УДК 004.054.53
DOI: 10.33764/2618-981X-2019-9-54-60

О ВЫБОРЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Алина Павловна Жумаева
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, бакалавр информационной безопасности, тел. (999)466-04-55, e-mail: zhumaevanalina@gmail.ru

Валентина Андреевна Ялбаева
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, бакалавр информационной безопасности, тел. (960)975-49-15, e-mail: valya_599@mail.ru

Полина Александровна Звягинцева
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, старший преподаватель кафедры информационной безопасности, тел. (383)343-91-11, e-mail: p.a.zvjaginceva@sgugit.ru

Валентин Валерьевич Селифанов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (383)343-91-11, e-mail: sfo1@mail.ru

В статье рассматривается проблема выбора средств защиты информации в государственной информационной системе, а именно межсетевые экраны и средства обнаружения вторжений. Данная проблема актуальна, так как в последние годы обеспечение информационной безопасности, как никогда, востребовано.

Ключевые слова: межсетевой экран, средства обнаружения вторжения, программное обеспечение, информационная система, средство защиты информации, сетевая атака, уровень защиты информации, недекларированные возможности, сервер.

CHOICE OF MEANS OF INFORMATION SECURITY FOR GOVERNMENT INFORMATION SYSTEMS

Alina P. Zhumaeva
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk, 630099, Russia, Bachelor of Information Security, phone: (999)466-04-55

Valentina A.Yalbaeva
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk, 630099, Russia, Bachelor of Information Security, phone: (960)975-49-15

Polina A. Zviagintcheva
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone: (383)343-91-11, e-mail: p.a.zvjaginceva@sgugit.ru

Valentin V. Selifanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, Department of Information Security, phone: (383)343-91-11, e-mail: sfo1@mail.ru

The article deals with the problem of choosing the means of information security in the state information system, namely firewalls and intrusion detection. The problem is relevant since information security is in demand more than ever.

Key words: firewall, intrusion detection system, software, information system, information security tool, network attack, information security level, undeclared capabilities, server.

Начиная с 2011 года, начался процесс изменения требований к средствам защиты информации. Осуществляется переход на систему требований нового поколения, основанную на международной серии стандартов ИСО/МЭК 15408 или «общие критерии». Все большее значение приобретают средства обеспечения безопасности межсетевого взаимодействия. Однако стоит рассмотреть комплексное решение.

После изменений требований все средства защиты информации (СЗИ) от несанкционированного доступа (НСД) классифицируются по видам, классам и типам.

Под видом СЗИ понимается конкретное средство, которое используется. Это может быть:

– антивирусное СЗИ, которое должно выявлять и соответствующим образом реагировать на средства несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации СЗИ;

– межсетевые экраны – средства, реализующие контроль за информацией, направленной в автоматизированную систему или исходящей из нее. Межсетевые экраны выполняют фильтрацию информации по заданным критериям;

– средство доверенной загрузки – программно-технические средства, которые реализуют функции по предотвращению несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники на этапе его загрузки;

– система обнаружения вторжений (СОВ, соответствующий английский термин Intrusion Detection System (IDS)– программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть, либо несанкционированного управления ими в основном через Интернет.

Каждому виду соответствует 6 классов, которые зависят от уровня защищаемой информации (1–3 это государственная тайна, 4–6 иная информация ограниченного доступа и т. д.). В данной работе будут рассмотрены СЗИ 4–6 классов.

Кроме вида и класса средства защиты, выделяется тип СЗИ – где применяется это средство защиты информации и что оно делает.

Проблема выбора СЗИ в ГИС.

Защита информационной системы нуждается не только в выборе средства защиты информации, но еще и выполнении ряда определенных требований, а также проведении оценки эффективности [8–10].

В соответствии с приказом ФСТЭК России № 17от 11 февраля 2013 г п. 26, для проектирования системы защиты информационной системы необходимо:

– определить типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа);

– определить методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в информационной системе;

– выбрать меры защиты информации, подлежащие реализации в системе защиты информации информационной системы [11];

– определить виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

– определить структуру системы защиты информации, информационной системы, включая состав (количество) и места размещения ее элементов;

– осуществить выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы;

– определить требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации;

– определить меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

Как правило, часть угроз можно нейтрализовать, используя волоконно-оптические линии связи, однако ограничиваться этим нельзя и необходимо выбирать виды систем защиты информационной системы исходя из актуальных угроз [7]. Серьезное внимание стоит уделить типам и классам. Сузим область и рассмотрим не все виды средств защиты, а лишь некоторые из них – межсетевые экраны и системы обнаружения вторжений и такой вид информационной системы как ГИС.

