МЕТОДИЧНИЙ ПОСІБНИК

ІЗ ЦИФРОВОЇ БЕЗПЕКИ

ДЛЯ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА, АКТИВІСТІВ/ОК ТА ВОЛОНТЕРІВ/ОК

КИЇВ
2023

ЗМІСТ

ВСТУП

Посилена увага до цифрової безпеки організацій громадянського суспільства та активістів/ок важлива з огляду не лише на специфіку діяльності громадських активістів/ок, правозахисників/ць та волонтерів/ок, а й цифрові ризики, спричинені війною в Україні.

Особливу увагу на свою цифрову безпеку мають звернути правозахисники/ці; активісти/ки, які працюють з військовими та постраждалими цивільними; волонтери/ки, які опікуються деокупованими та прифронтовими територіями.

Від початку повномасштабного вторгнення Росії урядова команда реагування на комп'ютерні надзвичайні події CERT-UA зареєструвала та дослідила понад 1500 кібератак на Україну. Більшість з них були здійснені Російською Федерацією.

Серед головних цілей хакерів у CERT-UA називають спроби отримання розвідданих про логістику, озброєння й плани Сил безпеки та оборони, спроби виведення з ладу об'єктів критичної та інформаційної інфраструктури, позбавлення доступу громадян до державних послуг і сервісів, банківського обслуговування тощо.

Окремо спеціалісти виділяють інформаційно-психологічні операції та дезінформаційні вкиди задля підриву довіри до органів державної влади, Сил безпеки та оборони, поширення панічних настроїв серед населення.
Проте навіть якщо ви не дотичні до згаданих сфер, це ще автоматично не означає, що ви не потрапите в поле зору шахраїв/йок. Окрім російських хакерів, які шукають тематичну інформацію, і надалі існують зловмисники/ці, які заробляють гроші, зламуючи чужі акаунти, шантажуючи людей або заражаючи їхні пристрої шкідливим програмним забезпеченням.

Тому важливо в розмові про цифрову безпеку пам'ятати про контекст — роботу вашої організації; країну, у якій ви зараз перебуваєте, ступінь чутливості інформації, яка у вас є. Врахування контексту допоможе правильно оцінити власні ризики й створити ефективні політики, не розпорошуючи увагу на речі, що не співвідносяться з реальністю.

Цифрова безпека — це безперервний процес, і концентрується вона на трьох параметрах: конфіденційність, цілісність, доступність.

Конфіденційність — це явище, під час якого доступ до інформації маєте тільки ви та ті особи чи організації / установи, кому ви дали такий дозвіл (наприклад, сайт, на якому ви зареєструвалися або ввели номер платіжної картки для оплати товару, або ваші співрозмовники/ці тощо).

Цілісність — це стан, за якого ніхто з неавторизованих осіб не змінює інформацію, вміст та структуру файлів тощо.

Доступність — ваша можливість мати доступ до ресурсу тоді, коли потрібно, у тому обсязі, якому необхідно. До цього параметра можна віднести захист сайтів від DDoS-атак (атака, спрямована на те, щоб зробити сайт недоступним для використання) або недоступність комп'ютера через його зараження вірусом.

У наступних розділах цього методичного посібника ми детальніше проаналізуємо основні ризики та загрози цифровій безпеці ОГС та активістів/ок, розберемося з процесом інвентаризації цифрових активів, пояснимо, як правильно провести оцінювання ризиків цифрової безпеки, і наголосимо на важливості наявності та практичного впровадження безпекових політик і процедур.

Методичний посібник підготовлено Аліною Елєвтєровою, незалежною експерткою із цифрової безпеки, для організацій громадянського суспільства та активістів/ок у співпраці з експертами/ками ЦЕДЕМ.

Цей методичний посібник створений ЦЕДЕМ у межах проєкту «Ініціатива секторальної підтримки громадянського суспільства України», що реалізується ICAP Єднання у консорціумі з Українським незалежним центром політичних досліджень (УНЦПД) та Центром демократії та верховенства права (ЦЕДЕМ) завдяки щирій підтримці американського народу, наданій через Агентство США з міжнародного розвитку. ICAP Єднання несе повну відповідальність за зміст, який може не відображати поглядів АМР США або Уряду Сполучених Штатів Америки.

РОЗДІЛ 1. Аналіз основних ризиків і загроз цифровій безпеці активіста/ки

Коли ми говоримо про цифрову безпеку, щоб вистачило уваги, ресурсу та бажання нею займатися, варто сконцентруватися на власних цифрових активах.

Цифрові активи — це все, що для вас важливе в мережі. До них можна віднести як акаунти в онлайн-банкінгу, так і сайти, акаунти в соцмережах, паролі, переписки в месенджерах тощо. Також до активів можуть належати всі предмети, які становлять цінність для вас та/або організації, — робочі комп'ютери, роутери, принтери, інша офісна техніка, паперові документи тощо. Власне, про захист активів ми й будемо говорити.

Також слід пам'ятати, що безпека — це компроміс між захищеністю та доступністю. Тобто до якихось практик буде потрібно звикнути (наприклад, до використання двофакторної аутентифікації), але вони в підсумку підвищать ваш рівень безпеки.

Структура цього посібника передбачає перехід від особистої безпеки до масштабування таких практик на всю організацію. У цьому розділі говоритимемо про безпеку особисту, надалі — про те, як створити безпекову систему в усій організації.

1.1. Атаки онлайн

Для зручності атаки можна поділити на два типи — онлайн і офлайн. У цьому підрозділі говоритимемо про те, що може відбутися з вашими цифровими активами онлайн.

Від чого захищатися?

1.1.1. Фішинг — це одна з найпростіших і найпопулярніших атак. Простими словами, це шахрайство в кіберпросторі. Один зі сценаріїв — коли людина видає себе за когось, щоб отримати від вас щось важливе. Шахраї/йки хочуть отримати гроші чи інформацію про доступ до облікових записів, пристроїв. Часто вони видають себе за людей, які мають довіру, — представників/ць держструктур, військових чи волонтерів/ок, іноді навіть ваших друзів у соцмережі тощо.

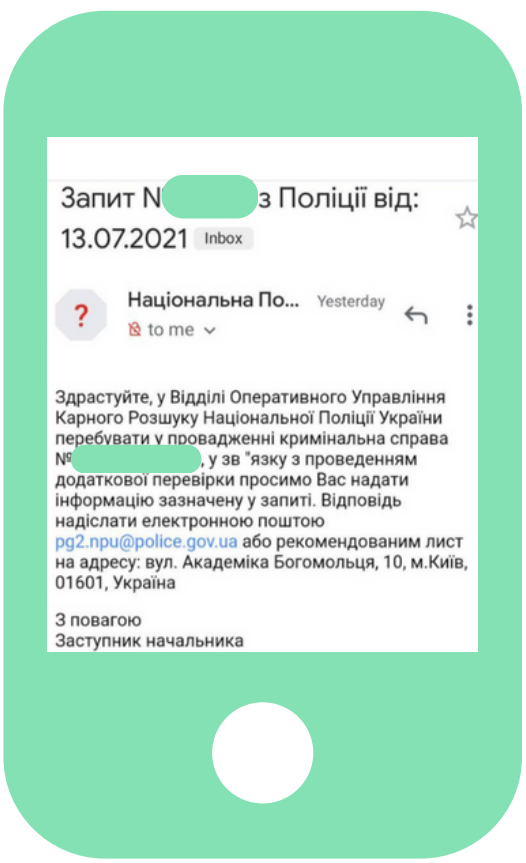
Фішинг концентрується на особливостях людської психіки. Найчастіше шахраї/йки використовують сильні емоції, щоб людина з більшою ймовірністю виконала певну дію. Ця атака може статися на будь-якій платформі, навіть у приватних повідомленнях у месенджері.

Основні гачки шахраїв/йок:

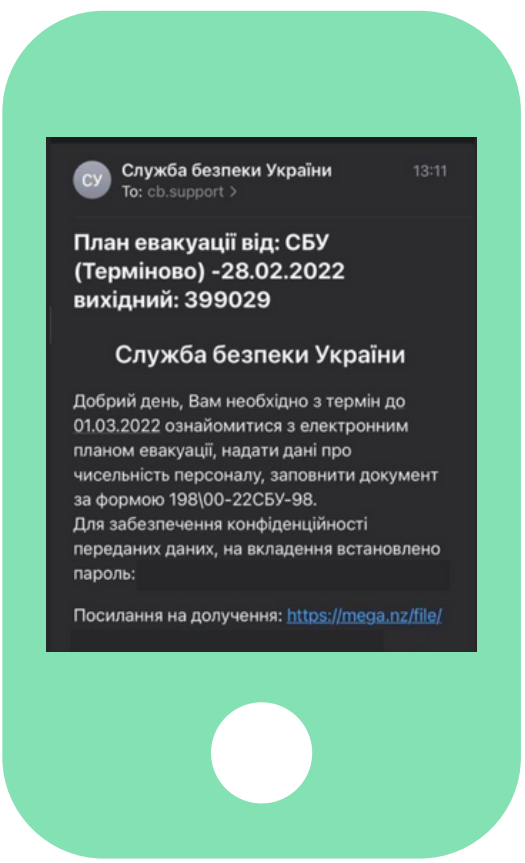
ЕМОЦІЇ
(налякати чи дати надію)

ЗАКЛИК ДО ДІЇ
(ввести пароль, щось завантажити)

ОБМЕЖЕННЯ В ЧАСІ
(потрібно терміново)

