Сучасні питання кібербезпеки

доцент
Горбенко В.І.
ауд.19, корп.1

Організаційні аспекти кібербезпеки

це сукупність управлінських, нормативних, освітніх і процедурних заходів, спрямованих на забезпечення належного рівня інформаційної безпеки підприємства чи установи.

Класифікація організаційних аспектів кібербезпеки:

1. Управлінські (стратегічні) аспекти: визначають політику, цілі та відповідальність у сфері кібербезпеки.
2. Нормативно-правові аспекти: регулюють діяльність у сфері кібербезпеки через закони, стандарти та внутрішні нормативи.
3. Організаційно-технічні аспекти: передбачають впровадження процедур і систем, що забезпечують безпеку інформаційних ресурсів.
4. Людський (соціальний) аспект: людина — найслабша ланка безпеки, тому важливо формувати культуру кібергігієни.
5. Операційні (процедурні) аспекти: регламентують щоденну діяльність, пов’язану з підтриманням безпеки.
6. Комунікаційно-координаційні аспекти: забезпечують взаємодію всередині організації та ззовні — з державними структурами, CERT/CSIRT, партнерами.

Управлінські (стратегічні) аспекти

Основні елементи:

- Розробка стратегії кібербезпеки організації.
- Призначення CISO (Chief Information Security Officer) або відповідального за ІБ.
- Формування політик безпеки інформації.
- Впровадження системи управління інформаційною безпекою (ISMS) за стандартом ISO/IEC 27001.
- Керування ризиками (Risk Management).

Стратегія кібербезпеки організації — це офіційний документ, який визначає довгострокове бачення, принципи, цілі та механізми управління кіберризиками.

Вона має забезпечити:

- захист інформаційних ресурсів (даних, мереж, систем, користувачів);
- безперервність діяльності (resilience);
- дотримання законодавчих і галузевих вимог;
- підвищення обізнаності персоналу і формування культури безпеки.

Етапи розробки стратегії

Етап	Зміст	Учасники
1. Аналіз середовища та ризиків	Визначення ключових загроз, активів, уразливостей, рівня зрілості кібербезпеки	IT-відділ, служба безпеки, зовнішні аудитори
2. Визначення цілей і пріоритетів	Формулюються стратегічні цілі: конфіденційність, цілісність, доступність, відповідність (compliance)	Керівництво, CISO, юристи
3. Розроблення політик і принципів	Визначення підходів: Security by Design, Zero Trust, Least Privilege, управління ризиками, безпечна розробка	IT-архітектори, аналітики
4. Планування організаційної структури безпеки	Хто за що відповідає (CISO, адміністратори, менеджери підрозділів, підрядники)	HR, керівництво, служба безпеки
5. Вибір технологічних засобів захисту	Антивіруси, системи виявлення вторгнень (IDS/IPS), резервування, SIEM, багатофакторна автентифікація	IT-служба, DevOps, фінансовий департамент
6. Підготовка плану реагування на інциденти	Хто і як діє при атаках, витоках, збої систем	CISO, PR-служба, технічна команда
7. Навчання персоналу та побудова культури безпеки	Розробка тренінгів, політик паролів, симуляцій фішингових атак	HR, CISO, IT-служба
8. Моніторинг і вдосконалення	Перевірка ефективності заходів, аудит, оновлення політик	Внутрішній аудит, керівництво

Участь у розробці стратегії кібербезпеки організації

1. Керівництво (CEO, CIO, CISO) — визначає пріоритети, ресурси, політику.
2. IT-відділ — технічна реалізація засобів безпеки.
3. Юридичний відділ — забезпечує відповідність законодавству (GDPR, Закон України про захист персональних даних тощо).
4. HR-відділ — політика доступу персоналу, навчання, дисциплінарні заходи.
5. Служба безпеки (фізична та інформаційна) — координація кібер- та фізичних ризиків.
6. Зовнішні консультанти/аудитори — незалежна оцінка ризиків і рекомендації.
7. Усі працівники — людський фактор є найчастішим джерелом інцидентів.

