Настанови

Настанови 01/2021

щодо прикладів повідомлення про порушення безпеки персональних даних

Прийнято 14 грудня 2021 року

Версія 2.0

Прийнято — після публічних консультацій

Історія версій

Версія 2.0	14.12.2021	Прийняття Настанов після публічних консультацій
Версія 1.0	14.01.2021	Прийняття Настанов для публічних консультацій

Зміст

No table of contents entries found.

Прийнято — після публічних консультацій

ЄВРОПЕЙСЬКА РАДА ІЗ ЗАХИСТУ ДАНИХ

Беручи до уваги статтю 70(1)(e) Регламенту Європейського Парламенту та Ради 2016/679/ЄС від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (далі — «GDPR»).

Беручи до уваги Угоду про ЄЕП, зокрема, Додаток XI та Протокол 37 до неї, зі змінами, внесеними Рішенням Спільного Комітету ЄЕП № 154/2018 від 6 липня 2018 року[1],

Беручи до уваги статтю 12 та статтю 22 його Регламенту,

Беручи до уваги Повідомлення Комісії Європейському Парламенту та Раді під назвою «Захист даних як основа розширення прав і можливостей громадян та підхід ЄС до цифрового переходу — два роки застосування Загального регламенту захисту даних»[2],

ПРИЙНЯЛА ТАКІ НАСТАНОВИ

1 ВСТУП

1. GDPR запроваджує, у певних випадках, вимогу повідомляти про порушення безпеки персональних даних компетентний національний наглядовий орган (далі — «НО»), а також повідомляти про порушення особам, чиї персональні дані були порушені (статті 33 та 34).

2. Робоча група за статтею 29 вже підготувала *загальні* настанови щодо повідомлення про порушення безпеки даних у жовтні 2017 року, проаналізувавши відповідні розділи GDPR (Настанови щодо повідомлення про порушення безпеки персональних даних відповідно до Регламенту 2016/679, РД 250) (далі — «Настанови РД 250»)[3]. Однак, зважаючи на свій характер та час, ці настанови не розглядали всі практичні питання достатньо детально. Тому виникла потреба в *орієнтованих на практику, заснованих на конкретних прикладах* настановах, які використовують досвід, набутий НО з моменту набуття чинності GDPR.

3. Цей документ має на меті доповнити Настанови РД 250 і відображає загальний досвід, набутий органами захисту даних у ЄЕП з моменту набуття чинності GDPR. Його мета — допомогти контролерам даних у прийнятті рішень про те, як реагувати на порушення безпеки даних і які фактори слід враховувати під час оцінки ризиків.

4. У рамках будь-якої спроби вирішити проблему порушення контролер і оператор повинні спочатку її розпізнати. GDPR визначає «порушення безпеки персональних даних» у статті 4(12) як «порушення безпеки, що призводить до випадкового чи незаконного знищення, втрати, зміни, несанкціонованого

[1] Посилання на «держави-члени», що містяться в цьому документі, слід розуміти як посилання на «держави-члени ЄЕП».

[2] Повідомлення Комісії Європейському Парламенту та Раді № 264 (2020), фінальна версія, 24 червня 2020 року.

[3] Настанови Робочої групи за статтею 29 щодо повідомлення про порушення безпеки персональних даних відповідно до Регламенту 2016/679, РД 250, версія 1, 6 лютого 2018 року – схвалені EDPB, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

розкриття або доступу до персональних даних, які передано, збережено або іншим чином оброблено».

5. У своєму Висновку 03/2014 щодо повідомлення про порушення[4] та в Настановах РД 250, Робоча група за статтею 29 пояснила, що порушення можна класифікувати відповідно до таких трьох добре відомих принципів інформаційної безпеки:

   - «Порушення конфіденційності» — коли відбувається несанкціоноване або випадкове розкриття персональних даних чи доступ до них.
   - «Порушення цілісності» — коли відбувається несанкціонована або випадкова зміна персональних даних.
   - «Порушення доступності» — випадкова або несанкціонована втрата доступу до персональних даних або їх знищення.[5]

6. Порушення потенційно може мати низку значних негативних наслідків для фізичних осіб, які можуть призвести до фізичної, матеріальної або моральної шкоди. GDPR пояснює, що це може включати втрату контролю над персональними даними, обмеження прав, дискримінацію, крадіжку особистих даних або шахрайство, фінансові втрати, несанкціоноване скасування псевдонімізації, шкоду репутації та втрату конфіденційності персональних даних, захищених професійною таємницею. Це також може включати будь-яку іншу значну економічну або соціальну шкоду для цих осіб. Одним із найважливіших обов'язків контролера даних є оцінка цих ризиків для прав і свобод суб'єктів даних та вжиття відповідних технічних та організаційних заходів для їх усунення.

7. Відповідно, GDPR вимагає від контролера:

   - документувати будь-які порушення безпеки персональних даних, включаючи факти, що стосуються порушення безпеки персональних даних, його наслідки та вжиті заходи щодо виправлення ситуації[6];
   - повідомляти про порушення безпеки персональних даних наглядовий орган, за винятком випадків, коли порушення безпеки даних малоймовірно призведе до ризику для прав і свобод фізичних осіб[7];
   - повідомляти про порушення безпеки персональних даних суб'єкту персональних даних, якщо порушення безпеки персональних даних може призвести до високого ризику для прав і свобод фізичних осіб[8].

8. Порушення безпеки даних є проблемою самі по собі, але вони також можуть бути симптомами вразливого, можливо, застарілого режиму захисту даних, вони також можуть вказувати на недоліки системи, які необхідно усунути. Загальновідомо, що завжди краще запобігти порушенню безпеки

---

[4] Робоча група за статтею 29, РД 213, 25 березня 2014 року, Висновок 03/2014 щодо повідомлення про порушення безпеки персональних даних, с. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[5] Див. Настанови РД 250, с. 7. – Необхідно враховувати, що порушення безпеки даних може стосуватися як однієї категорії, так і декількох категорій одночасно або сукупно.

[6] Стаття 33(5) GDPR.

[7] Стаття 33(1) GDPR.

[8] Стаття 34(1) GDPR.

даних, підготувавшись до нього заздалегідь, оскільки деякі його наслідки за своєю природою є незворотними. Перш ніж контролер зможе *повністю* оцінити ризик, пов'язаний з порушенням, спричиненим певною формою атаки, слід визначити першопричину проблеми, щоб з'ясувати, чи вразливості, які призвели до інциденту, все ще існують, а отже, можуть бути використані. У багатьох випадках контролер може визначити, що інцидент може призвести до ризику, а, отже, повинен бути повідомлений. В інших випадках повідомлення не потрібно відкладати до повної оцінки ризику та наслідків порушення, оскільки повна оцінка ризику може відбуватися паралельно з повідомленням, а отримана таким чином інформація може надаватися НО поетапно без невиправданих подальших затримок[9].

9. Про порушення слід повідомляти, якщо контролер вважає, що воно може призвести до ризику для прав і свобод суб'єкта даних. Контролери повинні зробити таку оцінку в той момент, коли їм стало відомо про порушення. Контролер не повинен чекати детальної судової експертизи та (ранніх) кроків щодо пом'якшення наслідків, перш ніж оцінити, чи може порушення безпеки даних призвести до виникнення ризику, а отже, має бути повідомлений про це.

10. Якщо контролер самостійно оцінює ризик як малоймовірний, але виявляється, що ризик матеріалізується, компетентний НО може використати свої коригувальні повноваження та прийняти рішення про застосування санкцій.

11. Кожен контролер та оператор повинні мати плани та процедури для реагування на можливі інциденти порушення безпеки даних. Організації повинні мати чіткі лінії підпорядкування та осіб, відповідальних за певні аспекти процесу відновлення.

12. Навчання та підвищення обізнаності з питань захисту даних для персоналу контролерів та операторів з акцентом на управлінні порушеннями безпеки персональних даних (ідентифікація інциденту порушення безпеки персональних даних та подальші дії, які необхідно вжити тощо) також має важливе значення для контролерів та операторів. Таке навчання слід регулярно повторювати, залежно від виду діяльності з обробки та обсягу діяльності контролера, з урахуванням останніх тенденцій та попереджень, що надходять від кібератак або інших інцидентів, пов'язаних з безпекою.

13. Принцип підзвітності та концепція захисту даних за призначенням можуть включати аналіз, який буде використовуватися у власному «Посібнику з реагування на інциденти порушення безпеки персональних даних» контролера та оператора даних, який має на меті встановити факти для кожного аспекту обробки на кожному важливому етапі операції. Такий посібник, підготовлений заздалегідь, забезпечить набагато швидше джерело інформації, що дозволить контролерам та операторам даних зменшити ризики та виконати свої зобов'язання без зайвих затримок. Це гарантуватиме, що в разі порушення безпеки персональних даних працівники в організації знатимуть, що робити, а інцидент, швидше за все, буде вирішено ефективніше, ніж за відсутності заходів зі зниження ризиків або плану.

14. Хоча наведені нижче випадки є вигаданими, вони ґрунтуються на типових випадках з колективного досвіду НО щодо повідомлень про порушення безпеки даних. Запропонований аналіз безпосередньо стосується випадків, що розглядаються, але має на меті надати допомогу контролерам даних в оцінці їхніх власних порушень безпеки даних. Будь-яка зміна обставин описаних нижче випадків може призвести до інших або більш значних рівнів ризику, а отже, вимагати вжиття інших або додаткових заходів. Ці настанови структурують випадки відповідно до певних категорій порушень (наприклад, атаки з вимогою викупу). У кожному випадку, коли йдеться про певну категорію порушень, необхідно

[9] Стаття 33(4) GDPR.

вжити певних заходів для зменшення ризиків. Ці заходи не обов'язково повторюються при аналізі кожного випадку, що належить до тієї ж категорії порушень. Для випадків, що належать до однієї категорії, викладено лише відмінності. Тому читач повинен ознайомитися з усіма випадками, що відносяться до відповідної категорії порушень, щоб визначити та виокремити всі правильні заходи, які необхідно вжити.

15. Внутрішнє документування порушення є обов'язком, який не залежить від ризиків, пов'язаних із порушенням, і повинен виконуватися в кожному конкретному випадку. Наведені нижче випадки намагаються пролити світло на те, чи потрібно повідомляти про порушення НО та інформувати про нього суб'єктів даних, яких це стосується.

2 ПРОГРАМА-ВИМАГАЧ

16. Частою причиною повідомлення про порушення безпеки даних є атака зловмисників з вимогою викупу, якої зазнав контролер даних. У цих випадках шкідливий код шифрує персональні дані, а згодом зловмисник вимагає від контролера викуп в обмін на код розшифрування. Цей вид атаки зазвичай можна класифікувати як порушення доступності, але часто може мати місце і порушення конфіденційності.