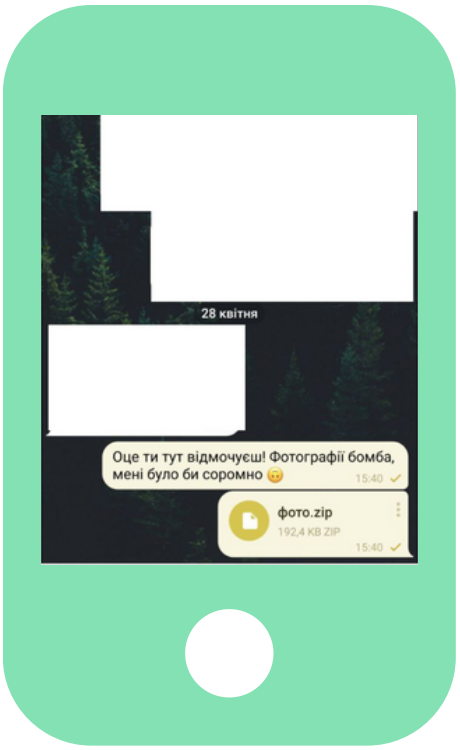


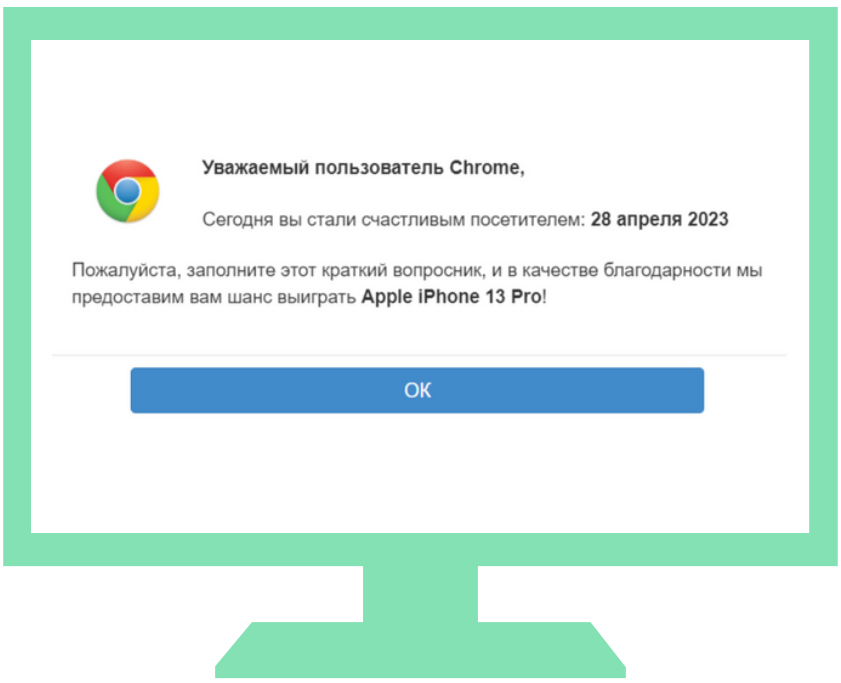
ФІШИНГ



ФІШИНГ

ФІШИНГ





Як розпізнати фішинг?

Звертайте увагу на вміст повідомлення, звертання та підписи — вони можуть видаватися дивними.

У повідомленні є вимога чи заклик до термінової дії.

Повідомлення тисне на емоції (сором, страх, надію, обіцянку виграшу тощо).

У тексті можуть траплятися неточності та помилки.

Посилання в повідомленні замасковане або підставне.

Посилання від людини, з якою ви давно не спілкувалися.

Є підозріле вкладення до листа.

Ви не очікуєте ніяких листів подібного формату.

Захист від фішингу можна поділити на технічний та нетехнічний.

Нетехнічний захист

Фішинг — це радше психологічна атака. Не робіть швидких дій, не поспішайте, знайдіть надійний спосіб верифікувати те, що вам справді пише певна людина. Файл і покликання можна перевірити на наявність вірусів на сервісі «Virus Total».

Перевіряйте адресу відправника, покликання, не відкривайте одразу покликання чи файли, використовуйте альтернативний канал зв'язку з відправником_цею повідомлення, щоб верифікувати його_її. Також добре мати людину, до якої можна звернутися, якщо ви отримаєте або побачите щось підозріле.

Технічний захист

Встановіть на важливі акаунти двофакторну аутентифікацію — навіть якщо шахрай/йка отримає ваш пароль, додатковий спосіб захисту утримає його/її від повного доступу.

Майте антивірус на комп'ютері, який у фоновому режимі сканує файли.

Оновлюйте операційну систему, програми та додатки. Оновлення захищають від вразливостей систем, які можуть експлуатувати зловмисники.

Якщо так сталося, що ви повелися на фішинг, то:

Зверніться по допомогу до колег або технічних спеціалістів/ок.

Попередьте людей, з якими ви спілкуєтеся за допомогою цього каналу комунікації, що вас зламали.

Перегляньте ваші безпекові налаштування, змініть паролі.

1.1.2. Віруси

Одна з найбільш звичних атак — завантаження шкідливого програмного забезпечення або, іншими словами, вірусів. Багато з вас з ними стикалися. Віруси можуть різним чином шкодити вашій системі. Деякі віруси шифрують ваші файли, інші — перехоплюють управління вашим комп'ютером, а є такі, що тихо та непомітно стежать за всім, що ви робите.

Як ми можемо підхопити вірус?

1. **З листа.** Цей спосіб ми розглянули раніше.

2. **З чату в месенджері.** До чатів застосовуються всі правила безпеки, як до звичайної пошти.

3. **Разом з піратським програмним забезпеченням.** У зламаному ПЗ можуть бути віруси, які активуються або одразу при встановленні програми, або коли зловмиснику_ці необхідно буде скористатися обчислювальними можливостями вашого комп'ютера. Тому початково всі піратські програми небезпечні та створюють велику вразливість у вашій системі.

4. **На флешці.** Ви можете знайти флешку на вулиці чи вам її дасть довірена людина. У будь-якому випадку кожну флешку, яку ви вставляєте в комп'ютер, потрібно просканувати антивірусом. Окрім цього, при підключенні флешки операційна система запропонує вам декілька дій на вибір: відкрити флешку в провіднику, відформатувати флешку або запустити автоматично. Ніколи не погоджуйтеся на автозапуск флешки, оскільки в програмі автозапуску може ховатися вірус. Відкрийте флешку в провіднику й далі досліджуйте потрібні вам файли.и захищаєте обидва облікові записи

Як захиститися від вірусів?

Встановіть і завжди оновлюйте антивірус. Ніколи не використовуйте зламані піратські версії антивірусів, якщо не хочете купувати якийсь з них, просто вмикайте Захисник Windows.

Використовуйте ліцензійне ПЗ. Спеціалізовані програми варто купувати, інші за можливості можна замінити безкоштовними аналогами.

Робіть час від часу ревізію програм. Якщо ви чимось не користуєтеся певний час, видаляйте програму. Стежте, чи ваші програми оновлюються. Регулярні оновлення — найкращий захист від вразливостей.

Використовуйте комп'ютер з облікового запису користувача, а не адміністратора. Для цього треба створити окремий обліковий запис і забрати в нього права адміністратора. Якщо ви захищаєте обидва облікові записи паролем, поставте різні на обліковий запис адміна та користувача. Це можна зробити на комп'ютерах з операційною системою Windows. Інструкцію можна почитати тут.

Шкідливе ПЗ можна завантажити й на телефон.

Не завантажуйте додатки з неофіційних джерел. Довіряйте тільки офіційним маркетам (Google Play, App Store) або офіційним сайтам розробників додатків.

Якщо у вас телефон на операційній системі Android, не зайвим буде завантажити антивірус. Зверніть увагу: безкоштовні версії антивірусів скоріше за все не скануватимуть систему в автоматичному режимі, тому це доведеться робити вручну. Для пристроїв Apple цілком достатньо регулярно оновлювати їх.

Оновлюйте операційну систему та додатки. Якщо можливо, налаштуйте автоматичне завантаження оновлень.

Видаляйте додатки, якими ви не користуєтеся та за можливості ті, які не оновлюються або не підтримуються самими розробниками.

1.1.3. Атаки на паролі

Наступні за популярністю атаки — на паролі. Окрім фішингу, зловмисники/ці можуть викрадати паролі й іншим чином.

Перша небезпека — **повторне використання паролів.** Це може відбуватися так: на ваших основних акаунтах використовується однаковий пароль. Якийсь з них виявився скомпрометованим (наприклад, через злам самого сервісу, тобто стався витік даних користувачів_ок або вас «зафішили»). Інформацію про паролі та логіни користувачів_ок зловмисники/ці можуть формувати в бази даних і потім продати іншим злочинцям, недобросовісним компаніям для розсилок тощо. З цього моменту дані починають жити своїм життям, і не зрозуміло, хто і коли спробує атакувати ваші акаунти. Якщо атака буде таргетована, тобто зловмисник_ця прагнутиме зламати якнайбільшу кількість акаунтів, існує ризик втратити багато важливої інформації.

Друга — **використання простих і типових паролів.** За даними компанії «Nord Pass», станом на 2023 рік серед користувачів одними з найпопулярніших паролів досі є «qwerty», «password», «12345» тощо. Про ці комбінації так само відомо і зловмисникам_цям, тому вони будуть першими для підбору та використання.

Простими паролями також можуть бути ті, які містять інформацію про користувача/ку, яка або є публічною, або її легко дізнатися. Наприклад, комбінація ім'я + дата народження, або номер телефону, або інші персональні дані суттєво підвищують шанси зламу акаунту при таргетованих атаках.

Третя небезпека — **ненадійне місце збереження паролів.** Цей сценарій може призвести до двох наслідків. Перший — ненадійне місце зламає шахрай. Другий — ви втратите паролі або доступ до місця їх збереження і не зможете отримати доступ до акаунтів. Обираючи місце збереження, звертайте увагу не тільки на комфорт, але й на те, наскільки воно захищене від зламу чи втрати.

Що варто враховувати, коли ми говоримо про паролі:

Не використовуйте один пароль для різних сервісів.

Визначте декілька найбільш важливих для себе сервісів (пошта, онлайн-банкінг, акаунти в соцмережах) і використовуйте для них унікальні паролі. Якщо зловмисник / ця отримає пароль, що використовується в декількох акаунтах, він / вона автоматично матиме доступ до всіх цих акаунтів.

Щоб не забути паролі, придумайте комфортну для себе систему збереження та генерації паролів. Вона має бути надійною, проте не сильно ускладнювати ваше життя. Якщо вам часто потрібно вводити пароль, а довгий набір випадкових символів / цифр для вас обтяжливий, скористайтеся методом парольних фраз. Це може бути набір випадкових слів, які розбавлені літерами, спеціальними символами, цифрами. У підсумку отримаєте комбінацію, яку легше ввести та запам'ятати. Приклад парольної фрази: 1!chashka-1!ruchka- 1!plyashka. За такою логікою можна формувати довгі складні комбінації, які простіше запам'ятати та ввести.