Стратегія має передбачити:

Напрям	Зміст
Політика безпеки	Визначає правила доступу, обробки даних, управління інцидентами
Оцінка ризиків	Каталог ризиків, їх вплив і способи мінімізації
План реагування на інциденти	Хто повідомляє, хто розслідує, як відновити роботу
Забезпечення безперервності (BCP)	Резервні копії, відновлення після катастрофи (DRP)
Контроль доступу	Ролі, паролі, MFA, Zero Trust
Моніторинг і аудит	Постійне спостереження, логування, SIEM
Навчання персоналу	Обов’язкові тренінги з фішингу, роботи з конфіденційними даними
Взаємодія з державними структурами	CERT-UA, НКЦК, правоохоронні органи
Юридичні аспекти	Відповідність нормам закону, зберігання та обробка персональних даних

Формування політик безпеки інформації

Політика безпеки інформації (Information Security Policy) — це офіційний документ, який визначає:

1)які інформаційні ресурси існують у організації;

2)які ризики для них є;

3)як ці ресурси мають бути захищені;

4)хто за що відповідає.

Формування політик — це процес розроблення, затвердження і впровадження таких правил.

Зазвичай політика безпеки включає:

1) Загальні положення — мета, сфера дії, відповідальність.

2) Класифікація інформації — наприклад: конфіденційна, внутрішня, публічна.

3) Доступ до інформації — хто має право бачити/змінювати/копіювати.

4) Паролі та аутентифікація — правила створення, оновлення, MFA.

5) Захист від шкідливого ПЗ — антивірус, оновлення, контроль флешок.

6) Електронна пошта та Інтернет — дозволене використання, обмеження.

- Захист персональних даних — порядок збору, обробки, зберігання.
- Резервне копіювання і відновлення.
- Реагування на інциденти — хто і як повідомляє про порушення.

1) Навчання і відповідальність працівників.

Основні етапи формування політики

Етап	Зміст	Приклад результату
1. Ідентифікація активів	Визначаються всі типи інформації (дані клієнтів, бухгалтерія, листування тощо)	Каталог активів
2. Аналіз ризиків	Виявляються можливі загрози, вразливості, наслідки	Матриця ризиків
3. Формулювання принципів і правил	Описується, як захищається інформація, хто має доступ, як поводитися з даними	Текст політики
4. Узгодження з керівництвом	Політика перевіряється юридично, фінансово, організаційно	Затвердження наказом
5. Впровадження і навчання персоналу	Працівники ознайомлюються з політикою, проходять інструктаж	Підписані ознайомлення
6. Контроль виконання	Перевірка дотримання політики, аудит, реагування на порушення	Звіти безпеки
7. Перегляд і оновлення	Раз на рік або при змінах у законодавстві чи структурі	Оновлена редакція політики

Керування ризиками

Це системний процес виявлення, оцінки, пріоритизації та мінімізації ризиків, що можуть вплинути на конфіденційність, цілісність і доступність інформаційних ресурсів організації. Це не одноразова дія, а постійний цикл управління, який інтегрований у загальну систему управління безпекою інформації (ISMS — Information Security Management System).

Етап	Зміст	Результат
1. Ідентифікація ризиків	Визначення всіх потенційних загроз, вразливостей, активів і сценаріїв атак.	Перелік ризиків для організації
2. Оцінка ризиків (Risk Assessment)	Визначення ймовірності реалізації загрози і можливого впливу (збитків).	Рейтинг ризиків (високий, середній, низький)
3. Аналіз ризиків (Risk Analysis)	Аналіз взаємозв’язків між активами, загрозами та вразливостями; кількісна або якісна оцінка.	Розуміння критичних зон безпеки
4. Обробка ризиків (Risk Treatment)	Розробка стратегії реагування: уникнення, зниження, передача (страхування), або прийняття ризику.	План дій і контролів
5. Моніторинг і перегляд (Risk Monitoring)	Регулярний контроль за змінами у середовищі, технологіях, політиках, інцидентах.	Актуальність карти ризиків
6. Комунікація	Інформування керівництва, співробітників і партнерів про ризики та політику їхнього контролю.	Підвищення культури безпеки

Карта ризиків (Risk Register)