2.1 ВИПАДОК № 01: Програма-вимагач з належним резервним копіюванням і без витоку

Комп'ютерні системи невеликої виробничої компанії зазнали атаки програми-вимагача, а дані, що зберігалися в цих системах, були зашифровані. Контролер даних використовував шифрування в режимі спокою, тому всі дані, до яких зверталася програма-вимагач, зберігалися в зашифрованому вигляді з використанням найсучаснішого алгоритму шифрування. Ключ дешифрування не був скомпрометований під час атаки, тобто зловмисник не міг ані отримати до нього доступ, ані використати його опосередковано. Як наслідок, зловмисник мав доступ лише до зашифрованих персональних даних. Зокрема, не постраждала ані електронна пошта компанії, ані клієнтські системи, які використовувалися для доступу до неї. Для розслідування інциденту компанія використовує експертизу зовнішньої компанії з кібербезпеки. Доступні журнали, що відстежують усі потоки даних, які залишають компанію (включаючи вихідну електронну пошту). Після аналізу журналів і даних, зібраних розгорнутими в компанії системами виявлення, внутрішнє розслідування, проведене за підтримки зовнішньої компанії з кібербезпеки, *з упевненістю* встановило, що зловмисник лише зашифрував дані, але не здійснив їх витоку. Журнали не зафіксували жодного зовнішнього потоку даних під час атаки. Персональні дані, які постраждали від зламу, стосуються клієнтів і співробітників компанії, загалом кількох десятків осіб. Резервна копія мала відкритий доступ, і дані були відновлені через кілька годин після того, як сталася атака. Порушення не призвело до жодних наслідків для повсякденної роботи контролера. Не було жодних затримок у виплатах працівникам або обробці запитів клієнтів.

17. У цьому випадку з визначення «порушення безпеки персональних даних» випливають такі елементи: порушення безпеки призвело до незаконної зміни та несанкціонованого доступу до збережених персональних даних.

2.1.1 ВИПАДОК № 01 — Попередні заходи та оцінка ризиків

18. Як і у випадку з усіма іншими ризиками, пов'язаними із зовнішніми суб'єктами, ймовірність успішної атаки з використанням програм-вимагачів можна значно зменшити, посиливши безпеку середовища, що контролює дані. Більшості таких порушень можна запобігти, забезпечивши відповідні організаційні, фізичні та технологічні заходи безпеки. Прикладами таких заходів є належне управління виправленнями та використання відповідної системи виявлення шкідливого програмного забезпечення. Належне та окреме резервне копіювання допоможе пом'якшити наслідки успішної атаки, якщо вона відбудеться. Крім того, програма навчання, підготовки та інформування працівників з питань безпеки (SETA) допоможе запобігти та розпізнати цей вид атак (Перелік рекомендованих заходів можна знайти в розділі 2.5.). Серед цих заходів, належне управління виправленнями, яке гарантує, що системи оновлені та всі відомі вразливості розгорнутих систем виправлені, є одним з найбільш важливих, оскільки більшість атак з використанням програм-вимагачів використовують добре відомі вразливості.

19. Оцінюючи ризики, контролер повинен дослідити порушення та визначити тип шкідливого коду, щоб зрозуміти можливі наслідки атаки. Серед тих ризиків, які слід враховувати, є ризик того, що дані були викрадені без залишення сліду в журналах систем.

20. У цьому прикладі зловмисник отримав доступ до персональних даних, і конфіденційність шифрованого тексту, що містить персональні дані в зашифрованому вигляді, була порушена. Однак будь-які дані, які могли бути виточені, не можуть бути прочитані або використані зловмисником, принаймні на той момент. Техніка шифрування, яку використовував контролер даних, відповідає сучасному рівню розвитку. Ключ дешифрування не був скомпрометований і, ймовірно, не міг бути визначений іншими способами. Як наслідок, ризики конфіденційності для прав і свобод фізичних осіб зведені до мінімуму, якщо не враховувати криптоаналітичний прогрес, який зробить зашифровані дані зрозумілими в майбутньому.

21. Контролер даних повинен враховувати ризик для фізичних осіб, пов'язаний з порушенням[10]. У цьому випадку, як видається, ризики для прав і свобод суб'єктів даних є наслідком відсутності доступу до персональних даних, а конфіденційність персональних даних не порушена[11]. У цьому прикладі негативні наслідки порушення були пом'якшені досить швидко після того, як воно сталося. Наявність належного режиму резервного копіювання[12] робить наслідки порушення менш серйозними, і в цьому випадку контролер зміг ефективно ним скористатися.

---

[10] Настанови щодо операцій з обробки даних, які *«можуть призвести до високого ризику»*, див. у документі Робочої групи за статтею 29 «Настанови щодо оцінки впливу на захист даних (DPIA) та визначення того, чи обробка даних «може призвести до високого ризику» для цілей Регламенту 2016/679», РД 248, версія 01, – схвалені EDPB, https://ec.europa.eu/newsroom/article29/items/611236, с. 9.

[11] Технічно шифрування даних передбачає «доступ» до оригінальних даних, а у випадку з програмами-вимагачами — видалення оригіналу: код програми-вимагача повинен отримати доступ до даних, щоб зашифрувати їх, і видалити оригінальні дані. Зловмисник може зробити копію оригіналу перед видаленням, але персональні дані не завжди будуть вилучені. Під час розслідування, яке проводить контролер даних, може з'явитися нова інформація, яка змінить цю оцінку. Доступ, який призводить до незаконного знищення, втрати, зміни, несанкціонованого розкриття персональних даних або до загрози безпеці суб'єкта даних, навіть без інтерпретації даних, може бути настільки ж серйозним, як і доступ з інтерпретацією персональних даних.

[12] Процедури резервного копіювання повинні бути структурованими, послідовними та повторюваними. Прикладами процедур резервного копіювання є метод 3-2-1 та метод «дідусь-батько-син». Будь-який метод

22. Щодо серйозності наслідків для суб'єктів даних, то можна визначити лише незначні наслідки, оскільки пошкоджені дані були відновлені за кілька годин, порушення не призвело до жодних наслідків для повсякденної роботи контролера та не мало значного впливу на суб'єктів даних (наприклад, на виплати працівникам або обробку запитів клієнтів).

2.1.2 ВИПАДОК № 01 — Пом'якшення наслідків та зобов'язання

23. Без резервної копії контролер може вжити лише кілька заходів для відновлення втрачених персональних даних, і дані доведеться збирати заново. Однак у цьому конкретному випадку наслідки атаки можна було б ефективно локалізувати, скинувши всі скомпрометовані системи до чистого стану, який, як відомо, не містить шкідливого коду, виправивши вразливості та відновивши постраждалі дані незабаром після атаки. Без резервної копії дані будуть втрачені, а тяжкість наслідків може зрости, оскільки це також може призвести до ризиків або впливу на окремих осіб.

24. Своєчасність ефективного відновлення даних з доступної резервної копії є ключовою змінною при аналізі порушення. Визначення відповідних часових рамок для відновлення скомпрометованих даних залежить від унікальних обставин конкретного порушення. GDPR передбачає, що про порушення безпеки персональних даних необхідно повідомляти без невиправданої затримки та, за можливості, не пізніше, ніж через 72 години. Таким чином, можна визначити, що перевищення 72-годинного строку є недоцільним у будь-якому випадку, але у випадках високого рівня ризику навіть дотримання цього строку може розглядатися як незадовільне.

25. У цьому випадку, після детальної оцінки впливу та процесу реагування на інцидент, контролер визначив, що порушення навряд чи призведе до ризику для прав і свобод фізичних осіб, отже, немає потреби повідомляти суб'єктів даних, а також не потрібно повідомляти про порушення НО. Однак, як і всі порушення безпеки даних, воно має бути задокументоване відповідно до статті 33(5). Організації також може знадобитися (або пізніше цього вимагатиме НО) оновити та виправити свої організаційні та технічні заходи й процедури щодо захисту персональних даних, а також заходи та процедури зі зменшення ризиків. У рамках такого оновлення та виправлення організація повинна ретельно розслідувати порушення та виявити його причини й методи, які використовував зловмисник, щоб запобігти будь-яким подібним подіям у майбутньому.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	X	X

завжди повинен бути протестований на предмет його ефективності, а також на предмет того, коли дані підлягають відновленню. Тестування також слід повторювати через певні проміжки часу, особливо коли відбуваються зміни в операції з обробки або її обставинах, щоб забезпечити цілісність системи.

2.2 ВИПАДОК № 02: Програма-вимагач без належного резервного копіювання

Один з комп'ютерів, що використовується сільськогосподарською компанією, зазнав атаки програми-вимагача, а дані на ньому були зашифровані зловмисником. Для моніторингу своєї мережі компанія використовує досвід зовнішньої компанії з кібербезпеки. Доступні журнали, що відстежують усі потоки даних, які залишають компанію (включаючи вихідну електронну пошту). Після аналізу журналів і даних, зібраних іншими системами виявлення, внутрішнє розслідування, проведене за допомогою компанії з кібербезпеки, встановило, що зловмисник лише зашифрував дані, але не викрав їх. Журнали не зафіксували жодного зовнішнього потоку даних під час атаки. Персональні дані, які постраждали від зламу, стосуються співробітників і клієнтів компанії, загалом кількох десятків осіб. Особливі категорії даних не постраждали. Резервна копія в електронному вигляді була відсутня. Більшість даних було відновлено з паперових резервних копій. Відновлення даних зайняло 5 робочих днів і призвело до незначних затримок у доставці замовлень клієнтам.

2.2.1 ВИПАДОК № 02 — Попередні заходи та оцінка ризиків

26. Контролеру даних слід було вжити тих самих попередніх заходів, що й у частині 2.1. та у розділі 2.9. Основною відмінністю від попереднього випадку є відсутність електронної резервної копії та відсутність шифрування у стані спокою. Це призводить до критичних відмінностей у наступних кроках.

27. Оцінюючи ризики, контролер повинен дослідити спосіб проникнення та визначити тип шкідливого коду, щоб зрозуміти можливі наслідки атаки. У цьому прикладі програма-вимагач зашифрувала персональні дані без їх витоку. Як наслідок, ризики для прав і свобод суб'єктів даних є наслідком відсутності доступу до персональних даних, а конфіденційність персональних даних не порушена. Ретельне вивчення журналів брандмауера та їхніх наслідків має важливе значення для визначення ризику. Контролер даних повинен надати фактичні результати цих розслідувань на запит.

28. Контролер повинен мати на увазі, що якщо атака є більш складною, шкідливе програмне забезпечення має можливість редагувати файли журналів і видаляти сліди. Таким чином, враховуючи, що журнали не надсилаються та не реплікуються на центральний сервер журналів, навіть після ретельного розслідування, яке встановило, що персональні дані не були викрадені зловмисником, контролер даних не може стверджувати, що відсутність запису в журналі доводить відсутність витоку, а отже, ймовірність порушення конфіденційності не може бути повністю відкинута.

29. Контролер даних повинен оцінити ризики такого порушення[13], якщо зловмисник отримав доступ до даних. Під час оцінки ризиків контролер даних повинен також враховувати характер, чутливість, обсяг та контекст персональних даних, які постраждали в результаті порушення. У цьому випадку не зачіпаються особливі категорії персональних даних, а кількість порушених даних та кількість суб'єктів даних, що постраждали, є низькою.

30. Збір точної інформації про несанкціонований доступ є ключовим для визначення рівня ризику та запобігання новій атаці або продовженню цієї атаки. Якби дані були скопійовані з бази даних, це, очевидно, було б фактором, що підвищує ризик. Якщо немає впевненості щодо характеру несанкціонованого доступу, слід розглядати найгірший сценарій і відповідно оцінювати ризик.

[13] Вказівки щодо операцій з обробки даних, які *«можуть призвести до високого ризику»*, див. у виносці 10 вище.

31. Відсутність резервної бази даних може розглядатися як фактор, що підвищує ризик, залежно від тяжкості наслідків для суб'єктів даних, спричинених відсутністю доступу до даних.

2.2.2 ВИПАДОК № 02 — Пом'якшення наслідків та зобов'язання

32. Без резервної копії контролер може вжити лише кілька заходів для виправлення втрати персональних даних, і дані доведеться збирати заново, якщо немає іншого джерела (наприклад, електронні листи з підтвердженням замовлення). Без резервної копії дані можуть бути втрачені, і ступінь тяжкості залежатиме від наслідків для фізичних осіб.