Послуговуйтеся двофакторною аутентифікацією. Це значить, що при спробі ввійти в акаунт вам, окрім пароля, потрібно буде додатково підтвердити, що ви — це ви. Найпростішим методом, з яким ви могли стикатися, є додатковий код у SMS або push-сповіщення від додатка. Необхідність мати доступ до другого фактору суттєво зменшить шанс успішної атаки на акаунт, якщо зловмисник_ця вже знатиме ваш пароль.

Як можна зберігати паролі:

1. **Аналоговий спосіб** (паперовий записник) — хоча багато людей вважає цей спосіб застарілим, його важливим плюсом є неможливість онлайн-зламу. Основний мінус — втрата паперового носія може призвести до втрати доступу до облікових засобів.

2. **Зберігання в браузерах** — це зручний спосіб, оскільки дані про паролі зазвичай синхронізуються між різними пристроями при використанні одного й того ж облікового запису в браузері. Мінус цього способу — якщо ви користуєтеся вашими пристроями спільно з іншими людьми, він небезпечний, оскільки будь-хто зі співкористувачів_ок може побачити або використати ваші дані. Іноді навіть випадково, тому що браузер сам підставить ваш логін і пароль для входу, якщо він збережений у ньому.

3. **Менеджери паролів** — їх суть полягає в тому, що спеціальна програма в зашифрованому вигляді зберігає всі паролі й вимагає введення одного мастер-пароля, щоб отримати доступ до них. Програму можна встановити на комп'ютер, телефон, також вони існують як розширення для браузера. Окрім збереження паролів, такі програми пропонують автогенерацію складних комбінацій, які не потрібно запам'ятовувати, а лише зберегти в менеджері паролів. Деякі з них мають безплатну версію, інші працюють лише за підпискою. Приклади таких програм: «LastPass», «Bitwarden», «Keepass», «NordPass».

Якими мають бути паролі:

- Довгі. Атака методом перебору (brute force) досі трапляється на різних платформах. Що довший ваш пароль, то довше обчислювальна система буде його вгадувати. З роками обчислювальні можливості збільшуються, тому довші комбінації означають надійніший захист від подібної атаки. Якщо можливо, намагайтеся генерувати паролі від 13 символів. Тоді, навіть якщо вони складатимуться лише з літер, комп'ютеру знадобиться рік, щоб вгадати комбінацію (дані від сервісу security.org).
- Унікальні. У випадку витоку одного з паролів ви зменшуєте ризик того, що зловмисник_ця зламає й інші ваші акаунти.
- Складні. Збагачення парольного алфавіту, тобто варіації символів у вашому паролі, ускладнить шанс того, що комбінацію швидко вгадають або підберуть.
- Нетипові.
- Збережені. Тому що, окрім інших факторів, нам також важливо зберегти доступ до ресурсу та інформації для нас самих.

Превентивні способи захисту від атак на паролі:

1. Перевірити, чи станом на зараз ваші акаунти та паролі фігурують у витоках даних. Якщо ви користуєтеся Google Chrome і зберігаєте там свої дані для входу, то в налаштуваннях можна подивитися цю інформацію в розділі Password Manager.
2. Подумати про певний алгоритм зберігання паролів. Зручна для вас система збереження підвищить шанси, що ви будете генерувати складніші комбінації, бо не переживатимете, що забудете їх.
3. Перевірити налаштування двофакторної аутентифікації на важливих облікових записах. Якщо вона відключена, то налаштувати її.

Багатофакторна аутентифікація значно захищає облікові записи від несанкціонованого віддаленого доступу. Її суть у створенні додаткового фактора захисту на випадок, якщо хтось дізнався пароль користувача.

Способи двофакторної аутентифікації:

Через смартфон (код у SMS, месенджері, push-повідомлення) — після введення пароля для входу необхідно також додатково ввести одноразовий пароль, який направляється на смартфон користувача.

Програма «Генератор кодів» — після введення пароля для входу необхідно ввести код, який генерується в спеціальному додатку на смартфоні або мобільному додатку сайту. Коди оновлюються що тридцять секунд.

Резервні коди — у випадку втрати пароля необхідно ввести резервний код, який був згенерований сервісом раніше. Коди рекомендується зберігати в аналоговому вигляді (наприклад, у паперовому блокноті тощо). Цей спосіб необхідний тоді, якщо ви втратили з якоїсь причини доступ до SIM-карти або телефону.

Важливо на кожному сервісі, важливому для конфіденційності даних користувача/ки, налаштувати двофакторну аутентифікацію.

1.1.4. Захист сайтів

Сайти організації також можуть бути вразливим місцем, особливо якщо в команді немає постійного_ї спеціаліста_ки, що надає технічну підтримку. У складних випадках у будь-якому разі доведеться звертатися по допомогу, але якщо сайтом займається хтось із членів організації, ось декілька порад, на що слід звертати увагу.

Безпека хостингу. Хостинг — це послуга, яку надає певна компанія для збереження інформації на сервері та доступу до неї в будь-який час. Важливо розуміти, яка компанія хостить ваш сайт, — чи вона велика, чи допомагає створювати резервні копії сайту, чи оновлює ПЗ серверів. Також у контексті постійної загрози ракетних обстрілів можна дізнатися, де зберігаються дата-центри компанії, — відповідь на ці питання допоможе ідентифікувати ймовірні вразливості.

Окрім аналізу самого хостингу, варто ще й захистити обліковий запис. який створюється на сервісі. Не зайвим буде дізнатися, чи надійний там пароль, чи є можливість увімкнути двофакторну аутентифікацію, у кого з команди є доступ до панелі керування, хто оплачує хостинг та оренду доменного імені.

Щоб зменшити ризик зламу, можна також використати нестандартне ім'я користувача. Тобто не називати акаунт адміністратора admin, а редактора — user. Краще скористатися чимось нетиповим — можливо, для вас спрацює варіант, коли як логін виступає ім'я та прізвище людини, якій надається доступ.

Оновлення CMS вашого сайту. CMS (Content Management System, або система керування вмістом) — це програмне забезпечення для створення вебсайтів. Однією з найпопулярніших систем є WordPress. Оновлення до останньої версії дозволяє обійти загрози для ресурсу, які могли зашкодити за старішої версії.

Оновлення плагінів і тем, які ви використовуєте. Встановлюйте лише надійні та перевірені теми та плагіни, які часто оновлюються. Якщо інформація про плагін відсутня або її мало, краще його не встановлювати. Також не забувайте видаляти вже не потрібні плагіни та ті, до яких не випускаються оновлення протягом тривалого часу.

Чи робиться резервна копія сайту, де вона зберігається і чи вона не пошкоджена. Іноді після оновлення системи або плагінів з'являються проблеми із сумісністю зі старими версіями, через що частина інформації може пошкоджуватися. Важливо перевіряти, чи все з нею в порядку. Якщо резервної копії немає, то при зламі або видаленні сайту існує велика ймовірність втратити його назавжди.

Наявність SSL-сертифіката. Він підтверджує, що дані між користувачем і сервером передаються в зашифрованому вигляді. Як дізнатися, чи ваш сайт підтримує захищене з'єднання: по-перше, подивіться на адресний рядок браузера, чи є там «замочок». По-друге, клацніть на адресу сайту й перевірте, чи вказано на початку «https». Якщо так, це означає, що сайт користується захищеним з'єднанням. Часто хостер надає автоматично безкоштовний SSL-сертифікат, але якщо з якоїсь причини у вас його немає, подбайте про нього самостійно.

Додаткова фільтрація коментарів і захист від спам-ботів, якщо на сайті є можливість коментувати записи. Спамери можуть не тільки рекламувати свої сайти, але й вставляти посилання на фішингові ресурси чи завантаження шкідливого ПЗ. Також через великий потік коментарів робота сайту може сповільнюватися. Варто подумати, чи необхідна ця опція сайту взагалі і якщо потрібна, що можна зробити з подібними вразливостями.

Захист від DDoS-атак. Для цього існує дуже багато технічних способів захисту, багато компаній пропонують різні комерційні рішення. Якщо ресурсів на комерційні рішення немає, можна скористатися безкоштовними варіантами, наприклад від «CloudFlare».

1.2. Атаки офлайн

Окрім небезпек онлайн, ми можемо стикнутися з офлайн-інцидентами. Сюди можна віднести як і вилитий сік на комп'ютер, так і загрозу вилучення техніки під час обшуку. У цьому підрозділі подивимося, як захиститися від загроз офлайн.

Фізичний доступ може бути короткостроковим (якщо ви залишили десь свій пристрій ненадовго і відійшли, а зловмисник/ця у цей час пробує його зламати) і довгостроковим (якщо пристрій викрали або вилучили під час обшуку).

1.2.1. Захист від короткострокового доступу

Головне завдання захисту від атак офлайн — упевнитися, що зловмисник/ця не зможе отримати доступ до інформації на пристрої, якщо він_вона якимось чином заволодіє вашим телефоном чи комп'ютером.

Встановіть пароль на вхід у систему на лептопі. Оскільки там немає обмежень від перебору пароля, то просту комбінацію можна швидко підібрати (актуально в разі тривалого доступу). Тому для входу бажано використовувати довгі та складні паролі від 13 символів. Якщо ваш пристрій підтримує Face-id або Touch-id, можна налаштувати вхід цим способом, проте так само збережіть пароль для входу. Він знадобиться, якщо біометричний вхід буде недоступний.

Встановіть пароль на вхід для смартфона. Для цього існує багато варіантів: Face-id, Touch-id, пін-код, графічний ключ і пароль. Найслабший варіант — це графічний ключ і чотиризначний пін-код. Краще використовувати щонайменше шестизначний пін-код. На смартфонах додатково можна налаштувати блокування телефону після десяти невдалих спроб введення пароля. Тоді зловмисники/ці будуть дуже обмежені в переборі комбінацій.

