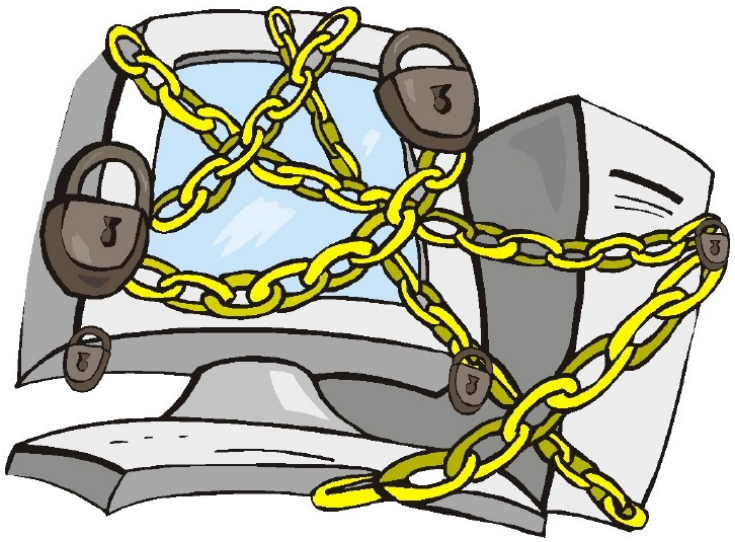
УНИВЕРСИТЕТ ИТМО

Т.А. Маркина

СРЕДСТВА ЗАЩИТЫ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ И СЕТЕЙ



Санкт-Петербург

2016

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

Т.А. Маркина

СРЕДСТВА ЗАЩИТЫ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ И СЕТЕЙ

Учебное пособие

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург

2016

Маркина Т.А. Средства защиты вычислительных систем и сетей. Учебное пособие. – СПб: Университет ИТМО, 2016. – 71 с.

Пособие содержит теоретический материал по дисциплине «Средства защиты вычислительных систем и сетей».

Пособие предназначено для направления подготовки магистров 09.04.01 «Информатика и вычислительная техника».

Пособие предназначено для магистерской программы «Безопасность вычислительных систем и сетей».

Рекомендовано к печати протокол №4 от 20 декабря 2016 г. Ученого совета факультета программной инженерии и компьютерной техники

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

Оглавление

Основные термины и документы

Средства защиты информации – совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Согласно **ГОСТ Р 50922-2006:**

- *средство защиты информации* – это техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Согласно **ГОСТ Р 50.1.056-2005:**

- *средство защиты информации от утечки по техническим каналам*: техническое средство, вещество или материал, предназначенные и (или) используемые для защиты информации от утечки по техническим каналам;
- *средство защиты информации от несанкционированного доступа*: техническое, программное или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа к информации или ресурсам информационной системы;
- *средство защиты информации от несанкционированного воздействия*: техническое, программное или программно-техническое средство, предназначенное для предотвращения несанкционированного воздействия на информацию или ресурсы информационной системы;
- *межсетевой экран*: локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и (или) выходящей из автоматизированной системы;
- *средство обеспечения технической защиты информации*: техническое, программное, программно-техническое средство, используемое и (или) создаваемое для обеспечения технической защиты информации на всех стадиях жизненного цикла защищаемого объекта.

Согласно **ГОСТ Р 53114–2008:**

- *техническое средство обеспечения информационной безопасности:* оборудование, используемое для обеспечения информационной безопасности организации некриптографическими методами;
- *средство обнаружения вторжений*, *средство обнаружения атак*: программное или программно-техническое средство, которое автоматизирует процесс контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализирует эти события в поисках признаков инцидента информационной безопасности;

- *средство защиты от несанкционированного доступа*: программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

В Российской Федерации вопросы информационной безопасности и защиты информации обеспечиваются соблюдением следующих указов Президента, федеральных законов, постановлений Правительства Российской Федерации, руководящих документов Гостехкомиссии России и других нормативных документов:

- Указ Президента РФ от 6 марта 1997 г. № 188. Об утверждении перечня сведений конфиденциального характера;
- Постановление Правительства Российской Федерации от 21.10.1. Об организации лицензирования отдельных видов деятельности;
- Закон Российской Федерации от 21 июля 1993 г. О государственной тайне;
- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006.

Основные стандарты информационной безопасности:

- ГОСТ Р 50922-2006 – Защита информации. Основные термины и определения.
- Р 50.1.053-2005 – Информационные технологии. Основные термины и определения в области технической защиты информации.
- ГОСТ Р 51188-98 – Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.
- ГОСТ Р 51275-2006 – Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
- ГОСТ Р ИСО/МЭК 15408-1-2008 – Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
- ГОСТ Р ИСО/МЭК 15408-2-2008 – Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
- ГОСТ Р ИСО/МЭК 15408-3-2008 – Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
- ГОСТ Р ИСО/МЭК 15408 – «Общие критерии оценки безопасности информационных технологий» – стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности – благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» – защита информации от несанкционированного доступа, модификации или

утечки, и другие способы защиты, реализуемые аппаратными и программными средствами.

- ГОСТ Р ИСО/МЭК 17799 – «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением – ISO/IEC 17799:2005.
- ГОСТ Р ИСО/МЭК 27001 – «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта – ISO/IEC 27001:2005.
- ГОСТ Р 51898-2002 – Аспекты безопасности. Правила включения в стандарты.

Основные руководящие документы:

- Руководящий документ. Руководство по разработке профилей защиты и заданий по безопасности.
- Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты.
- Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты.
- Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности.
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий.
- Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.
- Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации.
- Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования.
- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
- Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
- Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения.
- Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
- Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного

доступа в автоматизированных системах и средствах вычислительной техники.

Нормативные документы:

- Стандарт Банка России СТО БР ИББС-1.0-2014 – Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
- PCI DSS (Payment Card Industry Data Security Standard) – Стандарт безопасности данных индустрии платёжных карт.

Методические документы:

- Профили защиты средств контроля съемных машинных носителей информации.
- Меры защиты информации в государственных информационных системах.
- Профили защиты средств доверенной загрузки.
- Профили защиты средств антивирусной защиты.
- Профили защиты систем обнаружения вторжений.

Классификации средств защиты вычислительных систем и сетей

Многообразие целей, задач, объектов защиты и проводимых мероприятий предполагает рассмотрение некой системы классификаций.

Многообразие классификационных характеристик позволяет рассматривать средства ИТЗ по объектам воздействия, характеру мероприятий, способам реализации, масштабу охвата, классу средств злоумышленников, которым оказывается противодействие со стороны служб безопасности.

Инженерно-техническая защита (ИТЗ) – это совокупность специальных органов, технических и программных средств и мероприятий по их использованию в интересах защиты конфиденциальной информации (см. Рис.1).

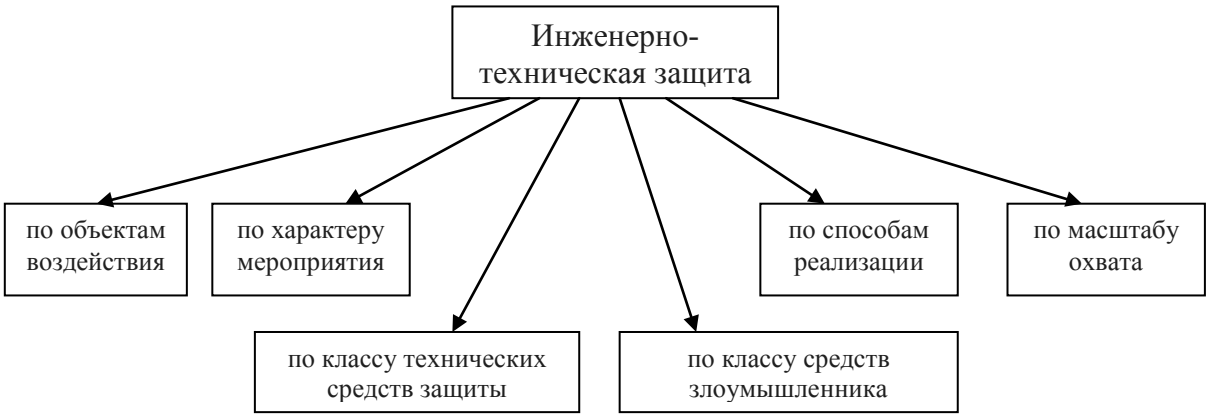


Рис. 1. Основная классификация

Очевидно, что такое деление средств защиты информации условно, т.к. они часто взаимодействуют и реализуются в комплексе в виде аппаратно-программных модулей с широким использованием алгоритмов закрытия информации (см. Рис.2).

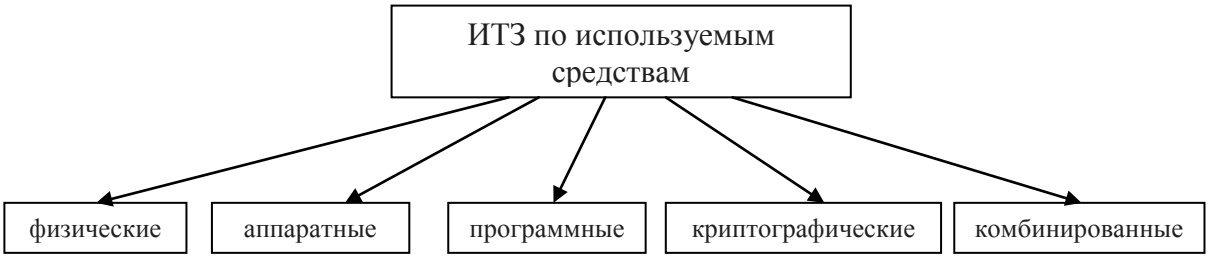


Рис. 2. Классификация ИТЗ по используемым средствам

Физические средства защиты информации – это разнообразные устройства, приспособления, конструкции, аппараты, изделия, сооружения и организационные меры, предназначенные для создания препятствий на пути движения злоумышленников (см. Рис.3).

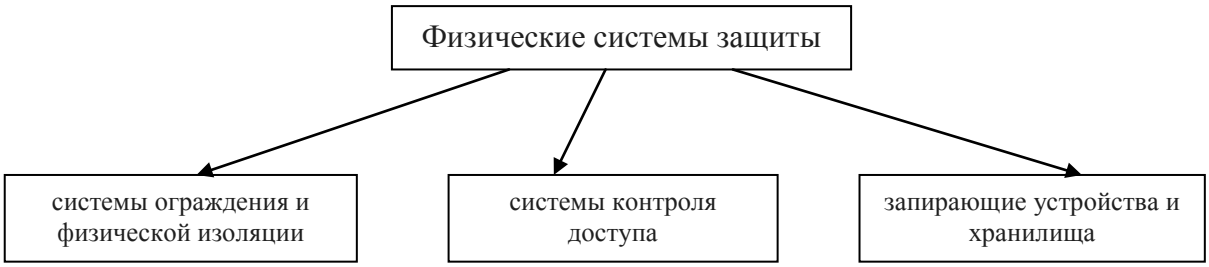


Рис. 3. Классификация физических систем защиты

К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.

Системы ограждения и физической изоляции обеспечивают:

- защиту объектов по периметру;
- защиту элементов зданий и помещений;
- защиту объемов зданий и помещений.

Системы контроля доступа реализуют:

- контроль доступа на охраняемые объекты;
- защиту документов, данных, фильм.

Запирающие устройства и хранилища включают:

- различные системы запирающих устройств (механические, электромеханические, электронные);
- различные системы шкафов и хранилищ;

Эти средства применяются для решения следующих задач:

- охрана территории предприятия и наблюдение за ней;
- охрана зданий, внутренних помещений и контроль за ними;
- охрана оборудования, продукции, финансов и информации;
- осуществление контролируемого доступа в здания и помещение.

Все физические средства защиты объектов можно разделить на три категории:

1. средства предупреждения;
2. средства обнаружения;
3. системы ликвидации угроз.

Охранная сигнализация и охранное телевидение, например, относятся к средствам обнаружения угроз; заборы вокруг объектов − это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие меры служат защитой и от проникновения, и от других преступных действий (подслушивание, обстрел, бросание гранат и взрывпакетов и др.). Средства пожаротушения относятся к системам ликвидации угроз.

В общем плане по физической природе и функциональному назначению все средства этой категории можно разделить на следующие группы:

- охранные и охранно-пожарные системы;
- охранное телевидение;
- охранное освещение;
- средства физической защиты.

К средствам физической защиты относятся:

- ограждение и физическая изоляция,
- запирающие устройства,
- системы контроля доступа.

К системам контроля доступа относятся:

- системы, использующие различные карты и карточки, на которых помещается кодированная или открытая информация о владельце,
- системы опознавания по отпечаткам пальцев,
- системы опознавания по голосу,
- системы опознавания по почерку,
- система опознавания по геометрии рук.

Все устройства идентификации могут работать как отдельно, так и в комплексе.

Аппаратные (технические) средства защиты информации – это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они препятствуют доступу к информации, в том числе с помощью её маскировки. К аппаратным средствам относятся: генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны − недостаточная гибкость, относительно большие объём и масса, высокая стоимость. К аппаратным средствам защиты информации относятся самые различные по принципу действия, устройству и возможностям технические конструкции, обеспечивающие пресечение разглашения, защиту от утечки и противодействие несанкционированному доступу к источникам конфиденциальной информации.

Аппаратные средства защиты информации применяются для решения следующих задач:

- проведение специальных исследований технических средств обеспечения производственной деятельности на наличие возможных каналов утечки информации;
- выявление каналов утечки информации на разных объектах и в помещениях;
- локализация каналов утечки информации;
- поиск и обнаружение средств промышленного шпионажа;
- противодействие несанкционированному доступу к источникам конфиденциальной информации и другим действиям.

По функциональному назначению аппаратные средства могут быть классифицированы на средства обнаружения, средства поиска и детальных измерений, средства активного и пассивного противодействия. При этом по своим техническим возможностям средства защиты информации могут быть общего назначения, рассчитанные на использование непрофессионалами с целью получения предварительных (общих) оценок, и профессиональные комплексы, позволяющие проводить тщательный поиск, обнаружение и прецизионные измерения всех характеристик средств промышленного шпионажа.

Поисковую аппаратуру можно подразделить на аппаратуру поиска средств съема информации и исследования каналов ее утечки. Аппаратура первого типа направлена на поиск и локализацию уже внедренных злоумышленниками средств

несанкционированного доступа. Аппаратура второго типа предназначается для выявления каналов утечки информации.

Программные средства защиты информации включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств − универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки − ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Основные направления защиты информации

Основные направления использования программной защиты информации:

- защита информации от НСД,
- защита программ от копирования,
- защита информации от разрушения,
- защита информации от вредоносных программ,
- защита программ от вредоносных программ,
- программная защита каналов связи.

Программные средства защиты информации можно разделить на следующие:

- *встроенные средства защиты информации;*
- *антивирусная программа* − программа для обнаружения компьютерных вредоносных программ и лечения инфицированных файлов, а также для профилактики − предотвращения заражения файлов или операционной системы вредоносным кодом;
- *межсетевые экраны* (также называемые брандмауэрами или файрволами). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода − это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой;
- *Proxy-servers* (proxy − доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью − маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях − например, на уровне приложения (вредоносные программы, код Java и JavaScript);
- *VPN* (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec;
- системы защиты от НСД:

- средства собственной защиты, предусмотренные общим программным обеспечением;
- средства защиты в составе вычислительной системы;
- средства защиты с запросом информации;
- средства пассивной защиты и т.д.

Криптографические средства защиты позволяют защитить информацию даже после ее перехвата.

Современная криптография является областью знаний, связанной с решением таких проблем безопасности информации, как конфиденциальность, целостность, аутентификация и невозможность отказа сторон от авторства. Достижение этих требований безопасности информационного взаимодействия и составляет основные цели криптографии.

Сертифицированные шифровальные средства, предназначенные для защиты информации, не содержащей сведения, составляющие государственную тайну, по функциональному назначению обеспечивают защиту от прочтения и от НСД к документальной информации при ее передачи по каналу связи, обработке и хранении, а также защиту информации от непосредственного прослушивания в телефонном канале связи. Основная категория программно-аппаратных и программных средств защиты документальной информации, как правило, совмещают в себе функцию шифрования с процедурами выработки и проверки электронной цифровой подписи (ЭЦП).

Программные средства защиты

Встроенные средства защиты ОС

Внутренняя защита Windows 7 и 8 строится по модульному принципу. Встроенные средства защиты ОС – это не один продукт с единой консолью, а взаимодействующие компоненты (представлены в Таблице 1). Условно их можно разделить на три зоны действия:

- первая часть модулей работает во время загрузки системы;
- вторая – во время её работы;
- третья же активируется вручную и помогает дополнительно защитить операционную систему.

Таблица 1. Сводная информация о встроенной защите Windows 7 и Windows 8

	Компонент	Windows 7	Windows 8
Загрузка системы	UEFI	—	+
	ASLR	+	+*
	ELAM	—	+
	Управление автозагрузкой	+	+*
	Вход в систему с помощью альтернативных паролей	—	+
Во время работы	Защитник	+	+*
	Брандмауэр	+	+
	SmartScreen	+	+*
	Запуск приложений в песочнице	—	+
	UAC	+	+
	Подсчёт сетевого трафика	—	
Дополнительно	Родительский контроль	+	+*
	Резервное копирование	+	+
	Шифрование	+	+
	Установка на накопитель	—	+
	Виртуализация	—	+

* − функция реализована лучшим образом.

Защита Windows на этапе загрузки UEFI (Unified Extensible Firmware Interface) − унифицированный расширяемый интерфейс прошивки. По сути, это самостоятельная легкая операционная система, представляющая собой интерфейс между основной ОС и микропрограммами, главной задачей которого является корректная инициализация оборудования и передача управления загрузчику основной («большой») ОС, установленной на компьютере.

Одними из наиболее востребованных особенностей UEFI, которые можно реализовать на работающем под ней компьютере являются: «безопасная загрузка», низкоуровневая криптография, сетевая аутентификация, универсальные

графические драйверы и еще многое другое. В свою очередь, функция Secure Boot в Windows 8 позволяет в процессе загрузки (до запуска операционной системы) организовать проверку всех запускаемых компонентов (драйвера, программы), гарантируя, что только доверенные (с цифровой подписью) программы смогут выполняться в процессе загрузки ОС. Неподписанный код и код без надлежащих сертификатов безопасности блокируется. В случае обнаружения компонента без цифровой подписи автоматически запустится служба Windows Recovery, которая попытается внести изменения в Windows, восстановив нужные системные файлы. Справедливости ради стоит отметить, что эту систему можно обойти, например, подписав вредоносную программу фальшивым сертификатом Microsoft (что уже было пару раз проделано злоумышленниками).

ASLR (Address Space Layout Randomization) – технология рандомизации адресного пространства. Она отвечает за защиту системы от эксплуатации багов в памяти. Технология случайным образом смещает данные и программный код в памяти для более сложной реализации эксплойтов. Разработчики реализовали её и в Windows 7, и в Windows 8, однако в последней она применяется для большего количества компонент.

ELAM (Early-Launch Anti-Malware) – функция раннего запуска защиты от руткитов, эксплойтов и вредоносных программ. За счёт этого антивирусные программы в Windows 8 могут запускаться в процессе загрузки ОС раньше, что позволяет им проверять драйверы, библиотеки и другие компоненты еще до их загрузки. Встроенный «Защитник Windows» по умолчанию использует данную функцию.