33. Відновлення даних не повинно виявитися надто проблематичним[14], якщо дані все ще доступні на папері, але, враховуючи відсутність електронної резервної бази даних, повідомлення НО вважається необхідним, оскільки відновлення даних займає певний час і може спричинити певні затримки в доставці замовлень клієнтам, а значна кількість метаданих (наприклад, журнали, позначки часу) може бути недоступною для відновлення.

34. Інформування суб'єктів даних про порушення може також залежати від тривалості недоступності персональних даних і труднощів, які це може спричинити в роботі контролера (наприклад, затримки в перерахуванні заробітної плати працівникам). Оскільки такі затримки в платежах і доставках можуть призвести до фінансових втрат для осіб, чиї дані були скомпрометовані, можна також стверджувати, що порушення, ймовірно, призведе до високого ризику. Крім того, можливо, не вдасться уникнути інформування суб'єктів даних, якщо для відновлення зашифрованих даних знадобиться їхня допомога.

35. Цей випадок слугує прикладом атаки з вимогою викупу з ризиком для прав і свобод суб'єктів даних, але не досягає високого рівня ризику. Його слід задокументувати відповідно до статті 33(5) та повідомити про нього НО відповідно до статті 33(1). Організації також може знадобитися (або цього вимагатиме НО) оновити та виправити свої організаційні та технічні заходи й процедури щодо захисту персональних даних, а також заходи та процедури зі зменшення ризиків.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	✓	X

[14] Це буде залежати від складності та структури персональних даних. У найскладніших сценаріях відновлення цілісності даних, узгодженості з метаданими, забезпечення правильних взаємозв'язків у структурах даних і перевірка точності даних може потребувати значних ресурсів і зусиль.

2.3 ВИПАДОК № 03: Програма-вимагач з резервною копією та без проникнення в лікарню

Інформаційна система лікарні/медичного центру зазнала атаки вірусу-вимагача, і значна частина даних була зашифрована зловмисником. Для моніторингу своєї мережі компанія використовує досвід зовнішньої компанії з кібербезпеки. Доступні журнали, що відстежують усі потоки даних, які залишають компанію (включаючи вихідну електронну пошту). Після аналізу журналів і даних, зібраних іншими системами виявлення, внутрішнє розслідування, проведене за допомогою компанії з кібербезпеки, встановило, що зловмисник лише зашифрував дані, але не викрав їх. Журнали не зафіксували жодного зовнішнього потоку даних під час атаки. Персональні дані, які постраждали від зламу, стосуються співробітників і пацієнтів, а це тисячі осіб. Резервні копії були доступні в електронному вигляді. Більшість даних було відновлено, але ця операція тривала 2 робочі дні та призвела до значних затримок у лікуванні пацієнтів, операції яких було скасовано/відкладено, а також до зниження рівня обслуговування через недоступність систем.

2.3.1 ВИПАДОК № 03 — Попередні заходи та оцінка ризиків

36. Контролеру даних слід було вжити тих самих попередніх заходів, що й у частині 2.1. та у розділі 2.5. Основною відмінністю від попереднього випадку є висока тяжкість наслідків для значної частини суб'єктів даних[15].

37. Кількість порушених даних та кількість постраждалих суб'єктів даних є великою, оскільки лікарні зазвичай обробляють великі обсяги даних. Відсутність даних має значний вплив на значну частину суб'єктів даних. Крім того, існує залишковий ризик високого ступеня тяжкості для конфіденційності даних про пацієнтів.

38. Важливими є тип порушення, характер, чутливість та обсяг персональних даних, які постраждали в результаті порушення. Навіть якщо існувала резервна копія даних і їх можна було відновити за кілька днів, все одно існує високий ризик через тяжкість наслідків для суб'єктів даних, пов'язаних із відсутністю доступу до даних у момент атаки та в наступні дні.

2.3.2 ВИПАДОК № 03 — Пом'якшення наслідків та зобов'язання

39. Повідомлення НО вважається необхідним, оскільки йдеться про особливі категорії персональних даних, а відновлення даних може зайняти тривалий час, що призведе до значних затримок у наданні допомоги пацієнтам. Інформування суб'єктів даних про порушення є необхідним через вплив на пацієнтів, навіть після відновлення зашифрованих даних. Хоча дані, що стосуються всіх пацієнтів, які лікувалися в лікарні протягом останніх років, були зашифровані, постраждали лише ті пацієнти, які були заплановані на лікування в лікарні в той час, коли комп'ютерна система була недоступна. Контролер повинен повідомити про порушення безпеки даних безпосередньо цим пацієнтам. Пряме повідомлення іншим пацієнтам, деякі з яких могли не перебувати в лікарні понад двадцять років, може не знадобитися через виняток у статті 34(3)(c). У такому випадку замість цього має бути

[15] Вказівки щодо операцій з обробки даних, які *«можуть призвести до високого ризику»*, див. у виносці 10 вище.

здійснено публічне повідомлення[16] або аналогічний захід, за допомогою якого суб'єкти даних будуть поінформовані в однаково ефективний спосіб. У цьому випадку лікарня повинна оприлюднити інформацію про атаку програми-вимагача та її наслідки.

40. Цей випадок є прикладом атаки з вимогою викупу з високим ризиком для прав і свобод суб'єктів даних. Він повинен бути задокументований відповідно до статті 33(5), повідомлений НО відповідно до статті 33(1) та повідомлений суб'єктам персональних даних відповідно до статті 34(1). Організація також повинна оновити та виправити свої організаційні й технічні заходи та процедури щодо захисту персональних даних, а також заходи та процедури щодо зменшення ризиків.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	✓	✓

2.4 ВИПАДОК № 04: Програма-вимагач без резервної копії та з можливістю витоку

Сервер компанії, що займається громадським транспортом, зазнав атаки програми-вимагача, який зашифрував дані на сервері. Згідно з результатами внутрішнього розслідування, зловмисник не лише зашифрував дані, але й викрав їх. Тип порушених даних — персональні дані клієнтів і співробітників, а також кількох тисяч людей, які користувалися послугами компанії (наприклад, купували квитки онлайн). Окрім основних ідентифікаційних даних, до витоку потрапили номери посвідчень особи та фінансові дані, такі як дані кредитних карток. Існувала резервна база даних, але вона також була зашифрована зловмисником.

2.4.1 ВИПАДОК № 04 — Попередні заходи та оцінка ризиків

41. Контролеру даних слід було вжити тих самих попередніх заходів, що й у частині 2.1. та у розділі 2.5. Хоча резервна копія була створена, вона також постраждала від атаки. Сам по собі цей факт викликає питання щодо якості попередніх заходів IT-безпеки контролера та має бути додатково перевірений під час розслідування, оскільки в добре розробленому режимі резервного копіювання кілька резервних копій повинні надійно зберігатися без доступу з основної системи, інакше вони можуть бути скомпрометовані під час тієї самої атаки. Крім того, атаки з вимогою викупу можуть залишатися невиявленими протягом декількох днів, повільно шифруючи дані, які рідко використовуються. Це може зробити марними багаторазові резервні копії, тому їх також слід періодично створювати та зберігати в ізольованому місці. Це підвищить ймовірність відновлення, хоча і з більшою втратою даних.

[16] Преамбула 86 GDPR пояснює, що *«Такі повідомлення суб'єктам даних повинні бути зроблені якнайшвидше, наскільки це можливо, і в тісній співпраці з наглядовим органом, дотримуючись вказівок, наданих ним або іншими відповідними органами, такими як правоохоронні органи. Наприклад, необхідність зменшити безпосередній ризик заподіяння шкоди вимагатиме негайної комунікації з суб'єктами даних, тоді як необхідність вжити відповідних заходів проти триваючих або подібних порушень безпеки персональних даних може виправдати більше часу для комунікації»*.

42. Це порушення стосується не лише доступності даних, але й конфіденційності, оскільки зловмисник міг змінити та/або скопіювати дані із сервера. Таким чином, тип порушення призводить до високого ризику[17].

43. Характер, чутливість та обсяг персональних даних ще більше підвищують ризики, оскільки кількість постраждалих осіб є великою, так само як і загальна кількість порушених персональних даних. Окрім базових ідентифікаційних даних, задіяні також документи, що посвідчують особу, та фінансові дані, такі як реквізити кредитних карток. Порушення безпеки даних, що стосуються цих типів даних, самі по собі становлять високий ризик, а якщо вони обробляються разом, то можуть бути використані, серед іншого, для крадіжки особистих даних або шахрайства.

44. Через несправність серверної логіки або організаційного контролю файли резервних копій були уражені програмою-вимагачем, що унеможливило відновлення даних і підвищило ризик.

45. Порушення безпеки даних становить високий ризик для прав і свобод фізичних осіб, оскільки може призвести як до матеріальної (наприклад, фінансових збитків, оскільки були порушені дані кредитних карток), так і до моральної шкоди (наприклад, крадіжки особистих даних або шахрайства, оскільки були порушені дані посвідчення особи).

2.4.2 ВИПАДОК № 04 — Пом’якшення наслідків та зобов’язання

46. Важливим є інформування суб’єктів даних, щоб вони могли вжити необхідних заходів для уникнення матеріальної шкоди (наприклад, заблокувати свої кредитні картки).

47. Окрім документування порушення відповідно до статті 33(5), у цьому випадку також обов’язковим є повідомлення наглядовому органу (стаття 33(1)), а контролер також зобов’язаний повідомити про порушення суб’єктам даних (стаття 34(1)). Останнє може бути здійснено на індивідуальній основі, але для осіб, контактні дані яких недоступні, контролер повинен зробити це публічно, за умови, що таке повідомлення не спричинить додаткових негативних наслідків для суб’єктів даних, наприклад, шляхом розміщення повідомлення на своєму вебсайті. В останньому випадку необхідне точне й чітке повідомлення, розміщене на видному місці на домашній сторінці контролера, з точними посиланнями на відповідні положення GDPR. Організації також може знадобитися оновити та виправити свої організаційні й технічні заходи та процедури щодо захисту персональних даних, а також заходи та процедури щодо зменшення ризиків.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб’єктами даних
✓	✓	✓

2.5 Організаційні та технічні заходи для запобігання/пом’якшення наслідків атак з використанням програм-вимагачів

48. Той факт, що атака з використанням програм-вимагачів могла відбутися, зазвичай є ознакою однієї або декількох вразливостей у системі контролера. Це також стосується випадків, коли персональні дані були зашифровані, але не були викрадені. Незалежно від результату та наслідків атаки, важливість всебічної оцінки системи захисту даних — з особливим акцентом на IT-безпеку —

[17] Вказівки щодо операцій з обробки даних, які *«можуть призвести до високого ризику»*, див. у виносці 10 вище.

неможливо переоцінити. Виявлені недоліки та прогалини в системі безпеки мають бути задокументовані та усунені без зволікань.

49. Рекомендовані заходи:

(Перелік наведених нижче заходів у жодному разі не є вичерпним або всеосяжним. Скоріше, метою є надання ідей щодо запобігання та можливих рішень. Кожна операція з обробки даних відрізняється від інших, тому контролер повинен прийняти рішення про те, які заходи найбільше відповідають конкретній ситуації).