№	**Актив (Asset)**	**Вразливість (Vulnerability)**	**Загроза (Threat)**	**Потенційний вплив (Impact)**	**Ймовірність (Likelihood)**	Рівень ризику **(Risk Level)**	**Поточні контролі (Existing Controls)**
1	**Сервер бази даних клієнтів**	Недостатній контроль доступу, слабкі паролі	Несанкціонований доступ / злам	Витік персональних даних, штрафи, репутаційні втрати	Висока	**Критичний**	Контроль доступу через AD, аудит логів
2	**Пошта співробітників**	Відсутність антифішингових фільтрів, низька обізнаність користувачів	Фішинг / крадіжка облікових даних	Злам облікових записів, поширення шкідливого ПЗ	Середня	**Високий**	Антивірус, базові фільтри спаму
3	**Корпоративна мережа (LAN)**	Непатчені маршрутизатори, застаріле ПЗ	Експлуатація вразливостей, DDoS	Втрата доступу до сервісів	Середня	**Високий**	Брандмауер, IDS/IPS
4	**Хмарне сховище документів**	Надмірні дозволи користувачам	Витік даних через сторонні акаунти	Розкриття конфіденційних файлів	Висока	**Критичний**	Рольова модель доступу
5	**Вебсайт організації**	Вразливість до SQL Injection, XSS	Злам сайту, модифікація контенту	Репутаційна шкода, компрометація користувачів	Висока	**Критичний**	Захист вебсерверу, HTTPS
6	**Резервні копії даних**	Зберігаються на тому ж сервері, що й основні дані	Ransomware / шифрування бекапів	Неможливість відновлення, фінансові втрати	Висока	**Критичний**	Регулярне створення копій
7	**Мобільні пристрої співробітників (BYOD)**	Відсутність MDM, відкрите Wi-Fi-з’єднання	Витік службових даних, крадіжка пристрою	Компрометація облікових записів	Середня	**Високий**	Політика BYOD
8	**VPN-доступ для віддалених працівників**	Використання старих протоколів, відсутність MFA	Несанкціонований доступ	Проникнення в корпоративну мережу	Середня	**Високий**	IPSec VPN
9	**Інформація про контрагентів**	Недостатній контроль над передачею документів	Несанкціоноване розповсюдження	Репутаційні втрати, розрив контрактів	Низька	**Середній**	NDA, контроль електронної пошти
10	**Система моніторингу безпеки (SIEM)**	Неправильна конфігурація кореляційних правил	Невиявлення інцидентів	Порушення SLA реагування	Низька	**Середній**	SIEM працює з базовими налаштуваннями

Нормативно-правові аспекти

Приклади:

- Закон України «Про основні засади забезпечення кібербезпеки України».
- GDPR — регламент ЄС про захист персональних даних.
- NIST Cybersecurity Framework, ISO/IEC 27000 series.
- Внутрішні накази, інструкції, положення про доступ.

Закон України «Про основні засади забезпечення кібербезпеки України»

- визначає правові та організаційні засади забезпечення кібербезпеки, тобто захисту життєво важливих інтересів людини, суспільства, держави у кіберпросторі
- охоплює такі елементи: цілі та напрями державної політики в сфері кібербезпеки, принципи, повноваження органів влади, суб'єктів, об'єктів кібербезпеки
- визначає об'єкти кібербезпеки — наприклад, права людини і громадянина, суспільство, держава, конституційний лад
- передбачає принципи забезпечення кібербезпеки: верховенство права, відкритість, державно-приватне партнерство, розвиток цифрового середовища
- визначає суб'єктів забезпечення кібербезпеки — органи влади, установи, також обов'язки громадян, підприємств
- закон встановлює правову основу: Конституція України, інші закони, міжнародні договори, нормативно-правові акти
- вводить вимоги щодо створення національної системи обміну інформацією про кіберінциденти (зміни 2025 р.)

GDPR (General Data Protection Regulation)

Це загальний регламент Європейського Союзу про захист даних, що набув чинності 25 травня 2018 року. Він регулює збір, обробку, зберігання, передачу та видалення персональних даних фізичних осіб, які перебувають на території ЄС.

Основна мета GDPR - забезпечити контроль людини над її персональними даними і встановити єдині правила їх обробки для всіх країн ЄС, а також для компаній за межами ЄС, якщо вони працюють із громадянами ЄС.

