DSPU CYBER SEC

КІБЕРЗАХИСТ ОРГАНІЗАЦІЙ: ІНСТРУМЕНТИ ДЛЯ СТВОРЕННЯ ПОЛІТИК, ПРОВЕДЕННЯ АУДИТІВ І НАВЧАННЯ ПЕРСОНАЛУ

with support from Google.org

ДМИТРО КАРПИН

ДРОГОБИЧ
2025

ЗМІСТ

1.1 НАВІЩО ОРГАНІЗАЦІЇ КІБЕРЗАХИСТ?

Понад 90% цифрових інцидентів, що трапляються в організаціях, не пов'язані з «хакерами у чорних худі», які зламують системи з іншого боку планети. Насправді, ці інциденти — результат звичайної неуважності, невстановлених оновлень, відкритого доступу до файлів, одного "не того" натискання на посилання в електронному листі. І що найважливіше — цифрові ризики стосуються всіх організацій, а не лише банків, армії чи великих IT-компаній.

Уявімо невелику громадську організацію, яка проводить тренінги. Вона має Google-диск зі списками учасників, копіями паспортів для проєкту, результати опитувань, фото з заходів. Один співробітник випадково відкриває доступ "усім у мережі", і хтось сторонній зчитує ці дані. Або хтось втратить ноутбук з відкритими документами. Це — порушення конфіденційності, за яке несе відповідальність організація. Те саме — у школі, де викладач веде облік успішності учнів у Google-таблиці, або у державній установі, яка отримала фішингового листа, схожого на запит з державного порталу.

Кіберзахист — це не щось додаткове до діяльності, це її частина. Він починається не з дорогих антивірусів, а з культури відповідального поводження з даними, чітких правил доступу до інформації, і — що найважливіше — розуміння працівниками того, що вони є частиною захисту.

Цифрова присутність: як ми стаємо вразливими

Сучасна організація працює у цифровому середовищі щодня. Ви надсилаєте запрошення на події, збираєте відповіді у Google Forms, ведете акаунти у Facebook та Instagram, завантажуєте документи у хмару, користуєтесь Zoom, Canva, Miro, Trello, Moodle, поштою, інтернет-банкінгом.

Але кожен цей інструмент — це не лише зручність, а й точка можливої атаки або помилки:

- Google Forms: створена форма автоматично відкривається для редагування всіма — і в ній вказані персональні дані.
- Zoom: акаунт не має паролю, бо використовується через Google SSO, а хтось у команді не поставив двоетапну перевірку.
- Instagram: акаунт ведеться з телефону одного з волонтерів, у якого пароль — дата народження, і відсутній бекап.

Інформація втрачається не тому, що її вкрали — а тому, що ніхто не передбачив ситуації, коли її можуть побачити сторонні. Не існувало жодного мінімального плану: хто має доступ, як його видавати, що робити в разі втрати пристрою, як діяти в ситуації, коли акаунт зламано або лист виглядає підозріло.

Що ми захищаємо насправді?

У кібербезпеці часто кажуть: ми захищаємо не комп'ютери, а цінності. Бо за всіма таблицями, файлами, доступами — стоять люди, їхня довіра, спільні цілі, проєкти, гроші, час.

Захист потрібен, щоби:

- не зникла база учасників проєкту, на яку витрачено місяці роботи;
- не викрали дані дітей, чиї фото публікувалися у звітах;
- не було зламано акаунт організації і не поширили через нього фальшиві заклики;
- не “втекли” банківські документи до невідомих третіх осіб;
- не була втрачена довіра донорів, партнерів, батьків чи громад.

Типові наслідки кіберінцидентів в організації

Тип втрати	Можливі наслідки
Дані працівників (контакти, паспорти)	Порушення законодавства, скарги, внутрішні конфлікти
Публічні акаунти (соцмережі, пошта)	Розсилка фейкових повідомлень, репутаційні ризики
Фінансові документи	Можливість шахрайства, підробка договорів
Освітні чи робочі матеріали	Знищення чи блокування результатів роботи, зрив заходів
Фото/відео з подій	Використання в чужих цілях, конфлікти з батьками, учасниками

Навіть один інцидент може знищити роки довіри. Саме тому кіберзахист має починатися не з IT, а з усвідомлення.

Захист — це не система, а звичка

Часто організації сприймають безпеку як разову подію: “Ми поставимо пароль і все”. Насправді ефективний кіберзахист — це:

- звичка не залишати акаунти відкритими;
- звичка перевіряти, кому ви відкрили доступ;
- звичка не натискати одразу на посилання в листі;
- звичка діяти за планом, коли щось іде не так.

Ці звички формуються через політики, навчання, інструкції та приклади, про які і буде йтися у наступних розділах. Але саме зараз — у цьому пункті — найголовніше: визнати, що це потрібно саме вам, саме тут і саме зараз, незалежно від того, скільки працівників у вас, яка система, і наскільки “простими” здаються ваші задачі.

1.2 ЩО ТАКЕ “ІНФОРМАЦІЙНІ АКТИВИ” ОРГАНІЗАЦІЇ

У класичному розумінні активи організації — це те, що має матеріальну цінність: офіс, меблі, обладнання, документи, кошти. Але в цифровому світі з’явилася ще одна категорія активів — інформаційні, і їх цінність іноді значно вища. Ці активи часто невидимі, але саме вони найчастіше стають об’єктами атак, помилок, витоків чи втрат.

Що вважати інформаційним активом?

Інформаційний актив — це будь-який елемент цифрового середовища організації, що має значення для її функціонування, розвитку або репутації. Це не лише дані як такі, а й доступи до них, канали, через які вони передаються, і люди, які мають до них стосунок.

Приклади:

- *Облікові записи — корпоративна пошта, акаунти в Google Workspace, Zoom, CRM, Moodle, Telegram-ботах.*
- *Хмарні сховища — Google Drive, Dropbox, OneDrive з документами, таблицями, архівами.*
- *Бази контактів — списки учасників, клієнтів, підписників, анкет, батьків учнів.*
- *Цифровий контент — фото, відео, презентації, записані трансляції заходів.*
- *Фінансові файли — кошториси, бюджети, скан-копії документів.*
- *Оцінювання, анкети — результати опитувань, відгуки, зворотний зв'язок.*
- *Інформація про працівників — внутрішні організаційні документи, посади, графіки.*

Все, що створено, зібрано або надіслано в цифровому вигляді — і що є важливим для роботи, — слід вважати інформаційним активом.

Як виглядають ці активи у реальному середовищі?

Середовище	Типовий актив	Приклад використання
Школа	Таблиця з оцінками	Google Sheets на диску класного керівника
Громадська Організація	Фото з заходів	Архів на Dropbox для звітування донору
Малий бізнес	Контактна база	Excel-файл із телефонами клієнтів
Установа	Доступ до Zoom	Загальний логін без обмеження MFA
ВНЗ	Moodle	Завантаження контрольних робіт учнів

Хто відповідає за ці активи?

Найчастіша помилка — вважати, що IT-відділ або один "відповідальний за безпеку" контролює все. Але насправді інформаційні активи належать структурним одиницям і їхнім користувачам.

Наприклад:

- *Учитель, який створив Google Форму — відповідає за її налаштування і безпечне поширення.*
- *Координатор проєкту, який зберігає скани документів — має контролювати, хто має до них доступ.*
- *Менеджер, що веде сторінку у Facebook — повинен захистити акаунт двофакторною автентифікацією.*

Без чіткої ідентифікації активів і відповідальності за них будь-яке порушення стає безіменним — а отже, некерованим.

Класифікація активів: для чого вона потрібна?

Важливо не просто знати, які активи є, а й розуміти:

- які з них найчутливіші;
- хто має до них доступ;
- як вони захищені;
- як часто оновлюються чи змінюються.

Категорія	Приклад	Рівень ризику
Публічні активи	Презентація для заходу	Низький
Обмежені для внутрішнього використання	План навчання, контакти працівників	Середній
Конфіденційні	Дані учасників, скани документів	Високий
Критичні	Доступ до банківських операцій	Дуже високий

В рамках внутрішнього аудиту чи створення політик — перелік активів має бути основою: що є, кому належить, як використовується, як захищається.

Що відбувається, коли актив не захищено

1. Відкритий доступ до таблиці з персональними даними → Витік → Репутаційна шкода.
2. Відсутність бекапу навчальних матеріалів → Випадкове видалення → Зрив курсу.
3. Спільний пароль до пошти → Компрометація → Втрата контролю над акаунтом.
4. Старі файли з доступами → Витік → Доступ колишнього співробітника до критичних документів.

Підсумок: Інформаційні активи — це не тільки технічна категорія. Це фундамент повсякденної цифрової діяльності. Їх ідентифікація — перший крок до кіберзахисту.

1.3 НАЙТИПОВІШІ ЦИФРОВІ ЗАГРОЗИ

Коли говорити про кіберзагрози, уявлення більшості обмежуються фільмами: хакер “ламає сервер”, лунають сирени, зникає світло. Але насправді реальні загрози набагато буденніші, і саме через це — небезпечніші. Вони діють тихо, повільно, іноді залишаються непоміченими, доки не завдають шкоди.

Людський фактор: найслабша ланка

У 8 із 10 випадків кіберінцидентів причина — не система, не вірус, не програма, а людина:

- відкрив лист із вкладенням “інвойс”;
- забув вийти з облікового запису;
- зробив Google-документ “доступним для всіх”;
- надіслав пароль у чат без шифрування;
- завантажив щось із “незрозумілого” сайту;
- дав доступ до акаунту новому колезі — і не відкликав його, коли той пішов.

Неуважність, поспіх і необізнаність — ось головні союзники кіберзагроз.

Типові загрози: просто і по суті

Загроза	Як це виглядає	Що може статись
Фішинг	Лист виглядає як повідомлення від банку, пошти або знайомої служби	Користувач вводить свої логін/пароль — їх крадуть
Malware (віруси)	Завантажений “документ” містить шкідливий код	Дані шифруються, крадуться або пристрій стає частиною бот-мережі
Втрати або викрадення пристроїв	Загублений ноутбук, телефон або флешка	Витік документів, доступ до акаунтів без пароля
Використання слабких паролів	“123456”, “qwerty”, дати народження	Атака методом перебору (brute force) — злам акаунтів
Відсутність резервного копіювання	Всі файли лише в одному місці	Один збій, вірус або випадкове видалення — і дані втрачені
Незахищені хмари	Файли в Google Drive відкриті “для всіх із посиланням”	Дані індексуються пошуковиками, доступ — для будь-кого
Старі акаунти	Доступи залишились у колишніх працівників	Можливість навмисного чи випадкового втручання
Неперевірені додатки	Установлення додатку з Play Market “для сканування”	Витік контактів, повідомлень або паролів
Соціальна інженерія	Дзвінок “від підтримки” із запитом надати код	Користувач віддає контроль над обліковим записом

Практичні приклади загроз

Приклад 1:

Школа завантажує список учнів на Google Диск, щоб поділитися з учителями. Хтось відкриває доступ "для всіх із посиланням". Через тиждень хтось знаходить файл у пошуковику.

Наслідки: витік персональних даних, скарги батьків, ризик перевірки.

Приклад 2:

Працівник установи отримує лист з темою “Оплата за січень”. Вкладення — архів. Він відкриває файл, після чого ноутбук починає працювати повільніше. За кілька днів дані зашифровані, а на екрані — повідомлення про викуп.

Наслідки: втрата документів, паралізована діяльність, паніка.

Приклад 3:

Громадська організація передає акаунт Instagram новому працівнику без зміни пароля. Через місяць працівник звільняється, але акаунт залишається “на ньому”. Через рік хтось видаляє всі пости і змінює логін.

Наслідки: втрата аудиторії, довіри, інструменту для комунікації.

Загрози “всередині” — не завжди злісні

Варто пам’ятати: не кожна внутрішня загроза — це саботаж. Іноді це звичайна помилка, яка сталася через відсутність правил або інструкцій:

- Працівник надіслав документ не тому адресатові.
- Студент мав доступ до папки адміністрації, бо структурування не було.
- Асистент скопіював папку, не знаючи, що там конфіденційні матеріали.