Управление автозагрузкой – такая возможность существовала и в Windows 7, однако для её использование требовались знания, отличные от базовых. В новой ОС управление приобрело интуитивно понятный и наглядный интерфейс, став одной из вкладок «Диспетчера задач». Если ранее для правки списка самостоятельно стартующих исполняемых файлов приходилось обращаться к редактору реестра или брать на вооружение утилиту msconfig, то в Windows 8 достаточно открыть соответствующую вкладку менеджера задач. Возможности последнего позволяют отслеживать влияние тех или иных приложений на скорость загрузки ОС и обеспечивают оперативный поиск в Интернете информации о запускаемых без разрешения программах. Все описанные модули работают на старте системы, то есть ещё до того, как пользователь начинает работать на ПК.

Вход в систему с помощью альтернативных паролей – функция, перекочевавшая из мобильных ОС.

Компоненты, использующиеся во время работы системы по своему функциональному наполнению больше всего похожи на антивирусные программы класса Internet Security. Первым из них является Защитник, который появился, начиная с Windows 7, и является встроенным антивирусом. Его возможности изначально не претендовали на обеспечение высокого уровня защиты пользователя и были ориентированы на то, чтобы хватило для защиты до момента покупки реального программного обеспечения от соответствующих производителей. Помимо этого без подобного рода защиты его машина представляет собой угрозу окружающим (будучи заражённой, она может стать частью ботнета, участвовать в рассылке спама и т.д.). Поэтому и нужна как минимум антивирусная программа хотя бы минимального базового уровня, чтобы снизить угрозу от компьютера такого пользователя для окружающих. Таковы были мотивы корпорации, разработавшей Защитника Windows и Microsoft Essentials в дополнение к нему.

Таблица 2. Сравнение функциональности Защитника Windows 7 и Windows 8

	Защитник Windows 7	Защитник Windows 8
Файловая защита в реальном времени	+	+
Проверка архивов	+	+
Проверка съёмных носителей	+	+
Проверка корреспонденции по популярным почтовым протоколам (POP3, SMTP и др.)	+	—
Проверка по расписанию	+	—
Сигнатурный анализ	+*	+
Эвристический анализ	+	+
Поведенческий анализ	—	—
Карантин	+	+
Облачные технологии	Microsoft SpyNet	MAPS

* − функция реализована лучшим образом.

Брандмауэр – встроенный в Windows межсетевой экран.

Репутационный фильтр SmartScreen. SmartScreen автоматически сканирует все исполняемые exe-файлы, которые пользователь загружает из сети Интернет. Также выступает в роли веб-экрана, синхронизируясь с серверами Microsoft для обновления баз неблагонадёжных сайтов, т.е. позволяет выполнять репутационную проверку сайтов. В Windows 7 существовал только как надстройка безопасности Internet Explorer. В Windows 8 работа модуля была перенесена на уровень операционной системы, тем самым отвязав компонент от конкретного браузера. При запуске загруженного файла, SmartScreen сканирует его и отправляет его цифровую подпись на серверы Microsoft. В случае если цифровая подпись соответствует хорошо известному приложению, система запускает его. Если о приложении мало что известно, или оно состоит в списке неблагонадежных, Windows 8 сообщит об этом, а в случае угрозы безопасности не станет запускать приложение без принудительных действий со стороны пользователя.

Запуск приложений из песочницы. Приложения для нового интерфейса Windows 8 Metro выполняются в «песочнице», т.е. не могут выполнять никаких действий, кроме прямо им разрешенных. Для сравнения, приложения для рабочего стола имеют полный доступ к системе. Например, если Вы скачали и запустили игру, она может установить дополнительные драйверы в операционной системе, прочесть любые файлы с жесткого диска, и проделать другие изменения. Особенно это касается процесса установки, который обычно запускается с привилегиями администратора. Приложения Windows 8 работают несколько иным способом. Данные программы не могут скрытно работать в операционной системе, записывая все Ваши действия, пароли, также они не обладают доступом к любому файлу на Вашем компьютере. Также нужно отметить, что приложения Windows 8 могут быть установлены только из магазина приложений Windows.

UAC (User Account Control) – известный компонент, который запрашивает подтверждение действий, если программе для выполнения требуются права администратора.

Подсчёт сетевого трафика – этот инструмент по умолчанию встроен в Windows 8 (в настройках сетевого соединения в контекстном меню выбрать пункт «Отображать сведения о предполагаемом использовании данных»). Для решения аналогичной задачи в Windows 7 приходится прибегать к сторонним программам или виджетам. Его связь с безопасностью косвенна. К примеру, если вы не

работаете за компьютером (и никаких обновлений не запущено), а активность трафика присутствует, возможно, это действия какой-нибудь вредоносной программы.

Следующие функции активируются пользователями довольно редко.

Родительский контроль. В представлении Microsoft должен включать в себя контроль проведённого времени за компьютером, контроль запуска приложений и игр, контроль посещаемых сайтов, а также ведение отчётности по каждому из направлений. В Windows 7 родительский контроль был тесно интегрирован с Windows Live, требовал дополнительной регистрации в этой службе. По сути, был полностью «завязан» на ней. В Windows 8 модуль стал «отвязанным», то есть не требующим дополнительной регистрации в Windows Live. Всё можно настраивать прямо в системе. Тем не менее, компонент по прежнему связывается с серверами Microsoft для обновления своих баз (возрастные ограничения в играх, сайты с «взрослым» контентом и т.п.).

Резервное копирование и восстановление данных. Основные компоненты системы:

- *История файлов (File History)* - создание локальных копий пользовательских данных

Компонент «История файлов» в Windows 8 позволяет организовывать непрерывные дополнительные резервные копии отобранных пользователем файлов в режиме реального времени. Созданные резервные копии хранятся на сетевом диске или переносном USB-накопителе. Если оригинальный файл был поврежден или случайно удален, его можно очень просто восстановить с помощью копии, созданной данным компонентом.

- *OneDrive* - удаленное резервное копирование пользовательских данных

Локальные копии критически необходимы, но в то же время они имеют очень важный недостаток: событие, которое может повредить компьютер или переносной накопитель, содержащие рабочие копии файлов может также привести к потере резервных копий. Решением данной проблемы может стать облачное резервное копирование, которое подразумевает хранение важных файлов на полностью защищенных файловых серверах, физически удаленных от вашего компьютера.

- *Резервная копия образа системы*

Windows 8 включает отдельные инструменты для создания резервных копий системы и восстановления ОС. Опция обновления позволяет выполнять переустановку системы, не затрагивая большинство пользовательских файлов. Сброс системы восстанавливает абсолютно чистую ОС с заводскими настройками.

Шифрование. За это отвечает BitLocker. Все данные на внешнем накопителе или переносном винчестере USB зашифровываются и при попытке открыть их требуется ввести придуманный ключ. Если добавляются новые файлы, они автоматически зашифровываются, при копировании файлов владельцем на другой носитель информации файлы автоматически расшифровываются.

Установка на накопитель. Нововведение в Windows 8 в виде функции Windows To Go, которая позволяет записать образ системы на флешку и получать доступ к привычному рабочему окружению практически на любом имеющемся под рукой компьютере. С точки зрения безопасности эта встроенная функция позволила штатными средствами создавать LiveUSB.

Виртуализация. Ещё одна новая встроенная функция Windows 8. Новая функциональность задействована в 64-разрядных сборках операционной системы и

может быть активирована только при наличии в компьютере процессора с поддержкой аппаратной виртуализации и механизма трансляции адресов второго уровня SLAT (Second Level Address Translation). Для включения VM-инструментария нужно в окне настройки компонентов Windows отметить флажком пункт Hyper-V и произвести установку дополнительного программного модуля. Тем самым, получаем полноценное средство для создания и управления виртуальными машинами. В качестве гостевых систем могут быть использованы не только клиентские и серверные продукты Microsoft, но и решения на базе Linux, развертывание которых может производиться без дополнительной правки пользователем конфигурационных файлов и параметров. В частности, встроенные средства виртуализации Windows 8 поддерживают Ubuntu. Это может оказаться хорошим подспорьем для любителей интернет-сёрфинга, т.к. большинство вредоносных программ являются Windows-ориентированными.

Идентификация и аутентификация

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности. Идентификация и аутентификация − это первая линия обороны, «проходная» информационного пространства организации.

Идентификация позволяет субъекту − пользователю или процессу, действующему от имени определенного пользователя, назвать себя, сообщив свое имя. Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого себя выдает. В качестве синонима слова «аутентификация» иногда используют сочетание «проверка подлинности». Субъект может подтвердить свою подлинность, если предъявит по крайней мере одну из следующих сущностей:

- нечто, что он знает: пароль, личный идентификационный номер, криптографический ключ и т.п.;
- нечто, чем он владеет: личную карточку или иное устройство аналогичного назначения;
- нечто, что является частью его самого: голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики;
- нечто, ассоциированное с ним, например координаты.

Главное достоинство парольной аутентификации − простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее по совокупности характеристик их следует признать самым слабым средством проверки подлинности. Надежность паролей основывается на способности помнить их и хранить в тайне. Ввод пароля можно подсмотреть. Пароль можно угадать методом грубой силы, используя, быть может, словарь. Если файл паролей зашифрован, но доступен на чтение, его можно перекачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор.

Пароли уязвимы по отношению к электронному перехвату − это наиболее принципиальный недостаток, который нельзя компенсировать улучшением администрирования или обучением пользователей. Практически единственный выход − использование криптографии для шифрования паролей перед передачей по линиям связи.

Тем не менее, следующие меры позволяют значительно повысить надежность парольной защиты:

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
- управление сроком действия паролей, их периодическая смена;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему, что затруднит применение метода грубой силы;
- обучение и воспитание пользователей;
- использование программных генераторов паролей, которые, основываясь на несложных правилах, могут порождать только благозвучные и, следовательно, запоминающиеся пароли.

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации, основанные, например, на применении токенов.

Токен − это предмет или устройство, владение которым подтверждает подлинность пользователя. Различают токены с памятью (пассивные, которые только хранят, но не обрабатывают информацию) и интеллектуальные токены (активные).

Самой распространенной разновидностью токенов с памятью являются карточки с магнитной полосой. Для использования подобных токенов необходимо устройство чтения, снабженное также клавиатурой и процессором. Обычно пользователь набирает на этой клавиатуре свой личный идентификационный номер, после чего процессор проверяет его совпадение с тем, что записано на карточке, а также подлинность самой карточки. Таким образом, здесь фактически применяется комбинация двух способов защиты, что существенно затрудняет действия злоумышленника.

Необходима обработка аутентификационной информации самим устройством чтения, без передачи в компьютер − это исключает возможность электронного перехвата.

Иногда (обычно для физического контроля доступа) карточки применяют сами по себе, без запроса личного идентификационного номера.

Как известно, одним из самых мощных средств в руках злоумышленника является изменение программы аутентификации, при котором пароли не только проверяются, но и запоминаются для последующего несанкционированного использования.

Интеллектуальные токены характеризуются наличием собственной вычислительной мощности. Они подразделяются на интеллектуальные карты, стандартизованные ISO и прочие токены. Карты нуждаются в интерфейсном устройстве, прочие токены обычно обладают ручным интерфейсом (дисплеем и клавиатурой) и по внешнему виду напоминают калькуляторы. Чтобы токен начал работать, пользователь должен ввести свой личный идентификационный номер.

По принципу действия интеллектуальные токены можно разделить на следующие категории:

- Статический обмен паролями: пользователь обычным образом доказывает токену свою подлинность, затем токен проверяется компьютерной системой;
- Динамическая генерация паролей: токен генерирует пароли, периодически изменяя их. Компьютерная система должна иметь синхронизированный генератор паролей. Информация от токена поступает по электронному интерфейсу или набирается пользователем на клавиатуре терминала;

- Запросно-ответные системы: компьютер выдает случайное число, которое преобразуется криптографическим механизмом, встроенным в токен, после чего результат возвращается в компьютер для проверки. Здесь также возможно использование электронного или ручного интерфейса. В последнем случае пользователь читает запрос с экрана терминала, набирает его на клавиатуре токена (возможно, в это время вводится и личный номер), а на дисплее токена видит ответ и переносит его на клавиатуру терминала.

Управление доступом

Средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты − пользователи и процессы могут выполнять над объектами − информацией и другими компьютерными ресурсами. Речь идет о логическом управлении доступом, который реализуется программными средствами. Логическое управление доступом − это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность путем запрещения обслуживания неавторизованных пользователей. Задача логического управления доступом состоит в том, чтобы для каждой пары (субъект, объект) определить множество допустимых операций, зависящее от некоторых дополнительных условий, и контролировать выполнение установленного порядка. Простой пример реализации таких прав доступа – какой-то пользователь (субъект) вошедший в информационную систему получил право доступа на чтение информации с какого-то диска (объект), право доступа на модификацию данных в каком-то каталоге (объект) и отсутствие всяких прав доступа к остальным ресурсам информационной системы.

Контроль прав доступа производится разными компонентами программной среды − ядром операционной системы, дополнительными средствами безопасности, системой управления базами данных, посредническим программным обеспечением (таким как монитор транзакций) и т.д.

Протоколирование и аудит

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационной системе. Например − кто и когда пытался входить в систему, чем завершилась эта попытка, кто и какими информациоными ресурсами пользовался, какие и кем модифицировались информационные ресурсы и много других.

Аудит − это анализ накопленной информации, проводимый оперативно, почти в реальном времени, или периодически.

Реализация протоколирования и аудита преследует следующие главные цели:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Антивирусная защита

Основной и по совместительству обязательный элемент в антивирусной защите − это, безусловно, антивирусная программа. Без нее нельзя говорить об эффективной антивирусной безопасности, если речь идет о компьютере, способном обмениваться информацией с другими внешними источниками. Даже соблюдение

пользователем всех правил компьютерной гигиены не гарантирует отсутствие вредоносных программ, если при этом не используется антивирус.

Антивирусное программное обеспечение − это достаточно сложный программный комплекс, для его создания требуются усилия команды высококвалифицированных вирусных аналитиков, экспертов и программистов с многолетним опытом и весьма специфическими знаниями и умениями. Основная технология антивирусной проверки − сигнатурный анализ подразумевает непрерывную работу по мониторингу вирусных инцидентов и регулярный выпуск обновлений антивирусных баз. Ввиду этих и других причин, антивирусные программы не встраиваются в операционные системы. Встроенным может быть только простейший фильтр, не обеспечивающий полноценной антивирусной проверки.

Меры защиты:

- Профилактика, к профилактическим средствам относятся:
  - перекрытие путей проникновения вредоносных программ в компьютер;
  - исключение возможности заражения и порчи вредоносными программами, проникшими в компьютер, других файлов.
- Диагностика:
  - диагностические средства позволяют обнаруживать вредоносные программы в компьютере и распознавать их тип.
- Лечение:
  - лечение состоит в удалении вредоносных программ из зараженных программных средств и восстановлении пораженных файлов.

Защитный комплекс основывается на применении антивирусных программ и проведении организационных мероприятий.

Организационные мероприятия

Вредоносные программы попадают в компьютер только вместе с программным обеспечением. Поэтому самым важным в защите от вредоносных программ является использование незараженных программ, так как главным источником вредоносных программ являются незаконные, так называемые «пиратские» копии программного обеспечения.

Методы антивирусной защиты

Программные средства антивирусной защиты обеспечивают диагностику (обнаружение) и лечение (нейтрализацию) вредоносных программ.

Из всех методов антивирусной защиты можно выделить две основные группы:

- Сигнатурные методы − точные методы обнаружения вредоносных программ, основанные на сравнении файла с известными образцами вредоносных программ.
- Эвристические методы − приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.
- Комбинированные.

Сигнатурный анализ

Слово сигнатура в данном случае является калькой на английское signature, означающее «подпись» или же в переносном смысле «характерная черта, нечто идентифицирующее». Собственно, этим все сказано. Сигнатурный анализ заключается в выявлении характерных идентифицирующих черт каждой

вредоносной программы и поиска вредоносных программ путем сравнения файлов с выявленными чертами.

Сигнатурой вредоносной программы будет считаться совокупность черт, позволяющих однозначно идентифицировать наличие вредоносной программы в файле (включая случаи, когда файл целиком является вредоносной программой). Все вместе сигнатуры известных вредоносных программ составляют антивирусную базу.

Задачу выделения сигнатур, как правило, решают люди − эксперты в области компьютерной вирусологии, способные выделить код вредоносной программы из кода программы и сформулировать его характерные черты в форме, наиболее удобной для поиска. Как правило, потому что в наиболее простых случаях могут применяться специальные автоматизированные средства выделения сигнатур. Например, в случае несложных по структуре троянов или червей, которые не заражают другие программы, а целиком являются вредоносными программами.

Практически в каждой компании, выпускающей антивирусы, есть своя группа экспертов, выполняющая анализ новых вредоносных программ и пополняющая антивирусную базу новыми сигнатурами. По этой причине антивирусные базы в разных антивирусах отличаются. Тем не менее, между антивирусными компаниями существует договоренность об обмене образцами вредоносных программ, а значит рано или поздно сигнатура новой вредоносной программы попадает в антивирусные базы практически всех антивирусов. Лучшим же антивирусом будет тот, для которого сигнатура новой вредоносной программы была выпущена раньше всех.

Одно из распространенных заблуждений насчет сигнатур заключается в том, каждая сигнатура соответствует ровно одной вредоносной программе. И как следствие, антивирусная база с большим количеством сигнатур позволяет обнаруживать больше вредоносных программ. На самом деле это не так. Очень часто для обнаружения семейства похожих вредоносных программ используется одна сигнатура, и поэтому считать, что количество сигнатур равно количеству обнаруживаемых вредоносных программ, уже нельзя.

Соотношение количества сигнатур и количества известных вредоносных программ для каждой антивирусной базы свое и вполне может оказаться, что база с меньшим количеством сигнатур в действительности содержит информацию о большем количестве вредоносных программ. Если же вспомнить, что антивирусные компании обмениваются образцами вредоносных программ, можно с высокой долей уверенности считать, что антивирусные базы наиболее известных антивирусных программ эквивалентны.

Важное дополнительное свойство сигнатур − точное и гарантированное определение типа вредоносной программы. Это свойство позволяет занести в базу не только сами сигнатуры, но и способы лечения вредоносной программы. Если бы сигнатурный анализ давал только ответ на вопрос, есть вредоносная программа или нет, но не давал ответа, что это за вредоносная программа, очевидно, лечение было бы не возможно − слишком большим был бы риск совершить не те действия и вместо лечения получить дополнительные потери информации.

Другое важное, но уже отрицательное свойство − для получения сигнатуры необходимо иметь образец вредоносной программы. Следовательно, сигнатурный метод непригоден для защиты от новых вредоносных программ, т. к. до тех пор, пока вредоносная программа не попала на анализ к экспертам, создать её сигнатуру невозможно. Именно поэтому все наиболее крупные эпидемии вызываются

новыми вредоносными программами. С момента появления вредоносной программы в сети Интернет до выпуска первых сигнатур обычно проходит несколько часов, и все это время вредоносная программа способна заражать компьютеры почти беспрепятственно. Почти − потому что в защите от новых вредоносных программ помогают дополнительные средства защиты, рассмотренные ранее, а также эвристические методы, используемые в антивирусных программах.

