Байлюк Є. М., старш. викладач кафедри КІ та КБ,
Гнип М. В., магістрант, гр. ІСТм-20-1
Державний університет «Житомирська політехніка»

ОРГАНІЗАЦІЯ ПЕРИМЕТРОВОГО ЗАХИСТУ ДЛЯ СУЧАСНИХ МЕРЕЖ

Інформаційний обмін в сучасному світі є невід'ємною складовою нашого життя. Зараз неможливо уявити світ без електронної пошти, спілкування в режимі «онлайн» чи інтернет-магазинів. Будь-який карантинний стан супроводжується тим, що працівники компанії змушені працювати віддалено – за допомогою мережі Інтернет. Все це сприяє тому, що кількість інформації в глобальній мережі з кожним днем лише збільшується. На сьогодні час відзначається зріст активності зовнішніх зловмисників, що використовують останні розробки в області нападу. Цим вони прагнуть проникнути в корпоративні мережі.

В наш час значного розвитку набули технології електронних платежів і електронного документообігу, тому будь-який збій мережі може спричинити порушення в роботі банків і цілих корпорацій, що призводить до великих матеріальних збитків. Щоб запобігти цьому потрібно організувати захист інформації в мережі. Обов'язковим елементом системи інформаційної безпеки організації є захист периметру мережі. Мінімізація зовнішніх загроз досягається шляхом впровадження багаторівневої системи захисту інформації, і в першу чергу на зовнішньому кордоні мережі. Важливим завданням системи захисту периметра є розділення мережі на внутрішню і зовнішню області. Розглядаючи проблему захисту інформації в мережі насамперед розглядають питання класифікації порушень роботи мережі та прав доступу, які можуть призвести до знищення чи небажаної модифікації даних. До потенційних загроз належать: порушення роботи обладнання; втрата інформації внаслідок некоректної роботи програмного забезпечення; втрата інформації, що пов'язана з несанкціонованим доступом; втрата інформації, що пов'язана з неправильним зберіганням архівних даних; помилки обслуговуючого персоналу і користувачів [1]. Існує два види несанкціонованого доступу до інформації, що знаходиться в мережі: з фізичним доступом до елементів мережі та без нього. Масовані кібератаки ініціюють створення спеціальних технічних рішень, засобів та систем протидії. Вони, в свою чергу, мають відповідати основоположним принципам інформаційної безпеки: конфіденційність, цілісність і доступність.

В залежності від можливих видів порушень роботи мережі чи несанкціонованого доступу, засоби захисту поділяються на: технічні засоби (апаратні пристрої, що сполучаються чи вбудовуються безпосередньо в апаратуру локальних мереж, охоронні сигналізації, замки на дверях, віконні ґрати та ін.) та програмні засоби (засоби архівації даних, антивірусні програми, криптографічні програми, засоби ідентифікації і автентифікації користувачів, засоби керування доступом, протоколювання та аудит та ін.). Сучасні технології розвиваються в напрямку поєднання цих засобів з метою підвищення захисту. Також до засобів захисту відносять організаційні, які, в свою чергу, розділяють на організаційно-технічні (підготовка приміщень, прокладка кабельної системи з обмеженим доступом до неї тощо) та організаційно-правові (правила роботи підприємства та національні законодавства) [2]. Фахівці галузі рекомендують використовувати комплексний підхід до застосування та розвитку всіх засобів і способів захисту інформації. Це підтверджується тим, що окремі сфери діяльності, які пов'язані з банківською справою чи системою державного управління, вимагають більш спеціалізованих заходів безпеки даних і висувають підвищені вимоги до надійності функціонування та захисту мереж, відповідно до характеру і важливості вирішуваних ними задач.

З вищесказаного можна зробити висновок, що правильний і повноцінний захист периметру сучасних корпоративних мереж дозволяє домогтися захищеності доступу внутрішніх користувачів в зовнішній мережі, надає доступ з зовнішніх мереж до публічних корпоративних ресурсів, захищає від мережевих атак на корпоративні ресурси, організовує системи електронної комерції, створює єдину точку антивірусної і антиспам фільтрації, запобігає витоку конфіденційної інформації, проводить моніторинг та аналіз подій інформаційної безпеки.

Список використаних джерел

1. Информационная безопасность открытых систем. Средства защиты в сетях / С. В.Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. – Москва: Горячая линия-Телеком, 2008. – 558 с. – (Горячая линия-Телеком).
2. Основы организации сетей Cisco / Вито Амато., 2004. – 464 с. – ("Вильямс").