- Постійне оновлення прошивки, операційної системи та прикладного програмного забезпечення на серверах, клієнтському обладнанні, активних мережевих компонентах і будь-якому іншому обладнанні в одній локальній мережі (включаючи пристрої Wi-Fi). Забезпечення наявності належних заходів IT-безпеки, переконання в їх ефективності та регулярне оновлення у разі зміни або розвитку обставин, пов'язаних з обробкою даних. Сюди входить ведення детальних журналів про те, які патчі застосовуються в який момент часу.
- Розроблення та організація систем обробки й інфраструктури для сегментації або ізоляції систем і мереж передачі даних, щоб уникнути поширення шкідливого програмного забезпечення всередині організації та в зовнішні системи.
- Наявність актуальної, безпечної та перевіреної процедури резервного копіювання. Носії для середньо- та довгострокового резервного копіювання повинні зберігатися окремо від оперативних сховищ даних і бути недоступними для третіх осіб навіть у разі успішної атаки (наприклад, щоденне інкрементне резервне копіювання та щотижневе повне резервне копіювання).
- Наявність/придбання відповідного, сучасного, ефективного та інтегрованого програмного забезпечення для захисту від шкідливого програмного забезпечення.
- Наявність відповідного, сучасного, ефективного та інтегрованого брандмауера, а також системи виявлення та запобігання вторгненням. Спрямування мережевого трафіку через брандмауер/систему виявлення вторгнень, навіть у випадку домашньої або мобільної роботи (наприклад, шляхом використання VPN-з'єднань із механізмами безпеки організації при доступі до Інтернету).
- Навчання працівників методам розпізнавання та запобігання IT-атакам. Контролер повинен забезпечити засоби для встановлення того, чи є електронні листи та повідомлення, отримані іншими засобами зв'язку, автентичними та достовірними. Працівники повинні вміти розпізнавати, коли така атака реалізувалася, як вивести кінцеву точку з мережі та їх обов'язку негайно повідомити про це співробітника служби безпеки.
- Необхідність ідентифікації типу шкідливого коду, щоб побачити наслідки атаки та мати змогу вжити правильних заходів для зменшення ризику. Якщо атака програми-вимагача була успішною, а резервна копія недоступна, для відновлення даних можуть застосовуватися доступні інструменти, такі як інструменти проекту «No More Ransom» (nomoreransom.org). Однак, якщо доступна безпечна резервна копія, бажано відновити дані з неї.
- Пересилання або реплікація всіх журналів на центральний сервер журналів (можливо, з підписом або криптографічною позначкою часу для записів журналу).
- Надійне шифрування та багатофакторна автентифікація, зокрема для адміністративного доступу до IT-систем, належне управління ключами та паролями.
- Регулярне тестування на вразливість та проникнення.
- Створіть в організації групу реагування на інциденти комп'ютерної безпеки (CSIRT) або групу реагування на комп'ютерні надзвичайні ситуації (CERT), або приєднайтеся до колективної

CSIRT/CERT. Створіть план реагування на інциденти, план аварійного відновлення та план безперервності роботи й переконайтеся, що вони ретельно протестовані.

- При оцінці контрзаходів слід переглядати, тестувати та оновлювати аналіз ризиків.

3 АТАКИ З ВИТОКОМ ДАНИХ

50. Атаки, які використовують вразливості в послугах, що пропонуються контролером третім особам через Інтернет, наприклад, шляхом ін'єкційних атак (наприклад, SQL-ін'єкції, обхід шляху), компрометації вебсайтів та подібних методів, можуть нагадувати атаки з вимогами викупу в тому сенсі, що ризик походить від дій неавторизованої третьої особи, але ці атаки, як правило, спрямовані на копіювання, проникнення та зловживання персональними даними з певною зловмисною метою. Таким чином, вони здебільшого порушують конфіденційність і, можливо, також цілісність даних. У той же час, якщо контролер обізнаний із характеристиками такого роду порушень, існує багато заходів, доступних для контролерів, які можуть істотно знизити ризик успішного здійснення атаки.

3.1 ВИПАДОК № 05: Витік даних заявок на роботу з вебсайту

Агентство з працевлаштування стало жертвою кібератаки, яка розмістила шкідливий код на його вебсайті. Цей шкідливий код зробив особисту інформацію, подану через онлайн-форми заяв на працевлаштування та збережену на вебсервері, доступною для несанкціонованих осіб. 213 таких форм можуть бути порушеними. Після аналізу постраждалих даних було встановлено, що жодних особливих категорій даних не було порушено. Встановлений інструментарій шкідливого програмного забезпечення мав функції, які дозволяли зловмиснику видаляти будь-яку історію проникнення, а також дозволяли відстежувати обробку на сервері та перехоплювати персональні дані. Інструментарій було виявлено лише через місяць після його встановлення.

3.1.1 ВИПАДОК № 05 — Попередні заходи та оцінка ризиків

51. Безпека середовища контролера даних є надзвичайно важливою, оскільки більшість таких порушень можна запобігти, забезпечивши постійне оновлення всіх систем, шифрування конфіденційних даних та розроблення додатків відповідно до високих стандартів безпеки, таких як надійна автентифікація, заходи проти грубої сили, атак, «екранування» або «очищення»[18] вхідних даних користувача тощо. Періодичні аудити IT-безпеки, оцінки вразливостей і тести на проникнення також необхідні для того, щоб заздалегідь виявити такі вразливості та виправити їх. У цьому конкретному випадку інструменти моніторингу цілісності файлів у виробничому середовищі могли б допомогти виявити ін'єкцію коду (Перелік рекомендованих заходів наведено в розділі 3.7).

52. Контролер завжди повинен починати розслідування порушення з визначення типу атаки та її методів, щоб оцінити, яких заходів необхідно вжити. Щоб зробити це швидко та ефективно, контролер даних повинен мати план реагування на інциденти, який визначає швидкі та необхідні кроки для взяття під контроль інциденту. У цьому конкретному випадку тип порушення був фактором, що підвищує ризик, оскільки не лише було порушено конфіденційність даних, але й зловмисник мав засоби для внесення змін до системи, тому цілісність даних також стала сумнівною.

[18] Екранування або очищення користувацьких даних — це форма перевірки даних, яка гарантує, що в інформаційну систему вводяться лише правильно відформатовані дані.

53. Характер, чутливість та обсяг персональних даних, які постраждали внаслідок порушення, слід оцінити, щоб визначити, якою мірою порушення вплинуло на суб'єктів даних. Хоча особливих категорій персональних даних не було порушено, доступні дані містять значний обсяг інформації про осіб з онлайн-форм, і ці дані можуть бути використані різними способами (таргетинг з метою небажаного маркетингу, крадіжка персональних даних тощо), тому тяжкість наслідків повинна підвищувати ризик для прав і свобод суб'єктів даних[19].

3.1.2 ВИПАДОК № 05 — Пом'якшення наслідків та зобов'язання

54. Якщо можливо, після вирішення проблеми слід порівняти базу даних з тією, що зберігається в захищеній резервній копії. Досвід, отриманий у результаті порушення, необхідно використати при оновленні ІТ-інфраструктури. Контролер даних повинен повернути всі постраждалі ІТ-системи до заздалегідь відомого чистого стану, усунути вразливість і впровадити нові заходи безпеки, щоб уникнути подібних випадків порушення безпеки даних у майбутньому, наприклад, перевірити цілісність файлів і провести аудит безпеки. Якщо персональні дані були не лише викрадені, але й видалені, контролер повинен вжити систематичних заходів для відновлення персональних даних у тому стані, в якому вони були до витоку. Може знадобитися застосування повних резервних копій, інкрементних змін, а потім, можливо, повторний запуск обробки з моменту останньої інкрементної резервної копії, що вимагає, щоб контролер був здатний відтворити зміни, внесені з моменту останньої резервної копії. Це може вимагати, щоб контролер мав систему, призначену для збереження щоденних вхідних файлів на випадок, якщо їх потрібно буде обробити знову, а також вимагає надійного методу зберігання та відповідної політики зберігання.

55. У світлі вищезазначеного, оскільки порушення може призвести до високого ризику для прав і свобод фізичних осіб, суб'єкти даних повинні бути обов'язково проінформовані про це (стаття 34(1)), що, звичайно, означає, що відповідний(-і) НО також повинен(-ні) бути залучений(-і) до процесу у формі повідомлення про порушення безпеки даних. Документування порушення є обов'язковим згідно зі статтею 33(5) GDPR і полегшує оцінку ситуації.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	✓	✓

3.2 ВИПАДОК № 06: Викрадення хешованого паролю з вебсайту

Була використана SQL-ін'єкція як вразливість для отримання доступу до бази даних сервера кулінарного вебсайту. Користувачам було дозволено вибирати лише довільні псевдоніми для імен користувачів. Використання адрес електронної пошти для цієї мети не рекомендувалося. Паролі, що зберігалися в базі даних, хешувалися за допомогою надійного алгоритму, і сіль не була скомпрометована. Постраждалі дані: хешовані паролі 1 200 користувачів. Задля безпеки контролер поінформував суб'єктів даних про порушення електронною поштою і попросив їх змінити свої паролі, особливо якщо той самий пароль використовувався для інших сервісів.

[19] Вказівки щодо операцій з обробки даних, які *«можуть призвести до високого ризику»*, див. у виносці 10 вище.

3.2.1 ВИПАДОК № 06 — Попередні заходи та оцінка ризиків

56. У цьому конкретному випадку конфіденційність даних була порушена, але паролі в базі даних були хешовані сучасним методом, що зменшило ризик щодо характеру, чутливості та обсягу персональних даних. Цей випадок не становить жодних ризиків для прав і свобод суб'єктів даних.

57. Крім того, жодна контактна інформація (наприклад, адреси електронної пошти або номери телефонів) суб'єктів даних не була скомпрометована, що означає відсутність значного ризику для суб'єктів даних стати мішенню для спроб шахрайства (наприклад, отримання фішингових електронних листів або шахрайських текстових повідомлень і телефонних дзвінків). Особливі категорії персональних даних не були задіяні.

58. Деякі імена користувачів можуть розглядатися як персональні дані, але тематика вебсайту не допускає негативних конотацій. Хоча слід зазначити, що оцінка ризику може змінитися[20], якщо тип вебсайту та дані, до яких здійснюється доступ, можуть виявити особливі категорії персональних даних (наприклад, вебсайт політичної партії або профспілки). Використання сучасного шифрування може пом'якшити негативні наслідки порушення. Забезпечення обмеженої кількості спроб входу в систему унеможливить успіх атак грубої сили, що значно зменшить ризики, пов'язані з тим, що зловмисникам вже відомі імена користувачів.

3.2.2 ВИПАДОК № 06 — Пом'якшення наслідків та зобов'язання

59. Повідомлення суб'єктів даних у деяких випадках можна вважати пом'якшувальною обставиною, оскільки суб'єкти даних також можуть вжити необхідних заходів для уникнення подальшої шкоди від порушення, наприклад, змінивши свій пароль. У цьому випадку повідомлення не було обов'язковим, але в багатьох випадках його можна вважати належною практикою.

60. Контролер даних повинен виправити вразливість та впровадити нові заходи безпеки, щоб уникнути подібних витоків даних у майбутньому, наприклад, систематично проводити аудит безпеки вебсайту.

61. Порушення має бути задокументоване відповідно до статті 33(5), але не вимагається жодних повідомлень чи сповіщень.

62. Також настійно рекомендується повідомляти суб'єктам даних про порушення, пов'язане з паролями, у будь-якому випадку, навіть якщо паролі зберігалися з використанням солоного хешу з алгоритмом, що відповідає сучасному рівню розвитку. Використання методів автентифікації, що виключають необхідність обробки паролів на стороні сервера, є кращим. Суб'єктам даних має бути надана можливість вибору щодо вжиття відповідних заходів стосовно їхніх власних паролів.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	X	X

[20] Вказівки щодо операцій з обробки даних, які *«можуть призвести до високого ризику»*, див. у виносці 10 вище.