Правильні інструкції, обмеження доступу та навчання персоналу — ключ до зменшення таких ризиків.

Як виявити цифрову загрозу?

Не завжди атака виглядає як кіно. Часто — це дрібна незвичність:

- на пошті з'явився підозрілий лист;
- аккаунт вийшов зі сторінки сам;
- зникають файли з диску;
- смартфон "пише" щось без вас;
- з'явилися нові адміністратори в акаунтах.

Реагуйте на незвичне. І не соромтесь звертатись до відповідальної особи.

Підсумок:

Цифрові загрози — це не фантастика. Це щоденні події, які можна вчасно зупинити, якщо розуміти механізми.

1.4 ХТО ВІДПОВІДАЄ ЗА БЕЗПЕКУ В ОРГАНІЗАЦІЇ?

У розмовах про безпеку часто виникає хибне уявлення: мовляв, якщо в організації немає "айтішника" або IT-відділу, то й кібербезпека — "не наша справа". Насправді ж вона стосується кожного, незалежно від посадової інструкції, технічних навичок чи обов'язків.

Відповідальність = колективна культура + конкретні ролі

Усі працівники взаємодіють з інформацією. Хтось надсилає листи з персональними даними, хтось зберігає таблиці, хтось веде соцмережі, хтось керує доступом до Zoom чи Google Meet.

Якщо кожен працівник сприйматиме цифрову безпеку як щось "вище за його обов'язки", то жодна система не встоїть. Як у фізичній безпеці — двері із замком не допоможуть, якщо їх залишили відкритими.

Тому варто говорити не про одну людину, а про розподіл відповідальностей, адаптований під структуру організації.

Ролі в сфері безпеки: від керівника до волонтера

Роль	Обов'язки у сфері кіберзахисту
Керівник	Затверджує політики, делегує повноваження, підтримує культуру безпеки
Адміністратор/IT-фахівець	Забезпечує налаштування систем, веде облік доступів, впроваджує технічні рішення
Координатори/менеджери	Контролюють доступи до спільних ресурсів, слідкують за виконанням правил у своїх командах
Уповноважена особа з захисту даних (DPO)	Відповідає за обробку персональних даних, перевіряє відповідність політик законодавству
Усі працівники	Виконують вимоги політик, повідомляють про підозрілі випадки, беруть участь у навчаннях
Волонтери, підрядники	Отримують доступ лише до потрібного мінімуму, діють за окремими інструкціями

У малих командах ролі можуть поєднуватись

Більшість невеликих організацій, особливо в громадському секторі або освітній сфері, не мають ресурсів на окремі посади для безпеки. Але навіть у таких випадках відповідальність не повинна розмиватися. Її можна зафіксувати чітко:

- Керівник призначає відповідального з числа постійних працівників.
- Координатори програм відповідають за захист у межах своїх проєктів.
- IT-підрядник чи консультант має інструкцію з дій у разі інциденту.

Навіть у групі з 3 людей можна і потрібно чітко розділити, хто що робить у сфері цифрової безпеки.

Як зафіксувати відповідальність на практиці?

1. Політика доступів і розподілу ролей.

Простий документ, де вказано, хто має доступ до яких акаунтів, хто керує ними, хто контролює зміну паролів.

2. Список адміністраторів.

Для кожного цифрового інструменту — таблиця з відповідальними. Наприклад:

Інструмент	Хто адмініструє	Резервна особа
Google Workspace	Іван Іванович	Олена Петрівна
Сторінка у Facebook	PR-менеджер	Керівник
CRM-система	Технічний консультант	Координатор проєкту

3. Інструкція для нових працівників.

Окремий лист з правилами: які паролі, які сервіси, що не можна робити, як повідомити про інцидент.

4. Призначення уповноваженої особи з кіберзахисту.

Не обов'язково повна посада — достатньо формального рішення або внутрішнього наказу.

Що відбувається, коли "ніхто не відповідає"

Доступ до чутливих даних отримують сторонні.

Про інцидент дізнаються надто пізно або взагалі не повідомляють.

Всі чекають, поки "хтось" виправить ситуацію.

Втрачаються файли, акаунти, інформація — без надії на відновлення.

У цифровій безпеці відсутність відповідального — це вже загроза.

Висновок

Розподіл відповідальності — це не бюрократія, а інструмент управління ризиками. Він дозволяє швидко реагувати, уникати конфліктів і планувати дії. Створення простої, але зрозумілої моделі: хто, за що і коли відповідає — один з найважливіших кроків до сталої цифрової культури.

1.5 ПРИНЦИПІВ ЗДОРОВОГО ЦИФРОВОГО СЕРЕДОВИЩА

Коли ми говоримо про безпеку в цифровому середовищі, на думку спадають складні системи, “антивіруси” чи технічні налаштування. Насправді, фундамент безпеки — це поведінка людей, які щодня працюють із цифровими інструментами.

Цей підрозділ — не про формальні політики. Він про здоровий глузд у цифровому світі, який можна перетворити на звичку.

Принцип сильних паролів і багатофакторної автентифікації

Пароль на кшталт 123456, qwerty або навіть ivan2023 — як двері без замка. Такі паролі зламуються автоматичною програмою за лічені секунди. А ще гірше — якщо один і той самий пароль використовується всюди.

Практика:

- Створюйте унікальні паролі для кожного сервісу.
- Додавайте багатофакторну автентифікацію (MFA) — наприклад, підтвердження в додатку або SMS.
- Використовуйте менеджери паролів (1Password, Bitwarden, Google Password Manager).

Рекомендація: MFA вмикати обов’язково на пошту, соцмережі, банкінг, доступи до документів.

Принцип регулярного оновлення

Більшість атак використовують вразливості, які вже давно виправлені — але працівники ще не оновили свої пристрої чи додатки.

Приклад:

“Витік” у старій версії Zoom дозволяє стороннім підключатись до відеодзвінків без запрошення.

Що робити:

Увімкнути автоматичне оновлення програм і браузера.

Не ігнорувати повідомлення “оновити зараз”.

Регулярно перевіряти, чи смартфон має останню версію ОС.

Принцип резервного копіювання

Один день без резервної копії — це день, який може коштувати вам місяці роботи. Найчастіше втрати трапляються через випадкове видалення, поломку пристрою або шкідливе ПЗ (наприклад, вірус-вимагач).

Як впровадити:

- Вибрати, які документи критично важливі.
- Створити копію на іншому хмарному диску або зовнішньому носії.
- Встановити автоматичне резервне копіювання щотижня.

Рекомендація: Копія повинна бути відокремлена від основного облікового запису.

Принцип обмеження доступу

Не всі мають бачити все. Ідея “зробимо доступ відкритим, бо так зручніше” часто обертається витоком. Кожен працівник повинен мати лише ті права, які необхідні для виконання його завдань.

Підхід:

- Встановлюйте “рівні доступу”: перегляд, коментування, редагування.
- Не передавайте логін/пароль — створюйте індивідуальні акаунти.
- Регулярно перевіряйте, хто має доступ до чутливих папок.

Інструменти: Google Workspace → “Спільні диски” з контрольованим доступом.

Принцип безперервного навчання

Цифрове середовище змінюється. З’являються нові сервіси, методи атак, інтерфейси. Те, що вважалося безпечним у 2020-му — може вже не працювати у 2025-му.

Що варто робити:

- Короткі інструктажі для нових працівників.
- Щорічні оновлення політик і нагадування.
- Симуляції інцидентів — “що робити, якщо отримали фішинговий лист”.

Навіть короткий 15-хвилинний тренінг може зменшити ризики в рази.

Принцип цифрової гігієни

У цифровому світі, як і в реальному, діють правила гігієни. Не варто зберігати “все під одним дахом”, переходити за будь-якими посиланнями чи відкривати “ліві” сайти.

Що входить:

- Не підключатися до невідомих Wi-Fi без VPN.
- Не вставляти чужі флешки у службовий комп’ютер.
- Завантажувати програми лише з офіційних джерел.
- Не писати логіни/паролі в Google Docs або чатах.

Принцип відкритості щодо інцидентів

Найгірше, що може статися після проблеми — мовчання. Інциденти не потрібно приховувати, їх потрібно фіксувати, аналізувати і використовувати як матеріал для навчання.

Культура реагування:

- “Якщо сумніваєшся — повідом.”
- “Якщо зробив помилку — скажи одразу.”
- “Якщо отримав дивне повідомлення — не відкривай, але передай.”

Усі працівники повинні знати, куди і до кого звертатися у разі інциденту.

Підсумок

Ці сім принципів не потребують технічної освіти. Вони — про звички, які формуються через приклади, політики та підтримку. Якщо в організації вони є — усі інші інструменти (антивіруси, паролі, шаблони) працюють. Якщо немає — жодна система не гарантує безпеку.

1.6 БАЗОВИЙ ЧЕК-ЛИСТ ДЛЯ ОЦІНКИ СТАНУ БЕЗПЕКИ

Перш ніж переходити до політик, шаблонів і технічних дій, варто дати собі відповідь на просте запитання: а на якому рівні ми зараз? Саме для цього створено короткий базовий чек-лист, що допоможе виявити прогалини та визначити пріоритети.

Заповнення цього інструмента не потребує технічної освіти. Він створений для керівників, координаторів, адміністраторів і всіх, хто працює з інформацією в організації.

Чек-лист (Самооцінка)

Позначте «✓» або «✗» навпроти кожного твердження. Ведеться підрахунок балів — чим більше «✓», тим краще базовий рівень безпеки.

№	Питання	Так ✓ / Ні ✗
1	Ми маємо список усіх цифрових інструментів, які використовує організація	
2	У кожного інструменту є визначений адміністратор	
3	Усі ключові акаунти захищено двофакторною автентифікацією (MFA)	
4	У нас є окрема політика або правило щодо створення надійних паролів	
5	Доступ до документів надається за мінімально необхідним принципом	
6	Персональні дані зберігаються в захищених і контрольованих папках	
7	Є резервні копії критично важливих даних	
8	Ми маємо процедуру на випадок цифрового інциденту (наприклад, злам, вірус)	
9	Після звільнення працівникам відключається доступ до акаунтів	
10	Організація проводила базове навчання з цифрової безпеки для працівників	
11	Нові працівники отримують пам’ятку з правилами цифрової гігієни	
12	В організації призначено відповідального(-у) за інформаційну безпеку	
13	Публікації у соцмережах відбуваються з акаунтів, які мають резервний доступ	
14	Вся діяльність з обробкою персональних даних відповідає чинному законодавству	
15	Ми маємо список інформаційних активів (що, де, хто має доступ)	

Підрахунок результатів

13–15 ✓ — Ваша організація має добрий стартовий рівень цифрової культури. Переходьте до поглиблення політик і навчання.

8–12 ✓ — Основи присутні, але варто вжити заходів щодо слабких місць.

4–7 ✓ — Безпека потребує серйозного посилення. Почніть з політик, навчання і призначення відповідальних.

0–3 ✓ — Ваша організація дуже вразлива. Рекомендується негайно впровадити базовий мінімум: захист паролів, MFA, навчання.

Цей чек-лист можна використовувати:

- як стартову оцінку перед аудитом;
- як вступ до внутрішнього тренінгу;
- як додаток до презентації на тему цифрової гігієни;
- для щорічної перевірки стану безпеки.

Підсумок

Розділ «Основи кіберзахисту в організації» дає вам не лише розуміння термінів, а й практичну базу — з чого почати. У наступних розділах ми будемо будувати системність: політики, шаблони, навчання, аудит, реагування. Але саме цей розділ — фундамент. І якщо його буде засвоєно — усі інші кроки стануть логічними й реалістичними.

ЩО ТАКЕ ПОЛІТИКА БЕЗПЕКИ ТА НАВІЩО ВОНА

Політика безпеки — це формалізований документ, який визначає правила поведінки, дозволені та заборонені дії, відповідальність і технічні вимоги для забезпечення інформаційної безпеки в організації. Вона створює спільні рамки для всіх: керівництва, технічного персоналу, звичайних користувачів, — і дозволяє діяти послідовно у звичайних умовах та у разі кіберінцидентів.

