МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ
УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)» (СГАУ)

Программно-аппаратные средства обеспечения информационной безопасности

Электронный учебно-методический комплекс
по дисциплине в LMS Moodle

САМАРА
2012

УДК 004.056.5

Автор-составитель: **Жмуров Денис Борисович**

Программно-аппаратные средства обеспечения информационной безопасности

[Электронный ресурс] : электрон. учеб.-метод. комплекс по дисциплине в LMS Moodle / Минобрнауки России, Самар. гос. аэрокосм. ун-т им. С. П. Королева (нац. исслед. ун-т); авт.-сост. Д.Б. Жмуров. - Электрон. текстовые и граф. дан. - Самара, 2012. – 1 эл. опт. диск (CDROM).

В состав учебно-методического комплекса входят:

1. Курс лекций.
2. Методические указания по выполнению лабораторных работ.
3. Примерные темы УИРС.
4. Тест по дисциплине.
5. Вопросы к экзамену по дисциплине.

УМКД «Программно-аппаратные средства обеспечения информационной безопасности» предназначен для студентов факультета информатики, обучающихся по направлению подготовки специалистов 090303.65 «Информационная безопасность автоматизированных систем» (специалитет) в 9 семестре.

УМКД разработан на кафедре ГИиИБ.

Политика информационной безопасности

Рассмотрены вопросы политики информационной безопасности, методика разработки политик, создания, развертывания и эффективного использования.

Наверное, самая неинтересная часть профессиональной работы в сфере информационной безопасности - это разработка политики. Развертывание политики не требует глубоких технических знаний и, таким образом, не очень привлекает профессионалов. Кроме того, не ждите благодарности, поскольку не многим сотрудникам понравятся результаты этой работы.

Политика устанавливает правила. Политика заставляет людей делать вещи, которые они не хотят делать. Но политика имеет огромное значение для организации и, вероятно, является наиболее важной работой отдела информационной безопасности.

Необходимость и важность политики

Политика безопасности организации (organizational security policies): Совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности(ГОСТ Р ИСО/МЭК 15408).

Политика устанавливает правила, которые определяют конфигурацию систем, действия служащих организации в обычных условиях и в случае непредвиденных обстоятельств. Таким образом, политика выполняет две основные функции:

- определяет безопасность внутри организации;
- определяет место каждого служащего в системе безопасности.

Какой должна быть безопасность

Политика определяет способы развертывания системы безопасности. Сюда входит правильная настройка компьютерных систем и сетей в соответствии с требованиями физической безопасности. Политика определяет надлежащие механизмы, используемые для защиты информации и систем.

Однако технические аспекты - это не единственное, что определяется политикой. Она ясно устанавливает порядок осуществления служащими своих обязанностей, связанных с вопросами безопасности, например, для администраторов. Она определяет поведение пользователей при использовании компьютерных систем, размещенных в организации.

И, наконец, устанавливает порядок реагирования в случае каких-либо непредвиденных обстоятельств. Если происходит инцидент, связанный с нарушением безопасности, или система дает сбой в работе, политики и процедуры устанавливают порядок действий и выполняемые задачи, направленные на устранение последствий этого инцидента.

Определение места каждого работника

Правила достаточно серьезны и являются необходимой частью действующей в организации программы безопасности. Таким образом, очень важно, что все службы работали во взаимодействии для построения надежной системы безопасности. Политика показывает основные направления деятельности работников компании в этой совместной работе. Политики и процедуры определяют задачи и цели программы безопасности. Когда эти задачи и цели должным образом поддерживаются служащими, это обеспечивает базу для коллективной работы в сфере безопасности.

Внимание!

В этой ситуации важную роль играет обучение, которое идет "рука об руку" с политикой. Если в организации не уделяется должного внимания программам информирования в сфере безопасности, то при развертывании политики возможно возникновение проблем.

Разработка различных политик

Существует большое количество типов политик и процедур, которые определяют функционирование системы безопасности в организации. В следующих разделах мы покажем основные концепции, полезные и широко используемые на практике. Все эти концепции можно скомбинировать для лучшего использования в вашей организации. Три раздела каждой политики являются общепринятыми.

- Цель. Каждая политика и процедура имеют четко определенную цель, которая ясно описывает, почему создана та или иная политика или процедура, и какую выгоду от этого надеется получить организация.
- Область. Каждая политика и процедура имеет раздел, описывающий ее сферу приложения. Например, политика безопасности применяется ко всем компьютерным и сетевым системам. Информационная политика применяется ко всем служащим.
- Ответственность. В разделе об ответственности определяются лица, ответственные за соблюдение политик или процедур. Этот человек должен быть надлежащим образом обучен и знать все требования политики.

Информационная политика

Информационная политика определяет секретную информацию внутри организации и способы ее защиты. Политика разрабатывается таким образом, чтобы охватить всю существующую информацию. Каждый служащий отвечает за безопасность секретной информации, с которой он сталкивается в работе. Информация может быть представлена на бумажных носителях или в виде файлов на компьютере. Политика должна предусмотреть защиту для всех форм представления информации.

Выявление секретной информации

Информация, считающаяся секретной, различается в зависимости от сферы деятельности организации. Секретные сведения включают деловые книги, проекты, патентную информацию, телефонные книги компании и т. д.

Определенная информация считается секретной для всех организаций - это сведения о выплатах, домашние адреса и номера телефонов служащих, информация о медицинском страховании и любая финансовая информация, закрытая для широкой публики.

Определение секретной информация должно быть тщательно и четко сформулировано в политике и донесено до служащих с документальным оформлением.

Определение секретной информации можно найти в законодательных актах и предписаниях. Поработайте с главным юрисконсультом своей организации и убедитесь, что вы четко представляете, какая информация является секретной..

Классифицирование

Двух или трех уровней классификации обычно достаточно для любой организации. Самый нижний уровень классификации - это общая информация. Над этим уровнем находится информация, недоступная для общего пользования. Она называется проприетарной, секретной или конфиденциальной. Такая информация доступна для отдельных служащих организации или для тех компаний, которые подписали соглашение о ее неразглашении. Если эта информация будет открыта для общего доступа или попадет к конкурентам, то организации будет нанесен значительный ущерб.

Существует третий уровень секретности, который называется "для служебного пользования" или "защищенная информация". Доступ к подобным сведениям открыт для ограниченного количества служащих.

Маркировка и хранение секретной информации

Для каждого уровня секретной информации, находящегося над уровнем общей, политика должна определять способ маркировки. Если информация представлена в виде бумажных документов, то каждая страница маркируется вверху и внизу. Это легко сделать в текстовом редакторе с помощью верхних и нижних колонтитулов. Обычно используют заглавные буквы, выделенные полужирным шрифтом или курсивом, различные гарнитуры шрифта, чтобы сделать текст удобочитаемым.

Никакие секретные документы не должны оставаться на рабочих столах, здесь должна работать политика чистых столов. Закрывайте секретные бумаги в сейфах или ящиках столов. Если кабинет служащего, работающего с секретной информацией, закрывается, то можно разрешить хранение информации в этом кабинете.

Если данные записаны в компьютерных системах, политика должна определить соответствующие уровни защиты. Это может быть управление доступом к файлам или специальная парольная защита для определенных типов документов. В ответственных ситуациях используется шифрование. Имейте в виду, что системным администраторам доступны любые документы в системе. Если вы хотите скрыть защищаемую информацию от них, то единственным способом является шифрование.

Передача секретной информации

Информационная политика должна определять способы передачи секретной информации. Данные передаются различными путями (электронная почта, обычная почта, факс), и в политике должен быть оговорен каждый из них.

Если секретные данные передаются через электронную почту, то устанавливается обязательное шифрование файлов, вложенных в сообщение, либо тела сообщения. Если посылается твердая копия данных, то определяется метод с использованием письменной расписки (квитанции) - срочная доставка курьерской почтой или заказным письмом. При передаче документа по факсу необходимо, чтобы получатель находился около аппарата во время приема документа, иначе вы рискуете выставить секретные сведения на обозрение всем сотрудникам организации

Уничтожение секретной информации

Если важный документ просто выбрасывается в мусорную корзину, то он становится добычей для злоумышленников. Секретные документы нужно разрезать на мелкие части. Канцелярская бумагорезательная машина дает дополнительный уровень защиты, измельчая документ в продольном и поперечном направлении. Вряд ли такой документ можно восстановить!

Информацию в компьютерных системах можно восстановить после удаления, если она удалена неправильно. Существуют коммерческие программы, которые стирают данные с магнитных носителей без возможности их восстановления, например PGP desktop и BCWipe.

Примечание

Существуют способы восстановления данных на электронных носителях, даже если поверх что-то записано. Однако такая аппаратура дорого стоит, поэтому вряд ли применяется для получения коммерческой информации. Таким образом, дополнительное физическое уничтожение самих носителей обычно не требуются.

Политика безопасности

Политика безопасности определяет технические требования к защите компьютерных систем и сетевой аппаратуры, способы настройки систем администратором с точки зрения их безопасности. Эта конфигурация будет оказывать влияние на пользователей, и некоторые требования, установленные в политике, связаны со всем коллективом пользователей. Главная ответственность за развертывание этой политики ложится на системных и сетевых администраторов при поддержке руководства.

Политика безопасности определяет требования, выполнение которых должно быть обеспечено на каждой системе. Однако политика сама по себе не определяет конкретную конфигурацию различных операционных систем. Это устанавливается в отдельных процедурах по настройке. Такие процедуры могут быть размещены в приложении к политике.

Идентификация и аутентификация

Политика безопасности определяет порядок идентификации пользователей: либо стандарт для идентификаторов пользователей, либо раздел в процедуре системного администрирования, в котором определяется этот стандарт.

Очень важно, чтобы был установлен основной механизм для аутентификации пользователей и администраторов. Если это пароли, то в политике определяется минимальная длина пароля, максимальный и минимальный возраст пароля и требования к его содержимому.

Каждая организация во время разработки своей политики безопасности должна определить, будут ли учетные записи администраторов использовать те же самые механизмы аутентификации, что и обычные пользователи, или же более строгие. Более строгий механизм должен быть описан в соответствующем разделе политики. Он может также использоваться для удаленного доступа через виртуальные частные сети или соединения наборного доступа (dial-up).

Примечание

В большинстве случаев учетные записи администраторов должны использовать сильные механизмы аутентификации (например смарт-карты).

Управление доступом

Политика безопасности устанавливает стандартные требования к управлению доступом к электронным файлам, в которых предусматриваются формы управления доступом пользователей по умолчанию, доступные для каждого файла в системе. Этот механизм работает в паре с аутентификационным механизмом и гарантирует, что только авторизованные пользователи получают доступ к файлам. Также четко оговариваются пользователи, имеющие доступ к файлам с разрешениями на чтение, запись и исполнение.

Настройки по умолчанию для новых файлов устанавливают разрешения, принимаемые при создании нового файла. В этом разделе политики определяются разрешения на чтение, запись и исполнение, которые даются владельцам файлов и прочим пользователям системы.

Аудит

Раздел, посвященный аудиту в политике безопасности, определяет типы событий, отслеживаемых во всех системах. Стандартными событиями являются следующие:

- попытки входа в систему (успешные или неудачные);
- выход из системы;
- ошибки доступа к файлам или системным объектам;
- попытки удаленного доступа (успешные или неудачные);
- действия привилегированных пользователей (администраторов), успешные или неудачные;
- системные события (выключение и перезагрузка).

Каждое событие должно включать следующую информацию:

- ID пользователя (если имеется);
- дата и время;
- ID процесса (если имеется);
- выполненное действие;
- успешное или неудачное завершение события.

В политике безопасности устанавливается срок и способ хранения записей аудита. По возможности указывается способ и частота просмотра этих записей.

Примечание

Во многих организациях применяется политика длительного хранения информации. Перед разработкой политики безопасности внимательно ознакомьтесь с существующими правилами, чтобы в разных политиках не было похожих требований.

Сетевые соединения

Для каждого типа соединений в сети политика безопасности описывает правила установки сетевых соединений и используемые механизмы защиты.

Соединения наборного доступа. Требования к этим соединениям устанавливают технические правила аутентификации и аутентификации для каждого типа соединения. Они излагаются в разделе аутентификации политики и могут устанавливать более сильные способы аутентификации, чем обычные. Кроме того, в политике определяются требования к аутентификации при получении доступа через соединения наборного доступа. Для организации целесообразно установить строгий контроль над разрешенными точками доступа, чтобы соблюдать требования авторизации в сети.

Выделенные линии. В организациях используются различные типы выделенных линий, и для каждого типа необходимо определить устройства защиты. Чаще всего такими устройствами являются межсетевые экраны.

Только лишь указание типа устройства само по себе не предусматривает какого-либо уровня защиты. Политика безопасности должна определять базовую политику контроля доступа, применяемую на устройстве, а также процедуру запроса и получения доступа, не являющуюся частью стандартной конфигурации.

Удаленный доступ к внутренним системам. Нередко организации позволяют своим сотрудникам осуществлять доступ к внутренним системам из внешних удаленных местоположений. Политика безопасности должна определять механизмы, используемые при осуществлении такого доступа. Необходимо указать, чтобы все соединения были защищены шифрованием, определить специфику, связанную с типом шифрования. Так как подключение осуществляется извне организации, рекомендуется использовать надежный механизм аутентификации. Кроме того, политика безопасности должна определять процедуру прохождения авторизации для такого доступа.

Беспроводные сети. Беспроводные сети становятся популярными, и установка в подразделении беспроводной связи без ведома отдела информационных технологий уже стала обычным делом. Политика безопасности должна определять условия, при

которых разрешается использование беспроводных соединений, и то, каким образом будет осуществляться авторизация в такой сети.

Если предполагается разрешить использование беспроводной сети, то необходимо указать дополнительные требования, предъявляемые к аутентификации или шифрованию.

Примечание

Беспроводные сети должны рассматриваться как внешние незащищенные сети, а не как часть внутренней сети организации. Если так и есть на самом деле, данный факт должен быть отмечен в политике.

Вредоносный код

В политике безопасности должно быть определено размещение программ безопасности, отслеживающих вредоносный код (вирусы, черви, "черные ходы" и "троянские кони"). В качестве мест размещения указываются файловые серверы, рабочие станции и серверы электронной почты.

Политика безопасности должна предусматривать определение требований для таких защитных программ. В эти требования может входить проверка определенных типов файлов и проверка файлов при открытии или согласно расписанию.

В политике также указываются требования к периодическому (например, ежемесячному) обновлению признаков вредоносного кода для защитных программ.

Шифрование

Политика безопасности должна определять приемлемые алгоритмы шифрования для применения внутри организации и ссылаться на информационную политику для указания соответствующих алгоритмов для защиты секретной информации. В такой политике совершенно не обязательно указывать какой-либо один конкретный алгоритм. Политика безопасности также определяет процедуры управления ключами.

Отказ от защиты

Несмотря на всевозможные усилия сотрудников отдела безопасности, менеджеров и системных администраторов, обязательно возникнут ситуации, когда будут запущены системы, не отвечающим требованиям политики безопасности. В этих системах, скорее всего, будут выполняться задачи, связанные с бизнес-процессами организации, причем эти задачи будут ставиться выше политик безопасности. На этот случай в политике безопасности предусматривается механизм, оценивающий степень риска, которому подвергается организация; кроме того, данная политика должна обеспечивать разработку плана действий, предпринимаемых при возникновении непредвиденных обстоятельств.

Процесс отказа от защиты предназначен для использования именно в этой ситуации. В каждом конкретном случае конструктор системы или менеджер проекта должен заполнять форму отказа следующей информацией.

- Система с отказом от защиты.
- Раздел политики безопасности, соответствие которому будет нарушено.
- Ответвления организации (обуславливают повышенную степень риска).
- Шаги, предпринимаемые для снижения или контроля степени опасности.
- План восстановления соответствия системы требованиям политики безопасности.

Отдел информационной безопасности должен просмотреть запрос об отказе от защиты и предоставить свою оценку риска, рекомендации по его снижению и управлению потенциально опасными ситуациями. На практике должна осуществляться совместная работа менеджера проекта и специалистов по безопасности для обработки всех возможных ситуаций, чтобы по завершении заполнения отказа от защиты обе стороны достигли договоренности по всем пунктам.

Наконец, отказ от защиты подписывается должностным лицом организации, ответственным за проект. Он таким образом заверяет свое понимание потенциальной опасности, связанной с отказом от защиты, и соглашается с необходимостью отказа организации от соответствия требованиям защиты. Кроме этого, подпись должностного лица означает согласие с тем, что шаги по контролю над степенью риска соответствуют требованиям и будут выполняться (при необходимости).

Приложения

В приложениях или в отдельных описаниях процедур должны размещаться подробные сведения о конфигурации для различных операционных систем, сетевых устройств и другого телекоммуникационного оборудования. Это позволяет модифицировать документы по мере необходимости без изменения политики безопасности организации.

Политика использования компьютеров

Политика использования компьютеров в случае судебного разбирательства определяет, кто может использовать компьютерные системы, и каким образом они могут использоваться. На первый взгляд, значительная часть информации в этой политике имеет лишь общий смысл, но если организация не определит явным образом политику принадлежности и использования компьютера, то будет велика вероятность судебных исков от ее сотрудников.

Принадлежность компьютеров

Политика должна четко определять, что все компьютеры принадлежат организации, и что они предоставляются сотрудникам для работы в соответствии с их должностными обязанностями. Политика также может запрещать использование компьютеров, не принадлежащих организации, для выполнения работы, связанной с деловой деятельностью этой организации. Например, если сотрудник предполагает выполнять работу дома, организация предоставит ему компьютер. Также в политике может указываться, что только компьютеры, принадлежащие организации, могут использоваться для подключения к внутренним системам компании через систему удаленного доступа.

Принадлежность информации

Политика должна определять, что вся информация, хранимая или используемая на компьютерах организации, принадлежит организации. Некоторые сотрудники могут использовать компьютеры организации для хранения личных данных. Если в политике не оговорить данный вопрос в отдельном порядке (или если сотрудники просто не поймут это), то личные данные, при условии хранения в частных папках, действительно могут считаться личными данными. Это обстоятельство может привести к судебным искам в случае разглашения данной информации.

Приемлемое использование компьютеров

Обычно предполагается, что сотрудники используют для выполнения работы только те компьютеры, которые предоставляются организацией. Это предположение не всегда верно. Следовательно, оно должно быть оговорено в политике. Достаточно просто указать, что "компьютеры организации предназначены только для выполнения сотрудниками их должностных обязанностей". В других организациях могут детально определяться обязанности сотрудников.

Иногда сотрудникам разрешается использовать компьютеры фирмы для других целей, например, запускать вечером сетевые игры. Если это не запрещено, то данное обстоятельство должно быть четко оговорено в политике.

При использовании компьютеров, предоставляемых организацией, возникает вопрос о программном обеспечении, загружаемом в эти системы. Иногда требуется установить правило, согласно которому на компьютерных системах запрещена загрузка неавторизованного программного обеспечения. В этом случае политика должна определять, кто может загружать авторизованные программы, и каким образом программы становятся авторизованными.

Приватность отсутствует

Возможно, самой важной частью политики использования компьютеров является заключение о том, что сотрудник не должен подразумевать частный статус любой информации, хранимой, отправляемой или получаемой на любых компьютерах организации. Очень важно, чтобы сотрудник понимал, что любая информация, включая электронную почту, может просматриваться администраторами. Кроме того, сотрудник должен знать, что администраторы или сотрудники отдела безопасности могут отслеживать все действия, связанные с компьютерами, включая посещение веб-сайтов.

Политика использования интернета

Политика использования интернета, как правило, включается в главную политику использования компьютеров. Однако в некоторых случаях эта политика представляется в виде отдельной политики в силу своих особенностей. Организации предоставляют своим сотрудникам доступ в интернет, чтобы они выполняли свои обязанности более эффективно и, следовательно, приносили большую прибыль. К сожалению, веб-сайты, посещаемые сотрудниками в интернете, далеко не всегда связаны с их работой.

Политика использования интернета определяет соответствующее назначение интернета (например, связанные с работой статистические исследования, покупка товаров или связь по электронной почте). Она определяет нецелевое использование интернета

(например, посещение веб-сайтов, не связанных с деятельностью компании, загрузка защищенного авторскими правами содержимого, продажа музыкальных файлов или отправка писем по цепочке).

Если политика отделена от политики использования компьютеров, в ней указывается, что организация может отслеживать работу в интернете, и что сотрудники не должны рассматривать обмен данными через интернет как операцию, проводимую в частном порядке.

Политика работы с электронной почтой

В некоторых организациях разрабатывается специальная политика, определяющая методы работы с электронной почтой (она может быть включена в политику использования компьютеров). Электронная почта используется огромным числом организаций при управлении бизнесом. Электронная почта представляет угрозу утечки важных данных. Если принято решение определить специальную политику электронной почты, то данная политика должна оговаривать как внутренние проблемы, так и внешние.

Внутренние проблемы, связанные с почтой

Политика работы с электронной почтой не должна конфликтовать с другими политиками, связанными с персоналом организации. Например, она должна указывать на все политики организации, в которых говорится о сексуальном притеснении. Если в организации запрещено передавать с помощью электронной почты неприличные шутки, то имеющиеся определения непристойных и неприличных комментариев нужно указать внутри данной политики.

Если в организации планируется отслеживание электронной почты на предмет наличия определенных ключевых слов или файловых вложений, в политике оговаривается данный типа мониторинга, однако не должны указываться конкретные слова, которые вызовут пометку сообщений. Политика также определяет, что сотрудник не должен считать электронную почту частной.

Внешние проблемы, связанные с почтой

Исходящая электронная почта может содержать секретную информацию. Политика почты должна определять, при каких условиях это обстоятельство допустимо, и в ней должны присутствовать ссылки на информационную политику, определяющую методы защиты секретных данных. Кроме того, может потребоваться определить отказ от прав или заключение внизу исходящих сообщений, в котором говорится о том, что информация, являющаяся собственностью организации, должна защищаться.

В политике почты оговариваются вопросы, связанные с входящей электронной почтой. Например, во многих организациях осуществляется тестирование входящих файлов на наличие вирусов. Политика должна ссылаться на политику безопасности организации, в которой говорится о соответствующих мерах, направленных на борьбу с вирусами.

Процедуры управления пользователями

Процедуры управления пользователями - это процедуры, выполняемые в рамках обеспечения безопасности, которым зачастую не уделяется должного внимания, что представляет собой огромный риск. Механизмы защиты систем от несанкционированного доступа посторонних лиц - отличные средства безопасности, однако они бесполезны при отсутствии должного управления пользователями компьютерных систем.

Процедура нового сотрудника

Для предоставления новым сотрудникам санкционированного доступа к компьютерным ресурсам необходимо разработать соответствующую процедуру. Над разработкой этой процедуры должны работать сотрудники отдела безопасности совместно с отделом кадров при участии системных администраторов. В идеальном случае запрос на компьютерные ресурсы будет генерироваться супервизором нового сотрудника. В зависимости от того, в какой отдел зачислен новый сотрудник, и от запроса доступа, сделанного супервизором, системные администраторы предоставят сотруднику соответствующий доступ к файлам и системам. Эта процедура должна использоваться при приеме на работу консультантов и совместителей, с присвоением срока действия их учетным записям для определения последнего рабочего дня в данной организации.

Процедура перемещенного сотрудника

В каждой организации должна быть разработана процедура пересмотра прав доступа сотрудников при их перемещении внутри организации. Эта процедура разрабатывается при поддержке отдела кадров и системных администраторов. В идеальном случае новый и старый руководитель сотрудника определяют тот факт, что сотрудник переходит на новое место, а также доступ, который ему больше не требуется, и доступ, необходимый для работы на новом месте. Соответствующий системный администратор затем внесет все необходимые изменения.

Процедура удаления сотрудника

Возможно, наиболее важной процедурой, связанной с управлением пользователями, является удаление уволившихся пользователей. Эта процедура разрабатывается при содействии отдела кадров и системных администраторов. Когда отдел кадров идентифицирует сотрудника, увольняющегося из компании, следует заблаговременно предупредить системного администратора, чтобы учетные записи данного сотрудника были удалены в последний день его работы.

В некоторых случаях необходимо отключать учетные записи сотрудника перед уведомлением сотрудника о его удалении. Данная ситуация также должна рассматриваться в процедуре удаления.

Совет

Процедуры удаления сотрудника должны предусматривать механизм очень быстрого удаления сотрудника (например, на тот случай, когда требуется немедленно выпроводить сотрудника из здания).

Процедура удаления сотрудника должна распространяться на совместителей и консультантов, имеющих учетные записи в системе. О таких пользователях отдел кадров может и не знать. Следует определить, кому будет известно о таких сотрудниках, и также включить этих лиц в процедуру.

Удаление системных или сетевых администраторов должно производиться под управлением отдельной задокументированной процедуры. Эти сотрудники, как правило, имеют множество учетных записей, и им известны основные административные пароли. Если такой сотрудник увольняется из организации, все эти пароли нужно сменить.

Внимание!

Очень легко упустить уволившегося сотрудника из виду. Чтобы организовать повторную проверку уволившихся сотрудников, рекомендуется разработать процедуру, осуществляющую периодическое подтверждение существующих учетных записей. Эта процедура содержит отключение учетных записей, не используемых в течение определенного промежутка времени, а также уведомление администраторов о наличии таких учетных записей.

Процедура системного администрирования

Процедура системного администрирования определяет, каким образом осуществляется совместная работа отдела безопасности и системных администраторов с целью обеспечения безопасности систем. Данный документ состоит из нескольких специальных процедур, определяющих, каким образом и как часто должны выполняться задачи системного администрирования, связанные с безопасностью. Эта процедура отмечается в политике использования компьютера (когда речь идет о возможности системных администраторов осуществлять мониторинг сети) и, следовательно, является отражением того, каким образом предполагается осуществлять управление системами.

Обновление программного обеспечения

Данная процедура определяет, как часто администратор проверяет наличие обновлений, выпускаемых производителем программного обеспечения. Предполагается, что новые надстройки не будут устанавливаться, следует предусмотреть выполнение предварительного тестирования.

Наконец, процедура должна документировать соответствующие сведения при проведении обновлений, а также процедуру отката в случае ошибки при установке обновления.

Сканирование уязвимостей

В каждой организации должна быть разработана процедура определения уязвимостей в системах. Как правило, сканирование осуществляется под руководством отдела безопасности, и соответствующие изменения вносятся системными администраторами. Существует ряд коммерческих средств сканирования и бесплатных программ, которые также могут использоваться для этой цели.

В процедуре определяется, насколько часто необходимо проводить сканирование. Результаты сканирования должны передаваться системным администраторам для корректировки или объяснения (может получиться так, что некоторые уязвимости не смогут быть устранены из-за программного обеспечения, установленного в системе). В этом случае администратору придется устранить уязвимости до следующего сканирования.

Проверка политики

Политика безопасности организации определяет требования безопасности для каждой системы. Для проверки соответствия информационной системы установленной политике используется периодическое проведение внешних или внутренних аудитов. В промежутке между основными аудитами отдел безопасности должен работать вместе с системными администраторами для проверки систем на соответствие политике безопасности. Это действие может осуществляться в автоматическом режиме или вручную.

Процедура проверки политики должна определять, насколько часто должна проводиться эта проверка. Кроме того, в ней описывается, кто получает результаты проверки, и каким образом разрешаются вопросы, возникающие при обнаружении несоответствий.

Примечание

Если проверку политики предполагается выполнять автоматически, то ее частота должна быть снижена, чтобы обеспечить запас времени на проверку конфигурации системы вручную.

Проверка журналов

Следует регулярно изучать журналы, полученные от различных систем. В идеальном случае сотрудники отдела безопасности просматривают записи журналов, помеченные программой, вместо просмотра всего журнала целиком.

Если предполагается использовать автоматическое средство, данная процедура должна определять конфигурацию этого средства, а также обработку исключений. Если процесс проводится вручную, в процедуре определяется частота проверки файлов журналов, а также типы событий, которые должны отмечаться для проведения более основательной оценки.

Регулярный мониторинг

В организации должна быть определена процедура, указывающая, когда следует осуществлять отслеживание сетевого трафика. В некоторых организациях данный тип мониторинга осуществляется непрерывно, в других - случайным образом.

Политика резервного копирования

Политика резервного копирования определяет, каким образом осуществляется резервное копирование данных. Зачастую эти требования включаются в политику безопасности организации.

Частота резервного копирования

Политика резервного копирования должна определять частоту резервного копирования данных. Как правило, конфигурация предусматривает проведение полного резервного копирования данных один раз в неделю с дополнительным резервным копированием, проводимым в остальные дни. Дополнительное резервное копирование сохраняет только файлы, изменившиеся с момента последнего резервирования, что сокращает время процедуры и обеспечивает меньший объем пространства на резервном носителе.

Хранение резервных копий

Необходимо хранить носители с резервными копиями в защищенных местах, которые, тем не менее, должны быть доступны в случае, если потребуется восстановить утерянные данные. Например, в большинстве организаций предусмотрена ротация резервных носителей, согласно которой последние резервные ленты отключаются и помещаются в место хранения, а более ранние копии изымаются из хранилища для повторного использования. В данном случае ключевым параметром является скорость отключения и перемещения в место хранения. Это время зависит от степени опасности, представляемой для организации, если сбой произойдет в то время, когда резервный носитель будет отключен, от убытков вследствие хранения резервного носителя и времени, затрачиваемого на доставку носителей из места хранения. В организации должно быть установлено, насколько часто требуется применение резервных носителей для восстановления файлов. Если носители требуются каждый день, то, вероятно, имеет смысл хранить их несколько дней, пока не будет создана лента с более новой информацией.

Политика резервного копирования должна ссылаться на архивную или информационную политику организации для определения времени хранения файлов до повторного использования носителя.

Резервируемая информация

Не каждый файл на компьютере требует ежедневного резервного копирования. Например, исполняемые системные файлы и файлы конфигурации практически не меняются, поэтому для них не обязательно ежедневное резервирование. Имеет смысл создать резервную копию системных файлов заранее и загружать их с надежного носителя, если требуется переустановить систему.

Файлы данных, в особенности часто изменяющиеся, должны резервироваться регулярно. В большинстве случаев необходимо осуществлять их ежедневное резервное копирование.

Совет

Структура каталогов, используемая на файловых серверах, облегчает определение данных, подлежащих резервированию. Если все файлы содержатся в одном каталоге

высокого уровня (содержащем подкаталоги), то осуществляется резервное копирование только одного каталога. Администратору не придется отыскивать отдельные файлы, разбросанные по всей файловой системе.

В политике резервного копирования предусматривается периодическое тестирование восстановления. Если даже резервное копирование осуществляется без ошибок, при восстановлении вероятно возникновение проблемы считывания файлов. Периодическое тестирование резервного носителя увеличивает вероятность обнаружения подобных проблем.

Процедура обработки инцидентов

Процедура обработки инцидентов (IRP) определяет способы реагирования на возникновение инцидентов, связанных с безопасностью. IRP определяет, кто имеет право доступа и что необходимо сделать, однако не всегда содержит описание конкретных действий.

Примечание

Если речь идет о банковской организации, название этой процедуры следует изменить (например, на "процедура обработки событий"). Термин "инцидент" имеет определенное значение в банковской сфере и необходимо избегать его использования, если событие не связано напрямую с финансовыми потерями.

Цели обработки инцидентов

Процедура IRP должна определять цели организации, достигаемые при обработке инцидента. Среди целей IRP можно выделить следующие:

- защита систем организации;
- защита данных организации;
- восстановление операций;
- пресечение деятельности злоумышленника;
- снижения уровня антирекламы или ущерба, наносимого торговой марке.

Эти цели не являются взаимоисключающими, и в организации вполне могут быть определены несколько целей. Ключевым моментом является определение целей организации до того, как возникнет инцидент.

Идентификация событий

Идентификация инцидента является, вероятно, наиболее важной и сложной частью процедуры обработки инцидента. Некоторые события очевидны (например, несанкционированное изменение содержимого веб-сайта), другие же события могут означать либо вторжение, либо просто ошибку пользователя (например, удаление файлов).

Перед объявлением конкретного инцидента сотрудники отдела безопасности и системные администраторы должны провести небольшое исследование, чтобы определить, действительно ли инцидент имел место. В этой части процедуры могут

быть выявлены события, представляющие собой очевидные инциденты, а также определены действия, которые необходимо предпринять, если событие не является очевидным инцидентом.

Совет

Оказать помощь в идентификации инцидентов может служба технической поддержки. Если ее сотрудники обучены задавать конкретные вопросы обращающимся к ним пользователям, то их можно использовать для формирования первичного представления о вероятном инциденте.

Эскалация

В IRP должна быть определена процедура эскалации данных по мере поступления информации о произошедшем событии. В большинстве организаций процедура эскалации предназначена для активизации действий группы сотрудников, которым поручена обработка инцидентов. В банковских структурах предусматривается два уровня эскалации, в зависимости от того, связано ли событие с финансовыми потерями.

В каждой организации должны быть определены сотрудники, являющиеся членами группы, ответственной за обработку инцидентов. Их следует выбирать из следующих подразделений организации:

- отдел безопасности;
- системные администраторы;
- юридический отдел;
- отдел кадров;
- рекламный отдел.

По мере необходимости в группу могут быть добавлены и другие сотрудники.

Контроль информации

При обнаружении инцидента необходимо обеспечить контроль информации об инциденте. Количество получаемой информации зависит от того, какое влияние окажет инцидент на организацию и ее клиентскую базу. Кроме того, информацию следует оглашать таким образом, чтобы она положительно сказалась на делах организации.

Примечание

Только сотрудники отдела рекламы и юридического отдела могут обсуждать информацию об инциденте с представителями прессы, и никто более.

Обработка

Обработка инцидента напрямую вытекает из целей, определенных в IRP. Например, если целью данной процедуры является защита систем и информации, имеет смысл отключить системы от сети и провести необходимые восстановительные работы. В других случаях важнее сохранить систему в рабочем режиме и подключенном

состоянии для продолжения обслуживания клиентов либо позволить злоумышленнику вернуться, чтобы собрать о нем больше данных и, возможно, идентифицировать.

В любом случае метод обработки, используемый организацией, должен обсуждаться и отрабатываться заблаговременно.

Примечание

Месть злоумышленнику никогда к добру не приводит. Такие ответные действия бывают незаконными - не делайте их никогда!

Полномочия

Важной частью IRP является определение того, кто в организации и в группе обработки инцидентов имеет полномочия на выполнение определенных действий. В этой части процедуры определяется, кто имеет полномочия на отключение системы и чьей обязанностью является контакт с клиентами, прессой и органами правопорядка. Назначается официальное лицо, которое будет заниматься именно этими вопросами. Обычно это сотрудник, входящий в группу обработки инцидентов либо внештатный консультант. В любом случае этот человек определяется в процессе разработки процедуры IRP, а не после проведенной атаки и не во время обработки инцидента.

Документирование

Процедура IRP должна определять, каким образом группа обработки инцидентов будет фиксировать свои действия, включая описание данных, подлежащих сбору и сохранению. Этот момент важен по двум причинам: он помогает разобраться в последствиях инцидента и, возможно, предотвращает дальнейшие неприятности посредством привлечения органов правопорядка. Как правило, группе обработки инцидента полезно иметь набор переносных компьютеров для работы.

Тестирование процедуры

Обработка инцидентов требует тестирования. Не следует надеяться на то, что при первом запуске процедуры IRP все пройдет гладко. Сразу после разработки процедуры IRP группе обработки следует провести некоторые тесты. Необходимо проговорить ситуацию и попросить каждого члена группы обработки рассказать о действиях, которые необходимо предпринять в описанных обстоятельствах. Каждый член группы должен следовать предписаниям процедуры. С помощью этого подхода определяются очевидные недостатки процедуры с последующим их устранением.