Налаштуйте автоматичне блокування екрана через певний час бездіяльності. На смартфоні бажано обрати опцію 30 секунд або менше, на комп'ютері — 5–15 хвилин. Коли ви залишаєте без нагляду телефон або лептоп, спробуйте привчити себе до ручного включення блокування. На телефоні вам потрібно тільки натиснути на клавішу блокування. Якщо ваш комп'ютер на Windows, вам потрібна комбінація Windows + L. На макбуку — налаштуйте блокування одразу після закриття кришки.

Перегляньте налаштування попереднього перегляду сповіщень на екрані блокування. Така функція доступна як на телефоні, так і лептопах. Якщо ви не хочете, щоб кожна людина, яка дивиться вам через плече, прочитала вміст вашої переписки, що спливає у сповіщеннях, рекомендуємо налаштувати сповіщення без вмісту. Тобто ви будете бачити, куди вам прийшло повідомлення, але не його вміст та відправника, поки не розблокуєте пристрій.

1.2.2. Захист від довгострокового доступу

Найкращим варіантом захисту від довгострокового доступу до пристрою є шифрування. Зловмисник/ця, який не знає пароля для розшифрування накопичувача вашого комп'ютера, не зможе отримати доступ до інформації. Звісно, для цього ви повинні мати надійний пароль, а комп'ютер має бути заблокований на момент, коли він потрапить у руки зловмисника/ці.

Шифрування можна дуже легко налаштувати на нових пристроях з версіями Windows 10 або 11 Pro, Enterprise або Education, достатньо увімкнути вбудовану утиліту BitLocker.

Дуже важливо зберегти ключ відновлення, який вам згенерує програма, тому що без нього не вдасться відновити дані. Ключ може знадобитися у випадку, якщо комп'ютер розбиратиметься або через інші причини система зчитає те, що відбувається, як несанкціонований доступ. Ключ треба зберегти не на жорсткому диску комп'ютера. Це може бути ваш перевірений знімний носій, менеджер паролів або хмарне сховище.

Якщо у вас версія Windows Home, то вбудованої утиліти для шифрування система не має, але можна використати інше ПЗ, наприклад VeraCrypt.

Якщо ви користуєтеся пристроєм від Apple, то можете використати вбудовану утиліту FileVault.

Важливо: якщо ви вирішили зашифрувати старий пристрій або використати невбудоване ПЗ вашої операційної системи, проконсультуйтеся зі спеціалістом.

1.2.3. Захист від втрати інформації

Резервне копіювання є важливою складовою захисту даних. Якщо бекапи не налаштовані, існує ризик назавжди втратити важливу інформацію разом з втратою або поломкою пристрою.

Що треба знати про бекапи:

Завжди робіть резервні копії важливих даних (у хмару або на окремий пристрій, залежить від того, що вам зручніше).

Налаштуйте автоматичне резервне копіювання необхідної інформації.

Регулярно перевіряйте бекапи, чи вони повні, чи вони доступні.

Пам'ятайте, що бекапи мають бути ізольованими та захищеними.

Як можна створювати резервні копії:

Регулярне резервне копіювання на зовнішні накопичувачі.

Автоматична синхронізація у хмарне сховище (Google-диск, iCloud, Mega та ін.).

Синхронізація медіафайлів (Google Photo).

Синхронізація контактів.

Резервне копіювання на зовнішні накопичувачі є одним з найбільш доступних і технічно простих способів захисту. Особливо актуальне для захисту великого обсягу інформації. Серед ризиків — фізична поломка накопичувача, його втрата або отримання фізичного доступу до нього інших осіб.

Автоматична синхронізація у хмарне сховище — це хороший і надійний спосіб захисту інформації на пристроях від втрати. Він трохи технічно складніший за попередній, але водночас його налаштування не потребує глибоких спеціальних знань. Найвідоміші сервіси хмарного зберігання — Google-диск, iCloud. Серед основних мінусів — потреба підключення до інтернету для отримання доступу до інформації. Також існує ймовірність, що вам не вистачить безкоштовного обсягу сховища, яке пропонує компанія, і доведеться раз на місяць оплачувати підписку.

Подібним за змістом є спосіб захисту медіафайлів. Оскільки розмір таких файлів зазвичай більший за розмір інших текстових або табличних файлів, існують спеціальні хмарні сервіси для автоматичної синхронізації та зберігання медіа. Також ці сервіси можуть автоматично зберігати файли в хмарі, видаляючи їх на вашому пристрої, що може бути доцільно для небезпечних ситуацій, коли вас можуть спробувати змусити видалити фото.

Синхронізацію контактів мають усі сучасні мобільні телефони. Ваші дані зберігаються в обліковому записі Google або iCloud. Важливо її попередньо налаштувати. Тоді, якщо ви втратите телефон, ваші контакти не зникнуть, тому що вони зберігатимуться в обліковому записі.

1.3. Безпечна комунікація

Комунікація в організації може відбуватися двома способами — через мобільні мережі та онлайн. Для онлайн-комунікації використовують месенджери, соцмережі, пошту та додатки. Кожен спосіб має свої особливості, про які слід знати. Більш детально про те, як зробити комунікацію безпечною, говоритимемо далі.

1.3.1. Загрози мобільного зв'язку

Заради соціального експерименту один німецький політик запитав свої дані, які має мобільний оператор, і в результаті стало зрозуміло, що мобільні оператори збирають і зберігають дані про всі переміщення людини з телефоном, історію дзвінків і повідомлень (та їхній зміст), активний час роботи та відпочинку тощо.

Важливою відмінністю мобільного зв'язку від інтернету в контексті безпеки є те, що ми не можемо напряму впливати на збір персональних даних. Мобільні оператори збирають і зберігають ваші дані завдяки технічним особливостям функціонування мобільного зв'язку, окрім того, провайдер мобільного зв'язку зобов'язаний зберігати такі дані певний час, щоб органи правопорядку могли отримати до них доступ у разі потреби.

Це важливо пам'ятати, якщо ваша діяльність відбувається на небезпечних територіях — близько до лінії фронту, на тимчасово окупованих територіях тощо. Розмови телефоном можна перехопити та прослухати, так само як і прочитати SMS. Також через мобільний зв'язок можливо встановити місце перебування користувача, тому що телефон і SIM-карта «спілкуються» з вежами зв'язку. Що більше їх навколо, то точнішою буде інформація про вашу локацію.

Жодні технічні засоби не захищають від такого зберігання даних, тому основна рекомендація щодо безпеки мобільної комунікації — не говорити жодної конфіденційної інформації телефоном, не передавати таку інформацію через SMS. Звичайно, в умовному Києві не варто одягати шапочку з фольги, якщо ви телефоном хочете поговорити з рідними, які так само на безпечній території. Але про заходи безпеки потрібно подбати, коли ваша комунікація відбувається або близько до небезпечних територій, або з людьми, які перебувають у тимчасовій окупації.

1.3.2. Безпечна комунікація між користувачами в месенджерах і соцмережах

З огляду на попередній пункт ми рекомендуємо вести чутливу комунікацію онлайн. Вона може відбуватися в соцмережах і месенджерах. Кожний з них має свої особливості. Тут поговоримо про комунікацію в месенджерах: який обрати, на що звертати увагу, чи існує найбезпечніший месенджер.

При виборі месенджера бажано відповісти на такі питання:

Що саме ви хочете захищати та від кого?

Чи є для вас проблемою, що сервіс матиме доступ до ваших переписок і вони будуть зберігатися на його серверах?

Якщо це проблема, чи важливі вам загалом ваші переписки? Чи потрібно зберігати їхні резервні копії в сторонніх акаунтах? Чи готові ви втратити їх у випадку зміни пристрою або його втрати?

Чи важливі вам додаткові функції, як-от двофакторна аутентифікація або реєстрація не за номером телефону, а за допомогою електронної адреси?

Чи ваші співрозмовники/ці користуються таким самим месенджером або чи зможуть вони його змінити?

Перше, на що слід звернути увагу при виборі програми, це тип шифрування, який використовується в месенджерах. Це може бути

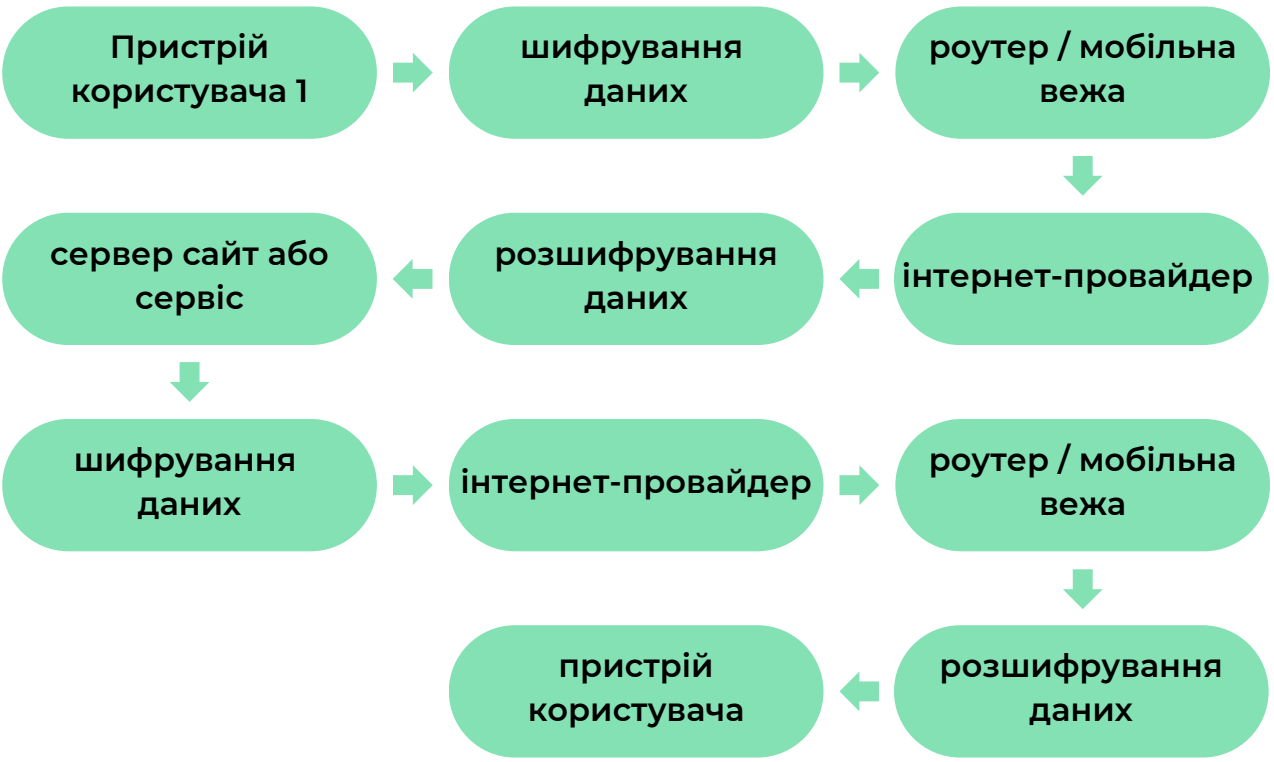
шифрування від пристрою до сервера

(звичайне захищене з'єднання)

