№ 3086

МИСиС
Национальный исследовательский технологический университет

В.Н. Костин

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

STORE.MISIS.RU

УДК 004.056
К72

Рецензент
проф., канд. техн. наук *Т.К. Кузищина*

Костин В.Н.

К72 Методы и средства защиты компьютерной информации : Криптографические методы для защиты информации : учеб. пособие / В.Н. Костин. – М. : Изд. Дом НИТУ «МИСиС», 2018. – 40 с.

ISBN 978-5-90695-334-6

В учебном пособии рассмотрены вопросы информационной безопасности вычислительных сетей с использованием межсетевых экранов. Представлена архитектура межсетевых экранов и стратегия их использования, описаны криптографические методы, используемые для защиты информации, и возможности их применения.

Предназначено для студентов, обучающихся по направлениям, связанным с разработкой компьютерных систем и технологий и обеспечением в них информационной безопасности.

УДК 004.056

ISBN 978-5-90695-334-6

ОГЛАВЛЕНИЕ

1. КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Средства защиты в компьютерных сетях называются как **Firewall** (англ.) или **брандмауэр** (нем.). В нашей литературе этот термин называется **межсетевой экран** (МЭ). Брандмауэр – это огнеупорный барьер, разделяющий отдельные блоки в многоквартирном доме, предотвращающий распространение огня. Межсетевой экран работает примерно также – помогает избежать риска повреждения систем или данных в локальной сети из-за проблем, вызванных взаимодействием с другими сетями. Межсетевой экран пропускает разрешенный трафик и блокирует остальное. Термин «**межсетевой экран»** обозначает совокупность компонентов, которые находятся между локальной сетью и внешним миром и образуют защитный барьер. В пособии используются два термина – межсетевой экран и брандмауэр.

В России существует документ Гостехкомиссии, устанавливающий классификацию межсетевых экранов по уровню защищенности к информации – «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации». В нем устанавливаются пять классов защищенности МЭ. Самый низкий класс защищенности – пятый, применяемый для безопасного взаимодействия автоматизированной системы (АС) класса 1Д с внешней средой, четвертый класс – для системы 1Г, третий класс – 1В, второй класс – 1Б, первый класс – 1А – для безопасного взаимодействия АС класса 1А с внешней средой. Для АС в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов:

– при обработке информации с грифом «секретно» – не ниже 3 класса;
– обработке информации с грифом «особой важности» – не ниже 1 класса.

В общем случае МЭ ставится для разграничения доступа клиентов из одного множества систем к информации, хранящейся на серверах в другом множестве.

Требования, предъявляемые к МЭ

1. Обеспечение безопасности внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи.

2. Экранирующая система должна обладать мощными и гибкими средствами управления.

3. Межсетевой экран должен работать незаметно для пользователей локальной сети и не затруднять выполнение ими легальных действий.

4. Процессор МЭ должен быть быстродействующим, работать достаточно эффективно и успевать обрабатывать все входящие и исходящие потоки в пиковых режимах.

5. Система обеспечения безопасности должна быть сама надежно защищена от любых несанкционированных воздействий, так как она является ключом к конфиденциальной информации в организации.

6. Межсетевой экран должен иметь средства авторизации доступа пользователей через внешние подключения в случае работы сотрудников в командировках.

Основные функции межсетевого экрана

1. Защищать сеть от небезопасных протоколов и служб.

2. Защищать информацию о пользователях, системах, сетевых адресах и выполняемых в сети приложениях от внешнего наблюдения.

3. Обеспечить ведение журнала, содержащего статистические данные и записи о доступе к защищенным ресурсам.

4. Гарантировать централизованное управление безопасностью сети по отношению к остальному миру.

Можно указать еще несколько функций, которые, которые дают некоторые гарантии безопасности, но в то же время предназначены для повышения производительности:

1. Кэширование – это свойство сетей, содержащих web-сервер с большим объемом информации, доступной из сети Интернет. Благодаря локальному хранению часто запрашиваемых данных кэширующий сервер может улучшать время реакции на запрос пользователя.

2. Трансляция адреса. Настроенный соответствующим образом МЭ позволяет применять для внутренней сети любые IP-адреса. При этом снаружи виден только адрес МЭ.

3. Переадресация – эта функция предоставляет МЭ возможность изменять, например, запросы HTTP так, чтобы они направлялись серверу не с указанным в пакете запроса IP-адресом, а с другим. Таким образом, удается распределять нагрузку между серверами, которые для внешнего пользователя выглядят как одиночный сервер.

Вместе с тем МЭ не гарантирует абсолютную защиту сети, и его нельзя рассматривать в качестве единственного средства обеспечения