], [9], [18], [27].

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII (зі змінами, внесеними Законом № 4336-IX від 27.03.2025). URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 01.11.2026).

2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : ISO, 2022. URL: https://www.iso.org/standard/27001 (дата звернення: 04.11.2026).

3. The NIST Cybersecurity Framework (CSF) 2.0 : NIST CSWP 29. Gaithersburg, MD : National Institute of Standards and Technology, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29 (дата звернення: 04.11.2026).

4. 2025 Data Breach Investigations Report. New York : Verizon Business, 2025. URL: https://www.verizon.com/dbir/ (дата звернення: 04.11.2026).

5. ENISA Threat Landscape 2025. Athens : European Union Agency for Cybersecurity (ENISA), 2025. ISBN 978-92-9204-723-8. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (дата звернення: 04.11.2026).

6. Cost of a Data Breach Report 2026 / IBM ; Ponemon Institute. Armonk, NY: IBM, 2026. URL: https://www.ibm.com/reports/data-breach (дата звернення: 07.11.2026).

7. Держспецзв’язку: Україна трансформує систему кібербезпеки за європейськими стандартами. Урядовий портал. Кабінет Міністрів України. URL: https://www.kmu.gov.ua/news/derzhspetszviazku-ukraina-transformuie-systemu-kiberbezpeky-za-ievropeiskymy-standartamy (дата звернення: 07.11.2026).

8. У 2025 році кількість кібератак зросла на 37 %: кого атакують найчастіше. DEV.ua. URL: https://dev.ua/news/u-2025-rotsi-kilkist-kiberatak-zrosla-na-37-1767858414 (дата звернення: 09.11.2026).

9. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної

інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20 (дата звернення: 09.11.2026).

10. 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. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата звернення: 09.11.2026).

11. 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. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj (дата звернення: 11.11.2026).

12. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Official Journal of the European Union. 2024. L 2024/2847, 20.11.2024. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj (дата звернення: 11.11.2026).

13. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. Geneva : ISO, 2022. URL: https://www.iso.org/standard/75652.html (дата звернення: 11.11.2026).

14. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT). Інформаційна безпека, кібербезпека та захист приватності. Системи управління інформаційною безпекою. Вимоги. Київ : УкрНДНЦ, 2023. 26 с.

15. CIS Critical Security Controls. Version 8.1. East Greenbush, NY : Center for Internet Security, 2024. URL: https://www.cisecurity.org/controls (дата звернення: 11.11.2026).

16. MITRE ATT&CK® Enterprise Matrix. MITRE Corporation. URL: https://attack.mitre.org/matrices/enterprise/ (дата звернення: 11.11.2026).

17. OWASP Top 10:2025. OWASP Foundation, 2025. URL: https://owasp.org/Top10/2025/ (дата звернення: 11.11.2026).

18. Common Vulnerability Scoring System Version 4.0 : Specification Document. Forum of Incident Response and Security Teams (FIRST), 2023. URL: https://www.first.org/cvss/v4-0/specification-document (дата звернення: 11.11.2026).

19. Exploit Prediction Scoring System (EPSS). Forum of Incident Response and Security Teams (FIRST). URL: https://www.first.org/epss/ (дата звернення: 11.11.2026).

20. Known Exploited Vulnerabilities Catalog. Cybersecurity and Infrastructure Security Agency (CISA). URL: https://www.cisa.gov/known-exploited-vulnerabilities-catalog (дата звернення: 11.11.2026).

21. Про авторське право і суміжні права : Закон України від 01.12.2022 № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20 (дата звернення: 11.11.2026).

22. Module-Lattice-Based Key-Encapsulation Mechanism Standard : FIPS 203. Gaithersburg, MD : National Institute of Standards and Technology, 2024. DOI: https://doi.org/10.6028/NIST.FIPS.203 (дата звернення: 11.11.2026).

23. Module-Lattice-Based Digital Signature Standard : FIPS 204. Gaithersburg, MD : National Institute of Standards and Technology, 2024. DOI: https://doi.org/10.6028/NIST.FIPS.204 (дата звернення: 11.11.2026).

24. Stateless Hash-Based Digital Signature Standard : FIPS 205. Gaithersburg, MD : National Institute of Standards and Technology, 2024. DOI: https://doi.org/10.6028/NIST.FIPS.205 (дата звернення: 11.11.2026).

25. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile : NIST SP 800-61r3. Gaithersburg, MD : National Institute of Standards and Technology, 2025. DOI: https://doi.org/10.6028/NIST.SP.800-61r3 (дата звернення: 11.11.2026).

26. Євсеєв С. П.. Основи кібербезпеки: навчально-практичний посібник. Львів : ПП «Новий Світ-2000», 2025. 320 с.

О75 Основи кібербезпеки : 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. І. Міскевич. Луцьк : ЛНТУ, 2026. 83 с.

Конспект лекцій з дисципліни «Основи кібербезпеки» складений відповідно до діючої програми курсу.

Призначений для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань F Інформаційні технології спеціальності 125 Кібербезпека та захист інформації.

Комп’ютерний набір О.І. Міскевич

Редактор О.І. Міскевич

Підп. до друку «___» _____ 2026 р.
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