ВІД РЕДАКЦІЙНОЇ КОЛЕГІЇ

Неофіційний переклад

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У КОМЕРЦІЙНИХ ОРГАНІЗАЦІЯХ

(за матеріалами посібника для бізнесу Федеральної торгової комісії США)

Якісний план по захисту персональних даних базується на 5 основних принципах:

1. **Здійснення інвентаризації.** Необхідно знати, які персональні дані зберігаються у ваших архівах та на комп’ютерах.
2. **Зменшення обсягів інформації, що зберігається.** Необхідно зберігати тільки те, що потрібно вам для здійснення вашого бізнесу.
3. **Зберігання інформації у захищеному від стороннього доступу місці.** Необхідно захищати інформацію, яку зберігаєте.
4. **Видалення даних**. Необхідно ретельно ліквідувати те, що вам більше не потрібно.
5. **Попереднє планування.** Необхідно створити план реагування на випадки порушення безпеки даних.

Стаття 1. Здійснення інвентаризації

Ефективний захист даних починається з оцінки того, яку інформацію ви маєте, і з визначення того, хто має доступ до неї. Розуміння того, як персональні дані потрапляють до компанії, як переміщується всередині і як виходять з неї, а також, хто має або може мати доступ до них, є важливим для оцінки слабких місць в системі захисту даних. Тільки після дослідження, як персональні дані переміщуються, можливо визначити спосіби для їх захисту.

1. Інвентаризуйте всі комп’ютери, ноутбуки, флеш-диски, диски, домашні комп’ютери та інше обладнання для того, щоб визначити, чи зберігає ваша компанія конфіденційні дані. Також необхідно здійснити структурування даних, якими ви володієте, за типом та місцезнаходженням: файли з даними і комп’ютерні системи є основними носіями даних або ваша компанія отримує персональні дані багатьма способами – через веб-сайти, від підрядників, через кол-центри і тому подібне. Щодо даних, які зберігаються на ноутбуках, домашніх комп’ютерах персоналу та флеш-дисках, інвентаризація буде вважатися закінченою тільки після того, як буде перевірено всі конфіденційні дані, що повинні зберігатися.

2. Відслідковуйте персональні дані у вашій компанії шляхом розмов з відділами продаж, персоналом з відділу інформаційних технологій, відділом кадрів, бухгалтерією і іншими відділами, що надають послуги. Отримайте повну картину щодо того:

(a) Хто відправляє конфіденційні персональні дані у вашу компанію – чи отримуєте ви її від клієнтів?; компаній, що займаються кредитними картками?; банків чи інших фінансових інститутів?; кредитних бюро?; інших компаній?

(b) Як ваша компанію отримує персональні дані – вони потрапляють через: веб-сайти?; електронну пошту?; пошту?, передаються через касові апарати в магазинах?

(c) Який вид інформації ви отримуєте на кожній вхідній точці – чи отримуєте ви інформацію щодо кредитних карток через Інтернет?; чи зберігає ваш бухгалтерський відділ інформацію про рахунки клієнтів до запитання?

(d) Де ви зберігаєте інформацію, що отримуєте на кожній вхідній точці – чи це централізована електронна база даних на індивідуальних ноутбуках, на дисках чи дискетах, в папках, філіях?; Чи знаходяться будь-які файли з даними вдома у співробітників?

(e) Хто має або може мати доступ до даних – хто з працівників має дозвіл на доступ до даних?; чи може хтось ще отримати його?; як щодо компаній, які встановлюють та оновлюють програмне забезпечення, яке ви використовуєте обробки даних з кредитними картками?

3. Різні види даних – різні ризики. Звертайте особливу увагу на те, як ви зберігаєте дані, що ідентифікують особу: номери соціального захисту, інформацію щодо кредитних карт, фінансову інформацію та інші конфіденційні дані. Це те, що злодії використовують найчастіше для того, щоб здійснити шахрайство чи крадіжку.