Ключові принципи обробки даних (ст. 5 GDPR)

Принцип	Суть
Законність, справедливість і прозорість	Дані повинні оброблятися чесно, на законних підставах і зрозуміло для суб'єкта.
Цільове обмеження	Дані можна збирати лише для конкретної, визначеної мети.
Мінімізація даних	Збираються тільки ті дані, які необхідні для виконання мети.
Точність	Дані мають бути актуальними та точними; неточні слід виправляти або видаляти.
Обмеження терміну зберігання	Дані не можна зберігати довше, ніж це потрібно.
Цілісність і конфіденційність	Дані повинні бути захищені від несанкціонованого доступу чи знищення.
Підзвітність	Організація повинна бути готова довести, що виконує всі вимоги GDPR.

Права суб’єктів персональних даних (ст. 12–22 GDPR)

Право	Опис
Право на доступ	Людина може дізнатись, які її дані зберігаються і як вони обробляються.
Право на виправлення	Людина може вимагати виправлення неточних або неповних даних.
Право на видалення ("право бути забутим")	Людина може вимагати видалення своїх даних у певних випадках.
Право на обмеження обробки	Тимчасове припинення обробки даних.
Право на переносимість даних	Людина може отримати свої дані у машиночитному форматі та передати іншому оператору.
Право на заперечення	Людина може заперечити проти обробки даних (наприклад, у маркетингових цілях).
Право не бути об’єктом автоматизованого рішення	Заборона рішень, прийнятих виключно автоматично (наприклад, алгоритмом).

Організаційно-технічні аспекти

Передбачають впровадження процедур і систем, що забезпечують безпеку інформаційних ресурсів.

Включають:

- Управління доступом (ідентифікація, автентифікація, авторизація).
- Сегментація мережі, контроль трафіку, резервування.
- Управління оновленнями та патчами.
- Централізований моніторинг (SOC, SIEM).
- Реагування на інциденти (Incident Response).

Управління доступом (Access Management) є одним із базових елементів організаційно-технічного аспекту, який визначає, хто, коли і до чого має право доступу в інформаційній системі. Це сукупність процедур, політик і технологічних засобів, які забезпечують, що доступ до інформаційних ресурсів отримують тільки ті користувачі, яким це дозволено, і лише в межах їхніх повноважень.

Основні етапи управління доступом включають три ключові кроки:

Ідентифікація → Автентифікація → Авторизація

1. Ідентифікація (Identification) - це етап, на якому користувач повідомляє систему про свою особу, тобто представляє себе:

- введення логіну, номера студента або ID користувача;
- зчитування картки доступу;
- сканування відбитка пальця чи RFID-мітки.

Результат: система «знає», хто намагається увійти, але ще не має впевненості.

2. **Автентифікація (Authentication)** - це перевірка достовірності особи, тобто підтвердження ідентифікації.

Способи автентифікації:

Тип	Приклад
Що знає користувач	пароль, PIN-код, секретне запитання
Що має користувач	смарт-карта, токен, смартфон (одноразовий код)
Ким є користувач	біометричні дані: відбиток пальця, розпізнавання обличчя, сітківки ока

3. **Авторизація (Authorization)**

Після автентифікації система визначає рівень доступу користувача: які саме ресурси він може переглядати, змінювати або адмініструвати.

Приклади:

- студент має доступ лише до перегляду власних оцінок;
- викладач може вносити оцінки до журналу;
- адміністратор може призначати користувачам ролі: студент, викладач, тощо.

Це реалізується через

ролі (Role-Based Access Control, RBAC)

атрибути (Attribute-Based Access Control, ABAC).

Сегментація мережі - це розподіл корпоративної мережі на логічні або фізичні підмережі (сегменти), які ізольовані одна від одної за допомогою маршрутизаторів, VLAN, фаєрволів або інших засобів.

Мета:

- обмежити поширення кіберзагроз (наприклад, шкідливого ПЗ або внутрішніх атак);
- мінімізувати наслідки компрометації одного сегмента;
- забезпечити принцип мінімально необхідного доступу (least privilege).

Виділення окремих сегментів для:

- офісної мережі користувачів;
- серверів, сховищ даних, систем адміністрування;
- IoT-пристроїв;
- гостьового Wi-Fi.