Процедура IRP должна пройти тестирование в реальных условиях. Попросите сотрудника отдела безопасности смоделировать атаку на организацию, обработку которой произведет группа обработки инцидентов. Эти тесты могут быть как плановыми, так и внезапными.

Процедура управления конфигурацией

Процедура управления конфигурацией определяет шаги, предпринимаемые для изменения состояния компьютерных систем, сетевых устройств и программных

компонентов. Целью данной процедуры является идентификация соответствующих изменений во избежание их ошибочного расценивания как инцидентов, связанных с нарушением безопасности, и для проверки новой конфигурации с точки зрения безопасности.

Вопрос эксперту

Вопрос. Действительно ли необходимо тестировать процедуру IRP?

Ответ. Да, это так. Процедура обработки инцидентов, как правило, выполняется не ежедневно и даже не еженедельно. Только имея опыт, можно безошибочно определять ту или иную ситуацию при исследовании инцидента. Ничто не может заменить регулярные упражнения.

Начальное состояние системы

Когда новая система начинает работу, это состояние следует задокументировать. Как минимум, в этой документации необходимо указывать следующие параметры:

- операционную систему и ее версию;
- уровень обновления;
- работающие приложения и их версии;
- начальные конфигурации устройств, программные компоненты и приложения.

Кроме того, может понадобиться создать криптографические проверочные суммы для всех системных файлов и любых других файлов, которые не должны изменяться в процессе функционирования системы.

Процедура контроля над изменениями

Когда в систему необходимо внести изменения, следует выполнять процедуру контроля над конфигурацией. Эта процедура призвана обеспечить резервирование старых данных конфигурации и тестирование предлагаемых изменений перед их реализацией. В дополнение к этому в запросе об изменении следует отобразить процедуры изменения и отката изменений. После внесения изменения конфигурацию системы нужно обновить для отражения нового состояния системы.

Методология разработки

В организациях, разрабатывающих новые системы, должна присутствовать методология разработки. Она включает множество шагов, которые не связаны с обеспечением безопасности и поэтому не будут здесь обсуждаться. Тем не менее, чем раньше в новом проекте будут рассмотрены вопросы безопасности, тем вероятнее, что конечная система будет должным образом защищена. Для каждой из фаз разработки, описанных в следующих разделах, мы обсудим вопросы безопасности, на которые следует обратить особое внимание.

Определение требований

Методология предусматривает учет требований безопасности в процессе сбора требований в любом проекте. Для некоторых требований методология должна ссылаться на политики информации и безопасности организации. Кроме того, в документе с требованиями необходимо определять секретную информацию и все ключевые требования безопасности для системы и проекта.

Разработка

В процессе разработки проекта методология предусматривает представление безопасности для обеспечения надежной защиты проекта. Сотрудники отдела безопасности могут участвовать в процессе в качестве членов группы разработки или рецензентов. Любые требования безопасности, которые не могут быть выполнены в процессе разработки, должны быть идентифицированы, при необходимости следует отказаться от защиты.

При программировании системы разработчики ПО должны быть осведомлены о проблемах программирования, таких как переполнение буфера. Перед тем как приступить к программированию, следует обучить персонал нужным аспектам компьютерной безопасности.

Тестирование

По достижении фазы тестирования необходимо осуществить проверку требований безопасности. Сотрудники отдела безопасности могут оказать помощь в написании плана тестирования. Имейте в виду, что тестирование требований безопасности зачастую оказывается сложным процессом (трудно доказать, например, что злоумышленник не сможет просматривать секретную информацию).

Примечание

Тестирование безопасности включает тесты, направленные на определение уровня защиты системы. Этот аспект можно выразить следующим вопросом: насколько вы уверены в том, что злоумышленник не сможет преодолеть средства контроля над безопасностью? Такое тестирование является очень дорогостоящим и отнимает много времени.

Реализация

Фаза реализации проекта также предусматривает требования безопасности. Группа реализации должна использовать нужные процедуры управления конфигурацией, а сотрудники отдела безопасности должны проверить систему на наличие уязвимостей и соответствие политике безопасности.

Примечание

Методология разработки предназначена не только для внутренних разработок. Аналогичные шаги следует предпринимать и при работе с коммерческими проектами.

Планы восстановления после сбоев

В каждой организации должен быть предусмотрен план восстановления после сбоев (DRP) для выхода из таких экстремальных ситуаций, как пожары, атаки на переполнение буфера и другие события, выводящие систему из строя. Часто этот план отсутствует, так как считается слишком дорогостоящим, либо организация не может держать альтернативную базу для выполнения операций с оборудованием, находящимся в состоянии готовности. DRP не обязательно требует наличия запасного помещения, это план, которому будет следовать организация, в случае если произойдет наихудшее. Это может быть либо простой документ, предписывающий сбор ключевых сотрудников в соседнем ресторане в случае пожара в здании, либо достаточно сложный, определяющий порядок функционирования организации, в случае если все (или отдельные) компьютеры выйдут из строя.

Правильный план DRP должен учитывать различные уровни неполадок: отдельные системы, хранилища данных и помещения в целом. В следующих параграфах этот материал рассматривается более подробно.

Сбои отдельной системы или устройства

Наиболее часто происходит сбой отдельной системы или устройства. Такие сбои происходят в сетевых устройствах, жестких дисках, материнских платах, сетевых картах или программных компонентах. В рамках разработки данной части DRP необходимо проверить среду организации на предмет ее уязвимости в случае такого сбоя. Для каждого сбоя должен быть разработан план, позволяющий возобновить функционирование системы за приемлемый промежуток времени. Каким по длительности является этот "приемлемый" промежуток, зависит от важности рассматриваемой системы. Например, компьютерный узел, задействованный в производственном процессе и предназначенный для разработки графиков производства и оформления заказов на поставку сырья потребует восстановления в течение четырех часов, в противном случае производство остановится. Для предотвращения подобного сбоя требуется запасная система, которую можно оперативно подключить, либо кластеризация. Выбор метода зависит от стоимости решения. Независимо от того, какому решению отдается предпочтение, DRP указывает, что необходимо предпринять для продолжения работы системы без потерявших работоспособность компонентов.

Совет

План DRP должен разрабатываться совместно с функциональными подразделениями организации, чтобы их сотрудники имели понятие о том, какие шаги они должны предпринимать для продолжения нормальной работы.

События, связанные с хранением данных

План DRP должен предусматривать процедуры на случай серьезной неполадки центра хранения данных. Например, что делать в случае, если центр сгорел, как восстановить его работу? Одним из обязательных вопросов для рассмотрения является поломка оборудования. В плане должны быть предусмотрены способы подключения дополнительного оборудования.

На тот случай, если центр данных вышел из строя, а остальная часть системы функционирует нормально, план DRP должен предусматривать размещение нового

оборудования, а также способы быстрого восстановления всех сетевых соединений. В данном случае можно использовать запасное помещение, однако этот способ является довольно дорогостоящим. Если наличие запасных помещений не входит в план, следует предусмотреть другие варианты восстановления компьютерных систем.

Как в случае с отдельными событиями, план DRP определяет порядок работы организация в процессе восстановления систем.

События, связанные с организацией в целом

Когда речь идет о плане DRP, обычно подразумеваются события, наносящие ущерб организации в целом. Такие события происходят не часто, но представляют наибольшую опасность. Чтобы предусмотреть в плане DRP подобные события, необходимо, чтобы каждое подразделение организации участвовало в создании этого плана. Первым шагом является выявление первоочередных систем, которые нужно восстановить для обеспечения жизнедеятельности организации. Если компания поддерживает сайт электронной коммерции, наиболее важными системами являются компьютеры и сеть. Если фирма выпускает продукцию, в первую очередь нужно восстанавливать производственное оборудование.

Тестирование DRP

План DRP - это сложный документ, и, скорее всего, вы не напишете его с первого раза. Следовательно, необходимо проводить тестирование DRP. Тестирование необходимо не только для обеспечения правильности DRP на данный момент времени, но и на будущее.

Проверка DRP может быть очень дорогостоящей операцией и привести к значительным финансовым затратам. Имея это в виду, целесообразно определить ответственных сотрудников и периодически выполнять проверку плана, а также ежегодное полномасштабное тестирование.

Вопросы для самопроверки

- Почему политика является важным документом?
- Политика, определяющая технические требования безопасности, называется.

Создание политики

Теперь, после обсуждения всех политик, действующих в организации, давайте поговорим о создании политики, соответствующей вашей компании. Каждая компания работает по собственным правилам, следовательно, должна иметь собственную уникальную политику. Для обучения персонала разработке политики полезно использовать шаблоны политик. Однако повторение слово в слово политики другой организации не является хорошим способом создания политик.

Определение наиболее важных аспектов

Первым шагом при создании политики организации является определение наиболее важных политик. Например, компания, занимающаяся распространением информации через интернет, будет придавать большее значение плану восстановления в сравнении с политикой использования компьютеров. Сотрудники отдела безопасности организации должны выявить и описать все важнейшие политики, в противном случае необходимую информацию в этой области можно будет получить посредством оценки угроз.

Совет

Сотрудники отдела безопасности должны прибегать к помощи системных администраторов, отдела кадров и руководителей организации для определения наиболее важных политик.

Определение допустимого поведения

То, что называется допустимым поведением сотрудников, зависит от порядков, установленных в организации (культуры организации). Например, в некоторых компаниях сотрудникам разрешается неограниченно работать в интернете. Культура организации призвана обеспечить эффективность исполнения обязанностей сотрудниками и их начальниками. В других компаниях налагаются ограничения на выход сотрудников в интернет, кроме того, работают программы, ограничивающие доступ к определенным веб-сайтам.

Политики этих компаний значительно отличаются друг от друга. Действительно, сотрудники первой компании вовсе не применяют политику использования интернета. Специалисты в области информационной безопасности должны помнить, что не все политики подходят для использования. Перед началом создания политики необходимо внимательно изучить культуру организации и требования, предъявляемые к ее сотрудникам.

Определение руководителей

Политика, созданная в вакууме, редко является успешной. Имея это в виду, разработку политики должны проводить работники отдела безопасности при помощи других сотрудников организации. Отдел безопасности при разработке любых политик должен руководствоваться рекомендациями генерального директора организации и сотрудников отдела кадров. В процессе создания политик, как правило, участвуют системные администраторы, пользователи компьютеров и отдел охраны.

Другими словами, в разработке политики должны быть задействованы те лица, на которые данная политика будет распространяться, чтобы сотрудники понимали, чего ожидать в той или иной ситуации.

Определение схем политик

Разработка политики начинается с формирования схемы (одна схема уже была представлен в этой лекции). Существует множество источников качественных схем

политик. Некоторые из них приведены в книгах, а некоторые доступны в интернете. Например, RFC 2196 "The Site Security Handbook" содержит перечень схем для различных политик.

Разработка

При разработке политик безопасности необходимо, в первую очередь, руководствоваться вопросами безопасности. Это не означает, что отдел безопасности должен разрабатывать политики без участия других подразделений, но он должен взять на себя ответственность за проект и проконтролировать его завершение.

Процесс разработки политики следует начать со схемы и черновых набросков каждого раздела политики. В то же время следует проконсультироваться с руководителями организации и сообщить им о выполняемом проекте. Пригласите руководителей для участия в проекте. Тем из них, кто примет предложение, необходимо выслать черновой вариант политики и пригласить на собрание, на котором он будет обсуждаться и корректироваться. В зависимости от размеров организации и того, какая именно политика разрабатывается, могут рассматриваться несколько аспектов.

Руководить собранием должны сотрудники отдела безопасности. Следует проработать каждый раздел политики, выслушать все комментарии и все обсудить. Однако имейте в виду, что некоторые предложения бывают ошибочными. В этом случае сотрудники отдела безопасности должны объяснить причины того, что предлагаемые решения увеличат риск или не смогут быть правильно реализованы. Следите за тем, чтобы остальные слушатели понимали, о чем идет речь, и осознали причины выбора тех или иных решений.

Данный процесс имеет смысл повторить при работе с окончательным черновым вариантом. По завершении обсуждения проекта его следует отдать менеджерам для утверждения и реализации.

Развертывание политики

Чтобы создать политику, требуется несколько человек. Чтобы эффективно применить политику, необходимо работать со всей организацией в целом.

Понимание политики

Сотрудники каждого подразделения компании, на которое распространяется политика, должны вникнуть в ее суть. Это достигается довольно легко, так как в процессе создания политики участвуют все руководители отделов. Менеджерам отделов можно сообщить, кто из подразделений организации участвовал в процессе, голосуя за нужды своего отдела.

Также требуется согласие менеджеров с важностью политики и необходимостью ее применения. Вышестоящий менеджер зафиксирует тот факт, что политика важна для успешной и безопасной работы организации, и этим заявлением будут руководствоваться подчиненные ему менеджеры.

Обучение

Сотрудники, на которых распространяется новая политика, должны пройти обучение согласно доли своей ответственности. В обучении могут участвовать отдел кадров или учебный отдел, однако это задача отдела безопасности, в особенности когда речь идет об изменениях, которые распространяются на всех пользователей. Возьмем, к примеру, изменение политики использования паролей. По состоянию на утро понедельника все пароли пользователей должны быть длиной в восемь символов и содержать некоторый набор из букв и цифр, срок действия паролей равен 30 дням. При внесении подобного изменения в домене Windows все пароли немедленно становятся недействительными. Это вынудит каждого пользователя изменить свой пароль в понедельник утром. Без соответствующего инструктажа пользователи не смогут выбрать сильные пароли и, вероятно, начнут обращаться в службу технической поддержки. Если пользователи выберут пароли и не запомнят их, то на следующий день они опять будут звонить в службу поддержки или начнут записывать пароли на листочках. И то и другое ведет к снижению безопасности системы.

Лучше всего провести учебу по вопросам, связанным с безопасностью, и рассказать сотрудникам о вносимых изменениях и их причинах. Их можно научить, как выбирать надежные пароли, простые для запоминания. Службу поддержки следует проинформировать о возможных проблемах с паролями. Сотрудники отдела безопасности совместно с системными администраторами выяснят, возможно ли в данной ситуации провести смену паролей в несколько этапов.

Примечание

Изменения, вносимые в систему аутентификации, оказывают влияние на максимально возможное число сотрудников (на всех!) и, следовательно, должны проводиться с осторожностью.

Реализация

Как показано в предыдущем разделе, радикальные изменения в среде безопасности могут плохо повлиять на безопасность организации. Постепенный и тщательно спланированный переход всегда более предпочтителен. Имея это в виду, отдел безопасности должен совместно с системными администраторами или другими подразделениями, на которые распространяется изменение, максимально упростить это изменение. Помните, что безопасность уже рассматривалась как препятствие для работы, доказывать эту мысль сотрудникам уже не требуется.

Эффективное использование политики

Политика может работать как полицейская дубинка, но она более эффективна, когда используется в качестве средства обучения. Имейте в виду, что большинство сотрудников работают, в первую очередь, в интересах организации и стараются выполнять свои обязанности по возможности лучше.

Новые системы и проекты

При запуске новых систем и проектов должны соблюдаться имеющиеся политики безопасности и процедуры разработки. Это позволяет отделу безопасности быть

участником разработки проекта и на ранней стадии процесса определить требования безопасности.

Если новая система не сможет отвечать требованиям безопасности, то у компании будет время, чтобы понять суть представляемой опасности и обеспечить другой механизм защиты.

Имеющиеся системы и проекты

По мере утверждения новых политик каждая система должна проверяться на соответствие утверждаемым политикам. Отдел безопасности совместно с системными администраторами и подразделением, использующим систему, должен внести в системы соответствующие коррективы. Иногда эти коррективы требуют перепрограммирования каких-либо модулей, которое не может быть выполнено мгновенно. Отдел безопасности в этом случае должен осознать, что функционирование организации может быть прервано на некоторое время, и совместно с администраторами и другими подразделениями приложить все усилия для обеспечения скорейшего внесения изменений в рамках бюджета и структурных ограничений системы.

Аудит

Во многих организациях имеются внутренние отделы аудита, которые периодически осуществляют аудит систем на соответствие политике. Отдел безопасности должен ознакомить сотрудников этого отдела с новыми политиками и поработать некоторое время вместе, чтобы аудиторы вникли в суть политики, прежде чем будут проверять системы на соответствие.

Обмен информацией должен быть двусторонним. Отдел безопасности должен объяснить аудиторам, как была разработана политика и что ожидается от политики с точки зрения безопасности. Аудиторы должны объяснить специалистам по безопасности, каким образом будет проводиться аудит и на поиск чего он будет нацелен. Необходимо разработать соглашение о том, какие типы систем являются адекватными для различных разделов политики.

Проверка политики

Даже качественно разработанная политика не вечна. Каждая политика должна регулярно проверяться на соответствие требованиям организации. В большинстве случаев достаточно проводить такую проверку раз в год. Некоторые процедуры, например процесс обработки инцидентов или план восстановления после сбоев, требуют более частых проверок.

В процессе проверки необходимо связаться со всеми руководителями и подразделениями, которые не участвовали в разработке политики. Попросите каждого сотрудника прокомментировать имеющуюся политику. Возможно, имеет смысл устроить общее собрание, если имеются какие-либо важные комментарии (например, комментарии сотрудников из отдела безопасности). Внесите корректировки в политику, получите подтверждение и возобновите процесс обучения.

Разработка политики использования интернета

Этот проект продемонстрирует, как разработать политику, а также какие вопросы могут возникнуть при использовании этой политики.

Шаг за шагом

1. Если вы работаете в группе, разделите группу на пары. Каждая пара будет разрабатывать свою собственную политику и представлять собой отдельную группу.
2. Разработайте схему политики. Не забудьте включить раздел для входящих и исходящих соединений.
3. Определите приемлемые типы входящих соединений.
4. Определите приемлемые типы исходящих соединений. Если вам кажется, что все указано правильно, перейдите к определению типов сайтов, которые могу посещать сотрудники.
5. Представьте политику другим членам группы. Некоторые из них должны выступать в роли сотрудников организации, а другие - в роли менеджеров.
6. Как вариант, различные пары могут работать над разными политиками организации.

Выводы

Разработка политики, как правило, осуществляется очень просто. Тем не менее, сотрудники и руководители встают перед выбором тех или иных подходов при разработке политики. Рядовым сотрудникам не нравится все, что может сказаться на их рабочей нагрузке или секретности их действий. Руководителям же не нравятся политики, предоставляющие слишком много свободы.

Безопасность - примерно то же самое, что и управление риском. Без понимания угроз безопасности по отношению к информационным активам организации может быть использовано либо слишком много, либо слишком мало ресурсов, или они не будут использоваться должным образом. Управление риском обеспечивает основу для оценки информационных активов. Определяя риск, вы определяете значимость отдельных типов информации и систем, в которых эта информация хранится.

Определение риска

Риск - это основополагающая концепция, формирующая фундамент того, что мы называем "безопасностью". Риск - это вероятность потерь, которая требует защиты. При отсутствии риска не нужна и защита. Риск - это концепция, которую понимают только те, кто работает в сфере безопасности.

Поясним определение риска на примере страхования. Человек приобретает страховку, потому что осознает вероятность автомобильной катастрофы, после которой придется серьезно восстанавливать автомобиль. Страхование снижает риск того, что

необходимых на это средств может не оказаться в наличии. Страховая компания устанавливает размер страховых выплат клиенту в зависимости от стоимости ремонта автомобиля и от вероятности аварии.

При более подробном рассмотрении этого примера можно выделить две составляющих риска. Во-первых, это денежные средства, необходимые для ремонта. При возникновении несчастного случая страховая компания должна выплатить установленную сумму. Назовем это уязвимостью страховой компании. Во-вторых, это вероятность дорожно-транспортного происшествия. Назовем это угрозой, которая приводит к проявлению уязвимости (оплата стоимости ремонта).

При исследовании риска вы должны понимать уязвимости и угрозы для организации. Совместно эти составляющие образуют основу риска, и их соотношение показано на рисунке. Как видно из рисунка, если нет угрозы или уязвимости, то нет и риска.

Рис. 7.1. Соотношение между уязвимостью и угрозой

Уязвимость

Уязвимость - это потенциальный путь для выполнения атаки. Уязвимость существует в компьютерных системах и сетях (делая систему открытой для атак с использованием технических методов) или в административных процедурах (делая среду открытой для атак без использования технических методов или атак социального инжиниринга).

Уязвимость характеризуется сложностью и уровнем технических навыков, необходимых для того, чтобы ею воспользоваться. Необходимо принимать во внимание результат, к

которому это может привести. Например, уязвимость, которой легко воспользоваться (с помощью сценария атаки) и которая позволяет злоумышленнику получить полный контроль над системой, является уязвимостью высокого уровня риска. Уязвимость, которая потребует от атакующего вложения значительных средств в оборудование и персонал и позволит лишь получить доступ к не особо ценной информации, считается уязвимостью низкого уровня риска.

Примечание

Уязвимость связана не только с компьютерными системами и сетями. Безопасность зданий и помещений, вопросы персонала и безопасность информации при передаче также требуют проработки.

Угроза

Угроза - это действие или событие, способное нарушить безопасность информационных систем. Рассмотрим три составляющих угрозы.

- **Цели.** Компонент безопасности, который подвергается атаке.
- **Агенты.** Люди или организации, представляющие угрозу.
- **События.** Действия, составляющие угрозу.

Рассмотрим более подробнее каждую из составляющих.

Цели

Целями угроз или атак в большинстве случаев являются службы безопасности (см. в лекции 4): службы конфиденциальности, целостности, доступности и идентифицируемости. И для этого есть реальные основания.

Конфиденциальность становится целью, если мотивом является добыча информации несанкционированными лицами или организациями. В этом случае нарушитель стремится получить, например, секретные правительственные данные. Конфиденциальная информация коммерческой организации (сведения о заработной плате или медицинские данные) также может стать целью.

Целостность является целью, если нарушитель стремится модифицировать информацию. В этом случае он подделывает личные или другие сведения, например, увеличивая сумму своего банковского счета. В другом случае целью становится уменьшение баланса в журнале банковских операций либо изменение записей в

важной базе данных, чтобы вызвать сомнения в правильности всей информации. Такой подход касается компаний, занимающихся исследованием архитектуры цифровых сетей.

Доступность становится целью при выполнении атаки на отказ в обслуживании. Такие атаки направлены на информацию, приложения, системы или инфраструктуру. Угрозы в этом случае носят как кратковременный, так и долгосрочный характер.

Идентифицируемость сама по себе редко является целью. Атака на идентифицируемость может быть направлена на предотвращение восстановления организации после инцидентов. Идентифицируемость выбирается в качестве начального этапа атаки по отношению к другим целям, таким как скрытие изменений в базе данных или взлом механизмов безопасности, существующих в организации.

Целей может быть несколько. Например, идентифицируемость служит исходной целью для предотвращения записи действий злоумышленника, нарушившего конфиденциальность секретных данных организации.

Агенты

Агентами угроз являются люди, которые стремятся нанести ущерб организации. Для этого они должны иметь следующее.

- **Доступ.** Способность для достижения цели.
- **Знания.** Уровень и тип имеющейся информации о цели.
- **Мотивация.** Причина для сокрушения цели.

Доступ. Агент должен иметь доступ к нужной системе, сети, оборудованию или информации. Этот доступ бывает прямым (например, у него есть учетная запись в системе) или косвенным (он получает доступ к оборудованию другим способом). Прямой доступ позволяет воспользоваться существующей уязвимостью и, следовательно, становится угрозой.

Примечание

Составной частью доступа является благоприятная возможность. Такая возможность существует в любой системе или сети только потому, что сотрудники оставляют двери открытыми.

Знания. Агент должен обладать некоторыми знаниями о цели:

- идентификатор пользователя;
- пароли;
- расположение файлов;
- процедуры выполнения физического доступа;
- имена служащих;
- доступные номера телефонов;
- сетевые адреса;
- процедуры обеспечения безопасности.

Чем больше агент знаком с целью, тем больше вероятность, что он знает о наличии уязвимых мест и о том, как ими воспользоваться.

Мотивация. Агенту нужна мотивация для совершения действия. Мотивация является побуждающим действием, ее можно определить как первичную цель.

Мотивацией обычно является:

- **привлечение внимания** - желание похвастаться своими "победами";
- **алчность** - жажда выгоды (денег, товаров, услуг или информации);
- **злые намерения** - желание причинить вред организации или отдельному лицу.

Агенты, которых следует принимать во внимание. Угроза возникает в том случае, если у агента, обладающего доступом и знаниями, появляется мотивация. Поэтому следует принимать во внимание следующих агентов.

- Служащие организации. Они имеют необходимый доступ и знания о системах в силу специфики своей работы. Здесь главный вопрос заключается в наличии мотивации. Не следует в каждом случае подозревать сотрудников организации, но и не учитывать их при проведении анализа риска тоже нельзя.
- Бывшие работники. Они также имеют знания о системах. В зависимости от процедур аннулирования доступа, существующих в организации, у них может сохраниться доступ к системе. Причина увольнения может породить мотивацию, например, уволенный будет испытывать злобу по отношению к организации.
- Предполагается, что у хакеров всегда есть мотивация для причинения ущерба. Даже при отсутствии сведений о системе и сети они могут получить доступ через имеющееся уязвимое место.
- Скорее всего, у конкурентов есть мотивация для получения конфиденциальной информации или для причинения вреда в зависимости от условий конкуренции. Эти конкурирующие организации обладают некоторыми знаниями о компании,

поскольку действуют в той же области. При наличии подходящей уязвимости они могут получить необходимые сведения и осуществить доступ.

- Террористы также имеют мотивацию для нанесения ущерба, их действия обычно нацелены на работоспособность систем. Следовательно, существует возможность доступа к привлекающим внимание системам или помещениям (это системы в интернете и здания, открытые для физического доступа). Учитывая особые намерения по отношению к конкретной организации, важно идентифицировать террористов как возможную угрозу компании.
- Преступники имеют свою мотивацию, их обычно интересуют ценные объекты (как виртуальные, так и физические). Доступ к представляющим ценность объектам, например, к портативным компьютерам - это ключевой момент при выявлении преступников в качестве угрозы компании.
- Общественность должна всегда рассматриваться как возможный источник угрозы. Однако за исключением того, что организация совершает преступление общего характера против цивилизации, мотивация отсутствует. Следовательно, доступ и знания об особенностях организации сводятся к минимуму.
- Компании, предоставляющие услуги, могут иметь подробные знания и доступ к системам организации. У деловых партнеров имеются сетевые подключения, консультанты имеют людей на местах, выполняющих исполнительные или управленческие функции. Мотивация одной организации к нарушению безопасности другой обычно отсутствует, но из-за наличия доступа и необходимых сведений компании-поставщики услуг должны рассматриваться как возможный источник угрозы.
- Клиенты также имеют доступ к системам организации и некоторые знания о ее работе. Из-за наличия потенциального доступа они должны рассматриваться как возможный источник угрозы.
- Посетители имеют доступ к организации на основании того факта, что они посещают организацию. Поэтому возможно получение информации или осуществление входа в систему. Следовательно, посетители также считаются потенциальным источником угроз.
- Такие стихийные бедствия, как землетрясения, торнадо или наводнения, всегда являются источником угроз.

При рассмотрении всех этих агентов необходимо принять рациональное решение о том, какие агенты смогут получить доступ в организацию. Рассмотрите возможные пути нарушения безопасности в свете заранее определенных уязвимостей.

События

События - это способы, с помощью которых агенты угроз могут причинить вред организации. Например, хакеры нанесут ущерб путем злонамеренного изменения информации веб-сайта организации. Следует также принять во внимание вред, который может быть нанесен при получении агентом доступа. Необходимо учитывать следующие события:

- злоупотребление санкционированным доступом к информации, системам или сайтам;
- злонамеренное изменение информации;
- случайное изменение информации;
- несанкционированный доступ к информации, системам или сайтам;
- злонамеренное разрушение информации, систем или сайтов;
- случайное разрушение информации, систем или сайтов;
- злонамеренное физическое вмешательство в системы или операции;
- случайное физическое вмешательство в системы или операции;
- естественные физические события, которые мешают системам или операциям;
- ввод в действие злоумышленного программного обеспечения (намеренно или нет);
- нарушение внутренних или внешних коммуникаций;
- несанкционированный пассивный перехват информации внутренних или внешних коммуникаций;
- кража аппаратного или программного обеспечения.

Угроза + Уязвимость = Риск

Риск - это сочетание угрозы и уязвимости. Угрозы без уязвимости не являются риском так же, как и уязвимости без угроз. В реальном мире ни одно из этих условий не существует. Следовательно, оценка риска - это определение вероятности того, что непредвиденное событие произойдет. Риск качественно определяется тремя уровнями.

- **Низкий.** Существует маленькая вероятность проявления угрозы. По возможности нужно предпринять действия по устранению уязвимого места, но их стоимость должна быть сопоставлена с малым ущербом от риска.
- **Средний.** Уязвимость является значительным уровнем риска для конфиденциальности, целостности, доступности и/или идентифицируемости информации, систем или помещений организации. Существует реальная возможность осуществления такого события. Действия по устранению уязвимости целесообразны.

- **Высокий.** Уязвимость представляет собой реальную угрозу для конфиденциальности, целостности, доступности и/или идентифицируемости информации, систем или помещений организации. Действия по устранению этой уязвимости должны быть предприняты незамедлительно.

Примечание

По возможности нужно учитывать вероятность успешного использования уязвимости злоумышленником. Выполните стоимостную оценку для определения того, сможете ли вы выполнить корректирующие действия (см. следующий раздел).

Выявление риска для организации

Выявление риска не является проблемой. Все, что нужно - это определить уязвимости и угрозы - и дело сделано. Возникает вопрос: как этот установленный риск соотносится с реальным риском организации? Если ответить коротко - не совсем точно. Определение риска в организации должно выполняться по ее заказу. На рисунке 7.2 показаны составные части этого процесса.

Как видно из рисунка, добавлен еще один компонент для определения риска - существующие контрмеры.

Рис. 7.2. Процесс определения риска в организации

Вопрос к эксперту

Вопрос. Используются ли понятия низкого, среднего и высокого уровня риска в реально существующей программе безопасности?

Ответ. И да, и нет. Качественное измерение риска может быть использовано для классификации рисков и для определения ближайших приоритетов (например, в первую очередь следует учитывать риск высокого уровня). Однако, качественная оценка не работает, если мы начинаем задавать вопрос: "Сколько следует потратить на корректировку этого риска?" Без дополнительной информации, такой как величина издержек организации, на этот вопрос ответить не просто.

Выявление уязвимых мест

При выявлении конкретных уязвимых мест начните с определения всех точек входа организации. Другими словами, выявите точки доступа к информации (как в электронной, так и в физической форме) и к системам, находящимся в организации. Сюда включается следующее:

- соединения с интернетом;
- точки удаленного доступа;
- соединения с другими организациями;
- физический доступ в помещения организации;
- точки доступа пользователей;
- точки доступа через беспроводную сеть.

Для каждой точки необходимо произвести оценку информации и систем, затем выявить способы доступа к ним. Убедитесь, что в этот список включены все известные уязвимые места операционных систем и прикладных программ. В лекции 8 мы рассмотрим более подробно, как произвести оценку риска. Здесь же приведена краткая методика, однако она позволяет определить главные уязвимые места организации.

Выявление реальных угроз

Определение угрозы - это всесторонняя и, в некоторых случаях, трудная задача. При попытках установления особенностей или целей угрозы очевидными кандидатами будут ваши конкуренты. Однако реальная угроза может остаться незамеченной. Как правило, существующие угрозы не проявляют себя до тех пор, пока не происходит какой-нибудь инцидент.

Направленная угроза - это сочетание известного агента, который имеет известный доступ и мотивацию, и известного события, направленного на известную цель.

Например, существует затаивший злобу сотрудник (агент), стремящийся узнать о последних проектах, над которыми работает компания (мотивация). Это работник имеет доступ к информационным системам организации (доступ) и знает, где находится эта информация (знания). Его действия направлены на конфиденциальность нового проекта, и он может попробовать получить нужные файлы (событие).

Как было сказано выше, выявление всех направленных угроз требует много времени и представляет собой довольно сложную задачу. Альтернативой этому является определение общего уровня угрозы. Предположив, что существует общий уровень угрозы в мировом масштабе, можно сделать вывод о том, что угрозу представляет каждый, кто имеет потенциальный доступ к информационным системам организации. Угроза существует, потому что человек (служащий, клиент, поставщик и т. д.) может войти в систему и использовать ее в своих интересах. Вовсе не обязательно знать о направленной или конкретной угрозе, адресованной подразделению компании.

Если предположить наличие общей угрозы (кто-то имеет доступ, знания и мотивацию совершить злоумышленные действия), то можно исследовать уязвимые места внутри организации, через которые возможно получение доступа. Каждая такая уязвимость превращается в риск, так как предполагается наличие угрозы, использующей эту уязвимость.

Исследование контрмер

Уязвимость нельзя исследовать на пустом месте. Возможные пути атак нужно рассматривать в контексте существующего окружения, и следует принимать во внимание меры компенсации, если вы уверены в том, что угроза на самом деле существует. Контрмеры включают следующее:

- межсетевые экраны;
- антивирусное программное обеспечение;
- контроль доступа;
- двухфакторную систему аутентификации;
- бейдж (идентификационную карточку);
- биометрию;
- устройства считывания смарт-карт при входе в помещения;
- охрану;
- контроль доступа к файлам;
- шифрование;
- сознательных, хорошо обученных работников;

- системы обнаружения вторжений;
- автоматизированное получение обновлений и политики управления.

Для каждой точки доступа внутри организации должна быть определена контрмера. Например, в компании имеется соединение с интернетом, что дает возможность доступа к системам организации. От такого способа доступа защищает межсетевой экран. С помощью правил, установленных на межсетевом экране, определяются внешние объекы, имеющие доступ к внутренним системам. Следовательно, снижается вероятность внешней атаки, т. к. межсетевой экран ограничивает полный доступ к уязвимым местам систем.

Выявление риска

Как только определены уязвимые места, угрозы и контрмеры, можно установить конкретный риск для данной организации. Вам просто нужно ответить на вопрос, какие действия можно выполнить через каждую точку доступа.

Для этого возьмем вероятные угрозы для каждой точки доступа (или общую угрозу) и установим возможные цели (конфиденциальность, целостность, доступность и идентифицируемость). Основываясь на возможных повреждениях, оценим для каждой точки риск (низкий, средний или высокий). Следует отметить, что одна и та же уязвимость может представлять собой различные уровни риска в зависимости от точки доступа. Например, внутренняя система имеет уязвимое место - почтовый сервер. Внешний нарушитель безопасности должен войти в систему через внешний межсетевой экран, поэтому система закрыта через эту точку доступа и нет никакого риска. Однако служащие внутри организации имеют доступ к системе, поскольку межсетевой экран является внешним. Это значит, что служащие могут воспользоваться данной уязвимостью и получить доступ к системе. Работники рассматриваются как маловероятный источник угрозы, поэтому можно установить уровень риска - средний.

И в завершении рассмотрим физический доступ к ценностям, которыми располагает организация. Предположим, мы установили, что физическая защита очень слаба, и пользователь может, не сходя с места, получить доступ к системе через локальную сеть. Управление сетью не защищает от несанкционированного входа и подключения ко внутренней сети. В таком случае вероятно, что злоумышленник, желающий причинить вред организации, способен получить доступ к сети и незаконно войти в

систему. В этом случае он может воспользоваться уязвимостью почтового сервера. Этот риск классифицируется как риск высокого уровня. Физические контрмеры отсутствуют.

Высокий, средний и низкий уровень риска не отображает всю картину целиком. Демонстрация управления рисками должна показать ущерб, который может быть причинен организации в случае использования уязвимого места. Каким образом организация определяет, сколько ресурсов выделить для уменьшения риска?

Вопросы для самопроверки

1. Риск - это сочетание _____ и _____.
2. Для определения реального риска, угроз и уязвимых мест необходимо предусмотреть наличие _____.