шифрування від пристрою до пристрою

(end-to-end-шифрування, шифрування з кінця в кінець)

Яким чином відбувається наше спілкування в месенджерах або поштою при звичайному захищеному з'єднанні (https):

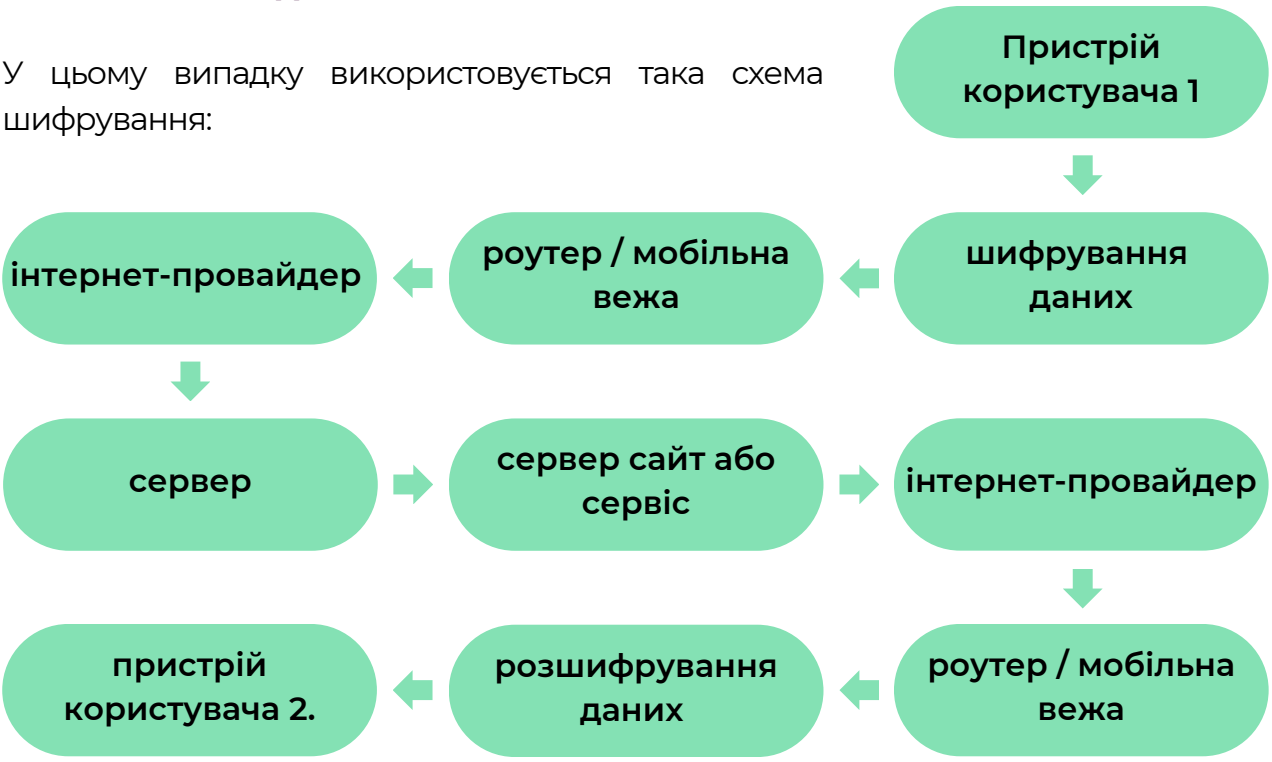


При такому з'єднанні ані інтернет-провайдери, ані особи, що мають доступ до роутера / мобільної вежі, не можуть побачити, кому та що ви пишете, проте вони бачать, якими сервісами для комунікації ви користуєтеся, скільки часу там проводите та який обсяг інформації передаєте.

Ризики конфіденційності під час передачі інформації виникають лише на серверах інтернет-сервісів, якими ви користуєтеся. Іншими словами, сервіс, через який ви спілкуєтеся, має технічну можливість за потреби побачити зміст вашої комунікації. За таким принципом працюють Telegram (як усталено), Facebook, Instagram, поштові сервіси. Якщо ви довіряєте сервісу і вам важлива зручність (тобто доступ до ваших переписок з будь-якого пристрою в будь-який час), можна використовувати месенджери з таким типом шифрування.

End-to-end-з'єднання

У цьому випадку використовується така схема шифрування:



При цьому з'єднанні інформація шифрується на одному пристрої, під час всіх стадій комунікації, включно з серверами самих сервісів, проходить у зашифрованому вигляді і приходить на пристрій іншого користувача також у зашифрованому вигляді. Потім інформація розшифровується у звичайний текст. Подібний тип шифрування є у WhatsApp, Signal; Telegram, Facebook (секретні чати), Instagram (повідомлення, які зникають). Viber заявляє, що також використовує end-to-end-шифрування, проте компанія ні разу не проходила аудит коду (тобто незалежні дослідники не робили експертний висновок, наскільки шифрування месенджера безпечне та наскільки якісно воно працює).

При такому виді з'єднання залишаються лише загрози, пов'язані з отриманням зловмисником_цею фізичного доступу до ваших гаджетів. Також страждає зручність, бо з'являються такі сценарії:

Якщо ви не налаштували резервне копіювання, ви можете втратити переписки, наприклад, загубивши пристрій.

Якщо ви змінюєте операційну систему (з Android на iOS і навпаки), необхідно вжити додаткових заходів для відновлення резервної копії на пристроях.

Потрібно подумати про захист резервної копії листування, якщо ви її робите.

Інші характеристики, на які можна звертати увагу

Складніші характеристики, за якими можна фільтрувати додатки: питання довіри до сервісу, фінансування, юрисдикція, кількість даних користувача, до яких додаток отримує доступ тощо. До прикладу, Signal і WhatsApp працюють лише в режимі наскрізного шифрування та використовують один і той самий протокол. При цьому WhatsApp, який належить Facebook, збирає метадані користувача (інформацію про те, з ким ви спілкуєтеся, звідки, у який час, як часто та з якого пристрою) і може їх використовувати (наприклад, щоб показувати таргетовану рекламу). Signal намагається мінімізувати кількість збереженої інформації та видаляти її час від часу.

Періодично незалежні дослідники безпеки або комерційні компанії публікують порівняльні таблиці або цикли матеріалів, за допомогою яких можна перевірити, чи відповідає обраний месенджер усім важливим для вас параметрам безпеки. Проте зважайте на час публікації матеріалів — з розвитком технологій подібний аналіз може швидко втратити актуальність. До прикладу, ось один з них. Тут можна ознайомитися з важливими безпековими аспектами того чи іншого месенджера.

Скоріше за все під час роботи вам доведеться користуватися декількома месенджерами, і це нормально. Варто знати, як найкраще налаштувати кожен з них.

1.3.3. Захист месенджерів

Зазвичай для того, щоб зайти в месенджер перший раз з нового пристрою, необхідно скористатися кодом, який надійшов у SMS на ваш номер, — це один зі способів аутентифікації. Як ми пам'ятаємо, до SMS можуть отримати доступ зловмисники_ці, тому необхідно додати будь-який інший спосіб аутентифікації для входу у ваш обліковий запис, неприв'язаний до мобільного зв'язку (пароль, пін-код тощо), тобто налаштувати двофакторну аутентифікацію для месенджера. Вона також врятує, якщо ви, наприклад, через фішинг повідомите комусь код із SMS, який вам надійшов.

Якщо ваш додаток використовується для великої кількості сенситивної інформації, подбайте про автовидалення чатів або окремих повідомлень і подумайте, як вам зручніше контролювати історію переписок. Це може бути таймер автовидалення на якусь кількість днів (наприклад, повідомлення, старіші за 90 днів, будуть автоматично видалені). Або вам зручніше чистити переписки вручну.

Автозавантаження медіафайлів також може бути вразливим місцем, якщо ви не хочете зберігати всі медіа, які вам присилають. Краще його вимкнути — це і місце збереже на пристрої, і дозволить вам краще контролювати те, яка інформація осідає в телефоні. Зверніть увагу: автозавантаження також може бути активним на комп'ютері (актуально для Telegram). Тож якщо ви користуєтеся додатком, а не web-версією, обов'язково перегляньте, що саме зберігається та в якій папці.

Контроль активних сесій допоможе зрозуміти, де і з якого пристрою ви зараз залогінені в акаунт. Це налаштування актуальне для Facebook, Instagram, Telegram та пошти. Якщо ви думаєте, що хтось отримав доступ до вашого акаунту, перше налаштування, куди варто зазирнути, — контроль активних сесій. Там можна завершити підозрілий або старий сеанс. Також час від часу варто переглядати цей список, якщо ви багато працюєте з різними пристроями, — щоб не забувати виходити з комп'ютерів, до яких мають доступ декілька людей. Що менше в списку активних сесій, то простіше зрозуміти, чи зараз відбувається щось підозріле, тому бажано видаляти старі та неактуальні сеанси.

Контроль групових чатів — ще одне налаштування, на яке слід звертати увагу. Хто є адміністратором групи чи публічного каналу, у якому стані безпека акаунту цієї людини, чи є в групах учасники, яких не має там бути тощо.

