сборник статей II Междунар. научно-техн. конф. "Минские научные чтения – 2019", Минск, 11-12 декабря 2019 г.: в 3 т. Т. 3. – Минск: БГТУ, 2020. – С. 180–185.

2. Ochrona informacji w sieciach komputerowych / pod red. prof. P. Urbanowicza. – Lublin : Wydawnictwo KUL, 2004. – 150 p.

3. Zander, S. Covert channels and countermeasures in computer network protocols / S. Zander, G. Armitage, P. Branch // IEEE Communications Surveys & Tutorials. – 2007. – № 9(3). – P. 44-56.

4. Simmons, G.J. The Prisoners' Problem and the Subliminal Channel / G. J. Simmons. – Proc. Advances in Cryptology (CRYPTO). – 1983. – P. 51–67.

5. National Computer Security Center, US DoD, Trusted Computer System Evaluation Criteria, Tech. Rep. DOD 5200.28- STD, National Computer Security Center, Dec., 1985.

УДК 004.056

О.Л. Сапун, доц., канд. пед. наук; А.С. Гончар, маг.
(БГАТУ, г. Минск)

ПРИМЕНЕНИЕ МЕЖСЕТЕВОГО ЭКРАНА ДЛЯ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Большинство предприятий сталкиваются с проблемами в компьютерных системах и утечки важной информации. Не являются исключением и предприятия агропромышленного комплекса. Существует множество программ или программно-аппаратных систем, позволяющих минимизировать данные проблемы.

Межсетевой экран (firewall, МЭ) – программная или программно-аппаратная система, обладающая искусственным интеллектом, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивающая защиту информационной системы посредством фильтрации информации [1].

МЭ выступает сегодня как наиболее действенное средство управления безопасностью. При многократно возросшем трафике данных очень важно, чтобы никакой вредоносный объект не проник в сеть организации. Проверки данных нужно проводить регулярно для поддержания системы, также необходимо проводить регулярно проверки антивирусами для обеспечения защиты операционной системы на виртуальном сервере и мониторинг безопасности сети.

Целью системы защиты на основе МЭ является своевременное реагирование на попытки доступа к ресурсам сети, выявлении попыток НСД и запись в журнал событий о произошедшем инциденте.

Применение межсетевого экрана иногда является причиной падения производительности сети. Они перехватывают весь входящий трафик сети для проверки и могут работать медленно.

Произведем сравнительный анализ и выбор средств межсетевого экранирования, с подходящими характеристиками, для внедрения на предприятии АПК. Объектом исследования выберем ОАО «Птицефабрика «Рассвет».

Система защиты периметра состоит из следующих основополагающих компонентов: персонал (сотрудники, студенты); программное обеспечение; аппаратное обеспечение; технологии взаимодействия.

В результате выбора среди продуктов от каждой фирмы можно выделить продукты D-link DFL-260, IBM Proventia Network IPS и Cisco 1801/K9. Стоит отметить, что в выборе ключевым показателем выступает цена программного продукта для расчета экономической эффективности. Результаты сравнительного анализа трех вариантов средств межсетевого экранирования по основным характеристикам приведены в таблице.

Таблица – Результаты сравнительного анализа средств межсетевого экранирования

Характеристика	D-link DFL-260	IBM Proventia IPS	Cisco 1801/K9
1	2	3	4
Класс отказоустойчивости	1 класс	нет	1 класс
Контроль на прикладном уровне с учетом состояния	Нет	Да	Да
Контроль прикладного протокола	Да	Да	Да
Прозрачная аутентификация Windows	Да	Да	Да
Пропускная способность	80Mbps	10Mbps	100Mbps
Wi-Fi	Нет	Нет	Да
Протоколирование всех имен пользователей и приложений Web и Winsock	Да	Да	Нет
Поддержка Exchange	Да	Да	Да
Демилитаризованная зона	Да	Да	Нет
Контроль шлюзового и клиентского трафика VPN на прикладном уровне	Нет	Да	Да
Обнаружение и предотвращение несанкционированного доступа	Да	Да	Да

Продолжение таблицы

1	2	3	4
Сервер удаленного доступа VPN и шлюз VPN	Да	Да	Да
VPN-клиент	Да	Да	Да
100-Мбит/с порты ЛВС	4	8	8
Число одновременных подключений	12000	10000	18000
Передача функций отказавшего МЭ исправному устройству	Нет	Нет	Да
Переключение Интернет-провайдера и объединение полосы пропускания	Нет	Да	Нет
Конфигурирование Web-интерфейс	Да	Да	Да
Web-кэширование и proxy	Да	Нет	Да
Цена	750 руб.	5110 руб.	1230 руб.