У багатьох організаціях безпека залишається на рівні "усної домовленості": не відкривай підозрілі листи, не передавай пароль, оновлюй комп'ютер. Проте без письмово закріпленої політики це не працює. Коли відбувається витік даних, важливо мати чіткі відповіді:

Хто був відповідальний за доступ до файлів?

Чи був заборонений доступ із домашніх пристроїв?

Яка дія є порушенням, а яка — ні?

Які заходи вже вжиті?

Політика безпеки допомагає:

- Упорядкувати роботу: користувач знає, що можна, а що — ні;
- Захистити дані: визначаються вимоги до паролів, оновлень, зберігання;
- Зменшити ризики: більшість атак відбуваються через людський фактор;
- Дотримуватися законодавства: наприклад, захист персональних даних;
- Знати, як діяти у разі інциденту;
- Побудувати довіру: до працівників, до партнерів, до клієнтів.

Політика — це не складний юридичний документ. Це набір зрозумілих і адаптованих для вашої організації правил. У школі це буде один формат, в офісі — інший, у громадській організації — ще інший. Але базові принципи однакові: обмеження доступу, відповідальність, резервне копіювання, навчання.

2.1 ПОЛІТИКА СТВОРЕННЯ ТА УПРАВЛІННЯ ПАРОЛЯМИ

Для чого потрібна:

Щоб кожен користувач розумів, які паролі допустимі, як їх зберігати, як змінювати, і що заборонено.

Коли застосовується:

При створенні акаунтів, видачі доступів, навчанні нових співробітників, у разі інцидентів.

Типовий шаблон політики:

Політика паролів в організації

1. Усі паролі повинні містити не менше 10 символів, включаючи цифри, великі та малі літери.

2. Заборонено використовувати імена, дати народження, слова з довколаорганізаційного середовища.
3. Для всіх важливих акаунтів обов'язкове увімкнення двофакторної автентифікації.
4. Паролі не можна передавати іншим особам усно, в чатах або на папері.
5. Рекомендується використовувати менеджер паролів (Bitwarden, Google Password Manager).
6. При виявленні інциденту паролі мають бути змінені негайно.
7. Зміна паролів здійснюється не рідше одного разу на 6 місяців (для критичних акаунтів — щоквартал).

Як адаптувати:

У школі — можна пояснити це як "набір правил для акаунтів в Google Classroom та e-mail". У громадській організації — як "порядок обліку і доступу до акаунтів Google, Zoom, Canva, Facebook".

2.2 ПОЛІТИКА КЕРУВАННЯ ДОСТУПАМИ

Для чого потрібна:

Щоб знати, хто має доступ до яких ресурсів і як ці доступи регулюються.

Ситуації застосування:

- Прийняття/звільнення працівників
- Початок/завершення проєктів
- Надання тимчасового доступу

Типові положення політики:

Політика доступів в організації

1. Доступ до документів, акаунтів і сервісів надається за принципом "мінімально необхідного рівня".
2. Адміністратор відповідає за створення, зміну та відкликання доступів.
3. При звільненні працівника доступи анулюються не пізніше 24 годин.
4. Створюється перелік ключових доступів із відповідальними особами (Google Диск, соцмережі, Zoom тощо).
5. Кожен користувач має особистий акаунт (спільні акаунти допускаються лише у виняткових випадках).

Примітка: Додатково до політики рекомендується вести таблицю доступів, яку оновлюють щомісяця.

2.3 ПОЛІТИКА ВИКОРИСТАННЯ ЕЛЕКТРОННОЇ ПОШТИ ТА ХМАРНИХ СЕРВІСІВ

Навіщо це потрібно?

Електронна пошта — один із найбільш використовуваних і водночас найвразливіших інструментів організації. Через неї надсилаються документи, паролі, скани, дані

учасників, звіти, заявки. Часто вона прив'язана до інших сервісів: Google Диску, Zoom, Moodle, Canva, банківського акаунту.

Хмарні сервіси — це не просто "місце для зберігання". Це — центральна точка цифрової взаємодії: туди завантажуються робочі файли, таблиці, архіви, медіа. Без чітких правил пошта стає джерелом фішингу, а хмара — вітриною конфіденційної інформації.

Типові загрози:

- Випадкове надсилання листа не тому одержувачу
- Завантаження конфіденційного документа в загальнодоступну папку
- Автоматичне перенаправлення пошти на приватну скриньку
- Випадкове видалення або зміна критично важливого файлу

Політика використання електронної пошти та хмарних сервісів

1. Уся офіційна цифрова комунікація здійснюється через службову пошту (на кшталт @orgname.org або Gmail-акаунти, що адмініструються організацією).
2. Заборонено використовувати особисту пошту для надсилання або отримання:

- документів з персональними даними,
- робочих звітів,
- даних доступу,
- фінансових файлів.

3. Усі важливі документи зберігаються на хмарному сховищі, доступ до якого контролює призначений адміністратор.
4. Файли на Google Drive/Dropbox/OneDrive не повинні бути доступні "для всіх з посиланням", окрім випадків публічного розповсюдження.
5. Для файлів з обмеженим доступом використовуються рівні прав:

- "Перегляд" для ознайомлення,
- "Коментування" для зворотного зв'язку,
- "Редагування" лише за потреби.

6. Усі акаунти повинні бути захищені двофакторною автентифікацією.
7. Заборонено використовувати автоматичне перенаправлення пошти на зовнішні адреси без погодження.
8. Архів важливих листів і файлів повинен створюватись регулярно (раз на місяць) і зберігатись у безпечному місці.

Практична порада: В окремому файлі рекомендується ввести перелік основних робочих хмар і доступів — хто адміністратор, хто має права перегляду.

Як адаптувати до невеликих організацій:

- У школі: стосується Google Classroom, Drive і шкільної пошти.
- У Громадських організаціях: охоплює Google Диск із проєктними файлами, пошту для комунікації з донорами.
- У бібліотеці чи держустанові: може поширюватися на Microsoft Outlook, документообіг через хмару та службові акаунти.

Простий варіант: створіть коротку інструкцію для працівників на 1 аркуш:

– як не зберігати все на робочому столі;

– як правильно надати доступ до файлу;

– як не загубити листи з архівом звітів.

2.4 ПОЛІТИКА РОБОТИ З ПЕРСОНАЛЬНИМИ ДАНИМИ

Чому це важливо?

Практично всі організації збирають, зберігають або обробляють персональні дані. Це може бути:

- список учасників події з телефонами;
- анкета реєстрації на тренінг;
- скани документів;
- база контактів донорів або партнерів;
- сторінки учасників на платформі.

Персональні дані — це не тільки ПІБ. Це будь-яка інформація, за якою можна ідентифікувати людину. Українське законодавство, як і європейські норми (GDPR), передбачає відповідальність за порушення у сфері їх захисту.

Типові ризики:

- Витік списку учасників події з телефонами через відкритий Google-документ;
- Відправлення сканів паспортів у чат без шифрування;
- Доступ до даних мають особи, які не повинні його мати;
- Відсутність погодження на збір даних у формі реєстрації.

Шаблон політики: персональні дані

Політика обробки персональних даних

1. Організація зобов’язується збирати лише ті персональні дані, які необхідні для її діяльності.
2. Перед збором даних (онлайн-форма, опитування тощо) обов’язково вказується мета обробки і спосіб зберігання.
3. Дані зберігаються лише протягом часу, необхідного для мети, з якою їх було зібрано.
4. Усі особи, які мають доступ до персональних даних, повинні бути офіційно уповноважені та ознайомлені з цією політикою.
5. Заборонено передавати персональні дані третім сторонам без згоди особи, крім випадків, передбачених законом.
6. Після завершення обробки дані повинні бути видалені або знеособлені.
7. Всі бази даних мають бути захищені паролем і, за можливості, шифруванням.
8. У разі інциденту (витоку, втрати, несанкціонованого доступу) організація повідомляє про нього відповідні органи і вживає заходів щодо мінімізації шкоди.

Окремий документ: “Згода на обробку персональних даних” — підписується в електронній або письмовій формі.

Практична адаптація:

- У школі — форми з персональними даними учнів/батьків обробляються через захищений Google Form + Диск із обмеженим доступом.
- У Громадських організаціях — перед опитуванням додається текст про мету збору, згоду та термін зберігання.
- У тренінговому центрі — реєстрація на події передбачає згоду на обробку даних у формі.

Рекомендовані кроки:

Провести інвентаризацію персональних даних: які дані ви зберігаєте, де, скільки часу.

Створити таблицю доступів: хто має доступ до яких масивів даних.

Розробити шаблон згоди — з коротким, зрозумілим формулюванням.

Перевірити всі форми на сайті — чи є там згода і контакт для запитів.

Приклад згоди:

"Я, ПІБ, даю згоду ГО “Х” на обробку моїх персональних даних з метою участі в освітньому заході. Згода діє протягом терміну реалізації проєкту, після чого дані будуть видалені."

Висновок

Обробка персональних даних — це не тільки вимога законодавства, але й питання довіри. Коли учасники, працівники, партнери бачать, що їхня інформація у безпеці — це зміцнює репутацію організації.

2.5 ПОЛІТИКА РЕАГУВАННЯ НА ІНЦИДЕНТИ

Чому це критично важливо?

У кожної організації можуть трапитися інциденти: фішинг, вірус, викрадення пристрою, витік документа, підозрілий лист, злам акаунта. Питання не в тому, "чи це трапиться", а "чи готові ми діяти правильно, коли це станеться".

Без політики:

- працівники мовчатимуть — бо не знають, кому і що повідомити;
- організація втратить цінну інформацію — і не відновить її;
- репутаційні та юридичні наслідки можуть бути серйозними.

Типові сценарії інцидентів:

- Отримано лист із вкладенням, після чого ноутбук "підвисає"
- Хтось випадково зробив загальнодоступною папку з персональними даними
- Телефон працівника, на якому був робочий акаунт, загублено
- Доступ до соцмережі змінено сторонньою особою

Шаблон політики: реагування на інциденти

Політика реагування на інциденти

1. Визначення інциденту:

Інцидент — будь-яка подія, яка потенційно ставить під загрозу безпеку даних, систем чи облікових записів. Наприклад:

- злам акаунта;
- втрата пристрою з даними;
- підозріла активність в електронній пошті;
- підозрілий лист або вкладення;
- витік персональної інформації.

2. Хто відповідає:

- Працівник, який помітив інцидент, негайно повідомляє відповідального за безпеку.
- У разі відсутності відповідального — безпосередньому керівнику або адміністратору.

3. Негайні дії (для всіх):

- Не відкривати підозрілі файли або посилання.
- Вийти з акаунта або тимчасово заблокувати сесію.
- Якщо йдеться про втрату пристрою — повідомити якомога швидше.
- Змінити паролі на критичні облікові записи.

4. Дії відповідального за безпеку:

- Фіксує інцидент (час, що сталося, хто повідомив, що зроблено).
- Блокує доступи або тимчасово обмежує доступ до даних.
- Оцінює масштаб загрози.
- Розробляє план дій: відновлення, сповіщення, запобігання.

5. Повідомлення третіх сторін:

Якщо інцидент стосується персональних даних або партнерських зобов'язань — повідомляються відповідні особи/органи.

6. Документування:

Створюється короткий звіт: дата, опис, вжиті заходи, наслідки. Цей звіт зберігається окремо.

7. Післяінцидентне навчання:

Проводиться короткий брифінг або поширюється інструкція, щоб уникнути повторення подібного.

Формат для фіксації інциденту

Дата/Час	Подія	Хто виявив	Що зроблено	Коментар
12.06.25 09:40	Отримано фішинговий лист	А.І. Петренко	Видалено, пароль змінено, MFA активовано	Пошта Gmail

Практична адаптація:

- У ГО: достатньо мати Google-таблицю з записами інцидентів та 1 відповідального з чітким планом.
- У закладі освіти: вказати для вчителів, куди звертатися в разі фішингу, зникнення документів.
- У проєкті: діяти згідно із внутрішньою процедурою, додати покрокову інструкцію у форму Google.