Эвристический анализ

Слово «эвристика» происходит от греческого глагола «находить». Суть эвристических методов состоит в том, что решение проблемы основывается на некоторых правдоподобных предположениях, а не на строгих выводах из имеющихся фактов и предпосылок. Поскольку такое определение звучит достаточно сложно и непонятно, проще объяснить на примерах различных эвристических методов.

Если сигнатурный метод основан на выделении характерных признаков вредоносной программы и поиске этих признаков в проверяемых файлах, то эвристический анализ основывается на (весьма правдоподобном) предположении, что новые вредоносные программы часто оказываются похожи на какие-либо из уже известных. Постфактум такое предположение оправдывается наличием в антивирусных базах сигнатур для определения не одного, а сразу нескольких вредоносных программ. Основанный на таком предположении эвристический метод заключается в поиске файлов, которые не полностью, но очень близко соответствуют сигнатурам известных вредоносных программ.

Положительным эффектом от использования этого метода является возможность обнаружить новые вредоносные программы еще до того, как для них будут выделены сигнатуры. Отрицательные стороны:

- Вероятность ошибочно определить наличие в файле вредоносной программы, когда на самом деле файл чист − такие события называются ложными срабатываниями
- Невозможность лечения − и в силу возможных ложных срабатываний, и в силу возможного неточного определения типа вредоносной программы, попытка лечения может привести к большим потерям информации, чем сама вредоносная программа, а это недопустимо
- Низкая эффективность − против действительно новаторских вредоносных программ, вызывающих наиболее масштабные эпидемии, этот вид эвристического анализа малопригоден

Поиск вредоносных программ, выполняющих подозрительные действия

Другой метод, основанный на эвристике, исходит из предположения, что вредоносные программы так или иначе стремятся нанести вред компьютеру. Метод основан на выделении основных вредоносных действий, таких как, например:

- удаление файла;
- запись в файл;
- запись в определенные области системного реестра;
- открытие порта на прослушивание;
- перехват данных вводимых с клавиатуры;
- рассылка писем;
- и др.

Понятно, что выполнение каждого такого действия по отдельности не является поводом считать программу вредоносной. Но если программа

последовательно выполняет несколько таких действий, например, записывает запуск себя же в ключ автозапуска системного реестра, перехватывает данные вводимые с клавиатуры и с определенной частотой пересылает эти данные на какой-то адрес в Интернет, значит эта программа, по меньшей мере, подозрительна. Основанный на этом принципе эвристический анализатор должен постоянно следить за действиями, которые выполняют программы.

Преимуществом описанного метода является возможность обнаруживать неизвестные ранее вредоносные программы, даже если они не очень похожи на уже известные. Например, новая вредоносная программа может использовать для проникновения на компьютер новую уязвимость, но после этого начинает выполнять уже привычные вредоносные действия. Такую программу может пропустить эвристический анализатор первого типа, но вполне может обнаружить анализатор второго типа.

Отрицательные черты те же, что и раньше:

- Ложные срабатывания
- Невозможность лечения
- Невысокая эффективность

Дополнительные средства

Практически любой антивирус сегодня использует все известные методы обнаружения вредоносных программ. Но одних средств обнаружения мало для успешной работы антивируса, для того, чтобы чисто антивирусные средства были эффективными, нужны дополнительные модули, выполняющие вспомогательные функции.

Модуль обновления

В первую очередь, каждый антивирус должен содержать модуль обновления. Это связано с тем, что основным методом обнаружения вредоносных программ сегодня является сигнатурный анализ, который полагается на использование антивирусной базы. Для того чтобы сигнатурный анализ эффективно справлялся с самыми последними вредоносными программами, антивирусные эксперты постоянно анализируют образцы новых вредоносных программ и выпускают для них сигнатуры. После этого главной проблемой становится доставка сигнатур на компьютеры всех пользователей, использующих соответствующую антивирусную программу.

Именно эту задачу и решает модуль обновления. После того, как эксперты создают новые сигнатуры, файлы с сигнатурами размещаются на серверах компании − производителя антивируса и становятся доступными для загрузки. Модуль обновления обращается к этим серверам, определяет наличие новых файлов, загружает их на компьютер пользователя и дает команду антивирусным модулям использовать новые файлы сигнатур.

Модули обновления разных антивирусов весьма похожи друг на друга и отличаются типами серверов, с которых они могут загружать файлы обновлений, а точнее, типами протоколов, которые они могут использовать при загрузке − HTTP, FTP, протоколы локальных Windows-сетей. Некоторые антивирусные компании создают специальные протоколы для загрузки своих обновлений антивирусной базы. В таком случае модуль обновления может использовать и этот специальный протокол.

Второе, в чем могут отличаться модули обновления − это настройка действий, на случай, если источник обновлений недоступен. Например, в некоторых модулях обновления можно указать не один адрес сервера с

обновлениями, а адреса нескольких серверов, и модуль обновления будет обращаться к ним по очереди, пока не обнаружит работающий сервер. Или же в модуле обновления может быть настройка − повторять попытки обновления с заданным интервалом определенное количество раз или же до тех пор, пока сервер не станет доступным. Эти две настройки могут присутствовать и одновременно.

Модуль планирования

Второй важный вспомогательный модуль − это модуль планирования. Существует ряд действий, которые антивирус должен выполнять регулярно: в частности, проверять весь компьютер на наличие вредоносных программ и обновлять антивирусную базу. Модуль планирования как раз и позволяет настроить периодичность выполнения этих действий.

Для обновления антивирусной базы рекомендуется использовать небольшой интервал − один час или три часа, в зависимости от возможностей канала доступа в Интернет. В настоящее время новые модификации вредоносных программ обнаруживаются постоянно, что вынуждает антивирусные компании выпускать новые файлы сигнатур буквально каждый час. Если пользователь компьютера много времени проводит в Интернете, он подвергает свой компьютер большому риску и поэтому должен обновлять антивирусную базу как можно чаще.

Полную проверку компьютера нужно проводить хотя бы потому, что сначала появляются новые вредоносные программы, а только потом сигнатуры к ним, а значит всегда есть возможность загрузить на компьютер вредоносную программу раньше, чем обновление антивирусных баз. Чтобы обнаружить эти вредоносные программы, компьютер нужно периодически перепроверять. Разумным расписанием для проверки компьютера можно считать раз в неделю.

Исходя из сказанного, основная задача модуля планирования − давать возможность выбрать для каждого действия расписание, которое больше всего подходит именно для этого типа действия. Следовательно, модуль обновления должен поддерживать много различных вариантов расписания из которых можно было бы выбирать.

Модуль управления

По мере увеличения количества модулей в антивирусной программе возникает необходимость в дополнительном модуле для управления и настройки. В простейшем случае − это общий интерфейсный модуль, при помощи которого можно в удобной форме получить доступ к наиболее важным функциям:

- настройке параметров антивирусных модулей;
- настройке обновлений;
- настройке периодического запуска обновления и проверки;
- запуску модулей вручную, по требованию пользователя;
- отчетам о проверке;
- другим функциям, в зависимости от конкретной антивирусной программы.

Основные требования к такому модулю − удобный доступ к настройкам, интуитивная понятность, подробная справочная система, описывающая каждую настройку, возможность защитить настройки от изменений, если за компьютером работает несколько человек. Подобным модулем управления обладают все антивирусные программы для домашнего использования. Антивирусные программы для защиты компьютеров в крупных сетях должны обладать несколько иными свойствами.

Уже не раз говорилось, что в большой организации за настройку и правильное функционирование антивирусной программы отвечают не

пользователи компьютеров, а специальные сотрудники. Если компьютеров в организации много, то каждому ответственному за безопасность сотруднику придется постоянно бегать от одного компьютера к другому, проверяя правильность настройки и просматривая историю обнаруженных заражений. Это очень неэффективный подход к обслуживанию системы безопасности.

Поэтому, чтобы упростить работу администраторов антивирусной безопасности, антивирусные программы, которые используются для защиты больших сетей, оборудованы специальным модулем управления. Основные свойства этого модуля управления:

- Поддержка удаленного управления и настройки − администратор безопасности может запускать и останавливать антивирусные модули, а также менять их настройки по сети, не вставая со своего места
- Защита настроек от изменений − модуль управления не позволяет локальному пользователю изменять настройки или останавливать антивирусную программу, чтобы пользователь не мог ослабить антивирусную защиту организации

Это далеко не все требования к управлению антивирусной защитой в крупной организации, а только основные принципы. Подробнее об особенностях антивирусной защиты сетей и требованиях к модулям управления будет рассказано позже в соответствующем разделе.

Карантин

Среди прочих вспомогательных средств во многих антивирусных программах есть специальные технологии, которые защищают от возможной потери данных в результате действий антивирусной программы.

Например, легко представить ситуацию, при которой файл детектируется как возможно зараженный эвристическим анализатором и удаляется согласно настройкам антивирусной программы. Однако эвристический анализатор никогда не дает стопроцентной гарантии того, что файл действительно заражен, а значит с определенной вероятностью антивирусная программа могла удалить незараженный файл.

Или же антивирусная программа обнаруживает важный документ зараженный вредоносной программой и пытается согласно настройкам выполнить лечение, но по каким-то причинам происходит сбой и вместе с вылеченной вредоносной программой теряется важная информация.

Разумеется, от таких случаев желательно застраховаться. Проще всего это сделать, если перед лечением или удалением файлов сохранить их резервные копии, тогда если окажется, что файл был удален ошибочно или была потеряна важная информация, всегда можно будет выполнить восстановление из резервной копии.

Виды антивирусных программ

Программы-детекторы

Программы-детекторы обеспечивают поиск и обнаружение вредоносных программ в оперативной памяти и на внешних носителях, и при обнаружении выдают соответствующее сообщение. Различают детекторы универсальные и специализированные.

- Универсальные детекторы в своей работе используют проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной

суммы. Недостаток универсальных детекторов связан с невозможностью определения причин искажения файлов.

- Специализированные детекторы выполняют поиск известных вредоносных программ по их сигнатуре (повторяющемуся участку кода). Недостаток таких детекторов состоит в том, что они неспособны обнаруживать все известные вредоносные программы. Детектор, позволяющий обнаруживать несколько вредоносных программ, называют полидетектором. Недостатком таких антивирусных программ является то, что они могут находить только те вредоносные программы, которые известны разработчикам таких программ.

Программы-доктора

Программы-доктора (фаги), не только находят зараженные вредоносными программы файлы, но и «лечат» их, т.е. удаляют из файла тело вредоносной программ, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вредоносные программы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вредоносных программ.

Учитывая, что постоянно появляются новые вредоносные программы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление их версий.

Программы-ревизоры

Программы-ревизоры относятся к самым надежным средствам защиты от вредоносных программ. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вредоносной программой, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран видеомонитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры.

Программы-ревизоры имеют достаточно развитые алгоритмы, могут даже отличить изменения версии проверяемой программы от изменений, внесенных вредоносной программой.

Программы-фильтры

Программы-фильтры (сторожа) представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вредоносных программ. Такими действиями могут являться:

- попытки коррекции файлов с расширениями COM и EXE;
- изменение атрибутов файлов;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так

как способны обнаружить вредоносную программу на самой ранней стадии её существования до размножения.

Однако они не «лечат» файлы и диски. Для уничтожения вредоносных программ требуется применить другие программы, например фаги. К недостаткам программ-сторожей можно отнести их «назойливость» (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением.

Поскольку функции детектора, ревизора и сторожа дополняют друг друга, то в современные антивирусные комплекты программ обычно входят компоненты, реализующие все эти функции. При этом часто функции детектора и ревизора совмещаются в одной программе.

Вакцины

Вакцины (иммунизаторы) – это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» эту вредоносную программу. Вакцинация возможна только от известных вредоносных программ. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вредоносная программа будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

Существенным недостатком таких программ является их ограниченные возможности по предотвращению заражения от большого числа разнообразных вредоносных программ.

Режимы проверки и обновление

Основные элементы любой антивирусной защиты рабочей станции или сетевого сервера − это постоянная проверка в режиме реального времени, проверка по требованию и механизм обновления антивирусных баз.

Проверка в режиме реального времени

Как правило, на домашнем компьютере происходит постоянный обмен информацией с внешними источниками: файлы загружаются из сети Интернет, копируются с компакт дисков или по домашней локальной сети и впоследствии открываются и запускаются. Следовательно, главное средство в арсенале антивирусной защиты домашнего компьютера − проверка в режиме реального времени. Ее задача − не допустить заражения системы.

На домашнем компьютере настоятельно рекомендуется использовать постоянную проверку всегда, когда он включен − вне зависимости от того, подключен ли он в данный момент к сети, используются ли чужие мобильные носители информации или выполняются только какие-либо внутренние задачи. Постоянная проверка характеризуется минимальными системными требованиями, необходимыми ей в работе, и поэтому запущенный в этом режиме антивирус в подавляющем большинстве случаев остается пользователем незамеченным и проявляется только при обнаружении вредоносных программ или других подозрительных программ.

Без особого ущерба качеству антивирусной защиты домашнего компьютера часто из проверки в режиме реального времени можно исключить проверку исходящих почтовых сообщений и архивов, однако все остальные объекты рекомендуется проверять.

Проверка по требованию

Как упоминалось выше, на домашнем компьютере часто происходит обмен информацией с помощью компакт дисков, дискет и других мобильных носителей информации: устанавливаются новые игры, копируются электронные книги и учебники, переписываются фильмы и музыка. Для того чтобы обнаружить проникший в систему вредоносный код, используется проверка по требованию. Всем домашним пользователям настоятельно рекомендуется проверять на наличие вредоносных программ все подозрительные носители информации, причем каждый раз перед тем как начать чтение или копирование с них файлов. Это простое действие занимает немного времени, но позволяет существенно сократить вероятность проникновения вредоносной программы на компьютер. Дополнительно рекомендуется не реже одного раза в неделю проверять на наличие вредоносных программ весь жесткий диск.

По настройкам проверок этот режим отличается особой тщательностью − в проверке по требованию обычно проверяются все объекты файловой системы.

Обновление антивирусных баз

Только своевременное обновление антивирусных баз может гарантировать правильную и эффективную работу наиболее надежной части антивирусной защиты − сигнатурного анализа.

Антивирусные базы − это файлы, содержащие сигнатуры вредоносных программ. Они выпускаются компаниями-производителями антивирусов и соответственно для разных программ они различны − например, Антивирус Касперского не сможет работать с базами антивируса Dr. Web и наоборот.

Получить самые последние версии нужных баз можно с веб-сайта компании-производителя с помощью встроенных в антивирусную программу средств, либо самостоятельно скопировав файлы с веб-сайта. В штатных ситуациях обновляться рекомендуется первым способом, второй − более сложный и предназначен для неординарных ситуаций, например при подозрении на неправильную работу встроенных модулей обновления или невозможности прямого выхода в Интернет.

Это означает, что для обновления антивирусных баз домашнему пользователю обычно достаточно соединиться с сетью Интернет и нажать в интерфейсе антивирусной программы кнопку, запускающую процесс обновления. Если же подключение к Интернет не предусмотрено, единственный выход − это зайти на сайт производителя антивируса с помощью другого компьютера, загрузить и скопировать базы на свой компьютер с помощью мобильного носителя. Подробное описание этой процедуры можно найти в руководстве пользователя или документации к программе.

Межсетевые экраны

Межсетевой экран (МЭ) − комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача − не пропускать пакеты, не подходящие под критерии, определённые в конфигурации.

Основные компоненты и технологии

- сетевая политика безопасности;
- усиленная аутентификация;
- централизованное управление;
- подсистема сбора статистики и предупреждения об атаке;
- простой фильтр пакетов;
- посредник уровня соединения;
- посредник прикладного уровня;
- пакетный фильтр инспекционного типа.

Сетевая политика безопасности

Существует два уровня сетевой политики безопасности, непосредственно влияющих на разработку, установку и использование МЭ. Политика более высокого уровня (принцип работы) определяет те службы, использование которых будет разрешено или явно исключено, как эти службы будут использоваться, и возможные исключения из этих правил. Политика более низкого уровня (режим доступа к службам) описывает, как фактически МЭ будет осуществлять фильтрацию и ограничение доступа к службам, определенным в политике более высокого уровня.

Принцип работы определяет наличие или отсутствие доступа к службам. Эти принципы нельзя разрабатывать без учета возможностей и ограничений, присущих конкретному МЭ, а также угроз, связанных с TCP/IP. Обычно МЭ реализует одну из двух основных политик: разрешено все, что не запрещено, или запрещено все, что не разрешено.

МЭ, реализующий первую политику, разрешает доступ всем службам, за исключением тех, которые явно определены как запрещенные. МЭ, реализующий вторую политику, по умолчанию отказывает во всех услугах, кроме тех которые явно определены как разрешенные. Эта политика представляет собой реализацию классической модели доступа, используемой во всех областях информационной безопасности.

Политика нижнего уровня состоит из описания порядка доступа к службам сети Интернет, а также касается ограничения внешнего доступа к сети (с помощью PPP, SLIP, dial-in доступ). Эта политика должна быть расширением общей организационной политики защиты информационных ресурсов. Для успешной работы МЭ политика доступа к службам должна быть безопасной, регламентированной и реалистичной.

Усиленная аутентификация

Аутентификация является одним из самых важных компонентов МЭ. Прежде чем пользователю из внешней сети будет предоставлено право получить

тот или иной сервис, не являющийся общедоступным, необходимо убедиться, что он действительно тот, за кого себя выдает (предполагается, что этот сервис для данного пользователя разрешен). Авторизация обычно рассматривается в контексте аутентификации − как только пользователь аутентифицирован (т.е. подтверждена его подлинность), для него определяются разрешенные ему сервисы. При получении запроса на использование сервиса от имени какого-либо пользователя, МЭ проверяет, какой способ аутентификации определен для данного пользователя и передает управление серверу аутентификации (точнее, программе, реализующей функции аутентификации). После получения положительного ответа МЭ формирует (или разрешает) запрашиваемое пользователем соединение.

При аутентификации используется, как правило, принцип, основанный на «знаниях» − пользователь знает некоторое секретное слово (парольную фразу), которое он посылает серверу аутентификации в ответ на его запрос. Одной из схем аутентификации является использование стандартных UNIX-паролей. Эта схема является наиболее уязвимой с точки зрения безопасности − пароль может быть перехвачен и использован другим лицом. Чаще всего используются схемы с применением одноразовых паролей на основе. Даже будучи перехваченным, этот пароль будет бесполезен при следующей регистрации, а получение следующего пароля из предыдущего является вычислительно трудноразрешимой задачей. Для генерации одноразовых паролей используются как программные, так и аппаратные генераторы, представляющие собой устройства, вставляемые в слот компьютера. Знание секретного слова-пароля необходимо пользователю для приведения этого устройства в действие.

Ряд МЭ поддерживает систему Kerberos − один из наиболее распространенных методов аутентификации. Некоторые схемы требуют изменения клиентского программного обеспечения − шаг, который далеко не всегда приемлем. Как правило, все коммерческие МЭ поддерживают несколько различных схем, позволяя администратору сделать наиболее удобный для конкретных условий выбор. Одной из наиболее простых систем, не требующих дополнительных затрат на оборудование, но в то же время обеспечивающих хороший уровень защиты, является S/Key.

Кроме аутентификации с помощью одноразовых паролей все большее количество МЭ поддерживают режим аутентификации с помощью специальных интеллектуальных карт, предназначенных именно для цели аутентификации пользователя (например, с помощью карточек SecurID фирмы SecurDynamics).