Как видно из таблицы, высокая цена продукта компании IBM обоснована высоким качеством, пропускной способностью. В данном случае рассматривается мало пропускаемая, т.е. самая дешёвая – 10 Mbps и функциональной полнотой их продуктов. Однако наилучшим продуктом в соотношении цена и качество является продукт компании D-link, который оптимизирован для работы в сетях различной архитектуры [2].

В качестве примера возьмем средство защиты МЭ D-link DFL-260. Данное устройство является лучшим в соотношении цена/качество, продукт оптимизирован для работы в сетях различной архитектуры, что является положительном фактором в широте использования данного продукта для ХС с классической архитектурой.

Однако, если организация действительно большая и информация, которая в ней циркулирует в защищаемой сети является жизненно важной для самой организации и ее цена достаточно высока, можно обратиться к продукту IBM Proventia Network IPS, основываясь на его качестве и защищаемых способностях, но его высокая цена не позволяет рекомендовать его широкому кругу компаний.

Затраты на организацию системы защиты складываются из:

- стоимости программно-аппаратных частей системы;
- затрат на обучение и выплату зарплат сотрудникам;
- затрат на поддержание системы.

Для расчета затрат на организацию системы защиты на основе использования МЭ необходимо воспользоваться методикой расчета совокупной стоимости владения, т.е. суммы прямых и косвенных затрат, которые несет владелец системы за период ее жизненного цикла.

Совокупная стоимость владения в общем виде представляется в виде следующей формулы:

– совокупная стоимость владения системой защиты;

– стоимость программно-аппаратных средств;

– кадровые издержки (оплата труда, плата за обучение, премии, штрафы);

– затраты на техническую поддержку.

Совокупная стоимость владения МЭ в общем виде представляется в следующем виде: совокупная стоимость владения системой защиты; стоимость программно-аппаратных средств; кадровые издержки (оплата труда, плата за обучение, премии, штрафы); затраты на техническую поддержку.

После проведенного расчета экономической эффективности на примере ОАО «Птицефабрика «Рассвет», рост производительности труда на рабочем месте работников за счет внедрения МЭ составит 39,58%. Срок окупаемости капитальных затрат на организацию системы информационной безопасности составит 0,76 года (9 месяцев).

Поскольку предполагаемый срок окупаемости составляет не более 5 лет (максимальный срок окупаемости капитальных вложений в рыночных условиях), внедрение системы межсетевого экранирования будет экономически выгодным [3].

Таким образом, внедрение системы межсетевого экранирования в запланированные сроки позволит предприятию выполнить поставленные задачи, снизить информационные риски, повысить эффективность деятельности ОАО «Птицефабрика Рассвет». Но межсетевые экраны не решают всех вопросов информационной безопасности корпоративных сетей. Отсюда следует, что технологии МЭ следует применять комплексно с другими технологиями и средствами защиты.

ЛИТЕРАТУРА

1. Дорофеев, А.В. Подготовка к CISSP: телекоммуникации и сетевая безопасность / А.В. Дорофеев – Москва: Вопросы кибербезопасности, 2016. – 69–74 с.

2. Шаго Ф.Н., Методика оптимизации планирования аудита системы менеджмента информационной безопасности / Ф. Н. Шаго, И.В. Зикратов – Ростов-на-Дону: Научно-технический вестник информационных технологий, механики и оптики, 2014. – 111–117 с.

3. Старков Д.И. Автоматизированное построение правил фильтрации межсетевых экранов на основе списка разрешенных сетевых служб // Решетневские чтения. – 2018. – № 22. – Том 2. – С. 348-349.