Поради:

Створіть «антивітрину» для працівників: Що робити, якщо… Повісьте інструкцію біля комп'ютера в офісі або розішліть e-mail Зробіть міні-навчання: фішингове повідомлення — і попросіть знайти проблему

Висновок

Інциденти трапляються. Але добре написана політика й мінімальний план дій дають змогу реагувати швидко, спокійно і результативно. Так організація не лише захищає себе — а й формує культуру відповідальності.

2.6 ПОЛІТИКА КОРИСТУВАННЯ ОСОБИСТИМИ ПРИСТРОЯМИ

Для чого це потрібно?

У більшості неприбуткових організацій, малих установ, шкіл або проєктів працівники використовують власні телефони й комп'ютери. Це зручно і економно. Але це також створює додаткові ризики:

- Дані організації можуть зберігатися на незахищених пристроях;
- Особисті акаунти працівників можуть змішуватись із робочими;
- Пристрій може бути втрачено або вкрадено;
- Неможливо контролювати, хто ще має доступ до пристрою (родичі, діти тощо).

Типові ситуації:

- Працівниця зберігає список учасників заходу у файлі на власному ноутбуці — без резервної копії.
- Волонтер встановлює пароль організаційної пошти на свій телефон — і забуває його змінити після завершення проєкту.
- Підрядник використовує робочий Google-акаунт разом із особистим браузером, залишаючи сесію відкритою.

Шаблон політики: особисті пристрої

Політика використання особистих пристроїв у робочих цілях

1. Співробітники та підрядники можуть використовувати особисті пристрої для роботи лише за умови дотримання мінімальних заходів безпеки.
2. Пристрої повинні бути захищені паролем або біометрією (PIN, TouchID тощо).
3. Обов'язково вмикається автоматичне блокування після періоду бездіяльності (не більше 5 хв).
4. Для критичних сервісів використовується окремий акаунт, не пов'язаний з особистим.
5. Зберігання робочих документів дозволено тільки в захищених папках (Google Drive, OneDrive, заборонено — "на робочому столі").
6. У випадку втрати або крадіжки пристрою користувач зобов'язаний негайно повідомити адміністратора або відповідального за безпеку.
7. По завершенні проєкту або співпраці:

- працівник видаляє всі робочі файли з пристрою;
- змінюється пароль до відповідних акаунтів;
- закривається сесія у хмарних сервісах.

Рекомендація: організація повинна повідомляти користувача про ці правила ще до початку використання пристрою — у письмовій або електронній формі.

Як адаптувати:

- У навчальному закладі: персонал, що працює з документами, має встановити на телефон пароль і не залишати його незахищеним на столі.
- У ГО: волонтери з доступом до пошти отримують коротку інструкцію + PDF-файл з базовими вимогами.
- У проєкті: перед початком співпраці підряднику надається шаблон із вимогами до пристрою.

Як це оформити практично?

Форма підтвердження:

Я, ПІБ, підтверджую, що використовую особистий пристрій для роботи з обліковими записами організації. Я зобов'язуюсь:

– захищати пристрій паролем;

– не передавати його стороннім особам;

– повідомити про втрату або злам;

– видалити робочі дані після завершення співпраці.

Можна додати це як окремий пункт у договір про надання послуг або у внутрішній регламент.

Чек-лист для самоперевірки

Чи мій пристрій має пароль/TouchID?

Чи я не зберігаю робочі файли на робочому столі?

Чи мій акаунт має MFA?

Чи я знаю, що робити в разі втрати пристрою?

Висновок

У сучасному робочому середовищі особисті пристрої — це норма. Але саме тому вони потребують чітких правил. Добре прописана політика користування особистими пристроями дозволяє знизити ризики без потреби в жорсткому технічному контролі.

2.7 ПОЛІТИКА ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ І ЦИФРОВОГО КОНТЕНТУ

Чому це важливо?

Соцмережі — вітрина будь-якої сучасної організації. Вони формують довіру, репутацію, публічний образ, залучають партнерів і аудиторію. Проте водночас соцмережі можуть бути джерелом ризиків:

- злам сторінки;
- витік інформації;
- публікація чутливих або некоректних матеріалів;
- втрата доступу до акаунту через зміну працівників;
- коментарі або дії, які компрометують установу.

Типові ситуації:

- SMM-менеджер звільнився і забрав із собою всі паролі.
- Доброволець випадково опублікував драфт-пост із внутрішньою інформацією.
- Коментар у Facebook, написаний від імені організації, викликав негативну реакцію.

Шаблон політики: соцмережі і контент

Політика використання соціальних мереж і цифрового контенту

1. Офіційні акаунти організації створюються на ім’я установи. Власником облікового запису є організація, а не окрема особа.
2. Доступ до акаунтів зберігається у захищеному менеджері паролів. Відповідальний за доступ — адміністратор або керівник напряму.
3. Усі публікації, що містять дані третіх осіб (учасники заходів, фото дітей, партнери), здійснюються лише після отримання згоди на публікацію.
4. Заборонено публікувати:

- незатверджену інформацію;
- особисті дані (телефони, адреси, фото з документами);
- драфтові або службові матеріали;
- критичні або емоційні висловлювання від імені установи.

5. При зміні відповідальної особи паролі оновлюються і передаються офіційно.
6. Фото- і відеоконтент зберігається в окремому хмарному просторі, упорядкованому за проєктами.

7. Усі сторінки мають резервного адміністратора з іншого акаунта (бажано — з керівної посади).

Практична адаптація:

- У школі: директори або IT-відповідальні мають доступ до сторінки школи. Кожна публікація — лише після погодження.
- У ГО: Google Диск із усім візуальним контентом впорядковується за подіями. На кожному акаунті — двоє адміністраторів.
- У бібліотеці: простий шаблон інструкції «що і як публікувати» (наприклад: день, опис, теги, автор, фото з дозволом).

Блок: Інструкція з безпеки для соцмереж

Чек-лист

- Увімкнено двофакторну автентифікацію для сторінки
- Є щонайменше 2 адміністратори
- Паролі зберігаються в менеджері, доступ мають лише відповідальні
- Перед публікацією перевіряється:

  (а) чи є дозвіл на фото;

  (б) чи немає конфіденційних елементів на задньому фоні;

  (в) чи правильна назва/дати/учасники.

Приклад згоди на використання фото/відео

Я, ПІБ, даю згоду організації "Назва" на використання мого зображення у фото- та відеоматеріалах із метою висвітлення заходу у соціальних мережах та на сайті організації. Згода дійсна протягом 12 місяців з моменту підписання.

Може бути розміщена в реєстраційній формі або підписуватись окремо.

Висновок

Соцмережі — це сила. Але вона працює на організацію лише тоді, коли контроль, безпека і повага до людей і контенту — на першому місці. Добре прописана політика — запорука того, що акаунт не стане точкою ризику або скандалу.

Аудит кібербезпеки — це перевірка того, наскільки організація дотримується встановлених правил, стандартів і практик інформаційної безпеки. Це не контроль заради контролю, а інструмент виявлення слабких місць ще до того, як ними скористаються зловмисники.

Проведення аудиту дозволяє:

- з'ясувати, чи відповідає технічна інфраструктура політикам безпеки;
- побачити "людські" ризики: слабкі паролі, небезпеку фішингу, відсутність навчання;
- оцінити ефективність політик та інструкцій, впроваджених у попередньому розділі;
- зафіксувати поточний стан для порівняння через 3–6 місяців;
- мати готову відповідь у разі запиту від партнерів, інвесторів, перевірок.

Аудит не потребує спеціального програмного забезпечення чи професійної сертифікації. У більшості випадків внутрішній аудит — достатній для базового рівня захисту. Його може провести:

- керівник (за спрощеним чек-листом),
- технічний працівник (якщо є),
- зовнішній консультант,
- або команда працівників, які відповідають за різні напрями.

3.1 ЩО ПЕРЕВІРЯЄТЬСЯ ПІД ЧАС АУДИТУ БЕЗПЕКИ?

Більшість організацій не стикаються з проблемами безпеки… до певного моменту. А коли щось трапляється — з’ясовується, що:

- політика існує, але її ніхто не читав;
- критичні документи лежали у відкритому доступі;
- колишній співробітник досі має доступ до пошти.

Аудит — це шанс виявити це ДО інциденту, а не після. І хоча слово “аудит” часто звучить надто офіційно, по суті — це звичайна перевірка за списком: чи все у нас справді так, як ми думаємо?

Що саме перевіряється?

Ми рекомендуємо ділити аудит на 6 блоків. Кожен з них охоплює окремий аспект цифрової стійкості організації.

Блок	Що входить	Приклад порушення
1. Акаунти і доступи	Хто має доступ до яких сервісів і з якими правами	Колишній волонтер має доступ до Facebook
2. Паролі і автентифікація	Чи є політика, MFA, парольні менеджери	Усі використовують один пароль до пошти
3. Документи і хмара	Де зберігаються файли, хто має доступ	Папка з даними доступна всім “по лінку”
4. Пристрої	Чи є захист ноутбуків і телефонів, резервне копіювання	Ноутбук без пароля, дані не зберігаються в хмарі

5. Політики і навчання	Чи є інструкції, тренінги, чек-листи	Працівники не знають, як діяти при фішингу
6. Реагування і інциденти	Чи є план дій, хто відповідає, фіксація	Ніхто не знає, що робити при втраті телефона

Як це перевіряти?

Найпростіший варіант — аудит за чек-листом, який проводиться самостійно або в команді. Кожен блок має набір питань (так/ні), і за результатами можна бачити слабкі місця.

Приклад:

Блок 1. Акаунти і доступи

– Чи є у вас список усіх сервісів, які використовуються?

– Хто має до них доступ?

– Коли востаннє перевіряли доступи після змін у команді?

Відповіді на такі питання дозволяють побачити неочевидні вразливості. Наприклад, старий акаунт Zoom, який ніхто не адмініструє, але має платну підписку та доступ до записів.

Чи потрібен IT-фахівець?

Ні, для базового аудиту достатньо однієї або двох осіб, які:

- мають доступ до акаунтів або можуть їх перевірити;
- розуміють внутрішні процеси;
- мають достатню довіру команди.

У складніших випадках (наприклад, інтеграція CRM, VPN, сервери) варто залучити фахівця, але це радше виняток для малих організацій.

Формати проведення:

1. Самоаудит — одна людина перевіряє блоки, фіксує результати.
2. Аудит у парі — двоє колег перевіряють одне одного (перехресна оцінка).
3. Командний огляд — коротка зустріч + спільне заповнення таблиці.
4. Зовнішній супровід — тренер або IT-волонтер веде через шаблон.

Висновок

Аудит — це не покарання і не контроль. Це спосіб побачити, що ми справді робимо, а не що планували зробити. Він відкриває двері до системності: після нього з’являється ясність, що варто змінити вже завтра.

3.2 ЯК ПІДГОТУВАТИ АУДИТ САМОСТІЙНО: КРОК ЗА КРОКОМ

Аудит кібербезпеки не вимагає дорогих інструментів чи залучення консультантів. Ви можете організувати його власними силами, витративши 1–2 дні на підготовку і ще стільки ж на перевірку. Головне — чітка структура, чесна оцінка і фіксація результатів.

Крок 1. Визначити відповідальних

Хто має провести аудит?

Рекомендовано обрати 1–2 осіб:

- адміністратора хмарних ресурсів;
- координатора проєкту;
- технічну особу або того, хто має доступ до акаунтів;
- у маленькій команді — керівника або відповідального за документообіг.

Важливо: особа має бути не формальною, а реально здатною перевірити, що і де працює.

Крок 2. Зібрати список цифрових активів

Потрібно скласти перелік усього, що використовує організація у цифровому середовищі:

- акаунти: Google Workspace, Facebook, Zoom, Canva, Moodle тощо;
- хмара: де і як зберігаються документи;
- пристрої: службові ноутбуки, мобільні телефони;
- персонал: хто користується чим;
- сервіси: CRM, поштові розсилки, форми, платіжні системи.

Зручно вести цей перелік у таблиці: назва сервісу, хто користується, рівень доступу.

