широко використовувати в роботі онлайн-проекти, здатні поліпшити систему протидії злочинності.

Список бібліографічних посилань

1. Law enforcement credits genetic genealogy in 1987 cold case arrest // The Monroe monitor & Valley news. May 18, 2018. URL: https://t/co/E1rsWpEANj (дата звернення: 26.10.2018).

2. Romano A. DNA profiles from ancestry websites helped identify the Golden State Killer suspect // VOX. Apr 27, 2018, 5:20pm EDT. URL: https://www.vox.com/2018/4/27/17290288/golden-state-killer-joseph-james-deangelo-dna-profile-match (дата звернення: 26.10.2018).

Одержано 26.10.2018

УДК 004.056.8

Вадим Андрійович БОКОВ,
слухач магістратури факультету № 6
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-0512-725X

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД МЕРЕЖЕВОГО НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Захист інформації в сучасних реаліях перебуває на першому місці, через велику кількість загроз несанкціонованого доступу до неї.

В рамках чинного кримінального законодавства під несанкціонованим доступом необхідно розуміти: проникнення до комп'ютерів, їх систем чи мереж і вчинення дій, які змінюють режим роботи машини, її системи чи комп'ютерної мережі, або ж повністю чи частково припиняють їх роботу, без дозволу (згоди) відповідного власника або уповноважених ним осіб, а також вплив на роботу автоматизованих ЕОМ за допомогою різних технічних пристроїв, здатних зашкодити роботі машини.

Загально прийнятими методами захисту інформації є установка перешкоди, системи управління доступом, та авжеж, маскування інформації. Зупинимося більш детально на визначених методах захисту інформації.

Найбільш розповсюдженим є метод встановлення перешкоди – це метод фізичного перегородження шляху зловмиснику до інформації, що захищається, у тому числі для попередження спроб з використанням технічних засобів знімання інформації і дії на неї.

Управління доступом, як метод захисту інформації передбачає регулювання використовування всіх інформаційних ресурсів, у тому числі автоматизованої інформаційної системи підприємства. Управління доступом включає наступні функції захисту:

– ідентифікацію користувачів, персоналу і ресурсів інформаційної системи (привласнення кожному об'єкту персонального ідентифікатора);

– аутентифікацію (встановлення автентичності) об'єкту або суб'єкта по пред'явленому їм ідентифікатору;

– перевірку повноважень (перевірка відповідності дня тижня, часу доби, запрошуваних ресурсів і процедур встановленому регламенту);

– дозвіл і створення умов роботи в межах встановленого регламенту;

– реєстрацію (протоколювання) звернень до ресурсів, що захищаються;

– реагування (сигналізація, відключення, затримка робіт, відмова в запиті) при спробах несанкціонованих дій.

Маскування – метод захисту інформації з використанням інженерних, технічних засобів, а також шляхом криптографічного закриття інформації.

Скремблери – програмне або апаратне забезпечення, яке використовується у процессі скремблювання (шифрування), являє собою зворотній процес перетворення цифрового потоку без зміни швидкості передачі, з метою отримання якостей випадкової послідовності.

Вокодери – пристрої, що передають мову в цифровому вигляді і зашифрованому. Даний інструмент, призначений для аналізу та синтезу звуків та мовлення. Початково був винайдений як кодифікатор мови для телекомунікацій в 1930-х роках. Вокодер призначався для забезпечення надійного радіозв'язку — голос відцифровувався, кодувався і передавався вузькосмуговим голосовим каналом.

Методи захисту інформації на практиці реалізуються із застосуванням засобів захисту.

Захист від несанкціонованого доступу може здійснюватися в різних складових інформаційної системи:

1. Прикладне й системне програмне забезпечення.
2. Апаратна частина серверів і робочих станцій.
3. Комунікаційне устаткування й канали зв'язку.
4. Периметр інформаційної системи.

Для захисту інформації на рівні прикладного й системного програмного забезпечення використовуються:

– системи розмежування доступу до інформації;

– системи ідентифікації й аутентифікації;

– системи аудиту й моніторингу;

– системи антивірусного захисту.

Для захисту інформації на рівні апаратного забезпечення використовуються:

– апаратні ключі;

– системи сигналізації;

– засоби блокування пристроїв і інтерфейсів вводу-виводу інформації.