3.3 ВИПАДОК № 07: Атака на банківський сайт через підбір облікових даних

Банк зазнав кібератаки на один зі своїх вебсайтів онлайн-банкінгу. Атака мала на меті перерахувати всі можливі логіни користувачів для входу, використовуючи фіксований тривіальний пароль. Паролі складаються із 8 цифр. Через вразливість вебсайту в деяких випадках інформація про суб'єктів даних (ім'я, прізвище, стать, дата і місце народження, фіскальний код, ідентифікаційні коди користувачів) потрапила до зловмисника, навіть якщо використаний пароль був неправильним або банківський рахунок більше не був активним. Це торкнулося близько 100 000 суб'єктів даних. З них зловмисник успішно увійшов до близько 2 000 облікових записів, які використовували тривіальний пароль, який намагався підібрати зловмисник. Після цього контролер зміг ідентифікувати всі незаконні спроби входу в систему. Контролер даних може підтвердити, що, згідно з перевірками системи захисту від шахрайства, під час атаки із цих облікових записів не було здійснено жодних транзакцій. Банк знав про порушення безпеки даних, оскільки його операційний центр безпеки виявив велику кількість запитів на вхід до вебсайту. У відповідь на це контролер відключив можливість входу на вебсайт, вимкнувши його та примусово змінивши паролі скомпрометованих облікових записів. Контролер повідомив про порушення лише користувачам, які мали скомпрометовані акаунти, тобто користувачам, чиї паролі були скомпрометовані або чиї дані були розкриті.

3.3.1 ВИПАДОК № 07 — Попередні заходи та оцінка ризиків

63. Важливо зазначити, що контролери, які оперують даними суто особистого характеру[21], несуть більшу відповідальність за забезпечення належного захисту даних, наприклад, створення центру безпеки та інших заходів із запобігання, виявлення та реагування на інциденти. Недотримання цих вищих стандартів неодмінно призведе до більш серйозних заходів під час розслідування НО.

64. Порушення стосується фінансових даних, окрім інформації про особу та дані користувача, що робить його особливо серйозним. Кількість постраждалих осіб є великою.

65. Той факт, що порушення могло статися в такому чутливому середовищі, вказує на значні прогалини в системі безпеки даних контролера й може бути індикатором того, що настав час переглянути та оновити відповідні заходи відповідно до статей 24(1), 25(1) та 32(1) GDPR. Порушені дані дозволяють унікально ідентифікувати суб'єктів даних та містять іншу інформацію про них (включаючи стать, дату та місце народження), крім того, вони можуть бути використані зловмисником для підбору паролів клієнтів або для проведення фішингової кампанії, спрямованої на клієнтів банку.

66. Із цих причин було визнано, що порушення безпеки даних може призвести до високого ризику для прав і свобод усіх відповідних суб'єктів даних[22]. Таким чином, виникнення матеріальної (наприклад, фінансові збитки) та моральної шкоди (наприклад, крадіжка особистих даних або шахрайство) є можливим результатом.

---

[21] Наприклад, інформація про суб'єктів даних, що стосується способів оплати, таких як номери карток, банківські рахунки, онлайн-платежі, платіжні відомості, банківські виписки, економічні дослідження або будь-яка інша інформація, яка може розкрити економічну інформацію, що стосується суб'єктів даних.

[22] Вказівки щодо операцій з обробки даних, які *«можуть призвести до високого ризику»*, див. у виносці 10 вище.

3.3.2 ВИПАДОК № 07 — Пом'якшення наслідків та зобов'язання

67. Заходи контролера, згадані в описі випадку, є належними. Після порушення він також виправив вразливість вебсайту та вжив інших заходів для запобігання подібним витокам даних у майбутньому, наприклад, додавши двофакторну автентифікацію на відповідний вебсайт та перейшовши на надійну автентифікацію клієнтів.

68. Документування порушення відповідно до статті 33(5) GDPR та повідомлення про нього НО не є необов'язковим у цьому сценарії. Крім того, контролер повинен повідомити всіх 100 000 суб'єктів даних (включаючи суб'єктів даних, чиї облікові записи не були скомпрометовані) відповідно до статті 34 GDPR.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	✓	✓

3.4 Організаційні та технічні заходи для запобігання/пом'якшення наслідків хакерських атак

69. Як і у випадку атак з використанням програм-вимагачів, незалежно від результату та наслідків атаки, переоцінка IT-безпеки є обов'язковою для контролерів у подібних випадках.

70. Рекомендовані заходи:[23]

(*Перелік наведених нижче заходів у жодному разі не є вичерпним або всеосяжним. Скоріше, метою є надання ідей щодо запобігання та можливих рішень. Кожна операція з обробки даних відрізняється від інших, тому контролер повинен прийняти рішення про те, які заходи найбільше відповідають конкретній ситуації*).

- Сучасне шифрування та управління ключами, особливо коли обробляються паролі, конфіденційні або фінансові дані. Криптографічне хешування та соління для секретної інформації (паролів) завжди є кращим за шифрування паролів. Використання методів автентифікації, що виключають необхідність обробки паролів на стороні сервера, є кращим.
- Підтримка системи в актуальному стані (програмне забезпечення та прошивка). Забезпечення наявності всіх заходів IT-безпеки, переконання в їх ефективності та регулярне оновлення у разі зміни або розвитку обставин, пов'язаних з обробкою даних. Для того, щоб мати можливість продемонструвати відповідність статті 5(1(f) відповідно до статті 5(2) GDPR, контролер повинен вести облік усіх виконаних оновлень, включаючи також час, коли вони були застосовані.
- Використання надійних методів автентифікації, таких як двофакторна автентифікація та сервери автентифікації, доповнені актуальною політикою паролів.
- Стандарти безпечного розроблення включають фільтрацію користувацького вводу (з використанням білих списків, наскільки це практично можливо), ескалацію користувацького вводу та заходи запобігання грубої сили (наприклад, обмеження максимальної кількості повторних спроб). «Брандмауери вебдодатків» можуть допомогти в ефективному використанні цього методу.
- Впровадження сильних користувацьких привілеїв та політики управління контролем доступу.

[23] Щодо безпечного розроблення вебдодатків див. також: https://www.owasp.org/index.php/Main_Page.

- Використання відповідних, сучасних, ефективних та інтегрованих брандмауерів, систем виявлення вторгнень та інших систем захисту периметра.
- Систематичний аудит IT-безпеки та оцінка вразливостей (тестування на проникнення).
- Регулярні перевірки та тестування для забезпечення можливості використання резервних копій для відновлення будь-яких даних, цілісність або доступність яких була порушена.
- Відсутність ідентифікатора сеансу в URL-адресі у вигляді простого тексту.

4 ВНУТРІШНІЙ ЛЮДСЬКИЙ ФАКТОР РИЗИКУ

71. Роль людської помилки у порушенні безпеки персональних даних слід підкреслити, зважаючи на її поширеність. Оскільки ці типи порушень можуть бути як навмисними, так і ненавмисними, контролерам даних дуже важко виявити вразливі місця та вжити заходів для їх уникнення. Міжнародна конференція комісарів із захисту даних та конфіденційності визнала важливість врахування таких людських факторів та ухвалила резолюцію щодо ролі людських помилок у порушеннях безпеки персональних даних у жовтні 2019 року[24]. Ця резолюція підкреслює, що для запобігання людським помилкам слід вживати належних запобіжних заходів, і надає невичерпний перелік таких запобіжних заходів та підходів.

4.1 ВИПАДОК № 08: Витік комерційної інформації внаслідок дій працівника

Під час перебування у відпустці працівник компанії копіює бізнес-дані з бази даних компанії. Працівник має право доступу до даних лише для виконання своїх робочих завдань. Через кілька місяців після звільнення він використовує отримані таким чином дані (основні контактні дані) для нової обробки даних, контролером якої він є, щоб зв'язатися з клієнтами компанії та залучити їх до свого нового бізнесу.

4.1.1 ВИПАДОК № 08 — Попередні заходи та оцінка ризиків

72. У цьому конкретному випадку не було вжито жодних попередніх заходів, щоб запобігти копіюванню працівником контактної інформації клієнтів компанії, оскільки він потребував — і мав — законний доступ до цієї інформації для виконання своїх робочих завдань. Оскільки виконання більшості робіт, пов'язаних з відносинами з клієнтами, вимагає певного доступу працівника до персональних даних, такі порушення безпеки даних може бути найскладніше запобігти. Обмеження обсягу доступу може обмежити роботу, яку може виконувати даний працівник. Однак добре продумана політика доступу та постійний контроль можуть допомогти запобігти таким порушенням.

73. Як завжди, під час оцінки ризиків слід брати до уваги тип порушення, а також характер, чутливість та обсяг персональних даних, які можуть бути порушені. Такі види порушень зазвичай є порушеннями конфіденційності, оскільки база даних зазвичай залишається недоторканою, її вміст «просто» копіюється для подальшого використання. Кількість даних, що порушуються, зазвичай також невелика або середня. У цьому конкретному випадку не було порушено жодних особливих категорій персональних даних, працівникові потрібна була лише контактна інформація клієнтів, щоб він міг зв'язатися з ними після звільнення з компанії. Таким чином, ці дані не є конфіденційними.

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf

74. Хоча єдина мета колишнього працівника, який зловмисно скопіював дані, може обмежуватися отриманням контактної інформації клієнтів компанії для власних комерційних цілей, контролер не може вважати ризик для постраждалих суб'єктів даних низьким, оскільки він не має жодних гарантій щодо намірів працівника. Таким чином, хоча наслідки порушення можуть бути обмежені небажаним самомаркетингом колишнього працівника, не виключені подальші та більш серйозні зловживання викраденими даними, залежно від мети обробки, яку запровадив колишній працівник[25].

4.1.2 ВИПАДОК № 08 — Пом'якшення наслідків та зобов'язання

75. Пом'якшення негативних наслідків порушення у вищезгаданому випадку є складним завданням. Можливо, доведеться негайно звернутися до суду, щоб запобігти подальшому зловживанню та поширенню даних колишнім працівником. Наступним кроком має бути уникнення подібних ситуацій у майбутньому. Контролер може спробувати наказати колишньому працівникові припинити використання даних, але успіх цієї дії в кращому випадку сумнівний. Допомогти можуть відповідні технічні заходи, такі як унеможливлення копіювання чи завантаження даних на знімні пристрої.

76. Універсального рішення для таких випадків не існує, але системний підхід може допомогти запобігти їм. Наприклад, компанія може розглянути можливість позбавлення певних форм доступу працівників, які повідомили про свій намір звільнитися, або запровадження журналів доступу, щоб можна було реєструвати небажаний доступ і позначати його. Договір, підписаний з працівниками, повинен містити пункти, які забороняють такі дії.

77. Загалом, оскільки дане порушення не призведе до високого ризику для прав і свобод фізичних осіб, достатньо буде повідомити про нього НО. Однак інформування суб'єктів даних може бути корисним і для контролера даних, оскільки їм буде краще дізнатися про витік даних від компанії, а не від колишнього працівника, який намагається з ними зв'язатися. Документування витоку даних відповідно до статті 33(5) є юридичним зобов'язанням.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	✓	X

[25] Вказівки щодо операцій з обробки даних, які *«можуть призвести до високого ризику»*, див. у виносці 10 вище.