Крок 3. Підготувати чек-лист

На основі попереднього підпункту або шаблону з довідника формуємо таблицю перевірки з 6 блоків:

Питання	Так / Ні	Коментар або пояснення
Чи змінюються паролі регулярно?	Ні	Один і той самий пароль вже 2 роки
Чи є MFA для пошти?	Так	Увімкнено через Google

Можна скористатись Google Sheets або надрукувати шаблон на папері.

Крок 4. Запланувати і провести аудит

Найкраще — відвести 2–3 години з командою або самостійно й перевірити кожен пункт. Важливо не пропускати питання, навіть якщо здаються “банальними”. Часто саме вони викривають реальні проблеми.

Під час аудиту:

- робіть нотатки;
- зберігайте приклади (наприклад, скріншоти відкритих доступів);
- не оцінюйте людей — оцінюйте процеси.

Крок 5. Підсумки і ризики

Після перевірки створіть просту таблицю:

Блок	Оцінка (1–5)	Основні проблеми	Пріоритет дій
Акаунти	3	2 акаунти без MFA, немає журналу доступів	Високий

Використайте червоний/жовтий/зелений колір, щоб бачити, де найгірше.

Крок 6. Перші дії після аудиту

Не потрібно змінювати все. Достатньо 3–5 простих кроків, щоб суттєво підвищити рівень захисту. Наприклад:

- змінити паролі;
- увімкнути MFA;
- обмежити доступ до чутливих документів;
- призначити відповідального за резервне копіювання;
- створити інструкцію реагування.

Крок 7. Оновлення

Аудит варто повторювати:

- щороку — для невеликих ГО чи навчальних закладів;
- щопівроку — для проєктів із великим обсягом даних або командою;
- після інциденту або змін у команді — обов'язково.

Рекомендація

Заведіть файл з результатами аудитів за роками (Google Sheet або PDF):

2023: оцінка 3/5 — змінено політику паролів, додано MFA

2024: оцінка 4/5 — покращено резервне копіювання, зменшено кількість спільних акаунтів

Висновок

Аудит — це не разова кампанія, а початок зрозумілої системи, яка дозволяє поступово підвищувати рівень безпеки. Іноді прості дії — як табличка з паролями чи згода на публікацію фото — змінюють усе.

3.3 ШАБЛОНИ ДЛЯ САМОСТІЙНОГО АУДИТУ

Чек-лист базового аудиту кібербезпеки

№	Запитання	Так / Ні	Коментар / Дії
1	Чи ведеться список усіх акаунтів організації?		
2	Чи увімкнено двофакторну автентифікацію на ключових сервісах (пошта, хмара)?		
3	Чи оновлюються паролі регулярно (раз на 6 місяців)?		
4	Чи є обмеження доступів до чутливих документів?		
5	Чи є політика використання особистих пристроїв?		
6	Чи мають співробітники інструкції для реагування на інциденти?		
7	Чи є регулярне резервне копіювання даних?		
8	Чи є призначена особа, відповідальна за безпеку?		
9	Чи є політика роботи з персональними даними?		
10	Чи оновлювались доступи після зміни команди?		

Формат: можна копіювати в Google Таблицю або роздрукувати як частину звіту.

Таблиця цифрових активів організації

Сервіс / Платформа	Тип (хмара, пошта, CRM тощо)	Хто має доступ	Рівень доступу	Двофакторка?	Примітки
Gmail (основна пошта)	Пошта	Марія Іваненко, адміністратор	Повний	Так	Доступ оновлено
Google Drive	Хмара	Команда проєкту	Частковий (перегляд)	Так	Є відкриті папки
Facebook	Соцмережі	SMM + директор	Адмін	Частково	MFA не увімкнено

Формат: Google Sheet / Excel / Word таблиця.

Форма фіксації інцидентів

Дата / Час	Тип інциденту	Хто виявив	Опис ситуації	Що зроблено	Потрібні дії
01.04.2025 13:45	Фішинговий лист	А. Семенюк	Отримано лист від підробного “ПриватБанку”	Видалено, змінено пароль	MFA ще не ввімкнено

Може вестись у хронологічному режимі або в окремому файлі щоквартально.

Бланк короткого підсумку аудиту

Аудит кібербезпеки ГО “Ініціатива+”

Дата проведення: 10.06.2025

Відповідальні особи: О. Петренко, Н. Савчук

Загальний стан: 3.5 / 5

Основні проблеми:

– недостатній контроль за пристроями;

– немає плану реагування на інциденти.

Рекомендовані дії:

– підключити MFA на всі акаунти до 20.06

– провести коротке навчання для команди до 01.07

– створити інструкцію “що робити у випадку фішингу”

Такий підсумок зручно додавати до грантових звітів, внутрішніх документів або презентацій.

Навіть найкраща політика чи аудит не захистять організацію, якщо працівники не знають, як діяти щодня: які сайти безпечні, як створити пароль, що робити при фішинговому листі. Інструкції — це міст між формальними правилами й реальними діями.

За даними досліджень, понад 80% кіберінцидентів починаються з людського фактору — помилкового кліку, слабкого пароля, ігнорування фішингу. Тому навчання — це не додатковий елемент, а фундаментальний рівень захисту.

4.1 ЩО МАЄ ЗНАТИ КОЖЕН ПРАЦІВНИК: ЦИФРОВИЙ МІНІМУМ

Більшість інцидентів — через людський фактор, а не хакерські атаки. Один клік на фішинговий лист, один неправильно наданий доступ — і витік, і репутаційні втрати вже сталися. Саме тому кожен член команди, від бухгалтера до дизайнера, повинен мати цифрову грамотність у сфері безпеки.

Мінімум знань і навичок

1. Паролі і MFA

Створення складного пароля (фраза з 3–4 слів, символи, цифри).

Збереження паролів: менеджер паролів, а не стікер на моніторі.

Вмикання двофакторної автентифікації (наприклад, код через телефон або додаток Google Authenticator).

2. Як розпізнати фішинг

Лист виглядає офіційно, але з дивною адресою.

Посилання веде не туди (підроблена форма входу).

Лист створює тиск або терміновість (“У вас 24 години!”).

Наявність вкладень від невідомих осіб.

Правило: якщо є сумнів — не відкривай, не клікай, не вводь.

3. Основи цифрової поведінки

Не передавати паролі у месенджерах.

Не залишати акаунт відкритим на публічному комп’ютері.

Завжди перевіряти, кому надсилається файл чи лист.

Використовувати окремі акаунти для роботи і особистого.

4. Пристрої і дані

Телефон чи ноутбук має бути захищений паролем.

Увімкнено блокування пристрою при бездіяльності.

Дані важливої роботи зберігаються у хмарі, а не лише на пристрої.

У разі втрати пристрою потрібно негайно повідомити відповідального.

5. Основи роботи з персональними даними

Не зберігати персональні дані без мети і терміну.

Не передавати таблиці з особистою інформацією у відкритих месенджерах.

Для анкет або фото з заходів — отримати згоду.

Після завершення проєкту — видалити непотрібні дані.

Навіть Google Форма з ПІБ і телефонами — це персональні дані.

Чек-лист для працівника

- Я знаю, як створити надійний пароль
- У мене увімкнено MFA хоча б на пошті
- Я розпізнаю фішинг і не клікаю на підозрілі листи
- Я не зберігаю робочі файли тільки на ноутбуці
- Я знаю, що робити при інциденті (втрата пристрою, фішинг тощо)
- Я знаю, як працювати з персональними даними

Спеціальні пам’ятки для різних типів працівників

Для працівників шкіл

5 правил кібергігієни для освітнього закладу:

1. Ніколи не залишайте увімкнений комп’ютер без нагляду — блокуйте екран навіть між уроками.
2. Уникайте флешок — краще пересилайте файли через Google Диск.
3. Використовуйте окремий акаунт Google для роботи — не змішуйте з особистим.
4. Не передавайте дані учнів у відкриті чати або публічні документи.
5. Якщо побачили підозрілий лист чи сайт — повідомте IT-працівника або директора.

Для працівників офісу/малого бізнесу

6 правил цифрової безпеки для офісу:

1. Використовуйте паролі-словосполучення, наприклад, RaketaLuna2025!
2. Увімкніть MFA для пошти, CRM, бухгалтерії.
3. Не відкривайте рахунки/прайси з невідомих джерел.
4. Скануйте пристрої раз на місяць (антивірус або захист Windows).
5. Не зберігайте файли на "робочому столі" — використовуйте спільну хмару.
6. Не завантажуйте програми самостійно — узгоджуйте з IT.

Для членів громадських організацій / волонтерів

5 простих правил для безпечної роботи з чутливими даними:

1. Працюйте лише в акаунтах організації, не використовуйте особисту пошту.
2. Не публікуйте Google-документи у відкритий доступ.

3. Видаляйте зайві копії документів після завершення проєкту.
4. Уникайте роботи з документами у відкритому Wi-Fi.
5. Якщо сумніваєтесь — краще спитайте, ніж натисніть.

Висновок

Цифровий мінімум — це як ремінь безпеки в авто. Він не гарантує, що нічого не станеться, але різко знижує ризики. Організація, де кожен знає базові правила, — вже на крок попереду.

4.2 ЯК ОРГАНІЗУВАТИ НАВЧАННЯ БЕЗ ТЕХНІЧНОЇ КОМАНДИ

Навчання з кібербезпеки не потребує технічних спеціалістів. Те, що потрібно працівникам — усвідомлення ризиків, звички, сценарії дій, а не знання термінів або глибоке розуміння протоколів. Тому проводити навчання може:

- координатор проєкту;
- адміністративна особа;
- навіть волонтер чи партнер.

Варіанти навчального формату

Формат	Як працює	Приклад
Презентація + обговорення	Один модерує, решта ставлять питання	20 хвилин слайдів, 20 хв практики
Ігрова симуляція	Працівники розпізнають фішинг, вибирають реакції	“Вас намагаються зламати – що робите?”
Тематичний тиждень	Кожного дня – одна порада, відео чи постер	Наприклад: “Понеділок паролів”
Відео + тест	Онлайн-урок (відео 5-10 хв) + Google Форма	Перевірка засвоєння одразу після перегляду
Листівка на робочому столі	Мінімальна модель — паперовий гайд або стікер	“5 речей, які НЕ робимо з поштою”

Структура базового тренінгу (1 година)

1. Вступ (5 хв) — приклад інциденту: “Отримали фішинг – втратили 5 днів роботи”.
2. Паролі та MFA (10 хв) — наочно: поганий пароль vs. добрий.
3. Фішинг (10 хв) — показати 2 приклади: справжній і підроблений.
4. Персональні дані (10 хв) — “Що не можна робити з анкетами і фото”.
5. Повторення (5 хв) — інтерактивне: "Хто відповість, як не дати доступ?"
6. Мінітест або чек-лист (10 хв) — Google Форма або анкета.
7. Підсумок і 1 річ, яку кожен зробить сьогодні (5 хв) — зміна пароля, ввімкнення MFA.

Неформальні формати (у малих командах)

- “П'ятнична фішка”: щотижня один з працівників ділиться порадою.
- “Кібершок”: розбір одного інциденту зі світу — обговорення, що було не так.

- Кібербатл: хто швидше знайде у листі фішинг чи небезпеку (гейміфікація).

Де брати матеріали?

Цей довідник — ви можете використати частини як готові презентації.

Сайти з відкритими матеріалами:

- https://cyberpolice.gov.ua
- https://virtual-routes.org
- https://security.google

Власний досвід або кейси з колегами — найкраща подача через життєві приклади.