Оценка риска

Для оценки риска следует определить ущерб, нанесенный организации при успешном выполнении атаки. На рисунке 7.3 показано итоговое уравнение для оценки риска. Издержки организации в случае реализации риска - это определяющий фактор для любого решения по управлению риском. Помните, что риск нельзя полностью устранить - им можно только управлять.

Рис. 7.3. Оценка риска

Деньги

Наиболее очевидный способ оценки риска - определение издержек организации в случае выполнения успешной атаки. Эти издержки складываются из следующего:

- снижение производительности;
- похищенное оборудование или деньги;
- стоимость расследования;
- стоимость восстановления или замены систем;
- стоимость помощи экспертов;
- сверхурочная работа сотрудников.

Как заметно из этого неполного списка, цена успешной атаки может быть достаточно большой. Некоторые затраты останутся неизвестными до тех пор, пока на самом деле не произойдет инцидент, и только тогда будут оценены.

Возможно, наиболее трудная для оценки категория - снижение производительности. Что это означает: невыполненную работу или издержки на выполнение восстановительных работ? Будем надеяться, что бухгалтерия или финансовый отдел организации помогут в определении некоторых издержек. Однако, в большинстве случаев их стоимость нельзя установить. Возьмем, к примеру, промышленное предприятие. Эта организация зависит от компьютерной системы, так как выполняет оперативное планирование, заказывает материалы и отслеживает выполнение работ. Если система придет в негодность, то материалы закончатся за 24 часа, а оперативный план устареет через 8 часов (одна смена). Если компьютерная система не будет работать в течение 8 дней, то каковы издержки? Их можно посчитать по количеству сверхурочного времени, необходимого для возвращения к графику, и стоимости продукции за 7 дней. Возможно, появятся скрытые издержки, связанные с опозданием поставки товара. В любом случае затраты для организации остаются очень высокими.

Время

Оценить потерянное время достаточно трудно. Сюда нужно включить то время, которого не хватило сотрудникам для выполнения своих повседневных задач из-за инцидента, связанного с нарушением безопасности. В этом случае затраты времени вычисляются как почасовая оплата технического персонала. Не забудьте посчитать время на ожидание восстановления компьютерных систем.

Время также означает простой ключевых систем. Если веб-сайт организации был взломан, то эту систему нужно перевести в автономный режим и восстановить. Этот простой тоже влияет на компанию.

Успешное выполнение атаки приводит к замедлению в выпуске продукта или предоставления услуги, что также следует учитывать при определении затрат организации. Безусловно, возможная потеря времени должна быть включена в оценку риска.

Ресурсы

Ресурсами могут быть люди, системы, линии коммуникации, приложения или доступ. При возникновении инцидента, связанного с безопасностью, для исправления ситуации потребуется определенное количество ресурсов. В этом случае можно рассчитать денежные затраты. Однако возникает сложность с подсчетом нематериальных затрат, связанных с отсутствием персонала, способного выполнять другие служебные обязанности.

Аналогичная проблема возникает при определении издержек, связанных с медленным сетевым соединением. Работники дольше ожидают доступа в интернет и медленнее выполняют свою работу, а какой-либо проект или научное исследование не выполняется вовсе.

Репутация

Потеря репутации для организации - это очень важная потеря. Измерить подобную утрату затруднительно. Каковы точные издержки в этом случае? Репутация может рассматриваться как эквивалент доверия, которое общественность имеет к организации. Например, репутация банка равна доверию общественности к сохранности денег, помещенных в этот банк. Если у банка слабая репутация или получены доказательства, что деньги, помещенные в банк, не находятся в безопасности, то банк, вероятно, потеряет клиентов. Если новости о том, что выполнен успешный взлом банковской системы будут опубликованы, то вряд ли общественность захочет вкладывать деньги в такой банк. Покинут ли банк существующие клиенты? Несомненно, в большинстве случаев именно так и произойдет. Как измерить такой ущерб?

Другим примером является репутация благотворительных организаций. Благотворительные организации популярны из-за своих добрых дел, выполняемых в

обществе. Основываясь на этой репутации, люди предоставляют денежные пожертвования, которые позволяют благотворительным организациям функционировать. Если репутация благотворительных организаций ослабеет из-за того, что обнаружится нецелевое расходование этих денежных средств? Сократятся ли денежные пожертвования? Несомненно, сократятся.

Примечание

Репутация - это нематериальный актив, который создается и развивается в течение определенного времени. Снижение репутации измерить не просто, но оно, несомненно, влияет на организацию.

Потерянные контракты

Потерянные контракты - это нереализованный потенциал. Организация планирует обслуживать новых клиентов и дополнительно реализовать свою продукцию. Как измерить потери, если эта возможность не реализована? Конечно, можно продемонстрировать, что не был выполнен объем запланированных продаж, но как связать это с риском для безопасности? Влияет ли реализация угроз на потерю потенциальных возможностей?

В некоторых случаях воздействие очевидно. Например, организация выполняет продажу продукцию через интернет. Веб-сайт организации не функционирует четыре дня. Он является основным каналом продаж, поэтому ясно, что на четыре дня торговля приостановится.

А если по непредвиденным обстоятельствам производитель вынужден остановить производство продукции на четыре дня? Могла ли компания продать эти товары, если бы они имелись в наличии? Нет точного способа определения таких потерь.

Методика оценки риска

Конечно, при оценке риска вопросов намного больше, чем ответов. Если весь вероятный риск можно выразить в денежной форме, то процесс намного упростится. Однако в реальной ситуации это сделать невозможно. Следовательно, мы должны воспользоваться данными, которые позволят выполнить эту оценку.

Для каждого риска необходимо установить наилучший, наихудший и наиболее вероятный план действий, затем определить величину ущерба для каждого варианта действий (денежные средства, время, ресурсы, репутация и потерянные контракты). Планы действий создаются на основе следующих критериев.

- Наилучший случай. Нарушение защиты замечено сразу же, проблема быстро устранена, и информация осталась внутри организации. Общий ущерб оказался незначительным.
- Наихудший случай. Нарушение защиты замечено клиентом, который и уведомил организацию. Проблема не была незамедлительно исправлена, информация об этом дошла до прессы. Общий ущерб оказался очень большим.
- Наиболее вероятный случай. Нарушение защиты замечено через некоторое время. Какая-то информация о событии "просочилась" к клиентам (но не вся), и организация была в состоянии контролировать большую часть информации. Общий ущерб был смягчен.

Параметры наиболее вероятного случая меняются в зависимости от реального состояния безопасности, существующей в организации. Иногда наиболее вероятный случай может оказаться самым плохим вариантом.

Теперь для каждого выявленного риска рассмотрим возможный результат.

Ответьте на следующие вопросы.

- Сколько денежных средств нужно затратить на ликвидацию последствий успешного взлома системы безопасности? Определите время работы персонала, консультантов и стоимость нового оборудования.
- Сколько времени потребуется на ликвидацию последствий успешного взлома системы безопасности? Как это повлияет на программу выпуска новой или существующей продукции?
- Какие ресурсы будут затронуты в случае взлома системы безопасности? Какие отделы вашей компании зависят от этих ресурсов?
- Как это событие повлияет на репутацию организации?
- Приведет ли это к срыву новых контрактов? Если да, то какого типа и в каких размерах?

Как только на каждый вопрос будут получены ответы, постройте таблицу, отражающую возможные последствия для каждого риска. Эта информация потребуется вам для улучшения подходов к управлению рисками.

Определение рисков, связанных с электроникой

Этот проект покажет вам способы определения рисков в вашей компании. Он не содержит методику полной оценки риска, а, скорее, является самым первым шагом. В этом задании мы рассмотрим только лишь риски, связанные с электроникой. При полной оценке риска необходимо дополнительного рассмотреть физический риск, риск, связанный с оборудованием и так далее.

Шаг за шагом

1. Определите все точки доступа к информации. Обратите внимание как на электронный, так и на физический доступ.
2. Определите возможные угрозы. Продумайте, какие уровни доступа к информации имеют сотрудники вашей организации. Предположите, какие цели могут преследовать злоумышленники по отношению к вашей организации, что они стараются здесь заполучить.
3. Определите уязвимые места, существующие в различных системах и отдельных рабочих местах с важной информацией. Помните, что уязвимые места существуют не только в структуре систем, но и в процессах и процедурах.
4. Для всех мест хранения информации определите уровень риска (высокий, средний или низкий), который обусловлен наличием уязвимых мест и угроз.
5. Проверьте контрмеры вашей организации. Определите, уменьшат ли применяемые контрмеры уровень установленных рисков.
6. Теперь рассмотрите каждый риск и определите потенциальный ущерб (деньги, время, ресурсы, репутация и потерянные контракты).

Вывод

Для крупной организации имеет смысл выполнять это задание для каждого отдела или рабочего места. Вероятно, будет обнаружено много различных угроз, и определение их точной сущности будет проблематичным. В этом случае предположите наличие общего уровня риска и переходите к уязвимым местам.

Рассматривая контрмеры, убедитесь, что они определены как для процедур, так и для технических средств.

Программно-аппаратные средства обеспечения информационной безопасности

Обеспечение информационной безопасности - это процесс, опережающий управление риском, а не следующий за ним. В отличие от ответной модели, когда вначале происходит чрезвычайное происшествие, а только потом принимаются меры по защите информационных ресурсов, предупредительная модель работает до того, как что-то случится.

В ответной модели общие затраты на безопасность неизвестны.

Общие затраты на безопасность = Стоимость ущерба от происшествия + Стоимость контрмер

К сожалению, мы не узнаем стоимость ущерба от происшествия, пока оно фактически не произойдет. Поскольку организация не предпринимает никаких шагов для предотвращения инцидента, нет никакой возможности узнать величину возможного ущерба. Следовательно, нельзя оценить риск, пока не произойдет реальный инцидент.

К счастью, организация может сократить затраты на обеспечение информационной безопасности. Правильное планирование и управление риском позволят значительно снизить, если не исключить, величину ущерба от происшествия. Если принимались правильные меры, и инцидент был предотвращен, то величина затрат составляет:

Общие затраты на безопасность = Стоимость контрмер

Также обратите внимание, что

Стоимость происшествия + Стоимость контрмер >> Стоимость контрмер

Предупредительное принятие необходимых мер - это правильный подход к информационной безопасности. В этом случае организация определяет свои уязвимые места, выявляет величину риска и выбирает экономически эффективные контрмеры. Это первый шаг в процессе обеспечения информационной безопасности.

Обеспечение информационной безопасности - это непрерывный процесс, включающий в себя пять ключевых этапов (см. рис. 8.1):

- оценку;
- политику;
- реализацию;
- квалифицированную подготовку;
- аудит.

Каждый из этих этапов по отдельности повышает уровень защищенности организации; однако только взятые вместе они обеспечивают основу, которая позволит эффективно управлять риском.

Рис. Обеспечение информационной безопасности

Оценка стоимости

Процесс обеспечения информационной безопасности начинается с оценки имущества: определения информационных активов организации, факторов, угрожающих этой информации, и ее уязвимости, значимости общего риска для организации. Это важно просто потому, что без понимания текущего состояния риска невозможно эффективно выполнить программу защиты этих активов.

Данный процесс выполняется при соблюдении метода управления риском. Сразу после выявления риска и его количественной оценки можно выбрать рентабельную контрмеру для уменьшения этого риска.

Цели оценки информационной безопасности следующие:

- определить ценность информационных активов;
- определить угрозы для конфиденциальности, целостности, доступности и/или идентифицируемости этих активов;
- определить существующие уязвимые места в практической деятельности организации;
- установить риски организации в отношении информационных активов;
- предложить изменения в существующей практике работы, которые позволят сократить величину рисков до допустимого уровня;
- обеспечить базу для создания соответствующего проекта обеспечения безопасности.

Перечисленные цели не изменят тип оценки, принятый в организации. Однако степень приближения каждой цели зависит от масштабов работы.

Перечислим пять основных видов оценки.

- Оценка уязвимых мест на системном уровне. Компьютерные системы исследованы на известные уязвимости и простейшие политики соответствия техническим требованиям.
- Оценка на сетевом уровне. Произведена оценка существующей компьютерной сети и информационной инфраструктуры и выявлены зоны риска.
- Общая оценка риска в рамках организации. Произведен анализ всей организации с целью выявления угроз для ее информационных активов. Установлены уязвимости в местах обработки информации по всей организации.

Исследована информация, представленная как в электронном виде, так и на физических носителях.

- Аудит. Исследована существующая политика и соответствие организации этой политике.
- Испытание на возможность проникновения. Исследована способность организации реагировать на смоделированное проникновение. Этот тип оценки пригоден только для организаций с высокоразвитой программой безопасности.

В последующем обсуждении предположим, что во время проведения аудита будет проведено также испытание на возможность проникновения. Эти виды оценки подразумевают некоторое предварительное понимание рисков и наличие опыта в практической реализации системы безопасности и управления риском. Ни один из видов оценки не подходит, когда организация пробует понять текущее состояние безопасности.

Необходимо провести оценку собранной информации из трех главных источников:

- опрос работников;
- проверка документации;
- инвентаризация.

Нужно проводить опрос работников, которые будут обеспечивать информацией существующие системы безопасности и направления деятельности организации. Не рекомендуется смешивать служебный персонал и руководителей. Опрашивающий должен непринужденно направить разговор на задачи оценки и на то, как человек может содействовать защите информационных активов. Имейте в виду, что сотрудник может заверить вас, что ни одно из направлений обеспечения информационной безопасности активов за ним не закреплено.

Обязательно изучите все существующие политики, связанные с безопасностью. Исследование не должно ограничиваться только готовыми документами, внимательно прочитайте и черновики.

Последний этап сбора информации - инвентаризация всех материальных ценностей организации.

При проведении оценки изучают следующие моменты:

- сетевое окружение;
- физические меры безопасности;

- существующие политики и процедуры;
- меры предосторожности, принятые на местах;
- осведомленность работников в вопросах безопасности;
- персонал;
- загруженность персонала;
- взаимоотношения работников;
- строгое соблюдение работниками установленной политики и мероприятий;
- специфику деятельности.

Сетевое окружение

Обычно в сетевом окружении находятся открытые точки доступа к информации и системам. Исследование сети начинают с построения диаграммы сети и рассматривают каждую точку возможного подключения.

Примечание

Диаграмма сети зачастую бывает неточной или устаревшей, следовательно, крайне важно, чтобы она была не единственным источником информации, используемым для определения критических сетевых компонентов.

Расположение серверов, рабочих станций, доступ в интернет, соединения наборного доступа, соединения с удаленными офисами и партнерами должны полностью представлены на диаграмме сети. На основании диаграммы и информации, полученной от системного администратора, собираются следующие данные:

- тип и количество систем в сети;
- операционные системы и их версии;
- топология сети (коммутаторы, маршрутизаторы, мосты и т. д.)
- точки доступа к интернету;
- использование интернета;
- типы, количество и версии всех межсетевых экранов;
- точки входа соединений наборного доступа;
- беспроводные точки доступа;
- тип удаленного доступа;
- топология глобальной сети;
- точки доступа в удаленных офисах;
- точки доступа других организаций;
- расположение веб-серверов, FTP-серверов и почтовых шлюзов;

- используемые протоколы;
- лица, осуществляющие управление сетью.

После определения архитектуры сети выявляются внутренние защитные механизмы сети:

- списки управления доступом маршрутизаторов, правила межсетевых экранов на всех точках доступа в интернет;
- механизмы идентификации, используемые для удаленного доступа;
- защитные механизмы во всех точках доступа других организаций;
- механизмы шифрования, используемые для передачи и хранения информации;
- механизмы шифрования, используемые для защиты переносных компьютеров;
- антивирусные системы, установленные на серверах, рабочих станциях и службах электронной почты;
- настройки безопасности сервера.

Если сетевые и системные администраторы не предоставят подробной информации о настройках безопасности сервера, то вам потребуется обследование сервера. Оно должно охватить требования к паролям, настройки аудита для каждой системы, а также используемые обновления системы и программ.

Узнайте у сетевых администраторов об использующейся системе управления сетью. Необходимо собрать информацию о типах оповещений и лицах, которые осуществляют мониторинг системы и сбор данных. Эта информация пригодится для выявления нарушителей в случае обнаружения вторжения администраторами системы.

Наконец, необходимо выполнить сканирование всех систем на предмет обнаружения уязвимых мест. Это можно сделать с помощью компьютера, размещенного внутри системы (внутреннее сканирование) или размещенного в интернете, за пределами межсетевых экранов организации. Оба результата очень важны, так как позволят выявить уязвимые места, которые могут использоваться злоумышленниками, которые находятся в вашей организации или за ее пределами.

Совет

Имейте в виду, что сетевые администраторы могут не знать обо всех точках удаленного доступа в организации.

Физическая безопасность

Физическая безопасность помещения - важнейшая составляющая системы защиты информации. Определение мер физической безопасности включает управление физическим доступом к подразделениям, а также к секретным отделам и помещениям. Например, центр регистрации и обработки данных должен иметь собственную систему контроля физического доступа. Как минимум, этот доступ должен быть строго ограничен. При определении мер физической безопасности необходимо выявить следующее:

- тип физической защиты здания, офисных помещений, документов на бумажных носителях и центра обработки данных;
- наличие ключей у персонала;
- засекреченные помещения здания или отдела (исключая центр обработки данных).

Определите расположение линий коммуникации внутри помещений и те места, где линии коммуникации входят в здание. В этих местах могут быть размещены подслушивающие устройства, поэтому подобные точки нужно включить в список критических областей. Включите в список и помещения, где возможно аварийное отключение.

Объектами физической безопасности являются источники энергии, системы контроля состояния окружающей среды и системы противопожарной безопасности, используемые в центре обработки данных. Соберите следующую информацию об этих системах:

- какую мощность потребляет подразделение;
- какую мощность потребляет центр обработки данных;
- какие типы источников бесперебойного питания установлены;
- как долго имеющиеся источники бесперебойного питания смогут поддерживать работоспособность системы;
- какие системы соединены с источниками бесперебойного питания;
- кто будет извещен в случае отключения электроэнергии;
- какая система контроля состояния окружающей среды подключена к источнику бесперебойного питания;
- какая система контроля состояния окружающей среды связана с центром обработки данных;
- кто будет извещен в случае выхода из строя системы контроля состояния окружающей среды;
- какой вид системы противопожарной безопасности установлен в центре обработки данных;

- может ли система противопожарной безопасности центра обработки данных среагировать на пожар, не угрожающий центру.

Примечание

Многие правила противопожарной безопасности требуют установки разбрызгивателей во всех частях здания. В последнем случае необходимо использовать систему пожаротушения, которая не использует воду.

Политики и процедуры

Многие политики и процедуры организации связаны с безопасностью. При проведении оценки должны быть исследованы следующие документы:

- политика безопасности;
- информационная политика;
- план восстановления в случае чрезвычайных происшествий;
- процедуры контрмер на чрезвычайное происшествие;
- политика и процедуры резервного копирования;
- справочное руководство работника или инструкции;
- процедуры найма-увольнения работников;
- принципы конфигурирования систем;
- правила межсетевых экранов;
- фильтры маршрутизатора;
- политика сексуальных домогательств на рабочем месте;
- политика физической безопасности;
- методология разработки программного обеспечения;
- методология смены программного обеспечения;
- телекоммуникационные политики;
- диаграммы сети;
- организационная диаграмма.

После получения вышеуказанных политик и процедур каждая из них исследуется на предмет значимости, правомерности, завершенности и актуальности.

Политика или процедура должна быть значимой для практической деловой деятельности, существующей в организации в настоящее время. Общие политики не всегда работают, поскольку не учитывают особенности той или иной организации. Процедуры должны определять методики выполнения текущих задач.

Политики и процедуры должны соответствовать цели, определенной в документе. При исследовании документа на правомерность проверяйте каждое требование на соответствие установленной цели политики или процедуры. Например, если целью политики безопасности является определение требований безопасности ко всем установленным компьютерным системам, она не должна описывать особые конфигурации для майн-фреймов, рабочих станций и клиент-серверных систем.

Политики и процедуры должны охватывать все стороны деятельности организации. Нередко можно обнаружить, что отдельные аспекты деятельности не нашли свое отражение в политике либо вовсе отсутствовали на момент создания политики. Изменения в технологиях очень часто приводят к изменениям в политиках и процедурах.

Политики и процедуры могут устаревать со временем. Причиной этому является не злоупотребление, а, скорее, небрежность. Морально устаревший документ становится бесполезным и "умирает". Организации в своей деятельности не стоят на месте, меняются системы и сетевое окружение. Если политики не адаптируются к появлению новых систем или новых направлений деятельности, то она теряет свое значение. Все политики и процедуры необходимо своевременно и обоснованно обновлять.

Кроме вышеописанных документов, в процессе оценки необходимо исследовать программу в области информированности о проблемах безопасности и материалы, используемые в соответствующих тренингах. Сравните эти материалы с существующими политиками и процедурами, чтобы увидеть, насколько точно они отражают организационную политику.

И в заключение, процедура оценки должна включать исследование сведений о недавних происшествиях и проверках. Это не значит, что вы можете всецело положиться на результаты предыдущей работы, скорее, требуется установить, есть ли прогресс в существующих сферах деятельности.

Меры предосторожности

Меры предосторожности обычно используются для восстановления работоспособного состояния после каких-либо инцидентов. Основными составляющими являются системы резервного копирования и план восстановления на случай чрезвычайных происшествий.

При оценке пригодности систем резервного копирования исследование должно быть глубже, чем просто просмотр политики и процедур резервного копирования. Необходимо произвести опрос системных операторов, чтобы понять, как на самом деле используется система. Получите ответы на следующие вопросы.

- Что представляет собой система резервного копирования?
- Для каких систем проводится резервное копирование и как часто?
- Где хранятся резервные копии?
- Как часто резервные копии перемещаются в архив?
- Выполнялась ли когда-либо проверка резервных копий?
- Как часто должны использоваться резервные копии?
- Повреждались когда-либо резервные копии?
- Как часто данные нуждаются в резервном копировании?

Ответы на эти вопросы прольют свет на эффективность существующих систем резервного копирования.

Исследуйте план восстановления на случай чрезвычайных происшествий, обращая внимание на его полноту. То, как план используется на самом деле, нельзя определить, просто читая его. Опросите служащих, которые будут использовать план, чтобы определить, использовался ли план когда-либо и был ли он действительно эффективен. Задайте им следующие вопросы.

- Использовался это план когда-либо?
- Какой был результат?
- Тестировался ли план?
- Какое оборудование имеется в распоряжении для устранения последствий бедствия?
- Какое альтернативное местоположение доступно?
- Кто несет ответственность за действия по устранению последствий бедствия?

Осведомленность

Политики и процедуры работают замечательно и позволяют значительно улучшить безопасность организации, если им следуют работники вашей организации. Проводя оценку, оставьте время для беседы с постоянными сотрудниками (не имеющими обязанностей управляющих или администраторов) для определения их уровня осведомленности по вопросам политик и процедур компании, а также практических положений должной безопасности. Обойдите офисные помещения для поиска

признаков несоблюдения политик. Обратите внимание на наличие бумажных листков с написанными паролями и на системы, оставленные в активированном состоянии после регистрации пользователей.

Осведомленность администратора также важна. Очевидно, что они обязаны знать политику компании по вопросам конфигурирования систем. Администраторы должны быть осведомлены об угрозах и уязвимостях, о признаках вторжений в системы. Главное, они должны знать, какие действия необходимо предпринять при обнаружении атаки.

Вопрос к эксперту

Вопрос. Имеет ли значение осведомленность сотрудников?

Ответ. Да, она имеет большое значение. Сотрудники имеют доступ и нужные сведения, следовательно, являются возможными источниками угроз. Именно поэтому злоумышленники проявляют к ним повышенный интерес. Есть много методов социального инжиниринга, позволяющих нарушителю достигнуть своей цели, когда все предыдущие попытки натолкнулись на надежную систему безопасности.

Человеческий фактор

Служащие являются одним из самых важных факторов, влияющих на общую безопасность. Отсутствие навыков или, наоборот, их избыток может стать причиной выхода из строя хорошо продуманных программ безопасности. Проверьте уровень навыков персонала, отвечающего за вопросы безопасности, и администраторов, чтобы определить, способны ли они выполнять программу обеспечения безопасности. Персонал, отвечающий за вопросы безопасности, должен понимать свою работу в плане общей политики так же хорошо, как разбираться в последних разработках в своей области. Администраторы должны иметь соответствующие навыки, чтобы на высоком уровне осуществлять управление системами и сетевым окружением внутри организации.

Все пользователи должны иметь базовые навыки в области компьютерных технологий. Тем не менее, при наличии более глубоких знаний (например, у разработчиков программного обеспечения) возможно возникновение дополнительных проблем в сфере безопасности. Если пользователи достаточно хорошо владеют компьютерными технологиями, то им не составит труда установить на свои рабочие станции дополнительное программное обеспечение, которое может повлиять на общую

безопасность организации. Эти люди с большей вероятностью обладают навыками и знаниями, необходимыми для использования уязвимостей внутренних систем.

От аудиторов организации потребуется обследование систем и сетей как часть их рабочего задания. В этом случае аудиторы, разбирающиеся в существующих технологиях и системах, используемых внутри организации, быстрее смогут отыскать проблемы.

Загруженность персонала

Даже очень квалифицированные и сообразительные работники не смогут поддерживать систему безопасности, если они перегружены работой. При возрастании объема работ первым делом будут забыты именно вопросы безопасности. Администраторы не проверяют записи журналов, пользовательские пароли на совместно используемые ресурсы, а менеджеры забывают о том, что говорилось на тренинге по защите систем. Тут даже самая серьезная организация с тщательно разработанными политиками и процедурами столкнется с уязвимостями.

Однако проблема может быть вовсе не такой страшной, как кажется. В процессе оценки необходимо определить, является ли большой объем работы временным явлением либо это постоянная практика, действующая в организации.

Отношение

Отношение управленческого персонала к вопросам безопасности - еще один ключевой аспект в общей среде безопасности. Это отношение определяется при назначении ответственных за безопасность внутри организации. Другая сторона этого отношения проявляется в том, как управляющее звено передает свои взгляды сотрудникам.

Передача взглядов на безопасность имеет две стороны: отношение управляющего звена и механизм передачи. Руководство может вполне осознавать важность процессов безопасности, но если они не доносят это до своих сотрудников, то последние не будут этого понимать.

Поэтому не забудьте исследовать состояние данного вопроса в организации, опросив руководящий состав и сотрудников.

Следование правилам

При составлении плана безопасной информационной среды необходимо определить фактическую среду безопасности. Планируемая среда устанавливается политикой, положениями и существующими механизмами. Фактическая среда определяется реальным согласием на участие в процессе обеспечения безопасности руководителей и сотрудников. Например, если политика безопасности требует еженедельного просмотра журналов аудита, а руководители не делают этого, то, значит, в организации не соблюдаются требования этой политики.

Политика использования восьмизначных паролей одинаково важна для всех сотрудников. Если руководство организации приказывает системным администраторам настроить конфигурацию их компьютеров на использование паролей с меньшим количеством знаков, это указывает на недостаточное следование правилам со стороны руководства.

Совет

Недостаточное следование правилам со стороны руководства однозначно приведет к рассогласованности действий администраторов и других сотрудников.

Специфика деятельности

В заключение исследуйте специфику деятельности организации. Опросите сотрудников и выясните издержки организации в случае нарушения конфиденциальности, целостности, доступности или идентифицируемости информации. Попробуйте выразить величину этих потерь в денежном выражении, времени простоя, утраченной репутации или в расторгнутых сделках.

При исследовании специфики деятельности определите движение информации внутри организации, между отделами и рабочими местами, внутри отделов и в другие организации. Выясните, как звенья этой цепи угрожают информации, как взаимосвязаны между собой отдельные части организации.

Частью процесса оценки является выявление систем и сетей, критичных для выполнения основной функции организации. Если организация связана с электронной коммерцией, выясните, какие системы используются для совершения сделок? Очевидно, необходим веб-сервер, но что насчет других серверных систем? Определение серверных систем позволит выявить прочие риски для организации.

Результаты оценки

После сбора всей информации группа оценки должна ее проанализировать. При оценке безопасности организации нельзя рассматривать отдельные блоки информации. Группа должна исследовать все уязвимости безопасности в контексте организации. Не все уязвимости превратятся в риски. Некоторые уязвимые места будут защищены каким-либо способом, который предотвратит их использование.

После завершения анализа группа оценки обязана представить полный набор рисков и рекомендаций для организации. Риски представляются по порядку - от наибольшего к наименьшему. Для каждого риска группа показывает возможные издержки в каком-либо выражении (денежном, временном, ресурсном, потере репутации и расторгнутых сделках). Каждый риск должен сопровождаться рекомендацией по управлению риском.

Последний шаг оценки - это разработка плана действий по безопасности. Организация должна определить, являются ли результаты оценки реальным отображением состояния безопасности, и учесть их при распределении ресурсов и составлении планов.

Примечание

Вполне вероятно, что в плане самый серьезный риск будет поставлен не на первое место. Этому могут помешать проблемы, связанные с бюджетом и ресурсами.

Разработка политики

Следующим шагом после оценки, как правило, является разработка политик и процедур. Они определяют предполагаемое состояние безопасности и перечень необходимых работ. Без политики нет плана, на основании которого организация разработает и выполнит эффективную программу информационной безопасности.

Необходимо разработать следующие политики и процедуры.

- Информационная политика. Выявляет секретную информацию и способы ее обработки, хранения, передачи и уничтожения.
- Политика безопасности. Определяет технические средства управления для различных компьютерных систем.
- Политика использования. Обеспечивает политику компании по использованию компьютерных систем.
- Политика резервного копирования. Определяет требования к резервным копиям компьютерных систем.
- Процедуры управления учетными записями. Определяют действия, выполняемые при добавлении или удалении пользователей.

- Процедура управления инцидентом. Определяет цели и действия при обработке происшествия, связанного с информационной безопасностью.
- План на случай чрезвычайных обстоятельств. Обеспечивает действия по восстановлению оборудования компании после стихийных бедствий или инцидентов, произошедших по вине человека.

Разработка политик является в большей степени политическим процессом. Во многих отделах найдутся люди, которые заинтересуются политиками и захотят сказать свое слово при их разработке.

Примечание

Как было сказано в лекции 6, определение заинтересованных сторон будет ключевым моментом в создании успешной политики.

Порядок разработки политик

Итак, какая политика должна быть разработана первой? Ответ зависит от рисков, определенных в процессе оценки. Если защита информации определена как область с высоким уровнем риска, информационная политика должна разрабатываться одной из первых. Если же вероятны потери в бизнесе из-за отсутствия плана на случай чрезвычайных действий, то этот план должен быть разработан в первую очередь.

Еще одним фактором в выборе порядка разработки политик является затрачиваемое время. Планы восстановления в случае ЧП обычно представляют очень подробные документы и требуют серьезных усилий со стороны отделов и сотрудников. Этот план потребует много времени для составления; возможно, потребуется помощь стороннего исполнителя, например, компании, поставляющей резервное оборудование для целей полного восстановления на случай стихийного бедствия.

Единственная политика, которая должна быть разработана на начальной стадии процесса, - это информационная политика. Информационная политика формирует основу понимания того, почему внутренняя информация важна и насколько она должна быть защищена. Этот документ послужит основой для программы обучения специалистов по вопросам безопасности, наряду с политикой использования и политикой паролей.

В самом лучшем случае возможна одновременная разработка нескольких политик, поскольку заинтересованные стороны будут объединены общими интересами. Например, системные администраторы интересуются политикой безопасности, но

информационная политика их интересует в меньшей степени. Сотрудникам более близка политика безопасности и процедуры управления пользователями, а не политика резервного копирования, и т. д. В этом случае отдел информационной безопасности становится координатором и носителем функций, облегчающих выполнение проекта. Его представители должны присутствовать на первом собрании, посвященном разработке черновой версии плана, и их предложения станут отправным пунктом.

Совет

Для начала попробуйте составить небольшой документ с небольшим числом заинтересованных сторон. Это создаст благоприятную возможность для достижения успеха, что позволит отделу безопасности прийти к соглашениям, необходимым для разработки остальных документов.

Обновление существующих политик

Если политики и процедуры уже существуют, это хорошо. Однако вероятно, что некоторые из этих документов потребуют обновления. Если в их создании принимал участие отдел информационной безопасности, то в первую очередь необходимо собрать все заинтересованные стороны, участвовавшие в работе над предыдущей версии политики, и начать работу по обновлению. Используйте как отправную точку исходный документ и выявленные неточности.

Если в разработке документа участвовал кто-то из сотрудников организации, его также нужно привлечь к работе над обновлением. Отдел информационной безопасности не должен ослаблять контроль над деятельностью бывшего владельца. В этом случае снова начните с исходного документа и выявленных неточностей.

Если разработчик исходного документа больше не числится в организации, то проще начать с чистого листа. Выявите заинтересованных лиц и пригласите их принять участие в процессе. Сообщите им, почему старый документ больше не является удовлетворительным

Вопросы для самопроверки

1. Общие затраты на безопасность = _____ + _____.
2. Перечислите главные элементы оценки в организации.

Реализация политики безопасности

Реализация политики заключается в реализации технических средств и средств непосредственного контроля, а также в подборе штата безопасности. Могут потребоваться изменения в конфигурации систем, находящихся вне компетенции отдела безопасности. В таких случаях в проведении программы безопасности должны участвовать системные и сетевые администраторы.

Исследуйте каждый этап для определения взаимодействий с другими системами управлениями. Например, усиление физической защиты позволит снизить требования к политике шифрования и наоборот. Установка межсетевых экранов позволит отложить немедленное устранение уязвимых мест внутренних систем.

Системы отчетности по безопасности

Системы отчетности по безопасности - это механизм, с помощью которого отдел безопасности отслеживает соблюдение политик и процедур, общее состояние уязвимых мест внутри организации. Для этого используются как ручные, так и автоматические системы. В большинстве случаев системы отчетности по безопасности включают оба типа систем.

Мониторинг использования

Механизмы мониторинга гарантируют, что работники следуют политикам использования компьютера. Они включают в себя программное обеспечение, отслеживающее использование интернета. Целью является выявление работников, постоянно нарушающих политику компании. Некоторые механизмы способны блокировать такой доступ и сохранять журнал попыток.

Мониторинг использования включает, например, удаление игр, установленных на рабочей станции. Сложные механизмы позволяют определить, что на компьютер пользователя загружено новое программное обеспечение, но они требуют взаимодействия между администраторами и службой безопасности.

Сканирование уязвимых мест систем

Уязвимые места системы стали очень важной темой в безопасности. Установка операционной системы с параметрами по умолчанию обычно сопровождается запуском ненужных процессов и появлением уязвимых мест. Выявление таких мест не составляет труда для службы безопасности, использующей современные инструментальные средства, а вот их исправление отнимает много времени. Служба безопасности должна отслеживать системы и их уязвимые места с определенной периодичностью.

Необходимо обеспечить администраторов отчетами об уязвимых местах для их удаления. Сведения о вновь установленных системах нужно доводить до сведения системного администратора.

Соблюдение политики

Соблюдение политики - это одно из заданий службы безопасности, отнимающее много времени. Для определения соблюдения политики используются ручной и автоматический режимы. Ручной механизм требует от работника службы безопасности исследования каждой системы и определения, как выполняются требования политики безопасности в конфигурации этой системы. Это отнимает чрезвычайно много времени, велика и вероятность ошибок. Намного чаще из общего количества систем выбирается одна, и проводится ее выборочное исследование. Такой способ требует меньше времени, но далек от совершенства.

Для проведения автоматической проверки соблюдения политики разрабатывается соответствующее программное обеспечение. Такой способ требует больше времени для установки и конфигурирования, но дает более точный результат в более короткие сроки. В этом случае требуется помощь системных администраторов, поскольку программное обеспечение необходимо установить в каждой проверяемой системе. Контроль соблюдения политики может выполняться на основе периодической выборки и результатов обращений к системным администраторам.