У комунікаційних системах використовуються наступні засоби мережевого захисту інформації:

– міжмережеві екрани (Firewall) – для блокування атак із зовнішнього середовища (Casio PIX Firewall, Symantec Enterprise FirewallTM, Alteon Switched Firewall). Вони управляють проходженням мережевого трафіка відповідно до правил (policies) безпеки. Як правило, міжмережеві екрани встановлюються на вході мережі й розділяють внутрішні (частки) і зовнішні (загального доступу) мережі;

– системи виявлення вторгнень (IDS – Intrusion Detection System) – для виявлення спроб несанкціонованого доступу як ззовні, так і усередині мережі, захисту від атак типу «відмова в обслуговуванні» (Cisco Secure IDS, Intruder Alert і NetProwel від компанії Symantec. Дані системи здатні запобігти шкідливим діям, що дозволяє знизити час простою в результаті атаки та витрати на підтримку працездатності мережі;

– засоби створення віртуальних приватних мереж (VPN – Virtual Private Network) – для організації захищених каналів передачі даних через незахищене середовище (Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator. Віртуальні приватні мережі забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації шляхом її динамічного шифрування;

– засоби аналізу захищеності – для аналізу захищеності корпоративної мережі й виявлення можливих каналів реалізації погроз інформації (Symantec Enterprise Security Manager, Symantec NetRecon). Їхнє застосування дозволяє запобігти можливим атакам на корпоративну мережу, оптимізувати витрати на захист інформації й контролювати поточний стан захищеності мережі.

Для захисту периметра інформаційної системи створюються:

– системи охоронної й пожежної сигналізації;

– системи цифрового відеоспостереження;

– системи контролю й керування доступом (СККД).

Засоби, призначені для захисту інформації. Ці засоби не призначені для безпосередньої обробки, зберігання, накопичення і

передачі інформації, що захищається, але що знаходяться в одному приміщенні з ними.

Діляться на:

– пасивні – фізичні (інженерні) засоби, технічні засоби виявлення, ПС, СЬКУД, ВН, прилади контролю радіоефіру, ліній зв'язку і т.п.;

– активні – джерела безперебійного живлення, шумогенератори, скремблери, пристрої відключення лінії зв'язку, програмно-апаратні засоби маскування інформації та ін.

Засоби, призначені для безпосередньої обробки, зберігання, накопичення і передачі інформації, що захищається, виготовлені в захищеному виконанні.

Засоби, призначені для контролю ефективності захисту інформації.

Пасивні засоби захисту акустичного і віброакустичного каналів просочування мовної інформації.

Для запобігання просочування мовної інформації по акустичному і віброакустичному каналам здійснюються заходи щодо виявлення каналів витоку. В більшості випадків для несанкціонованого знімання інформації з приміщення супротивник застосовує відповідні заставні пристрої.

Висновок: В роботі проаналізовано деякі методи та засоби захисту інформації від несанкціонованого доступу. Відповідно до загально прийнятих стандартів та умов сьогодення радикальне вирішення проблем захисту електронної інформації може бути отримано тільки на базі використання криптографічних методів, які дозволяють вирішувати найважливіші проблеми захищеної автоматизованої обробки та передачі даних.

Список бібліографічних посилань

1. Максим М., Полино Д. Безопасность беспроводных сетей. М. : Компания «АйТи»; ДМК Пресс, 2004. 288 с.

2. Олифер В. Г., Олифер Н. А. Основы сетей передачи данных : курс лекций. М. : Интернет-университет информационных технологий, Бином, 2005. С. 176.

3. Методы и средства защиты информации. В 2-х томах / Ленков С. В., Перегудов Д. А., Хорошко В. А. Под ред. В. А. Хорошко. К. : Арий, 2008. Том 1, 464 с. Том 2, 344 с.

4. Василенко В. С., Бордюк О. С., Полонський С. М. Оцінювання ризиків безпеці інформації в локальних обчислювальних мережах. *Сучасні інформаційні технології*. Інформаційна безпека. URL: http://www.rusnauka.com/11_EISN_2010/Informatica/64068.doc.htm (дата звернення: 31.10.2018)

Одержано 02.11.2018