Стаття 2. Зменшення обсягів інформації, що зберігається

Якщо для вашого бізнесу не має необхідності в силу дії законодавства у зберіганні персональних даних, не зберігайте їх. А краще, не збирайте їх. Якщо ж в силу дії законодавства для вашого бізнесу вам необхідні певні конфіденційні персональні дані, зберігайте їх тільки до тих пір, допоки вони вам необхідні.

1. Використовуйте номери соціального захисту тільки для необхідних та законних цілей, наприклад, для звітів про податки із сум, що виплачуються найманим працівникам.

2. Закон вимагає від вас скоротити чеки по кредитних та дебетних картках, які надаються в електронному вигляді вашим клієнтам. Ви можете включити не більше ніж п’ять останніх значень картки, і повинні видалити дату закінчення.

3. Не зберігайте дані щодо кредитних карток клієнтів, якщо ці дані не потрібні для вашого бізнесу. Наприклад, не зберігайте номер рахунку та дату закінчення, якщо не маєте суттєвої потреби для зберігання таких даних. Зберігання такої інформації, або зберігання її довше ніж це необхідно – підвищує ризик того, що дані можуть бути використані завдяки крадіжчі чи шахрайству.

4. Перевіряйте стандартні налаштування вашого програмного забезпечення, яке зчитує номери кредитних карток клієнтів і обробляє трансакції. Іноді воно налаштоване на постійне зберігання даних. Змініть стандартні налаштування, для того щоб впевнитись, що ви не зберігаєте дані, які вам не потрібні.

5. Якщо необхідно зберігати дані для вашого бізнесу або у силу дії законодавства, розробіть задокументовану політику такого зберігання для того, щоб визначити, які дані повинні зберігатися, як захистити їх, як довго їх зберігати і як розпорядитись ними, забезпечуючи безпеку таких даних, коли вони вам більше не потрібні.

Стаття 3. Зберігання інформації у захищеному від стороннього доступу місці

Який найкращий спосіб захисту конфіденційних персональних даних, які необхідно зберігати? Це залежить від виду даних та того, як вони зберігаються. Найбільш ефективні плани зберігання даних базуються на ключових елементах: фізична безпека, електронна безпека, навчання персоналу та практика щодо безпеки підрядників та постачальників послуг.

3.1. Фізична безпека

1. Зберігайте паперові документи чи файли, а також CD-диски, жорсткі диски, зіп-драйвери, касети і резервні копії, що містять персональні дані, в кімнатах, що закриваються на замок, або в закритих на замок папках. Обмежте доступ співробітників тільки доступом для законних цілей необхідних для бізнесу. Контролюйте, хто має ключі і їх кількість.

2. Вимагайте щоб файли, які містять конфіденційні персональні дані, зберігалися в папках, закритих на замок, коли найманий працівник працює з файлом. Нагадуйте працівникам не залишати конфіденційні документи на столах, після того як вони залишають свої місця.

3. Вимагайте від найманих працівників класти документи на місце, виключати їх комп’ютери і закривати їх папки з файлами і офісні двері по закінченню робочого дня.

4. Впроваджуйте необхідний контроль за доступом до будівлі вашої компанії. Розказуйте найманим працівникам, що робити і кому дзвонити, якщо вони бачать незнайому особу.

5. Якщо є склади, обмежте доступ найманих працівників тільки доступом у законних цілях, необхідних для бізнесу. Відслідковуйте, хто і коли має доступ до даних, що зберігаються на складі.

6. Якщо ви пересилаєте конфіденційну інформацію, використовуючи зовнішніх кур’єрів чи підрядників, зашифруйте дані і сформуйте перелік даних, що пересилаються.

3.2. Електронна безпека

Безпека комп’ютера є не тільки справою персоналу відділу інформаційних технологій. Ви повинні чітко розуміти вразливість вашої комп’ютерної системи і слідувати порадам експертів у цій сфері.

3.2.1. Загальна безпека інформаційної мережі

1. Визначте комп’ютери чи сервери, де зберігаються персональні дані.

2. Визначте всі можливості підключення до комп’ютерів, де зберігаються персональні дані. Це може бути Інтернет, електронні касові апарати, комп’ютери у ваших філіях, комп’ютери, що використовуються вашими постачальниками послуг з підтримкою вашої інформаційної мережі, і безпровідні пристрої, наприклад, сотові телефони.

