Дячук О. Ю., магістрантка,
Єфіменко А. А., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ ОСНОВНИХ МЕТОДІВ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

Інформаційна безпека та захист інформації нерозривно пов'язані. Захист інформації – це комплекс операцій для забезпечення безпеки (цілісності та секретності) під час збирання, обробки, зберігання та передачі. Безпека інформації включає конфіденційність, скритність і цілісність даних. У розширеному розумінні захист інформації – це сукупність заходів (організаційних, законодавчих, технічних), спрямованих на нівелювання потенційних небезпек та ліквідацію їхніх наслідків. Суть захисту інформаційних даних полягає у виявленні та усуненні можливих загроз, шкідливих джерел і критичних причин, що можуть пошкодити інформацію.

Основні методи захисту інформації:

1. Неформальні методи захисту.

Неформальні методи захисту інформації включають законодавчі, адміністративні та морально-етичні засоби. Законодавча база, надана державою, регулює захист даних через різноманітні законодавчі проекти та документи. Адміністративні заходи є основою для формування ефективних механізмів захисту інформаційних даних, оскільки багато загроз пов'язані з неправомірними діями осіб та порушенням посадових повноважень.

Для зниження небезпек інформаційної безпеки важливо створити стійку базу, яка об'єднає законодавчо-правові та організаційно-технічні заходи. Морально-етичні методи включають норми і правила, сформовані в суспільстві чи колективі, які, хоча не врегульовані державною правовою системою, проте гарантують збереження інформаційних даних. Порушення цих норм може призвести до втрати довіри та підриву авторитету особи чи компанії.

2. Технічні способи захисту інформації.

У захисному програмному забезпеченні немає сенсу, якщо зловмисники можуть без зусиль отримати доступ до жорстких дисків з інформацією. Тому важливо спочатку забезпечити фізичний захист для технічних пристроїв і приміщень. Це можна здійснити за допомогою віконних ґрат, дверей з кодовими замками, сигналізації та камер цілодобового відеоспостереження.

Приміщення також слід захищати від природних катаклізмів і надзвичайних подій, використовуючи пожежну сигналізацію, датчики води і диму. Фізичні засоби забезпечення інформаційної безпеки не гарантують захист від отримання доступу через мережу, проте ефективно оберігають комп'ютерне обладнання та носії інформаційних даних.

3. Програмні способи захисту інформації.

Інструментарій для захисту відомостей включає програмні компоненти для комп'ютерів, ноутбуків та серверів. Серед програмних методів захисту виділяють такі:

- Антивірусні програми для виявлення та видалення вірусів;
- Обмеження доступу до інформаційної системи через особисті кабінети та паролі;
- Віртуалізація для створення «пісочниць» для неперевірених програм;
- Міжмережні брандмауери для контролю вхідного трофіку;
- DLP-системи, що обмежують копіювання і перенос відомостей;
- SIEM-системи для відстеження підозрілих активностей.

Важливо пам'ятати, що окремі програми захищають від обмеженого числа загроз. Для максимального рівня захисту потрібна взаємодія між програмами і технічними засобами, де кожен компонент «прикриває тили» іншого.

4. Апаратні способи захисту інформації.

Апаратні технічні методи захисту інформації включають:

- Спеціалізовані генератори цифрового шуму, які шифрують дані та створюють інформаційний шум для маскування каналів зв'язку.
- Апаратні регістри паролів, що зберігають паролі і обов'язкові для доступу до інформаційних даних.
- Апаратні системи довіреного завантаження, які обмежують установку сторонніх операційних систем та програмного забезпечення для захисту даних на жорсткому диску.

Хоча апаратні методи можуть здаватися подібними до програмних, вони виявляються продуктивнішими і надійнішими, маючи підвищену стійкість перед атаками. Забезпечення максимального рівня інформаційної безпеки вимагає поєднання програмних та апаратних інструментів. Важливо віддавати перевагу сертифікованим та ліцензійним програмам для гарантії надійності, контрольованої органами держави.

5. Криптографічні способи захисту інформації.

Криптографія використовує спеціальні методи шифрування для захисту даних від змін, забезпечуючи безпеку інформації без обмеження доступу. Це дозволяє зберігати дані в зашифрованому вигляді, недоступному без відповідного криптографічного ключа.

