УДК 004.056

Іващенко Д.О., Данилов А.Д.

АНАЛІЗ МЕТОДІВ НЕЗАКОННОГО ВИЛУЧЕННЯ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Робота присвячена захисту інформації та інформаційних активів. В тезах доповіді наведено результати аналізу методів незаконного вилучення та захисту інформації, надані загальні рекомендації щодо використання методів захисту від втрати або пошкодження інформаційних активів.

В сучасному світі, де інформаційні технології є невід'ємною частиною нашого життя, захист інформації стає все більш важливим завданням. Незаконне вилучення інформації може призвести до серйозних наслідків, таких як порушення конфіденційності, цілісності та доступності даних.

З кожним роком збільшується кількість злочинів, пов'язаних з кібербезпекою.

Зокрема, зловмисники застосовують різноманітні методи незаконного вилучення інформації, такі як фішинг, кібератаки, розповсюдження шкідливих програм тощо. Ці злочинні дії можуть призвести до значних фінансових втрат, порушення конфіденційності та приватності даних, а також вплинути на репутацію компаній та організацій.

Незаконне вилучення інформації є серйозною загрозою для конфіденційності, цілісності та доступності даних. Конфіденційні дані, такі як особисті дані або комерційна інформація, можуть бути вилучені і використані для злочинних цілей, таких як шахрайство, вимагання викупу або крадіжка особистої інформації. Цілісність даних також може бути порушена, якщо зловмисники вносять небажані зміни до даних або використовують методи шифрування для блокування доступу до даних власникам. Крім того, доступність даних може бути обмежена, якщо зловмисники використовують методи Denial of Service або інші методи атак на мережу, щоб перевантажити систему і заблокувати доступ до даних.

Основні методи незаконного вилучення інформації включають:

1. Фішинг – це метод, при якому злочинці використовують підроблені електронні листи або веб-сайти, щоб отримати доступ до конфіденційної інформації, такої як паролі, номери кредитних карток, паспортні дані і т.д.

2. Віруси та троянські програми – це програми, які можуть використовуватись для вилучення конфіденційної інформації з комп'ютерів без дозволу власника. Віруси можуть поширюватись через електронну пошту, соціальні мережі або програми, які завантажуються з Інтернету.

3. Перехоплення трафіку – це метод, при якому злочинці перехоплюють трафік мережі, щоб отримати доступ до конфіденційної інформації, яку пересилають користувачі. Цей метод може бути використаний для отримання доступу до паролів, номерів кредитних карток та іншої конфіденційної інформації.

4. Фізичний доступ до даних – це метод, при якому злочинці отримують доступ до комп'ютерів або інших пристроїв, щоб викрасти конфіденційну інформацію. Цей метод може використовуватись в офісах або інших місцях, де зберігається конфіденційна інформація.

5. Соціальна інженерія – це метод, при якому злочинці використовують соціальні навички, щоб отримати доступ до конфіденційної інформації. Наприклад, злочинець може намагатись переконати працівника компанії надати йому доступ до системи, надавши підробку ідентифікації або зламавши пароль. Також соціальна інженерія може включати в себе фішинг-атаки, коли злочинці надсилають електронні листи, які здаються легітимними, але насправді містять шкідливі посилання або додатки для вилучення інформації.

Існує кілька методів захисту від незаконного вилучення інформації, які допомагають зменшити ризики втрати даних і зберегти конфіденційність, цілісність і доступність інформації. Основні методи захисту включають:

1. Фізичні методи захисту, такі як захист приміщення з обладнанням, забезпечення фізичної безпеки пристроїв зберігання даних, контроль доступу до приміщення з серверами і іншим обладнанням.

2. Організаційні методи захисту, які включають політику безпеки, культуру безпеки, процедури, правила і інструкції, що встановлюються в компанії для забезпечення безпеки інформації. Такі методи також включають регулярні навчання працівників з питань безпеки даних та аудит безпеки даних.

3. Технічні методи захисту, які включають захист мереж, захист даних, використання сильних паролів, шифрування даних, контроль доступу і ідентифікацію користувачів.

4. Юридичні методи захисту, такі як договірні зобов'язання, які є обов'язковою умовою взаємодії між компаніями, правові засоби, що захищають права на

інтелектуальну власність та конфіденційність даних.

Існує декілька методів протидії незаконному вилученню інформації, серед яких можна виділити такі:

1. Використання комплексної системи захисту: використання технічних, організаційних та юридичних методів захисту даних.
2. Регулярні оновлення програмного забезпечення: оновлення програмного забезпечення, що дозволяють закрити вразливості та запобігти злому.
3. Використання шифрування даних: шифрування даних дозволяє зберігати інформацію в зашифрованому вигляді, що ускладнює доступ до неї для зловмисників.
4. Політика безпеки та культура безпеки: розробка та впровадження політики безпеки, яка містить вимоги щодо захисту даних, а також створення культури безпеки серед співробітників.
5. Навчання персоналу: навчання співробітників технікам безпеки та правилам користування комп'ютерною технікою та інформаційними системами.
6. Контроль доступу та ідентифікація: використання засобів контролю доступу до інформації та ідентифікації користувачів.
7. Резервне копіювання даних: регулярне створення резервних копій даних дозволяє відновити інформацію у разі її втрати або пошкодження.
8. Моніторинг та аудит безпеки: проведення моніторингу та аудиту безпеки даних для виявлення можливих загроз та вразливостей системи.

Методи незаконного вилучення інформації можуть бути дуже різноманітними і складними, тому потрібно розробляти ефективні методи протидії несанкціонованого та незаконного вилучення інформації. Для цього необхідно розуміти потенційні загрози та використовувати відповідні методи захисту даних та інформаційних активів, щоб забезпечити їхню конфіденційність, цілісність та доступність. Також важливо постійно оновлювати методи протидії відповідно до нових загроз та викликів, які постійно змінюються.