3. Оцініть слабкі місця для загальновідомих та обґрунтованопередбачуваних нападів під час кожного підключення.

4. Не зберігайте конфіденційні персональні дані на будь-якому комп’ютері, що підключений до Інтернету, окрім випадку, якщо це необхідно для ведення бізнесу.

5. Зашифровуйте конфіденційні дані, які ви надсилаєте іншим особам по загальній мережі (Інтернет), і відслідковуйте зашифровані конфіденційні дані, що зберігаються у вашій мережі або на дисках чи портативних пристроях зберігання даних. Відслідковуйте відправки електронної почти в рамках вашої бізнес-діяльності, якщо вони містять конфіденційні персональні дані.

6. Регулярно встановлюйте сучасні антивірусні програми на персональних комп’ютерах і серверах вашої мережі.

7. Регулярно перевіряйте спеціалізовані веб-сайти і сайти ваших продавців програмного забезпечення на предмет наявності нових версій і впроваджуйте політику встановлення оновлень, що затверджені продавцями.

8. Перевіряйте комп’ютери вашої мережі на предмет визначення робочих систем та робочих послуг мережі. Якщо ви знайдете програми, які вам не потрібні, деактивуйте їх, щоб запобігти потенційним проблемам щодо безпеки. Наприклад, у разі якщо електронна пошта чи Інтернет не потрібен на конкретному комп’ютері, розгляньте можливість закриття портів для таких послуг на цьому комп’ютері для того, щоб запобігти неавторизованому доступу до цього комп’ютера.

9. Коли ви отримуєте дані щодо переказів по кредитних карткам і інші фінансові конфіденційні дані, використовуйте Протокол захищених сокетів[1] або інші види безпечного зв’язку, які захищають дані під час відправки.

10. Звертайте особливу увагу на безпеку ваших Інтернет-додатків – програмного забезпечення, що використовується для того, щоб надати дані відвідувачам вашої веб-сторінки і для отримання даних від них. Інтернет-додатки можуть частково бути пошкоджені хакерськими нападами. Під назвою “напад шляхом ін’єкції” хакери встановлюють команди, які націлені на зловмисні дії, що виглядають як законний запит даних. При цьому хакери у вашій системі пересилають конфіденційні дані з вашої мережі на їх комп’ютери. Відносно легкий захист від таких нападів доступний з багатьох ресурсів.

3.2.2. Управління паролями

1. Контролюйте доступ до конфіденційних даних шляхом встановлення вимоги до найманих працівників використання “сильних” паролів. Експерти з технічної безпеки кажуть, що чим довший пароль, тим це краще. Так як легкі паролі, такі як часто вживані слова, можна легко вгадати, вимагайте, щоб наймані працівники вибирали паролі, які міститимуть літери, числа і символи. Вимагайте, щоб логін та пароль найманого працівника були різними і часто змінювалися.

2. Пояснюйте працівникам, чому надання будь-кому свого паролю або його запис будь-де за межами робочого приміщення є дією проти компанії.

3. Використовуйте програму захисту екрану, яка автоматично виключає комп’ютер найманого співробітника після певного періоду неактивності.

4. Відключайте користувачів, які ввели неправильний пароль певну кількість разів.

5. Попереджайте найманих працівників про можливі крадіжки персональної інформації шляхом представлення як персонал відділу інформаційних технологій вашої компанії і запиту ваших паролів. Повідомляйте працівникам, що запит їх паролю являється незаконною дією і що не в кого не повинні вимагати розкриття їх паролю.

6. При інсталяції нового програмного забезпечення одразу ж змініть стандартні паролі продавців або постачальників на більш безпечні і надійні паролі.

7. Застерігайте найманих працівників відправляти конфіденційні персональні дані (номери соціального захисту, паролі, дані щодо рахунків) електронною поштою. Незашифровані електронні листи не є безпечним способом відправки даних.