Централизованное управление

Легкость администрирования является одним из ключевых аспектов при создании эффективной и надежной системы защиты. Так как безопасность всей защищаемой локальной сети зависит в основном от возможностей МЭ, установленного на границе между данной внутренней сетью и внешней глобальной сетью, то управлять безопасностью всей защищаемой локальной сети можно централизованно. Подобная возможность МЭ, наряду с очевидными достоинствами, таит в себе и большую опасность. Ошибки при определении правил доступа могут образовать лазейку, через которую рано или поздно будет взломана любая система защищаемой сети (в случае если данная система не «закрывает» данную лазейку самостоятельно). Поэтому в большинстве МЭ реализованы сервисные утилиты, облегчающие ввод, удаление и просмотр набора правил. Наличие этих утилит позволяет также производить проверки на синтаксические или логические ошибки при вводе или редактировании правил.

Обычно эти утилиты позволяют просматривать информацию, сгруппированную по каким-либо критериям (например, все, что относится к конкретному пользователю или сервису).

Подсистема сбора статистики и предупреждения об атаке

Еще одним важным компонентом МЭ является система сбора статистики и предупреждения об атаке. Информация обо всех событиях − отказах, входящих, выходящих соединениях, числе переданных байт, использовавшихся сервисах, времени соединения и т.д. − накапливается в файлах статистики. Многие МЭ позволяют гибко определять подлежащие протоколированию события, описывать порядок действия при атаках или попытках несанкционированного доступа: немедленное закрытие соединения, сообщение на пейджер, почтовое послание администратору системы и т.д. Немедленный вывод сообщения о попытке взлома на экран консоли или администратора может помочь, если попытка оказалась успешной, и взломщик уже проник в систему. В состав многих МЭ входят генераторы отчетов, служащие для обработки статистики и позволяющие собрать статистику по использованию ресурсов конкретными пользователями, по использованию сервисов, отказам, источникам, с которых проводились попытки несанкционированного доступа и т.д.

Простой фильтр пакетов

Простая фильтрация пакетов − возможность некоторых МЭ по блокированию (уничтожению) пакетов, попадающих на МЭ, по заданному критерию на основе данных, содержащихся в заголовках пакетов и текущих параметров окружающей среды. Дополнительной возможностью являются: модификация некоторых полей в заголовках пакетов, трансляция адресов и номеров портов, протоколирование и ведение статистики, немедленное уведомление администратора о появлении пакетов, которые блокируются фильтром. Конструктивной особенностью простых фильтров пакетов является отсутствие памяти состояния соединения. Простая фильтрация пакетов действует только на сетевом уровне. В качестве данных из заголовков IP-пакетов для фильтрации могут использоваться (в порядке убывания значимости):

- цифровой адрес компьютера-источника;
- цифровой адрес компьютера-приемника;
- тип протокола транспортного уровня;
- порт источника TCP/UDP;
- порт приемника TCP/UDP;
- дополнительные параметры TCP/UDP;
- длина IP-пакета;
- дополнительные параметры IP-пакета.

Параметрами окружающей среды, которые могут использоваться для фильтрации, являются:

- интерфейс контроля;
- направление передачи пакета;
- текущее время.

Фильтрация на основе цифровых адресов источника и приемника является минимальным требованием к МЭ с возможностью простой фильтрации пакетов. Задание только этих данных в критериях фильтрации позволяет запретить установление связи между определенными компьютерами, что позволяет сделать достижимыми из глобальной сети только те компьютеры организации, которые предоставляют службы внешним пользователям или пользуются службами

внешней сети. Следует отметить, что фильтрацию на основе цифровых адресов, указанных в заголовках IP-пакетов, могут осуществлять все маршрутизаторы.

Важной дополнительной возможностью МЭ на основе простой фильтрации пакетов является трансляция сетевых адресов и портов (network address & port translation) или изменение реальных адресов компьютеров внутренней сети на вымышленные (виртуальные), причем несколько (или все) реальных внутренних адресов могут транслироваться в один сетевой адрес (с изменением номеров портов). Кроме аспектов, связанных с аспектами защиты, данная возможность может использоваться в случае, если количество компьютеров, подключенных к сети Интернет, в организации больше, чем количество сетевых адресов, официально выделенных данной организации.

Правила политики усиливаются посредством использования фильтров пакетов. Фильтры изучают пакеты и определяют, является ли трафик разрешенным, согласно правилам политики и состоянию протокола (проверка с учетом состояния). Если протокол приложения функционирует через TCP, определить состояние относительно просто, так как TCP сам по себе поддерживает состояния. Это означает, что когда протокол находится в определенном состоянии, разрешена передача только определенных пакетов. Рассмотрим в качестве примера последовательность установки соединения. Первый ожидаемый пакет − пакет SYN. Межсетевой экран обнаруживает этот пакет и переводит соединение в состояние SYN. В данном состоянии ожидается один из двух пакетов − либо SYN ACK (опознавание пакета и разрешение соединения) или пакет RST (сброс соединения по причине отказа в соединении получателем). Если в данном соединении появятся другие пакеты, межсетевой экран аннулирует или отклонит их, так как они не подходят для данного состояния соединения, даже если соединение разрешено набором правил.

Если протоколом соединения является UDP, межсетевой экран с пакетной фильтрацией не может использовать присущее протоколу состояние, вместо чего отслеживает состояние трафика UDP. Как правило, межсетевой экран принимает внешний пакет UDP и ожидает входящий пакет от получателя, соответствующий исходному пакету по адресу и порту, в течение определенного времени. Если пакет принимается в течение этого отрезка времени, его передача разрешается. В противном случае межсетевой экран определяет, что трафик UDP не является ответом на запрос, и аннулирует его.

При использовании межсетевого экрана с пакетной фильтрацией соединения не прерываются на межсетевом экране, а направляются непосредственно к конечной системе. При поступлении пакетов межсетевой экран выясняет, разрешен ли данный пакет и состояние соединения правилами политики. Если это так, пакет передается по своему маршруту. В противном случае пакет отклоняется или аннулируется.

Межсетевые экраны с пакетной фильтрацией могут также быть программными пакетами, базирующимися на операционных системах общего назначения (таких как Windows NT и Unix) либо на аппаратных платформах межсетевых экранов. Межсетевой экран имеет несколько интерфейсов, по одному на каждую из сетей, к которым подключен экран. Аналогично межсетевым экранам прикладного уровня, доставка трафика из одной сети в другую определяется набором правил политики. Если правило не разрешает явным образом определенный трафик, то соответствующие пакеты будут отклонены или аннулированы межсетевым экраном.

Правила политики усиливаются посредством использования фильтров пакетов. Фильтры изучают пакеты и определяют, является ли трафик разрешенным, согласно правилам политики и состоянию протокола (проверка с учетом состояния). Если протокол приложения функционирует через TCP, определить состояние относительно просто, так как TCP сам по себе поддерживает состояния. Это означает, что когда протокол находится в определенном состоянии, разрешена передача только определенных пакетов. Рассмотрим в качестве примера последовательность установки соединения. Первый ожидаемый пакет − пакет SYN. Межсетевой экран обнаруживает этот пакет и переводит соединение в состояние SYN. В данном состоянии ожидается один из двух пакетов − либо SYN ACK (опознавание пакета и разрешение соединения) или пакет RST (сброс соединения по причине отказа в соединении получателем). Если в данном соединении появятся другие пакеты, межсетевой экран аннулирует или отклонит их, так как они не подходят для данного состояния соединения, даже если соединение разрешено набором правил.

Если протоколом соединения является UDP, межсетевой экран с пакетной фильтрацией не может использовать присущее протоколу состояние, вместо чего отслеживает состояние трафика UDP. Как правило, межсетевой экран принимает внешний пакет UDP и ожидает входящий пакет от получателя, соответствующий исходному пакету по адресу и порту, в течение определенного времени. Если пакет принимается в течение этого отрезка времени, его передача разрешается. В противном случае межсетевой экран определяет, что трафик UDP не является ответом на запрос, и аннулирует его.

При использовании межсетевого экрана с пакетной фильтрацией соединения не прерываются на межсетевом экране, а направляются непосредственно к конечной системе. При поступлении пакетов межсетевой экран выясняет, разрешен ли данный пакет и состояние соединения правилами политики (см. Рис.4). Если это так, пакет передается по своему маршруту. В противном случае пакет отклоняется или аннулируется.

Рис. 4. Клиент передает на сервер запрос на соединение

Передача трафика через межсетевой экран с фильтрацией пакетов

Межсетевые экраны с фильтрацией пакетов не используют модули доступа для каждого протокола и поэтому могут использоваться с любым протоколом,

работающим через IP. Некоторые протоколы требуют распознавания межсетевым экраном выполняемых ими действий. Например, FTP будет использовать одно соединение для начального входа и команд, а другое − для передачи файлов. Соединения, используемые для передачи файлов, устанавливаются как часть соединения FTP, и поэтому межсетевой экран должен уметь считывать трафик и определять порты, которые будут использоваться новым соединением. Если межсетевой экран не поддерживает эту функцию, передача файлов невозможна.

Межсетевые экраны с фильтрацией пакетов не используют модули доступа для каждого протокола и поэтому могут использоваться с любым протоколом, работающим через IP. Некоторые протоколы требуют распознавания межсетевым экраном выполняемых ими действий. Например, FTP будет использовать одно соединение для начального входа и команд, а другое − для передачи файлов. Соединения, используемые для передачи файлов, устанавливаются как часть соединения FTP, и поэтому межсетевой экран должен уметь считывать трафик и определять порты, которые будут использоваться новым соединением. Если межсетевой экран не поддерживает эту функцию, передача файлов невозможна.

К положительным качествам простой пакетной фильтрации (по сравнению с другими методами фильтрации) следует отнести следующие:

- относительно невысокая стоимость;
- гибкость в определении правил фильтрации;
- «прозрачность» связи;
- небольшая задержка при прохождении пакетов.

Недостатки у простой фильтрации пакетов следующие:

- локальная сеть видна (маршрутизируется) из сети Интернет;
- не учитывается содержимое IP-пакетов;
- правила фильтрации пакетов трудны в описании;
- не учитывается состояние соединения транспортного и прикладного уровней;
- при нарушении работоспособности МЭ все компьютеры за ним становятся полностью незащищенными либо недоступными;
- аутентификацию с использованием IP-адреса (внешней сети) можно обмануть подменой адреса;
- отсутствует аутентификация на пользовательском уровне.

Посредник уровня соединения

Посредник (транспортного) уровня соединения (circuit-level proxy) − это подсистема МЭ, осуществляющая посреднические услуги по передаче данных на уровне соединения TCP двумя компьютерами в сети. Посредничество заключается в том, что связь между двумя компьютерами физически осуществляется через систему-посредника и реально состоит из двух TCP-соединений. Весь процесс связи состоит из следующих шагов:

1. Компьютер-инициатор начинает процесс установки TCP-соединения с посредником.
2. Посредник проверяет допустимость установления связи компьютером-инициатором.
3. Посредник протоколирует попытку установки связи и/или уведомляет о ней администратора безопасности.
4. Если связь недопустима, то посредник завершает процесс связи, иначе процесс продолжается.
5. Посредник устанавливает TCP-соединение с компьютером-адресатом.

6. Посредник завершает установление связи с компьютером-инициатором.
7. Посредник копирует (пересылает) данные из одного соединения в другое в обоих направлениях и, возможно, протоколирует пересылаемые данные.
8. Посредник завершает процесс связи по требованию одной из сторон или по собственной инициативе.
9. Посредник протоколирует причину завершения связи, а также записывает статистическую информацию о состоявшемся сеансе связи.

Следует отметить, что компьютер-инициатор не передает посреднику имя компьютера-адресата − его цифровой адрес и номер TCP-порта фиксированы для конкретного посредника и известны. Из этого замечания следует, что, во-первых, связь через посредника осуществляется от многих к одному, а, во-вторых, посредники уровня соединения используются только для организации безопасного соединения от внешних компьютеров (удаленных рабочих станций) к внутреннему компьютеру (серверу поддержки локальной сети или информационному серверу). Тем не менее, возможен случай, когда компьютеров-адресатов будет несколько − случай применения техники «зеркального отображения» сервера. При этом посредник, поддерживающий этот случай, перед установлением связи с адресатом должен выбрать конкретный компьютер из нескольких идентичных. Алгоритм выбора может быть одним из следующих (или их комбинацией):

- циклический выбор;
- случайный выбор;
- выбор наиболее доступного (с минимальным временем ответа на ping-запрос);
- выбор с минимальным временем ответа на запрос установления связи;
- выбор наименее загруженного (с минимальной текущей загрузкой процессора).

Под безопасностью связи подразумевается то, что после установления связи факт ее существования уже запротоколирован и проведена аутентификация компьютера-инициатора связи. Протоколирование факта связи (и ее некоторых доступных параметров) означает не только возможность в дальнейшем выследить злоумышленника, но и возможность обнаружения атаки в реальном масштабе времени. Под аутентификацией компьютера-инициатора понимаются действия, предпринимаемые посредником при проверке допустимости связи.

Проверка допустимости связи выполняется посредником непосредственно после запроса на соединение компьютером-инициатором и может основываться на данных из пакета-запроса на соединение, данных окружающей среды и статистических данных. В качестве данных пакета-запроса на соединение могут использоваться (в порядке убывания значимости):

- IP-адрес компьютера-инициатора;
- начальный номер (SYN) пакета TCP-соединения;
- дополнительные параметры TCP-соединения.

Статистические данные (обновляемые после каждой попытки соединения) − это:

- частота запроса соединений от данного компьютера-инициатора;
- отношение количества отвергнутых запросов к общему числу запросов;
- типичный объем и характер пересылаемых по TCP-соединению данных.

Наиболее важными из перечисленных выше являются IP-адрес компьютера-инициатора и ответ DNS-сервера, содержащий символьное имя (если таковое имеется) компьютера-инициатора, и текущее время запроса соединения. По

цифровому адресу компьютера можно запретить доступ (или разрешить доступ только) для компьютеров из определенных сетей, а по символьному адресу − для компьютеров без имен или с именами, содержащими определенные символы или их последовательности, а также для компьютеров из определенных доменов. Текущее время используется для блокирования доступа к защищаемому сервису сети в нерабочее время или в периоды наиболее высокой сетевой активности внутренних пользователей.

Посредник прикладного уровня

Посредник прикладного уровня (application proxy) − это подсистема МЭ, осуществляющая посреднические услуги по передаче данных и команд прикладного уровня двумя компьютерами в сети. Посредничество заключается в том, что связь между двумя компьютерами физически осуществляется через систему-посредника и реально состоит из двух соединений прикладного уровня. Весь процесс связи состоит из следующих шагов:

1. Компьютер-инициатор устанавливает соединение прикладного уровня с посредником.
2. Посредник аутентифицирует компьютер-инициатор и пользователя.
3. Компьютер-инициатор пересылает посреднику имя компьютера-адресата.
4. Посредник проверяет допустимость данной связи.
5. Посредник протоколирует попытку установки связи и уведомляет о ней администратора безопасности.
6. Если связь недопустима, то посредник завершает процесс связи, иначе процесс продолжается.
7. Посредник устанавливает соединение прикладного уровня с компьютером-адресатом.
8. Посредник пересылает данные и команды из одного соединения в другое в обоих направлениях, фильтруя их (перекодируя данные, организуя кэширование и т.п.), и протоколирует попытки выполнения неразрешенных команд.
9. Посредник завершает процесс связи по требованию одной из сторон или по собственной инициативе.
10. Посредник протоколирует причину завершения связи, а также записывает статистическую информацию о состоявшемся сеансе связи.

Следует отметить, что в общих чертах принцип работы посредника прикладного уровня такой же как и у посредника уровня соединения, однако функционирование на более высоком уровне и возможность поддержки специальных безопасных протоколов (SSH, SSL, S/MIME, SOCKS и др.) позволяют организовывать более качественную защиту внутренней сети с использованием посредников данного типа. Далее будут рассмотрены наиболее характерные отличия посредников прикладного уровня от посредников уровня соединения.

Прежде всего, необходимо отметить, что в отличие от посредника уровня соединения, ориентированного на один-единственный протокол TCP, посредников прикладного уровня существует много − под каждый протокол прикладного (и сеансового) уровня. Каждый посредник допускает и защищает только тот протокол, который он поддерживает (тем самым реализуется политика «запрещено все, что не разрешено»). Наиболее популярные поддерживаемые посредниками протоколы можно разделить на следующие группы:

- гипертекстовые протоколы − HTTP, SHTTP, HTTPS, Gopher;

- протокол пересылки файлов − FTP;
- почтовые протоколы − SMTP, POP3, IMAP, NNTP;
- протоколы удаленного доступа − Telnet, rlogin, rsh, rexec, RPC, XWindow;
- протокол сетевой файловой системы − NFS, NetBEUI;
- протокол службы имен − DNS;
- «безопасные» протоколы сеансового уровня − SSH, SSL, S/MIME, SOCKS.

Так как посредник функционирует на прикладном уровне, то у него существуют большие возможности по фильтрации прикладных команд и данных. Например, для протокола FTP возможно запрещение команды «put» − команды записи файла на сервер. Возможна организация разграничения доступа к объектам сервера дополнительно к возможностям самого сервера по разграничению доступа.

Если посредник поддерживает «безопасный» протокол, то возможно поддержание конфиденциальности и целостности передаваемых через внешнюю сеть данных путем шифрования данных и вычисления криптографических контрольных сумм (т.е. туннелируя трафик прикладного уровня). В этом случае компьютер-инициатор тоже должен поддерживать тот же самый «безопасный» протокол (удаленная защищенная рабочая станция) либо необходим еще один посредник прикладного уровня, поддерживающий тот же самый «безопасный» протокол (виртуальная частная сеть − VPN).

Способ реализации схемы усиленной аутентификации компьютера-инициатора и пользователя зависит от используемого протокола, поддержка посредником (и компьютером-инициатором) «безопасного» протокола позволяют не только увеличить надежность аутентификации, но и унифицировать процесс аутентификации.

Следует также отметить, что компьютер-инициатор в начале сеанса связи передает посреднику имя компьютера-адресата и запрашиваемого сервиса (в общем случае − URL), т.е. связь с через посредника может осуществляется от многих ко многим. Способ передачи этого имени зависит от используемого протокола. Здесь же может передаваться и имя пользователя, с правами которого будет осуществляться доступ.

Также возможен случай применения техники «зеркального отображения» сервера для повышения надежности. При этом посредник, поддерживающий этот случай, перед установлением связи с адресатом должен выбрать конкретный компьютер из нескольких идентичных, а алгоритм выбора должен работать так, чтобы один и тот же пользователь попадали на один и тот же «реальный» компьютер-сервер во время всех сеансов связи, т.к. сервер может хранить контекст каждого пользователя.

Пакетный фильтр инспекционного типа

Пакетная фильтрация инспекционного типа (packet state-full inspection) − способность некоторых МЭ по блокированию (уничтожению) и изменению пакетов, проходящих через МЭ, по заданному критерию на основе данных, содержащихся в этих пакетах, данных контекстов соединений транспортного, сеансового и прикладного уровней, текущих параметров окружающей среды и статистических данных.