Аутентификация систем

Аутентификация систем - это механизм, предназначенный для установления личности пользователей, желающих получить доступ в систему или сеть. Она позволяет также идентифицировать лиц, пытающихся завладеть оборудованием организации. Механизмы аутентификации - это пароли, смарт-карты и биометрия. Требования к ним должны быть включены в программы профессиональной переподготовки по вопросам безопасности.

Примечание

Механизмы аутентификации можно применить к любому пользователю системы. Отсюда следует, что обучение и компетентность пользователя являются важными сторонами развертывания любого механизма аутентификации.

Если пользователи не ознакомлены с работой системы аутентификации, то отдел ИТ будет перегружен звонками в службу технической поддержки. Производительность

работы будет снижена, поскольку пользователи начнут изучать, как пользоваться новой системой. Ни при каких обстоятельствах изменения в способах аутентификации не должны осуществляться без обучения пользователей. Эти способы оказывают влияние на все системы организации, и их реализация должна сопровождаться подробным планированием. Служба безопасности должна работать во взаимодействии с системными администраторами, чтобы процесс реализации проходил без сбоев.

Безопасность в интернете

Реализация безопасности в интернете включает такие механизмы, как межсетевые экраны и виртуальные частные сети (VPN), и ведет к изменениям в сетевой архитектуре (см. лекции 10, 11, 16). Наиболее важным аспектом ее реализации является размещение устройства управления доступом (типа межсетевого экрана) между интернетом и внутренней сетью организации. Без подобной защиты все внутренние системы открыты для неконтролируемых нарушений безопасности. Установка межсетевого экрана является достаточно сложным процессом и может повлечь за собой сбои в нормальной работе пользователей.

Примечание

Размещение межсетевого экрана или другого устройства управления доступом ведет к изменению архитектуры. Подобная операция не должна выполняться до тех пор, пока не будет определена основная сетевая архитектура: ведь нужно установить межсетевой экран соответствующей мощности и задать на нем правила в соответствии с используемыми политиками организации.

Виртуальные частные сети обеспечивают безопасность для информации, передаваемой через интернет и периметр организации. Вопросы, связанные с VPN, могут быть включены в реализацию механизмов безопасности в интернете.

Системы обнаружения вторжений

Системы обнаружения вторжений (IDS) - это системы охранной сигнализации сети. Охранная сигнализация предназначена для обнаружения попыток проникновения в защищаемое помещение, а IDS - для разграничения санкционированного входа и вторжения злоумышленника в защищаемую сеть.

Имеется несколько типов систем обнаружения вторжения, и выбор нужной зависит от совокупного риска организации и располагаемых ресурсов (см. лекцию 13). Системы обнаружения вторжений требуют значительных финансовых вложений.

Самым общим механизмом обнаружения вторжений является антивирусное программное обеспечение. Это программное обеспечение должно работать на каждой рабочей станции и, разумеется, на сервере. Антивирусное программное обеспечение - наименее ресурсоемкий способ обнаружения вторжений.

Перечислим другие способы обнаружения вторжений:

- ручная проверка журнала;
- автоматическая проверка журнала;
- клиентское программное обеспечение для обнаружения вторжения;
- сетевое программное обеспечение для обнаружения вторжения.

Ручная проверка журнала весьма эффективна, но занимает много времени и склонна к ошибкам. Люди для этой цели не подходят. Наилучшим способом проверки журналов является создание программ или скриптов, которые просматривают журналы компьютера в поисках возможных отклонений.

Совет

Развертывание механизмов обнаружения вторжения не следует проводить до тех пор, пока не будут выявлены области с повышенным риском.

Шифрование

Шифрование обычно применяют для защиты конфиденциальных или частных интересов (см. лекцию 12). Механизмы шифрования используются для защиты передаваемой или сохраняемой информации. Вне зависимости от типа используемого механизма возникают два вопроса, на которые нужно ответить до его реализации:

- алгоритмы;
- управление ключом защиты.

Примечание

Шифрование ведет к замедлению обработки или передачи данных. Следовательно, шифрование всей передаваемой информации не всегда является целесообразным.

Алгоритмы

При выполнении шифрования выбор алгоритма обуславливается конечной целью. Шифрование на личном ключе происходит быстрее, чем на открытом. Однако такой

способ не позволяет использовать цифровую подпись или подписывание информации. Важно выбрать известные и хорошо изученные алгоритмы. Такие алгоритмы с большой долей вероятности исключают лазейки, через которые возможен доступ к защищенной информации.

Управление ключом защиты

Развертывание механизмов шифрования должно включать управление ключом защиты. При использовании шифровального блока (устройства для шифрования трафика, передаваемого от узла к узлу) система должна разрешать периодическое изменение ключа. При шифровании на открытом ключе, когда сертификаты выдаются большому количеству лиц, проблема намного серьезнее.

Если планируется введение подобной системы, удостоверьтесь в наличии времени для испытания ключа защиты. Также имейте в виду, что экспериментальная программа позволяет охватить ограниченное число пользователей, а система управления ключом защиты должна быть соразмерна всей системе.

Физическая безопасность

Физическая безопасность традиционно обособлена от информационной или компьютерной безопасности. Установка видеокамер, замков и охранников обычно не очень хорошо понималась работниками отдела компьютерной безопасности. Если в вашей организации дело обстоит именно так, вы должны найти поддержку со стороны. Имейте в виду, что устройства физической безопасности затронут работников организации, как и изменение способа аутентификации. Работники, которые видят видеокамеры в туалете или предъявляют пластиковую карту для входа в кабинет, должны приспособиться к новым обстоятельствам. Если сотрудники пользуются такими картами, то организация должна разработать процедуру действий работников, потерявших или оставивших их дома.

Такая процедура должна доказать, что данный человек действительно является сотрудником организации. Это могут быть цифровые фотографии или звонок коллеги для подтверждения подлинности. Некоторые организации полагаются только на подпись работника в соответствующем журнале. Такой метод позволяет злоумышленнику получить доступ к ее материальным ценностям.

Применяя механизмы физической безопасности, вы не должны забывать о безопасности центра обработки данных. Доступ к центру данных должен быть

ограничен, как следует защищен от огня, высокой температуры и отключения электричества. Внедрение систем пожаротушения и климат-контроля заставит вас провести всестороннюю модернизацию центра данных. Применение источника бесперебойного питания следует применять в системах, отключающихся на короткое время.

Персонал

При применении любых новых систем безопасности вы должны располагать подходящим персоналом. Некоторые системы потребуют постоянного обслуживания (механизмы идентификации пользователей и системы обнаружения вторжений). Другим системам потребуются люди для выполнения положений плана (например, для сканирования уязвимостей).

Вам потребуются обученные сотрудники при проведении учебных программ по повышению осведомленности. Сотрудник отдела информационной безопасности должен присутствовать на каждом учебном занятии, чтобы отвечать на специфические вопросы, даже если обучение проводится отделом обучения.

Последняя проблема, связанная с персоналом, - это ответственность. Ответственность за безопасность организации должна устанавливаться индивидуально. В большинстве случаев ответственным назначается руководитель отдела безопасности, который отвечает за разработку политики, исполнение плана и реализацию механизмов безопасности. Назначение этой обязанности должно быть первым шагом по пути реализации нового плана безопасности.

Проведение профессиональной переподготовки

Организация не может обеспечить защиту секретной информации, не привлекая своих сотрудников. Грамотная профессиональная переподготовка - это механизм обеспечения сотрудников необходимой информацией. Программы обучения могут иметь форму коротких занятий, информационных статей или плакатов. Наиболее эффективные программы используют все три формы.

Сотрудники

Сотрудники должны знать, почему вопросы безопасности так важны, должны быть обучены выявлению и защите секретной информации. Компетентная профессиональная переподготовка по безопасности обеспечивает их необходимой информацией в области

политики организации, выбора пароля и предупреждения атак социального инжиниринга.

Обучение сотрудников лучше всего проводить короткими занятиями - по часу или менее. Видеоматериалы способствуют более качественному уровню занятий, чем обычная лекция. Все новые сотрудники должны проходить обучение как часть инструктажа, а все работающие - раз в два года.

Администраторы

Обучение важно и для системных администраторов. Они должны быть осведомлены о последних на данный момент технических приемах хакеров, угрозах безопасности и обновления программных продуктов. Это обучение должно проходить часто (возможно, раз в месяц) и проводиться сотрудниками отдела безопасности. Информация об обновлениях может быть включена в регулярные совещания штата администраторов для экономии времени, так необходимого администраторам. В дополнение к этому отдел безопасности должен передавать обновления администраторам сразу после появления новых версий, не дожидаясь очередного совещания.

Разработчики

Обучение для разработчиков должно быть расширенной версией учебных занятий для сотрудников. Дополнительный материал включает специфические технические приемы программирования для устранения уязвимых мест и соответствующее понимание роли отдела безопасности в процессе разработки.

Для всех новых разрабатываемых проектов необходимо вовлекать на стадии проектирования отдел безопасности. Это позволит анализировать новые проекты на предмет приоритетного выделения средств на вопросы, связанные с безопасностью. Обучение разработчиков должно дать объяснение важности такого подхода.

Руководители

Презентация для руководителей организации - это отчасти и обучение, и маркетинг. Без поддержки руководства программа безопасности просто не сможет существовать. Следовательно, руководство должно быть проинформировано о состоянии безопасности и о дальнейшем развитии программы.

Периодические презентации руководству должны включать результаты недавних оценок и состояние различных проектов по безопасности. По возможности система

показателей, выражающая риски для организации, должна быть общепризнанной. Например, нужно отследить и отразить в отчете число уязвимых мест организации и нарушений системной политики.

Совет

В ходе этих презентаций можно представить информацию, используемую для обучения сотрудников, чтобы напомнить руководству об их обязанностях в плане обеспечения безопасности.

Персонал отдела безопасности

Персонал отдела безопасности должен быть осведомлен о современном состоянии дел, чтобы грамотно выполнять свою работу. Важно проводить как внешнее, так и внутреннее обучение. Например, каждому сотруднику отдела безопасности можно назначить время для проведения обучения остальных сотрудников этого отдела на любую тему по выбору. Темы должны быть связаны с безопасностью либо с текущим вопросом, интересующим персонал, либо с навыком, отсутствующим у персонала.

Проведение аудита

Аудит - это последний шаг в процессе реализации информационной безопасности. После определения состояния информационной безопасности внутри организации, создания соответствующих политик и процедур, приведения в действие технических средств контроля и обучения персонала проведение аудита позволит удостовериться, что все средства контроля сконфигурированы правильно.

Обсуждая место аудита в процессе безопасности, мы в действительности говорим о трех разных функциях:

- аудит соблюдения политики;
- периодическая оценка существующих проектов и оценка новых проектов;
- проверка возможности нарушения защиты.

Каждая из этих функций занимает свое место в процессе обеспечения безопасности.

Аудит соблюдения политики

Аудит соблюдения политики - это традиционная функция аудита. Организация имеет политику, определяющую настройки и конфигурацию систем безопасности. Аудит

определяет реальное состояние дел. Любые отклонения отмечаются как нарушения. Подобные проверки могут выполняться внутренним персоналом или внешними консультантами. И в том и в другом случае этот процесс требует участия системных администраторов.

Аудит соблюдения политики не должен ограничиваться только проверкой конфигурации систем. Он должен проявлять интерес к тому, как выполняются другие формы управления информацией. Соблюдается ли информационная политика? Как хранятся и передаются секретные документы?

Проверки должны проводиться раз в год. Они могут выполняться персоналом отдела безопасности, но, возможно, выполнение аудита больше подходит для отдела аудита организации или для сторонней фирмы. Причина в том, что в данном случае могут быть затронуты интересы самого отдела безопасности, что приведет к возникновению конфликта интересов.

Периодическая оценка проектов и оценка новых проектов

Компьютерная и сетевая среда внутри организации находятся в состоянии постоянного изменения. Эти изменения приводят к быстрому старению результатов оценки за счет сокращения некоторых рисков и введения новых. По этой причине оценка должна выполняться периодически. Полная оценка организации должна выполняться раз в два года. Как и в случае с крупными проверками, серьезные оценки выполняются персоналом отдела безопасности, если он обладает необходимыми навыками. Возможно, для этих целей больше подходит сторонняя организация.

Небольшие оценки должны выполняться в случае разработки новых проектов или изменений в организационной среде. Для каждого нового проекта отдел безопасности привлекается к работе на стадии проектирования, чтобы определить, имеет ли проект какие-либо риски, и происходит ли в результате разработки проекта появление или сокращение рисков внутри организации. Этот тип оценки должен изучать новый проект в контексте его использования по отношению к другим структурным элементам организации. Если риски определены на ранней стадии проекта, проектирование может быть скорректировано или введены другие механизмы для управления риском.

Проверка возможности нарушения защиты

Проверка возможности нарушения защиты - это спорная тема. Часто такие проверки выполняются вместо оценки. На самом деле, они имеют ограниченную ценность в

программе безопасности. Причина этого проста: при проверках предпринимаются попытки воспользоваться установленной уязвимостью, чтобы получить доступ к системам и информации внутри организации. Если такая проверка имеет успех, то единственный вывод из всего этого - обнаружена, по крайней мере, одна уязвимость. Если проверка нарушения защиты терпит неудачу, то вывод такой - проверяющий не смог обнаружить и использовать уязвимость. Это вовсе не значит, что уязвимости не существует.

Почему же тогда необходимо выполнять проверку возможности нарушения защиты? Если организация провела оценку и применила подходящие средства управления риском, она может выборочно проверить некоторых из них. Проверка защиты подходит для следующих случаев.

- Способность системы обнаружения вторжений выявить попытку нарушения защиты.
- Уместность процедуры реагирования на инцидент, связанный с безопасностью.
- Информация о сети, которую можно узнать через средства управления сетевым доступом.
- Уместность физической безопасности помещения.
- Адекватность информации, предоставляемой сотрудникам программой повышения осведомленности в плане безопасности.

Внимание!

Какой бы ни была причина проведения проверки возможности нарушения защиты, подробный план этой проверки должен быть предоставлен до ее начала. Для каждого этапа плана необходимо определить цель проверки.

Организация определяет также масштаб проверки. Проверка возможности нарушения защиты через внешнюю сеть ограничена внешними сетевыми соединениями организации (соединения через интернет или с другими внешними организациями). Они могут включать доступ через коммутируемое подключение к сети компании или доступ к беспроводным сетям. Проверка физического нарушения защиты выявляют людей, пытающихся получить несанкционированный доступ к оборудованию. Масштаб подобных тестов может быть ограничен как рабочим, так и нерабочим временем. Проверка возможности атак социального инжиниринга связана с тестированием осведомленности сотрудников, она разрешает проверяющим вступать в контакт с сотрудниками, пытаясь заставить их разгласить информацию или предоставить доступ к внутренним системам.

Многие организации начинают развертывание систем безопасности с проверки возможности нарушения защиты. Однако большой пользы это не принесет, поскольку организация не получит достаточного количества информации, позволяющего управлять ее рисками.

Разработайте программу повышения осведомленности в плане безопасности

Осведомленность в плане безопасности - это важная часть любой хорошей программы безопасности. Самым важным моментом здесь является использование наглядных и выразительных способов предоставления информации сотрудникам. Для этого у вас есть занятия, плакаты, информационные листки и электронная почта.

Шаг за шагом

1. Определите ключевую информацию, которая должна быть передана сотрудникам вашей организации. Ее можно найти в различных политиках, используемых в организации. Обратите особое внимание на требования паролей, идентификационные карточки, использование политик, в общем, на все, что напрямую влияет на работу сотрудников.
2. Определите этапы программы повышения осведомленности и то, что будет использоваться для обучения сотрудников (например, проведение занятий или вывешивание плакатов).
3. Наметьте в общих чертах, как будет представлен материал.
4. Определите ресурсы, необходимые для выполнения программы обучения (инструкторы для занятий, кабинеты и т. д.).

Выводы

В большинстве случаев лучше всего использовать сочетание ежегодных занятий с ежемесячными информационными статьями и плакатами. Занятия для сотрудников не должны длиться больше одного часа, и даже тогда они должны быть более интересными, чем просто лекция сотрудника отдела безопасности. Старайтесь повышать уровень новаторскими идеями, чтобы удерживать интерес сотрудников.

Программно-аппаратные средства обеспечения информационной безопасности

Обновить Ресурс

Обеспечение информационной безопасности - это процесс, опережающий управление риском, а не следующий за ним. В отличие от ответной модели, когда вначале происходит чрезвычайное происшествие, а только потом принимаются меры по защите информационных ресурсов, предупредительная модель работает до того, как что-то случится.

В ответной модели общие затраты на безопасность неизвестны.

Общие затраты на безопасность = Стоимость ущерба от происшествия + Стоимость контрмер

К сожалению, мы не узнаем стоимость ущерба от происшествия, пока оно фактически не произойдет. Поскольку организация не предпринимает никаких шагов для предотвращения инцидента, нет никакой возможности узнать величину возможного ущерба. Следовательно, нельзя оценить риск, пока не произойдет реальный инцидент.

К счастью, организация может сократить затраты на обеспечение информационной безопасности. Правильное планирование и управление риском позволят значительно снизить, если не исключить, величину ущерба от происшествия. Если принимались правильные меры, и инцидент был предотвращен, то величина затрат составляет:

Общие затраты на безопасность = Стоимость контрмер

Также обратите внимание, что

Стоимость происшествия + Стоимость контрмер >> Стоимость контрмер

Предупредительное принятие необходимых мер - это правильный подход к информационной безопасности. В этом случае организация определяет свои уязвимые места, выявляет величину риска и выбирает экономически эффективные контрмеры. Это первый шаг в процессе обеспечения информационной безопасности.

Обеспечение информационной безопасности - это непрерывный процесс, включающий в себя пять ключевых этапов (см. рис. 8.1):

- оценку;
- политику;
- реализацию;
- квалифицированную подготовку;
- аудит.

Каждый из этих этапов по отдельности повышает уровень защищенности организации; однако только взятые вместе они обеспечивают основу, которая позволит эффективно управлять риском.

Рис. Обеспечение информационной безопасности

Оценка стоимости

Процесс обеспечения информационной безопасности начинается с оценки имущества: определения информационных активов организации, факторов, угрожающих этой информации, и ее уязвимости, значимости общего риска для организации. Это важно просто потому, что без понимания текущего состояния риска невозможно эффективно выполнить программу защиты этих активов.

Данный процесс выполняется при соблюдении метода управления риском. Сразу после выявления риска и его количественной оценки можно выбрать рентабельную контрмеру для уменьшения этого риска.

Цели оценки информационной безопасности следующие:

- определить ценность информационных активов;
- определить угрозы для конфиденциальности, целостности, доступности и/или идентифицируемости этих активов;
- определить существующие уязвимые места в практической деятельности организации;
- установить риски организации в отношении информационных активов;
- предложить изменения в существующей практике работы, которые позволят сократить величину рисков до допустимого уровня;
- обеспечить базу для создания соответствующего проекта обеспечения безопасности.

Перечисленные цели не изменят тип оценки, принятый в организации. Однако степень приближения каждой цели зависит от масштабов работы.

Перечислим пять основных видов оценки.

- Оценка уязвимых мест на системном уровне. Компьютерные системы исследованы на известные уязвимости и простейшие политики соответствия техническим требованиям.
- Оценка на сетевом уровне. Произведена оценка существующей компьютерной сети и информационной инфраструктуры и выявлены зоны риска.
- Общая оценка риска в рамках организации. Произведен анализ всей организации с целью выявления угроз для ее информационных активов. Установлены уязвимости в местах обработки информации по всей организации.

Исследована информация, представленная как в электронном виде, так и на физических носителях.

- Аудит. Исследована существующая политика и соответствие организации этой политике.
- Испытание на возможность проникновения. Исследована способность организации реагировать на смоделированное проникновение. Этот тип оценки пригоден только для организаций с высокоразвитой программой безопасности.

В последующем обсуждении предположим, что во время проведения аудита будет проведено также испытание на возможность проникновения. Эти виды оценки подразумевают некоторое предварительное понимание рисков и наличие опыта в практической реализации системы безопасности и управления риском. Ни один из видов оценки не подходит, когда организация пробует понять текущее состояние безопасности.

Необходимо провести оценку собранной информации из трех главных источников:

- опрос работников;
- проверка документации;
- инвентаризация.

Нужно проводить опрос работников, которые будут обеспечивать информацией существующие системы безопасности и направления деятельности организации. Не рекомендуется смешивать служебный персонал и руководителей. Опрашивающий должен непринужденно направить разговор на задачи оценки и на то, как человек может содействовать защите информационных активов. Имейте в виду, что сотрудник может заверить вас, что ни одно из направлений обеспечения информационной безопасности активов за ним не закреплено.

Обязательно изучите все существующие политики, связанные с безопасностью. Исследование не должно ограничиваться только готовыми документами, внимательно прочитайте и черновики.

Последний этап сбора информации - инвентаризация всех материальных ценностей организации.

При проведении оценки изучают следующие моменты:

- сетевое окружение;
- физические меры безопасности;

- существующие политики и процедуры;
- меры предосторожности, принятые на местах;
- осведомленность работников в вопросах безопасности;
- персонал;
- загруженность персонала;
- взаимоотношения работников;
- строгое соблюдение работниками установленной политики и мероприятий;
- специфику деятельности.

Сетевое окружение

Обычно в сетевом окружении находятся открытые точки доступа к информации и системам. Исследование сети начинают с построения диаграммы сети и рассматривают каждую точку возможного подключения.

Примечание

Диаграмма сети зачастую бывает неточной или устаревшей, следовательно, крайне важно, чтобы она была не единственным источником информации, используемым для определения критических сетевых компонентов.

Расположение серверов, рабочих станций, доступ в интернет, соединения наборного доступа, соединения с удаленными офисами и партнерами должны полностью представлены на диаграмме сети. На основании диаграммы и информации, полученной от системного администратора, собираются следующие данные:

- тип и количество систем в сети;
- операционные системы и их версии;
- топология сети (коммутаторы, маршрутизаторы, мосты и т. д.)
- точки доступа к интернету;
- использование интернета;
- типы, количество и версии всех межсетевых экранов;
- точки входа соединений наборного доступа;
- беспроводные точки доступа;
- тип удаленного доступа;
- топология глобальной сети;
- точки доступа в удаленных офисах;
- точки доступа других организаций;
- расположение веб-серверов, FTP-серверов и почтовых шлюзов;

- используемые протоколы;
- лица, осуществляющие управление сетью.

После определения архитектуры сети выявляются внутренние защитные механизмы сети:

- списки управления доступом маршрутизаторов, правила межсетевых экранов на всех точках доступа в интернет;
- механизмы идентификации, используемые для удаленного доступа;
- защитные механизмы во всех точках доступа других организаций;
- механизмы шифрования, используемые для передачи и хранения информации;
- механизмы шифрования, используемые для защиты переносных компьютеров;
- антивирусные системы, установленные на серверах, рабочих станциях и службах электронной почты;
- настройки безопасности сервера.

Если сетевые и системные администраторы не предоставят подробной информации о настройках безопасности сервера, то вам потребуется обследование сервера. Оно должно охватить требования к паролям, настройки аудита для каждой системы, а также используемые обновления системы и программ.

Узнайте у сетевых администраторов об использующейся системе управления сетью. Необходимо собрать информацию о типах оповещений и лицах, которые осуществляют мониторинг системы и сбор данных. Эта информация пригодится для выявления нарушителей в случае обнаружения вторжения администраторами системы.

Наконец, необходимо выполнить сканирование всех систем на предмет обнаружения уязвимых мест. Это можно сделать с помощью компьютера, размещенного внутри системы (внутреннее сканирование) или размещенного в интернете, за пределами межсетевых экранов организации. Оба результата очень важны, так как позволят выявить уязвимые места, которые могут использоваться злоумышленниками, которые находятся в вашей организации или за ее пределами.

Совет

Имейте в виду, что сетевые администраторы могут не знать обо всех точках удаленного доступа в организации.

Физическая безопасность

Физическая безопасность помещения - важнейшая составляющая системы защиты информации. Определение мер физической безопасности включает управление физическим доступом к подразделениям, а также к секретным отделам и помещениям. Например, центр регистрации и обработки данных должен иметь собственную систему контроля физического доступа. Как минимум, этот доступ должен быть строго ограничен. При определении мер физической безопасности необходимо выявить следующее:

- тип физической защиты здания, офисных помещений, документов на бумажных носителях и центра обработки данных;
- наличие ключей у персонала;
- засекреченные помещения здания или отдела (исключая центр обработки данных).

Определите расположение линий коммуникации внутри помещений и те места, где линии коммуникации входят в здание. В этих местах могут быть размещены подслушивающие устройства, поэтому подобные точки нужно включить в список критических областей. Включите в список и помещения, где возможно аварийное отключение.

Объектами физической безопасности являются источники энергии, системы контроля состояния окружающей среды и системы противопожарной безопасности, используемые в центре обработки данных. Соберите следующую информацию об этих системах:

- какую мощность потребляет подразделение;
- какую мощность потребляет центр обработки данных;
- какие типы источников бесперебойного питания установлены;
- как долго имеющиеся источники бесперебойного питания смогут поддерживать работоспособность системы;
- какие системы соединены с источниками бесперебойного питания;
- кто будет извещен в случае отключения электроэнергии;
- какая система контроля состояния окружающей среды подключена к источнику бесперебойного питания;
- какая система контроля состояния окружающей среды связана с центром обработки данных;
- кто будет извещен в случае выхода из строя системы контроля состояния окружающей среды;
- какой вид системы противопожарной безопасности установлен в центре обработки данных;

- может ли система противопожарной безопасности центра обработки данных среагировать на пожар, не угрожающий центру.

Примечание

Многие правила противопожарной безопасности требуют установки разбрызгивателей во всех частях здания. В последнем случае необходимо использовать систему пожаротушения, которая не использует воду.

Политики и процедуры

Многие политики и процедуры организации связаны с безопасностью. При проведении оценки должны быть исследованы следующие документы:

- политика безопасности;
- информационная политика;
- план восстановления в случае чрезвычайных происшествий;
- процедуры контрмер на чрезвычайное происшествие;
- политика и процедуры резервного копирования;
- справочное руководство работника или инструкции;
- процедуры найма-увольнения работников;
- принципы конфигурирования систем;
- правила межсетевых экранов;
- фильтры маршрутизатора;
- политика сексуальных домогательств на рабочем месте;
- политика физической безопасности;
- методология разработки программного обеспечения;
- методология смены программного обеспечения;
- телекоммуникационные политики;
- диаграммы сети;
- организационная диаграмма.

После получения вышеуказанных политик и процедур каждая из них исследуется на предмет значимости, правомерности, завершенности и актуальности.

Политика или процедура должна быть значимой для практической деловой деятельности, существующей в организации в настоящее время. Общие политики не всегда работают, поскольку не учитывают особенности той или иной организации. Процедуры должны определять методики выполнения текущих задач.

Политики и процедуры должны соответствовать цели, определенной в документе. При исследовании документа на правомерность проверяйте каждое требование на соответствие установленной цели политики или процедуры. Например, если целью политики безопасности является определение требований безопасности ко всем установленным компьютерным системам, она не должна описывать особые конфигурации для майн-фреймов, рабочих станций и клиент-серверных систем.

Политики и процедуры должны охватывать все стороны деятельности организации. Нередко можно обнаружить, что отдельные аспекты деятельности не нашли свое отражение в политике либо вовсе отсутствовали на момент создания политики. Изменения в технологиях очень часто приводят к изменениям в политиках и процедурах.

Политики и процедуры могут устаревать со временем. Причиной этому является не злоупотребление, а, скорее, небрежность. Морально устаревший документ становится бесполезным и "умирает". Организации в своей деятельности не стоят на месте, меняются системы и сетевое окружение. Если политики не адаптируются к появлению новых систем или новых направлений деятельности, то она теряет свое значение. Все политики и процедуры необходимо своевременно и обоснованно обновлять.

Кроме вышеописанных документов, в процессе оценки необходимо исследовать программу в области информированности о проблемах безопасности и материалы, используемые в соответствующих тренингах. Сравните эти материалы с существующими политиками и процедурами, чтобы увидеть, насколько точно они отражают организационную политику.

И в заключение, процедура оценки должна включать исследование сведений о недавних происшествиях и проверках. Это не значит, что вы можете всецело положиться на результаты предыдущей работы, скорее, требуется установить, есть ли прогресс в существующих сферах деятельности.

Меры предосторожности

Меры предосторожности обычно используются для восстановления работоспособного состояния после каких-либо инцидентов. Основными составляющими являются системы резервного копирования и план восстановления на случай чрезвычайных происшествий.

При оценке пригодности систем резервного копирования исследование должно быть глубже, чем просто просмотр политики и процедур резервного копирования. Необходимо произвести опрос системных операторов, чтобы понять, как на самом деле используется система. Получите ответы на следующие вопросы.

- Что представляет собой система резервного копирования?
- Для каких систем проводится резервное копирование и как часто?
- Где хранятся резервные копии?
- Как часто резервные копии перемещаются в архив?
- Выполнялась ли когда-либо проверка резервных копий?
- Как часто должны использоваться резервные копии?
- Повреждались когда-либо резервные копии?
- Как часто данные нуждаются в резервном копировании?

Ответы на эти вопросы прольют свет на эффективность существующих систем резервного копирования.

Исследуйте план восстановления на случай чрезвычайных происшествий, обращая внимание на его полноту. То, как план используется на самом деле, нельзя определить, просто читая его. Опросите служащих, которые будут использовать план, чтобы определить, использовался ли план когда-либо и был ли он действительно эффективен. Задайте им следующие вопросы.

- Использовался это план когда-либо?
- Какой был результат?
- Тестировался ли план?
- Какое оборудование имеется в распоряжении для устранения последствий бедствия?
- Какое альтернативное местоположение доступно?
- Кто несет ответственность за действия по устранению последствий бедствия?

Осведомленность

Политики и процедуры работают замечательно и позволяют значительно улучшить безопасность организации, если им следуют работники вашей организации. Проводя оценку, оставьте время для беседы с постоянными сотрудниками (не имеющими обязанностей управляющих или администраторов) для определения их уровня осведомленности по вопросам политик и процедур компании, а также практических положений должной безопасности. Обойдите офисные помещения для поиска

признаков несоблюдения политик. Обратите внимание на наличие бумажных листков с написанными паролями и на системы, оставленные в активированном состоянии после регистрации пользователей.

Осведомленность администратора также важна. Очевидно, что они обязаны знать политику компании по вопросам конфигурирования систем. Администраторы должны быть осведомлены об угрозах и уязвимостях, о признаках вторжений в системы. Главное, они должны знать, какие действия необходимо предпринять при обнаружении атаки.

Вопрос к эксперту

Вопрос. Имеет ли значение осведомленность сотрудников?

Ответ. Да, она имеет большое значение. Сотрудники имеют доступ и нужные сведения, следовательно, являются возможными источниками угроз. Именно поэтому злоумышленники проявляют к ним повышенный интерес. Есть много методов социального инжиниринга, позволяющих нарушителю достигнуть своей цели, когда все предыдущие попытки натолкнулись на надежную систему безопасности.

Человеческий фактор

Служащие являются одним из самых важных факторов, влияющих на общую безопасность. Отсутствие навыков или, наоборот, их избыток может стать причиной выхода из строя хорошо продуманных программ безопасности. Проверьте уровень навыков персонала, отвечающего за вопросы безопасности, и администраторов, чтобы определить, способны ли они выполнять программу обеспечения безопасности. Персонал, отвечающий за вопросы безопасности, должен понимать свою работу в плане общей политики так же хорошо, как разбираться в последних разработках в своей области. Администраторы должны иметь соответствующие навыки, чтобы на высоком уровне осуществлять управление системами и сетевым окружением внутри организации.

Все пользователи должны иметь базовые навыки в области компьютерных технологий. Тем не менее, при наличии более глубоких знаний (например, у разработчиков программного обеспечения) возможно возникновение дополнительных проблем в сфере безопасности. Если пользователи достаточно хорошо владеют компьютерными технологиями, то им не составит труда установить на свои рабочие станции дополнительное программное обеспечение, которое может повлиять на общую

безопасность организации. Эти люди с большей вероятностью обладают навыками и знаниями, необходимыми для использования уязвимостей внутренних систем.

От аудиторов организации потребуется обследование систем и сетей как часть их рабочего задания. В этом случае аудиторы, разбирающиеся в существующих технологиях и системах, используемых внутри организации, быстрее смогут отыскать проблемы.

Загруженность персонала

Даже очень квалифицированные и сообразительные работники не смогут поддерживать систему безопасности, если они перегружены работой. При возрастании объема работ первым делом будут забыты именно вопросы безопасности. Администраторы не проверяют записи журналов, пользовательские пароли на совместно используемые ресурсы, а менеджеры забывают о том, что говорилось на тренинге по защите систем. Тут даже самая серьезная организация с тщательно разработанными политиками и процедурами столкнется с уязвимостями.

Однако проблема может быть вовсе не такой страшной, как кажется. В процессе оценки необходимо определить, является ли большой объем работы временным явлением либо это постоянная практика, действующая в организации.

Отношение

Отношение управленческого персонала к вопросам безопасности - еще один ключевой аспект в общей среде безопасности. Это отношение определяется при назначении ответственных за безопасность внутри организации. Другая сторона этого отношения проявляется в том, как управляющее звено передает свои взгляды сотрудникам.

Передача взглядов на безопасность имеет две стороны: отношение управляющего звена и механизм передачи. Руководство может вполне осознавать важность процессов безопасности, но если они не доносят это до своих сотрудников, то последние не будут этого понимать.

Поэтому не забудьте исследовать состояние данного вопроса в организации, опросив руководящий состав и сотрудников.

Следование правилам

При составлении плана безопасной информационной среды необходимо определить фактическую среду безопасности. Планируемая среда устанавливается политикой, положениями и существующими механизмами. Фактическая среда определяется реальным согласием на участие в процессе обеспечения безопасности руководителей и сотрудников. Например, если политика безопасности требует еженедельного просмотра журналов аудита, а руководители не делают этого, то, значит, в организации не соблюдаются требования этой политики.

Политика использования восьмизначных паролей одинаково важна для всех сотрудников. Если руководство организации приказывает системным администраторам настроить конфигурацию их компьютеров на использование паролей с меньшим количеством знаков, это указывает на недостаточное следование правилам со стороны руководства.

Совет

Недостаточное следование правилам со стороны руководства однозначно приведет к рассогласованности действий администраторов и других сотрудников.

Специфика деятельности

В заключение исследуйте специфику деятельности организации. Опросите сотрудников и выясните издержки организации в случае нарушения конфиденциальности, целостности, доступности или идентифицируемости информации. Попробуйте выразить величину этих потерь в денежном выражении, времени простоя, утраченной репутации или в расторгнутых сделках.

При исследовании специфики деятельности определите движение информации внутри организации, между отделами и рабочими местами, внутри отделов и в другие организации. Выясните, как звенья этой цепи угрожают информации, как взаимосвязаны между собой отдельные части организации.

Частью процесса оценки является выявление систем и сетей, критичных для выполнения основной функции организации. Если организация связана с электронной коммерцией, выясните, какие системы используются для совершения сделок? Очевидно, необходим веб-сервер, но что насчет других серверных систем? Определение серверных систем позволит выявить прочие риски для организации.

Результаты оценки

После сбора всей информации группа оценки должна ее проанализировать. При оценке безопасности организации нельзя рассматривать отдельные блоки информации. Группа должна исследовать все уязвимости безопасности в контексте организации. Не все уязвимости превратятся в риски. Некоторые уязвимые места будут защищены каким-либо способом, который предотвратит их использование.

После завершения анализа группа оценки обязана представить полный набор рисков и рекомендаций для организации. Риски представляются по порядку - от наибольшего к наименьшему. Для каждого риска группа показывает возможные издержки в каком-либо выражении (денежном, временном, ресурсном, потере репутации и расторгнутых сделках). Каждый риск должен сопровождаться рекомендацией по управлению риском.