3.2.3. Безпека ноутбуків

1. Обмежуйте використання ноутбуків тільки тими найманими працівниками, які потребують їх для виконання їх роботи.

2. Оцініть, чи потрібно конфіденційні дані дійсно зберігати на ноутбуці. Якщо ні, видаліть їх спеціальною програмою з очистки інформації. Видалити файли,

[1] Протокол, що гарантує безпечну передачу даних через мережу, комбінуючи криптографічну систему з відкритим ключем і блочне шифрування даних.

використовуючи стандартні команди, недостатньо, тому що дані можуть залишитися на жорсткому диску ноутбуку. Програми з очистки інформації можливо придбати в більшості спеціалізованих магазинах.

3. Вимагайте від найманих працівників збереження ноутбуків у безпечних місцях.

4. Розгляньте можливість дозволити користувачам ноутбуків мати тільки доступ до конфіденційних даних, а не зберігати дані на ноутбуках. Дані провинні зберігатися на безпечних головних комп’ютерах, ноут-буки повинні використовуватися тільки як пристрої, що відображають дані з головного комп’ютера, але не зберігають їх. Інформація може бути також захищена шляхом використання е-токенів, смарт-карт, засобів зчитування відбитків пальців та тощо, а також паролів для доступу до головного комп’ютера.

5. Якщо ноутбук містить конфіденційні дані, шифруйте та кодируйтє їх так, щоб користувачі не могли завантажити будь-яке програмне забезпечення або змінити налаштування щодо захисту без погодження спеціалістів відділу програмного забезпечення вашої компанії. Розгляньте можливість використання автоматично функції знищення для того, щоб дані на комп’ютері, які було викрадено, були знищені, як тільки грабіжник намагатиметься використовувати їх в Інтернеті.

6. Навчайте найманих працівників дотримуватися безпеки даних під час подорожі. Вони ніколи не повинні залишали ноутбуки в машинах на видноті, в місцях для багажу в готелях або здавати в багаж, якщо тільки це не вимагається безпекою аеропорту. Якщо необхідно залишити ноутбук в машині, його потрібно зачинити в багажнику. Кожен, хто проходить через безпеку аеропорту, повинен слідкувати за своїм ноутбуком.

3.2.4. Захисна система

1. Використовуйте захисні системи для того, щоб захистити ваш комп’ютер від нападів хакерів, якщо він підключений до Інтернету. Захисні системи є програмним забезпеченням або обладнанням, яке розроблено для того щоб блокувати входження хакерів на ваш комп’ютер. Належним чином налаштована захисна система зробить важчим можливість хакерів знайти ваш комп’ютер та ввійти у ваші програми та файли.

2. Визначте, чи необхідно вам встановлення “обмеженої” захисної системи під час підключення до Інтернету. “Обмежена” захисна система відділяє вашу локальну мережу від Інтернету і може запобігти нападам шляхом спроб увійти в комп’ютер у мережі, де ви зберігаєте конфіденційні дані. Встановіть “контроль за входом” – налаштування, що визначають, хто пройшов через захисні системи і що вони бажають побачити – для того щоб дати можливість заходити до мережі тільки тим найманим працівникам, до яких є довіра і їм необхідний такий доступ для законних потреб вашого бізнесу.

3. Якщо деякі комп’ютери вашої мережі зберігають конфіденційні дані, а інші не зберігають, розгляньте можливість використання додаткових захисних систем для того, щоб захистити комп’ютери з конфіденційними даними.

3.2.5. Бездротовий та дистанційних доступ

1. Визначте, чи використовуєте ви бездротові пристрої, такі як сканери або сотові телефони, що підключені до вашої комп’ютерної мережі або якими передаються персональні дані.

2. Якщо ви використовуєте бездротові пристрої, розгляньте можливість їх обмеженого підключення до вашої комп’ютерної мережі. Шляхом обмеження

бездротових пристроїв, що можуть підключатися до вашої мережі, ви зробите доступ незнайомців до мережі важчим.