Технология фильтрации пакетов инспекционного (или экспертного) типа сочетает в себе элементы всех трех описанных выше технологий. Как и простая фильтрация пакетов, фильтрация инспекционного типа работает на сетевом уровне

модели OSI, фильтруя входящие и исходящие пакеты на основе проверки IP-адресов и номеров портов и т.п. Фильтры пакетов инспекционного типа также выполняют функции посредника уровня соединения, определяя, относятся ли пакеты к соответствующему сеансу связи. И, наконец, фильтры инспекционного типа берут на себя функции многих посредников прикладного уровня (одновременно), оценивая и модифицируя содержимое каждого пакета в соответствии с политикой безопасности, выработанной в конкретной организации.

Как и посредник прикладного уровня, фильтр пакетов инспекционного типа может быть сконфигурирован для блокирования пакетов, содержащих определенные команды, например команду «put» службы FTP. Однако, в отличие от посредников прикладного уровня, при анализе данных прикладного уровня такой фильтр не нарушает модели клиент-сервер взаимодействия в сети − фильтр инспекционного типа допускает прямые соединения между компьютером-инициатором соединения и компьютером-адресатом. Для обеспечения защиты такие фильтры перехватывают и анализируют каждый пакет на прикладном уровне модели OSI. Вместо применения связанных с приложениями программ-посредников, фильтр пакетов инспекционного типа использует специальные алгоритмы распознавания и обработки данных на уровне приложений.

Обладая всеми преимуществами трех вышерассмотренных типов фильтров и минимальным количеством недостатков, МЭ с функцией фильтрации пакетов инспекционного типа обеспечивают один из самых высоких на сегодняшний день уровней защиты локальных сетей.

Недостатки, связанные с применением МЭ

Существуют угрозы, которым МЭ не может противостоять. Кроме того, применение МЭ создает определенные трудности.

Наиболее очевидным недостатком МЭ является большая вероятность того, что он может заблокировать некоторые необходимые пользователю службы, такие как Telnet, FTP, XWindow, NFS и т.д. Однако, эти недостатки присущи не только МЭ, доступ к сети может быть ограничен также и на уровне отдельных СВТ, в зависимости от методики обеспечения безопасности сети.

Некоторые объекты могут обладать топологией, не предназначенной для использования МЭ, или использовать службы (сервисы) таким образом, что его использование потребовало бы полной реорганизации локальной сети.

Далее, МЭ не защищают системы локальной сети от проникновения через «люки» (backdoors). Например, если на систему, защищенную МЭ, все же разрешается неограниченный модемный доступ, злоумышленник может с успехом обойти МЭ. Связь через протоколы PPP (Point-to-Point) и SLIP (Serial Line IP) в рамках защищенной подсети является, по существу, еще одним сетевым соединением и потенциальным каналом нападения.

МЭ, как правило, не обеспечивает защиту от внутренних угроз. С одной стороны, МЭ можно разработать так, чтобы предотвратить получение конфиденциальной информации злоумышленниками из внешней сети, однако, МЭ не запрещает пользователям внутренней сети копировать информацию на магнитные носители или выводить ее на печатающее устройство. Таким образом, было бы ошибкой полагать, что наличие МЭ обеспечивает защиту от внутренних атак или вообще атак, для которых не требуется использование МЭ.

Кроме того, есть недостаток МЭ, связанный с низкой пропускной способностью − МЭ представляют собой потенциально узкое место, поскольку все

соединения с сетью Интернет должны осуществляться через него и еще подвергаться фильтрации.

Существует также и возможность «общего риска» − в МЭ все средства безопасности сосредоточены в одном месте, а не распределены между системами сети. Компрометация МЭ ведет к нарушению безопасности для других, менее защищенных систем.

В общем, несмотря на все вышеперечисленные недостатки, использование МЭ для защиты локальной сети в большинстве случаев более чем оправдано.

VPN

VPN (англ. Virtual Private Network − виртуальная частная сеть) − логическая сеть, создаваемая поверх другой сети, например Internet. Несмотря на то, что коммуникации осуществляются по публичным сетям с использованием небезопасных протоколов, за счёт шифрования создаются закрытые от посторонних каналы обмена информацией. VPN позволяет объединить, например, несколько офисов организации в единую сеть с использованием для связи между ними неподконтрольных каналов. По своей сути VPN обладает многими свойствами выделенной линии, однако развертывается она в пределах общедоступной сети, например Интернета. С помощью методики туннелирования пакеты данных транслируются через общедоступную сеть как по обычному двухточечному соединению. Между каждой парой «отправитель-получатель данных» устанавливается своеобразный туннель − безопасное логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого. Основными компонентами туннеля являются: инициатор; маршрутизируемая сеть; туннельный коммутатор; один или несколько туннельных терминаторов. Сам по себе принцип работы VPN не противоречит основным сетевым технологиям и протоколам.

Например, при установлении соединения удаленного доступа клиент посылает серверу поток пакетов стандартного протокола PPP. В случае организации виртуальных выделенных линий между локальными сетями их маршрутизаторы также обмениваются пакетами PPP. Тем не менее, принципиально новым моментом является пересылка пакетов через безопасный туннель, организованный в пределах общедоступной сети. Туннелирование позволяет организовать передачу пакетов одного протокола в логической среде, использующей другой протокол. В результате появляется возможность решить проблемы взаимодействия нескольких разнотипных сетей, начиная с необходимости обеспечения целостности и конфиденциальности передаваемых данных и заканчивая преодолением несоответствий внешних протоколов или схем адресации. Существующая сетевая инфраструктура корпорации может быть подготовлена к использованию VPN как с помощью программного, так и с помощью аппаратного обеспечения. Организацию виртуальной частной сети можно сравнить с прокладкой кабеля через глобальную сеть. Как правило, непосредственное соединение между удаленным пользователем и оконечным устройством туннеля устанавливается по протоколу PPP. Наиболее распространенный метод создания туннелей VPN − инкапсуляция сетевых протоколов (IP, IPX, AppleTalk и т.д.) в PPP и последующая инкапсуляция образованных пакетов в протокол туннелирования. Обычно в качестве последнего выступает IP или (гораздо реже) ATM и Frame Relay. Такой подход называется туннелированием второго уровня, поскольку «пассажиром» здесь является протокол именно второго уровня. Альтернативный подход − инкапсуляция пакетов

сетевого протокола непосредственно в протокол туннелирования (например, VTP) называется туннелированием третьего уровня. Независимо от того, какие протоколы используются или какие цели преследуются при организации туннеля, основная методика остается практически неизменной. Обычно один протокол используется для установления соединения с удаленным узлом, а другой − для инкапсуляции данных и служебной информации с целью передачи через туннель.

Классификация VPN сетей

Классифицировать VPN решения можно по нескольким основным параметрам:

1. По типу используемой среды:

a) *Защищённые VPN сети.* Данный тип наиболее распространён. С его помощью возможно создать надежную и защищенную подсеть на основе ненадёжной сети, как правило, Интернета. Примером защищённых VPN являются: IPSec, OpenVPN и PPTP.

b) *Доверительные VPN сети.* Данный тип используется в случаях, когда передающая среда надёжная. Примерами подобных VPN решении являются: MPLS и L2TP. Корректнее сказать, что эти протоколы перекладывают задачу обеспечения безопасности на другие, например L2TP, как правило, используется в паре с IPSec.

2. По способу реализации: VPN сети в виде специального программно-аппаратного обеспечения. Реализация VPN сети осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости. VPN сети в виде программного решения. Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN. VPN сети с интегрированным решением. Функциональность VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.
3. По назначению: Intranet VPN. Используют для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи. Remote Access VPN. Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера или, находясь в командировке, подключается к корпоративным ресурсам при помощи ноутбука. Extranet VPN. Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубежей» защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации.
4. По типу протокола: Существуют реализации виртуальных частных сетей под TCP/IP, IPX и AppleTalk. Но на сегодняшний день наблюдается

тенденция к всеобщему переходу на протокол TCP/IP, и абсолютное большинство VPN решений поддерживает именно его.

5. По уровню сетевого протокола: По уровню сетевого протокола на основе сопоставления с уровнями эталонной сетевой модели ISO/OSI.

Построение VPN

Существуют несколько вариантов построения VPN. При выборе варианта требуется учитывать факторы производительности средств построения VPN. Например, если маршрутизатор и так работает на пределе мощности своего процессора, то добавление туннелей VPN и применение шифрования/дешифрования информации могут остановить работу всей сети из-за того, что этот маршрутизатор не будет справляться с простым трафиком, не говоря уже о VPN. Опыт показывает, что для построения VPN лучше всего использовать специализированное оборудование, однако если имеется ограничение в средствах, то можно обратить внимание на чисто программное решение. Рассмотрим некоторые варианты построения VPN.

VPN на базе брандмауэров

Брандмауэры большинства производителей поддерживают туннелирование и шифрование данных. Все подобные продукты основаны на том, что трафик, проходящий через брандмауэр шифруется. К программному обеспечению собственно брандмауэра добавляется модуль шифрования. Недостатком этого метода можно назвать зависимость производительности от аппаратного обеспечения, на котором работает брандмауэр. При использовании брандмауэров на базе ПК надо помнить, что подобное решение можно применять только для небольших сетей с небольшим объемом передаваемой информации.

VPN на базе маршрутизаторов

Другим способом построения VPN является применение для создания защищенных каналов маршрутизаторов. Так как вся информация, исходящая из локальной сети, проходит через маршрутизатор, то целесообразно возложить на этот маршрутизатор и задачи шифрования. Примером оборудования для построения VPN на маршрутизаторах является оборудование компании Cisco Systems. Начиная с версии программного обеспечения IOS 11.3, маршрутизаторы Cisco поддерживают протоколы L2TP и IPSec. Помимо простого шифрования проходящей информации Cisco поддерживает и другие функции VPN, такие как идентификация при установлении туннельного соединения и обмен ключами. Для повышения производительности маршрутизатора может быть использован дополнительный модуль шифрования ESA. Кроме того, компания Cisco System выпустила специализированное устройство для VPN, которое так и называется Cisco 1720 VPN Access Router (маршрутизатор доступа к VPN), предназначенное для установки в компаниях малого и среднего размера, а также в отделениях крупных организаций.

VPN на базе программного обеспечения

Следующим подходом к построению VPN являются чисто программные решения. При реализации такого решения используется специализированное программное обеспечение, которое работает на выделенном компьютере, и в большинстве случаев выполняет роль proxy-сервера. Компьютер с таким программным обеспечением может быть расположен за брандмауэром. VPN на

базе сетевой ОС. Решения на базе сетевой ОС рассмотрим на примере ОС Windows компании Microsoft. Для создания VPN Microsoft использует протокол PPTP, который интегрирован в систему Windows. Данное решение очень привлекательно для организаций использующих Windows в качестве корпоративной операционной системы. Необходимо отметить, что стоимость такого решения значительно ниже стоимости прочих решений. В работе VPN на базе Windows используется база пользователей, хранящаяся на Primary Domain Controller (PDC). При подключении к PPTP-серверу пользователь аутентифицируется по протоколам PAP, CHAP или MS-CHAP. Передаваемые пакеты инкапсулируются в пакеты GRE/PPTP. Для шифрования пакетов используется нестандартный протокол от Microsoft Point-to-Point Encryption с 40 или 128 битным ключом, получаемым в момент установки соединения. Недостатками данной системы являются отсутствие проверки целостности данных и невозможность смены ключей во время соединения. Положительными моментами являются легкость интеграции с Windows и низкая стоимость.

VPN на базе аппаратных средств

Вариант построения VPN на специальных устройствах может быть использован в сетях, требующих высокой производительности. Примером такого решения служит продукт с IPro-VPN компании Radguard. Данный продукт использует аппаратное шифрование передаваемой информации, способное пропускать поток в 100 Мбит/с. IPro-VPN поддерживает протокол IPSec и механизм управления ключами ISAKMP/Oakley. Помимо прочего, данное устройство поддерживает средства трансляции сетевых адресов и может быть дополнено специальной платой, добавляющей функции брандмауэра

Протоколы VPN сетей

Сети VPN строятся с использованием протоколов туннелирования данных через сеть связи общего пользования Интернет, причем протоколы туннелирования обеспечивают шифрование данных и осуществляют их сквозную передачу между пользователями. Как правило, на сегодняшний день для построения сетей VPN используются протоколы следующих уровней:

- канальный уровень;
- сетевой уровень;
- транспортный уровень.

Методы реализации VPN сетей

Виртуальная частная сеть базируется на трех методах реализации:

- туннелирование;
- аутентификация;
- шифрование.

Туннелирование

Туннелирование обеспечивает передачу данных между двумя точками − окончаниями туннеля − таким образом, что для источника и приемника данных оказывается скрытой вся сетевая инфраструктура, лежащая между ними. Транспортная среда туннеля, как паром, подхватывает пакеты используемого сетевого протокола у входа в туннель и без изменений доставляет их к выходу. Построения туннеля достаточно для того, чтобы соединить два сетевых узла так, что с точки зрения работающего на них программного обеспечения они выглядят

подключенными к одной (локальной) сети. Однако нельзя забывать, что на самом деле «паром» с данными проходит через множество промежуточных узлов (маршрутизаторов) открытой публичной сети. Такое положение дел таит в себе две проблемы. Первая заключается в том, что передаваемая через туннель информация может быть перехвачена злоумышленниками. Если она конфиденциальна (номера банковских карточек, финансовые отчеты, сведения личного характера), то вполне реальна угроза ее компрометации, что уже само по себе неприятно. Хуже того, злоумышленники имеют возможность модифицировать передаваемые через туннель данные так, что получатель не сможет проверить их достоверность. Последствия могут быть самыми плачевными. Учитывая сказанное, мы приходим к выводу, что туннель в чистом виде пригоден разве что для некоторых типов сетевых компьютерных игр и не может претендовать на более серьезное применение. Обе проблемы решаются современными средствами криптографической защиты информации. Чтобы воспрепятствовать внесению несанкционированных изменений в пакет с данными на пути его следования по туннелю, используется метод электронной цифровой подписи (ЭЦП). Суть метода состоит в том, что каждый передаваемый пакет снабжается дополнительным блоком информации, который вырабатывается в соответствии с асимметричным криптографическим алгоритмом и уникален для содержимого пакета и секретного ключа ЭЦП отправителя. Этот блок информации является ЭЦП пакета и позволяет выполнить аутентификацию данных получателем, которому известен открытый ключ ЭЦП отправителя. Защита передаваемых через туннель данных от несанкционированного просмотра достигается путем использования сильных алгоритмов шифрования.

Аутентификация

Обеспечение безопасности является основной функцией VPN. Все данные от компьютеров-клиентов проходят через Internet к VPN-серверу. Такой сервер может находиться на большом расстоянии от клиентского компьютера, и данные на пути к сети организации проходят через оборудование множества провайдеров. Как убедиться, что данные не были прочитаны или изменены? Для этого применяются различные методы аутентификации и шифрования. Для аутентификации пользователей PPTP может задействовать любой из протоколов, применяемых для PPP EAP или Extensible Authentication Protocol; MSCHAP или Microsoft Challenge Handshake Authentication Protocol (версии 1 и 2); CHAP или Challenge Handshake Authentication Protocol; SPAP или Shiva Password Authentication Protocol; PAP или Password Authentication Protocol. Лучшими считаются протоколы MSCHAP версии 2 и Transport Layer Security (EAP-TLS), поскольку они обеспечивают взаимную аутентификацию, т.е. VPN-сервер и клиент идентифицируют друг друга. Во всех остальных протоколах только сервер проводит аутентификацию клиентов. Хотя PPTP обеспечивает достаточную степень безопасности, но все же L2TP поверх IPSec надежнее. L2TP поверх IPSec обеспечивает аутентификацию на уровнях «пользователь» и компьютер, а также выполняет аутентификацию и шифрование данных. Аутентификация осуществляется либо отрытым тестом (clear text password), либо по схеме запрос/отклик (challenge/response). С прямым текстом все ясно. Клиент посылает серверу пароль. Сервер сравнивает это с эталоном и либо запрещает доступ, либо говорит «добро пожаловать». Открытая аутентификация практически не встречается. Схема запрос/отклик намного более продвинута. В общем виде она выглядит так: клиент посылает серверу запрос (request) на аутентификацию; сервер

возвращает случайный отклик (challenge); клиент снимает со своего пароля хеш (хешем называется результат хеш-функции, которая преобразовывает входной массив данных произвольной длины в выходную битовую строку фиксированной длины), шифрует им отклик и передает его серверу; то же самое проделывает и сервер, сравнивая полученный результат с ответом клиента; если зашифрованный отклик совпадает, аутентификация считается успешной; На первом этапе аутентификации клиентов и серверов VPN, L2TP поверх IPSec использует локальные сертификаты, полученные от службы сертификации. Клиент и сервер обмениваются сертификатами и создают защищенное соединение ESP SA (security association). После того как L2TP (поверх IPSec) завершает процесс аутентификации компьютера, выполняется аутентификация на уровне пользователя. Для аутентификации можно задействовать любой протокол, даже PAP, передающий имя пользователя и пароль в открытом виде. Это вполне безопасно, так как L2TP поверх IPSec шифрует всю сессию. Однако проведение аутентификации пользователя при помощи MSCHAP, применяющего различные ключи шифрования для аутентификации компьютера и пользователя, может усилить защиту.

Шифрование

Шифрование с помощью PPTP гарантирует, что никто не сможет получить доступ к данным при пересылке через Internet. В настоящее время поддерживаются два метода шифрования: Протокол шифрования MPPE или Microsoft Point-to-Point Encryption совместим только с MSCHAP (версии 1 и 2); EAP-TLS и умеет автоматически выбирать длину ключа шифрования при согласовании параметров между клиентом и сервером. MPPE поддерживает работу с ключами длиной 40, 56 или 128 бит. Старые операционные системы Windows поддерживают шифрование с длиной ключа только 40 бит, поэтому в смешанной среде Windows следует выбирать минимальную длину ключа. PPTP изменяет значение ключа шифрации после каждого принятого пакета. Протокол MMPE разрабатывался для каналов связи точка-точка, в которых пакеты передаются последовательно, и потеря данных очень мала. В этой ситуации значение ключа для очередного пакета зависит от результатов дешифрации предыдущего пакета. При построении виртуальных сетей через сети общего доступа эти условия соблюдать невозможно, так как пакеты данных часто приходят к получателю не в той последовательности, в какой были отправлены. Поэтому PPTP использует для изменения ключа шифрования порядковые номера пакетов. Это позволяет выполнять дешифрацию независимо от предыдущих принятых пакетов. Оба протокола реализованы как в Microsoft Windows, так и вне ее (например, в BSD), на алгоритмы работы VPN могут существенно отличаться. Таким образом, связка «туннелирование + аутентификация + шифрование» позволяет передавать данные между двумя точками через сеть общего пользования, моделируя работу частной (локальной) сети. Иными словами, рассмотренные средства позволяют построить виртуальную частную сеть.

Прокси-сервер

Proxy-servers (proxy – доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью – маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся

невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях – например, на уровне приложения (вредоносные программы, код Java и Java Script).

Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс, расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша (в случаях, если прокси имеет свой кэш). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях. Прокси-сервер позволяет защищать компьютер клиента от некоторых сетевых атак и помогает сохранять анонимность клиента.