4.3 ПРИКЛАДИ ПРОГРАМ НАВЧАННЯ

(1 година, 1 день, 1 тиждень)

Програма на 1 годину — "Цифрова безпека: основи для кожного"

Формат: короткий тренінг у Zoom / Teams або офлайн

Ціль: дати базові знання і спонукати до першого кроку (зміна пароля, MFA)

Час	Тема	Форма	Мета
0:00–0:10	Що таке кібербезпека і чому це всіх стосується	Вступна розповідь	Мотивація через приклади
0:10–0:25	Паролі, MFA, як уникнути злому	Демонстрація + обговорення	Практичне розуміння
0:25–0:40	Як розпізнати фішинг + реальні приклади	Інтерактив (демо листів)	Візуальне запам'ятовування
0:40–0:55	Що робити при втраті пристрою / інциденті	Покрокова інструкція	Підготовка до дій
0:55–1:00	Мікротест або зворотній зв'язок	Google Форма / усно	Перевірка засвоєння

Програма на 1 день — "Кібербезпека у команді: все, що треба знати"

Формат: одноденний тренінг для всієї команди

Ціль: сформувати усвідомлення + звички

Час	Сесія	Опис
10:00–10:30	Вступ: "Цифрова поведінка — зона відповідальності кожного"	Мотивація через реальні кейси
10:30–11:30	Основи захисту акаунтів	Практика створення паролів, MFA
11:30–12:00	Робота з документами: доступи, хмара, резервне копіювання	Візуальна демонстрація
12:00–13:00	Обід	—
13:00–14:00	Фішинг, соціальна інженерія, поведінка у пошті	Гра: знайди фішинг
14:00–15:00	Персональні дані і юридичні аспекти	Що дозволено і як фіксувати згоду
15:00–16:00	Що робити при інциденті: ролі, кроки, хто що робить	Моделювання ситуації
16:00–16:30	Підсумки, запитання, інструкції на майбутнє	План особистих дій + мінітест

Програма на 1 тиждень — “Тематичний тиждень безпеки”

Формат: 5 днів, по 15–20 хв на день

Ціль: через малу дозу, але щоденно — сформувати сталі звички

День	Тема	Як подається
Пн	Паролі та MFA	Постер + коротке відео (5 хв) + порада
Вт	Доступ до документів	Приклад з відкритою папкою + фіксація
Ср	Фішинг і фейкові листи	2 приклади на порівняння + мінітест
Чт	Пристрої і резервні копії	Фото зламаного ноутбука + обговорення
Пт	Реагування на інциденти	Шаблон інструкції + опитування “що б ви зробили”

Поради до адаптації

- Якщо команда зайнята — 1 година краще за 0 годин.
- Для освітніх або бюджетних організацій підійде 1 тиждень у форматі пошти або Google Class.

4.4 МАТЕРІАЛИ, ЯКІ ВАРТО РОЗДАТИ АБО ПОКАЗАТИ

Приклади корисних матеріалів

1. "Паролі безпечні та небезпечні"

Формат: табличка А4 або інфографіка

Зміст:

Небезпечно	Безпечно
123456	ВаренняПес2024!
qwerty	Синє_небо$345
Дата народження	Фраза з 3-4 випадкових слів
Один пароль скрізь	Унікальний пароль на кожен акаунт

2. “Розпізнай фішинг”

Формат: картка / слайд для тренінгу

Зміст: 2 листи — один справжній, інший фейковий.

Питання: “Який з них фішинговий і чому?”

Пояснення:

- помилкова адреса (admin@goooogle[.]com);
- підроблений логотип;
- заклик натиснути негайно;
- дивна граматика.

3. “Що сказати, якщо щось підозріле?”

Формат: листівка або постер біля робочого місця

Якщо не впевнений — скажи:

- “Я не впевнений у цьому файлі — можеш перевірити?”

- “Це виглядає підозріло. Чи точно це від банку?”
- “Я краще не буду відкривати це без підтвердження.”

4. “Що робити при втраті пристрою?”

Формат: інструкція A5

1. Повідомити відповідального або керівника.
2. Якщо можливо — віддалено вийти з акаунтів.
3. Змінити паролі: пошта, соцмережі, хмара.
4. Перевірити, чи була службова інформація на пристрої.
5. Записати інцидент у журнал.

5. Міні-гайд “Персональні дані: що можна, а що ні”

Формат: шпаргалка A4

Можна	Не можна
Збирати ПІБ, телефони з чіткою метою	Ділитися списком учасників у Viber
Питати згоду на фото	Виставляти фото дітей без згоди батьків
Видаляти дані після завершення проєкту	Зберігати анкети без захисту в Google Docs

Папка для нового працівника

Рекомендуємо створити набір стартових матеріалів:

- “Цифровий мінімум” (A4, коротко)
- Лист із 5 порадами для безпечної роботи
- Посилання на відео (короткі ролики YouTube або внутрішні записи)
- Чек-лист “Мій старт у кібербезпеці”

Для повторного нагадування

- Щомісяця: коротка порада поштою / в чаті (“кібервівторок”)
- Раз на квартал: візуалізація на дошці, у внутрішньому сайті
- Перед проєктами або звітністю: чек-лист безпеки

4.5 ЯК ПЕРЕВІРИТИ, ЩО ЛЮДИ ЩОСЬ ЗАСВОЇЛИ

Навіть найкраще подане навчання втрачає ефективність, якщо:

- працівники не сприйняли інформацію як серйозну;
- не відбулось осмислення (тільки прослухали);
- не сформувалась звичка діяти по-новому.

Перевірка — це не контроль, а підтвердження, що ключові речі дійшли “до дії”.

Варіанти перевірки знань

1. Мінітест (5–10 запитань)

Інструмент: Google Форми або на папері.

Запитання:

- Що таке MFA і чому воно важливе?
- Як ви розпізнаєте фішинговий лист?
- Що робити, якщо втрачено пристрій?
- Який із паролів є надійним: “qwerty123” чи “КаваЛіто2024!”?

Автоматичне оцінювання, можна показати результат одразу.

2. Мікросценарії

Працівникам надається ситуація:

“Вам приходить лист з темою ‘Ваша виплата готова’. Надсилає його hr.payments@notbank.com. У вкладенні — Excel-файл.”

Запитання:

- Що ви зробите?
- Що насторожує у цьому листі?

Мета — не правильна відповідь, а виявлення мислення.

Розмова 1:1 або в малих групах

Запропонуйте співробітникам обрати 1 ситуацію:

- “Мене зламали — що я роблю?”
- “Я бачу підозріле повідомлення — як реагую?”
- “Мені пише колега, але щось дивне — що перевірити?”

Розмова як спосіб закріплення знання + нормалізація сумніву.

Чек-лист дій

Роздрукуйте або поширте чек-лист "Що я вже зробив":

- Увімкнув MFA для пошти
- Змінив пароль на складніший
- Пройшов навчання (вказати дату)
- Ознайомився з політикою безпеки
- Знаю, кому повідомити про інцидент

Можна збирати анонімно або з іменами.

Гра або вікторина

Формат Kahoot, Quizizz, Telegram-бот або сесія “Правда чи міф”:

- Паролі можна передавати, якщо довіряєш — ✗ МІФ
- MFA означає, що треба підтвердження двома способами — ✓ ПРАВДА
- Якщо вкрали ноутбук, нічого страшного — ✗ МІФ

Ідеально підходить для залучення молодших команд або волонтерів.

Повторний тест через 2–4 тижні

Після початкового тренінгу — короткий тест через місяць:

- ті ж запитання, трохи переформульовані;
- аналітика: що засвоєно, що забуто;
- час для повторення та додаткових пояснень.

Головне — не “оцінка”, а зміна поведінки

Людина, яка почала сумніватися і перевіряти, — це успіх. Навіть якщо вона не знає терміна “фішинг”, але не відкриє підозрілий лист — це перемога навчання.

РОЗДІЛ 5. РЕАГУВАННЯ НА ІНЦИДЕНТИ — ПОКРОКОВІ ІНСТРУКЦІЇ

Ніхто не може гарантувати абсолютний захист. Але те, наскільки швидко й адекватно організація реагує, визначає рівень її кіберзрілості. Витік, блокування доступу, фішинг, зараження пристрою — ці інциденти не є катастрофою самі по собі. Катастрофою стає відсутність плану реагування.

Підготовка включає:

- прописані дії на випадок надзвичайної ситуації;
- визначення відповідальних;
- тренування команди на симульованих кейсах;
- збереження інформації про події (журнали, логування);
- план відновлення.

5.1 ЩО ТАКЕ ІНЦИДЕНТ І КОЛИ РЕАГУВАТИ

Визначення простими словами

Кіберінцидент — це будь-яка подія, яка:

- порушує політику безпеки організації;
- загрожує конфіденційності, цілісності або доступності інформації;
- створює ризик для працівників, партнерів або даних.

Інцидент — це не обов'язково "атака хакера". Це також:

- людська помилка (відкритий доступ до файлів);
- технічний збій (сервер не зберіг резервну копію);
- неправомірна поведінка (використання чужого акаунта).

Приклади інцидентів в реальному житті

Ситуація	Чи це інцидент?	Пояснення
Працівник відкрив фішинговий лист і ввів пароль	✓ Так	Злам облікового запису можливий
Колега поділився посиланням на відкритий документ з персональними даними	✓ Так	Дані можуть бути скомпрометовані
Втрачено флешку з файлами про учасників проєкту	✓ Так	Конфіденційна інформація втрачена
Хтось випадково видалив загальну таблицю	✗ Ні (але близько)	Це операційна помилка, важливо мати резервне копіювання
Один з акаунтів несподівано заблоковано	☐ Можливо	Треба перевірити причину: якщо через порушення, то так

Чому важливо реагувати?

У перші хвилини після інциденту:

- можна втратити дані, якщо нічого не зробити;
- доступи залишаються активними — і ситуація погіршується;

- без швидкої реакції важко буде відстежити, що саме сталося.

Реакція — це не “покарання” когось, а запобігання масштабнішим наслідкам.

Ознаки, що діяти треба негайно

1. Надійшло повідомлення про підозрілу активність на акаунті.
2. Хтось повідомив, що його дані стали публічними без дозволу.
3. Сайт або інструмент раптом стали недоступними.
4. Надійшло повідомлення про зміну пароля без вашої участі.
5. Ви отримали повідомлення від Google/Meta тощо: “Ваш обліковий запис підозрюється у порушеннях”.

У таких випадках: реагувати одразу, не чекаючи “поки пройде”.

Але… не кожен збій — це інцидент

Іноді технічні несправності або непорозуміння не вимагають формального реагування, а лише:

- повідомлення відповідальному;
- короткого внутрішнього пояснення;
- оновлення інструкції або перевірки системи.

Але краще випадково “перереагувати”, ніж проігнорувати справжню загрозу.

Рекомендація для організацій

Створіть просте внутрішнє правило:

“Якщо ти не впевнений, чи це інцидент — все одно повідом людину, що відповідає за безпеку (або координатора).”

Це правило дозволяє зняти страх, що повідомлення буде “дурним” або “перебільшеним”.

5.2 АЛГОРИТМ РЕАГУВАННЯ

КРОК 1. Виявлення інциденту

Сигнал може надійти від працівника, антивіруса, користувача.

Не ігноруйте дивні листи, блокування, масові запити.

КРОК 2. Ізоляція

Вимкніть доступ до ураженого пристрою / акаунта.

Змініть паролі, обмежте мережеву активність.

КРОК 3. Документування

Що трапилось, коли, хто помітив, де зберігається інформація.

Фіксуйте навіть емоційні реакції — це частина оцінки.

КРОК 4. Інформування

Керівництво, IT-відповідальний, працівники (лише потрібні).

Якщо витік — постраждалі особи, згідно із законодавством.

КРОК 5. Відновлення

Відновлення з резервної копії / перевірка систем.

Забезпечення повторного доступу лише після перевірки.

КРОК 6. Аналіз

Чому це сталось? Чи було попередження? Як уникнути?

Що оновити в політиках чи навчанні?

5.3 ПОКРОКОВА ІНСТРУКЦІЯ РЕАГУВАННЯ

Загальні принципи перед діями

Перед тим як почати будь-які дії, варто пам'ятати:

- Не приховуйте інцидент — краще швидка реакція, ніж тиша.
- Не поспішайте "прибирати сліди" — вони можуть допомогти відновити ситуацію.
- Зберігайте спокій — для більшості інцидентів є алгоритм, і ви не самі.

Сценарій 1: Фішинг — хтось відкрив лист і ввів дані

Що сталося:

Працівник отримав фішинговий лист, відкрив посилання та ввів пароль.