4.2 ВИПАДОК № 09: Випадкова передача даних довіреній третій стороні

Страховий агент помітив, що через неправильні налаштування файлу Excel, отриманого електронною поштою, він отримав доступ до інформації про два десятки клієнтів, які не належать до його сфери діяльності. Він зобов'язаний зберігати професійну таємницю і був єдиним одержувачем електронного листа. Домовленість між контролером даних і страховим агентом зобов'язує агента негайно повідомляти контролера даних про порушення безпеки персональних даних. Тому агент миттєво повідомив про помилку контролеру, який виправив файл і розіслав його повторно, попросивши агента видалити попереднє повідомлення. Відповідно до вищезгаданої домовленості, агент повинен був підтвердити видалення в письмовій заяві, що він і зробив. Отримана інформація не містить особливих категорій персональних даних, лише контактні дані та дані про саме страхування (вид страхування, сума). Проаналізувавши персональні дані, на які вплинуло порушення, контролер даних не виявив жодних особливих характеристик з боку фізичних осіб або контролера даних, які могли б вплинути на рівень впливу порушення.

4.2.1 ВИПАДОК № 09 — Попередні заходи та оцінка ризиків

78. Тут порушення не є наслідком навмисних дій працівника, а ненавмисної людської помилки, спричиненої неуважністю. Таких порушень можна уникнути або зменшити їхню частоту, якщо: a) впроваджувати програми навчання, освіти та підвищення обізнаності, де працівники краще розуміють важливість захисту персональних даних; b) зменшити обмін файлами електронною поштою, натомість використовувати спеціальні системи для обробки даних клієнтів, наприклад, c) двічі перевіряти файли перед надсиланням; d) розмежувати створення та надсилання файлів.

79. Це порушення стосується лише конфіденційності даних, а їх цілісність та доступність не порушені. Порушення безпеки даних стосувалося лише близько двох десятків учасників, отже, кількість порушених даних можна вважати незначною. Крім того, персональні дані, що постраждали, не містять жодних чутливих даних. Той факт, що оператор даних негайно зв'язався з контролером після того, як йому стало відомо про порушення безпеки даних, можна вважати фактором, що зменшує ризик. (Слід також оцінити можливість того, що дані були надіслані іншим страховим агентам, і, якщо це підтвердиться, вжити належних заходів). Завдяки належним заходам, вжитим після порушення безпеки даних, воно, ймовірно, не матиме жодного впливу на права та свободи суб'єктів даних.

80. Поєднання невеликої кількості постраждалих осіб, негайного виявлення порушення та заходів, вжитих для мінімізації його наслідків, робить цей конкретний випадок не ризикованим.

4.2.2 ВИПАДОК № 09 — Пом'якшення наслідків та зобов'язання

81. Крім того, є й інші обставини, що зменшують ризик: агент зобов'язаний зберігати професійну таємницю; він сам повідомив про проблему контролеру; і він видалив файл на вимогу. Підвищення обізнаності та, можливо, включення додаткових кроків у перевірку документів, що містять персональні дані, ймовірно, допоможе уникнути подібних випадків у майбутньому.

82. Окрім документування порушення відповідно до статті 33(5), немає потреби в будь-яких інших діях.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	X	X

4.3 Організаційні та технічні заходи щодо запобігання/пом'якшення впливу внутрішнього людського фактору ризику

83. Поєднання наведених нижче заходів, що застосовуються залежно від унікальних особливостей конкретного випадку, має допомогти знизити ймовірність повторення подібних порушень.

84. Рекомендовані заходи:

(*Перелік наведених нижче заходів у жодному разі не є вичерпним або всеосяжним. Скоріше, метою є надання ідей щодо запобігання та можливих рішень. Кожна операція з обробки даних відрізняється від інших, тому контролер повинен прийняти рішення про те, які заходи найбільше відповідають конкретній ситуації*).

- Періодичне впровадження програми підготовки, навчання та підвищення обізнаності працівників щодо їхніх зобов'язань у сфері конфіденційності та безпеки, а також виявлення та інформування про загрози безпеці персональних даних [26]. Розроблення інформаційної програми, яка б нагадувала працівникам про найпоширеніші помилки, що призводять до порушення безпеки персональних даних, та про те, як їх уникнути.
- Створення надійних та ефективних практик, процедур та систем захисту даних і конфіденційності[27].
- Оцінка практик, процедур і систем конфіденційності для забезпечення постійної ефективності[28].
- Створення належних політик контролю доступу та примушення користувачів дотримуватися правил.
- Впровадження методів примусової автентифікації користувачів при доступі до конфіденційних персональних даних.
- Вимкнення облікового запису користувача, пов'язаного з компанією, як тільки він звільняється з компанії.
- Перевірка незвичайного потоку даних між файловим сервером і робочими станціями співробітників.
- Налаштування безпеки інтерфейсів вводу/виводу в BIOS або за допомогою програмного забезпечення, що контролює використання комп'ютерних інтерфейсів (блокування або розблокування, наприклад, USB/CD/DVD і т.д.).
- Перегляд політики доступу співробітників (наприклад, реєстрація доступу до конфіденційних даних і вимоги щодо зазначення ділової причини для доступу, що має бути доступним для аудиту).
- Відключення відкритих хмарних сервісів.
- Заборона та запобігання доступу до відомих відкритих поштових сервісів.
- Вимкнення функції екрана друку в операційній системі.
- Впровадження політики чистого робочого столу.
- Автоматичне блокування всіх комп'ютерів після певного часу бездіяльності.
- Використання механізмів (наприклад, (бездротових) токенів для входу/відкриття заблокованих облікових записів) для швидкого перемикання користувачів у спільних середовищах.
- Використання спеціальних систем для управління персональними даними, які застосовують відповідні механізми контролю доступу та запобігають людським помилкам, таким як надсилання

[26] Розділ 2) підрозділ (i) Резолюції щодо ролі людської помилки у порушенні безпеки персональних даних.

[27] Розділ 2) підрозділ (ii) Резолюції щодо ролі людської помилки у порушенні безпеки персональних даних.

[28] Розділ 2) підрозділ (iii) Резолюції щодо ролі людської помилки у порушенні безпеки персональних даних.

повідомлень не тому суб'єкту. Використання електронних таблиць та інших офісних документів не є належним засобом для управління даними клієнтів.

5 ЗАГУБЛЕНІ АБО ВИКРАДЕНІ ПРИСТРОЇ ТА ПАПЕРОВІ ДОКУМЕНТИ

85. Частим типом випадків є втрата або крадіжка портативних пристроїв. У таких випадках контролер повинен враховувати обставини операції з обробки, такі як тип даних, що зберігаються на пристрої, а також допоміжні засоби, і заходи, вжиті до порушення для забезпечення належного рівня безпеки. Всі ці елементи впливають на потенційні наслідки порушення безпеки даних. Оцінка ризику може бути ускладнена, оскільки пристрій більше не є доступним.

86. Такі види порушень завжди можна класифікувати як порушення конфіденційності. Однак, якщо немає резервної копії викраденої бази даних, то тип порушення може бути також порушенням доступності та порушенням цілісності.

87. Наведені нижче сценарії демонструють, як вищезазначені обставини впливають на ймовірність та тяжкість порушення безпеки даних.

5.1 ВИПАДОК № 10: Викрадення носія, на якому зберігаються зашифровані персональні дані

Під час проникнення до дитячого садка було викрадено два планшети. У планшетах був додаток, який містив персональні дані про дітей, які відвідують дитячий садок. Йшлося про ім'я, дату народження, особисті дані про освіту дітей. І зашифровані планшети, які були вимкнені під час злому, і додаток були захищені надійним паролем. Резервне копіювання даних було ефективним і легкодоступним для контролера. Після того, як стало відомо про злом, дитячий садок віддалено віддав команду видалити дані з планшетів незабаром після виявлення злому.

5.1.1 ВИПАДОК № 10 — Попередні заходи та оцінка ризиків

88. У цьому конкретному випадку контролер даних вжив належних заходів для запобігання та пом'якшення наслідків потенційного порушення безпеки даних, використовуючи шифрування пристроїв, запровадивши належний захист паролем та забезпечивши резервне копіювання даних, що зберігалися на планшетах (Перелік рекомендованих заходів наведено в розділі 5.7).

89. Дізнавшись про витік даних, контролер даних повинен оцінити джерело ризику, системи, що підтримують обробку даних, тип персональних даних, а також потенційний вплив витоку даних на відповідних осіб. Витік даних, описаний вище, міг би стосуватися конфіденційності, доступності та цілісності відповідних даних, однак завдяки належним діям контролера даних до та після витоку даних жодного із цих аспектів не було порушено.

5.1.2 ВИПАДОК № 10 — Пом'якшення наслідків та зобов'язання

90. Конфіденційність персональних даних на пристроях не була порушена завдяки надійному захисту паролем як на планшетах, так і в додатках. Планшети були налаштовані таким чином, що встановлення пароля також означає, що дані на пристрої зашифровані. Це ще більше посилювалося діями контролера, який намагався віддалено видалити все з викрадених пристроїв.

91. Завдяки вжитим заходам, конфіденційність даних також була збережена. Крім того, резервне копіювання забезпечило постійну доступність персональних даних, отже, не могло виникнути жодних потенційних негативних наслідків.

92. З огляду на ці факти, описане вище порушення безпеки даних навряд чи могло призвести до ризику для прав і свобод суб'єктів даних, а отже, не було необхідності повідомляти про нього НО або відповідних суб'єктів даних. Однак це порушення безпеки даних також має бути задокументоване відповідно до статті 33(5).

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	X	**X**

5.2 ВИПАДОК № 11: Викрадення носія, на якому зберігаються незашифровані персональні дані

У співробітника компанії, що надає послуги, було викрадено електронний планшет для нотаток. Викрадений планшет містив імена, прізвища, стать, адреси та дати народження понад 100 000 клієнтів. Через недоступність викраденого пристрою не вдалося встановити, чи постраждали також інші категорії персональних даних. Доступ до жорсткого диску планшета не був захищений жодним паролем. Персональні дані можна було відновити зі щоденних резервних копій.

5.2.1 ВИПАДОК № 11 — Попередні заходи та оцінка ризиків

93. Контролер даних не вжив жодних попередніх заходів безпеки, тому персональні дані, що зберігалися на викраденому планшеті, були легкодоступними для крадія або будь-якої іншої особи, яка заволоділа цим пристроєм.

94. Це порушення стосується конфіденційності даних, що зберігалися на викраденому пристрої.

95. У цьому випадку планшет, що містив персональні дані, був вразливим, оскільки він не був захищений паролем чи шифруванням. Відсутність базових заходів безпеки підвищує рівень ризику для постраждалих суб'єктів даних. Крім того, ідентифікація відповідних суб'єктів даних також є проблематичною, що також збільшує серйозність порушення. Значна кількість таких осіб збільшує ризик, однак, попри те, що витік даних не стосувався особливих категорій персональних даних.

96. Під час оцінки ризиків[29] контролер повинен взяти до уваги потенційні наслідки та несприятливий вплив порушення конфіденційності. У результаті порушення відповідні суб'єкти даних можуть постраждати від шахрайства з ідентифікаційними даними, що ґрунтуються на даних, наявних на викраденому пристрої, тому ризик вважається високим.

5.2.2 ВИПАДОК № 11 — Пом'якшення наслідків та зобов'язання

97. Увімкнення шифрування пристрою та використання надійного захисту з паролем збереженої бази даних могло б запобігти порушенню безпеки даних, який би призвів до ризику для прав і свобод суб'єктів даних.