Цели

- *Обеспечение доступа компьютеров локальной сети к сети Интернет*.
- *Кэширование данных*: если часто происходят обращения к одним и тем же внешним ресурсам, то можно держать их копию на прокси-сервере и выдавать по запросу, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентом запрошенной информации. С развитием динамического контента кэширование утратило актуальность.
- *Сжатие данных*: прокси-сервер загружает информацию из Интернета и передаёт информацию конечному пользователю в сжатом виде. Такие прокси-серверы используются в основном с целью экономии внешнего сетевого трафика клиента или внутреннего − компании, в которой установлен прокси-сервер.
- *Защита локальной сети от внешнего доступа*: например, можно настроить прокси-сервер так, что локальные компьютеры будут обращаться к внешним ресурсам только через него, а внешние компьютеры не смогут обращаться к локальным вообще (они «видят» только прокси-сервер).
- *Ограничение доступа из локальной сети к внешней*: например, можно запретить доступ к определённым веб-сайтам, ограничить использование интернета каким-то локальным пользователям, устанавливать квоты на трафик или полосу пропускания, фильтровать рекламу и вредоносные программы.
- *Анонимизация доступа к различным ресурсам*. Прокси-сервер может скрывать сведения об источнике запроса или пользователе. В таком случае целевой сервер видит лишь информацию о прокси-сервере, например, IP-адрес, но не имеет возможности определить истинный источник запроса. Существуют также искажающие прокси-серверы, которые передают целевому серверу ложную информацию об истинном пользователе.
- *Обход ограничений доступа*. Прокси-серверы популярны среди пользователей стран, где доступ к некоторым ресурсам ограничен законодательно и фильтруется.

Прокси-сервер, к которому может получить доступ любой пользователь сети интернет, называется открытым.

Виды прокси-серверов

Прозрачный прокси − схема связи, при которой трафик, или его часть, перенаправляется на прокси-сервер неявно (средствами маршрутизатора). При этом клиент может использовать все преимущества прокси-сервера без дополнительных настроек браузера (или другого приложения для работы с интернетом).

Обратный прокси – прокси-сервер, который в отличие от прямого, ретранслирует запросы клиентов из внешней сети на один или несколько серверов, логически расположенных во внутренней сети. Часто используется для балансировки сетевой нагрузки между несколькими веб-серверами и повышения их безопасности, играя при этом роль межсетевого экрана на прикладном уровне.

Технические подробности

Клиентский компьютер имеет настройку (конкретной программы или операционной системы), в соответствии с которой все сетевые соединения по некоторому протоколу совершаются не на IP-адрес сервера (ресурса), выделяемый из DNS-имени ресурса, или напрямую заданный, а на IP-адрес (и другой порт) прокси-сервера.

При необходимости обращения к любому ресурсу по этому протоколу, клиентский компьютер открывает сетевое соединение с прокси-сервером (на нужном порту) и совершает обычный запрос, как если бы он обращался непосредственно к ресурсу.

Распознав данные запроса, проверив его корректность и разрешения для клиентского компьютера, прокси-сервер, не разрывая соединения, сам открывает новое сетевое соединение непосредственно с ресурсом и делает тот же самый запрос. Получив данные (или сообщение об ошибке), прокси-сервер передаёт их клиентскому компьютеру.

Таким образом прокси-сервер является полнофункциональным сервером и клиентом для каждого поддерживаемого протокола и имеет полный контроль над всеми деталями реализации этого протокола, имеет возможность применения заданных администратором политик доступа на каждом этапе работы протокола.

Прокси-серверы являются самым популярным способом выхода в Интернет из локальных сетей предприятий и организаций. Этому способствуют следующие обстоятельства:

- основной используемый в интернете протокол − HTTP, в стандарте которого описана поддержка работы через прокси;
- поддержка прокси большинством браузеров и операционных систем;
- контроль доступа и учёт трафика по пользователям;
- фильтрация трафика (интеграция прокси с антивирусами);
- прокси-сервер − может работать с минимальными правами на любой ОС с поддержкой сети (стека TCP/IP);
- многие приложения, использующие собственные специализированные протоколы, могут использовать HTTP как альтернативный транспорт или SOCKS-прокси как универсальный прокси, подходящий для практически любого протокола;
- отсутствие доступа в сеть Интернет по другим (нестандартным) протоколам может повысить безопасность в корпоративной сети.

В настоящее время, несмотря на возрастание роли других сетевых протоколов, переход к тарификации услуг сети Интернет по скорости доступа, а также появлением дешёвых аппаратных маршрутизаторов с функцией NAT, прокси-серверы продолжают широко использоваться на предприятиях, так как NAT не может обеспечить достаточный уровень контроля над использованием Интернета (аутентификацию пользователей, фильтрацию контента).

Комбинированные средства защиты

Система обнаружения вторжений

Система обнаружения вторжения (IDS – Intrusion Detection System) являются программными или аппаратными системами, которые автоматизируют процесс просмотра событий, возникающих в компьютерной системе или сети, и анализируют их с точки зрения безопасности. Так как количество сетевых атак возрастает, IDS становятся необходимым дополнением инфраструктуры безопасности. Рассмотрим, для каких целей предназначены IDS, как выбрать и сконфигурировать IDS для конкретных систем и сетевых окружений, как обрабатывать результаты работы IDS и как интегрировать IDS с остальной инфраструктурой безопасности предприятия.

Обнаружение проникновения является процессом мониторинга событий, происходящих в компьютерной системе или сети, и анализа их. Проникновения определяются как попытки компрометации конфиденциальности, целостности, доступности или обхода механизмов безопасности компьютера или сети. Проникновения могут осуществляться как атакующими, получающими доступ к системам из Интернета, так и авторизованными пользователями систем, пытающимися получить дополнительные привилегии, которых у них нет. IDS являются программными или аппаратными устройствами, которые автоматизируют процесс мониторинга и анализа событий, происходящих в сети или системе, с целью обнаружения проникновений.

IDS состоят из трех функциональных компонентов: информационных источников, анализа и ответа. Система получает информацию о событии из одного или более источников информации, выполняет определяемый конфигурацией анализ данных события и затем создает специальные ответы – от простейших отчетов до активного вмешательства при определении проникновений.

Классификация IDS

Для проведения классификации IDS необходимо учесть несколько факторов (см. Рис.5).

Метод обнаружения описывает характеристики анализатора. Когда IDS использует информацию о нормальном поведении контролируемой системы, она называется поведенческой. Когда IDS работает с информацией об атаках, она называется интеллектуальной.

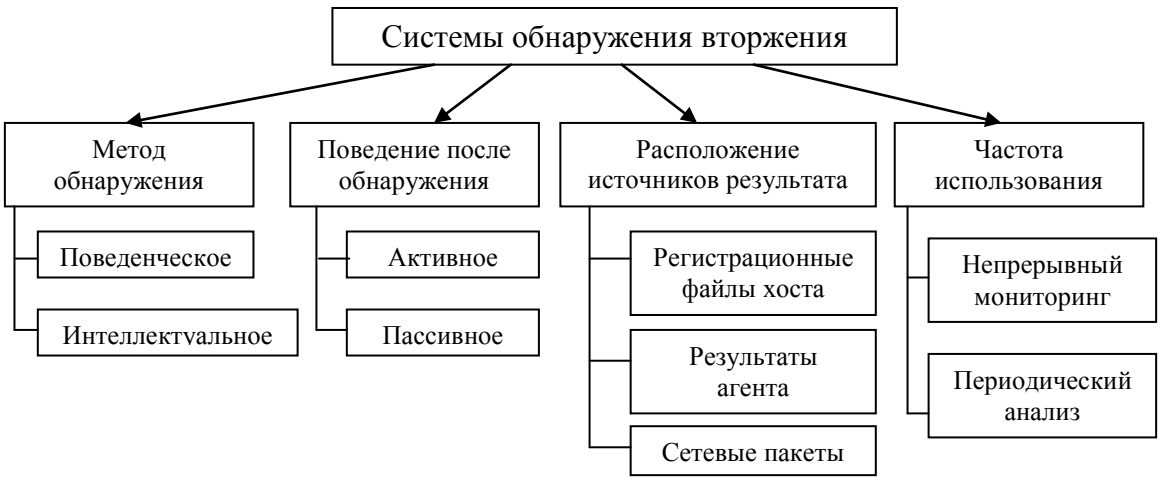


Рис. 5. Характеристики систем обнаружения вторжений

Поведение после обнаружения указывает на реакцию IDS на атаки. Реакция может быть активной – IDS предпринимает корректирующие (устраняет лазейки) или действительно активные (закрывает доступ для возможных нарушителей, делая недоступными сервисы) действия. Если IDS только выдаёт предупреждения, её называют пассивной.

Расположение источников результата аудита подразделяет IDS в зависимости от вида исходной информации, которую они анализируют. Входными данными для них могут быть результаты аудита, системные регистрационные файлы или сетевые пакеты.

Частота использования отражает либо непрерывный мониторинг контролируемой системы со стороны IDS, либо соответствующие периодическим запускам IDS для проведения анализа.

Классифицировать IDS можно также по нескольким параметрам (см. Рис.6).

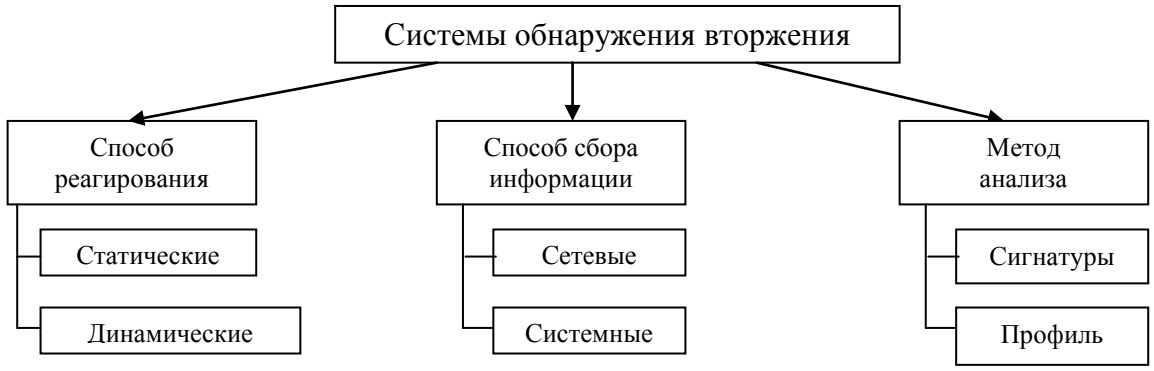


Рис. 6. Классификация систем обнаружения вторжений

По способам реагирования различают статические и динамические IDS. Статические средства делают «снимки» (snapshot) среды и осуществляют их анализ, разыскивая уязвимое ПО, ошибки в конфигурациях и т.д. Статические IDS проверяют версии работающих в системе приложений на наличие известных уязвимостей и слабых паролей, проверяют содержимое специальных файлов в директориях пользователей или проверяют конфигурацию открытых сетевых сервисов. Статические IDS обнаруживают следы вторжения. Динамические IDS осуществляют мониторинг в реальном времени всех действий, происходящих в системе, просматривая файлы аудита или сетевые пакеты, передаваемые за определённый промежуток времени. Динамические IDS реализуют анализ в реальном времени и позволяют постоянно следить за безопасностью системы.

По способу сбора информации различают сетевые и системные IDS. Сетевые (NIDS) контролируют пакеты в сетевом окружении и обнаруживают попытки злоумышленника проникнуть внутрь защищаемой системы или реализовать атаку «отказ в обслуживании». Эти IDS работают с сетевыми потоками данных. Типичный пример NIDS – система, которая контролирует большое число TPC-запросов на соединение (SYN) со многими портами на выбранном компьютере, обнаруживая, таким образом, что кто-то пытается осуществить сканирование TCP-портов. Сетевая IDS может запускаться либо на отдельном компьютере, который контролирует свой собственный трафик, либо на выделенном компьютере, прозрачно просматривающим весь трафик в сети (концентратор, маршрутизатор). Сетевые IDS контролируют много компьютеров, тогда как другие IDS контролируют только один. IDS, которые устанавливаются на хосте и обнаруживают злонамеренные действия на нём называются хостовыми или системными IDS. Примерами хостовых IDS могут быть системы контроля

целостности файлов (СКЦФ), которые проверяют системные файлы с целью определения, когда в них были внесены изменения. Мониторы регистрационных файлов (Log-file monitors, LFM), контролируют регистрационные файлы, создаваемые сетевыми сервисами и службами. Обманные системы, работающие с псевдосервисами, цель которых заключается в воспроизведении хорошо известных уязвимостей для обмана злоумышленников.

По методам анализа IDS делят на две группы: IDS, которые сравнивают информацию с предустановленной базой сигнатур атак и IDS, контролирующие частоту событий или обнаружение статистических аномалий.

Анализ сигнатур был первым методом, примененным для обнаружения вторжений. Он базируется на простом понятии совпадения последовательности с образцом. Во входящем пакете просматривается байт за байтом и сравнивается с сигнатурой (подписью) – характерной строкой программы, указывающей на характеристику вредного трафика. Такая подпись может содержать ключевую фразу или команду, которая связана с нападением. Если совпадение найдено, объявляется тревога.

Второй метод анализа состоит в рассмотрении строго форматированных данных трафика сети, известных как протоколы. Каждый пакет сопровождается различными протоколами. Авторы IDS, зная это, внедрили инструменты, которые разворачивают и осматривают эти протоколы, согласно стандартам. Каждый протокол имеет несколько полей с ожидаемыми или нормальными значениями. Если что-нибудь нарушает эти стандарты, то вероятна злонамеренность. IDS просматривает каждое поле всех протоколов входящих пакетов: IP, TCP, и UDP. Если имеются нарушения протокола, например, если он содержит неожиданное значение в одном из полей, объявляется тревога

Системы анализа сигнатуры имеют несколько важных сильных сторон. Во-первых, они очень быстры, так как полный анализ пакета − относительно тяжелая задача. Правила легко написать, понять и настроить. Кроме того, имеется просто фантастическая поддержка компьютерного сообщества в быстром производстве сигнатур для новых опасностей. Эти системы превосходят все другие при отлове хакеров на первичном этапе: простые атаки имеют привычку использовать некие предварительные действия, которые легко распознать. Наконец, анализ, основанный на сигнатуре, точно и быстро сообщает, что в системе все нормально (если это действительно так), поскольку должны произойти некие особые события для объявления тревоги.

С другой стороны IDS, основывающаяся только на анализе сигнатур, имеет определенные слабости. Являясь первоначально очень быстрой, со временем скорость ее работы будет замедляться, поскольку возрастает число проверяемых сигнатур. Это – существенная проблема, поскольку число проверяемых сигнатур может расти очень быстро. Фактически, каждая новая атака или действие, придуманное атакующим, увеличивает список проверяемых сигнатур. Не помогут даже эффективные методы работы с данными и пакетами: огромное количество слегка измененных атак могут проскользнуть через такую систему

Имеется и другая сторона проблемы: так как система работает, сравнивая список имеющихся сигнатур с данными пакета, такая IDS может выявить только уже известные атаки, сигнатуры которых имеются.

Архитектура IDS

Архитектура IDS определяет, какие имеются функциональные компоненты IDS и как они взаимодействуют друг с другом. Основными архитектурными

компонентами являются: Host − система, на которой выполняется ПО IDS, и Target − система, за которой IDS наблюдает.

У систем обнаружения вторжений целесообразно различать локальную и глобальную архитектуру. В рамках локальной архитектуры реализуются элементарные составляющие, которые затем могут быть объединены для обслуживания корпоративных систем.

Основные элементы локальной архитектуры и связи между ними показаны на рисунке 7. Первичный сбор данных осуществляют агенты, называемые также сенсорами. Регистрационная информация может извлекаться из системных или прикладных журналов (технически несложно получать ее и напрямую от ядра ОС), либо добываться из сети с помощью соответствующих механизмов активного сетевого оборудования или путем перехвата пакетов посредством установленной в режим мониторинга сетевой карты.

Рис. 7. Основные элементы локальной архитектуры систем обнаружения вторжений

На уровне агентов (сенсоров) может выполняться фильтрация данных с целью уменьшения их объема. Это требует от агентов некоторого интеллекта, но зато разгружает остальные компоненты системы.

Агенты передают информацию в центр распределения, который приводит ее к единому формату, возможно, осуществляет дальнейшую фильтрацию, сохраняет в базе данных и направляет для анализа статистическому и экспертному компонентам. Один центр распределения может обслуживать несколько сенсоров.

Содержательный активный аудит начинается со статистического и экспертного компонентов. Если в процессе статистического или экспертного анализа выявляется подозрительная активность, соответствующее сообщение направляется решателю, который определяет, является ли тревога оправданной, и выбирает способ реагирования.

Хорошая система обнаружения вторжений должна уметь внятно объяснить, почему она подняла тревогу, насколько серьезна ситуация и каковы рекомендуемые способы действия. Если выбор должен оставаться за человеком, то пусть он сводится к нескольким элементам меню, а не к решению концептуальных проблем.

Глобальная архитектура подразумевает организацию одноранговых и разноранговых связей между локальными системами обнаружения вторжений (см. Рис.8).

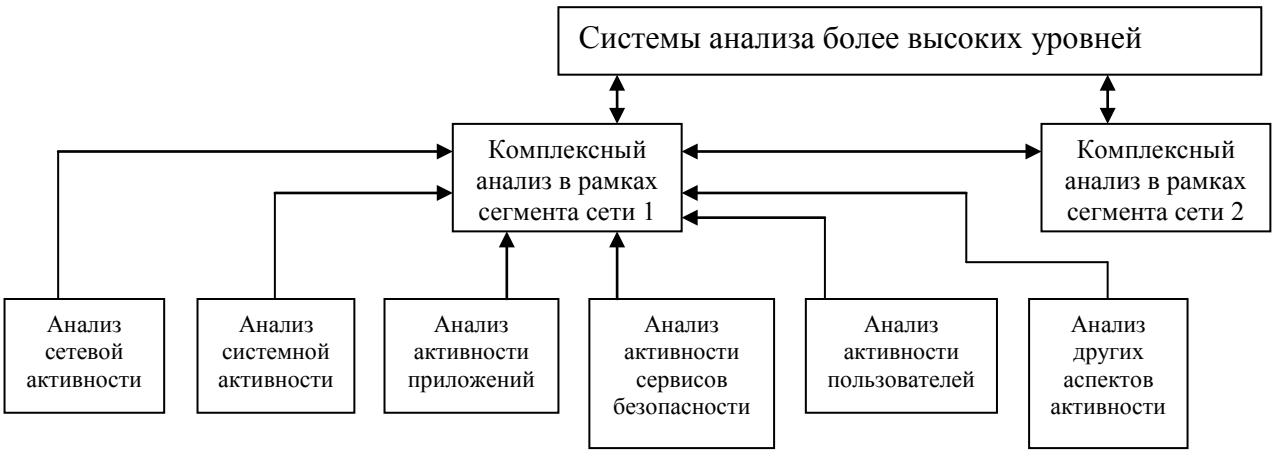


Рис. 8. Глобальная архитектура систем обнаружения вторжений

На одном уровне иерархии располагаются компоненты, анализирующие подозрительную активность с разных точек зрения. Например, на хосте могут располагаться подсистемы анализа поведения пользователей и приложений. Их может дополнять подсистема анализа сетевой активности. Когда один компонент обнаруживает что-то подозрительное, то во многих случаях целесообразно сообщить об этом соседям либо для принятия мер, либо для усиления внимания к определенным аспектам поведения системы.