Дії:

1. Негайно змінити пароль до скомпрометованого акаунту.
2. Якщо акаунт використовувався повторно — змінити пароль у всіх інших місцях, де він такий самий.
3. Увімкнути двофакторну автентифікацію (якщо ще не ввімкнено).
4. Повідомити відповідальну особу за безпеку.
5. Заблокувати доступ стороннім додаткам (у Google, Meta, тощо).
6. Якщо є підозра на злам — вийти з усіх сесій акаунту.
7. Зафіксувати інцидент у журналі кіберінцидентів.

Порада: збережіть фішинговий лист (без кліку) — для подальшого аналізу.

Сценарій 2: Втрачено пристрій (ноутбук, смартфон)

Що сталося:

Пристрій загублено, вкрадено або передано стороннім особам.

Дії:

1. Повідомити відповідального одразу.

2. Якщо є можливість — видалити або заблокувати пристрій віддалено (через Google, iCloud тощо).
3. Змінити паролі до всіх акаунтів, які були доступні з пристрою.
4. Деактивувати токени доступу (наприклад, у Google Account > Security).
5. Проаналізувати, які файли/дані були на пристрої, і вжити додаткових заходів.
6. Зафіксувати інцидент у журналі.
7. Якщо є персональні дані — повідомити керівництво і можливо регуляторів (GDPR/ЗУ “Про захист персональних даних”).

Якщо був робочий акаунт без пароля на пристрої — це високий ризик, дійте швидко.

Сценарій 3: Випадковий або публічний витік даних

Що сталося:

Таблиця з персональними даними була випадково надіслана публічно або збережена без захисту.

Дії:

1. Негайно закрити доступ до документа.
2. Перевірити, хто отримав доступ (історія змін / email-лог).
3. Оцінити, які саме дані стали публічними.
4. Повідомити відповідальну особу / керівника.
5. Вирішити, чи потрібно повідомити осіб, чиї дані розкрито.
6. Зробити короткий звіт про ситуацію.
7. Оновити інструкції або політики щодо обігу даних.

Порада: введіть правило — усі документи з даними мають мати обмеження “лише за посиланням з правами читання”.

Сценарій 4: Підозра на злам акаунту

Що сталося:

В акаунті з’явилися невідомі дії або надходять сповіщення про спробу входу.

Дії:

1. Змінити пароль і увімкнути MFA.
2. Перевірити останні дії (Google: Security activity, Microsoft: Recent activity).
3. Вийти з усіх сесій на інших пристроях.
4. Перевірити, чи не додано нові адреси відновлення / пересилання листів.
5. Заблокувати сторонні додатки, які мають доступ до акаунту.
6. Повідомити відповідального і зафіксувати інцидент.
7. Моніторити пошту або інші дії кілька днів.

У великих організаціях може бути доцільно відновити акаунт із резервної копії або створити новий.

Універсальна порада

Кожен інцидент варто описати коротко у внутрішньому журналі:

- що сталося;
- коли і як помітили;
- хто був залучений;
- що зроблено;
- які висновки.

5.4 ФОРМА ДЛЯ ФІКСАЦІЇ ІНЦИДЕНТІВ

Навіщо потрібна форма?

- Формалізувати реагування — щоб не забути важливі кроки.
- Створити "історію" інциденту, яка допоможе при аналізі або звітуванні.
- Побачити повторювані проблеми (якщо виникають схожі інциденти).
- Захистити організацію — показати, що ви реагували добросовісно.

Шаблон: картка фіксації інциденту

Поле	Опис
Номер інциденту	Наприклад, 2025/04
Дата та час виявлення	Коли інцидент став помітним
Тип інциденту	(оберіть) Фішинг / Втрата пристрою / Витік даних / Злам / Інше
Стислий опис	Що сталося? Як було виявлено?
Місце/платформа	Напр., Gmail, Google Drive, фізичний носій тощо
Особи, залучені до інциденту	Хто постраждав, хто реагував
Перші дії після виявлення	Що зробили негайно
Кінцеві дії	Паролі змінено, доступи відкликано, повідомлено тощо
Ризики, які виникли	Які потенційні наслідки
Висновки / уроки	Що треба змінити, щоб не повторилось
Хто фіксував інцидент	ПІБ і дата заповнення

Поради щодо використання

- Форму можна вести в Google Таблиці або у вигляді окремих Google Форм — зберігати в папці "Кібербезпека".
- Варто пронумерувати інциденти хронологічно — це спрощує аудит.
- У малих організаціях форму може заповнювати будь-хто, хто помітив інцидент. У більших — відповідальна особа.
- Якщо інцидент серйозний, форму можна розширити — додати поле для дій інших осіб, аналізу втрат, повідомлення партнерів тощо.

Зберігайте форми у захищеній папці з обмеженим доступом — тільки для відповідальних осіб.

5.5 ЯК ПРОАНАЛІЗУВАТИ ІНЦИДЕНТ І ЗРОБИТИ ВИСНОВКИ

Чому аналіз інциденту — це не “розбір польотів”

Більшість організацій після інциденту або:

- просто замовчують його (щоб не розкручувати тему);
- карають винних, але не змінюють підхід;
- забувають, хоча проблема може повторитися.

правильний підхід — це записати, подумати і змінити хоч одну річ.

Що варто проаналізувати?

1. Як інцидент стався?

Які дії, помилки, або обставини до нього призвели?

2. Як швидко його помітили?

Якщо пройшло багато часу — чому не побачили одразу?

3. Як реагували?

Була паніка, чи все пішло по інструкції? Чого не вистачило?

4. Які наслідки могли бути гіршими?

Це дозволяє оцінити “на волосині від катастрофи”.

5. Чого бракувало в інструкціях, навчанні, інструментах?

Тут — поле для вдосконалення.

Шаблон простого аналізу

Питання	Ваша відповідь
Який тип інциденту?	Наприклад: злам акаунту
Що саме дозволило інциденту статися?	Слабкий пароль, не увімкнено MFA
Як швидко це помітили?	Через 6 годин після листа від Google
Хто брав участь у реагуванні?	Працівник, координатор безпеки
Чого не вистачило під час дій?	Інструкції, хто що робить
Що треба зробити, щоб таке не повторилося?	Провести навчання, змінити політику паролів

Цей шаблон можна включити в загальну форму фіксації або тримати окремо.

Перевірка: чи зроблено хоча б одне покращення?

Після кожного інциденту організація має змінити щось у процесах, наприклад:

- оновити інструкцію;
- додати політику MFA для всіх;
- провести коротке нагадування для колег;
- змінити правила доступу до документів.

Навіть одна маленька зміна після інциденту — це вже безпековий прогрес.

Приклад живого аналізу

Інцидент: працівник надіслав таблицю з персональними даними партнерам у відкритому доступі.

Аналіз:

Було дозволено створювати відкриті посилання без обмежень.

Людина не знала, що “публічний доступ” означає доступ для всіх.

Дія:

Увімкнули блокування публічного доступу до файлів у Google Admin.

Додали короткий гайд: як перевіряти налаштування перед відправкою.

5.6 ЩО СКАЗАТИ КОМАНДІ, ДОНОРАМ АБО ПАРТНЕРАМ

Чому важливо говорити, а не мовчати?

Мовчання під час інциденту:

- викликає підозру і домисли;
- зменшує довіру;
- посилює наслідки — бо люди не знають, що робити.

Натомість коротка, чесна і впевнена комунікація знижує шкоду та показує вашу зрілість як організації.

Команда: що, коли і як сказати

“У нас трапився інцидент, який потенційно впливає на ваші акаунти або інформацію. Ми вже вжили кроків і тримаємо ситуацію під контролем. Ось що варто зробити...”

Формат:

- коротко пояснити суть;
- що вже зроблено;
- які дії треба від людей (змінити пароль, перевірити листи тощо);
- запевнити, що буде додаткове пояснення/навчання.

Приклад повідомлення для чату/листування:

У вівторок ми виявили інцидент безпеки, пов'язаний із доступом до спільної таблиці з контактами. Ми вже закрили доступ, перевірили журнал активності та не виявили несанкціонованого доступу.

Для безпеки просимо всіх змінити паролі до службових акаунтів і не поширювати файли без перевірки налаштувань.

Дякуємо за розуміння — команда безпеки.

Партнери або донори

Якщо інцидент зачіпає сторонніх осіб — краще сказати чесно, ніж чекати, поки вони дізнаються випадково.

Що має містити повідомлення:

- Суть інциденту (без технічних деталей);
- Яка інформація могла бути скомпрометована;
- Які дії вже вжито;
- Які кроки буде зроблено додатково;
- Контакт для уточнень.

Приклад листа:

Шановні партнери,

15 червня наша команда виявила, що один із файлів з контактами учасників заходу був доступний за відкритим посиланням. Файл уже вилучено, ми проаналізували журнали і не зафіксували сторонніх завантажень.

На знак відповідальності ми посилили правила обміну файлами і проводимо додаткове навчання працівників. Якщо у вас є запитання — звертайтесь до [контактна особа].

Дякуємо за розуміння.

Чого НЕ варто робити

- Замовчувати: люди все одно дізнаються, і втратять довіру.
- “Перекидати вину”: звинувачення окремого працівника виглядає слабко.
- Надмірна технічність: партнерів цікавить ситуація і рішення, а не терміни.
- Паніка або фрази “ми не знаємо що робити”.

Якщо інцидент серйозний або повторюється

1. Проведіть зустріч або Q&A-сесію.
2. Дайте людям можливість задати питання анонімно.
3. Створіть документ з “поясненням інциденту” (для команди).
4. Попросіть донорів / партнерів дати зворотний зв’язок — це покаже відкритість.

Таким чином, реагування на інцидент — це не лише технічний процес, а й комунікаційний. І правильна взаємодія часто важить більше, ніж сама проблема.

Кібербезпека — це не лише технічна чи організаційна сфера. Вона тісно пов'язана з правом. Організації несуть юридичну відповідальність за захист персональних даних, реагування на інциденти, інформування користувачів і дотримання стандартів обробки інформації.

Невиконання цих вимог може призвести не лише до репутаційних втрат, а й до штрафів, перевірок і судових позовів.

6.1 ЯКІ Є ВИМОГИ ДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Що таке "персональні дані" і чому вони важливі?

Персональні дані — це будь-яка інформація, що дозволяє ідентифікувати людину. Це може бути:

- ім'я, прізвище, по батькові;
- email, номер телефону;
- ІПН, серія і номер паспорта;
- IP-адреса або геолокація;
- фото, голос, відео;
- медичні або фінансові дані.

Навіть один рядок у Google Таблиці з іменем і номером телефону — це персональні дані.

Який закон регулює це в Україні?

Основний документ — Закон України "Про захист персональних даних" (ЗУ №2297-VI). Але також враховують:

- Конституцію України (ст. 32);
- європейські практики (наприклад, GDPR, якщо організація має партнерів з ЄС);
- окремі вимоги донорів, банків, міжнародних структур.

Закон стосується як державних, так і недержавних установ, якщо вони зберігають або обробляють персональні дані.

Що зобов'язана зробити організація?

1. Мати документ, що описує політику конфіденційності

- Це внутрішній або публічний документ, де вказано:
- які саме дані збираються;
- навіщо вони потрібні;
- хто має до них доступ;
- скільки часу їх зберігають;
- як особа може їх змінити або видалити.

2. Отримувати згоду на обробку даних

- Якщо ви збираєте реєстраційні форми, анкети, фото — необхідно вказати, як буде використано ці дані, і отримати згоду.
- Згода може бути цифровою або письмовою, але має бути явною.

Приклад: "Надсилаючи цю форму, ви погоджуєтесь на обробку ваших персональних даних згідно з політикою конфіденційності організації."

3. Захищати дані від сторонніх осіб

- Захист паролями, MFA, доступами "лише для обраних";
- Не використовувати загальні акаунти;
- Архівувати старі дані;
- Знищувати дані, якщо вони вже не потрібні.

4. Призначити відповідального (необов'язково штатного)

Організація має визначити, хто стежить за дотриманням політики захисту даних. Це може бути:

- адміністратор сайту;
- координатор проєкту;
- директор або інша довірена особа.

У випадку витоку або скарги — саме ця особа першою контактує з регулятором.