3. Для того щоб ускладнити для незнайомців можливість читати вміст конфіденційних документів, розгляньте можливість шифрування даних. Зашифровані передачі даних з бездротових пристроїв на вашу комп’ютерну мережу можуть запобігти доступу шляхом так званого “спуфінгу” – імітування одного з ваших комп’ютерів з ціллю отримання доступу до вашої мережі.

4. Розгляньте можливість використання шифрування, якщо вам необхідний дистанційних вхід до вашої комп’ютерної мережі найманими працівниками або постачальниками послуг, такими як компанії, що виявляють неполадки та оновлюють програмне забезпечення, що ви використовуєте для того, щоб обробляти покупки до кредитних картках.

3.2.6. Виявлення порушень

1. Якщо трапляються порушення в роботі мережі розгляньте можливість використання систем, що визначають такі порушення. Для їх ефективності вони потребують частого оновлення для того щоб бути націленими на нові типи хакерства.

2. Підтримуйте центральні реєстраційні файли конфіденційної інформації з ціллю перевірки діяльності в вашій мережі для відслідковування та вчасного реагування на напади. Якщо на вашу мережу здійснено напад, в такому файлі будуть міститися дані про комп’ютери, яким загрожує ризик.

3. Перевіряйте вхідний трафік, який хтось намагається підвергнути нападу хакерів. Слідкуйте за діяльністю нових користувачів, кількістю спроб невідомих користувачів або комп’ютерів увійти в систему, а також більш високим та більшим, ніж середній трафіком у незвичний для цього час доби.

4. Перевіряйте вихідній трафік з ціллю відслідковування порушень захисту персональних даних. Звертайте увагу на занадто великі розміри даних, що передаються з вашої системи до невідомих користувачів. Якщо велика кількість даних передається з вашої мережі, впевніться, що така передача здійснена на законних підставах.

5. У відповідь на порушення захисту даних вам необхідно мати і впроваджувати план дій.

3.3. Навчання персоналу

Ваш план по захисту персональних даних може виглядати дуже гарним на папері, але він буде настільки сильним, наскільки сильний персонал, що впроваджує його. Виділіть час для того щоб пояснити правила вашому персоналу і навчити їх виявляти слабкі місця в безпеці даних. Періодичні тренінги підкреслюють важливість практичного застосування захисту даних. Добре навчена робоча сила являється найкращим захистом проти порушень захисту даних.

1. Перевіряйте біографію перед тим, як наймати працівників, які матимуть доступ до конфіденційних даних.

2. Вимагайте від кожного з ваших нових працівників підписання договору щодо дотримання стандартів конфіденційності та безпеки даних. Впевніться, що вони розуміють, що дотримання плану захисту даних вашої компанії є суттєвою частиною їх обов’язків. Регулярно нагадуйте працівникам про політику вашої компанії та будь-які законодавчі вимоги зберігання інформації про клієнтів у захищеному місці.

3. Майте інформацію щодо того, хто з працівників має доступ до конфіденційних персональних даних клієнтів. Звертайте особливу увагу на такі дані, як номери соціального захисту та номери рахунків. Обмежуйте доступ до персональних даних працівників, що мають необхідність доступу до конфіденційної інформації.

4. Ваша компанія повинна мати процедури, які забезпечуватимуть, щоб працівники, які звільняються або переходять до іншого підрозділу вашої компанії, не мали доступу до конфіденційної інформації. Обмежуйте термін дії їх паролів, зберігайте в безпечному місці ключі та індентифікаційні карти як частину звичайного режиму перевірки.

5. Розповідайте працівникам про політику компанії стосовно дотримання безпеки та конфіденційності даних. Впевніться, що ваша політика донесена до працівників, що мають доступ до конфіденційних даних з дому чи іншого місця.

6. Попереджайте працівників про телефонний фішинг[2]. Навчайте їх бути обережними з незнайомими людьми, що телефонують, вимагають номер рахунку для оброблення замовлення або які запитують контактні дані клієнтів чи співробітників. Зробіть стандартною практикою подвійну перевірку шляхом контакту з компанією, що використовує номер телефону, який ви знаєте.