Контроль трафіку - моніторинг, фільтрація та аналіз вхідного, вихідного і внутрішнього мережевого трафіку з метою виявлення підозрілих або заборонених дій.

Основні інструменти: Firewall, системи виявлення/запобігання вторгненням (IDS/IPS), системи аналізу мережевого трафіку (NTA), проксі-сервери.

Мета:

- забезпечити контроль за тим, хто, куди і що передає через мережу;
- виявити атаки, спроби витоку даних або зловмисну активність;
- запобігти використанню шкідливих протоколів.

Резервування (Redundancy)

Створення резервних копій ресурсів або паралельних систем, які дозволяють забезпечити безперервність роботи у разі збою, атаки чи втрати даних.

Основні напрями резервування:

- резервування даних — регулярне створення копій баз даних, конфігурацій, файлів;
- резервування інфраструктури — дублювання серверів, маршрутизаторів, ліній зв’язку;
- резервування живлення — UPS, генератори, подвійні лінії електроживлення;
- географічне резервування — зберігання копій у віддалених центрах обробки даних (DR-сайти).

Мета:

- зменшити час простою (downtime);
- гарантувати відновлення після кіберінцидентів або катастроф;
- забезпечити Business Continuity та Disaster Recovery.

Управління оновленнями та патчами має бути систематичним процесом виявлення, тестування, розгортання та контролю оновлень усіх типів програмного забезпечення для усунення вразливостей, помилок і підвищення безпеки.

Мета:

- закрити відомі вразливості, які можуть бути використані хакерами;
- підтримувати сумісність між компонентами систем;
- зменшити ризики зараження шкідливим ПЗ або експлуатації систем через застарілий код;
- забезпечити відповідність стандартам безпеки (ISO/IEC 27001, NIST, CIS тощо).

Основними етапами процесу є:

- інвентаризація: створення переліку всіх IT-активів: ОС, додатків, обладнання;
- моніторинг оновлень та патчів від постачальників (Microsoft, Cisco, Oracle, тощо);
- оцінка ризику: визначення критичності оновлення, його важливості для безпеки;
- тестування: перевірка оновлень спочатку у тестовому середовищі;
- розгортання (деплой): встановлення оновлень на робочих системах, автоматично або вручну;
- верифікація: перевірка успішності оновлення, відсутності конфліктів або збоїв;
- документування: фіксація дати, версії, відповідальної особи, результатів тестування.

Типи оновлень:

- Security patches: виправлення вразливостей безпеки.
- Bug fixes: усунення програмних помилок, що можуть впливати на стабільність.
- Feature updates: додавання нових можливостей.
- Cumulative updates / Service packs: сукупні пакети змін.
- Firmware updates: оновлення мікропрограмного забезпечення обладнання (BIOS, маршрутизатори тощо).

Реагування на інциденти (Incident Response) — це комплекс організаційних, технічних і комунікаційних дій, спрямованих на:
- виявлення інцидента,
- локалізацію інцидента,
- ліквідацію наслідків,
- відновлення нормальної роботи після кіберінциденту.

Це план дій у кризових ситуаціях кібербезпеки, який дає змогу мінімізувати збитки й швидко повернути контроль над системою.

Мета реагування на інциденти:

- мінімізувати наслідки інциденту (збитки, витік даних, простої систем);

- зберегти докази для подальшого розслідування;

- відновити безпечну роботу IT-інфраструктури;

- запобігти повторенню подібних інцидентів у майбутньому.

Типовий цикл реагування:

- підготовка (Preparation): розроблення плану IR, створення команди, навчання персоналу, створення каналів зв’язку.

- виявлення та аналіз (Detection & Analysis): виявлення інциденту за допомогою моніторингу, логів, IDS/IPS, SIEM.

- локалізація (Containment): ізоляція уражених систем, відключення вузла від мережі, обмеження облікових записів.

- усунення (Eradication): видалення шкідливого ПЗ, закриття вразливостей, відновлення нормальної конфігурації, встановлення патчів, зміна паролів, очищення систем.

- відновлення (Recovery): повернення систем до нормальної роботи, перевірка стабільності, відновлення з резервних копій, моніторинг повторних атак.

- аналіз після інциденту (Post-Incident Activity): аналіз причин, оцінка ефективності дій, оновлення політик і процедур.