Последний шаг оценки - это разработка плана действий по безопасности. Организация должна определить, являются ли результаты оценки реальным отображением состояния безопасности, и учесть их при распределении ресурсов и составлении планов.

Примечание

Вполне вероятно, что в плане самый серьезный риск будет поставлен не на первое место. Этому могут помешать проблемы, связанные с бюджетом и ресурсами.

Разработка политики

Следующим шагом после оценки, как правило, является разработка политик и процедур. Они определяют предполагаемое состояние безопасности и перечень необходимых работ. Без политики нет плана, на основании которого организация разработает и выполнит эффективную программу информационной безопасности.

Необходимо разработать следующие политики и процедуры.

- Информационная политика. Выявляет секретную информацию и способы ее обработки, хранения, передачи и уничтожения.
- Политика безопасности. Определяет технические средства управления для различных компьютерных систем.
- Политика использования. Обеспечивает политику компании по использованию компьютерных систем.
- Политика резервного копирования. Определяет требования к резервным копиям компьютерных систем.
- Процедуры управления учетными записями. Определяют действия, выполняемые при добавлении или удалении пользователей.

- Процедура управления инцидентом. Определяет цели и действия при обработке происшествия, связанного с информационной безопасностью.
- План на случай чрезвычайных обстоятельств. Обеспечивает действия по восстановлению оборудования компании после стихийных бедствий или инцидентов, произошедших по вине человека.

Разработка политик является в большей степени политическим процессом. Во многих отделах найдутся люди, которые заинтересуются политиками и захотят сказать свое слово при их разработке.

Примечание

Как было сказано в лекции 6, определение заинтересованных сторон будет ключевым моментом в создании успешной политики.

Порядок разработки политик

Итак, какая политика должна быть разработана первой? Ответ зависит от рисков, определенных в процессе оценки. Если защита информации определена как область с высоким уровнем риска, информационная политика должна разрабатываться одной из первых. Если же вероятны потери в бизнесе из-за отсутствия плана на случай чрезвычайных действий, то этот план должен быть разработан в первую очередь.

Еще одним фактором в выборе порядка разработки политик является затрачиваемое время. Планы восстановления в случае ЧП обычно представляют очень подробные документы и требуют серьезных усилий со стороны отделов и сотрудников. Этот план потребует много времени для составления; возможно, потребуется помощь стороннего исполнителя, например, компании, поставляющей резервное оборудование для целей полного восстановления на случай стихийного бедствия.

Единственная политика, которая должна быть разработана на начальной стадии процесса, - это информационная политика. Информационная политика формирует основу понимания того, почему внутренняя информация важна и насколько она должна быть защищена. Этот документ послужит основой для программы обучения специалистов по вопросам безопасности, наряду с политикой использования и политикой паролей.

В самом лучшем случае возможна одновременная разработка нескольких политик, поскольку заинтересованные стороны будут объединены общими интересами. Например, системные администраторы интересуются политикой безопасности, но

информационная политика их интересует в меньшей степени. Сотрудникам более близка политика безопасности и процедуры управления пользователями, а не политика резервного копирования, и т. д. В этом случае отдел информационной безопасности становится координатором и носителем функций, облегчающих выполнение проекта. Его представители должны присутствовать на первом собрании, посвященном разработке черновой версии плана, и их предложения станут отправным пунктом.

Совет

Для начала попробуйте составить небольшой документ с небольшим числом заинтересованных сторон. Это создаст благоприятную возможность для достижения успеха, что позволит отделу безопасности прийти к соглашениям, необходимым для разработки остальных документов.

Обновление существующих политик

Если политики и процедуры уже существуют, это хорошо. Однако вероятно, что некоторые из этих документов потребуют обновления. Если в их создании принимал участие отдел информационной безопасности, то в первую очередь необходимо собрать все заинтересованные стороны, участвовавшие в работе над предыдущей версии политики, и начать работу по обновлению. Используйте как отправную точку исходный документ и выявленные неточности.

Если в разработке документа участвовал кто-то из сотрудников организации, его также нужно привлечь к работе над обновлением. Отдел информационной безопасности не должен ослаблять контроль над деятельностью бывшего владельца. В этом случае снова начните с исходного документа и выявленных неточностей.

Если разработчик исходного документа больше не числится в организации, то проще начать с чистого листа. Выявите заинтересованных лиц и пригласите их принять участие в процессе. Сообщите им, почему старый документ больше не является удовлетворительным

Вопросы для самопроверки

1. Общие затраты на безопасность = _____ + _____.
2. Перечислите главные элементы оценки в организации.

Реализация политики безопасности

Реализация политики заключается в реализации технических средств и средств непосредственного контроля, а также в подборе штата безопасности. Могут потребоваться изменения в конфигурации систем, находящихся вне компетенции отдела безопасности. В таких случаях в проведении программы безопасности должны участвовать системные и сетевые администраторы.

Исследуйте каждый этап для определения взаимодействий с другими системами управлениями. Например, усиление физической защиты позволит снизить требования к политике шифрования и наоборот. Установка межсетевых экранов позволит отложить немедленное устранение уязвимых мест внутренних систем.

Системы отчетности по безопасности

Системы отчетности по безопасности - это механизм, с помощью которого отдел безопасности отслеживает соблюдение политик и процедур, общее состояние уязвимых мест внутри организации. Для этого используются как ручные, так и автоматические системы. В большинстве случаев системы отчетности по безопасности включают оба типа систем.

Мониторинг использования

Механизмы мониторинга гарантируют, что работники следуют политикам использования компьютера. Они включают в себя программное обеспечение, отслеживающее использование интернета. Целью является выявление работников, постоянно нарушающих политику компании. Некоторые механизмы способны блокировать такой доступ и сохранять журнал попыток.

Мониторинг использования включает, например, удаление игр, установленных на рабочей станции. Сложные механизмы позволяют определить, что на компьютер пользователя загружено новое программное обеспечение, но они требуют взаимодействия между администраторами и службой безопасности.

Сканирование уязвимых мест систем

Уязвимые места системы стали очень важной темой в безопасности. Установка операционной системы с параметрами по умолчанию обычно сопровождается запуском ненужных процессов и появлением уязвимых мест. Выявление таких мест не составляет труда для службы безопасности, использующей современные инструментальные средства, а вот их исправление отнимает много времени. Служба безопасности должна отслеживать системы и их уязвимые места с определенной периодичностью.

Необходимо обеспечить администраторов отчетами об уязвимых местах для их удаления. Сведения о вновь установленных системах нужно доводить до сведения системного администратора.

Соблюдение политики

Соблюдение политики - это одно из заданий службы безопасности, отнимающее много времени. Для определения соблюдения политики используются ручной и автоматический режимы. Ручной механизм требует от работника службы безопасности исследования каждой системы и определения, как выполняются требования политики безопасности в конфигурации этой системы. Это отнимает чрезвычайно много времени, велика и вероятность ошибок. Намного чаще из общего количества систем выбирается одна, и проводится ее выборочное исследование. Такой способ требует меньше времени, но далек от совершенства.

Для проведения автоматической проверки соблюдения политики разрабатывается соответствующее программное обеспечение. Такой способ требует больше времени для установки и конфигурирования, но дает более точный результат в более короткие сроки. В этом случае требуется помощь системных администраторов, поскольку программное обеспечение необходимо установить в каждой проверяемой системе. Контроль соблюдения политики может выполняться на основе периодической выборки и результатов обращений к системным администраторам.

Аутентификация систем

Аутентификация систем - это механизм, предназначенный для установления личности пользователей, желающих получить доступ в систему или сеть. Она позволяет также идентифицировать лиц, пытающихся завладеть оборудованием организации. Механизмы аутентификации - это пароли, смарт-карты и биометрия. Требования к ним должны быть включены в программы профессиональной переподготовки по вопросам безопасности.

Примечание

Механизмы аутентификации можно применить к любому пользователю системы. Отсюда следует, что обучение и компетентность пользователя являются важными сторонами развертывания любого механизма аутентификации.

Если пользователи не ознакомлены с работой системы аутентификации, то отдел ИТ будет перегружен звонками в службу технической поддержки. Производительность

работы будет снижена, поскольку пользователи начнут изучать, как пользоваться новой системой. Ни при каких обстоятельствах изменения в способах аутентификации не должны осуществляться без обучения пользователей. Эти способы оказывают влияние на все системы организации, и их реализация должна сопровождаться подробным планированием. Служба безопасности должна работать во взаимодействии с системными администраторами, чтобы процесс реализации проходил без сбоев.

Безопасность в интернете

Реализация безопасности в интернете включает такие механизмы, как межсетевые экраны и виртуальные частные сети (VPN), и ведет к изменениям в сетевой архитектуре (см. лекции 10, 11, 16). Наиболее важным аспектом ее реализации является размещение устройства управления доступом (типа межсетевого экрана) между интернетом и внутренней сетью организации. Без подобной защиты все внутренние системы открыты для неконтролируемых нарушений безопасности. Установка межсетевого экрана является достаточно сложным процессом и может повлечь за собой сбои в нормальной работе пользователей.

Примечание

Размещение межсетевого экрана или другого устройства управления доступом ведет к изменению архитектуры. Подобная операция не должна выполняться до тех пор, пока не будет определена основная сетевая архитектура: ведь нужно установить межсетевой экран соответствующей мощности и задать на нем правила в соответствии с используемыми политиками организации.

Виртуальные частные сети обеспечивают безопасность для информации, передаваемой через интернет и периметр организации. Вопросы, связанные с VPN, могут быть включены в реализацию механизмов безопасности в интернете.

Системы обнаружения вторжений

Системы обнаружения вторжений (IDS) - это системы охранной сигнализации сети. Охранная сигнализация предназначена для обнаружения попыток проникновения в защищаемое помещение, а IDS - для разграничения санкционированного входа и вторжения злоумышленника в защищаемую сеть.

Имеется несколько типов систем обнаружения вторжения, и выбор нужной зависит от совокупного риска организации и располагаемых ресурсов (см. лекцию 13). Системы обнаружения вторжений требуют значительных финансовых вложений.

Самым общим механизмом обнаружения вторжений является антивирусное программное обеспечение. Это программное обеспечение должно работать на каждой рабочей станции и, разумеется, на сервере. Антивирусное программное обеспечение - наименее ресурсоемкий способ обнаружения вторжений.

Перечислим другие способы обнаружения вторжений:

- ручная проверка журнала;
- автоматическая проверка журнала;
- клиентское программное обеспечение для обнаружения вторжения;
- сетевое программное обеспечение для обнаружения вторжения.

Ручная проверка журнала весьма эффективна, но занимает много времени и склонна к ошибкам. Люди для этой цели не подходят. Наилучшим способом проверки журналов является создание программ или скриптов, которые просматривают журналы компьютера в поисках возможных отклонений.

Совет

Развертывание механизмов обнаружения вторжения не следует проводить до тех пор, пока не будут выявлены области с повышенным риском.

Шифрование

Шифрование обычно применяют для защиты конфиденциальных или частных интересов (см. лекцию 12). Механизмы шифрования используются для защиты передаваемой или сохраняемой информации. Вне зависимости от типа используемого механизма возникают два вопроса, на которые нужно ответить до его реализации:

- алгоритмы;
- управление ключом защиты.

Примечание

Шифрование ведет к замедлению обработки или передачи данных. Следовательно, шифрование всей передаваемой информации не всегда является целесообразным.

Алгоритмы

При выполнении шифрования выбор алгоритма обуславливается конечной целью. Шифрование на личном ключе происходит быстрее, чем на открытом. Однако такой

способ не позволяет использовать цифровую подпись или подписывание информации. Важно выбрать известные и хорошо изученные алгоритмы. Такие алгоритмы с большой долей вероятности исключают лазейки, через которые возможен доступ к защищенной информации.

Управление ключом защиты

Развертывание механизмов шифрования должно включать управление ключом защиты. При использовании шифровального блока (устройства для шифрования трафика, передаваемого от узла к узлу) система должна разрешать периодическое изменение ключа. При шифровании на открытом ключе, когда сертификаты выдаются большому количеству лиц, проблема намного серьезнее.

Если планируется введение подобной системы, удостоверьтесь в наличии времени для испытания ключа защиты. Также имейте в виду, что экспериментальная программа позволяет охватить ограниченное число пользователей, а система управления ключом защиты должна быть соразмерна всей системе.

Физическая безопасность

Физическая безопасность традиционно обособлена от информационной или компьютерной безопасности. Установка видеокамер, замков и охранников обычно не очень хорошо понималась работниками отдела компьютерной безопасности. Если в вашей организации дело обстоит именно так, вы должны найти поддержку со стороны. Имейте в виду, что устройства физической безопасности затронут работников организации, как и изменение способа аутентификации. Работники, которые видят видеокамеры в туалете или предъявляют пластиковую карту для входа в кабинет, должны приспособиться к новым обстоятельствам. Если сотрудники пользуются такими картами, то организация должна разработать процедуру действий работников, потерявших или оставивших их дома.

Такая процедура должна доказать, что данный человек действительно является сотрудником организации. Это могут быть цифровые фотографии или звонок коллеги для подтверждения подлинности. Некоторые организации полагаются только на подпись работника в соответствующем журнале. Такой метод позволяет злоумышленнику получить доступ к ее материальным ценностям.

Применяя механизмы физической безопасности, вы не должны забывать о безопасности центра обработки данных. Доступ к центру данных должен быть

ограничен, как следует защищен от огня, высокой температуры и отключения электричества. Внедрение систем пожаротушения и климат-контроля заставит вас провести всестороннюю модернизацию центра данных. Применение источника бесперебойного питания следует применять в системах, отключающихся на короткое время.

Персонал

При применении любых новых систем безопасности вы должны располагать подходящим персоналом. Некоторые системы потребуют постоянного обслуживания (механизмы идентификации пользователей и системы обнаружения вторжений). Другим системам потребуются люди для выполнения положений плана (например, для сканирования уязвимостей).

Вам потребуются обученные сотрудники при проведении учебных программ по повышению осведомленности. Сотрудник отдела информационной безопасности должен присутствовать на каждом учебном занятии, чтобы отвечать на специфические вопросы, даже если обучение проводится отделом обучения.

Последняя проблема, связанная с персоналом, - это ответственность. Ответственность за безопасность организации должна устанавливаться индивидуально. В большинстве случаев ответственным назначается руководитель отдела безопасности, который отвечает за разработку политики, исполнение плана и реализацию механизмов безопасности. Назначение этой обязанности должно быть первым шагом по пути реализации нового плана безопасности.

Проведение профессиональной переподготовки

Организация не может обеспечить защиту секретной информации, не привлекая своих сотрудников. Грамотная профессиональная переподготовка - это механизм обеспечения сотрудников необходимой информацией. Программы обучения могут иметь форму коротких занятий, информационных статей или плакатов. Наиболее эффективные программы используют все три формы.

Сотрудники

Сотрудники должны знать, почему вопросы безопасности так важны, должны быть обучены выявлению и защите секретной информации. Компетентная профессиональная переподготовка по безопасности обеспечивает их необходимой информацией в области

политики организации, выбора пароля и предупреждения атак социального инжиниринга.

Обучение сотрудников лучше всего проводить короткими занятиями - по часу или менее. Видеоматериалы способствуют более качественному уровню занятий, чем обычная лекция. Все новые сотрудники должны проходить обучение как часть инструктажа, а все работающие - раз в два года.

Администраторы

Обучение важно и для системных администраторов. Они должны быть осведомлены о последних на данный момент технических приемах хакеров, угрозах безопасности и обновления программных продуктов. Это обучение должно проходить часто (возможно, раз в месяц) и проводиться сотрудниками отдела безопасности. Информация об обновлениях может быть включена в регулярные совещания штата администраторов для экономии времени, так необходимого администраторам. В дополнение к этому отдел безопасности должен передавать обновления администраторам сразу после появления новых версий, не дожидаясь очередного совещания.

Разработчики

Обучение для разработчиков должно быть расширенной версией учебных занятий для сотрудников. Дополнительный материал включает специфические технические приемы программирования для устранения уязвимых мест и соответствующее понимание роли отдела безопасности в процессе разработки.

Для всех новых разрабатываемых проектов необходимо вовлекать на стадии проектирования отдел безопасности. Это позволит анализировать новые проекты на предмет приоритетного выделения средств на вопросы, связанные с безопасностью. Обучение разработчиков должно дать объяснение важности такого подхода.

Руководители

Презентация для руководителей организации - это отчасти и обучение, и маркетинг. Без поддержки руководства программа безопасности просто не сможет существовать. Следовательно, руководство должно быть проинформировано о состоянии безопасности и о дальнейшем развитии программы.

Периодические презентации руководству должны включать результаты недавних оценок и состояние различных проектов по безопасности. По возможности система

показателей, выражающая риски для организации, должна быть общепризнанной. Например, нужно отследить и отразить в отчете число уязвимых мест организации и нарушений системной политики.

Совет

В ходе этих презентаций можно представить информацию, используемую для обучения сотрудников, чтобы напомнить руководству об их обязанностях в плане обеспечения безопасности.

Персонал отдела безопасности

Персонал отдела безопасности должен быть осведомлен о современном состоянии дел, чтобы грамотно выполнять свою работу. Важно проводить как внешнее, так и внутреннее обучение. Например, каждому сотруднику отдела безопасности можно назначить время для проведения обучения остальных сотрудников этого отдела на любую тему по выбору. Темы должны быть связаны с безопасностью либо с текущим вопросом, интересующим персонал, либо с навыком, отсутствующим у персонала.

Проведение аудита

Аудит - это последний шаг в процессе реализации информационной безопасности. После определения состояния информационной безопасности внутри организации, создания соответствующих политик и процедур, приведения в действие технических средств контроля и обучения персонала проведение аудита позволит удостовериться, что все средства контроля сконфигурированы правильно.

Обсуждая место аудита в процессе безопасности, мы в действительности говорим о трех разных функциях:

- аудит соблюдения политики;
- периодическая оценка существующих проектов и оценка новых проектов;
- проверка возможности нарушения защиты.

Каждая из этих функций занимает свое место в процессе обеспечения безопасности.

Аудит соблюдения политики

Аудит соблюдения политики - это традиционная функция аудита. Организация имеет политику, определяющую настройки и конфигурацию систем безопасности. Аудит

определяет реальное состояние дел. Любые отклонения отмечаются как нарушения. Подобные проверки могут выполняться внутренним персоналом или внешними консультантами. И в том и в другом случае этот процесс требует участия системных администраторов.

Аудит соблюдения политики не должен ограничиваться только проверкой конфигурации систем. Он должен проявлять интерес к тому, как выполняются другие формы управления информацией. Соблюдается ли информационная политика? Как хранятся и передаются секретные документы?

Проверки должны проводиться раз в год. Они могут выполняться персоналом отдела безопасности, но, возможно, выполнение аудита больше подходит для отдела аудита организации или для сторонней фирмы. Причина в том, что в данном случае могут быть затронуты интересы самого отдела безопасности, что приведет к возникновению конфликта интересов.

Периодическая оценка проектов и оценка новых проектов

Компьютерная и сетевая среда внутри организации находятся в состоянии постоянного изменения. Эти изменения приводят к быстрому старению результатов оценки за счет сокращения некоторых рисков и введения новых. По этой причине оценка должна выполняться периодически. Полная оценка организации должна выполняться раз в два года. Как и в случае с крупными проверками, серьезные оценки выполняются персоналом отдела безопасности, если он обладает необходимыми навыками. Возможно, для этих целей больше подходит сторонняя организация.

Небольшие оценки должны выполняться в случае разработки новых проектов или изменений в организационной среде. Для каждого нового проекта отдел безопасности привлекается к работе на стадии проектирования, чтобы определить, имеет ли проект какие-либо риски, и происходит ли в результате разработки проекта появление или сокращение рисков внутри организации. Этот тип оценки должен изучать новый проект в контексте его использования по отношению к другим структурным элементам организации. Если риски определены на ранней стадии проекта, проектирование может быть скорректировано или введены другие механизмы для управления риском.

Проверка возможности нарушения защиты

Проверка возможности нарушения защиты - это спорная тема. Часто такие проверки выполняются вместо оценки. На самом деле, они имеют ограниченную ценность в

программе безопасности. Причина этого проста: при проверках предпринимаются попытки воспользоваться установленной уязвимостью, чтобы получить доступ к системам и информации внутри организации. Если такая проверка имеет успех, то единственный вывод из всего этого - обнаружена, по крайней мере, одна уязвимость. Если проверка нарушения защиты терпит неудачу, то вывод такой - проверяющий не смог обнаружить и использовать уязвимость. Это вовсе не значит, что уязвимости не существует.

Почему же тогда необходимо выполнять проверку возможности нарушения защиты? Если организация провела оценку и применила подходящие средства управления риском, она может выборочно проверить некоторых из них. Проверка защиты подходит для следующих случаев.

- Способность системы обнаружения вторжений выявить попытку нарушения защиты.
- Уместность процедуры реагирования на инцидент, связанный с безопасностью.
- Информация о сети, которую можно узнать через средства управления сетевым доступом.
- Уместность физической безопасности помещения.
- Адекватность информации, предоставляемой сотрудникам программой повышения осведомленности в плане безопасности.

Внимание!

Какой бы ни была причина проведения проверки возможности нарушения защиты, подробный план этой проверки должен быть предоставлен до ее начала. Для каждого этапа плана необходимо определить цель проверки.

Организация определяет также масштаб проверки. Проверка возможности нарушения защиты через внешнюю сеть ограничена внешними сетевыми соединениями организации (соединения через интернет или с другими внешними организациями). Они могут включать доступ через коммутируемое подключение к сети компании или доступ к беспроводным сетям. Проверка физического нарушения защиты выявляют людей, пытающихся получить несанкционированный доступ к оборудованию. Масштаб подобных тестов может быть ограничен как рабочим, так и нерабочим временем. Проверка возможности атак социального инжиниринга связана с тестированием осведомленности сотрудников, она разрешает проверяющим вступать в контакт с сотрудниками, пытаясь заставить их разгласить информацию или предоставить доступ к внутренним системам.

Многие организации начинают развертывание систем безопасности с проверки возможности нарушения защиты. Однако большой пользы это не принесет, поскольку организация не получит достаточного количества информации, позволяющего управлять ее рисками.

Разработайте программу повышения осведомленности в плане безопасности

Осведомленность в плане безопасности - это важная часть любой хорошей программы безопасности. Самым важным моментом здесь является использование наглядных и выразительных способов предоставления информации сотрудникам. Для этого у вас есть занятия, плакаты, информационные листки и электронная почта.

Шаг за шагом

1. Определите ключевую информацию, которая должна быть передана сотрудникам вашей организации. Ее можно найти в различных политиках, используемых в организации. Обратите особое внимание на требования паролей, идентификационные карточки, использование политик, в общем, на все, что напрямую влияет на работу сотрудников.
2. Определите этапы программы повышения осведомленности и то, что будет использоваться для обучения сотрудников (например, проведение занятий или вывешивание плакатов).
3. Наметьте в общих чертах, как будет представлен материал.
4. Определите ресурсы, необходимые для выполнения программы обучения (инструкторы для занятий, кабинеты и т. д.).

Выводы

В большинстве случаев лучше всего использовать сочетание ежегодных занятий с ежемесячными информационными статьями и плакатами. Занятия для сотрудников не должны длиться больше одного часа, и даже тогда они должны быть более интересными, чем просто лекция сотрудника отдела безопасности. Старайтесь повышать уровень новаторскими идеями, чтобы удерживать интерес сотрудников.

Программно-аппаратные средства обеспечения информационной безопасности

Особенности функционирования МЭ на различных уровнях модели OSI

МЭ поддерживают безопасность межсетевого взаимодействия на различных уровнях модели OSI. При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга. Поэтому комплексный МЭ удобно представить в виде совокупности неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI.

Чаще всего комплексный экран функционирует на сетевом, сеансовом и прикладном уровнях эталонной модели. Соответственно различают такие неделимые МЭ (рис. 9.5), как:

• экранирующий маршрутизатор;

• шлюз сеансового уровня (экранирующий транспорт);

• шлюз прикладного уровня (экранирующий шлюз).

Используемые в сетях протоколы (TCP/IP, SPX/IPX) не полностью соответствуют эталонной модели OSI, поэтому экраны перечисленных типов при выполнении своих функций могут охватывать и соседние уровни эталонной модели. Например, прикладной экран может осуществлять автоматическое зашифровывание сообщений при их передаче во внешнюю сеть, а также автоматическое расшифровывание криптографически закрытых принимаемых данных. В этом случае такой экран функционирует не только на прикладном уровне модели OSI, но и на уровне представления.

Шлюз сеансового уровня при своем функционировании охватывает транспортный и сетевой уровни модели OSI. Экранирующий маршрутизатор при анализе пакетов сообщений проверяет их заголовки не только сетевого, но и транспортного уровня.

МЭ указанных типов имеют свои достоинства и недостатки. Многие из используемых МЭ являются либо прикладными шлюзами, либо экранирующими маршрутизаторами, не обеспечивая полную безопасность межсетевого взаимодействия. Надежную защиту обеспечивают только комплексные межсетевые экраны, каждый из которых объединяет экранирующий маршрутизатор, шлюз сеансового уровня, а также прикладной шлюз.

Рассмотрим более детально особенности их функционирования.

Прикладной шлюз

Прикладной шлюз, называемый также *экранирующим шлюзом*, функционирует на прикладном уровне модели OSI, охватывая также уровень представления, и обеспечивает наиболее надежную защиту межсетевых взаимодействий. Защитные функции прикладного шлюза, как и шлюза сеансового уровня, относятся к функциям посредничества. Однако прикладной шлюз, в отличие от шлюза сеансового уровня, может выполнять существенно большее количество функций защиты, к которым относятся следующие:

• идентификация и аутентификация пользователей при попытке установления соединений

через МЭ;
• проверка подлинности информации, передаваемой через шлюз;
• разграничение доступа к ресурсам внутренней и внешней сетей;
• фильтрация и преобразование потока сообщений, например динамический поиск вирусов и прозрачное шифрование информации;
• регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерация отчетов;
• кэширование данных, запрашиваемых из внешней сети.

Поскольку функции прикладного шлюза относятся к функциям посредничества, этот шлюз представляет собой универсальный компьютер, на котором функционируют программные посредники (экранирующие агенты) — по одному для каждого обслуживаемого прикладного протокола (HTTP, FTP, SMTP, NNTP и др.). Программный посредник (application proxy)каждой службы TCP/IP ориентирован на обработку сообщений и выполнение функций защиты, относящихся именно к этой службе.

Прикладной шлюз перехватывает с помощью соответствующих экранирующих агентов входящие и исходящие пакеты, копирует и перенаправляет информацию, т. е. функционирует в качестве сервера-посредника, исключая прямые соединения между внутренней и внешней сетью (рис. 9.6).

Посредники, используемые прикладным шлюзом, имеют важные отличия от канальных посредников шлюзов сеансового уровня. Во-первых, посредники прикладного шлюза связаны с конкретными приложениями (программными серверами), во-вторых, они могут фильтровать поток сообщений на прикладном уровне модели OSI.

Прикладные шлюзы используют в качестве посредников специально разработанные для этой цели программные серверы конкретных служб TCP/IP —

серверы HTTP, FTP, SMTP, NNTP и др. Эти программные серверы функционируют на МЭ в резидентном режиме и реализуют функции защиты, относящиеся к соответствующим службам TCP/IP.

Шлюз прикладного уровня обладает следующими достоинствами:

• обеспечивает высокий уровень защиты локальной сети благодаря возможности выполнения большинства функций посредничества;

• защита на уровне приложений позволяет осуществлять большое число дополнительных проверок, уменьшая тем самым вероятность проведения успешных атак, возможных из-за недостатков программного обеспечения;

• при нарушении его работоспособности блокируется сквозное прохождение пакетов между разделяемыми сетями, в результате чего безопасность защищаемой сети не снижается из-за возникновения отказов.

К недостаткам прикладного шлюза относятся:

• высокие требования к производительности и ресурсоемко-сти компьютерной платформы;

• отсутствие «прозрачности» для пользователей и снижение пропускной способности при реализации межсетевых взаимодействий.

Шлюзы уровня приложений

С целью защиты ряда уязвимых мест, присущих фильтрующим маршрутизаторам, межсетевые экраны должны использовать прикладные программы для фильтрации соединений с такими сервисами, как Telnet и FTP. Подобное приложение называется proxy-службой, а хост, на котором работает proxy-служба, — шлюзом уровня приложений. Такой шлюз исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне.

Обнаружив сетевой сеанс, шлюз приложений останавливает его и вызывает уполномоченное приложение для оказания завершаемой услуги. Для достижения более

высокого уровня безопасности и гибкости шлюзы уровня приложений и фильтрующие маршрутизаторы могут быть объединены в межсетевом экране.

Шлюзы прикладного уровня позволяют обеспечить надежную защиту, поскольку взаимодействие с внешним миром реализуется через небольшое число уполномоченных приложений, полностью контролирующих весь входящий и исходящий трафик. Следует отметить, что шлюзы уровня приложений требуют отдельного приложения для каждого сетевого сервиса.

По сравнению с работающими в обычном режиме, при котором прикладной трафик пропускается непосредственно к внутренним хостам, шлюзы прикладного уровня имеют ряд преимуществ:

- невидимость структуры защищаемой сети из глобальной сети Интернет. Имена внутренних систем можно не сообщать внешним системам через DNS, поскольку шлюз прикладного уровня может быть единственным хостом, имя которого будет известно внешним системам;
- надежная аутентификация и регистрация. Прикладной трафик может быть аутентифицирован, прежде чем он достигнет внутренних хостов, и зарегистрирован более эффективно, чем с помощью стандартной регистрации;
- приемлемое соотношение цены и эффективности. Дополнительные программные или аппаратные средства аутентификации или регистрации нужно устанавливать только на шлюзе прикладного уровня;
- простые правила фильтрации. Правила на фильтрующем маршрутизаторе оказываются менее сложными, чем на маршрутизаторе, который самостоятельно фильтрует прикладной трафик и отправляет его большому числу внутренних систем. Маршрутизатор должен пропускать прикладной трафик, предназначенный только для шлюза прикладного уровня, и блокировать весь остальной;
- возможность организации большого числа проверок. Защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, что снижает вероятность взлома с использованием «дыр» в программном обеспечении.

Недостатками шлюзов уровня приложений являются:

- относительно низкая производительность по сравнению с фильтрующими маршрутизаторами. В частности, при использовании клиент-серверных протоколов, таких как Telnet, требуется двухшаговая процедура для входных и выходных соединений;
- более высокая стоимость по сравнению с фильтрующими маршрутизаторами.

Одним из важных элементов концепции межсетевых экранов является аутентификация (проверка подлинности пользователя), то есть пользователь получает право воспользоваться тем или иным сервисом только после того, как будет установлено, что он действительно тот, за кого себя выдает. При этом считается, что сервис для данного пользователя разрешен (процесс определения, какие сервисы разрешены конкретному пользователю, называется авторизацией).

При получении запроса на использование сервиса от имени какого-либо пользователя межсетевой экран проверяет, какой способ аутентификации определен для данного субъекта, и передает управление серверу аутентификации. После получения положительного ответа от сервера аутентификации межсетевой экран осуществляет запрашиваемое пользователем соединение. Как правило, большинство коммерческих межсетевых экранов поддерживает несколько различных схем аутентификации, предоставляя администратору сетевой безопасности возможность сделать выбор наиболее приемлемой в сложившихся условиях схемы.

Классификация межсетевых экранов

В настоящее время не существует единой и общепризнанной классификации межсетевых экранов. Выделим следующие классы межсетевых экранов:

1. Фильтрующие маршрутизаторы.
2. Шлюзы сеансового уровня.
3. Шлюзы уровня приложений.

Эти категории можно рассматривать как базовые компоненты реальных межсетевых экранов. Лишь немногие межсетевые экраны включают лишь одну из перечисленных категорий. Тем не менее эти компоненты отражают ключевые возможности, отличающие межсетевые экраны друг от друга.

Фильтрующие маршрутизаторы

Фильтрующий маршрутизатор представляет собой маршрутизатор или работающую на сервере программу, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP-заголовках пакетов.

Фильтрующий маршрутизатор обычно может фильтровать IP-пакеты на основе группы следующих полей заголовка пакета:

- IP-адрес отправителя;
- IP-адрес получателя;
- порт отправителя;
- порт получателя.

Некоторые маршрутизаторы проверяют, с какого сетевого интерфейса маршрутизатора пришел пакет, и затем используют эту информацию как дополнительный критерий фильтрации.

Фильтрация может быть реализована различными способами для блокирования соединений с определенными компьютерами или портами. Например, можно блокировать соединения, идущие от конкретных адресов тех компьютеров и сетей, которые считаются враждебными или ненадежными.

Правила фильтрации пакетов формулируются сложно, к тому же обычно не существует средств для проверки их корректности, кроме медленного ручного тестирования. При

этом в отсутствие фильтрующего маршрутизатора средств протоколирования (если правила фильтрации пакетов все-таки позволят опасным пакетам пройти через маршрутизатор) такие пакеты не смогут быть выявлены до обнаружения последствий проникновения. Даже если администратору сети удастся создать эффективные правила фильтрации, их возможности останутся ограниченными. Например, администратор задает правило, в соответствии с которым маршрутизатор будет отбраковывать все пакеты с неизвестным адресом отправителя. Однако в данном случае хакер для проникновения внутрь защищенной сети может осуществить атаку, которую называют подменой адреса. В таких условиях фильтрующий маршрутизатор не сумеет отличить поддельный пакет от настоящего и пропустит его.

К положительным качествам фильтрующих маршрутизаторов можно отнести следующие:

- сравнительно невысокая стоимость;
- гибкость в определении правил фильтрации;
- небольшая задержка при прохождении пакетов.

Недостатки фильтрующих маршрутизаторов:

- внутренняя сеть видна (маршрутизируется) из сети Интернет;
- правила фильтрации пакетов трудны в описании и требуют очень хороших знаний технологий TCP и UDP;
- при нарушении работоспособности межсетевого экрана с фильтрацией пакетов все компьютеры за ним становятся полностью незащищенными либо недоступными;

Списки доступа на маршрутизаторах Cisco

Список доступа – это набор записей (строк), определяющих некие образцы, на соответствие которым проверяются пакеты IP. Когда пакет проходит через интерфейс маршрутизатора, то для поиска соответствующего пакету образца просматриваются все записи приписанного к интерфейсу списка доступа. Связанное с этим образцом правило разрешает или запрещает проход пакета. Можно использовать маску для определения того, какую часть IP-адреса отправителя или получателя задействовать при проверке на совпадение с образцом. Задавая образец, можно также указать номер протокольного порта TCP или UDP.

Поддерживаются следующие виды списков доступа для IP:

* Стандартные списки доступа (проверяют адрес отправителя пакета)

* Расширенные списки доступа (проверяют адрес отправителя, адрес получателя и еще ряд параметров пакета)
* Динамические расширенные списки доступа (имеют конечное и условия применения)

ACL разделяются на два типа:

- Стандартные (Standard): *могут проверять только адреса источников*
- Расширенные (Extended): *могут проверять адреса источников, а также адреса получателей, в случае IP ещё тип протокола и TCP/UDP порты*

Обозначаются списки доступа либо номерами, либо символьными именами. ACL также используются для разных сетевых протоколов. Мы в свою очередь будем работать с IP. Обозначаются они следующим образом, нумерованные списки доступа:

- Стандартные: *от 1 до 99*
- Расширенные: *от 100 до 199*

Функционал ACL состоит в классификации трафика, нужно его проверить сначала, а потом что-то с ним сделать в зависимости от того, куда ACL применяется. ACL применяется везде, например:

- На интерфейсе: *пакетная фильтрация*
- На линии Telnet: *ограничения доступа к маршрутизатору*
- VPN: *какой трафик нужно шифровать*
- QoS: *какой трафик обрабатывать приоритетнее*
- NAT: *какие адреса транслировать*

Для применения ACL для всех этих компонентов нужно понять как они работают. И мы в первую очередь будем касаться пакетной фильтрации. Применительно к пакетной фильтрации, ACL размещаются на интерфейсах, сами они создаются независимо, а уже потом они прикручиваются к интерфейсу. Как только вы его прикрутили к
интерфейсу маршрутизатор начинает просматривать трафик. Маршрутизаторрассматривает трафик как входящий и исходящий. Тот трафик, который входит в маршрутизатор называется входящим, тот который из него выходит — исходящий. Соответственно ACL размещаются на входящем или на исходящем направлении.