Захист резервної копії, якщо у вас налаштований бекап. Перевірте, у який акаунт відбувається резервне копіювання, чи маєте ви до нього доступ, чи достатньо він захищений, чи підтримує ваш месенджер шифрування резервної копії. Якщо так, рекомендуємо його налаштувати. Якщо резервна копія вам не потрібна, її необхідно не тільки вимкнути, а й видалити зі свого пристрою. Детальніше про те, як це зробити, може бути написано в довідці вашого месенджера.

Звичайно, важлива й безпека самого пристрою. Як краще налаштувати телефони та комп'ютери, ми писали в першому підрозділі.

1.3.4. Захист онлайн облікових записів

Превентивні способи захисту онлайн-акаунтів:

- Багатофакторна аутентифікація
- Надійні способи відновлення
- Технічна підтримка
- Унікальні паролі
- Надійні пристрої

Способи відновлення акаунтів. Зазвичай використовуються два способи відновлення доступу до облікових засобів — через номер телефону та через резервну електронну пошту. Важливо контролювати прив'язку номера телефону та резервної електронної адреси, щоб не втратити можливість доступу до облікового запису разом з втратою, наприклад, старого телефону. Якщо у вас налаштована резервна електронна пошта, перевірте, чи вона актуальна та захищена. Можливо, до неї вже немає доступу, тож її необхідно видалити.

Контроль активних сесій і додатків, зв'язаних з акаунтом. Про контроль активних сесій ми говорили в попередньому підрозділі. Схожою функцією є контроль додатків, тобто це перелік додатків, які використовують дані з вашого облікового запису для реєстрації у своєму сервісі (наприклад, залогінення в сервіс «Spotify» через обліковий запис Gmail). Необхідно звертати увагу на сервіси, якими ви вже не користуєтеся або не знаєте, що це за додаток. Необхідно їх видаляти з відкликанням доступу.

Перевірка підозрілих вкладень. Нагадаємо короткий порядок дій, якщо ви отримали лист з вкладенням, яке треба відкрити, але ви сумніваєтеся в його безпеці:

зберегти файл на комп'ютер, але НЕ відкривати; → **відкрити сайт virustotal.com;** → **завантажити файл на перевірку;** → **дізнатися результати перевірки.**

Детальніше про це читайте в підрозділі про фішинг.

Ви можете вважати, що зробили всі необхідні дії для захисту своїх облікових записів від зламу, якщо:

- маєте, до кого звернутися для перевірки підозрілих повідомлень;
- обліковий запис зареєстрований на довірену пошту (пошта, яку ви додатково захищаєте);
- використовуєте унікальні паролі на важливих акаунтах;
- налаштована двоетапна перевірка (SMS, генератор кодів, резервні коди);
- обліковий запис використовується лише на ваших пристроях;
- налаштовані способи відновлення або ви надійно зберігаєте пароль.

Що робити, якщо ваш акаунт зламали:

- зверніться по допомогу до знайомих IT-спеціалістів/ок;
- попередьте близьких, колег, партнерів;
- фіксуйте все, що відбувається, — скріншоти, повідомлення, IP-адреси тощо.

РОЗДІЛ 2. Інвентаризація цифрових активів

Знаючи, які сценарії та атаки можуть статися з особистими активами, можна краще зрозуміти, які активи доведеться захищати в організації, від чого та кого. Процес деталізації називається інвентаризацією цифрових активів.

Як проводити інвентаризацію? Подивитися, чим користується організація та кожна конкретна людина, про безпеку якої слід подбати. Які є корпоративні акаунти в соцмережах, чи є робочі комп'ютери або інші робочі пристрої (жорсткі диски, спільні флешки). Якщо в організації немає корпоративних поштових скриньок і робота відбувається із залученням особистих акаунтів співробітників/ць, це також можна зазначити.

Мета інвентаризації — зрозуміти, з чим надалі буде працювати організація при створенні політики безпеки та інших планів / безпекових протоколів. У процесі також можна зазначити, у кого станом на зараз є доступ до цього активу.

Приблизний список можливих активів:

- сайт (доступ до хостингу, домену, адміністраторського облікового запису);
- резервна копія сайту;
- сервер;
- робочі комп'ютери, телефони, інші пристрої, які закуповувала організація (принтери, роутери, сканери тощо);
- ліцензійне ПЗ, пакети програм, які закуповуються для роботи працівників/ць (бухгалтерські програми, відеоредактори тощо);
- соцмережі (корпоративна пошта, акаунти у Facebook, Instagram, Twitter, канал у Telegram тощо);
- чи важлива робоча переписка? Якщо так, у яких месенджерах вона відбувається?
- чи відбувається робота з хмарними документами, чи вона важлива? Якщо так, власником цих документів є організація чи кожен/кожна зі співробітників/ць створює їх окремо?
- чи є корпоративні SIM-карти?
- чи потрібно захищати паперові документи? Якщо так, чи є в організації місце для цього (сейф тощо)?
- чи налаштований захист в офісі (сигналізація, решітки на вікнах тощо)?
- чи зберігається щось в нецифровому вигляді (документи, особисті справи працівників/ць тощо)?

Список може вийти чималим, але що більш детальний опис, то краще. Можна об'єднати пункти в тематичні блоки (техніка, сайт, соцмережі тощо).

РОЗДІЛ 3. Оцінювання ризиків і як його проводити

Для початку подивимося на наш список цифрових активів. Щоб вистачило ресурсу, маємо визначити, які з напрямів пріоритетні, і почнемо розмову про цифрову безпеку саме з них.

Як це будемо робити? Скористаємося оцінюванням ризиків.

Щоб оцінити ризики для цифрових активів, поставимо до кожного такі питання:

Де цей актив розміщений (чи це інформація на пристроях — телефоні, лептопі, планшеті, робочому комп'ютері, зовнішньому жорсткому диску, флешці, чи це сама техніка, яка десь зберігається тощо)?

Кому ця інформація може бути цікавою? Можливо, уже траплялися інциденти, коли вас хтось зламував або шахрайством намагався вибити дані для входу в акаунт чи дані банківських карток або намагався змусити вас переказати гроші й не надати послугу? Ким були ці люди — пересічні шахраї/йки, хакери, які намагалася вас зламати через вашу діяльність, можливо, конкретний політичний опонент?

Чи є у вас людина, до якої можна звернутися, якщо трапиться безпековий інцидент?

Врахування цих обставин допоможе краще зрозуміти, які вразливості станом на зараз у вас існують.

Приклад. Для організації є цінними файли на Google-диску, бо там багато робочої та сенситивної інформації. Тобто це електронна пошта, пароль до акаунту, пристрої, з яких ви станом на зараз залогінені в акаунт, можливо, доступ інших людей до пошти, якщо вона шериться між колегами.

Пароль для входу ви зберігаєте у файлі на робочому столі комп'ютера. Також цей пароль не унікальний і досить простий. Ви давно не переглядали безпекові налаштування акаунту. До пошти мають доступ ще декілька людей.

Ви думаєте, що інформація може бути цікавою зловмисникам/цям, яких приваблює діяльність організації, тому що вам час від часу приходять фішингові листи, які обігрують цю тему.

У цьому сценарії можна побачити деякі вразливості:

Збереження пароля на робочому столі комп'ютера. Його можуть підгледіти інші, порушивши конфіденційність інформації. Також можна випадково видалити файл з паролем або банально втратити документ, якщо вийде з ладу система, — обидві ситуації порушують доступність сервісу.

Доступ до пошти мають інші люди. Ви не знаєте, наскільки захищені їхні пристрої, де вони зберігають пароль, чи вони використовують пошту зі своїх пристроїв, чи ні.

Використання однакового пароля для Google-диску та інших облікових записів. Якщо інші облікові записи будуть фігурувати у витоках даних, можна вважати, що ця інформація вже є публічною.

Використання простого або типового пароля. Комбінація, наприклад, містить ваше ім'я та дату народження або це банальне «qwerty1234».

Фішинг, який час від часу приходить на пошту.

Для зручності можемо заповнити таблицю, де чіткіше для себе розпишемо фактори ризиків та оцінимо ступінь наслідків.

Фактори ризиків					
Актив (що)	Порушник (хто)	Загроза (що зробить)	Ризик (що станеться)	Актуальність	Наслідки
					Критичні
					Середня критичність
					Низька критичність
					Незначні

Актив — те, що ми захищаємо.

Порушник/ця — той/та, кому актив може бути цікавий, або той/та, у кого є доступ до цього активу. Порушник_ця може бути внутрішній/я і зовнішній/я. Зовнішній/я порушник/ця може бажати зламати акаунт і робити для цього певні дії, внутрішній/я порушник/ця може випадково «зафішитися» або іншим чином вплинути на конфіденційність, цілісність чи доступність інформації.

Загроза — те, що порушник/ця зробить з нашим активом.

Ризик — те, що станеться з активом в результаті реалізації загрози.

Актуальність — чи вважаєте ви ризик станом на зараз реальним.

Наслідки — чи вони критичні для організації, чи ні.

Приклад заповненої таблиці наведено нижче.

Фактори ризиків

Актив (що)	Порушник (хто)	Загроза (що зробить)	Ризик (що станеться)	Актуальність	Наслідки
Файли на гугл-диску	Зловмисники (таргетована атака)	Розішлють фішингові листи	Втрата доступу до акаунта, чутливі дані стануть відомими	5 (не вмію відрізняти фішинг)	**Критичні**
	Зловмисники (не таргетована атака)	Зламають пароль	Втрата доступу до акаунта, можливо чутливі дані стануть відомими	5 (маю слабкий пароль, немає двофакторної)	**Середня критичність**
	я	Пароль дізнаються інші люди	Втрата доступу до акаунта, хтось може подивитись інформацію в акаунті	3 (зберігаю пароль на роб. столі, але комп'ютер мій)	**Низька критичність**
	Колеги	Передають паролі небезпечним способом	Втрата доступу до акаунта, чутливі дані стануть відомими	5 (не знаю, де передавався пароль, в яких переписках він зберігається і наскільки ті акаунти захищені)	**Незначні**

Що ж робити з результатами оцінювання ризиків?