7. Вимагайте, щоб працівники повідомляли вам негайно, якщо є небезпека порушення захисту даних, наприклад, втрата чи крадіжка ноутбуку.

8. Впровадьте дисциплінарне покарання за порушення заходів безпеки.

3.4. Практика щодо безпеки підрядників та постачальників послуг

Практика вашої компанії щодо безпеки даних залежить від людей, які впроваджують її, включаючи підрядників та постачальників послуг.

1. Перед тим як ви передасте аутсайдерам будь-які функції вашого бізнесу (веб-хостинг, клієнтські кол-центри, обробка даних), вивчіть практику захисту даних компанії і порівняйте з вашими стандартами.

2. Під час укладання контрактів з вашими постачальниками послуг звертайте увагу на положення щодо безпеки даних в таких контрактах.

3. Вимагайте, щоб ваші постачальники послуг повідомляли вам про кожний випадок порушення безпеки, що стався, навіть якщо такий випадок не завдав фактичної шкоди.

Стаття 4. Видалення даних

Те, що для вас купа сміття, може бути золотою знахідкою для грабіжника даних. Залишення рахунків по кредитних картках або паперів чи дисків з персональними даними в ящику для сміття посилює можливість вчинення злочину і піддає клієнтів ризику викрадення їх персональних даних. Шляхом правильного використання конфіденційних даних ви забезпечуєте, щоб їх не було прочитано чи відновлено.

1. Впроваджуйте практику щодо розкриття інформації, яка необхідна для того, щоб запобігти несанкціонованому доступу до персональних даних або їх використанню.

2. Ефективно знищуйте паперові записи, використовуючи спеціальне обладнання для подрібнення паперу, спалюючи їх та інше. Зробіть так, щоб обладнання для подрібнення паперу було доступне на робочих місцях.

3. При ліквідації старих комп’ютерів та засобів зберігання даних використовуйте сервісні програми для стирання даних. Вони недорогі та більш результативні при

[2] Різновид Інтернет-шахрайства, вивужування інформації, що дає змогу здійснити викрадення персональних даних.

перезапису жорсткого диску, здійснюючи це таким чином, щоб файли неможливо було більше відновити. Видалення файлів, використовуючи клавіатуру або команди миші, як правило неефективне тому, що файли можуть продовжувати існування на комп’ютерному жорсткому диску і можуть були легко відновлені.

4. Впевніться, що наймані працівники, які працюють вдома, дотримуються тих же процедур по ліквідації конфіденційних документів і даних, що зберігаються на старих комп’ютерах та портативних засобах зберігання даних.

5. Якщо використовуєте кредитну історію клієнтів для цілей вашої діяльності, на вас поширюються правила щодо ліквідації даних Федеральної торгової комісії.

Стаття 5. Попереднє планування

Здійснення заходів по захисту даних, що знаходяться у вашому розпорядженні, з метою запобігання порушенням системи безпеки може зайняти довгий період часу. Тим не менш, порушення можуть траплятися. Вищенаведеними способами ви можете зменшити такий вплив на вашу діяльність, ваших найманих працівників та ваших клієнтів:

1. З ціллю реагування на випадки порушення безпеки майте відповідний план реагування. Призначте одного з ваших співробітників головним по координації і впровадженню відповідного плану.

2. Якщо до вашого комп’ютера було здійснено несанкціонований доступ, відключіть його негайно від Інтернету.

3. Одразу ж розслідуйте випадки порушення безпеки та вживайте необхідних заходів блокування слабких місць в системі захисту даних або загроз безпеці персональних даних.

4. Визначтесь, кого потрібно повідомити, як всередині вашої організації, так і зовнішні інстанції, якщо трапився випадок порушення безпеки даних. Можливо, вам необхідно буде повідомити покупців, правоохоронні органи, клієнтів, кредитні бюро та інші компанії, на яких може вплинути таке порушення. Окрім того, багато регулюючих органів держав та федеральних банків мають закони або посібники щодо порушення захисту даних.

Переклад з англ. – Віри Брижко.
Режим доступу: *//www.ftc.gov/bcp/edu/pubs /business/ idtheft/bus69.pdf*