Людський (соціальний) аспект

Людський або соціальний аспект кібербезпеки є сукупністю факторів, що пов’язані з поведінкою, знаннями, звичками та етичними рішеннями людей, які мають доступ до інформаційних ресурсів організації. Ніякі технічні засоби не здатні забезпечити безпеку, якщо користувачі нехтують встановленими правилами, використовують слабкі паролі, відкривають фішингові листи, не контролюють поширення конфіденційної інформації.

Головні складові людського аспекту

- **Освіченість та обізнаність** визначається рівнем знань користувачів про кіберзагрози і правила безпеки. Необхідне постійне проведення тренінгів щодо фішингу, тестових симуляцій атак.
- **Поведінка користувачів** визначається певними звичками у використанні паролів, електронної пошти, соцмереж. Проблема виникає при використанні одного пароля скрізь, натискані на невідомі посилання.
- **Соціальна інженерія** проявляється в маніпуляціях з боку зловмисників, що використовують довіру людей. Наприклад, дзвінки «від банку», фейкові повідомлення від «колеги».
- **Культура безпеки** вимагає формування системи цінностей і норм поведінки, які орієнтовано на захист інформації. Політика “Security first” запроваджена у всіх підрозділах організації.
- **Відповідальність** полягає в усвідомлені наслідків власних дій у кіберпросторі, повідомлення про інциденти, дотримання політик доступу.

Типові людські помилки, що призводять до інцидентів:

1. Використання простих або повторення паролів.

2. Ігнорування оновлень програмного забезпечення.

3. Перехід за невідомими (шахрайськими) посиланнями або відкриття вкладень у фішингових листах.

4. Передача конфіденційних даних через незахищені канали.

5. Порушення стандартів та політик безпеки. Наприклад, встановлення несанкціонованих та неперевірених застосунків.

6. Недостатня критичність до інформації в соціальних мережах.

Методи зменшення людського фактору в кіберзагрозах

1. Навчання персоналу: регулярні тренінги, симуляції атак та фішингу.

2. Формування культури безпеки: кібербезпека має бути частиною корпоративної культури.

3. Система мотивації потребує заохочення до дотримання правил безпеки. Наприклад, певні нагороди, рейтинги, внутрішні відзнаки.

4. Чіткі політики та інструкції. Кожен має знати, що робити у разі певного інциденту. Це реалізується через безпекові політики та правила, інструкції реагування.

5. Тестування персоналу. За встановленим регламентом виконуються перевірки реакцій на реальні сценарії атак. У роботі застосовують соціально-інженерні тести, контрольні ситуації.

Операційні (процедурні) аспекти

Це практична складова системи управління безпекою, що забезпечує щоденне підтримання належного рівня захисту інформаційних систем. Якщо організаційна політика визначає “що” потрібно робити, то операційні аспекти відповідають за “як” це робиться на практиці.

1. Контроль за оновленнями систем (Patch & Update Management)
Систематичне відстеження, тестування і встановлення оновлень ПЗ, драйверів та операційних систем задля усунення відомих уразливостей, які можуть бути використані зловмисниками.
- Створення графіка регулярних оновлень;
- Тестування оновлень у безпечному середовищі перед розгортанням;
- Автоматизація через системи на кшталт WSUS, SCCM, Ansible чи Puppet;
- Ведення журналу змін для відстеження сумісності та впливу оновлень.

2. Регулярні резервні копії (Backup and Recovery)
Створення копій критичних даних для запобігання їх втраті у разі інцидентів (збоїв, шкідливих атак, людських помилок), що необхідно для відновлення інформації та безперервності бізнес-процесів.
- Використання правил “3–2–1”: 3 копії даних, 2 різних носії, 1 копія поза основним майданчиком;
- Регулярне тестування відновлення даних;
- Захист резервних копій від несанкціонованого доступу та шифрування ransomware;
- Автоматизація процесів резервування.

3. Аналіз журналів подій (Log Management & Monitoring)
Збір, зберігання та аналіз системних і мережевих журналів (logs) для виявлення підозрілих дій, що забезпечує своєчасне виявлення загроз, інцидентів або відхилень у поведінці систем.
- Централізований збір логів через системи типу SIEM (Splunk, ELK, QRadar);
- Встановлення політик журналювання (які події логуються, як довго зберігаються);
- Кореляція подій для виявлення складних атак;
- Автоматичні сповіщення адміністраторів про критичні події.