Из вашей частной сети приходит пакет на

интерфейс маршрутизатора fa0/1, маршрутизатор проверяет есть ли ACL на интерфейсе или нет, если он есть, то дальше обработка ведется по правилам списка доступа **строго в том порядке, в котором записаны выражения**, если список доступа разрешает проходить пакету, то в данном случае маршрутизатор отправляет пакет провайдеру через интерфейс fa0/0, если список доступа не разрешает проходить пакету, пакет уничтожается. Если списка доступа нет — пакет пролетает без всяких ограничений. Перед тем как отправить пакет провайдеру, маршрутизатор ещё проверяет интерфейс fa0/0 на наличие исходящего ACL. Дело в том, что ACL может быть прикреплен на интерфейсе как входящий или исходящий. К примеру у нас есть ACL с правилом запретить всем узлам в Интернете посылать в нашу сеть
сы. Так на какой интерфейс прикрепить данную ACL? Если мы прикрепим ACL на интерфейс fa0/1 как исходящий, это будет не совсем верно, хотя и ACL работать будет. На маршрутизатор приходит эхо-запрос для какого-то узла в частной сети, он проверяет на интерфейсе fa0/0 естьли ACL, его нет, дальше проверяет интерфейс fa0/1, на данном интерфейсе есть ACL, он настроен как исходящий, всё верно пакет не проникает в сеть, а уничтожается маршрутизатором. Но если мы прикрепим ACL за интерфейсом fa0/0 как входящий, то пакет будетуничтожатся сразу как пришел на маршрутизатор. Последнее решение является правильным, так как маршрутизатор меньше нагружает свои вычислительные ресурсы. **ACL необходимо размещать как можно ближе к источнику**. Это нужно для того, чтобы не гонять пакеты по всей сети зря.

Сам же ACL представляет собой набор текстовых выражений, в которых
написано **permit** (разрешить) либо **deny** (запретить), и обработка ведется строго в том порядке в котором заданы выражения. Соответственно когда пакет попадает на интерфейс он проверяется на первое условие, если первое условие совпадает с пакетом, дальнейшая его обработка прекращается. Пакет либо перейдет дальше, либо уничтожится.
Ещё раз, **если пакет совпал с условием, дальше он не обрабатывается.** Если первое условие не совпало, идет обработка второго условия, если оно совпало, обработка прекращается, если нет, идет обработка третьего условия и так дальше пока не проверятся все условия, **если никакое из условий не совпадает, пакет просто уничтожается**. Помните, в каждом конце списка стоит неявный deny any (запретить весь трафик). Будьте очень внимательны с этими правилами, которые я выделил, потому что очень часто происходят ошибки при конфигурации.

ACL разделяются на два типа:

- Стандартные (Standard): *могут проверять только адреса источников*
- Расширенные (Extended): *могут проверять адреса источников, а также адреса получателей, в случае IP ещё тип протокола и TCP/UDP порты*

Обозначаются списки доступа либо номерами, либо символьными именами. ACL также

используются для разных сетевых протоколов. Мы в свою очередь будем работать с IP. Обозначаются они следующим образом, нумерованные списки доступа:

- Стандартные: *от 1 до 99*
- Расширенные: *от 100 до 199*

Символьные ACL разделяются тоже на стандартные и расширенные. Расширенные напомню могут проверять гораздо больше, нежели стандартные, но и работают они медленнее, так как придется заглядывать внутрь пакета, в отличии от стандартных где мы смотрим только поле Source Address (Адрес отправителя). При создании ACL каждая запись списка доступа обозначается порядковым номером, по умолчанию в рамках десяти (10, 20, 30 и т.д). Благодаря чему, можно удалить конкретную запись и на её место вставить другую, но эта возможность появилась в Cisco IOS 12.3, до 12.3 приходилось ACL удалять, а потом создать заново полностью. **Нельзя разместить более 1 списка доступа на интерфейс, на протокол, на направление**. Объясняю: если у нас есть маршрутизатор и у него есть интерфейс, мы можем на входящее направление для IP-протокола разместить только один список доступа, например под номером 10. Ещё одно правило, касающееся самих маршрутизаторов, **ACL не действует трафик, сгенерированный самим маршрутизатором**.

Для фильтрации адресов в ACL используется WildCard-маска. Это обратная маска. Берем шаблонное выражение: 255.255.255.255 и отнимаем от шаблона обычную маску.
255.255.255.255-255.255.255.0, у нас получается маска 0.0.0.255, что является копией обычной маски 255.255.255.0 только 0.0.0.255
является WildCard маской.

Виды ACL

Динамический (Dynamic ACL)

Позволяет сделать следующее, например у вас есть маршрутизатор, который подключен к какому-то серверу и нам нужно закрыть доступ к нему из внешнего мира, но в тоже время есть несколько человек, которые могут подключаться к серверу.
Мы настраиваем динамический список доступа, прикрепляем его на входящем направлении, а дальше людям, которым нужно подключиться, подключаться через Telnet к данному устройству, в результате динамический ACL открывает проход к серверу, и уже человек может зайтискажем

через HTTP попасть на сервер. По умолчанию через 10 минут этот проход закрывается и пользователь вынужден ещё раз выполнитьTelnet чтобы подключиться к устройству.

Рефлексивный (Reflexive ACL)

Здесь ситуация немножко отличается, когда узел в локальной сети отправляет TCP запрос в Интернет, у нас должен быть открытый проход, чтобы пришел TCP ответ для установки соединения. Если прохода не будет — мы не сможем установить соединение, и вот этим проходом могут воспользоваться злоумышленники, например проникнуть в сеть. Рефлексивные ACL работают таким образом, блокируется полностью доступ (deny any) но формируется ещё один специальный ACL, который может читать параметры пользовательских сессий, которыесгенерированны из локальной сети и для них открывать проход в deny any, в результате получается что из Интернета не смогут установить соединение. А на сессии сгенерированны из локальной сети будут приходить ответы.

Ограничение по времени (Time-based ACL)

Обычный ACL, но с ограничением по времени, вы можете ввести специальное расписание, которое активирует ту или иную запись списка доступа. И сделать такой фокус, например пишем список доступа, в котором запрещаем HTTP-доступ в течении рабочего дня и вешаем его на интерфейс маршрутизатора, то есть, сотрудники предприятия пришли на работу, им закрывается HTTP-доступ, рабочий день закончился, HTTP-доступ открывается, пожалуйста, если хотите — сидите в Интернете.

Настройка

Сами ACL создаются отдельно, то есть это просто некий список, который создается в глобальном конфиге, потом он присваивается к интерфейсу и только тогда он и начинает работать. Необходимо помнить некоторые моменты, для того, чтобы правильно настроить списки доступа:

- Обработка ведется строго в том порядке, в котором записаны условия
- Если пакет совпал с условием, дальше он не обрабатывается
- В конце каждого списка доступа стоит неявный deny any (запретить всё)
- ACL необходимо размещать как можно ближе к источнику
- Нельзя разместить более 1 списка доступа на интерфейс, на протокол, на направление
- ACL не действует трафик, сгенерированный самим маршрутизатором
- Для фильтрации адресов используется WildCard маска

Стандартный список доступа

```
Router(config)#access-list <номер списка от 1 до
99> {permit | deny | remark} {address | any | host} [source-wildcard][log]
```

- permit: *разрешить*
- deny: *запретить*
- remark: *комментарий о списке доступа*
- address: *запрещаем или разрешаем сеть*
- any: *разрешаем или запрещаем всё*
- host: *разрешаем или запрещаем хосту*
- source-wildcard: *WildCard маска сети*
- log: *включаем логгирование пакеты проходящие через данную запись ACL*

Расширенный список доступа

```
Router(config)#access-list <номер списка от 100 до
199> {permit | deny | remark} protocol source [source-wildcard]
[operator operand] [port <порт или название протокола> [established]
```

- protocol source: *какой протокол будем разрешать или закрывать (ICMP, TCP, UDP, IP, OSPF и т.д)*
- deny: *запретить*
- operator:
  A.B.C.D — адрес получателя
  any — любой конечный хост
  eq — только пакеты на этом порте
  gt — только пакеты с большим номером порта
  host — единственный конечный хост
  lt — только пакеты с более низким номером порта
  neq — только пакеты не на данном номере порта
  range — диапазон портов
- port: *номер порта (TCP или UDP), можно указать имя*
- established: *разрешаем прохождение TCP-сегментов, которые являются частью уже созданной TCP-сессии*

Конфигурирование списков доступа

Списки доступа либо нумеруются, либо именуются. Использование нумерованных, либо именованных списков доступа определяется их применением (некоторые протоколы требуют использования только нумерованных списков, некоторые - допускают как именованные, так и нумерованные списки).

Если используются нумерованные списки, то номера их должны лежать в определенных диапазонах, в зависимости от области применения списка. Некоторые, наиболее часто применяемые диапазоны приведены ниже:

Протокол	Диапазон номеров
Стандартный список IP	1 to 99
Расширенный список IP	100 to 199
MAC Ethernet address	700 to 799
IPX	800 to 899
Extended IPX	900 to 999
IPX SAP	1000 to 1099

Задачи и правила построения списков доступа для различных протоколов различны, но, в общем, можно выделить два этапа работы с любыми списками доступа. Сначала, необходимо создать список доступа, затем применить его к соответствующему интерфейсу, линии или логической операции, выполняемой роутером.

Создание списков доступа (краткий обзор)

Списки доступа определяют критерии, на соответствие которым проверяется каждый пакет, обрабатываемый роутером в точке списка доступа.

Типичными критериями являются адреса отправителя и получателя пакета, тип протокола. Однако, для каждого конкретного протокола существует свой собственный набор критериев, которые можно задавать в списках доступа.

Каждый критерий в списке доступа записывается отдельной строкой. Список доступа в целом представляет собой набор строк с критериями, имеющих один и тот же номер (или имя).

Запомните, что дополнение списка новыми критериями производится в конец списка. Запомните также, что нет возможности исключить какой-либо критерий из списка. Есть только возможность стереть весь вписок целиком.

Список доступа просматривается от начала до конца в том же порядке, в каком были введены его записи. Если в списке необходимо что-то изменить, весь список придется вводить заново.

Запрещение доступа к хосту. Наш первый пример -- запрещение доступа к хосту с IP-адресом 130.120.110.100. Убедившись, что вы вошли в режим "config", введите следующее выражение:

access-list 101 deny ip 0.0.0.0 255.255.255.255 130.120.110.100 0.0.0.0

Маска со значением 255 для каждого октета адреса отправителя означает, что при фильтрации этот адрес должен быть полностью проигнорирован. И не важно, какой адрес указан в качестве IP-адреса отправителя, -- все равно проверяться он не будет. Маска для адреса получателя, состоящая только из нулей, означает, что этот адрес будет проверен полностью. Если необходимо запретить доступ ко всем узлам сети 130.120.110, вы должны использовать маску 0.0.0.255. В этом случае 255 означает игнорирование последнего октета адреса при проверке пакетов.

Разрешение доступа к хосту только по протоколу HTTP. Давайте разрешим доступ к протокольному порту HTTP хоста и запретим любой другой доступ к хосту. Для этого потребуется написать две строки:

access-list 101 permit tcp 0.0.0.0 255.255.255.255 130.120.110.100 0.0.0.0 eq 80
access-list 101 deny ip 0.0.0.0 255.255.255.255 130.120.110.100 0.0.0.0

Первая строка разрешает проход любого пакета с адресом получателя 130.120.110.100 и с протокольным портом TCP, равным 80. Благодаря второй -- блокируются все IP-пакеты с адресом получателя 130.120.110.100, проход которых не был разрешен первой строкой.

Подвязываем болтающиеся концы

Пакеты, для которых в списке доступа не нашлось соответствующего образца, по умолчанию сбрасываются. Тем не менее, неплохо завершить список записью, запрещающей доступ всем пакетам. Эта запись, указывающая на конец списка, выглядит так:

access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255

Если вы хотите начать список с запрещения прохода отдельных пакетов, а затем разрешить доступ всем остальным, то для выполнения последнего действия нужно использовать такую же запись, но со словом "permit" ("разрешить") вместо слова "deny" ("запретить").

Запретить доступ всем пакетам можно и с помощью выражения

access-list 101 deny ip any any

Смысл его тот же, что и приведенного выше. Последние версии IOS сами преобразуют длинную форму в компактную. При выводе списка доступа на экран номера протокольных портов TCP и UDP могут быть изменены на их текстовое описание. Мы же предпочитаем вводить номера, поскольку такой синтаксис совместим с более ранними версиями системы IOS.

Вводим в действие

После того как список доступа сформирован, его необходимо связать с тем интерфейсом маршрутизатора, на котором вы хотите использовать фильтрацию. Список можно применять к входящим или исходящим пакетам, причем в большинстве случаев допустимы оба варианта. Если список доступа используется для исходящих пакетов, фильтры нужно установить только на одном, выходном, интерфейсе. Это повышает производительность работы маршрутизатора, поскольку список будет просматриваться только при передаче трафика в защищаемую сеть.

После того как список доступа сформирован, его нужно связать с интерфейсом маршрутизатора. Для этого, как и при внесении любого другого изменения в конфигурацию интерфейса, необходимо войти в режим "config" и указать тот интерфейс, для которого вы хотите использовать фильтр. На этом этапе список доступа представляется как "группа" (group).

Для каждого протокола на интерфейс может быть назначен только один список доступа.

Для большинства протоколов можно задать раздельные списки для разных направлений траффика. Если список доступа назначен на входящий через интерфейс траффик, то при получении пакета, ротуер проверяет критерии, заданные в списке. Если пакет разрешен данным списком, то он передается для дальнейшей обработки. Если пакет запрещен, то он отбрасывается.
Если список доступа назначен на выходящий через интерфейс траффик, то после приянтия решения о передаче пакета через данный интерфейс роутер проверяет критерии, заданные в списке. Если пакет разрешен данным списком, то он передается в интерфейс. Если пакет запрещен, то он отбрасывается.

Например, чтобы использовать список доступа номер 101 для входящих пакетов, потребуется команда:

ip access-group 101 in

Список доступа начинает работать сразу же после ее ввода. Для проверки правильности его использования полезно с помощью команды pingпровести непрерывное тестирование связи с хостом, находящимся по другую сторону интерфейса. Рекомендуем сохранить сделанные вами изменения с помощью команд "write memory" и "write network" (если вы дублируете параметры конфигурации на сервере TFTP).

Чтобы посмотреть, какие группы доступа приписаны к конкретным интерфейсам, можно использовать команду "show config". В конце она выведет и все записи списка доступа. Но более удобный способ для получения этой информации -- задействовать команду "show access list". Если в качестве аргумента задать номер списка доступа, то будет выведен только соответствующий список. (Это полезно проделывать при каждом назначении номера для нового списка, чтобы убедиться, что данный номер еще не был использован.) Рассматриваемая команда выдает и статистику о совпадениях для каждой записи списка доступа. Для очистки счетчиков статистики предназначена команда "clear access-list counters", в качестве аргумента здесь также используется номер списка.

Как уже отмечалось выше, нельзя просто вернуться и изменить запись списка доступа, поскольку эти записи обрабатываются точно в том порядке, в каком были первоначально внесены в маршрутизатор. (В системе IOS версии 11.2 можно выборочно удалять строки, но не вставлять их.) Если для загрузки новой конфигурации в маршрутизатор вы используете протокол TFTP, то можете редактировать конфигурационный файл на хосте TFTP и затем загружать уже поправленный вариант. Недостатком подобного подхода

является необходимость согласования времени загрузки нового конфигурационного файла с моментом перезапуска маршрутизатора.

Вносим изменения

Другой подход к внесению изменений в списки -- скопировать список в текстовый редактор и править его там. Перед тем как записать новую версию списка в маршрутизатор, вы сначала должны избавиться от старой версии, иначе новая будет просто дописана к старой. Для удаления записи с параметрами конфигурации на маршрутизаторе фирмы Cisco необходимо ввести ее еще раз, поставив перед ней слово "no" ("нет"). Для удаления всего списка доступа достаточно ввести слово "no" и одну из его записей. В этом случае серьезным недостатком является то, что на некоторое время вы остаетесь без работающего списка доступа. Если вы ошиблись или случайно запретили доступ к хосту или службе, вам придется отключить список до выяснения, что же сделано не так.

Нам кажется, лучшим способом внесения изменений в список доступа будет редактирование старого списка в текстовом редакторе с последующим переименованием его перед припиской к интерфейсу маршрутизатора. Последовательность ваших действий будет следующей:

1. Выведите используемый список доступа на экран с помощью команды "show config" и скопируйте его в текстовый редактор.
2. Измените номер списка доступа и отредактируйте список.
3. Войдите в режим "config" и запишите новый список в маршрутизатор.
4. Определите интерфейс, для которого вы хотите изменить список, а затем свяжите с ним новый список с помощью команды "ip access-group xxx in/out" (вам даже не придется отключать старый список, поскольку это произойдет автоматически при введении в действие нового; на каждом интерфейсе может быть только один список доступа).

При возникновении проблем с новым списком можно перейти к старому, используя команду "ip access-groups xxx in/out" и его номер.

Производительность

Задействуя фильтры списков доступа, вы жертвуете производительностью маршрутизатора. При использовании фильтров не будут работать некоторые средства ее повышения, встроенные в устройства фирмы Cisco. Это может

повысить нагрузку на центральный процессормаршрутизатора. Советуем вам понаблюдать за использованием ресурсов этого процессора (команда "show process CPU") и за числом пакетов, сброшенных на интерфейсе. Технология NetFlow фирмы Cisco поддерживает списки доступа, но ее новая функция скоростной пересылки данных -- нет. Поэтому механизмы фильтрации желательно использовать на маршрутизаторах, установленных на границе сети, и не включать их на магистрали, где передаются значительно большие объемы трафика.

Очевидно, на производительность влияет и размер списка доступа: чем он длиннее, тем больше приходится "трудиться" маршрутизатору при обработке каждого пакета. Этот фактор влияет на производительность в меньшей степени, чем те, о которых говорилось выше, но, тем неменее записи с параметрами наиболее часто встречающихся пакетов постарайтесь расположить в начале списка. Один из способов достижения этого заключается в следующем: разместите в самом начале правило, пропускающее все пакеты уже установленного сеанса TCP или пакеты-подтверждения. В целом, большинство сетевых пакетов -- это пакеты, передаваемые уже после установления сеанса связи. Маловероятно, чтобы такие пакеты были опасны (даже если они подделаны злоумышленником), поэтому их можно свободно пропустить. Попробуйте использовать список доступа с этим правилом и без него, проследив за изменением коэффициента использования ресурсов центрального процессора.

Разрешить проход всех пакетов уже установленных сеансов связи можно с помощью следующей записи:

access-list 101 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 established.

Если вы используете много списков доступа, обратите внимание на продукт Router Management Module фирмы Check Point Software Technologies, поставляемый вместе с ее системой Firewall-1. Он позволит вам из графического интерфейса централизованно управлять конфигурацией списков доступа, расположенных на маршрутизаторах фирм Bay Networks, Cisco и 3Com. Может оказаться полезным и продукт Netsys EnterpriseSolver фирмы Cisco, который поможет обнаружить ошибки в списках доступа и изучить их влияние на работу сети.

Настройка базовой проверки TCP/UDP/ICMP

Воспользуйтесь встроенными функциями брандмауэра, если они есть в версии IOS. Брандмауэр IOS не обеспечивает глубокой инспекции на прикладном уровне, как, например, в брандмауэре ISA Server, но задействовать его стоит по двум причинам. Во-первых, дабы убедиться, что трафик, заявленный как TCP, UDP или ICMP, действительно принадлежит протоколам TCP, UDP или ICMP. Во-вторых, проверка позволяет управлять доступом на основе контекста Context-Based Access Control (CBAC). С помощью CBAC операционная система IOS может создавать динамические записи в списке доступа, разрешая прохождение обратного трафика через маршрутизатор. Приведенные выше списки доступа очень общие (например, разрешен весь трафик TCP), поэтому после того, как будет получена работоспособная конфигурация, наверняка потребуется применить более строгие условия, назначить внутренние серверы, доступные из Internet, и т. д. После того как это будет сделано, CBAC обеспечит прохождение обратного трафика через маршрутизатор. Например, при просмотре Amazon.com CBAC динамически помещает записи в исходящий список доступа, применяемый к внешнему (WAN) интерфейсу, чтобы разрешить поступление в маршрутизаторобратного трафика из Amazon.com. Когда соединение разрывается, эти записи автоматически удаляются.

Обязательно установите порог тайм-аута TCP SYN, чтобы предотвратить flood-атаки SYN с отказом в обслуживании:

ip tcp synwait-time 30

Эта команда указывает IOS на необходимость закрыть любой TCP-сеанс, не установленный в течение 30 секунд.

Затем назначьте отдельные правила проверки для ICMP, TCP и UDP:

ip inspect name InspectRule icmp
ip inspect name InspectRule tcp
ip inspect name InspectRule udp
InspectRule можно заменить другим именем.

Шлюзы сеансового уровня

Данный класс маршрутизаторов представляет собой транслятор TCP-соединения. Шлюз принимает запрос авторизованного клиента на конкретные услуги и после проверки допустимости запрошенного сеанса устанавливает соединение с местом назначения (внешним хостом). После этого шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации. Как правило, пункт назначения задается заранее, в то время

как источников может быть много. Используя различные порты, можно создавать разнообразные конфигурации соединений. Данный тип шлюза позволяет создать транслятор TCP-соединения для любого определенного пользователем сервиса, базирующегося на TCP, осуществлять контроль доступа к этому сервису и сбор статистики по его использованию.

Шлюз следит за подтверждением (квитированием) связи между авторизованным клиентом и внешним хостом, определяя, является ли запрашиваемый сеанс связи допустимым. Чтобы выявить допустимость запроса на сеанс связи, шлюз выполняет следующую процедуру. Когда авторизованный клиент запрашивает некоторый сервис, шлюз принимает этот запрос, проверяя, удовлетворяет ли данный клиент базовым критериям фильтрации. Затем, действуя от имени клиента, шлюз устанавливает соединение с внешним хостом и следит за выполнением процедуры квитирования связи по протоколу TCP. Эта процедура состоит из обмена TCP-пакетами, которые помечаются флагами SYN (синхронизировать) и ACK (подтвердить).

Первый пакет сеанса TCP, помеченный флагом SYN и содержащий произвольное число, например 500, является запросом клиента на открытие сеанса. Внешний хост, получивший этот пакет, посылает в ответ другой, помеченный флагом ACK и содержащий число на единицу большее, чем в принятом пакете (в нашем случае 501), подтверждая тем самым прием пакета SYN от клиента.

Далее осуществляется обратная процедура: хост посылает клиенту пакет SYN с исходным числом, например 700, а клиент подтверждает его получение передачей пакета ACK, содержащего число 701. На этом процесс квитирования связи завершается.

Шлюз сеансового уровня признает завершенное соединение допустимым только в том случае, если при выполнении процедуры квитирования связи флаги SYN и ACK, а также числа, содержащиеся в TCP-пакетах, оказываются логически связанными между собой.

После того как шлюз определил, что доверенный клиент и внешний хост являются авторизованными участниками сеанса TCP, и проверил его допустимость, он устанавливает соединение. Начиная с этого момента шлюз копирует и перенаправляет пакеты туда и обратно, не проводя никакой фильтрации. Он поддерживает таблицу установленных соединений, пропуская данные, которые относятся к одному из сеансов связи, зафиксированных в данной таблице. Когда сеанс завершается, шлюз удаляет соответствующий элемент из таблицы и разрывает сеть, использовавшуюся в текущем сеансе.

Недостатком шлюзов сеансового уровня является отсутствие проверки содержимого передаваемых пакетов, что дает возможность нарушителю проникнуть через такой шлюз.

Программно-аппаратные средства обеспечения информационной безопасности

◄ Предыдущий элемент курса

Перейти на...

Следующий элемент курса ►

Обновить Ресурс

VPN, или Virtual Private Network, что в переводе означает Виртуальная Частная Сеть - это криптосистема, позволяющая защитить данные при передаче их по незащищенной сети, такой, как Интернет. Несмотря на то, что данное описание подходит и для криптосистемы SSH, VPN имеет другое предназначение. SSH разрабатывался как средство, позволяющее пользователю безопасно зайти и удаленно управлять другим компьютером. Цель VPN - прозрачный доступ к ресурсам сети, где пользователь может делать все то, что он делает обычно независимо от того, насколько он удален. По этой причине VPN приобрел популярность среди дистанционных работников и офисов, которые нуждаются в совместном использовании ресурсов территориально разделенных сетей.

VPN-туннели

Прежде чем приступить к настройке VPN, необходимо познакомится с общепринятой терминологией и с некоторыми проблемами настройки. Начнем с терминологии. VPN соединение всегда состоит из канала типа точка-точка, также известного под названием туннель. Туннель создается в незащищенной сети, в качестве которой чаще всего выступает Интернет. Соединение точка-точка подразумевает, что оно всегда устанавливается между двумя компьютерами, которые называются узлами или peers. Каждый peer отвечает за шифрование данных до того, как они попадут в туннель и расшифровку этих данных после того, как они туннель покинут.

Хотя VPN-туннель всегда устанавливается между двумя точками, каждый peer может устанавливать дополнительные туннели с другими узлами. Для примера, когда трем удаленным станциям необходимо связаться с одним и тем же офисом, будет создано три отдельных VPN-туннеля к этому офису. Для всех туннелей peer на стороне офиса может быть одним и тем же. Это возможно благодаря тому, что узел может шифровать и расшифровывать данные от имени всей сети, как это показано на рисунке 1:

Рисунок 1. VPN-шлюз к сети.

В этом случае VPN-узел называется VPN-шлюзом, а сеть за ним - доменом шифрования (encryption domain). Использование шлюзов удобно по нескольким причинам. Во-первых, все пользователи должны пройти через одно устройство, которое облегчает задачу управления политикой безопасности и контроля входящего и исходящего трафика сети. Во-вторых, персональные туннели к каждой рабочей станции, к которой пользователю надо получить доступ, очень быстро станут неуправляемыми (так как туннель - это канал типа точка-точка). При наличии шлюза, пользователь устанавливает соединение с ним, после чего пользователю открывается доступ к сети (домену шифрования).

Интересно отметить, что внутри домена шифрования самого шифрования не происходит. Причина в том, что эта часть сети считается безопасной и находящейся под непосредственным контролем в противоположность Интернет. Это справедливо и при соединении офисов с помощью VPN-

шлюзов. Таким образом гарантируется шифрование только той информации, которая передается по небезопасному каналу между офисами. Рисунок 2 показывает VPN, соединяющую два офиса.

Рисунок 2. Защищенная сеть на основе незащищенной сети.

Сеть А считается доменом шифрования VPN-шлюза А, а сеть В - доменом шифрования VPN-шлюза В, соответственно. Когда пользователь сети А изъявляет желание отправить данные в сеть В, VPN шлюз А зашифрует их и отошлет через VPN-туннель. VPN шлюз В расшифрует информацию и передаст получателю в сети В.
Всякий раз, когда соединение сетей обслуживают два VPN-шлюза, они используют режим туннеля. Это означает, что шифруется весь пакет IP, после чего к нему добавляется новый IP-заголовок. Новый заголовок содержит IP-адреса двух VPN-шлюзов, которые и увидит пакетный сниффер при перехвате. Невозможно определить компьютер-источник в первом домене шифрования и компьютер-получатель во втором домене.

Посмотрите на рисунок 1, иллюстрирующий типичное использование VPN, которая позволяет удаленным пользователям с переносыми компьютерами и пользователям, работающим из дома, иметь доступ к офисной сети. Чтобы эта схема заработала, пользователь должен иметь установленное ПО – VPN- клиент, который обеспечит создание VPN-туннеля к удаленному VPN-шлюзу. По сценарию используется режим туннеля, так как пользователь хочет получить доступ к ресурсам домена, а не самого шлюза. Единственной случай, когда включается режим транспорта - это если одному компьютеру нужно получить доступ к другому непосредственно.
Существует много вариантов VPN-шлюзов и VPN-клиентов. Это может быть аппаратное устройство или программное обеспечение, которое устанавливается на маршрутизаторах или на ПК. Скажем, ОС FreeBSD поставляется вместе с ПО для создания VPN-шлюза и для настройки VPN-клиента. Свои VPN-решения существуют и для ПО компании Microsoft.
К счастью, в Интернет есть много источников информации о VPN, технические статьи, FAQ и варианты настроек. Я могу порекомендоватьTina Bird's VPN Information, VPN Labs, и Virtual Private Network Consortium (VPNC).

Назависимо от используемого ПО, все VPN работают по следующим принципам:
1. Каждый из узлов идентифицирует друг друга перед созданием туннеля, чтобы удостовериться, что шифрованные данные будут отправлены на нужный узел.
2. Оба узла требуют заранее настроеной политики, указывающей, какие протоколы могут

использоваться для шифрования и обеспечения целостности данных.
3. Узлы сверяют политики, чтобы договориться об используемых алгоритмах; если это не получается, то туннель не устанавливается.
4. Как только достигнуто соглашение по алгоритмам, создается ключ, который будет использован в симметричном алгоритме для шифрования/расшифровки данных.
Есть несколько стандартов, регламентирующих вышеописанное взаимодействие. Вы, должно быть, слышали о некоторых из них: L2TP, PPTP, и IPSec. Так как IPSec - наиболее широко поддерживаемый стандарт, оставшуюся часть статьи стоит посвятить именно ему.

IPSec

Стандарт IPSec был разработан для повышения безопасности IP-протокола. Это достигается за счет дополнительных протоколов, добавляющих к IP- пакету собственные заголовки. Т.к. IPSec - стандарт Интернет, то для него существуют RFC (Requests For Comments). Если есть интерес покопаться во внутренностях IPSec, то следующие RFC могут оказаться полезными:
- RFC 2401 IPSec;
- RFC 2402 AH;
- RFC 2406 ESP;
- RFC 2409 IKE.
Приведем краткое описание каждого дополнительного протокола. Начнем с сокращений, а затем посмотрим, как они укладываются в общую картину создания виртуальной частной сети.

AH (Authentication Header) - протокол заголовка идентификации. Обеспечивает целостность путем проверки того, что ни один бит в защищаемой части пакета не был изменен во время передачи. Не будем вдаваться в подробности, какая часть пакета защищается и где находятся данные AH-заголовка, так как это зависит от используемого типа шифрования и в деталях, с диаграммами описывается в соответствующем RFC. Отметим лишь, что использование AH может вызвать проблемы, например, при прохождении пакета через NAT-устройство. NAT меняет IP-адрес пакета, чтобы, например, разрешить доступ в Интернет с закрытого локального адреса. Так как пакет в таком случае изменится, контрольная сумма AH станет неверной. Также стоит отметить, что AH разрабатывался только для обеспечения целостности. Он не гарантирует конфиденциальности путем шифрования содержимого пакета.

ESP (Encapsulating Security Protocol) - инкапсулирующий протокол безопасности, который обеспечивает и целостность и конфиденциальность. В режиме транспорта ESP-заголовок находится между оригинальным IP-заголовком и заголовком TCP или UDP. В режиме туннеля заголовок ESP размещается между новым IP-заголовком и полностью зашифрованным оригинальным IP-пакетом.

Так как оба протокола - AH и ESP - добавляют собственные заголовки, они имеют свой ID протокола, по которому можно определить, что последует за заголовком IP. Каждый тип заголовка имеет собственный номер. Например, для TCP это 6, а для UDP - 17. При работе через firewall важно не забыть настроить фильтры, чтобы пропускать пакеты с ID AH-и/или ESP-протокола. Для AH номер ID - 51, а ESP имеет ID протокола равный 50. При создании правила не перепутайте случайно ID протокола с номером порта.

Третий протокол, используемый IPSec - это IKE или Internet Key Exchange protocol. Как следует из названия, он предназначен для обмена ключами между двумя узлами VPN. Насмотря на то, что генерировать ключи можно вручную, лучшим и более масштабируемым вариантом будет автоматизация этого процесса с помощью IKE. Помните, что ключи должны часто меняться, и вам наверняка не хочется полагаться на свою память, чтобы найти время для совершения этой операции вручную. Главное - не забудьте настроить правило на файрволе для UDP-порта с номером 500, так как именно этот порт используется IKE.

SA (Security Association), что можно приближенно перевести как "связь или ассоциация безопасности" - это термин IPSec для обозначения соединения. При настроенном VPN, для каждого используемого протокола создается одна SA-пара (то есть одна для AH и одна для ESP). SA создаются парами, так как каждая SA - это однонаправленное соединение, а данные необходимо передавать в двух направлениях. Полученные SA-пары хранятся на каждом узле. Если ваш узел имеет SA, значит VPN-туннель был установлен успешно.

Так как каждый узел способен устанавливать несколько туннелей с другими узлами, каждый SA имеет уникальный номер, позволяющий определить, к какому узлу он относится. Это номер называется SPI (Security Parameter Index) или индекс параметра безопасности.
SA хранятся в базе данных с названием - кто бы подумал ;) - SAD (Security Association Database) или БД ассоциаций безопасности.
Каждый узел IPSec также имеет вторую БД - SPD или Security Policy Database (БД политики безопасности). Она содержит настроенную вами политику узла. Большинство VPN-решений разрешают создание нескольких политик с комбинациями подходящих алгоритмов для каждого узла, с которым нужно установить соединение.

Программно-аппаратные средства обеспечения информационной безопасности

Вы здесь

Обновить Ресурс

Проблема остаточной информации на жестких дисках. Уровни программного уничтожения остаточной информации с жестких дисков. Алгоритмы программного удаления остаточной информации. Достоинства и недостатки программного удаления остаточной информации. Программное обеспечение для уничтожения остаточной информации с жестких дисков.

Рассмотрим проблему. При удалении файлового объекта (либо при записи в объект информации меньшего объема, чем объем располагаемой в нем информации – при модификации файлового объекта) штатными средствами ОС (в том числи и ОС семейства Windows) собственно информация на диске остается (не удаляется) – осуществляется лишь переразметка файловых объектов. Данная информация называется остаточной. Поэтому имеет место угроза получения прямого доступа к диску (заметим, не к файловому объекту, которого уже на диске не существует) - к остаточной информации на диске, что является функцией некоторых утилит. Почему мы говорим, что это дополнительная задача СЗИ? Дело в том, что любая СЗИ – это комплекс механизмов защиты, поэтому частично задача защиты здесь может осуществляться иными механизмами. В частности, если в СЗИ НСД присутствует механизм обеспечения замкнутости программной среды (о котором мы подробно рассказывали в одной из

предыдущих частей работы), то можно настроить систему защиты таким образом, чтобы запустить утилиту, функцией которой является реализация прямого доступа к диску, стало бы невозможным. Причем это является задачей, которая должна решаться в любом случае, не только с целью противодействия доступу к остаточной информации, т.к. средствами прямого доступа к диску можно обратиться и к актуальной информации, расположенной на диске в обход механизмов контроля доступа к файловым объектам (к файловом объекту при этом обращения нет). Однако остается проблема внешних носителей (например, дискета, Flash-устройство и т.д). Задумайтесь, какая информация остается на внешнем носителе, используемом на вашем предприятии, после удаления на нем файлового объекта штатными средствами ОС?