Разноранговые связи используются для обобщения результатов анализа и получения целостной картины происходящего. Иногда у локального компонента недостаточно оснований для возбуждения тревоги, но «по совокупности» подозрительные ситуации могут быть объединены и совместно проанализированы, после чего порог подозрительности окажется превышенным. Целостная картина, возможно, позволит выявить скоординированные атаки на разные участки информационной системы и оценить ущерб в масштабе организации.

Скорость реакции

Скорость реакции указывает на время, прошедшее между событиями, которые были обнаружены монитором, анализом этих событий и реакцией на них.

1. IDS, реакция которых происходит *через определенные интервалы времени (пакетный режим)*

   В IDS, реакция которых происходит через определенные интервалы времени, информационный поток от точек мониторинга до инструментов анализа не является непрерывным. В результате информация обрабатывается способом, аналогичным коммуникационным схемам «сохранить и перенаправить». Многие ранние host-based IDS используют данную схему хронометража, так как они зависят от записей аудита в ОС. Основанные на интервале IDS не выполняют никаких действий, являющихся результатом анализа событий.

2. *Real-Time (непрерывные)*
   Real-time IDS обрабатывают непрерывный поток информации от источников. Чаще всего это является преобладающей схемой в network-based IDS, которые получают информацию из потока сетевого трафика. Термин «реальное время» используется в том же смысле, что и в системах управления процессом. Это означает, что определение проникновения, выполняемое IDS «реального времени», приводит к результатам достаточно быстро, что позволяет IDS выполнять определенные действия в автоматическом режиме.

Network-Based IDS

Основными коммерческими IDS являются Network-based. Эти IDS определяют атаки, захватывая и анализируя сетевые пакеты. Слушая сетевой сегмент, Network-based IDS может просматривать сетевой трафик от нескольких хостов, которые присоединены к сетевому сегменту, и таким образом защищать эти хосты.

Network-based IDS часто состоят из множества сенсоров, расположенных в различных точках сети. Эти устройства просматривают сетевой трафик, выполняя локальный анализ данного трафика и создавая отчеты об атаках для центральной управляющей консоли. Многие из этих сенсоров разработаны для выполнения в «невидимом (stealth)» режиме, чтобы сделать более трудным для атакующего обнаружение их присутствия и расположения.

Преимущества Network-based IDS

- Несколько оптимально расположенных Network-based IDS могут просматривать большую сеть.
- Развертывание network-based IDS не оказывает большого влияния на производительность сети. Network-based IDS обычно являются пассивными устройствами, которые прослушивают сетевой канал без воздействия на нормальное функционирование сети. Таким образом, обычно бывает легко модифицировать топологию сети для размещения Network-based IDS.
- Network-based IDS могут быть сделаны практически неуязвимыми для атак или даже абсолютно невидимыми для атакующих.

Недостатки Network-based IDS

- Для Network-based IDS может быть трудно обрабатывать все пакеты в большой или занятой сети, и, следовательно, они могут пропустить распознавание атаки, которая началась при большом трафике. Некоторые производители пытаются решить данную проблему, полностью реализуя IDS аппаратно, что делает IDS более быстрой. Необходимость быстро анализировать пакеты также может привести к тому, что производители IDS будут определять небольшое количество атак или же использовать как можно меньшие вычислительные ресурсы, что снижает эффективность обнаружения.
- Многие преимущества Network-based IDS неприменимы к более современным сетям, основанным на сетевых коммутаторах (switch). Коммутаторы делят сети на много маленьких сегментов (обычно один fast Ethernet кабель на хост) и обеспечивают выделенные линии между хостами, обслуживаемыми одним и тем же коммутатором. Многие коммутаторы не предоставляют универсального мониторинга портов, и это ограничивает диапазон мониторинга сенсора Network-based IDS только одним хостом.

Даже когда коммутаторы предоставляют такой мониторинг портов, часто единственный порт не может охватить весь трафик, передаваемый коммутатором.

- Network-based IDS не могут анализировать зашифрованную информацию. Эта проблема возрастает, чем больше организации (и атакующие) используют VPN.
- Большинство Network-based IDS не могут сказать, была ли атака успешной; они могут только определить, что атака была начата. Это означает, что после того как Network-based IDS определит атаку, администратор должен вручную исследовать каждый атакованный хост для определения, происходило ли реальное проникновение.
- Некоторые Network-based IDS имеют проблемы с определением сетевых атак, которые включают фрагментированные пакеты. Такие фрагментированные пакеты могут привести к тому, что IDS будет функционировать нестабильно.

Host-Based IDS

Host-based IDS имеют дело с информацией, собранной внутри единственного компьютера. (Заметим, что Application-based IDS на самом деле являются подмножеством Host-based IDS.) Такое выгодное расположение позволяет Host-based IDS анализировать деятельность с большой достоверностью и точностью, определяя только те процессы и пользователей, которые имеют отношение к конкретной атаке в ОС. Более того, в отличии от Network-based IDS, Host-based IDS могут «видеть» последствия предпринятой атаки, так как они могут иметь непосредственный доступ к системной информации, файлам данных и системным процессам, являющимся целью атаки.

Host-based IDS обычно используют информационные источники двух типов: результаты аудита ОС и системные логи. Результаты аудита ОС обычно создаются на уровне ядра ОС и, следовательно, являются более детальными и лучше защищенными, чем системные логи. Однако системные логи намного меньше и не столь многочисленны, как результаты аудита, и, следовательно, легче для понимания. Некоторые Host-based IDS разработаны для поддержки централизованной инфраструктуры управления и получения отчетов IDS, что может допускать единственную консоль управления для отслеживания многих хостов. Другие создают сообщения в формате, который совместим с системами сетевого управления.

Преимущества Host-based IDS

- Host-based IDS, с их возможностью следить за событиями локально относительно хоста, могут определить атаки, которые не могут видеть Network-based IDS.
- Host-based IDS часто могут функционировать в окружении, в котором сетевой трафик зашифрован, когда Host-based источники информации создаются до того, как данные шифруются, и/или после того, как данные расшифровываются на хосте назначения.
- На функционирование Host-based IDS не влияет наличие в сети коммутаторов.
- Когда Host-based IDS работают с результатами аудита ОС, они могут оказать помощь в определении Троянских программ или других атак, которые нарушают целостность ПО.

Недостатки Host-based IDS

- Host-based IDS более трудны в управлении, так как информация должна быть сконфигурирована и должна управляться для каждого просматриваемого хоста.
- Так как, по крайней мере, источники информации (и иногда часть средств анализа) для Host-based IDS расположены на том же хосте, который является целью атаки, то, как составная часть атаки, IDS может быть атакована и запрещена.
- Host-based IDS не полностью соответствуют возможности определения сканирования сети или других аналогичных исследований, когда целью является вся сеть, так как IDS наблюдает только за сетевыми пакетами, получаемыми конкретным хостом.
- Host-based IDS могут быть блокированы некоторыми DoS-атаками.
- Когда Host-based IDS использует результаты аудита ОС в качестве источника информации, количество информации может быть огромно, что потребует дополнительного локального хранения в системе.
- Host-based IDS используют вычислительные ресурсы хостов, за которыми они наблюдают, что влияет на производительность наблюдаемой системы.

Application-Based IDS

Application-Based IDS является специальным подмножеством Host-based IDS, которые анализируют события, поступившие в ПО приложения. Наиболее общими источниками информации, используемыми Application-based IDS, являются лог-файлы транзакций приложения.

Способность взаимодействовать непосредственно с приложением, с конкретным доменом или использовать знания, специфичные для приложения, позволяет Application-based IDS определять подозрительное поведение авторизованных пользователей, которое превышает их права доступа. Такие проблемы могут проявиться только при взаимодействии пользователя с приложением.

Преимущества Application-based IDS

- Application-based IDS могут анализировать взаимодействие между пользователем и приложением, что часто позволяет отследить неавторизованную деятельность конкретного пользователя.
- Application-based IDS зачастую могут работать в зашифрованных окружениях, так как они взаимодействуют с приложением в конечной точке транзакции, где информация представлена уже в незашифрованном виде.

Недостатки application-based IDS

- Application-based IDS могут быть более уязвимы, чем Host-based IDS, для атак на логи приложения, которые могут быть не так хорошо защищены, как результаты аудита ОС, используемые Host-based IDS.
- Application-based IDS часто просматривают события на пользовательском уровне абстракции, на котором обычно невозможно определить Троянские программы или другие подобные атаки, связанные с нарушением целостности ПО. Следовательно, целесообразно использовать Application-based IDS в комбинации с Host-based и/или Network-based IDS.

Анализ, выполняемый IDS

Существует два основных подхода к анализу событий для определения атак: *определение злоупотреблений* (misuse detection) и *определение аномалий* (anomaly detection).

В технологии определения злоупотреблений известно, какая последовательность данных является признаком атаки. Анализ событий состоит в определении таких «плохих» последовательностей данных. Технология определения злоупотреблений используется в большинстве коммерческих систем.

В технологии определения аномалий известно, что представляет собой «нормальная» деятельность и «нормальная» сетевая активность. Анализ событий состоит в попытке определить аномальное поведение пользователя или аномальную сетевую активность. Данная технология на сегодняшний день является предметом исследований и используется в ограниченной форме небольшим числом IDS. Существуют сильные и слабые стороны, связанные с каждым подходом; считается, что наиболее эффективные IDS применяют в основном определение злоупотреблений с небольшими компонентами определения аномалий.

Определение злоупотреблений

Детекторы злоупотреблений анализируют деятельность системы, анализируя событие или множество событий на соответствие заранее определенному образцу, который описывает известную атаку. Соответствие образца известной атаке называется сигнатурой, определение злоупотребления иногда называют «сигнатурным определением». Наиболее общая форма определения злоупотреблений, используемая в коммерческих продуктах, специфицирует каждый образец событий, соответствующий атаке, как отдельную сигнатуру. Тем не менее существует несколько более сложных подходов для выполнения определения злоупотреблений (называемых state-based технологиями анализа), которые могут использовать единственную сигнатуру для определения группы атак.

Преимущества сигнатурного метода

- Детекторы злоупотреблений являются очень эффективными для определения атак и не создают при этом огромного числа ложных сообщений.
- Детекторы злоупотреблений могут быстро и надежно диагностировать использование конкретного инструментального средства или технологии атаки. Это может помочь администратору скорректировать меры обеспечения безопасности.
- Детекторы злоупотреблений позволяют администраторам, независимо от уровня их квалификации в области безопасности, начать процедуры обработки инцидента.

Недостатки сигнатурного метода

- Детекторы злоупотреблений могут определить только те атаки, о которых они знают, следовательно, надо постоянно обновлять их базы данных для получения сигнатур новых атак.
- Многие детекторы злоупотреблений разработаны таким образом, что могут использовать только строго определенные сигнатуры, а это не допускает определения вариантов общих атак. State-based детекторы злоупотреблений

могут обойти данное ограничение, но они применяются в коммерческих IDS не столь широко.

Определение аномалий

Детекторы аномалий определяют ненормальное (необычное) поведение на хосте или в сети. Они предполагают, что атаки отличаются от «нормальной» (законной) деятельности и могут, следовательно, быть определены системой, которая умеет отслеживать эти отличия. Детекторы аномалий создают профили, представляющие собой нормальное поведение пользователей, хостов или сетевых соединений. Эти профили создаются, исходя из данных истории, собранных в период нормального функционирования. Затем детекторы собирают данные о событиях и используют различные метрики для определения того, что анализируемая деятельность отклоняется от нормальной.

Метрики и технологии, используемые при определении аномалий, включают:

- определение допустимого порога. В этом случае основные атрибуты поведения пользователя и системы выражаются в количественных терминах. Для каждого атрибута определяется некоторый уровень, который устанавливается как допустимый. Такие атрибуты поведения могут определять число файлов, доступных пользователю в данный период времени, число неудачных попыток входа в систему, количество времени ЦП, используемое процессом и т.п. Данный уровень может быть статическим или эвристическим − например, может определяться изменением анализируемых значений.
- статистические метрики: параметрические, при которых предполагается, что распределение атрибутов профиля соответствует конкретному образцу, и непараметрические, при которых распределение атрибутов профиля является «обучаемым» исходя из набора значений истории, которые наблюдались за определенный период времени.
- метрики, основанные на правилах, которые аналогичны непараметрическим статистическим метрикам в том, что наблюдаемые данные определяют допустимые используемые образцы, но отличаются от них в том, что эти образцы специфицированы как правила, а не как численные характеристики.
- другие метрики, включая нейросети, генетические алгоритмы и модели иммунных систем.

Только первые две технологии используются в современных коммерческих IDS.

К сожалению, детекторы аномалий и IDS, основанные на них, часто создают большое количество ложных сообщений, так как образцы нормального поведения пользователя или системы могут быть очень неопределенными. Несмотря на этот недостаток, исследователи предполагают, что IDS, основанные на аномалиях, имеют возможность определять новые формы атак, в отличие от IDS, основанных на сигнатурах, которые полагаются на соответствие образцу прошлых атак.

Более того, некоторые формы определения аномалий создают выходные данные, которые могут быть далее использованы в качестве источников информации для детекторов злоупотреблений. Например, детектор аномалий, основанный на пороге, может создавать диаграмму, представляющую собой «нормальное» количество файлов, доступных конкретному пользователю; детектор злоупотреблений может использовать данную диаграмму как часть сигнатуры

обнаружения, которая говорит: «если количество файлов, доступных данному пользователю, превышает данную «нормальную» диаграмму более чем на 10%, следует инициировать предупреждающий сигнал».

Хотя некоторые коммерческие IDS включают ограниченные формы определения аномалий, мало кто полагается исключительно на данную технологию. Определение аномалий, которое существует в коммерческих системах, обычно используется для определения зондирования сети или сканирования портов. Тем не менее определение аномалий остается предметом исследований в области активного определения проникновений, и скорее всего будет играть возрастающую роль в IDS следующих поколений.

Преимущества определения аномалий

- IDS, основанные на определении аномалий, обнаруживают неожиданное поведение и, таким образом, имеют возможность определить симптомы атак без знания конкретных деталей атаки.
- Детекторы аномалий могут создавать информацию, которая в дальнейшем будет использоваться для определения сигнатур для детекторов злоупотреблений.

Недостатки определения аномалий

- Подходы определения аномалий обычно создают большое количество ложных сигналов при непредсказуемом поведении пользователей и непредсказуемой сетевой активности.
- Подходы определения аномалий часто требуют некоторого этапа обучения системы, во время которого определяются характеристики нормального поведения.

Проверка целостности файлов

Проверки целостности файлов являются другим классом инструментальных средств безопасности, которые дополняют IDS. Эти инструментальные средства используют дайджест сообщений или другие криптографические контрольные суммы для критичных файлов и объектов, сравнивая их с хранимыми значениями и оповещая о любых различиях или изменениях.

Использование криптографических контрольных сумм важно, так как атакующие часто изменяют системные файлы по трем причинам. Во-первых, изменение системных файлов могут быть целью атаки (например, размещение Троянских программ), во-вторых, атакующие могут пытаться оставить лазейку (back door) в систему, через которую они смогут снова войти в систему позднее, и, наконец, они пытаются скрыть свои следы, чтобы собственники системы не смогли обнаружить атаку.

Хотя проверка целостности файлов часто используется для определения, были ли изменены системные или выполняемые файлы, такая проверка может также помочь определить, применялись ли модификации для исправления ошибок к программам конкретных производителей или системным файлам. Это также является очень ценным при судебных разбирательствах, так как позволяет быстро и надежно диагностировать следы атаки. Она дает возможность менеджерам оптимизировать восстановление сервиса после произошедшего инцидента.

Система предотвращения вторжений

Intrusion prevention system (IPS) – это программные и аппаратные средства, предназначенные для предотвращения вторжений. Они предназначены для

обнаружения и предотвращения попыток несанкционированного доступа, использования или вывода из строя компьютерных систем, главным образом через Интернет или локальную сеть. Такие попытки могут иметь форму как атаки хакеров или инсайдеров, так и быть результатом действий вредоносных программ. IDS/IPS-системы используются для обнаружения аномальных действий в сети, которые могут нарушить безопасность и конфиденциальность данных, например: попытки использования уязвимостей программного обеспечения; попытки повешения привилегий; несанкционированный доступ к конфиденциальным данным; активность вредоносных программ и т.д.

Использование IPS-систем преследует несколько целей:

- Обнаружить вторжение или сетевую атаку и предотвратить их;
- Спрогнозировать возможные будущие атаки и выявить уязвимости для предотвращения их дальнейшего развития;
- Выполнить документирование существующих угроз;
- Обеспечить контроль качества администрирования с точки зрения безопасности, особенно в больших и сложных сетях;
- Получить полезную информацию о проникновениях, которые имели место, для восстановления и корректирования вызвавших проникновение факторов; Определить расположение источника атаки по отношению к локальной сети (внешние или внутренние атаки), что важно при принятии решений о расположении ресурсов в сети.

В целом, IPS аналогичны IDS. Главное же отличие состоит в том, что они функционируют в реальном времени и могут в автоматическом режиме блокировать сетевые атаки. Каждая IPS включает в себя модуль IDS. IDS, в свою очередь, обычно состоит из:

- системы сбора событий;
- системы анализа собранных событий;
- хранилища, в котором накапливаются собранные события и результаты их анализа;
- базы данных об уязвимостях (этот параметр является ключевым, так как чем больше база у производителя, тем больше угроз способна выявлять система);
- консоли управления, которая позволяет настраивать все системы, осуществлять мониторинг состояния защищаемой сети, просматривать выявленные нарушения и подозрительные действия.

По способам мониторинга IPS-системы можно разделить на две большие группы:

1. NIPS (Network Intrusion Prevention System);
2. HIPS (Host Intrusion Prevention System).

Первая группа ориентирована на сетевой уровень и корпоративный сектор, в то время как представители второй имеют дело с информацией, собранной внутри единственного компьютера, а следовательно могут использоваться на персональных компьютерах. Сегодня HIPS часто входят в состав антивирусных продуктов. Среди NIPS и HIPS также выделяют: Protocol-based IPS, PIPS. Представляет собой систему (либо агент), которая отслеживает и анализирует коммуникационные протоколы со связанными системами или пользователями. Application Protocol-based IPS, APIPS. Представляет собой систему (или агент), которая ведет наблюдение и анализ данных, передаваемых с использованием специфичных для определенных приложений протоколов. Например, отслеживание содержимого SQL-команд. Что касается форм-фактора, IPS-системы

могут быть представлены как в виде отдельного «железного» решения, так и в виде виртуальной машины или софта.