[29] Вказівки щодо операцій з обробки даних, які *«можуть призвести до високого ризику»*, див. у виносці 10 вище.

98. У зв'язку із цими обставинами необхідним є повідомлення НО, а також відповідних суб'єктів даних.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	✓	✓

5.3 ВИПАДОК № 12: Викрадення паперових файлів з конфіденційними даними

З реабілітаційного центру для наркозалежних було викрадено паперовий журнал. Журнал містив основні дані про особу та стан здоров'я пацієнтів, які потрапляли до реабілітаційного центру. Дані зберігалися лише на папері, і лікарі, які лікували пацієнтів, не мали жодної резервної копії. Книга не зберігалася у замкненій шафі або кімнаті, у контролера даних не було ані режиму контролю доступу, ані інших заходів захисту паперової документації.

5.3.1 ВИПАДОК № 12 — Попередні заходи та оцінка ризиків

99. Контролер не вжив жодних попередніх заходів безпеки, тому персональні дані, що зберігалися в цьому журналі, були легкодоступними для особи, яка його знайшла. Крім того, характер персональних даних, що зберігалися в журналі, робить відсутність резервних копій дуже серйозним фактором ризику.

100. Цей випадок слугує прикладом порушення безпеки даних з високим ступенем ризику. Через недотримання належних заходів безпеки було втрачено конфіденційні дані про стан здоров'я відповідно до статті 9(1) GDPR. Оскільки в цьому випадку йшлося про особливу категорію персональних даних, потенційні ризики для відповідних суб'єктів даних були підвищені, що також має бути враховано контролером, який оцінює ризик[30].

101. Це порушення стосується конфіденційності, доступності та цілісності відповідних персональних даних. У результаті такої ситуації порушується лікарська таємниця, і неуповноважені треті особи можуть отримати доступ до приватної медичної інформації пацієнтів, що може мати серйозні наслідки для їхнього здоров'я та життя. Порушення доступності може також порушити безперервність лікування пацієнтів. Оскільки не виключена можливість модифікації/видалення частини змісту журналу, цілісність персональних даних також може бути порушена.

5.3.2 ВИПАДОК № 12 — Пом'якшення наслідків та зобов'язання

102. Під час оцінки заходів захисту слід також враховувати тип допоміжного активу. Оскільки медична карта пацієнта була фізичним документом, її захист мав бути організований інакше, ніж захист електронного пристрою. Псевдонімізація імен пацієнтів, зберігання журналу в приміщенні, що охороняється, у замкненій шухляді або кімнаті, а також належний контроль доступу з автентифікацією під час доступу до нього могли б запобігти порушенню безпеки даних.

103. Описане вище порушення безпеки даних може серйозно вплинути на відповідних суб'єктів даних; отже, повідомлення НО та інформування про порушення відповідних суб'єктів даних є обов'язковим.

Необхідні дії на основі виявлених ризиків

[30] Вказівки щодо операцій з обробки даних, які *«можуть призвести до високого ризику»*, див. у виносці 10 вище.

Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	✓	✓

5.4 Організаційні та технічні заходи для запобігання/пом'якшення наслідків втрати або крадіжки пристроїв

104. Поєднання наведених нижче заходів, що застосовуються залежно від унікальних особливостей конкретного випадку, має допомогти знизити ймовірність повторення подібних порушень.

105. Рекомендовані заходи:

(*Перелік наведених нижче заходів у жодному разі не є вичерпним або всеосяжним. Скоріше, метою є надання ідей щодо запобігання та можливих рішень. Кожна операція з обробки даних відрізняється від інших, тому контролер повинен прийняти рішення про те, які заходи найбільше відповідають конкретній ситуації*).

- Увімкніть шифрування пристрою (наприклад, Bitlocker, Veracrypt або DM-Crypt).
- Використовуйте код/пароль на всіх пристроях. Зашифруйте всі мобільні електронні пристрої таким чином, щоб для розшифрування потрібно було вводити складний пароль.
- Використовуйте багатофакторну автентифікацію.
- Увімкніть функції високомобільних пристроїв, які дозволяють визначити їх місцезнаходження у разі втрати або неправильного розміщення.
- Використовуйте програмне забезпечення/додаток MDM (Mobile Devices Management) та локалізацію. Використовуйте антиблікові фільтри. Вимикайте всі пристрої, що залишаються без нагляду.
- Якщо це можливо і відповідає обробці даних, про яку йдеться, зберігайте персональні дані не на мобільному пристрої, а на центральному сервері.
- Якщо робоча станція підключена до корпоративної локальної мережі, робіть автоматичне резервне копіювання з робочих папок, за відсутності інших альтернатив, якщо там зберігаються персональні дані.
- Використовуйте безпечний VPN (наприклад, який вимагає окремого ключа другого фактору автентифікації для встановлення безпечного з'єднання) для підключення мобільних пристроїв до внутрішніх серверів.
- Надайте працівникам фізичні замки, щоб вони могли фізично захистити мобільні пристрої, якими вони користуються, поки вони залишаються без нагляду.
- Забезпечте належне регулювання використання пристроїв за межами компанії.
- Забезпечте належне регулювання використання пристроїв всередині компанії.
- Використовуйте програмне забезпечення/додаток MDM (Mobile Devices Management) та увімкніть функцію віддаленого видалення.
- Використовуйте централізоване управління пристроями з мінімальними правами для кінцевих користувачів на встановлення програмного забезпечення.
- Встановіть фізичні засоби контролю доступу.
- Уникайте зберігання конфіденційної інформації на мобільних пристроях або жорстких дисках. Якщо є потреба у доступі до внутрішньої системи компанії, слід використовувати захищені канали, як зазначено вище.

6 ПОМИЛКА ПОШТОВОГО ВІДПРАВЛЕННЯ

106. У цьому випадку джерелом ризику також є внутрішня людська помилка, але до порушення не призвела жодна зловмисна дія. Це результат неуважності. Контролер мало що може зробити після того, як це сталося, тому профілактика в цих випадках навіть важливіша, ніж в інших типах порушень.

6.1 ВИПАДОК № 13: Помилка поштового відправлення

Два замовлення на взуття були упаковані компанією, що займається роздрібною торгівлею. Через людську помилку було переплутано дві пакувальні накладні, в результаті чого обидва товари та відповідні пакувальні накладні були відправлені не тій особі. Це означає, що два клієнти отримали замовлення один одного, включаючи пакувальні накладні, що містять персональні дані. Дізнавшись про порушення, контролер відкликав замовлення та відправив їх належним одержувачам.

6.1.1 ВИПАДОК № 13 — Попередні заходи та оцінка ризиків

107. Рахунки містили персональні дані, необхідні для успішної доставки (ім'я, адреса, а також придбаний товар і його ціна). Важливо визначити, як взагалі могла статися людська помилка, і чи можна було їй запобігти. В описаному конкретному випадку ризик є низьким, оскільки не йдеться про особливі категорії персональних даних або інші дані, зловживання якими могло б призвести до значних негативних наслідків, порушення не є результатом системної помилки з боку контролера, і йдеться лише про двох осіб. Негативного впливу на цих осіб не було виявлено.

6.1.2 ВИПАДОК № 13 — Пом'якшення наслідків та зобов'язання

108. Контролер повинен забезпечити безкоштовне повернення товарів та супровідних рахунків, а також вимагати від неправильних одержувачів знищити/видалити всі можливі копії рахунків, що містять персональні дані іншої особи.

109. Навіть якщо саме порушення не становить високого ризику для прав і свобод постраждалих осіб, а отже, повідомлення суб'єктам даних не є обов'язковим згідно зі статтею 34 GDPR, повідомлення їм про порушення не можна уникнути, оскільки для зменшення ризику необхідна їхня співпраця.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	X	X

6.2 ВИПАДОК № 14: Помилково надіслані поштою конфіденційні персональні дані

Відділ працевлаштування органу державного управління надіслав електронне повідомлення про майбутні тренінги особам, зареєстрованим у його системі як шукачі роботи. Помилково до цього електронного листа було прикріплено документ, що містив усі персональні дані цих осіб (ім'я, адреса електронної пошти, поштова адреса, номер соціального страхування). Кількість постраждалих осіб становить понад 60 000. Згодом відділ зв'язався з усіма одержувачами та попросив їх видалити попереднє повідомлення і не використовувати інформацію, що містилася в ньому.

6.2.1 ВИПАДОК № 14 — Попередні заходи та оцінка ризиків

110. Для надсилання таких повідомлень слід було б запровадити суворіші правила. Необхідно розглянути можливість запровадження додаткових механізмів контролю.

111. Кількість постраждалих осіб є значною, а залучення їхніх номерів соціального страхування разом з іншими, більш базовими персональними даними, ще більше підвищує ризик, який можна визначити як високий[31]. Контролер не може запобігти подальшому поширенню даних будь-яким з одержувачів.

6.2.2 ВИПАДОК № 14 — Пом'якшення наслідків та зобов'язання

112. Як згадувалося раніше, засоби ефективного зниження ризиків подібних порушень є обмеженими. Хоча контролер просить видалити повідомлення, він не може змусити одержувачів зробити це, і, як наслідок, не може бути впевненим у тому, що вони виконають вимогу.

113. Виконання всіх трьох нижчезазначених дій має бути само собою зрозумілим у подібних випадках.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	✓	✓

6.3 ВИПАДОК № 15: Помилково надіслані поштою персональні дані

Список учасників курсу юридичної англійської мови, який проходив у готелі протягом 5 днів, помилково було надіслано 15 колишнім учасникам курсу замість готелю. Список містить імена, адреси електронної пошти та вподобання щодо харчування цих 15 учасників. Лише двоє учасників вказали свої харчові вподобання, зазначивши, що у них непереносимість лактози. Жоден з учасників не має захищених особистих даних. Контролер виявляє помилку одразу після відправлення списку, інформує про неї одержувачів і просить їх видалити список.

6.3.1 ВИПАДОК № 15 — Попередні заходи та оцінка ризиків

114. Необхідно було запровадити суворі правила для надсилання повідомлень, що містять персональні дані. Необхідно розглянути можливість запровадження додаткових механізмів контролю.

115. Ризики, пов'язані з характером, конфіденційністю, обсягом та контекстом персональних даних, є низькими. Персональні дані включають конфіденційні дані про харчові вподобання двох учасників. Навіть якщо інформація про непереносимість лактози є медичними даними, ризик того, що ці дані будуть використані у зловмисний спосіб, слід вважати відносно низьким. Хоча у випадку даних про здоров'я зазвичай передбачається, що порушення може призвести до високого ризику для суб'єкта даних[32], водночас у цьому конкретному випадку не можна визначити ризик того, що порушення призведе до фізичної, матеріальної або моральної шкоди суб'єкту даних через несанкціоноване розкриття інформації про непереносимість лактози. На відміну від деяких інших харчових вподобань, непереносимість лактози зазвичай не може бути пов'язана з будь-якими релігійними чи

[31] Вказівки щодо операцій з обробки даних, які *«можуть призвести до високого ризику»*, див. у виносці 10 вище.

[32] Див. Настанови РД 250, с. 23.

філософськими переконаннями. Кількість порушених даних та кількість постраждалих суб'єктів даних також є дуже низькою.

6.3.2 ВИПАДОК № 15 — Пом'якшення наслідків та зобов'язання

116. Підсумовуючи, можна стверджувати, що порушення не мало значного впливу на суб'єктів даних. Той факт, що контролер негайно зв'язався з одержувачами після того, як дізнався про помилку, можна вважати пом'якшувальною обставиною.