Заметим, что требование к гарантированной очистке остаточной информации, ввиду чрезвычайной важности данного механизма защиты, устанавливается и соответствующим нормативным документом [1], которое, в частности, для СВТ 5 класса защищенности сформулировано следующим образом: при первоначальном назначении или при перераспределении внешней памяти КСЗ должен предотвращать доступ субъекту к остаточной информации.

Заметим, что ОС семейства Windows (естественно технологии NT) обеспечивают лишь очистку (запись "0") в выделяемую системой область памяти на диске, при создании файла, с последующим размещением файла в этой области, т.е. ни о какой гарантированной очистке остаточной информации (при удалении, либо при модификации файла) здесь говорить не приходится.

Алгоритмы уничтожения информации — последовательность операций, предназначенных для осуществления необратимого программными и (или) аппаратными средствами удаления данных, в том числе остаточной информации.

Как правило, данные алгоритмы используются государственными учреждениями, специализированными структурами и предприятиями в целях сохранения государственной и коммерческой тайны. В настоящее время всем желающим сохранить удалённую информацию в тайне доступно программные средства безопасного удаления (уничтожения) информации, в том числе и программы с открытым исходным кодом.

Алгоритмы уничтожения информации используются так же в средствах программного шифрования информации для безопасного удаления временных файлов и уничтожения исходных, поскольку в противном случае, используя классическое удаление, существует возможность восстановления исходного файла лицом, желающим получить доступ к личной либо секретной информации.

Алгоритмы уничтожения информации на данный момент стандартизированы, практически во всех ведущих государствах изданы национальные стандарты, нормы и правила, регламентирующие использование программного уничтожения информации и описывающие механизм его реализации.

Все программные реализации алгоритмов уничтожения информации основаны на простейших операциях записи, тем самым происходит многократная перезапись информации в секторах жесткого диска ложными данными. В зависимости от алгоритма это может быть случайное число генератора псевдослучайных чисел либо фиксированное значение. Как правило, каждый алгоритм предусматривает запись восьми битовых единиц (#FF) и нуля (#00). В существующих алгоритмах перезапись может производиться от одного до 35 и более раз. Существуют реализации с возможностью произвольного выбора числа циклов перезаписи.

Теоретически, простейшим методом уничтожении исходного файла является его полная перезапись байтом #FF, то есть битовой маской из восьми логических единиц (11111111), нулей либо произвольных чисел, тем самым исключив его программное восстановление стандартными средствами, доступными пользователю. Однако с использованием специализированных аппаратных средств, анализирующих поверхность магнитных носителей и позволяющих восстановить исходную информацию исходя из показателей остаточной намагниченности, существует вероятность, что простейшая перезапись не гарантирует полноценное уничтожение.

С целью исключения возможности восстановления и разработаны существующие алгоритмы уничтожения информации.

Наиболее известен и распространён алгоритм, применяемый в американском национальном стандарте Министерства обороны DoD5220.22-M. Вариант E согласно данному стандарту предусматривает два цикла записи псевдослучайных чисел и один — фиксированных значений, зависимых от значений первого цикла, четвёртый цикл — верификация записей. В варианте ECE перезапись данных производится 7 раз — 3 раза байтом #FF, три #00 и один #F6.[1]

В алгоритме Брюса Шнайра в первом цикле записывается #FF, во втором — #00 и в пяти циклах — псевдослучайные числа. Считается одним из наиболее эффективных.

В наиболее медленном, но, по мнению множества экспертов, наиболее эффективном алгоритме Питера Гутмана, существует 35 циклов, в которых записывают все наиболее эффективные битовые маски, данный алгоритм основан на его теории уничтожения информации.

В алгоритме, предусмотренного американским национальным стандартом NAVSO P-5239-26 для MFM-кодируемых устройств в первом цикле записывается #01, во втором — #7FFFFF, в третьем — последовательность псевдослучайных чисел, в четвёртом проходит верификация. В

варианте для RLL — кодируемых устройств данного алгоритма во втором цикле записывается #27FFFFFF

В алгоритме, который описывает германский национальный стандарт VSITR с первого по шестой цикл записываются последовательно байты #00 и #FF, в седьмом #AA.

Существует мнение о существовании алгоритма, описанного Российским национальным стандартом ГОСТ Р 50739-95, предусматривающего запись #00 в каждый байт каждого сектора для систем с 4-6 класса защиты и запись псевдослучайных чисел в каждый байт каждого сектора для систем 1-3 класса защиты[3]. Однако данный стандарт содержит лишь формулировку «Очистка должна производиться путём записи маскирующей информации в память при ее освобождении перераспределении», которая не содержит какой-либо детализации относительно порядка перезаписи, количества циклов и битовых масок[4]. В то же время, существует действующий Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», изданный в 1992 году и предусматривающий ряд требований к механизму уничтожения информации для систем определённых классов защищенности. В частности, для классов 3А и 2А «Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов)», для класса 1Г предусмотрена однократная перезапись.[5]

В алгоритме Парагона первый цикл заключается в перезаписи уникальными 512-битными блоками, используя криптографическибезопасный генератор случайных чисел, затем, во втором цикле каждый перезаписываемый блок переписывается своим двоичным дополнением, третий цикл повторяет первый цикл с новыми уникальными случайными блокам, в четвёртом цикле происходит перезапись байтом #AA. Завершается уничтожение информации циклом верификации.

Как правило, для затруднения программного восстановления информации, перезапись информации в отдельном файле согласно алгоритму уничтожения сопровождается установкой нулевого размера файла и его переименованием, используя произвольный набор символов. Затем следует удаление файла из таблицы размещения файлов.

Классификация алгоритмов шифрования

- Симметричные (с секретным, единым ключом, одноключевые, single-key).
    - Потоковые (шифрование потока данных):
        - с одноразовым или бесконечным ключом (infinite-key cipher);
        - с конечным ключом (система Вернама - Vernam);
        - на основе генератора псевдослучайных чисел (ПСЧ).
    - Блочные (шифрование данных поблочно):
        - Шифры перестановки (permutation, P-блоки);
        - Шифры замены (подстановки, substitution, S-блоки):
        - моноалфавитные (код Цезаря);
        - полиалфавитные (шифр Видженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma);
    - Составные:
        - Lucipher (фирма IBM, США);
        - DES (Data Encryption Standard, США);
        - FEAL-1 (Fast Enciphering Algoritm, Япония);
        - IDEA/IPES (International Data Encryption Algorithm/
        - Improved Proposed Encryption Standard, фирма Ascom-Tech AG, Швейцария);
        - B-Crypt (фирма British Telecom, Великобритания);
        - ГОСТ 28147-89 (СССР); * Skipjack (США).
- Асимметричные (с открытым ключом, public-key):

- Диффи-Хеллман DH (Diffie, Hellman);
- Райвест-Шамир-Адлеман RSA (Rivest, Shamir, Adleman);
- Эль-Гамаль ElGamal.

Кроме того, есть разделение алгоритмов шифрования на собственно шифры (ciphers) и коды (codes). Шифры работают с отдельными битами, буквами, символами. Коды оперируют лингвистическими элементами (слоги, слова, фразы).

Криптопровайдер (CSP, Cryptographic Service Provider) — независимый программный модуль, интегрированный в MS Windows и содержащий библиотеку криптографических функций со стандартизованным интерфейсом. CSP выполняет следующие криптографические функции:

- формирование/проверка электронной цифровой подписи (ЭЦП),
- шифрование информации,
- хранение ключей всех типов.

Криптопровайдер предназначен для авторизации, обеспечения конфиденциальности и юридической значимости электронных документов при обмене ими между пользователями, контроля целостности информации и др.

В составе ОС Windows пользователь получает несколько CSP, которые реализуют наиболее часто используемые методы шифрования. Наряду со стандартными криптопровайдерами, поставляемыми Microsoft, можно использовать CSP собственной разработки, предварительно сертифицировав его.

Цифровые подписи относятся к криптографическим алгоритмам с открытым ключом, но с измененными ролями открытого и закрытого ключей. Отправитель может зашифровать и подписать сообщение своим закрым ключом. Когда сообщение получено, получатель может дешифровать его, используя открытый ключ отправителя. Ввиду того, что отправитель — это единственное лицо, обладающее доступом к закрытому ключу, то получатель достаточно точно знает, от кого получено сообщение, а также может быть уверен, что сообщение не было изменено.

Цифровые подписи могут оказаться весьма полезными. Они гарантируют получателю, что сообщение не подделано, а также не позволяют отправителю отказаться от обязательств, отрицая факт отправки сообщения.

Важно заметить, что хотя сообщения шифруются, их может прочитать любой обладатель открытого ключа. Несмотря на то что используются те же методы и ключи, в данном случае назначением шифрования является не запретить чтение, а предотвратить подделку и отказ от обязательств.

Поскольку алгоритмы с открытым ключом работают достаточно медленно с большими сообщениями, для повышения производительности обычно используется алгоритм другого типа, называемый хеш-функцией.

Хеш-функция вычисляет дайджест, или хеш-значение, для каждого указанного сообщения. Совершенно не важно, какое значение генерирует алгоритм. Важно, что результат этой функции является детермированным, то есть результат будет одним и тем же каждый раз, когда на вход передаются одни и те же данные. Кроме того, важно, что результат имеет небольшой размер, и алгоритм быстро работает.

Наиболее известные хеш-функции — это MD5 и SHA.

Хеш-функция генерирует дайджест, соответствующий определенному сообщению. Располагая сообщением и его дайджестом, можно убедиться, не подделывалось ли сообщение, но только в том случае, если дайджест не был подделан вместе с ним.

И, наконец, обычный способ создания цифровой подписи — это создание с помощью быстрой хеш-функции дайджеста для всего сообщения, а затем шифрование только короткого дайджеста с использованием медленного алгоритма с открытым ключом. Теперь подпись можно отправить вместе с сообщением по любому обычному, незащищенному каналу связи.

После получения можно проверить подлинность подписания сообщения. Подпись дешифруется с помощью открытого ключа отправителю. Хеш-значение для сообщения генерируется с помощью того же метода, который использовал отправитель. Если дешифрованноехеш-значение совпадает со сгенерированным значением, значит, сообщение действительно прислано отправителем и при пересылке не изменялось.

Цифровые сертификаты

Хорошо бы иметь возможность проверять, что сообщение не было изменено, а вся последовательность сообщений поступила от определенного компьютера или пользователя. Для коммерческих взаимодействий еще лучше было бы иметь возможность связать пользователя или сервер с каким-либо реальным правовым понятием, таким как физическое или юридическое лицо.

Цифровой сертификат объединяет в цифровой подписанной форме открытый ключ и подробную информацию о человеке или организации. Получив сертификат, вы получаете открытый ключ другой стороны для отправки ей, при необходимости, зашифрованных сообщений. Кроме того, цифровой сертификат содержит подробную информацию о другой стороне, которая заведомо не подвергалась изменениям.

В данном случае проблема состоит в том, что информация из сертификата заслуживает ровно столько доверия, сколько и подписавший его человек. Любой человек может создать и подписать сертификат, в котором будет утверждаться все, что угодно. Для коммерческих транзакций полезно наличие третьей, заслуживающей доверия стороны, которая будет проверять подлинность участников и сведений, записанной в их сертификатах.

Такие третьи стороны называются центрами сертификации. Центры сертификации выдают цифровые сертификаты отдельным лицам и компаниям, которые должны для этого пройти проверку на подлинность.

Из всех центров сертификации наиболее известными являются VeriSing (http://www.verising.com)и Thawte (http://www.thawte.com). VeriSingи Thawte являются собственностью одной компании, поэтому существенной разницы между их сертификатами нет. Сертификаты некоторых из менее известных центров сертификации, таких как Equifax Secure (http://www.equifaxsecure.com)стоят значительно дешевле.

Центры сертификации подписывают сертификаты, подтверждая, что им были представлены доказательства подлинности лица или компании. Важно заметить, что сертификат не является справкой или официальным подтверждением платежеспособности. Он не гарантирует, что вы имеете дело с кем-то, обладающим хорошей репутацией. Сертификаты гарантируют то, что если вас ограбят, то у вас будет шанс найти реальный физический адрес того, кого можно будет привлечь к суду.

Сертификаты позволяют создать сеть доверия. Предположим, вы решили доверить центру сертификации. Тогда вы можете решить доверять людям и компаниям, которым доверяет выбранный центр сертификации. Далее можно решить доверять всем лицам и организациям, которым доверяе владелец сертификата.

Цифровые сертификаты чаще всего используются с целью поддержки атмосферы респектабельности на сайте электронной коммерции. При наличии сертификата, выданного хорошо известным центром сертификации, веб-браузер может установить SSL-соединение с сайтом, не выводя при этом никаких предупреждающих диалоговых окон. Веб-серверы, которые поддерживают SSL-соединения, часто называютбезопастными веб-серверами.

Электронные ключи

Хранение секретных ключей в тайне является главным требованием при эксплуатации системы электронной цифровой подписи. Одним из эффективных способов хранения секретных ключей является использование отчуждаемых носителей.

Отчуждаемые носители - это портативные устройства, выполненные в форме USB-брелка или смарт-карты, обеспечивающие хранение конфиденциальной ключевой информации и аутентификацию пользователя.

Наиболее функциональным, перспективным, удобным и эргономичным носителем ключевой информации в настоящее время считается USB брелок.

Для получения доступа к защищённым на компьютере и в сети данным он не требует никаких дополнительных устройств считывания информации и подключается к компьютеру через usb-порт. USB-брелки удобно и просто использовать. Нужно всего лишь вставить идентификатор в USB-порт, а затем набрать на клавиатуре PIN-код. USB-брелок удобно носить на связке ключей

Современное программно-аппаратное обеспечение для работы с системами шифрования и ЭЦП.

- Криптон-Шифрование
- Криптон-подпись
- КриптоПро CSP

50. Назначение и основные возможности использования защищенных виртуальных дисков. Создание и использование защищенных виртуальных дисков: реализация двухфакторной аутентификации, используемые средства шифрования, управление сертификатами и ключами.

Программно-аппаратный комплекс *Secret Disk NG* защищает конфиденциальную информацию на персональном компьютере. С его помощью вы можете создавать на рабочей станции так называемые защищённые диски (*секретные диски*) – диски с зашифрованным содержимым, работать с которыми можете только вы и ваши доверенные лица. Любой другой пользователь, пусть даже наделённый административными полномочиями на данном компьютере, не может получить доступ к защищённым дискам.

Защита конфиденциальной информации обеспечивается шифрованием данных «на лету» с помощью надежных алгоритмов шифрования. При чтении данных с защищенного диска происходит их расшифрование, при записи на диск — зашифрование. Находящиеся на защищенном диске данные всегда зашифрованы.

Secret Disk NG позволяет превращать существующие диски, в том числе съёмные, в защищённые тома, а также создавать так называемые защищённые виртуальные диски. Всё содержимое защищённого виртуального диска хранится в одном файле в зашифрованном виде. Подключенный защищённый виртуальный диск операционная система воспринимает как обычный диск. Удаление файла подключенного защищённого виртуального диска невозможно.

Управление *Secret Disk NG* тесно интегрировано с операционной системой Windows 2000/XP и предоставляет возможность удаленного администрирования защищенных дисков. Непосредственная работа с защищенными дисками предполагается только с локального компьютера.

Для доступа к защищённым дискам используется персональный USB-ключ или смарт-карта *eToken*. По умолчанию работа с защищёнными дисками возможна только при наличии *eToken*. Если вы отключаете *eToken*, то все защищённые диски автоматически становятся недоступными. Отключенные защищённые тома операционная система воспринимает как неформатированные.

Подключив eToken и указав сертификат, вы вводите PIN-код, подтверждая тем самым владение соответствующим закрытым ключом. Таким образом, аутентификация пользователя в Secret Disk NG 3.1.2 основана на двух факторах:

1. владение *eToken*;
2. знание PIN-кода.

В *Secret Disk NG* наборы операций, которые можно совершать над тем или иным диском, различаются у разных пользователей. У защищённого диска может быть только один владелец. Другие пользователи *Secret Disk NG* на данном компьютере не могут форматировать,перешифровывать этот защищённый диск и выполнять ряд других операций. Более того, подключать защищённый диск могут не все пользователи *Secret Disk NG*, а только те, кому владелец предоставил соответствующие права.

Режим работы *Secret Disk NG*, при котором один из пользователей может реализовывать свои полномочия для подключения и отключения защищённых дисков, зашифрования, перешифрования, расшифрования, выполнения операций с резервными копиями мастер-ключей и настройки параметров работы *Secret Disk NG*, называется сеансом данного пользователя.

Утилита *eToken Properties*, устанавливаемая вместе с *eToken RTE*, служит для настройки параметров *eToken* и его драйверов, просмотра общей информации относительно *eToken*, хранящихся в памяти *eToken* сертификатов и ключевых контейнеров RSA, а также удаления просматриваемых сертификатов вместе с соответствующими закрытыми ключами.

Программно-аппаратные средства обеспечения информационной безопасности

Концепция "авторитетных рекомендаций" представляет собой набор указаний, которые обеспечивают должный уровень безопасности. Авторитетные рекомендации (далее - рекомендации) - это комбинация указаний, эффективность которых доказана при применении в самых различных организациях. Не все указания пригодны для использования в конкретной организации. В некоторых компаниях необходимы дополнительные политики и процедуры, обучение персонала или контроль за технической безопасностью для достижения приемлемого уровня управления безопасностью.

Административная безопасность

Рекомендации по административной безопасности - это те решения, которые соответствуют политикам и процедурам, ресурсам, степени ответственности, потребностям в обучении персонала и планам по выходу из критических ситуаций. Эти меры призваны определить важность информации и информационных систем для компании и объяснить персоналу, в чем именно заключается эта важность. Рекомендации по обеспечению административной безопасности определяют ресурсы,

необходимые для осуществления должного управления рисками и определения лиц, несущих ответственность за управление безопасностью организации.

Политики и процедуры

Политики безопасности определяют метод, согласно которому обеспечивается безопасность внутри организации. После определения политики предполагается, что большинство сотрудников компании будут ее соблюдать. Следует понимать, что полного и безоговорочного выполнения политики не будет. В некоторых случаях политика будет нарушаться из-за требований, связанных с деловой деятельностью организации. В других случаях игнорирование политики обусловлено сложностью ее выполнения.

Даже принимая во внимание тот факт, что политика будет выполняться не постоянно, она формирует ключевой компонент программы по обеспечению безопасности и должна быть включена в перечень рекомендаций по защите. При отсутствии политики сотрудники не будут знать, что делать для защиты информации и компьютерных систем.

В качестве рекомендаций по безопасности необходимо рассматривать следующие политики.

- Информационная политика. Определяет степень секретности информации внутри организации и необходимые требования к хранению, передаче, пометке и управлению этой информацией.
- Политика безопасности. Определяет технические средства управления и настройки безопасности, применяемые пользователями и администраторами на всех компьютерных системах.
- Политика использования. Определяет допустимый уровень использования компьютерных систем организации и штрафные санкции, предусмотренные за их нецелевое использование. Данная политика также определяет принятый в организации метод установки программного обеспечения и известна как политика приемлемого использования.
- Политика резервного копирования. Определяет периодичность резервного копирования данных и требования к перемещению резервных данных в отдельное хранилище. Кроме того, политики резервного копирования определяют время, в течение которого данные должны быть зарезервированы перед повторным использованием.

Политики сами по себе не формируют исчерпывающих инструкций по выполнению программы безопасности организации. Следует определить процедуры, согласно которым сотрудники будут выполнять определенные задачи, и которые будут определять дальнейшие шаги по обработке различных ситуаций с точки зрения безопасности. Внутри организации должны быть определены следующие процедуры.

- Процедура управления пользователями. Определяет, кто может осуществлять авторизованный доступ к тем или иным компьютерам организации, и какую информацию администраторы должны предоставлять пользователям, запрашивающим поддержку. Процедуры управления пользователями также определяют, кто несет ответственность за информирование администраторов о том, что сотруднику больше не требуется учетная запись. Аннулирование учетных записей важно с той точки зрения, чтобы доступ к системам и сетям организации имели только лица с соответствующими деловыми потребностями.
- Процедуры системного администрирования. Описывают, каким образом в данный момент времени применяется политика безопасности на различных системах, имеющихся в организации. Эта процедура подробно определяет, каким образом должна осуществляться работа с обновлениями и их установка на системы.
- Процедуры управления конфигурацией. Определяют шаги по внесению изменений в функционирующие системы. Изменения могут включать в себя обновление программного и аппаратного обеспечения, подключение новых систем и удаление ненужных систем.

Примечание

Во многих организациях управление обновлениями представляет собой большую проблему. Отслеживание обновлений для снижения уровня уязвимости систем, а также тестирование этих обновлений перед установкой на функционирующие системы (чтобы не отключать работающие приложения) занимает очень много времени, но эти задачи очень важны для любой организации.

Наряду с процедурами по управлению конфигурацией устанавливаются методологии разработки новых систем. Они очень важны для управления уязвимостями новых систем и для защиты функционирующих систем от несанкционированного изменения. Методология разработки определяет, как и когда должны разрабатываться и применяться меры защиты. Необходимо делать акцент на этих сведениях при проведении любых инструктажей разработчиков и менеджеров проектов.

Ресурсы

Для применения корректных рекомендаций по безопасности необходимо осуществить присвоение ресурсов. К сожалению, не существует формулы, которую можно использовать для определения того, сколько ресурсов (денег или сотрудников) должно быть выделено в соответствии с программой безопасности, руководствуясь лишь размерами организации. В этом уравнении слишком много переменных. Необходимые ресурсы обуславливаются размером организации, деловыми процессами организации и опасностями, угрожающими ей.

Количество ресурсов должно определяться на базе корректной и полной оценки рисков, в соответствии с алгоритмом обработки рисков. В этом случае используется управление проектом. На рисунке 9.1 показано, каким образом относятся друг к другу ресурсы, время и область проекта. Если программа безопасности воспринимается как проект, то организация должна выделить достаточно ресурсов для уравновешивания треугольника либо расширить время или уменьшить область.

Персонал

Независимо от того, насколько велика или мала организация, некоторым сотрудникам должно быть поручено выполнение задач, связанных с обработкой уязвимостей и обеспечением информационной безопасности. В небольших организациях это может быть возложено на сотрудника отдела информационных технологий. В более крупных организациях могут существовать целые отделы безопасности. В рекомендациях не предписывается какое-либо определенное число сотрудников, однако настоятельно рекомендуется, чтобы, по крайней мере, на одного сотрудника были возложены обязанности по обеспечению безопасности.

Сотрудники отдела безопасности должны иметь следующие навыки.

- Администрирование безопасности. Понимание ежедневного процесса администрирования устройств обеспечения безопасности.
- Разработка политик. Опыт в разработке и поддержке политик безопасности, процедур и планов.
- Архитектура. Понимание сетевой и системной архитектур и применение новых систем.
- Исследование. Проверка новых технологий безопасности на предмет того, насколько они могут противостоять риску, представляемому для организации.
- Оценка. Наличие опыта сбора сведений о потенциальных рисках в организациях или подразделениях. Оценка может включать в себя навыки проникновения и тестирования безопасности.

- Аудит. Наличие опыта ведения аудита систем или процедур.

Рис. 9.1. Треугольная диаграмма управления проектом

Все эти навыки полезны для организации, однако мелкие компании могут не иметь возможности привлечь сотрудников, обладающих всеми этими навыками. В данном случае наиболее рациональным выходом из положения является привлечение администратора безопасности или разработчика политик в качестве сотрудника, а для выполнения других функций следует воспользоваться услугами сторонних организаций.

Существуют люди, у которых есть практически все перечисленные навыки. Эти специалисты, как правило, обладают большим опытом и, следовательно, требуют очень высокой зарплаты. Если в рассматриваемой организации бюджет ограничен, и зарплата соответствующего уровня не может быть обеспечена, не стоит надеяться на то, что удастся привлечь такого специалиста. Вместо этого следует заняться поиском лиц, у которых есть общее представление обо всех перечисленных моментах и конкретные навыки, которые необходимы в наибольшей степени.

Бюджет

Размер бюджета безопасности организации зависит от области действия и временных рамок проекта безопасности, а не от размеров организации. Организации с мощными программами безопасности могут иметь меньший бюджет, чем мелкие организации, которые только начинают создавать свою программу безопасности.

Распределение средств играет важную роль в вопросах, связанных с бюджетом безопасности. Бюджет безопасности должен быть разделен между капитальными затратами, текущими операциями и обучением персонала. Во многих организациях допускается ошибка, заключающаяся в том, что компаниями приобретаются дорогие средства безопасности без резервирования достаточного количества средств на обучение персонала работе с этими средствами. В других случаях организации приобретают эти средства, предполагая, что число сотрудников может быть сокращено, или руководство сотрудниками может осуществляться на разных уровнях. В большинстве случаев новые средства безопасности не позволяют сократить штат сотрудников. Несомненно, данному вопросу следует уделить дополнительное внимание.

Во многих организациях сотрудники и руководящий состав полагают, что повышенный уровень автоматизации средств безопасности позволит сократить число сотрудников, задействованных в обеспечении безопасности. К сожалению, это предположение оправдывается очень редко. Причина в том, что новые средства безопасности не автоматизируют процесс, выполняемый вручную. В большинстве случаев получается так, что процесс в данный момент времени не выполняется вовсе. Следовательно, новое средство безопасности "предоставляет новую возможность", а не повышает эффективность системы безопасности. Таким образом, покупка нового средства, как правило, увеличивает нагрузку на сотрудников и требует привлечения дополнительного персонала.

Распределение бюджета, согласно рекомендациям, должно основываться на планах проекта безопасности (которые, в свою очередь, базируются на риске, существующем для организации). Для успешного выполнения планов проекта безопасности должны быть выделены все необходимые средства.

Ответственность

Некоторое должностное лицо в организации должно нести ответственность за управление рисками, связанными с безопасностью информации. С недавнего времени эти обязанности в крупных компаниях принято возлагать на специального сотрудника исполнительного уровня - главного специалиста по безопасности информации (Chief Information Security Officer, CISO).

Вопрос эксперту

Вопрос. Старший руководящий сотрудник попросил обосновать бюджет безопасности. Каким образом это лучше сделать?

Ответ. Бюджет безопасности должен быть связан с уменьшением уровня опасности, представляемой для информации организации. Иными словами, бюджет должен четко соответствовать потенциальным результатам оценки рисков. Выделите следующие моменты.

- Во-первых, покажите, что существует опасность, которую необходимо взять под контроль или снизить. Это подтвердит актуальность и необходимость проекта.
- Во-вторых, оценка риска должна включать в себя определение потенциального ущерба, наносимого организации в случае успешного проведения атаки. Здесь

речь идет о том, во сколько организации обойдется устранение последствий инцидента.

Независимо от размеров организации, должностное лицо исполнительного уровня должно нести эту ответственность. В некоторых компаниях главный специалист по финансам предоставляет соответствующие отчеты безопасности. В других компаниях эти обязанности выполняют главный специалист по безопасности информации или главный специалист по технологии.

Независимо от того, какое должностное лицо предоставляет отчеты, этот сотрудник должен понимать, что безопасность - очень важная часть его работы. Сотрудник исполнительного уровня должен иметь право на определение политики организации и проверять все политики, связанные с безопасностью организации. Этот сотрудник также должен иметь право на принуждение к использованию политики системных администраторов и сотрудников, задействованных в обеспечении физической безопасности организации.

Не предполагается, что рассматриваемый сотрудник будет выполнять ежедневные операции по администрированию и обеспечению безопасности. Эти функции могут и должны быть поручены сотрудникам отдела безопасности.

Главный специалист по безопасности организации должен разработать систему измерения, фиксирующую степень достижения целей по обеспечению безопасности. Среди измеряемых параметров могут быть число уязвимостей в системах, степень выполнения проекта безопасности или реализации соответствия рекомендациям. Измеренные параметры должны регулярно сообщаться старшему руководящему составу (как правило, ежемесячно). Данные отчеты также должны представляться совету директоров компании. Так как безопасность стала важной частью процесса управления рисками в организациях, необходимо обеспечить широкую огласку и понимание данного вопроса всеми сотрудниками компании.

Примечание

Инструкции по выполнению финансовых операций и страхованию должны требовать предоставление совету директоров регулярных отчетов о состоянии безопасности организации.

Обучение

Обучение сотрудников является одной из наиболее важных составляющих процесса управления угрозами, представляемыми для безопасности информации. Если сотрудники не будут обладать достаточным уровнем знаний и не будут работать сообща, любые попытки управления рисками безуспешны. Рекомендуется осуществлять три формы обучения.

- Превентивные меры.
- Принудительные меры.
- Поощрительные меры.

Превентивные меры

Обучение превентивным мерам обеспечивает сотрудников детальными знаниями о защите информационных ресурсов организации. Сотрудникам следует рассказать, почему требуется защищать информационные ресурсы организации; понимание причин применения превентивных мер сделает их более совместимыми с политиками и процедурами. Если сотрудники не будут знать, каковы цели обеспечения безопасности, то попытаются нарушить установленные политики и процедуры.

Кроме информирования сотрудников о важности обеспечения безопасности, необходимо предоставить подробные сведения и подходы к обеспечению соответствия политике организации. Такие мифы, как, например, "надежные пароли трудно запоминать, поэтому их следует записывать на бумаге", следует рассмотреть и скорректировать.

Строгие превентивные меры могут принимать различные формы. В осведомительные программы следует включить как рекламные кампании, так и обучение сотрудников. Рекламные кампании должны включать в себя статьи новостей и плакаты. Для напоминания сотрудникам об их обязанностях используйте электронные сообщения и всплывающие окна. Ключевыми темами рекламных кампаний должны являться следующие.

- Распространенные ошибки сотрудников, например, запись на бумаге или разглашение паролей.
- Распространенные случаи несоблюдения безопасности, например, предоставление слишком большого объема информации клиенту.
- Важная информация, связанная с вопросами безопасности, например, с кем необходимо связываться в случае подозрения на угрозу безопасности.

- Текущие вопросы информационной безопасности, такие как антивирусная защита и безопасность удаленного доступа.
- Темы, помогающие сотрудникам в работе, например, защита переносных компьютеров в поездке или защита детей от злоумышленников в интернете.

Занятия по обучению безопасности должны быть нацелены на различные группы сотрудников организации. Все новые сотрудники должны проходить краткий инструктаж (длительностью до часа). Других сотрудников следует обучать примерно каждые два года. В процессе этого обучения предоставляется следующая информация.

- Почему в организации необходимо обеспечивать безопасность.
- Ответственность сотрудника относительно вопросов безопасности.
- Детальные сведения о политиках информационной безопасности организации.
- Детальные сведения о политиках использования, установленных в организации.
- Предлагаемые методы выбора надежных паролей.
- Предлагаемые методы предотвращения атак социального инжиниринга, включая вопросы, заданные и не заданные сотрудниками справочной службы.

Совет

Вместо того чтобы тратить час на устную лекцию, попробуйте включить в занятия практические примеры и видеоматериал. На сайте Commonwealth Films (http://www.commonwealthfilms.com//) есть хороший выбор обучающих видеоматериалов по теме безопасности.

Администраторы должны получить базовые инструкции по вопросам безопасности и пройти дополнительное обучение согласно их конкретной ответственности. Длительность дополнительных уроков не должна превышать полчаса, и на этих занятиях необходимо рассмотреть следующие вопросы.

- Самые последние методы работы хакеров.
- Текущие угрозы безопасности.
- Текущие уязвимости и обновления безопасности.

Разработчики должны получить базовые инструкции по вопросам безопасности. Для них следует проводить дополнительные занятия в зависимости от вопросов, за которые они ответственны, в частности, за обеспечение безопасности процесса разработки. Во время этих занятий необходимо сконцентрироваться на методологии разработки и процедурах управления конфигурацией.

Для менеджеров компании следует периодически устраивать презентации о текущем состоянии дел с предоставлением актуальных и детальных оценок угроз и планов по снижению риска. В презентации включается обсуждение системы измерения и методов определения эффективности программы безопасности при помощи этой системы.

Не следует считать, что сотрудникам отдела безопасности не нужно проходить инструктаж по обеспечению безопасности. Можно предположить, что как добросовестные сотрудники они и так прекрасно знают о своих обязанностях, однако им следует периодически предоставлять инструкции по самым последним средствам безопасности и методам работы хакеров.

Принудительные меры

Большинство сотрудников будут выполнять превентивные меры и следовать политике организации. Тем не менее, некоторые сотрудники могут уклоняться от этого (непреднамеренно или даже умышленно), что может нанести организации вред. В организациях следует принимать меры для защиты от таких сотрудников.

Важной составляющей процесса "избавления" от таких сотрудников является обеспечение осведомленности сотрудников об основах политики организации. Обеспечить эту осведомленность можно при помощи соглашений о безопасности. По завершении прохождения сотрудником обучения безопасности ему нужно предоставить копии соответствующих политик и предложить подписать соглашение о том, что он ознакомился и согласился с политиками организации. Эти подписанные документы отдаются на хранение в отдел кадров и могут использоваться в случае судебного процесса.

Поощрительные меры

Вследствие природы вопросов, связанных с безопасностью, сотрудники могут не утруждать себя информированием отделов безопасности о наличии нарушений безопасности. Однако, так как сотрудники отдела безопасности не могут одновременно находиться в нескольких местах и уследить абсолютно за всем, сотрудники являются важной частью системы оповещения об опасностях.

Одним из методов, используемым здесь для увеличения уровня отчетности сотрудников об аспектах безопасности, является программа поощрений сотрудников организации. Поощрения не должны быть большими. На самом деле, лучше, если поощрения будут выдаваться в виде небольших денежных сумм. Сотрудников также следует убедить в

том, что такие отчеты очень нужны организации, и что сотрудники не будут наказываться за ложные оповещения.

Поощряться могут сотрудники, вносящие предложения о повышении уровня безопасности и решении других проблем, связанных с безопасностью. Успешные поощрительные программы реализуются посредством запросов у сотрудников ответов на вопросы через службу новостей организации. В такой программе организация может публиковать полученные рекомендации с указанием сотрудников, внесших соответствующие предложения.

Планы выхода из критических ситуаций

Даже в наиболее благоприятных обстоятельствах никогда не получится полностью устранить опасности, представляемые для информационных ресурсов организации. Чтобы обеспечить быстрое восстановление и снижение ущерба, нанесенного организации в результате инцидента, необходимо сформулировать планы выхода из критических ситуаций.

Обработка инцидентов

В каждой организации должна присутствовать процедура обработки инцидентов. Она определяет шаги, которые необходимо предпринимать в случае взлома защиты или проникновения в систему злоумышленника. Без этой процедуры вы можете потратить много времени на устранение его последствий. Это время является для потенциальных клиентов компании антирекламой и означать потерю средств и утечку информации.

В процедуре обработки инцидента следует детально определить, кто несет ответственность за обработку инцидентов в организации. Без предоставления четких инструкций по этому поводу может быть потрачено лишнее время на поиск виновного в происшествии и ответственного за перевод систем в автономный режим и обращение в органы правопорядка.

В рекомендациях указывается, что периодически нужно тестировать процедуры обработки инцидентов. Изначальные тесты могут анонсироваться заранее и заключаться в совместном диалоге сотрудников в форуме и высказывании ими своего мнения по поводу того, каким

образом можно обработать тот или иной инцидент. Дополнительное тестирование в "реальном" мире должно проводиться таким образом, чтобы неожиданные события симулировали реальные вторжения злоумышленников.

Резервное копирование и архивация данных

Процедуры резервного копирования должны исходить из политики резервного копирования. Процедуры определяют время выполнения резервного копирования и указывают шаги, которые следует выполнять при резервировании данных и их безопасном сохранении. В процедурах архивации данных указывается периодичность повторного использования резервных носителей и места, где должны располагаться носители.