Методы реагирования:

1. После начала атаки:
    - Методы реализуются уже после того, как была обнаружена информационная атака. Это значит, что даже в случае успешного выполнения защищаемой системе может быть нанесён ущерб.
2. Блокирование соединения:
    - Если для атаки используется TCP-соединение, то реализуется его закрытие с помощью посылки каждому или одному из участников TCP-пакета с установленным флагом RST.
    - В результате злоумышленник лишается возможности продолжать атаку, используя это сетевое соединение. Данный метод, чаще всего, реализуется с помощью имеющихся сетевых датчиков.
    - Метод характеризуется двумя основными недостатки:
        i. Не поддерживает протоколы, отличные от TCP, для которых не требуется предварительного установления соединения (например, UDP и ICMP).
        ii. Метод может быть использован только после того, как злоумышленник уже получил несанкционированное соединение.
3. Блокирование записей пользователей:
    - Если несколько учётных записей пользователей были скомпрометированы в результате атаки или оказались их источниками, то осуществляется их блокирование хостовыми датчиками системы. Для блокировки датчики должны быть запущены от имени учётной записи, имеющей права администратора.
    - Также блокирование может происходить на заданный срок, который определяется настройками Системы предотвращения вторжений.
4. Блокирование хоста компьютерной сети
    - Если с одного из хостов была зафиксирована атака, то может быть произведена его блокировка хостовыми датчиками или блокирование сетевых интерфейсов либо на нём, либо на маршрутизаторе или коммутаторе, при помощи которых хост подключён к сети. Разблокирование может происходить спустя заданный промежуток времени или при помощи активации администратора безопасности. Блокировка не отменяется из-за перезапуска или отключения от сети хоста. Так же для нейтрализации атаки можно блокировать цель, хост компьютерной сети.
5. Блокирование атаки с помощью межсетевого экрана
    - IPS формирует и отсылает новые конфигурации в МЭ, по которым экран будет фильтровать трафик от нарушителя.

Такая реконфигурация может происходить в автоматическом режиме с помощью стандартов OPSEC (например, SAMP, CPMI).

6. Изменение конфигурации коммуникационного оборудования:
    - Для протокола SNMP, IPS анализирует и изменяет параметры из базы данных MIB (такие как таблиц маршрутизации, настройки портов) с помощью агента устройства, чтобы блокировать атаку. Также могут использованы протоколы TFTP, Telnet и др.
7. Активное подавление источника атаки:
    - Метод теоретически может быть использован, если другие методы окажутся бесполезны. IPS выявляет и блокирует пакеты нарушителя, и осуществляет атаку на его узел, при условии, что его адрес однозначно определён и в результате таких действий не будет нанесён вред другим легальным узлам.
    - Так как гарантировать выполнение всех условий невозможно, широкое применение метода на практике пока невозможно.
8. В начале атаки:
    - Методы реализуют меры, которые предотвращают обнаруженные атаки до того как они достигают цели.
9. С помощью сетевых датчиков:
    - Сетевые датчики устанавливаются в разрыв канала связи так, чтобы анализировать все проходящие пакеты. Для этого они оснащаются двумя сетевыми адаптерами, функционирующими в «смешанном режиме», на приём и на передачу, записывая все проходящие пакеты в буферную память, откуда они считываются модулем выявления атак IPS. В случае обнаружения атаки эти пакеты могут быть удалены.
    - Анализ пакетов проводится на основе сигнатурного или поведенческого методов.
10. С помощью хостовых датчиков:
    - Удаленные атаки, реализуемые отправкой от злоумышленника серией пакетов. Защита реализуется с помощью сетевой компоненты IPS по аналогии с сетевыми датчиками, но в отличие от последних сетевая компонента перехватывает и анализирует пакеты на различных уровнях взаимодействия, что даёт предотвращать атаки по криптозащищённым IPsec- и SSL/TLS соединениям.
    - Локальные атаки при несанкционированном запуске злоумышленником программ или других действиях, нарушающих информационную безопасность. Перехватывая системные вызовы всех приложений и анализируя их, датчики блокируют те вызовы, которые представляют опасность.

Криптографические средства защиты информации

Современная криптография включает в себя четыре крупных раздела:

1. *Симметричные криптосистемы*. В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ. (Шифрование − преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом, дешифрование − обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный).
2. *Криптосистемы с открытым ключом*. В системах с открытым ключом используются два ключа − открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения (ключ − информация, необходимая для беспрепятственного шифрования и дешифрования текстов.).
3. *Электронная подпись*. Системой электронной подписи называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.
4. *Управление ключами*. Это процесс системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Основные направления использования криптографических методов − передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Требования к криптосистемам

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;
- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);
- знание алгоритма шифрования не должно влиять на надежность защиты;

- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
- структурные элементы алгоритма шифрования должны быть неизменными;
- дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;
- длина шифрованного текста должна быть равной длине исходного текста;
- не должно быть простых и легко устанавливаемых зависимостью между ключами, последовательно используемыми в процессе шифрования;
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Симметричные криптосистемы

Все многообразие существующих криптографических методов в симметричных криптосистемах можно свести к следующим 4 классам преобразований:

- подстановка − символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее определенным правилом;
- перестановка − символы шифруемого текста переставляются по некоторому правилу в пределах заданного блока передаваемого текста;
- аналитическое преобразование − шифруемый текст преобразуется по некоторому аналитическому правилу, например гаммирование − заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа;
- комбинированное преобразование − представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста. Блочные шифры на практике встречаются чаще, чем “чистые” преобразования того или иного класса в силу их более высокой криптостойкости. Российский и американский стандарты шифрования основаны именно на этом классе.

Системы с открытым ключом

Как бы ни были сложны и надежны криптографические системы − их слабое место при практической реализации − проблема распределения ключей. Для того чтобы был возможен обмен конфиденциальной информацией между двумя субъектами ИС, ключ должен быть сгенерирован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому. Т.е. в общем случае для передачи ключа опять же требуется использование какой-то криптосистемы. Для решения этой проблемы на основе результатов, полученных классической и современной алгеброй, были предложены системы с открытым ключом. Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым, а другой закрытым. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне. Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст в принципе не может быть расшифрован

тем же открытым ключом. Дешифрование сообщения возможно только с использованием закрытого ключа, который известен только самому адресату. Криптографические системы с открытым ключом используют так называемые необратимые или односторонние функции, которые обладают следующим свойством: при заданном значении x относительно просто вычислить значение f(x), однако если y=f(x), то нет простого пути для вычисления значения x. Множество классов необратимых функций и порождает все разнообразие систем с открытым ключом. Однако не всякая необратимая функция годится для использования в реальных ИС. В самом определении необратимости присутствует неопределенность. Под необратимостью понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение используя современные вычислительные средства за обозримый интервал времени. Поэтому чтобы гарантировать надежную защиту информации, к системам с открытым ключом (СОК) предъявляются два важных и очевидных требования:

1. Преобразование исходного текста должно быть необратимым и исключать его восстановление на основе открытого ключа.
2. Определение закрытого ключа на основе открытого также должно быть невозможным на современном технологическом уровне. При этом желательна точная нижняя оценка сложности (количества операций) раскрытия шифра.

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах. Так, алгоритм RSA стал мировым стандартом де-факто для открытых систем. Вообще же все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований:

- Разложение больших чисел на простые множители;
- Вычисление логарифма в конечном поле;
- Вычисление корней алгебраических уравнений.

Здесь же следует отметить, что алгоритмы криптосистемы с открытым ключом (СОК) можно использовать в следующих назначениях:

1. Как самостоятельные средства защиты передаваемых и хранимых данных.
2. Как средства для распределения ключей.

Алгоритмы СОК более трудоемки, чем традиционные криптосистемы. Поэтому часто на практике рационально с помощью СОК распределять ключи, объем которых как информации незначителен. А потом с помощью обычных алгоритмов осуществлять обмен большими информационными потоками. Один из наиболее распространенных − система с открытым ключом − RSA. Криптосистема RSA, разработанная в 1977 году и получила название в честь ее создателей: Рона Ривеста, Ади Шамира и Леонарда Эйдельмана. Они воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо. Доказано (теорема Рабина), что раскрытие шифра RSA эквивалентно такому разложению. Поэтому для любой длины ключа можно дать нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время. Возможность гарантированно оценить защищенность алгоритма RSA стала одной из причин популярности этой СОК на фоне десятков других схем. Поэтому алгоритм RSA используется в банковских компьютерных сетях, особенно для работы с удаленными клиентами (обслуживание кредитных карточек).

Электронная подпись

В чем состоит проблема аутентификации данных? В конце обычного письма или документа исполнитель или ответственное лицо обычно ставит свою подпись. Подобное действие обычно преследует две цели. Во-первых, получатель имеет возможность убедиться в истинности письма, сличив подпись с имеющимся у него образцом. Во-вторых, личная подпись является юридическим гарантом авторства документа. Последний аспект особенно важен при заключении разного рода торговых сделок, составлении доверенностей, обязательств и т.д. Если подделать подпись человека на бумаге весьма непросто, а установить авторство подписи современными криминалистическими методами − техническая деталь, то с подписью электронной дело обстоит иначе. Подделать цепочку битов, просто её, скопировав, или незаметно внести нелегальные исправления в документ сможет любой пользователь. С широким распространением в современном мире электронных форм документов (в том числе и конфиденциальных) и средств их обработки особо актуальной стала проблема установления подлинности и авторства безбумажной документации. В разделе криптографических систем с открытым ключом было показано, что при всех преимуществах современных систем шифрования они не позволяют обеспечить аутентификацию данных. Поэтому средства аутентификации должны использоваться в комплексе и криптографическими алгоритмами.

Управление ключами

Кроме выбора подходящей для конкретной ИС криптографической системы, важная проблема − управление ключами. Как бы ни была сложна и надежна сама криптосистема, она основана на использовании ключей. Если для обеспечения конфиденциального обмена информацией между двумя пользователями процесс обмена ключами тривиален, то в ИС, где количество пользователей составляет десятки и сотни управление ключами − серьезная проблема. Под ключевой информацией понимается совокупность всех действующих в ИС ключей. Если не обеспечено достаточно надежное управление ключевой информацией, то завладев ею, злоумышленник получает неограниченный доступ ко всей информации. Управление ключами − информационный процесс, включающий в себя три элемента:

- генерацию ключей;
- накопление ключей;
- распределение ключей.

Рассмотрим, как они должны быть реализованы для того, чтобы обеспечить безопасность ключевой информации в ИС.

Генерация ключей

Не стоит использовать неслучайные ключи с целью легкости их запоминания. В серьезных ИС используются специальные аппаратные и программные методы генерации случайных ключей. Как правило, используют датчики ПСЧ. Однако степень случайности их генерации должна быть достаточно высоким. Идеальным генераторами являются устройства на основе “натуральных” случайных процессов. Например, случайным математическим объектом являются десятичные знаки иррациональных чисел, которые вычисляются с помощью стандартных математических методов.

Накопление ключей

Под накоплением ключей понимается организация их хранения, учета и удаления. Поскольку ключ является самым привлекательным для злоумышленника объектом, открывающим ему путь к конфиденциальной информации, то вопросам накопления ключей следует уделять особое внимание. Секретные ключи никогда не должны записываться в явном виде на носителе, который может быть считан или скопирован. В достаточно сложной ИС один пользователь может работать с большим объемом ключевой информации, и иногда даже возникает необходимость организации мини-баз данных по ключевой информации. Такие базы данных отвечают за принятие, хранение, учет и удаление используемых ключей. Итак, каждая информация об используемых ключах должна храниться в зашифрованном виде. Ключи, зашифровывающие ключевую информацию называются мастер-ключами. Желательно, чтобы мастер-ключи каждый пользователь знал наизусть, и не хранил их вообще на каких-либо материальных носителях. Очень важным условием безопасности информации является периодическое обновление ключевой информации в ИС. При этом переназначаться должны как обычные ключи, так и мастер-ключи. В особо ответственных ИС обновление ключевой информации желательно делать ежедневно. Вопрос обновления ключевой информации связан и с третьим элементом управления ключами − распределением ключей.

Распределение ключей

Распределение ключей − самый ответственный процесс в управлении ключами. К нему предъявляются два требования:

- Оперативность и точность распределения;
- Скрытность распределяемых ключей.

В последнее время заметен сдвиг в сторону использования криптосистем с открытым ключом, в которых проблема распределения ключей отпадает. Тем не менее распределение ключевой информации в ИС требует новых эффективных решений. Распределение ключей между пользователями реализуются двумя разными подходами:

1. Путем создания одного ли нескольких центров распределения ключей. Недостаток такого подхода состоит в том, что в центре распределения известно, кому и какие ключи назначены и это позволяет читать все сообщения, циркулирующие в ИС. Возможные злоупотребления существенно влияют на защиту.
2. Прямой обмен ключами между пользователями информационной системы. В этом случае проблема состоит в том, чтобы надежно удостоверить подлинность субъектов. Для обмена ключами можно использовать криптосистемы с открытым ключом, используя тот же алгоритм RSA.

В качестве обобщения сказанного о распределении ключей следует сказать следующее. Задача управления ключами сводится к поиску такого протокола распределения ключей, который обеспечивал бы:

- возможность отказа от центра распределения ключей;
- взаимное подтверждение подлинности участников сеанса;
- подтверждение достоверности сеанса механизмом запроса-ответа, использование для этого программных или аппаратных средств;
- использование при обмене ключами минимального числа сообщений.

Реализация криптографических методов

Проблема реализации методов защиты информации имеет два аспекта:

- разработку средств, реализующих криптографические алгоритмы;
- методику использования этих средств.

Каждый из рассмотренных криптографических методов могут быть реализованы либо программным, либо аппаратным способом. Возможность программной реализации обуславливается тем, что все методы криптографического преобразования формальны и могут быть представлены в виде конечной алгоритмической процедуры. При аппаратной реализации все процедуры шифрования и дешифрования выполняются специальными электронными схемами. Наибольшее распространение получили модули, реализующие комбинированные методы. Большинство зарубежных серийных средств шифрования основано на американском стандарте DES. Отечественные же разработки, такие как, например, устройство КРИПТОН, использует отечественный стандарт шифрования. Основным достоинством программных методов реализации защиты является их гибкость, т.е. возможность быстрого изменения алгоритмов шифрования. Основным же недостатком программной реализации является существенно меньшее быстродействие по сравнению с аппаратными средствами (примерно в 10 раз). В последнее время стали появляться комбинированные средства шифрования, так называемые программно-аппаратные средства. В этом случае в компьютере используется своеобразный «криптографический сопроцессор» − вычислительное устройство, ориентированное на выполнение криптографических операций (сложение по модулю, сдвиг и т.д.). Меняя программное обеспечения для такого устройства, можно выбирать тот или иной метод шифрования. Такой метод объединяет в себе достоинства программных и аппаратных методов.

Таким образом, выбор типа реализации криптозащиты для конкретной ИС в существенной мере зависит от ее особенностей и должен опираться на всесторонний анализ требований, предъявляемых к системе защиты информации.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА И РЕСУРСЫ СЕТИ ИНТЕРНЕТ

1. Беляев М.А. Основы информатики / Беляев М.А., Лысенко В.В., Малинина Л.А. – СПБ: Высшее образование, 1999. – 200 с.
2. Фролов А. В. Антивирусная защита: Учебное пособие для защиты информационных ресурсов – СПБ: Питер, 2004. – 324 с.
3. Официальная страница INTUIT: [Электронный ресурс]. – URL: http://www.intuit.ru/studies/courses/102/102/lecture/2989.
4. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. − М.: КУДИЦ-ОБРАЗ, 2001. − 368 с.
5. Кульгин М. Технологии корпоративных сетей. Энциклопедия. − СПб.: Питер, 2000. − 704 с.
6. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. − СПб.: Питер, 2001. − 672 с.
7. Романец Ю. В. Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2-е изд. − М: Радио и связь, 2002. − 328 с.
8. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. Высш. Учеб. Заведений / Павел борисович Хорев. – М.: Издательский центр «Академия», 2005. – 356 с.
9. Официальная страница NETCONFIG: [Электронный ресурс]. – URL: http://www.netconfig.ru/server/ids-ips/ .
10. Denning, Dorothy E. An Intrusion Detection Model, Proceedings of the Seventh IEEE Symposium on Security and Privacy. May 1986, 119-131 с.
11. Официальная страница ANTI-MALWARE: [Электронный ресурс]. – URL: https://www.anti−malware.ru/node/12201.
12. Официальная страница infosecmd: [Электронный ресурс]. – URL: http://infosecmd.narod.ru/gl5.html.

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Кафедра была создана в 1937 году и является одной из старейших и авторитетнейших научно-педагогических школ России. Первым заведующим кафедрой был **профессор М.Ф. Маликов.**

Первоначально кафедра называлась кафедрой счетно-решающих и математических приборов и занималась разработкой электромеханических вычислительных устройств и приборов управления. На кафедре развивалось два направления вычислительной техники: машины непрерывного действия (приборы управления) и машины дискретного действия (счетные или, как они тогда назывались, счетно-аналитические).

В сентябре 1937 года при кафедре была создана лаборатория. Ее первым заведующим был К.Г. Кроль (впоследствии – доцент кафедры). К осени 1939 года кафедра стала одной из ведущих в институте. Для чтения отдельных разделов курсов и руководства дипломными проектами привлекались ведущие специалисты промышленности. Все курсы были обеспечены преподавателями, велись лекционные и лабораторные занятия, выполнялись курсовые и дипломные проекты. В эти годы кафедра ежегодно выпускала около 20 инженеров.

С 1944 года кафедрой заведовал **профессор С.А. Изенбек.** В послевоенный период на кафедре были развернуты исследования принципов построения электромеханических вычислительных устройств. На их основе были разработаны тренажеры, приборы для автоматизации прочностных расчетов и обработки результатов ходовых испытаний кораблей.

В 1950-х годах на кафедре функционировали три учебно-исследовательские лаборатории: электромеханических и счетно-решающих устройств, счетных и счетно-аналитических машин, приборов управления. В них исследовались счетно-решающие устройства на потенциометрах, приборы для автоматизации расчетов и электронные счетные устройства.

Эксперименты по применению электронных машин для выполнения операций над числами, проводимые доцентом Ф.Я. Галкиным и инженером М.Н.Романовым, позволили разработать проект электронной вычислительной машины для инженерных расчетов. Он был поддержан руководителем проблемной оптической лаборатории института **профессором М.М. Русиновым.**

В 1956 году началось изготовление ЭВМ. Создание электронно-вычислительных машин собственной разработки началось в ЛИТМО, когда ЭВМ, такие как «Урал», еще только создавались. В 1962 − 1964 годах была создана ЭВМ «ЛИТМО-2» на ферриттранзисторных модулях.

В 1962 году заведующим кафедрой был избран **профессор С.А. Майоров**, и в 1963 году кафедра была переименована в **кафедру вычислительной техники**.

С начала 60−х годов на кафедре развернулись работы по методам проектирования ЭВМ: имитационному моделированию цифровых устройств (**Новиков Геннадий Иванович**), анализу и синтезу переключательных схем (**Немолочнов Олег Фомич**), тестированию и диагностике схем (Гольдман Р.С., Немолочнов О.Ф.), машинному анализу электронных схем (Ермолаенков Э.Г.), монтажно-коммутационному проектированию (Шипилов П.А.). Автоматизация проектирования ЭВМ стала основным научным направление кафедры.

Кафедра вычислительной техники является одной из крупнейших в университете, на которой работают высококвалифицированные специалисты, в том числе 8 профессоров и 15 доцентов, обучающие около 500 студентов и 30 аспирантов.

Кафедра имеет 4 компьютерных класса, объединяющих более 70 компьютеров в локальную вычислительную сеть кафедры и обеспечивающих доступ студентов ко всем информационным ресурсам кафедры и выход в Интернет. Кроме того, на кафедре имеются учебные и научно-исследовательские лаборатории по вычислительной технике, в которых работают студенты кафедры.

На кафедре сформировалась и действует **научно-педагогическая школа «Организация вычислительных систем и сетей».**

В настоящее время кафедрой заведует **доктор технических наук, профессор Алиев Тауфик Измайлович.**

Маркина Татьяна Анатольевна

Управление проектами в информационных технологиях

Учебное пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати 26.12.2016
Заказ № 3809
Тираж 70
Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49