4. Періодичні аудити безпеки (Security Audits)
Перевірка відповідності існуючих заходів безпеки політикам, стандартам (ISO/IEC 27001, NIST, GDPR) та законодавству задля оцінки ефективності системи захисту, виявлення недоліків, визначення зони ризику.
- Проведення як внутрішніх, так і зовнішніх аудитів;
- Аналіз конфігурацій, доступів, процедур реагування на інциденти;
- Звіти з рекомендаціями та пріоритетами усунення недоліків;
- Регулярність перевірок (щорічно або після значних змін в IT-інфраструктурі).

5. Тестування на проникнення (Penetration Testing)
Імітація дій кіберзлочинців з метою перевірки реальної стійкості системи до атак, виявлення вразливостей до того, як ними можуть скористатись зловмисники.
- Використання спеціалізованих інструментів (Metasploit, Burp Suite, Nmap тощо);
- Проведення тестів “чорної скриньки” (без знань про систему) і “білої скриньки” (з повним доступом);
- Документування знайдених вразливостей та рекомендації щодо їх усунення;
- Частота тестів — не рідше ніж раз на рік або після великих змін у системі.

Комунікаційно-координаційні аспекти

Це система управлінських, організаційних і процедурних заходів, спрямованих на забезпечення узгодженої взаємодії між усіма учасниками процесу кіберзахисту як всередині організації, так і зовнішніми суб’єктами (державні органи, CERT/CSIRT, партнери, постачальники, споживачі послуг).

Мета комунікаційно-координаційного аспекту

- Забезпечення оперативного обміну інформацією про кіберзагрози, інциденти та уразливості.
- Узгодження реакційних дій і пріоритетів між різними підрозділами (IT, безпека, юристи, PR, менеджмент).
- Встановлення каналів взаємодії із зовнішніми суб’єктами кіберзахисту: державними структурами, CERT/CSIRT, партнерами.
- Забезпечення послідовності дій у кризових ситуаціях, щоб мінімізувати наслідки атак.

Внутрішня комунікація - координація дій між підрозділами всередині організації

Підрозділ	Основна роль у комунікації
CISO / IT-безпека	Координує технічне реагування на інциденти, звітує керівництву.
Керівництво (CEO, CIO)	Приймає стратегічні рішення, санкціонує залучення зовнішніх структур.
Юридичний відділ	Оцінює правові наслідки, готує офіційні повідомлення про витік даних.
PR / Комунікаційний відділ	Формує публічні повідомлення, взаємодіє зі ЗМІ, запобігає репутаційним ризикам.
HR / Персонал	Організовує внутрішнє інформування, навчання працівників, дисциплінарні заходи.

Комунікаційно-координаційні аспекти

Основні інструменти:

1. План реагування на інциденти (Incident Response Plan) з визначенням каналів зв’язку та рівнів ескалації.

2. Система внутрішніх сповіщень (alerting, ticketing) — SIEM, SOC, email-сповіщення.

3. Регулярні координаційні наради після інцидентів (post-incident review).

Зовнішня комунікація: передбачає взаємодію із зовнішніми структурами, які допомагають виявляти, аналізувати й реагувати на кіберзагрози.

1. CERT/CSIRT (Computer Emergency Response Team / Incident Response Team): отримання попереджень про загрози, обмін індикаторами компрометації, технічна допомога у реагуванні.

2. Державні органи (Держспецзв’язку, Кіберполіція України): офіційне розслідування інцидентів, фіксацію доказів, забезпечують правову відповідальність.

3. Партнери та постачальники: координація дій у спільних IT-ланцюгах (supply chain security).

4. Міжнародні організації (FIRST, ENISA): участь у спільних програмах обміну кіберінформацією.

Механізми зовнішньої комунікації:

- меморандуми про взаєморозуміння (MoU) з CERT/CSIRT;

- стандартизовані формати обміну інформацією: STIX/TAXII, OpenIOC;

- процедури повідомлення про кіберінциденти, наприклад, обов’язкові звіти у державні органи.