Ризики, які ви визначили, можна

зменшити **уникнути** **прийняти** **передати**

Зменшення ризиків — найпопулярніша практика. Використання двофакторної аутентифікації, унікального пароля, обрання найбільш відповідного для вас месенджеру та його налаштування — це все практики, які знижують ймовірність успішної атаки на ваші цифрові активи.

У нашому сценарії зменшити ризик зламу Google-диску з огляду на вразливості, які ми ідентифікували, допоможуть такі дії:

Не зберігати пароль на робочому столі комп'ютера. Можна перенести цей пароль у більш надійне місце (умовно в менеджері паролів).

Переглянути безпекові налаштування акаунту, оновити їх за потреби.

Попросити переглянути безпекові налаштування пристрою колег, які використовують цю ж пошту, спитати, де вони зберігають пароль, і порекомендувати змінити місце збереження за потреби.

Не використовувати всюди однаковий пароль. Тобто придумати для важливого акаунту окрему надійну, нетипову та довгу комбінацію, щоб її було складно підібрати шахраям.

Змінити наявний слабкий пароль на більш надійний.

Пройти навчання про те, як відрізняти фішинг від реальних листів, щоб стати більш упевненими у своїх силах.

Ризиків можна уникнути. У нашому сценарії це означає не мати Google-диску взагалі.

Передати ризик означає передати відповідальність за нього третій стороні.

Наприклад, призначити відповідальним/ою за нього IT-спеціаліста/ку організації, якщо він/вона є.

Ризик можна прийняти — ухвалити рішення, що вам простіше нічого не змінювати. Це також валідне рішення в деяких сценаріях.

З огляду на результати оцінювання ризиків можна буде створювати політики безпеки організацій, плани зі зменшення ризиків та інші документи, які покращать безпекову ситуацію в організації.

РОЗДІЛ 4. Цифрова безпека волонтерів/ок

Волонтери/ки стикаються з багатьма загрозами. Зокрема, їхня діяльність супроводжується кібернебезпеками. Фішинг, витікання чутливих персональних даних, проблема зламу акаунтів і підробки паролів — усе це може стати реальністю, якщо не дбати про власну цифрову безпеку. Обізнаність у цій сфері є однією з критично важливих для будь-якого волонтера чи волонтерки. Більшість загроз ми описали та пояснили вище, проте хочемо наголосити на окремих факторах.

4.1. Робота з персональними комп'ютерами

Якщо волонтери/ки працюють з організацією зі своїми пристроями, подумайте, чи необхідно вам знати, як саме вони налаштовані. Якщо так, подумайте, чи є в організації ресурси, щоб допомогти волонтерам/кам налаштувати пристрій, перевстановити ПЗ за потреби, допомогти зашифрувати лептоп тощо.

Якщо у волонтерів/ок є доступ до офісу та роботи з комп'ютерами організації, створіть для них окремий обліковий запис без прав адміністратора. Це допоможе у випадку, якщо вони завантажать щось з листа або якусь підозрілу програму, не встановити її на комп'ютер. Також якщо на лептопі зберігаються файли інших співробітників_ць, розділення акаунтів допоможе обмежити до них доступ.

4.2. Мережа WiFi в офісі

Якщо до вашого офісу приходить велика кількість людей, які не є постійними працівниками/цями, проконсультуйтеся з IT-спеціалістом/кою: можливо, організації варто зробити дві мережі. Зовнішню — для всіх охочих і внутрішню — тільки для працівників/ць. Обидві мережі необхідно захистити надійним паролем. Це допоможе зменшити несанкціонований доступ до мережі сторонніх осіб. Також подбайте про те, щоб замінити стандартні логіни та паролі в кабінеті налаштування роутера. Інакше залишається вразливість, що стандартні дані для входу хтось зможе підібрати.

4.3. Адміністрування корпоративних соцмереж

Якщо ваші волонтери/ки адмініструють соцмережі організації, подбайте про налаштування доступу таким чином, щоб їхні ролі поширювалися лише на роботу з контентом.

У Facebook волонтерів/ок краще призначати модераторами або редакторами, а не адміністраторами. Доступ до Instagram також можна налаштувати через Facebook — робити публікації через Creator Studio. Єдиний мінус — таким чином не можна публікувати сторіз.

Якщо ви даєте доступ до Telegram-каналу, не забудьте заборонити волонтерам/кам призначати і видаляти інших адміністраторів каналу.

Для модерування Twitter можна використати TweetDeck.

У налаштуваннях Youtube можна надати дозвіл певному акаунту для модерування і проведення трансляцій.

За допомогою таких опцій ви можете не передавати волонтерам/кам паролі до корпоративних соцмереж. Але якщо існує потреба це зробити, подбайте про те, щоб надалі видалити пароль з переписки. А коли доступ волонтерів/ок до соцмережі вже не потрібний, бажано змінити всі паролі, які ви поширювали.

4.4. Навчання волонтерів/ок

Якщо в організації вже є політика із цифрової безпеки, варто ознайомити волонтерів/ок з нею. За можливості проведіть для них навчання з розпізнавання і протидії фішингу або з іншої теми, яку ви вважаєте важливою.

Якщо ресурси організації дозволяють, допоможіть волонтерам/кам налаштувати для роботи власні пристрої.

Головне завдання всіх цих заходів — зберегти якомога більше контролю над активами, до роботи з якими залучаються волонтери/ки. Щоб ніхто випадково не змінив критично важливі налаштування або не видалив документи.

РОЗДІЛ 5. Про політику та процедури із цифрової безпеки

Політика із цифрової безпеки — це важливий документ, який описує, як необхідно поводитися з критично важливими активами організації. Політику можна створювати різними способами, зупинитися варто на тому, який вам буде комфортний.

Перед тим, як створювати політики, варто хоча б раз пройти аудит із цифрової безпеки. Він може бути внутрішнім, тобто його робить IT- спеціаліст/ка, який/яка є частиною команди, або зовнішнім, тобто його проводять зовнішні спеціалісти/ки.

Мета аудиту — визначити вашу безпекову ситуацію станом на зараз. Якщо ви ніколи не робили інвентаризацію активів або не налаштовували цифрове робоче середовище, аудит допоможе зрозуміти, з чого почати. У підсумку можна отримати список ризиків організації, аналіз, наскільки вони критичні, та попередні рекомендації для їх зниження.

Спираючись на результати аудиту, ви можете робити висновки, які правила ви б хотіли прийняти в організації. На цьому етапі вже можна створювати політику безпеки.

Політика із цифрової безпеки — це документ довільної, зручної для вас форми про те, якою ви бачите цифрову безпеку в організації. Політика може будуватися по-різному, залежно від побажань організації.

1. Політика, яка будується на ризиках, визначених під час аудиту. Документ буде містити опис ризиків, відповідальних осіб, які мають подбати про їх зменшення, передачу чи прийняття. Також може бути алгоритм дій на випадок надзвичайної ситуації.

2. Політика, побудована на правилах, які організація хоче імплементувати у свою роботу. Тобто це опис того, як має бути налаштована мережа в офісі, робочі комп'ютери, корпоративні соцмережі, хто за це відповідає та що робити, коли стається безпековий інцидент.

3. Політика, яка будується на стандартах. Тобто ви хочете, щоб безпека організації відповідала передовим безпековим практикам, тому те, як ви бачите функціонування такої системи в організації, ґрунтується на певних стандартах.

Важливо, щоб будь-який варіант політики будувався на захисті основних активів організації.

Після створення політики можна перейти до підготовки плану, який допоможе досягнути бажаного стану цифрової безпеки в організації. У плані обов'язково потрібно вказати відповідальну особу та термін виконання завдання, тому що безособовий документ не буде достатньо ефективним.

Через певний час, який визначить організація, можна переглянути актуальність плану та документа загалом.

Нижче подані шаблони політики із цифрової безпеки.

РОЗДІЛ 6. Шаблони документів

Чекліст для оцінювання індивідуальної цифрової безпеки

Ми не захищаємося від усього поспіль. Щоб вистачило уваги й сил, можна рухатися за таким алгоритмом:

1. Скласти список цифрових активів. Визначити, що в нас є важливого: онлайн-акаунти й фізичні пристрої загалом.
2. Оцінити наслідки. Зрозуміти для себе, що станеться, якщо зловмисник/ця отримає доступ до активу або актив буде втрачено.
3. Ухвалити рішення. Ризик можна прийняти, якщо він незначний, зменшити, уникнути або передати.

Список найбільш розповсюджених атак:

1. Атаки на паролі. До всіх акаунтів одна комбінація. Зловмисники/ці дізналися ваш пароль на іншому сайті, який зламали, і пробують його використати для електронної пошти / сторінки у Facebook.
2. Простий або типовий пароль. «qwerty», «12345», «password» дуже легко підбираються. Також ненадійними є паролі, у яких міститься інформація про вас.
3. Ненадійний спосіб відновлення. Зловмисники_ці отримали доступ до вашої старої пошти, на яку зареєстрований акаунт, і скидають пароль до нього.
4. Фішинг. Зловмисники/ці отримали ваші дані для входу за допомогою шахрайства.
5. Віруси. Ви завантажили підозрілий архів або піратську програму й отримали шифрувальника, який унеможливив доступ до даних.

Як захищатися?

Паролі:

1. Мати унікальні складні паролі на важливих облікових записах.
2. Подбати про надійне місце для збереження паролів, використати парольний менеджер за потреби.
3. Налаштувати двофакторну аутентифікацію на важливих сервісах.
4. Перевірити пошту, підключену до акаунта, чи вона актуальна. Перевірити резервну пошту, чи є до неї доступ. Якщо ні, то видалити її. Захистити основну та резервну пошти (надійний пароль, двофакторна аутентифікація), перевірити актуальність номера телефону.
5. Подивитися, чи фігурувала ваша пошта в зливах даних. Це можна зробити тут: haveibeenpwned.com.
6. Знати базові ознаки фішингу, знати правила сайтів, якими користуєтеся, мати людей, до яких можна звернутися по допомогу.

Який пароль можна назвати надійним?