5. Бути готовим до запиту або перевірки

- Ви повинні знати, які дані зберігаються і де;
- Мати можливість їх видалити або передати особі;
- Мати хоча б базову документацію (політика + згода).

Що буде, якщо не виконувати?

- Скарги від людей, чиї дані опинилися у відкритому доступі;
- Втрата партнерств — донори або компанії часто вимагають відповідності нормам;
- Можливі санкції (зараз обмежено, але практика посилюється);Проблеми з репутацією: "у них все публічно, не варто довіряти".

Юридична обізнаність у сфері захисту даних — це як мінімальний рівень безпеки на дорозі. Вам не потрібно бути юристом, але потрібно мати ремені безпеки — у вигляді політик, згод і доступу.

6.2 ПОЛІТИКА КОНФІДЕНЦІЙНОСТІ: ОБОВ'ЯЗКОВИЙ МІНІМУМ

Політика конфіденційності:

- формалізує, що ви обробляєте персональні дані відповідально;
- демонструє, що ви дотримуєтесь закону і поважаєте приватність;

- потрібна для партнерів, донорів, міжнародних грантів;
- дозволяє уникнути непорозумінь і конфліктів.

Що має містити базова політика?

Ось мінімальний набір пунктів, які повинна включати ваша політика:

Розділ	Зміст
1. Хто збирає дані	Назва організації, контакти
2. Які дані збираються	Ім'я, email, телефон, фото, IP, тощо
3. З якою метою	Реєстрація на заходи, зворотний зв'язок, статистика
4. Як обробляються	У Google Forms, CRM, внутрішніх таблицях
5. Хто має доступ	Вказати рівні доступу: лише співробітники, партнери, тощо
6. Скільки часу зберігаються	Наприклад: до 1 року після завершення проєкту
7. Як видалити або змінити дані	Email для запиту на видалення чи зміну
8. Куди звертатися у випадку питань	Контактна особа, email, телефон

Рекомендується додати останній пункт: "Ми можемо оновлювати цю політику в майбутньому. Зміни будуть публікуватися на нашому сайті або повідомлятися користувачам."

Приклад короткої політики (для друку/сайту)

Політика конфіденційності

Ця політика описує, як [назва організації] обробляє ваші персональні дані.

Ми можемо збирати ім'я, email, телефон, фото, IP-адресу для організації заходів, зворотного зв'язку та покращення сервісу.

Дані зберігаються в захищеній формі на серверах Google або внутрішніх системах.

Доступ до даних мають лише працівники організації. Термін зберігання — до 12 місяців після завершення відповідного заходу або проєкту.

Ви можете звернутись для зміни чи видалення ваших даних на email:

privacy@org.ua

[назва організації], контактна особа: Ім'я Прізвище

Чого не варто робити

- Копіювати політику з великих сайтів (там складна юридична мова і GDPR);
- Писати "ми нічого не зберігаємо" — це майже ніколи не правда;
- Ігнорувати запити людей щодо їхніх даних — навіть якщо це "незручно".

Політика конфіденційності — це сигнал: ми діємо відповідально. Це не папірець "для перевірки", а засіб зменшити ризики і побудувати довіру.

6.3 ЗГОДА НА ОБРОБКУ ДАНИХ: КОЛИ І ЯК

Коли потрібна згода?

Згода на обробку персональних даних потрібна у всіх випадках, коли:

- ви збираєте непублічну інформацію (ім'я, телефон, email, тощо);

- дані зберігаються або обробляються в інформаційних системах;
- ви хочете використати дані публічно (фото, відео, цитати);
- дані можуть бути передані третім сторонам (партнерам, донорам);
- є ризик, що інформація буде зберігатися довше, ніж “на момент проведення заходу”.

Якщо сумніваєтесь — краще отримати згоду, ніж не отримати.

У яких випадках згода не обов’язкова

- Публічна подія, на якій немає збору персональних даних.
- Людина сама публікує свої дані (наприклад, у Facebook) і передає вам їх добровільно.
- Ви не зберігаєте ці дані після завершення процесу (наприклад, телефон дзвінка, не збережений ніде).

Але навіть у таких випадках краще мати підтвердження наміру використання.

Якою має бути згода?

Згода повинна бути:

Критерій	Пояснення
Добровільною	Людина не повинна бути змушена
Інформованою	Зрозуміло пояснено, що саме буде з даними
Однозначною	“Я згоден”, а не просто галочка без пояснення
Залежною від мети	Якщо мета змінюється — потрібна нова згода

Формати згоди

Формат	Пояснення	Коли використовувати
Паперова форма	Підпис на анкеті чи заяві	Заходи, договори, внутрішні документи
Цифрова форма (Google Form)	Галочка або текст “Я погоджуюсь”	Онлайн-реєстрація, опитування
Email-підтвердження	“Я підтверджую згоду на...”	Індивідуальні кейси, листування
Згода через платформу	Кнопка “Приймаю”	Сайт, CRM, портал

Приклад тексту згоди

Я погоджуюсь на обробку моїх персональних даних (ім’я, електронна адреса, телефон), наданих у цій формі, з метою реєстрації на захід/отримання інформації/участі в проєкті.

Дані не будуть передані третім сторонам без окремої згоди. Мені відомо про право відкликати згоду у будь-який момент, звернувшись за адресою privacy@org.ua.

У Google Form це можна оформити як окреме запитання з обов’язковим підтвердженням.

Часті помилки

- Немає згадок про цілі обробки (навіщо ви це збираєте);
- Немає контактів для відкликання згоди;
- Згода “загальна на все” без конкретики;
- Люди не розуміють, що погоджуються на довготривале зберігання.

Зберігання згод

- У папці або базі даних (електронно чи на папері);
- Прив’язано до імені або ID особи;
- Із можливістю швидко знайти і підтвердити її наявність.

У будь-якому процесі збору персональних даних — згода є правовим “щитом” для організації. Вона формалізує відповідальність і захищає обидві сторони.

6.4 КОЛИ І КОМУ ПОТРІБНО ПОВІДОМЛЯТИ ПРО ВИТІК

Що таке “витік даних”?

Витік персональних даних — це будь-яка ситуація, коли інформація:

- стала доступною неавторизованим особам;
- була надіслана або скопійована не туди;
- загублена або викрадена (наприклад, втрачений пристрій);
- доступна в Інтернеті через відкриті налаштування.

Навіть тимчасовий відкритий доступ до Google-документа з особистими даними — це теж витік.

Чому важливо повідомити?

- Це вимога закону (ЗУ “Про захист персональних даних”).
- Це етичний обов’язок перед тими, чиї дані скомпрометовано.
- Це попередження повторних витоків — дозволяє іншим вжити заходів.
- Це зменшує репутаційні ризики (прозорість підвищує довіру).

Коли обов’язково повідомляти?

Тип витоку	Повідомлення обов’язкове?
Витік прізвищ, email, телефонів	✓ Так, особам, яких це стосується
Доступ до фінансових, медичних або чутливих даних	✓ Так + рекомендовано повідомити уповноваженого з питань захисту персональних даних
Масовий витік (100+ осіб) або витік через публічну платформу	✓ Так + варто повідомити партнерів, донорів
Випадкове відкриття документа без чутливої інформації	✗ Необов’язково (якщо доступ закрито до перегляду)

Як повідомити про витік?

1. Якнайшвидше після виявлення (рекомендовано — протягом 72 годин).
2. Простими словами, без технічного жаргону.
3. Чітко пояснити, що сталося, кого це стосується, що вже зроблено і що слід зробити.

Приклад повідомлення:

Шановні учасники,

3 квітня ми виявили, що один із документів із вашими контактними даними тимчасово мав відкритий доступ. Ми одразу обмежили доступ, перевірили журнал активності і не зафіксували несанкціонованих переглядів.

З міркувань безпеки просимо вас змінити паролі, якщо ви використовували ті самі email/логіни на інших ресурсах.

Якщо у вас є запитання — звертайтесь до [Контактна особа, email].

Чи потрібно повідомляти державу?

В Україні діє Уповноважений Верховної Ради з прав людини — саме він є регулятором у сфері захисту персональних даних.

Повідомляти офіційно рекомендовано у випадках:

- великого обсягу даних;
- суттєвої шкоди для осіб;
- систематичних порушень;
- офіційних запитів/скарг від постраждалих.

Форму повідомлення можна подати через лист, email або через контактну форму на сайті Уповноваженого.

Внутрішній облік інцидентів

Кожен інцидент варто фіксувати у журналі кіберінцидентів, навіть якщо він не призвів до великої шкоди. Це:

- допоможе під час перевірок;
- покаже, що організація діє відповідально;
- дозволить виявити слабкі місця у політиках або навчанні.

Витік даних — це не лише загроза, але й можливість покращити процеси. Вчасне повідомлення зменшує ризики і підвищує довіру.

6.5 ЯК ДІЯТИ ПІД ЧАС ПЕРЕВІРКИ АБО ЗАПИТУ ВІД РЕГУЛЯТОРА

Що означає перевірка?

Перевірка або запит може надійти від:

- Уповноваженого Верховної Ради України з прав людини (у сфері персональних даних);
- донорської організації або міжнародного партнера;
- суду або поліції (в контексті інциденту, скарги або розслідування).

Це не обов'язково "штраф" — часто це просто прохання надати пояснення або документи.

Що зазвичай запитують?

Що можуть запитати	Приклад
Копію політики конфіденційності	"Просимо надати чинну редакцію політики"
Інформацію про згоду осіб	"Надайте копії форм, де отримано згоду учасників"
Хто відповідальний за захист даних	"Назвіть контактну особу, яка відповідає за захист"
Документацію щодо інциденту	"Надайте опис, хронологію та дії, здійснені після витоку"
Підтвердження захисту	"Які засоби ви використовуєте для обмеження доступу до даних"

Як підготуватись до відповіді

1. Зберігайте спокій. Запит — це процедура, не вирок.
2. Зберіть документи. Підготуйте політику, зразки згод, інструкції.
3. Призначте відповідальну особу. Один голос — одна лінія відповідей.
4. Сформулюйте чітку письмову відповідь. Краще — офіційним листом із переліком документів.
5. Не вигадуйте. Якщо чогось немає — напишіть чесно: "В процесі розробки. Очікувана дата завершення — …".

Приклад відповіді на запит

Шановні колеги,

У відповідь на ваш запит щодо захисту персональних даних у нашій організації, повідомляємо наступне:

- *Політика конфіденційності додається (Додаток 1);*
- *Зразок форми згоди на обробку даних — Додаток 2;*
- *Відповідальна особа — Іваненко І.П., координатор з цифрової безпеки, ivanenko@org.ua;*
- *Доступ до даних регулюється відповідно до Інструкції з кібербезпеки (Додаток 3).*

Ми відкриті до співпраці і готові надати додаткову інформацію за потреби.

Поради

- Зберігайте електронну копію всіх офіційних листів і відповідей.
- Створіть папку "Документи з кібербезпеки", де є:
  - політика конфіденційності;
  - шаблон згод;
  - внутрішні інструкції;
  - журнал інцидентів;
  - контакти відповідальних осіб.

Чого не варто робити

- Ігнорувати запит — це підстави для санкцій або ескалації;
- Давати недостовірну інформацію — це легко перевірити;
- Перекидати відповідальність — “то наш IT-спеціаліст винен” виглядає непрофесійно;
- Панікувати — у більшості випадків це формальна перевірка.

Якщо ваша організація веде хоча б базовий облік і має основні документи — ви вже на правильному шляху. Перевірка — це можливість вдосконалитись, а не покарання.

ВИСНОВКИ

У сучасному цифровому середовищі кіберзахист — це не привілей, а базова потреба кожної організації. Цей довідник показує, що для формування культури безпеки не обов’язково бути технічним спеціалістом або витрачати великі ресурси. Достатньо:

- усвідомити базові загрози;
- впровадити мінімальні політики і правила;
- навчити команду;
- перевіряти свою роботу через аудит;
- бути готовими реагувати — юридично, технічно та емоційно.

Найважливіше — послідовність і зрозумілість: навіть прості речі, виконані системно, дають результат.

Організації, які з повагою ставляться до даних, працівників та партнерів, отримують довіру і стабільність у цифрову добу.