117. Якщо електронний лист було надіслано неправильному/неналежному одержувачу, рекомендується, щоб контролер даних надіслав наступний електронний лист випадковим одержувачам з вибаченнями, інструкціями щодо видалення помилкового електронного листа та повідомленням одержувачів про те, що вони не мають права надалі використовувати ідентифіковані їм електронні адреси.

118. З огляду на ці факти, таке порушення безпеки даних навряд чи могло призвести до ризику для прав і свобод суб'єктів даних, а отже, не було необхідності повідомляти про нього НО або відповідних суб'єктів даних. Однак це порушення безпеки даних також має бути задокументоване відповідно до статті 33(5).

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	X	X

6.4 ВИПАДОК № 16: Помилка поштового відправлення

Страхова група пропонує страхування автомобілів. Для цього вона розсилає поштою регулярно кориговані поліси внесків. Крім імені та адреси страхувальника, в листі вказується реєстраційний номер транспортного засобу без замаскованих цифр, страхові тарифи поточного та наступного страхового року, приблизний річний пробіг та дата народження страхувальника. Медичні дані відповідно до статті 9 GDPR, платіжні дані (банківські реквізити), економічні та фінансові дані не включаються.

Листи запаковуються автоматизованим обладнанням для упаковки в конверти. Через механічну помилку два листи для різних страхувальників вкладаються в один конверт і надсилаються одному страхувальнику поштою. Страхувальник відкриває лист вдома і дивиться на свій правильно доставлений лист, а також на неправильно доставлений лист від іншого страхувальника.

6.4.1 ВИПАДОК № 16 — Попередні заходи та оцінка ризиків

119. Неправильно доставлений лист містить ім'я, адресу, дату народження, реєстраційний номер транспортного засобу та класифікацію страхового тарифу поточного та наступного року. Вплив на постраждалу особу можна оцінити як середній, оскільки інформація, яка не є загальнодоступною, наприклад, дата народження або незамасковані реєстраційні номери транспортних засобів, а також інформація про підвищення страхових тарифів, стає відомою неналежному одержувачу. Ймовірність неправомірного використання цих даних оцінюється як низька та середня. Однак хоча багато одержувачів, ймовірно, викинуть помилково отриманий лист у смітник, в окремих випадках не можна повністю виключити, що лист буде розміщено в соціальних мережах або що зі страхувальником зв'яжуться.

6.4.2 ВИПАДОК № 16 — Пом'якшення наслідків та зобов'язання

120. Контролер повинен повернути оригінал документа власним коштом. Неправильний одержувач також має бути поінформований про те, що він не може зловживати прочитаною інформацією.

121. Ймовірно, ніколи не вдасться повністю запобігти помилці доставки поштових відправлень під час масової розсилки з використанням повністю автоматизованого обладнання. Однак у разі збільшення частоти таких помилок необхідно перевірити, чи достатньо правильно налаштоване та обслуговується обладнання для упаковки в конверти, чи не призводить до них будь-яка інша системна проблема.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	✓	X

6.5 Організаційні та технічні заходи для запобігання/пом'якшення наслідків неправильного поштового відправлення

122. Поєднання наведених нижче заходів, що застосовуються залежно від унікальних особливостей конкретного випадку, має допомогти знизити ймовірність повторення подібних порушень.

123. Рекомендовані заходи:

(*Перелік наведених нижче заходів у жодному разі не є вичерпним або всеосяжним. Скоріше, метою є надання ідей щодо запобігання та можливих рішень. Кожна операція з обробки даних відрізняється від інших, тому контролер повинен прийняти рішення про те, які заходи найбільше відповідають конкретній ситуації*).

- Встановлення точних стандартів — без можливості для інтерпретації — для надсилання листів/електронних листів.
- Належне навчання персоналу тому, як надсилати листи/електронні листи.
- При надсиланні електронних листів кільком одержувачам вони за замовчуванням вказуються в полі «прихована копія».
- При надсиланні електронних листів кільком одержувачам, які не вказані в полі «прихована копія», потрібне додаткове підтвердження.
- Застосування принципу чотирьох очей.
- Автоматична адресація замість ручної, дані беруться з доступної та актуальної бази даних; систему автоматичної адресації слід регулярно перевіряти на наявність прихованих помилок і неправильних налаштувань.
- Застосування затримки повідомлення (наприклад, повідомлення може бути видалене/відредаговане протягом певного періоду часу після натискання кнопки).
- Вимкнення автозаповнення при введенні адрес електронної пошти.
- Інформаційні сесії про найпоширеніші помилки, що призводять до порушення безпеки персональних даних.
- Навчальні тренінги та посібники про те, як реагувати на інциденти, що призводять до порушення безпеки персональних даних, і кого інформувати (залучати фахівця з питань захисту даних).

7 ІНШІ ВИПАДКИ – СОЦІАЛЬНА ІНЖЕНЕРІЯ

7.1 ВИПАДОК № 17: Крадіжка особистих даних

До контакт-центру телекомунікаційної компанії надходить телефонний дзвінок від особи, яка представляється клієнтом. Так званий клієнт вимагає від компанії змінити адресу електронної пошти, на яку надалі надсилатиметься платіжна інформація. Працівник контакт-центру перевіряє особу клієнта, запитуючи певні персональні дані, визначені процедурами компанії. Абонент правильно вказує запитуваний фіскальний номер та поштову адресу клієнта (оскільки він мав доступ до цих даних). Після перевірки оператор вносить запитувані зміни, і з цього моменту платіжна інформація надсилається на нову електронну адресу. Процедура не передбачає жодних повідомлень на попередню адресу електронної пошти. Наступного місяця справжній клієнт звертається до компанії з питанням, чому він не отримує рахунки на свою електронну адресу, і заперечує будь-які дзвінки від нього з вимогою змінити адресу електронної пошти. Пізніше компанія усвідомлює, що інформація була надіслана недійсному користувачеві, і скасовує зміну.

7.1.1 ВИПАДОК № 17 — Оцінка ризиків, їх зменшення та зобов'язання

124. Ця справа слугує прикладом важливості попередніх заходів. Порушення, з точки зору ризику, становить високий рівень ризику[33], оскільки платіжні дані можуть містити інформацію про приватне життя суб'єкта даних (наприклад, звички, контакти) й можуть призвести до матеріальної шкоди (наприклад, переслідування, ризик для фізичної недоторканності). Персональні дані, отримані під час такої атаки, також можуть бути використані для полегшення заволодіння обліковими записами в цій організації або зловживання подальшими заходами автентифікації в інших організаціях. З огляду на ці ризики, «належні» заходи автентифікації повинні відповідати високому рівню, залежно від того, які персональні дані можуть оброблятися в результаті автентифікації.

125. Як наслідок, від контролера вимагається як повідомлення НО, так і суб'єкту даних.

126. Процес попередньої верифікації клієнта, очевидно, повинен бути вдосконалений у світлі цього випадку. Методи, використані для автентифікації, були недостатніми. Зловмисник зміг видати себе за певного користувача, використовуючи загальнодоступну інформацію та інформацію, до якої він мав доступ в інший спосіб.

127. Не рекомендується використовувати цей тип статичної автентифікації на основі знань (коли відповідь не змінюється і коли інформація не є «конфіденційною», як у випадку з паролем).

128. Замість цього організація повинна використовувати таку форму автентифікації, яка забезпечить високий ступінь впевненості в тому, що автентифікований користувач є саме тією особою, а не кимось іншим. Впровадження позасмугового методу багатофакторної автентифікації вирішило б цю проблему, наприклад, для перевірки запиту на зміну, надсилаючи запит на підтвердження колишньому контакту; або додаючи додаткові запитання та вимагаючи інформацію, яку можна було побачити лише на попередніх рахунках. Рішення про те, які заходи запровадити, має приймати контролер, оскільки він найкраще знає деталі та вимоги своєї внутрішньої роботи.

---

[33] Вказівки щодо операцій з обробки даних, які *«можуть призвести до високого ризику»*, див. у виносці 10 вище.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	✓	✓

7.2 ВИПАДОК № 18: Перехоплення електронної пошти

Мережа гіпермаркетів виявила, що через 3 місяці після конфігурації деякі електронні поштові скриньки були змінені та створені правила, згідно з якими кожен електронний лист, що містить певні вирази (наприклад, «рахунок-фактура», «платіж», «банківський переказ», «автентифікація кредитної картки», «реквізити банківського рахунку»), переміщувався до невикористовуваної папки, а також перенаправлявся на зовнішню адресу електронної пошти. Крім того, на той час вже була проведена атака соціальної інженерії, тобто зловмисник, який видавав себе за постачальника, змінив реквізити банківського рахунку цього постачальника на свої власні. Зрештою, на той час було надіслано кілька фальшивих рахунків-фактур, які містили нові реквізити банківського рахунку. Система моніторингу поштової платформи зрештою видала попередження щодо папок. Компанія не змогла з'ясувати, як зловмисник отримав доступ до поштових скриньок, але припустила, що заражений електронний лист надав доступ до групи користувачів, відповідальних за платежі, і це призвело до того, що зловмисник отримав доступ до цих скриньок.

Завдяки пересиланню електронних листів на основі ключових слів зловмисник отримав інформацію про 99 працівників: ім'я та заробітну плату за певний місяць щодо 89 суб'єктів даних; ім'я, цивільний стан, кількість дітей, заробітну плату, робочі години та решту інформації про отримання заробітної плати 10 працівників, з якими закінчилися договори. Контролер повідомив лише 10 працівників, що належать до останньої групи.

7.2.1 ВИПАДОК № 18 — Оцінка ризиків, їх зменшення та зобов'язання

129. Навіть якщо зловмисник, ймовірно, не мав на меті збір персональних даних, оскільки порушення може призвести як до матеріальної (наприклад, фінансових збитків), так і до моральної шкоди (наприклад, крадіжки особистих даних або шахрайства), або дані можуть бути використані для полегшення інших атак (наприклад, фішингу), витік персональних даних, ймовірно, призведе до високого ризику для прав і свобод фізичних осіб. Тому про порушення слід повідомити всіх 99 працівників, а не лише 10 працівників, інформація про заробітну плату яких була витоком.

130. Дізнавшись про порушення, контролер примусово змінив пароль для скомпрометованих облікових записів, заблокував надсилання електронних листів на електронну скриньку зловмисника, повідомив постачальника послуг електронної пошти, якою користувався зловмисник, про його дії, видалив правила, встановлені зловмисником, і вдосконалив сповіщення системи моніторингу, щоб вони надсилали сповіщення, як тільки створюється автоматичне правило. Крім того, контролер може позбавити користувачів права встановлювати правила переадресації, доручивши ІТ-службі робити це лише за запитом, або запровадити політику, згідно з якою користувачі повинні перевіряти та звітувати про правила, встановлені для їхніх облікових записів, раз на тиждень або частіше, якщо мова йде про роботу з фінансовими даними.

131. Той факт, що порушення могло статися й залишатися непоміченим протягом такого тривалого часу, а також той факт, що за довший час соціальна інженерія могла бути використана для зміни більшої кількості даних, вказує на значні проблеми в системі ІТ-безпеки контролера. Їх слід вирішити без зволікань, наприклад, приділити особливу увагу перевірці автоматизації та контролю за змінами, виявленню інцидентів та заходам реагування на них. Контролери, які обробляють конфіденційні дані,

фінансову інформацію тощо, несуть більшу відповідальність за забезпечення належного захисту даних.

Необхідні дії на основі виявлених ризиків		
Внутрішня документація	Повідомлення НО	Комунікація із суб'єктами даних
✓	✓	✓