1. Унікальний на важливих сервісах.
2. Не містить персональних даних та інформацію, яку легко нагуглити.
3. Довгий. Такий пароль може містити лише букви, але завдяки довжині його буде складно підібрати.
4. Збережений. Обов'язково зберігайте паролі, бо інакше зростає ймовірність втратити доступ до акаунту.
5. Згенерований менеджером паролів або браузером.
6. **Парольна фраза замість набору символів, бо її простіше запам'ятати. Парольна фраза — це пароль, який складається з речення або комбінації слів.**

Важливо: не використовуйте популярні цитати як паролі.

Логотипи

1. Не завантажуйте піратське ПЗ, намагайтеся знайти ліцензійні аналоги потрібних програм, якщо немає можливості придбати ті, які треба. Ліцензійне ПЗ може бути безоплатним, якщо це програми з відкритим кодом або урізана версія основної програми.
2. Завантажте ліцензійний антивірус або налаштуйте «Захисник» Windows.
3. Не завантажуйте та не встановлюйте підозрілі програми, не розпаковуйте підозрілі вкладення з листа. Спершу перевірте їх тут.
4. Якщо у вас комп'ютер на Windows, розділіть обліковий запис користувача та адміністратора. Інструкцію можна почитати тут.
5. Встановіть автоблокування екрана після певного часу бездіяльності для Windows, для Apple — після закриття кришки.
6. Встановіть пароль на вхід у систему. Якщо пристрій підтримує вхід за допомогою біометричних даних, можна налаштувати його.
7. За потреби зашифруйте пристрій (важливо: спершу проконсультуйтеся зі спеціалістом).
8. Оновлюйте операційну систему та програми, які використовуєте.
9. Налаштуйте бекапи для важливих файлів.

Смартфони:

1. Налаштуйте автоблокування екрана через певний час бездіяльності.
2. Налаштуйте пароль на вхід або пін-код (щонайменше шість символів) або, якщо пристрій підтримує вхід за біометричними даними, налаштуйте їх.
3. Регулярно проводьте ревізію додатків, видаляйте старі, ті, якими не користуєтеся, та ті, які не оновлюються.
4. Оновлюйте операційну систему.
5. Майте резервні копії важливих файлів.

Акаунти:

1. Подбайте про наявність доступу до пошти, на яку зареєстрований акаунт.
2. Встановіть на вхід надійний пароль, збережіть його.
3. Налаштуйте багатофакторну аутентифікацію.
4. Подивіться список активних сесій, щоб зрозуміти, з яких пристроїв використовується акаунт. Завершіть старі або підозрілі сеанси.
5. Якщо отримуєте підозрілі повідомлення, які спонукають щось робити або здаються шахрайськими, зверніться по допомогу.

Месенджери:

1. Telegram, WhatsApp, Signal — налаштуйте двофакторну аутентифікацію та пошту для відновлення пароля.
2. Захистіть пристрої, з яких використовуєте месенджер.
3. Використовуйте лише на довірених пристроях.
4. Подбайте про наявність доступу до акаунту, куди відбувається резервне копіювання.
5. Налаштуйте месенджер під свої потреби, подумайте про автовидалення повідомлень, вимкніть автозавантаження медіа.
6. За потреби перегляньте налаштування групових чатів, дозахистіть акаунти людей, які їх адмініструють.

Приблизний список можливих активів:

- сайт (доступ до хостингу, домену, адміністраторського облікового запису);
- резервна копія сайту;
- сервер;
- робочі комп'ютери, телефони, інші пристрої, які закуповувала організація (принтери, роутери, сканери тощо);
- ліцензійне ПЗ, пакети програм, які закуповуються для роботи працівників/ць (бухгалтерські програми, відеоредактори тощо);
- соцмережі (корпоративна пошта, акаунти у Facebook, Instagram, Twitter, канал у Telegram тощо);
- чи важлива робоча переписка? Якщо так, то в яких месенджерах вона відбувається?
- чи відбувається робота з хмарними документами, чи вона важлива? Якщо так, власником цих документів є організація чи кожен/ кожна зі співробітників/ць створює їх окремо?
- чи є корпоративні SIM-карти?
- чи потрібно захищати паперові документи? Якщо так, чи є в організації місце для цього (сейф тощо)?
- чи налаштований захист в офісі (сигналізація, решітки на вікнах тощо)?
- чи зберігається щось у нецифровому вигляді (документи, особисті справи працівників/ць тощо).

Таблиця для оцінювання ризиків

Фактори ризиків					
Актив (що)	Порушник (хто)	Загроза (що зробить)	Ризик (що станеться)	Актуальність	Наслідки
					Критичні
					Середня критичність
					Низька критичність
					Незначні

Актив — те, що ми захищаємо.

Порушник/ця — той/та, кому актив може бути цікавий, або той/та, у кого є доступ до цього активу. Порушник_ця може бути внутрішній/я і зовнішній/я. Зовнішній/я порушник/ця може бажати зламати акаунт і робити для цього певні дії, внутрішній/я порушник/ця може випадково «зафішитися» або іншим чином вплинути на конфіденційність, цілісність чи доступність інформації.

Загроза — те, що порушник_ця зробить з нашим активом.

Ризик — те, що станеться з активом в результаті реалізації загрози.

Актуальність — чи вважаєте ви ризик станом на зараз реальним.

Наслідки — чи вони критичні для організації, чи ні.

За допомогою таблиці можна зрозуміти, які сценарії більш ймовірні та які активи більш вразливі.

Політика інформаційної безпеки *[назва організації]*

Ухвалена: *[дата]*

Діє до: *[після строку дії політику можна або продовжити, або переглянути за потреби]*

Відповідальна особа: *[директор/ка організації або технічний/а директор/ка, менеджер/ка, людина керівної посади; не рядовий/а працівник/ця]*

Відповідальна особа разом з представниками/цями організації *[можна перелічити]* обговорили ризики та проблеми, які можуть відбуватися в цифровому полі організації, і зробили такі висновки:

Станом на *[дата]* представники/ці організації визначили такі ризики:

1. Ризик / проблема
2. Ризик / проблема
3. Ризик / проблема
....

Після обговорення для кожного ризику та проблеми визначили такий алгоритм дій:

Ризик / проблема 1. *[Яке рішення: прийняти, зменшити, передати чи усунути ризик, хто відповідальний, до якого часу мають відбутися зміни, чи планується впровадження певних правил, щоб цей ризик зменшити (які будуть виконувати всі співробітники_ці). Чіткий перелік відповідальних осіб, дедлайнів, якщо вони потрібні, і правил]*
....

Будь-який безпековий інцидент може стати приводом для перегляду політики безпеки. Та людина, яка дізналася першою про інцидент, обов'язково повідомляє відповідальному/ій за політику безпеки. Далі він/вона організовує обговорення для мінімізації ризиків повторення інциденту.

Після завершення строку дії політики або у випадку кардинальної зміни ситуації для організації (зміна діяльності, активні бойові дії тощо) її можна переглянути.

Підпис, дата

Політика інформаційної безпеки *[назва організації]*

Ухвалена: *[дата]*

Діє до: *[після строку дії політику можна або продовжити, або переглянути за потреби]*

Відповідальна особа: *[директор/ка організації або технічний/а директор/ка, менеджер/ка, людина керівної посади; не рядовий/а працівник/ця]*

Присутні обговорили правила роботи та обслуговування цифрової системи організації, її техніки та інші правила. Зокрема, було визначено:

[далі за блоками можна розбити основні активи організації та для кожного пункту написати детальні правила, які мають виконуватися в організації, приклад нижче]

1. Облікові записи Google (пошти + Google-диск)

Зараз в організації є ХХХ акаунтів, доступ до них мають ХХХ.

- Усім співробітникам_цям пройти навчання, щоб уміти розрізняти фішингові листи
- Мати складні довгі паролі для входу в обліковий запис
- Не передавати паролі стороннім особам
- Відповідальній особі до ХХХ числа стандартизувати збереження та класифікацію файлів на Google-диску
- Відповідальній особі перевірити безпекові налаштування акаунтів

….

Будь-який безпековий інцидент може стати приводом для перегляду політики безпеки. Та людина, яка дізналася першою про інцидент, обов'язково повідомляє відповідальному/ій за політику безпеки. Далі він/вона організовує обговорення для мінімізації ризиків повторення інциденту.

Після завершення строку дії політики або у випадку кардинальної зміни ситуації для організації (зміна діяльності, активні бойові дії тощо) її можна переглянути.

Підпис, дата

Додатки до політики безпеки

1. Висновки аудиту або плани дій з чіткими строками та відповідальними особами, щоб узгодити інфраструктуру організації з ухваленими правилами.
2. Перелік завдань на найближчі шість місяців,

Важливо: упорядкування аспектів цифрової безпеки в організації може стати довгим процесом. До цього варто бути готовими, а також реально оцінювати ресурси та спроможність команди. Питання, які не потребують нагального розв'язання, можна перенести та посунути, питання, які потребують рішення просто зараз, можна розбити на етапи. Пам'ятайте, що політики та інші процедури створюються для полегшення життя організації, вона має працювати на вас, а не команда на забезпечення документа.

Корисні джерела для отримання інформації від розробників посібника

Перелік організацій, які займаються питаннями цифрової безпеки як в Україні, так і на міжнародному рівні, а також корисні освітні матеріали (перелік є рекомендованим і не є виключним):

1. ГО «Лабораторія цифрової безпеки»
2. Освітній проєкт від Лабораторії цифрової безпеки «Як»:
3. Міжнародна фундація захисту правозахисників «Frontline Defenders»
4. Освітні матеріали від «Frontline Defenders»

МЕТОДИЧНИЙ ПОСІБНИК ІЗ ЦИФРОВОЇ БЕЗПЕКИ ДЛЯ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА, АКТИВІСТІВ/ОК ТА ВОЛОНТЕРІВ/ОК

Цей методичний посібник створений ЦЕДЕМ у межах проєкту «Ініціатива секторальної підтримки громадянського суспільства України», що реалізується ICAP Єднання у консорціумі з Українським незалежним центром політичних досліджень (УНЦПД) та Центром демократії та верховенства права (ЦЕДЕМ) завдяки щирій підтримці американського народу, наданій через Агентство США з міжнародного розвитку. ICAP Єднання несе повну відповідальність за зміст, який може не відображати поглядів АМР США або Уряду Сполучених Штатів Америки.