Классы защиты определяются в соответствии с нормативными правовыми актами ФСТЭК России.

Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. При этом:

– в информационных системах 1 класса защищенности применяются средства защиты информации не ниже 4 класса;

– в информационных системах 2 класса защищенности применяются средства защиты информации не ниже 5 класса;

– в информационных системах 3 класса защищенности применяются средства защиты информации 6 класса.

Если посмотреть на оборудование Cisco (Cisco – американская компания, разрабатывающая и продающая сетевое оборудование, предназначенное в основном для крупных организаций и телекоммуникационных предприятий), в нем присутствует много межсетевых экранов, соответствующих 5 классу защиты для межсетевых экранов [4], при этом контроль отсутствия недекларированных возможностей не проводился. Таким образом использовать рассматриваемые средства в системе защиты информации ГИС 1 и 2 класса защиты, а так же информационных систем персональных данных 1, 2 и частично 3 уровня защищенности нельзя [3].

Обратимся к типам межсетевых экранов. Требованиями Информационного сообщения ФСТЭК от 28 апреля 2016 г. № 240/24/1986, выделены 5 типов межсетевых экранов:

– уровня сети (тип «А») – межсетевой экран, применяемый на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы;

– уровня логических границ сети (тип «Б») – межсетевой экран, применяемый на логической границе (периметре) информационной системы или между логическими границами сегментов информационной системы;

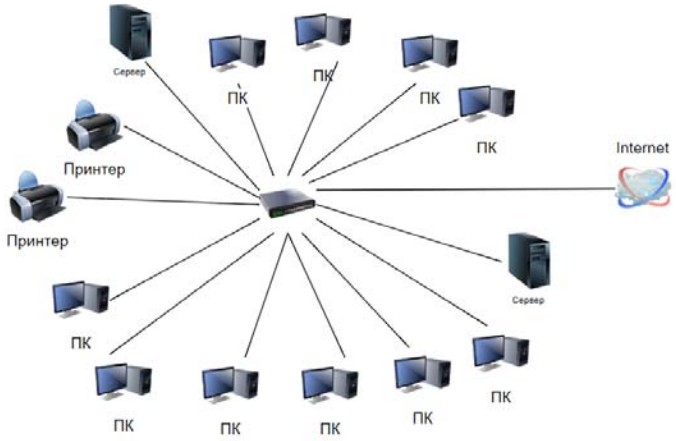
– уровня узла (тип «В») – межсетевой экран, применяемый на узле (хосте) информационной системы;

– уровня веб-сервера (тип «Г») – межсетевой экран, применяемый на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов (сервера);

– уровня промышленной сети (тип «Д») – межсетевой экран, применяемый в автоматизированной системе управления технологическими или производственными процессами.

Если рассмотреть небольшие государственные информационные системы (до 20 автоматизированных рабочих мест – это рабочее место интерпретатора, оборудованное персональным компьютером с периферийными устройствами, для автоматизированной обработки и интерпретации материалов, а также выдачи результатов), то можно наблюдать, что пользователи выбирают исключи-

тельно программные межсетевые экраны, так как для их использования достаточно установить лишь специальное программное обеспечение. Обычно организация с трудом может найти компьютер, отвечающий всем техническим требованиям, зачастую довольно высоким.



Топология сети

Разберем данную проблему на примере сети, состоящей из 2 серверов, 2 сетевых принтеров, 10 рабочих мест, и одного коммутатора (рис.1). Даже если на свой домашний компьютер поставить персональный межсетевой экран (межсетевой экран типа «В» может иметь только программное исполнение), можно увидеть, что при таком простом коммутируемом подключении к Интернет с динамически выделяемым IP-адресом он подвергается, по крайней мере, одной сетевой атаке (например: вирусы, троянские программы, распространение сетевого червя, логические бомбы, эксплойты, бот сети, руткиты, фишинг, фарминг) каждые несколько часов работы в сети. А в нашем случае это сеть, состоящая из 10 рабочих станций. Можно сделать вывод о том, насколько интенсивное давление испытывает эта информационная система. А ущерб от любой из этих атак на сеть может многократно превысить не только стоимость системы безопасности, но и всей информационной сети.

