УДК 004.49
Скалецький П. – ст. гр. СКмз-61
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ МЕТОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ

Науковий керівник: ст. викладач Маєвський О.В.

Skaletskyy P.
Ternopil Ivan Pul`uy National Technical University

RESEARCH METHODS OF INFORMATION SECURITY BUSINESS NETWORK

Supervisor: Majevskiy A.

Ключові слова: захист інформації, корпоративні мережі, захист ресурсів.
Keywords: information security, corporate network, protection resources.

Комплексна система захисту інформації (КСЗІ) – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [1].

Одним із напрямків захисту інформації в комп'ютерних системах є технічний захист інформації (ТЗІ). В свою чергу, питання ТЗІ розбиваються на два великих класи задач: захист інформації від несанкціонованого доступу; захист інформації від витоку технічними каналами.

Для забезпечення ТЗІ створюється комплекс технічного захисту інформації, що є складовою КСЗІ.

Під НСД звичайно розуміється доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розглядаються канали побічних електромагнітних випромінювань і наводок, акустичні канали, оптичні канали та інші.

Захист від НСД може здійснюватися в різних складових інформаційної системи: прикладне та системне ПЗ; апаратна частина серверів та робочих станцій; комунікаційне обладнання та канали зв'язку; периметр інформаційної системи.

Організаційний захист інформації – захист інформації шляхом регулювання за допомогою організаційних заходів доступу до всіх ресурсів інформаційної системи [2].

Згідно з ДСТУ 3396.1-96 організаційні заходи захисту інформації – комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціювання засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення ТЗІ.

Сучасні системи захисту інформації повинні відповідати запитам сучасного бізнесу в умовах росту числа загроз безпеки інформації, що виходять із самої корпоративної мережі. Сучасні системи безпеки повинні захищати не окремі елементи мережі, а інформацію у вигляді інформаційних ресурсів і потоків незалежно від місця й часу їхнього виникнення [3]. Інформаційна безпека є складовою частиною інформаційних технологій - області, що розвивається надзвичайно високими темпами. Розробка сучасної системи інформаційної безпеки вимагає, з одного боку, відстеження

швидких змін в інформаційних технологіях і погрозах, що з'являються, а з іншого боку – обліку реальних характеристик апаратного й програмного забезпечення корпоративних мереж і систем. Процедура придбання пристроїв інформаційної безпеки не складна. Істотно більш складним є рішення проблем: як захищати і які засоби безпеки застосовувати. Це рішення охоплює й керування інформаційною безпекою, включаючи планування, розробку політики безпеки й проектування необхідних процедур безпеки [3, 4]. Інформаційна безпека представляє собою багатогранну сферу діяльності, в якій успіх можливий тільки при систематичному, комплексному підході.

У забезпеченні інформаційної безпеки виступають три основні категорії суб'єктів: державні організації, комерційні структури, окремі громадяни. Спектр інтересів суб'єктів, пов'язаних з використанням інформаційних систем, можна поділити на наступні основні категорії [4]: доступність (можливість за прийнятний час одержати необхідну інформаційну послугу); цілісність (актуальність і несуперечність інформації, її захищеність від руйнування й несанкціонованої зміни); конфіденційність (захист від несанкціонованого ознайомлення).

Для того, щоб забезпечити надійний захист ресурсів корпоративної інформаційної системи на сьогодні і на найближче майбутнє, у системі інформаційної безпеки повинні бути реалізовані самі прогресивні й перспективні технології інформаційної безпеки. До них відносяться: комплексний підхід до формування інформаційної безпеки, що забезпечує раціональне об'єднання технологій і засобів інформаційного захисту; застосування захищених віртуальних мереж VPN для захисту інформації, переданої по відкритих каналах зв'язку; криптографічне перетворення даних для забезпечення цілісності, дійсності й конфіденційності інформації; застосування міжмережевих екранів для захисту корпоративної мережі від зовнішніх погроз при підключенні до загальнодоступних мереж зв'язку; керування доступом на рівні користувачів і захист від несанкціонованого доступу до інформації; гарантована ідентифікація користувачів шляхом застосування токенів (смарт-карт, touch-memory, ключі для USB-портів і т.п.) та інших засобів аутентифікації; підтримка інфраструктури керування відкритими ключами РКГ; захист інформації на файловому рівні (шляхом шифрування файлів і каталогів) для забезпечення її надійного зберігання; захист від вірусів з використанням спеціалізованих комплексів антивірусної профілактики й захисту; технологія виявлення вторгнень (Intrusion Detection) і активного дослідження захищеності інформаційних ресурсів; централізоване керування засобами інформаційної безпеки.

Наявність централізованих засобів керування продуктами безпеки є обов'язковою вимогою для можливості їхнього застосування в корпоративному масштабі. Необхідно зауважити, що системи централізованого керування продуктами безпеки різних виробників поки що не сумісні один з одним.

Література:

1. Комплексна система захисту інформації // Вікіпедія. Вільна енциклопедія. – Режим доступу: https://uk.wikipedia.org/wiki/Комплексна_система_захисту_інформації. – Дата доступу: 2 квітня 2016 року. – Заголовок з екрану.

2. Організаційний захист інформації // Вікіпедія. Вільна енциклопедія. – Режим доступу: https://uk.wikipedia.org/wiki/Організаційний_захист_інформації. – Дата доступу: 2 квітня 2016 року. – Заголовок з екрану.

3. С.В. Вихорев. Новые подходы к проектированию систем защиты информации / Вихорев С. В., Березин А. С. // Документальная электросвязь. – 2006. – № 6. – с. 35-37.

4. А.В. Галицкий. Защита информации в сети - анализ технологий и синтез решений / Галицкий А. В., Рябко С. Д., Шаньган В. Ф. – М.:ДМК Пресс, 2004. - 616 с. – ISBN:5-94074-244-0.