НАЦІОНАЛЬНА БЕЗПЕКА

Дубовик О.І.
студент,
Науковий керівник: **Шевчук Є.В.**
викладач,
Науковий керівник: **Гутнік К.О.**
викладач другої категорії,
Коледж інформаційних технологій та землевпорядкування
Національного авіаційного університету

ПРОБЛЕМАТИКА КОРПОРАТИВНИХ МЕРЕЖ ТА МЕТОДИ ЗАХИСТУ ПРОТИ АТАК

Основним розвитком мереж зв'язку є глобалізація та інтеграція. Інтеграція мережевих і комунікаційних технологій полягає у спільному використанні та інтеграції різноманітних мережевих протоколів, у взаємному використанні комунікаційними провайдерами ресурсів і засобів передачі даних і стикуванні транспортних і сервісних послуг. Необхідність сучасних комп'ютерних систем спонукає до виникнення нових корпоративних мереж, в яких відбувається обмін інформацією як в середині, так і поза межами локальної мережі корпорації. Серед відомим кожному переваг, існують також проблеми, пов'язані з самим процесом передачі конфіденційної інформації через Інтернет. Зростання складності комунікаційних технологій призводить до загроз безпеки інформації, що в умовах відсутності кваліфікованої та гарантованої системи забезпечення безпеки інформаційних ресурсів корпоративних мереж, призводить до функціонального руйнування мережі.

Поширеною атакою інформаційних систем є несанкціонований доступ до паролів чи конфіденційної інформації, порушення прав доступу, атаки типу «відмова в обслуговуванні», «пряма» атака, віруси, сучасні атаки по побічних каналах витоку інформації. Несанкціонований доступ полягає у підборі чи викраденні пароля або підміні IP-адреси законного користувача системи. До цього виду атак вразливі усі компоненти інформаційної системи. Існує чотири стандартні підходи, за допомогою яких можна обмежити доступ до інформації: 1) контроль доступу (перевірка IP-адреси, обмеження доступу за допомогою паролів, застосування програмних засобів); 2) розширення парольного захисту (відповідь на віддалений виклик, тобто перевірка паролю «передзвонюванням», безупинне квітірування зв'язку – система, при якій сервер постійно опитує клієнтський комп'ютер протягом усього сеансу підключення); 3) шифрування (найпопулярнішою асиметричною системою захисту інформації є RSA-шифрування, яке дозволяє створювати стійкий цифровий підпис); 4) використання

брандмауерів (комбінація апаратного і програмного забезпечення для запобігання доступу з Інтернету до інформації).

Для ефективної протидії мережевим атакам і забезпечення можливості активного і безпечного використання в бізнесі започаткованих мереж на початку 90-х років активно розвивається концепція побудови захищених віртуальних приватних мереж – VPN (Virtual Private Networks).

Захищеною віртуальною мережею VPN називають об'єднання локальних мереж і окремих комп'ютерів через відкриту зовнішню середу передачі інформації в єдину віртуальну корпоративну мережу, що забезпечує безпеку циркулюючих даних. Захист інформації в процесі передачі по відкритих каналах зв'язку заснована на виконанні таких основних функцій: автентифікації взаємодіючих сторін; криптографічним закриттям (шифруванні) переданих даних; перевірці автентичності та цілісності доставленої інформації.

Атака «відмова в обслуговуванні» полягає у створенні невідповідного пакету даних чи передачі об'ємної кількості даних у мережі з метою блокування роботи контролера домену, що зупиняє роботу комп'ютерної системи. Для захисту компонентів інформаційної системи застосовуються спеціальні програми виявлення такого типу атак чи міжмережевий екран.

Для захисту від вірусних атак на даний час існує багато програм, що захищає інформаційну систему від пошкодження. Побічними каналами витоку інформації під час передачі пакетів даних мережею є електромагнітне випромінювання, час виконання алгоритмів шифрування та реакція системи на спеціально внесені помилки. Для протидії таким атакам використовуються, як правило, архітектурна та операційна надлишковість, тобто додаткові апаратні та програмні засоби [3].

Керуючись змінами до Положення про державну експертизу в сфері технічного захисту інформації у 2017 році, передбачемо кваліфікацію внутрішнього порушника. Орієнтовно порушники за можливостями в системі відносятся до 3-го рівня. Третій рівень визначається можливістю управління функціонуванням автоматизованих систем, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування. Рівень 4-тий – відповідає системний адміністратор або адміністратор безпеки, чиї можливості в системі максимальні. Віжповідно до розглянутого положення, в своєму рівні порушник є спеціалістом вищої кваліфікації, знає все про АС і, зокрема, про систему і засоби її захисту [4].

Пропонуємо основний список персоналу типовою корпоративної мережі, відповідно до ризику: 1. *Найбільший ризик*: Мережевий адміністратор; Адміністратор безпеки. 2. *Підвищений ризик:* Оператор системи; Менеджер обробки; Системний програміст. 3. *Середній ризик*: Інженер системи; Менеджер програмного забезпечення. 4. *Обмежений ризик*: Прикладний програміст; Інженер або оператор з зв'язку; Адміністратор баз даних; Інженер з обладнання. 5. *Низький ризик*: Інженер периферійному обладнанню; Користувач мережі.

На сьогоднішній день в Україні проблема захисту комерційної таємниці є досить актуальною. Згідно з результатами наших досліджень, 65% співробіт-

ників крадуть конфіденційну інформацію з робочих місць. Найчастіше у зоні ризику – книги електронних адрес, бази даних клієнтів, а також комерційні пропозиції і презентації. На Заході подібні проблеми вже не актуальні – дбайливо зберігати й захищати комерційні таємниці там навчилися давно. А якщо витік інформації все-таки відбувся, то компанії, в яких це відбулося, мають можливість захистити свої інтереси в суді. Наприклад, компанія Apple виграла кілька позовів проти блогерських сайтів, що передчасно розкривали таємниці комп'ютерних новинок. Керівництво компанії помітило, що ці сайти надавали інформацію про нові розробки ще до того, як Apple повідомляла про них офіційно. Суд штату Каліфорнія прийшов до висновку, що розголошення корпоративних таємниць рівнозначне крадіжці ІВ, і власники сайтів AppleInsider.com й PowerPage.org, цілком присвячених техніці Apple, були притягнуті до відповідальності. Більше того, компанія Apple подала позови й проти 25 своїх співробітників, помічених у зв'язках з підсудними блогерами [2].

Отже, проблематика захисту інформаційних атак цілком актуальна. На сьогоднішній день, спеціалісти сфери засобів захисту, усвідомили крайню необхідність у розробці засобів захисту від внутрішніх порушників.

Список використаних джерел:

1. Васильцов І.В. Атаки спеціального виду на криптопристрої та методи боротьби з ними / І.В. Васильцов / За ред. В.П. Широчина – Кременець: Видавничий центр КОГПІ, 2009. – 264 с.
2. Захист прав інтелектуальної власності в Україні: проблеми законодавчого забезпечення та правозастосування. [Електронний ресурс]. – Режим доступу: http://patent.km.ua.
3. Лукацкий А. Атаки на информационные системы. Типы и объекты воздействия // А. Лукацкий / Электроника: Наука, Технология, Бизнес, № 1, 2000. – С. 16-21.
4. Структура руководства по обеспечению информационной безопасности [Електронный ресурс]. – URL: http://www.globaltrust.ru/security/knowbase/Policies/Guide_Struct. – Назва з екрану.