Именно поэтому крупные компании предпочитают установку специализированных программно-аппаратных комплексов (межсетевые экраны типа «А»), получивших название «security appliance». Работают они чаще всего на основе систем Linux.

Такое решение имеет следующие преимущества:

– легкое и простое управление: контроль работы программно-аппаратного комплекса осуществляется с любого стандартного протокола (Telnet, SNMP) – или защищенного (SSL, SSH);

– высокая производительность: работа операционной системы направлена на одну единственную функцию, из нее исключены любые посторонние сервисы;

– отказоустойчивость: программно-аппаратные комплексы эффективно выполняют свою задачу, вероятность сбоя практически исключена.

Данная проблема касается всех: ситуация, когда работа с сервером осуществляется через веб-браузер, но ни межсетевого экрана типа «Г», ни системы обнаружения вторжений нет. Система обнаружения вторжений и межсетевой экран не позволяют злоумышленникам воздействовать на информационную систему посредством сетевых атак. Но отличаются они тем, что межсетевой экран ограничивает поступление на хост или подсеть определенных видов трафика для предотвращения вторжений и не отслеживает вторжения, происходящие внутри сети, а СОВ пропускает трафик, анализируя его и сигнализируя при обнаружении подозрительной активности. В данном случае опасен как внутренний, так и внешний нарушитель, потому что есть возможность подключения к Интернету. В этом случае злоумышленник может реализовать атаки:

- взлом паролей;
- отключение/обход систем аудита;
- использование снифферов и sweepers (систем контроля содержимого);
- использование программ диагностики сети для получения необходимых данных;
- подмена данных в IP-пакетах;
- атаки типа «отказ в обслуживании» (DoS);
- атаки на Web-серверы (CGI-скрипты).

Во избежание вышеперечисленных проблем рекомендуется устанавливать комплексную защиту, включающую в себя такие средства защиты информации как межсетевые экраны типа «А», «Г» (SecretNet Studio) и систему обнаружения вторжений (Security Studio Endpoint Protection).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Информационное письмо ФСТЭК России об утверждении требований к системам обнаружения вторжений.

2. Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г.

3. Приказ 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

4. Информационное сообщение ФСТЭК России об утверждении требований к межсетевым экранам от 28 апреля 2016 г. N 240/24/1986.

5. Информационное сообщение ФСТЭК России об утверждении методических документов, содержащих профили защиты межсетевых экранов от 12 сентября 2016 г. N 240/24/4278.

6. Информационное сообщение ФСТЭК России по вопросам разработки, производства, поставки и применения межсетевых экранов, сертифицированных ФСТЭК России по требованиям безопасности информации от 24 марта 2017 г. N 240/24/1382.

7. Селифанов В.В., Звягинцева П.А., Юракова Я.Ю. Применение методов автоматизации при определении актуальных угроз безопасности информации в информационных системах с применением банка данных угроз ФСТЭК России // Вестник СГУГиТ. – 2017. – Т. 22, № 4. – С. 202–209.

8. Селифанов В. В. Оценка эффективности системы защиты информации государственных информационных систем от несанкционированного доступа // Интеграция науки, общества, производства и промышленности: сборник статей Международной научно-практической конференции, 2016. С. 109-113.

9. Оценка эффективности системы защиты информации ИСПДН с учетом профиля защиты / В. В. Селифанов, П. А. Звягинцева, А. С. Голдобина, Ю. А. Исаева // Вестник СГУГиТ. – 2017. – Т. 22, № 4. – С. 220–225.

10. Селифанов В.В., Ремизова В.А. Проведение аттестационных испытаний средств антивирусной защиты // Информационные системы и процессы, сборник научных трудов, Новосибирский государственный университет экономики и управления «НИНХ» (Новосибирск), 2015, стр. 208-213

11. Селифанов В.В., Курносов К.В. Требования к системе защиты информации для виртуальной инфраструктуры // Информационное противодействие угрозам терроризма. 2014. № 23. С. 188.