Криптографія поділяється на чотири групи:

- Симетричні криптосистеми: Використовує один і той самий ключ для шифрування і розшифрування інформації.

- Криптосистеми з відкритим ключем: Використовують два пов’язаних ключі – відкритий і закритий – для кодування та розкодування.
- Криптосистеми на основі електронного підпису: Використовуються для підтвердження достовірності документів і авторства.
- Системи управління ключами: Взаємодіють з інформаційними даними на основі розподілу ключів між працівниками.

Криптографічні засоби застосовуються для передачі конфіденційної інформації, підтвердження автентичності, авторства та для зберігання закодованих даних на зовнішніх носіях. Це надійний метод забезпечення інформаційної безпеки.

6. Мережеві способи захисту інформації.

Для забезпечення інформаційної безпеки в комп’ютерних мережах використовують спеціалізовані програмно-технічні продукти, такі як фільтрувальні пакетні засоби, маршрутизатори та програмні шлюзи для контролю доступу. Однак основним засобом захисту від несанкціонованих атак є Firewall, який забезпечує зовнішній захист і обмежує доступ до мережі.

Firewall відбиває атаки, фільтрує вхідний трафік, обмежує доступ до ресурсів, фільтрує небажану кореспонденцію через електронну пошту. Ще один ефективний інструмент – маршрутизатор, який фільтрує пакети відомостей, обмежує доступ до певних адрес і хостів, а також контролює відправників і одержувачів.

Мережеві засоби дозволяють захищати дані як у глобальній мережі Інтернет, так і всередині корпоративних систем. Комплексний захист включає в себе організацію програмно-апаратних комплексів для забезпечення безпеки інформаційних даних на підприємстві.

7. Способи захисту інформації в Інтернеті

Для захисту інформаційного контенту компанії в Інтернеті потрібно розробити внутрішній документ, що визначає види інформації, етапи отримання дозволу на її розміщення, місце та доступність для різних категорій користувачів. Важливо розділити інформацію на конфіденційну та загальну, забезпечуючи захист корпоративних даних.

Забезпечення інформаційної безпеки включає захист конфіденційних корпоративних даних. Важливо встановити різні рівні доступу для співробітників та визначити, яка інформація доступна для загального використання.

При наявності веб-сайту слід обдумати рівні доступу до збережених відомостей. Рекомендується розділити співробітників на групи та надавати відповідний рівень доступу, зокрема для вищого адміністративного апарату, керівників підрозділів та пересічних фахівців.

Для клієнтів важливо розміщувати відкриту інформацію про вартість товарів і послуг, знижки та акції. Якщо необхідно обмежити доступ конкурентам, ці дані можуть бачити лише зареєстровані користувачі.

У підсумку, можна визначити, що забезпечення інформаційної безпеки в сучасному цифровому середовищі є надзвичайно складним завданням, яке вимагає комплексного підходу та поєднання різноманітних програмних і технічних засобів захисту. Успішна імплементація заходів із забезпечення безпеки включає в себе не лише застосування передових технологій, але й врахування законодавчих, адміністративних та морально-етичних аспектів.

Таким чином, сучасний підхід до забезпечення інформаційної безпеки передбачає використання широкого арсеналу інструментів, які взаємодіють між собою для створення повноцінної та надійної системи захисту. Поєднання апаратних методів зі спеціалізованими програмними компонентами стає запорукою найвищого рівня інформаційної безпеки, враховуючи різноманітні вектори загроз і високий рівень вимог до збереження конфіденційності та цілісності даних.

Список використаної літератури

1. E. Knipp et al., Managing Cisco Network Security. Elsevier Inc., 2002
2. S. Wilkins, T. Smith CCNP Security. SECURE 642-637 Official Cert Guide. Cisco Press, 2011
3. A. D wankhade and P. N. Dr Chatur Comparison of Firewall and Intrusion Detection System, Int. J. Comput. Sci. Inf. Technol.
vol. 5, no 1. 674-678 pp., 2014, URL: http://ijcsit.com/docs/
Volume 5/vol5issue01/ijcsit20140501145.pdf/.