Когда резервный носитель требуется извлечь из места отдельного хранения, необходимо руководствоваться инструкциями, включенными в процедуру и указывающими, каким образом осуществляется запрос и идентификация носителей, метод восстановления данных и способ возвращения носителя в место хранения.

Если в организациях такие процедуры отсутствуют, то существует опасность неправильной интерпретации сотрудниками политики резервного копирования. В этом случае возможны ситуации, когда резервные носители не будут вовремя отсоединяться от сайта или восстановление данных будет происходить некорректно.

Внимание!

Убедитесь, что процедуры разработаны в соответствии с политикой хранения данных организации.

Восстановление после сбоев

В каждой организации должны присутствовать планы восстановления после сбоев для определения требований и целей, достигаемых при возникновении каких-либо неполадок. Планы детально описывают, какие вычислительные ресурсы являются наиболее критичными для организации, и с помощью этих планов формируются конкретные требования по возврату этих ресурсов в работоспособное состояние.

В организациях необходимо иметь планы, предусматривающие выход из различных неблагоприятных ситуаций, начиная от потери одного компьютера и заканчивая выходом из строя всей сети. Кроме того, в сценарии восстановления следует включить ключевые компоненты инфраструктуры, такие как каналы связи и оборудование.

Планы восстановления после сбоев могут не предусматривать наличие резервных "горячих сайтов" с полными копиями всего имеющегося оборудования. Тем не менее, эти планы должны быть хорошо продуманными, а стоимость применения плана -

взвешена относительно потенциального ущерба, который может быть нанесен организации.

Любой план восстановления после сбоев необходимо периодически тестировать. По крайней мере, один раз в год должно проводиться полное тестирование. При выполнении этого теста возможно перемещение сотрудников в альтернативные помещения, если это предусматривается в плане.

Планы проектов безопасности

Так как обеспечение безопасности является непрерывным процессом, безопасность информации следует рассматривать как постоянно выполняемый проект. Разделим общий проект на несколько мелких, которые должны быть завершены. Согласно рекомендациям, отдел безопасности организации должен утверждать следующие планы.

- Планы усовершенствования.
- Планы проведения оценок.
- Планы оценки уязвимостей.
- Планы аудита.
- Планы обучения.
- Планы оценки политики.

Усовершенствование

Планы усовершенствования вытекают из процедур оценки. Если в результате оценки определены некоторые опасные области, следует создать планы по усовершенствованию для разрешения возможных проблем и внесения соответствующих изменений в среду. Планы усовершенствования могут включать в себя планирование установки политики, применения средств или внесения изменений в систему, либо создания обучающих программ. Каждая оценка, проводимая в рамках организации, должна быть отправной точкой плана усовершенствования.

Оценка

Отдел безопасности организации должен разрабатывать ежегодные планы оценки риска для организации. В средних организациях это может быть план полной оценки, проводимой один раз в год. В крупных организациях план может предусматривать оценки по подразделениям, а полные оценки могут проводиться реже одного раза в год.

Большим организациям рекомендуется отклоняться от концепции ежегодных оценок. На практике оценки занимают много времени при их организации, выполнении и анализе. В очень больших компаниях может быть затрачено несколько месяцев на планирование, несколько месяцев на выполнение и несколько месяцев - на анализ, в результате чего останется совсем немного времени на непосредственное применение изменений, перед тем как наступит время следующей оценки. В подобных случаях эффективнее выполнять менее масштабные оценки с большей частотой, а полные оценки осуществлять периодически, согласно имеющимся условиям.

Оценка уязвимостей

Отделы безопасности организаций должны регулярно проводить оценку уязвимостей (сканирование) систем организации. Отдел безопасности должен планировать ежемесячную оценку всех систем внутри организации. Если в организации очень много компьютеров, то их нужно сгруппировать и по частям сканировать каждую неделю. Необходимо наличие планов к исполнению, с помощью которых администраторы смогут внести соответствующие коррективы в системы.

Внимание!

При сообщении системным администраторам результатов сканирования уязвимостей необходимо соблюдать внимательность. Помните, что администраторы выполняют свою работу на благо организации, и это их "хлеб". Здесь не должна идти речь о каком-либо соперничестве; наоборот, системные администраторы и администраторы безопасности должны работать совместно для выявления уязвимостей и контроля рисков в организации.

Аудит

Отдел безопасности должен разработать планы проведения аудита на соответствие политике организации. Такие аудиты могут быть сфокусированы на конфигурации систем, соответствии политике резервного копирования или на защите информации в физической форме. Так как аудиты требуют больших усилий со стороны персонала, каждый аудит нацелен на небольшую часть организации. При проведении аудитов системных конфигураций из всех систем можно выбрать образец. При обнаружении значительных расхождений и несоответствий в соответствующем подразделении проводится более масштабный аудит.

Внутренний отдел аудита организации должен иметь свои собственные расписания и планы аудитов. Аудиты, проводимые отделом безопасности, не заменяют аудиты, осуществляемые внутренним отделом аудита. Эти аудиты направлены на определение того, насколько хорошо понимаются и выполняются политики и процедуры безопасности, с дальнейшим устранением несоответствий и недостатков.

Обучение

Планы обучения должны создаваться совместно с отделом кадров. Эти планы включают в себя расписание учебных занятий и планы проведения рекламных кампаний. В расписании необходимо учитывать, что каждый сотрудник должен проходить обучение один раз в два года.

Оценка политики

Каждая политика организации должна предусматривать даты пересмотра политики. Отдел безопасности должен разрабатывать планы для начала пересмотра и оценки политики по мере приближения даты пересмотра. Как правило, каждый год требуется пересмотр двух политик.

Вопросы для самопроверки

1. Бюджет безопасности должен быть обоснован результатами _____.
2. Когда сотрудники организации должны в первый раз проходить обучение безопасности?

Техническая безопасность

Меры по обеспечению технической безопасности связаны с применением элементов управления безопасностью на компьютерах и в компьютерных сетях. Эти элементы управления являются отражением политик и процедур организации.

Сетевые соединения

Результатом перемещения информации между организациями явились возросшие коммуникационные возможности между сетями различных организаций. Соединение с интернетом сегодня доступно практически в любой организации, и большая часть компаний использует интернет в определенных деловых целях. Чтобы защитить организацию от нежелательных вторжений, необходимо соблюдать следующие рекомендации.

Постоянные соединения

Сетевые соединения с другими организациями или с интернетом должны защищаться межсетевым экраном. Межсетевой экран играет роль огнеупорной стены между двумя комнатами, которая разделяет пространство на два различных участка, и при возникновении пожара в одной из комнат огонь не перекинется на вторую. Аналогичным образом межсетевые экраны отделяют сети организаций от интернета или сетей других организаций для предотвращения распространения ущерба. Межсетевые экраны являются фильтрующими маршрутизаторами, фильтрами пакетов или межсетевыми экранами прикладного уровня, в зависимости от требований организации (см. лекцию 10).

Примечание

Беспроводные сети следует также отделять от внутренней сети организации (для этого рекомендуется использовать межсетевой экран), так как беспроводное соединение, по сути, представляет собой постоянное соединение с некоторыми неизвестными объектами (это может быть любой пользователь, находящийся поблизости и имеющий карту беспроводного сетевого интерфейса!).

Соединения удаленного доступа

Соединения удаленного доступа могут использоваться для получения несанкционированного доступа к организациям и, следовательно, эти соединения необходимо защищать. Такие соединения могут устанавливаться посредством коммутируемого телефонного подключения либо через интернет. Поскольку они обеспечивают доступ во внутреннюю сеть организации как обычное постоянное соединение, необходимо использовать некоторую форму двухфакторной аутентификации. Речь идет о следующих механизмах аутентификации.

- Модемы обратного вызова. Используются совместно с механизмом аутентификации и являются достаточным средством аутентификации для телефонных соединений. Модемы обратного вызова настраиваются на определенный номер, который они набирают перед установкой телефонного соединения. Пользователь, пытающийся подключиться, не может изменить этот номер. Модемы обратного вызова не подходят для мобильных пользователей (т. е. пользователей, постоянно переезжающих с места на место).

- Динамические пароли. Используются в качестве механизма аутентификации и являются таковыми, если комбинируются с какими-либо данными, известными пользователю.
- Устройства шифрования. Портативные устройства шифрования используются в качестве механизмов аутентификации при их комбинировании с какими-либо данными, известными пользователю. Устройство шифрования должно быть предварительно снабжено соответствующими ключами шифрования и соответствовать тому, что имеет пользователь.

Любой из этих механизмов подходит для аутентификации пользователей через соединения удаленного доступа.

Примечание

Некоторые типы механизмов аутентификации не подходят для виртуальных частных сетей (VPN). Например, если бы для аутентификации использовался биометрический сканер отпечатков пальцев, потенциальная опасность обмана системы была бы намного выше, так как компьютер находится за пределами защищаемого физического местоположения.

Защита от вредоносного кода

Вредоносный код (компьютерные вирусы, троянские программы и черви) является одной из наиболее серьезных угроз для информации. Число и степень сложности этих программ продолжает с каждым днем увеличиваться, и также возрастает степень подверженности современных приложений нецелевому использованию этими программами. Вредоносный код проникает в организации четырьмя основными способами.

- Файлы с общим доступом с домашних и рабочих компьютеров.
- Файлы, загружаемые с сайтов интернета.
- Файлы, поступающие в организацию в виде вложений электронной почты.
- Файлы, внедряемые в системы посредством использования уязвимостей.

Для контроля этой опасности в организации нужно разработать эффективную антивирусную программу. Хорошая антивирусная программа осуществляет контроль за вредоносным кодом в трех точках.

- Серверы. Антивирусное ПО устанавливается на всех файловых серверах и настраивается на периодическое выполнение полной проверки наличия вирусов во всех файлах.
- Рабочие станции. Антивирусное ПО устанавливается на всех рабочих станциях и настраивается на периодическое выполнение полной проверки наличия вирусов во всех файлах. Кроме того, антивирусное ПО настраивается на проверку каждого открываемого файла.
- Системы электронной почты. Антивирусное ПО устанавливается либо на главный почтовый сервер, либо на пути следования электронной почты внутри организации. Настраивается на проверку каждого файлового вложения перед непосредственной доставкой пользователю.

Примечание

Системные уязвимости устраняются посредством регулярного сканирования уязвимостей и установкой соответствующих обновлений.

Установка и настройка антивирусного программного обеспечения лишь наполовину решает проблему вредоносного кода. Для полноты антивирусной программы необходимо обеспечить частые обновления признаков вредоносного ПО и доставку этих обновлений на серверы, рабочие станции и системы электронной почты. Обновления необходимо получать согласно рекомендациям производителя программного обеспечения. Это действие должно выполняться не реже одного раза в месяц.

Многие производители антивирусного ПО предоставляют автоматизированные механизмы загрузки самых последних признаков вирусов и распространения их по организации. Это позволяет осуществлять ежедневную загрузку признаков вредоносного ПО.

Аутентификация

Аутентификация авторизованных пользователей предотвращает получение неавторизованными пользователями доступа к корпоративным информационным системам. Использование механизмов аутентификации предотвращает доступ авторизованных пользователей к той информации, просмотр которой им запрещен. В настоящее время главным механизмом аутентификации при внутрисистемном доступе являются пароли. При использовании паролей следует руководствоваться приводимыми ниже рекомендациями.

- Длина пароля. Минимальная длина пароля должна составлять не менее 8 символов.
- Частота смены пароля. Возраст паролей не должен превышать 60 дней. Кроме того, пароли не должны изменяться в течение дня после плановой смены пароля.
- История пароля. Не должны использоваться последние десять прежних паролей.
- Содержимое паролей. Пароли не должны состоять только из букв; они должны представлять комбинацию букв, цифр и специальных символов пунктуации. При изменении паролей система должна в принудительном порядке налагать эти ограничения.

Примечание

Точные характеристики паролей корректируются в зависимости от используемой системы. Например, пароли Windows 2000 обладают самой высокой надежностью, если имеют длину в семь или четырнадцать символов. Пароли из восьми символов лишь немного надежнее, чем пароли из семи символов.

Пароли всегда хранятся в зашифрованном виде и недоступны обычным пользователям. Для систем или информации особой секретности пароли могут не обеспечивать должной защиты. В этих случаях следует использовать динамические пароли или двухфакторную аутентификацию. Имейте в виду, что аутентификация представляет собой комбинацию следующих компонентов.

- То, что известно пользователю, например пароль.
- То, что есть у пользователя, например карта доступа.
- То, что представляет личность пользователя, например отпечаток пальца.

Двухфакторная аутентификация используется для снижения уязвимости каждого типа аутентификационных данных. Например, пароли записываются на бумаге и, следовательно, могут быть раскрыты. Карты доступа можно украсть, а биометрические средства аутентификации дороги и требуют контролируемого или доверенного доступа между пользователем и компьютером.

Все системы организации следует настроить на запуск экранной заставки для удаления информации с экрана и требование повторной аутентификации, если пользователя нет за компьютером больше 10 минут. Если сотрудник оставит компьютер без присмотра, не выходя из сети, то при отсутствии повторной аутентификации злоумышленник сможет использовать этот компьютер под видом работника организации.

Отслеживание

Отслеживание (мониторинг) сетей на предмет наличия подозрительной активности стал необходимым и обязательным действием. Это действие включает как аудит, так и мониторинг сети и системы в реальном времени. Как правило, оно разделяется на аудит и обнаружение вторжений.

Аудит

Аудит - это механизм, записывающий действия, происходящие на компьютере. Журнал содержит информацию о произошедших событиях (вход в систему, выход из системы, доступ к файлам и т. д.), о том, кто выполнил то или иное действие, когда выполнено действие, было ли это действие успешным. Журнал аудита - это материал для исследовательских действий, выполняемых после какого-либо происшествия. Журнал содержит информацию о том, каким образом осуществлено проникновение в компьютерную систему, какая информация считана или изменена. Должна вестись запись следующих событий.

- Вход/выход пользователей.
- Неудачные попытки входа.
- Попытки сетевого подключения.
- Попытки удаленного подключения по телефонной линии.
- Вход супервизора/администратора/основателя.
- Функции, привилегии на выполнение которых имеются у супервизора/администратора/основателя.
- Доступ к секретным файлам.

В идеальном случае эти события записываются в файл, расположенный на защищенной системе - злоумышленник не сможет удалить следы своих действий.

Журналы аудита полезны в том случае, если они регулярно просматриваются. К сожалению, журналы аудита - это одни из наиболее сложных файлов для просмотра вручную. Человеку очень трудно искать в огромном файле журнала несколько записей, которые могут означать некоторое интересуемое событие. Следовательно, в организациях следует использовать автоматизированные средства просмотра журналов аудита. Эти средства представляют собой сценарии, просматривающие файлы журналов на предмет поиска определенных строк текста. Рекомендуется осуществлять еженедельный просмотр журналов аудита.

Совет

Процесс воссоздания часто затрудняется тем, что временные метки в различных журналах не соответствуют друг другу. Чтобы упростить процесс просмотра журнала, рекомендуется синхронизировать часы на всех системах при помощи централизованной системы синхронизации времени, такой как NTP.

Обнаружение вторжений

Системы обнаружения вторжений (IDS) используются для мониторинга сетей или систем и оповещения в реальном времени о событии, представляющем интерес для лиц, обеспечивающих безопасность (см. лекцию 13). Использование узловой системы обнаружения вторжений помогает при проверке журналов аудита, т. к. дает возможность просмотра файлов журналов. Сетевая IDS используется для мониторинга сети на предмет атак или трафика, который отличается от нормального потока данных, обычно наблюдаемого в сети. Системы IDS обоих типов обеспечивают безопасность посредством выдачи предупреждений и оповещений при наличии необычной активности в системе, тем самым снижая время, затрачиваемое на обработку инцидента.

Внимание!

Не следует ограничиваться только лишь применением IDS. Развертываемая IDS должна быть тесно связана с политикой использования компьютеров и политикой безопасности, а также с процедурами обработки инцидентов, имеющимися в организации.

Шифрование

Секретная информация подвергается опасности при передаче незащищенным способом, например через электронную почту или телефонные линии. Секретная информация подвергается опасности при хранении на незащищенном переносном компьютере. Защиту информации обеспечивает шифрование.

Если уровень секретности информации того требует, информация должна шифроваться при передаче по незащищенным каналам связи или через электронную почту. Используемый алгоритм шифрования должен обеспечивать уровень защищенности, соответствующий степени секретности защищаемой информации. На линиях связи между компьютерами организации должно применяться шифрование канала связи. Если между компьютерами используются VPN-соединения, то VPN должны использовать

очень мощное шифрование для всей информации, передаваемой между двумя расположениями.

Если электронная почта используется для передачи секретной информации внутри организации, шифрование сообщений не обязательно. Однако если секретные данные передаются за пределы внутренней сети организации, необходимо шифровать сообщения. Если сообщение передается в другую организацию, следует заранее разработать процедуры, обеспечивающие шифрование сообщения. Некоторые правила (такие как HIPAA) требуют шифрования секретной информации при ее прохождении через открытые сети.

При хранении на переносных компьютерах секретная информация должна находиться в зашифрованном виде. Используемый алгоритм шифрования должен обеспечивать уровень надежности, соответствующий степени секретности защищаемой информации. Система на портативном компьютере должна требовать аутентификацию пользователя перед тем, как он сможет осуществить доступ к информации. В идеальном случае система должна запрещать доступ к информации, если пользователь компьютера недоступен.

При шифровании любых данных следует использовать хорошо известные и проверенные алгоритмы шифрования (см. лекцию 12).

Обновление систем

Поставщики программного обеспечения выпускают обновления для устранения уязвимостей и ошибок в своих программах. Эти обновления очень важны с точки зрения безопасности, так как без них системы будут находиться в состоянии, уязвимом для атаки и проникновения. Тем не менее, обновления не следует устанавливать без их тестирования.

В каждой организации должна быть тестовая лаборатория, в которой будет проводиться проверка новых обновлений различными приложениями перед установкой на функционирующие системы. Администраторы должны регулярно проверять наличие новых обновлений. Все обновления должны устанавливаться в соответствии с процедурами контроля за изменениями, установленными в организации.

Резервное копирование и восстановление

Как говорилось в разделе "Административная безопасность", резервное копирование и восстановление являются неотъемлемыми процедурами для обеспечения

восстановления после сбоя. Чем более "свежими" являются резервные копии, тем легче восстановить все текущие операции. Информация на серверах должна резервироваться ежедневно. Один раз в неделю необходимо осуществлять полное резервное копирование. Резервирование данных в течение последующих шести дней должно дополнять полное резервирование.

Все резервные копии должны периодически проверяться для определения того, успешно ли созданы резервные копии важных файлов. Должны быть установлены регулярные расписания тестирования, чтобы осуществлялось периодическое тестирование всех носителей.

Резервное копирование рабочих станций и портативных компьютеров может вызвать проблемы в любой организации. Одной из них является большой объем данных. Вторая проблема заключается в надобности выполнения резервного копирования между различными сетями. Как правило, резервное копирование рабочей станции и портативных компьютеров производится только в том случае, если информация является слишком секретной, чтобы находиться на файловом сервере. В данном случае резервная система должна находиться в одном местоположении с рассматриваемым компьютером.

Внимание!

Если информация слишком секретна для размещения на файловых серверах, резервные носители требуют особой защиты.

Не менее важно обеспечить правильное хранение резервных копий после их создания. Резервное копирование осуществляется таким образом, чтобы организация смогла восстановить информацию в случае сбоя. Под сбоями подразумеваются такие события, как случайное удаление важного файла пользователем или выход из строя всего сайта. Для восстановления из первой и второй ситуации предъявляются конфликтующие требования к хранению резервных копий. Для восстановления важных пользовательских файлов резервные копии должны находиться под рукой, чтобы восстановление можно было произвести быстро. Для защиты от сбоев и других непредвиденных обстоятельств резервные копии должны храниться в отключенном от сети состоянии.

Согласно рекомендациям, резервные копии нужно отключать от сети для максимизации уровня защиты информации. Резервные копии следует систематизировать, чтобы их

можно было быстро найти и использовать для восстановления определенных файлов. Резервные копии необходимо отключить от сети в течение 24 часов после создания.

Физическая безопасность

Для обеспечения полной защиты необходимо выполнять требования физической безопасности, наряду с обеспечением технической и административной безопасности. Все меры по обеспечению технической безопасности не смогут защитить секретную информацию, если не контролировать физический доступ к серверам. Кроме того, на доступность информационных систем могут повлиять такие факторы, как электроэнергия и климатические условия. Согласно рекомендациям, физическая безопасность обеспечивает защиту информационных систем в следующих областях.

- Физический доступ.
- Климатические условия.
- Защита от пожара.
- Электроэнергия.

Физический доступ

Все секретные компьютерные системы должны быть защищены от несанкционированного доступа. Как правило, это реализуется посредством содержания систем в едином информационном центре. Доступ к информационному центру контролируется различными способами. Доступ с помощью магнитной карты или кодового замка призван ограничить число сотрудников, которые могут входить в информационный центр. Стены информационного центра должны быть капитальными, чтобы исключить доступ через пространство над фальш-потолком.

Климатические условия

Компьютерные системы чувствительны к высоким температурам. Кроме того, компьютеры сами по себе генерируют большое количество тепла. Модули контроля за климатом в информационном центре должны обеспечивать постоянную температуру и влажность, а также обладать мощностью, соответствующей размерам помещения и количеству теплоты, выделяемому компьютерными системами. Эти модули настраиваются на уведомление администраторов о сбоях либо о выходе температуры за пределы допустимого интервала. Если вокруг кондиционеров в информационном центре конденсируется влага, то из помещения центра необходимо убрать все емкости с водой.

Защита от пожара

В информационных центрах нельзя использовать водяные системы пожаротушения, так как в этом случае компьютерные системы выйдут из строя. Следует использовать системы пожаротушения, активное вещество которых основано не на воде. Система пожаротушения должна быть размещена и настроена таким образом, чтобы огонь в прилегающем пространстве не смог изолировать какую-либо систему информационного центра.

Если применение неводяной системы пожаротушения требует слишком больших затрат, можно использовать "сухую" систему, отключающую электроэнергию в информационном центре перед последующей подачей воды. Посоветуйтесь с пожарным инспектором, чтобы выяснить, можно ли использовать этот вариант.

Во многих инструкциях по борьбе с огнем говорится о том, что во всех помещениях здания должны быть установлены распылительные системы пожаротушения, независимо от наличия других систем. В этом случае неводяные системы подавления огня должны быть настроены на работу перед распылительными системами.

Электроэнергия

Для функционирования компьютерных систем необходима электроэнергия. Часто происходят скачки напряжения и кратковременное отключение электроэнергии. Такие прерывания в электроснабжении могут вывести компьютеры из строя и, следовательно, привести к потере данных. Все важные компьютерные системы должны быть защищены от кратковременных отключений электроэнергии.

Лучше всего с этой задачей справляются резервные источники питания. Эти источники должны обеспечивать электропитание в течение времени, достаточного для выполнения корректного отключения компьютеров. Чтобы защитить системы от более длительных отключений электричества, следует использовать резервные генераторы. В любом случае должны быть настроены оповещения, сообщающие администраторам об отключении электроэнергии.

Совет

Если резервный электрогенератор недоступен, следует приобрести аккумуляторные системы, позволяющие осуществить корректное отключение систем в случае продолжительного отсутствия электропитания. Это предотвратит выход компьютеров из строя при внезапном отключении из-за "севших" аккумуляторов.

Использование стандарта ISO 17799

Существует много различных инструкций, в которых приводятся разного рода рекомендации по той или иной тематике (в данном случае их количество слишком велико для отражения в материале этой книги). Подобные документы опубликованы многими ассоциациями и правительственными агентствами. В 2000 г. Международная организация по стандартизации (ISO) издала международный стандарт для методов безопасности информации. Документ называется "Информационные технологии - методы обеспечения информационной безопасности" - ISO/IEC 17799 (доступен на сайте американского Национального института стандартов http://www.ansi.org/; его стоимость - 112 долларов). Документ напрямую базируется на BS (British Standards Institution) 7799.

Данный документ предназначен для использования в качестве стартовой точки. Несмотря на то, что это очень качественный и полезный документ, каждая организация уникальна и, как правило, требует дополнительных мер контроля или же, наоборот, применения меньшего их количества, нежели указано в стандарте.

Ключевые концепции стандарта

ISO 17799 охватывает десять основных областей.

- Политика безопасности. В данном разделе рассказывается о необходимости политики безопасности и регулярного пересмотра и оценки этого документа.
- Организационная безопасность. В данном разделе описывается, как следует обеспечивать безопасность информации. Содержится информация о работе со сторонними организациями и управлении безопасностью при этих взаимоотношениях.
- Классификация и контроль имущества. В данном разделе обсуждается необходимость правильной защиты как физических, так и информационных ресурсов.
- Безопасность персонала. В данном разделе обсуждается необходимость контроля рисков, связанных с наймом на работу сотрудников, а также обсуждается обучение сотрудников организации. Кроме того, здесь впервые затрагивается тема обработки инцидентов.
- Физическая безопасность и безопасность среды. Все физическое имущество должно быть надежно защищено от хищения, пожара и других воздействий. Данный раздел посвящен именно этой теме.

- Управление коммуникациями и операциями. Рассматривается необходимость в документируемых процедурах управления компьютерами и сетями, а также обсуждается вопрос безопасности информации при ее передаче. Здесь также упоминается необходимость защиты компьютеров от вредоносных программ.
- Контроль доступа. В данном разделе обсуждается контроль доступа к информации, системам, сетям и приложениям, а также говорится об управлении пользователями и о необходимости мониторинга.
- Разработка и поддержка систем. В данном разделе рассматриваются вопросы безопасности, связанные с разработкой проектов. Кроме того, здесь обсуждаются необходимость в шифровании и управлении ключами, а также контроль конфигурации системных файлов.
- Поддержка непрерывности деловых процессов. Здесь рассказывается об опасности прерывания деловых процессов и о различных альтернативных способах поддержки их непрерывности.
- Соответствие политике. В данном разделе говорится о том, каким образом в организации следует соблюдать установленную политику и как должна проводиться проверка на соответствие установленной политике.

Для каждого раздела четко определены цели тех или иных контролирующих действий. Кроме того, во введении приводится полезная информация о том, как достичь защищенного состояния информации внутри организации.

Каким образом использовать этот стандарт

Стандарт ISO 17799 используется как стартовая точка для разработки программ безопасности. При построении программы безопасности необходимо ознакомиться с этим документом и использовать его в качестве руководства при работе в той или иной области. Если уже имеется разработанная программа безопасности, то с помощью стандарта ISO 17799 можно проверить, не упущены ли какие-либо важные вопросы.

Во введении в документ говорится о том, что некоторые меры контроля могут не понадобиться, и что могут потребоваться некоторые дополнительные меры, не включенные в материал стандарта. Точный набор средств, мер и действий по управлению, включаемый в каждую программу безопасности, определяется в процессе оценки угроз.

Внимание!

Не используйте стандарт ISO 17799 или какой-либо другой рекомендательный документ в качестве требований, соответствие которым должно быть полным и безусловным. Всегда проводите оценку угроз и определяйте действительные требования безопасности для вашей конкретной организации.

Проведение анализа уязвимостей

Этот проект покажет, насколько рассматриваемая организация соответствует авторитетным рекомендациям. Имейте в виду, что это несколько иная задача, нежели оценка угроз. Вы не будете пытаться выявить угрозы, а будете искать вещи, о которых раньше могли и не знать.

Шаг за шагом

1. Начните прорабатывать рекомендации, приводимые в данной лекции или в стандарте ISO 17799, если у вас имеется этот документ.
2. При работе с каждым разделом определите, соответствует ли ваша организация (или последняя проведенная оценка угроз) приводимым рекомендациям.
3. Если рассматриваемая организация не соответствует какой-либо рекомендации, попробуйте понять причину. Возможно, имеются другие меры и средства контроля, или степень угрозы для организации очень мала, вследствие чего неэффективно применять рекомендуемое средство или метод контроля. Кроме того, какая-либо рекомендация могла попросту ранее нигде не приводиться.
4. Для тех рекомендаций, явная причина применения которых в организации отсутствует, разработайте рекомендацию, обеспечивающую соответствующий уровень контроля.

Выводы

Как уже упоминалось выше, этот проект не является повторным проведением оценки угроз, а представляет собой наименее дорогостоящий способ рассмотреть под другим ракурсом имеющуюся программу безопасности. Даже самые опытные сотрудники отдела безопасности могут слишком "зацикливаться" на имеющейся программе, и день ото дня бороться с проблемами, возникающими при поддержке этой программы. Внешний наблюдатель, как правило, может внести "свежую струю" в виде рекомендаций, которые позволят усовершенствовать программу безопасности лишь потому, что не будут скованы ежедневным функционированием этой программы. Точно таким же образом может использоваться и документ с авторитетными рекомендациями.

Программно-аппаратные средства обеспечения информационной безопасности

Обновить Ресурс

Роль стандартов и спецификаций. Наиболее важные стандарты и спецификации в области информационной безопасности

Специалистам в области информационной безопасности (ИБ) сегодня почти невозможно обойтись без знаний соответствующих стандартов и спецификаций. На то имеется несколько причин.

Формальная состоит в том, что необходимость следования некоторым стандартам (например, криптографическим и/или Руководящим документам Гостехкомиссии России) закреплена законодательно. Однако наиболее убедительны содержательные причины. Во-первых, стандарты и спецификации - одна из форм накопления знаний, прежде всего о процедурном и программно-техническом уровнях ИБ. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами. Во-вторых, и те, и

другие являются основным средством обеспечения взаимной совместимости аппаратно-программных систем и их компонентов, причем в Internet-сообществе это средство действительно работает, и весьма эффективно.

Отмеченная роль стандартов зафиксирована в основных понятиях закона РФ "О техническом регулировании" от 27 декабря 2002 года под номером 184-ФЗ (принят Государственной Думой 15 декабря 2002 года):

стандарт - документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения;

стандартизация - деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг.

Примечательно также, что в число принципов стандартизации, провозглашенных в статье 12 упомянутого закона, входит принцип применения международного стандарта как основы разработки национального, за исключением случаев, если "такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и (или) технологическим особенностям или по иным основаниям, либо Российская Федерация, в соответствии с установленными процедурами, выступала против принятия международного стандарта или отдельного его положения". С практической точки зрения, количество стандартов и спецификаций (международных, национальных, отраслевых и т.п.) в области информационной безопасности бесконечно. В курсе рассматриваются наиболее важные из них, знание которых необходимо всем или почти всем разработчикам и оценщикам защитных средств, многим сетевым и системным администраторам, руководителям соответствующих подразделений, пользователям.

Отбор проводился таким образом, чтобы охватить различные аспекты информационной безопасности, разные виды и конфигурации информационных систем (ИС), предоставить полезные сведения для самых разнообразных групп целевой аудитории.

На верхнем уровне можно выделить две существенно отличающиеся друг от друга группы стандартов и спецификаций:

оценочные стандарты, предназначенные для оценки и классификации информационных систем и средств защиты по требованиям безопасности;

спецификации, регламентирующие различные аспекты реализации и использования средств и методов защиты.

Эти группы, разумеется, не конфликтуют, а дополняют друг друга. Оценочные стандарты описывают важнейшие, с точки зрения информационной безопасности, понятия и аспекты ИС, играя роль организационных и архитектурных спецификаций. Другие спецификации определяют, как именно строить ИС предписанной архитектуры и выполнять организационные требования.

Из числа оценочных необходимо выделить стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем" и его интерпретацию для сетевых конфигураций, "Гармонизированные критерии Европейских стран", международный стандарт "Критерии оценки безопасности информационных технологий" и, конечно, Руководящие документы Гостехкомиссии России. К этой же группе относится и Федеральный стандарт США "Требования безопасности для криптографических модулей", регламентирующий конкретный, но очень важный и сложный аспект информационной безопасности.

Технические спецификации, применимые к современным распределенным ИС, создаются, главным образом, "Тематической группой по технологии Internet" (Internet Engineering Task Force, IETF) и ее подразделением - рабочей группой по безопасности. Ядром рассматриваемых технических спецификаций служат документы по безопасности на IP-уровне (IPsec). Кроме этого, анализируется защита на транспортном уровне (Transport Layer Security, TLS), а также на уровне приложений (спецификации GSS-API, Kerberos). Необходимо отметить, что Internet-сообщество уделяет должное внимание административному и процедурному уровням безопасности

("Руководство по информационной безопасности предприятия", "Как выбирать поставщика Интернет-услуг", "Как реагировать на нарушения информационной безопасности").

В вопросах сетевой безопасности невозможно разобраться без освоения спецификаций X.800 "Архитектура безопасности для взаимодействия открытых систем", X.500 "Служба директорий: обзор концепций, моделей и сервисов" и X.509 "Служба директорий: каркасы сертификатов открытых ключей и атрибутов".

Британский стандарт BS 7799 "Управление информационной безопасностью. Практические правила", полезный для руководителей организаций и лиц, отвечающих за информационную безопасность, без сколько-нибудь существенных изменений воспроизведен в международном стандарте ISO/IEC 17799.

Таков, на наш взгляд, "стандартный минимум", которым должны активно владеть все действующие специалисты в области информационной безопасности.

Краткие сведения о стандартах и спецификациях, не являющихся предметом данного курса.

Упоминаемые в данном разделе стандарты и спецификации детально рассмотрены в курсе "Основы информационной безопасности" и в книге "Информационная безопасность - практический подход" [86]. Только по этой причине они не включены в настоящий курс в качестве предмета изучения.

Первым оценочным стандартом, получившим международное признание и оказавшим исключительно сильное влияние на последующие разработки в области информационной безопасности, стал стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем" (Department of Defense Trusted Computer System Evaliation Criteria, TCSEC, [41]), более известный (по цвету обложки) под названием "Оранжевая книга".

Без преувеличения можно утверждать, что в "Оранжевой книге" заложен понятийный базис ИБ. Достаточно лишь перечислить содержащиеся в нем понятия: безопасная и доверенная системы, политика безопасности, уровень гарантированности, подотчетность, доверенная вычислительная

база, монитор обращений, ядро и периметр безопасности. Исключительно важно и выделение таких аспектов политики безопасности, как добровольное (дискреционное) и принудительное (мандатное) управление доступом, безопасность повторного использования объектов. Последним по порядку, но отнюдь не по значению следует назвать принципы классификации по требованиям безопасности на основе параллельного ужесточения требований к политике безопасности и уровню гарантированности.

После "Оранжевой книги" была выпущена целая "Радужная серия". С концептуальной точки зрения, наиболее значимый документ в ней - "Интерпретация "Оранжевой книги" для сетевых конфигураций" (Trusted Network Interpretation, [71]). Он состоит из двух частей. Первая содержит собственно интерпретацию, во второй описываются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

Важнейшее понятие, введенное в первой части, - сетевая доверенная вычислительная база. Другой принципиальный аспект - учет динамичности сетевых конфигураций. Среди защитных механизмов выделена криптография, помогающая поддерживать как конфиденциальность, так и целостность.

Новым для своего времени стал систематический подход к вопросам доступности, формирование архитектурных принципов ее обеспечения.

Упомянем также достаточное условие корректности фрагментирования монитора обращений, являющееся теоретической основой декомпозиции распределенной ИС в объектно-ориентированном стиле в сочетании с криптографической защитой коммуникаций.

Переходя к знакомству с "Гармонизированными критериями Европейских стран", отметим отсутствие в них априорных требований к условиям, в которых должна работать информационная система. Предполагается, что сначала формулируется цель оценки, затем орган сертификации определяет, насколько полно она достигается, т. е. в какой мере корректны и эффективны архитектура и реализация механизмов безопасности в конкретной ситуации. Чтобы облегчить формулировку цели оценки, стандарт содержит описание десяти примерных классов функциональности, типичных для правительственных и коммерческих систем.

В "Гармонизированных критериях" подчеркивается различие между системами и продуктами информационных технологий, но для унификации требований вводится единое понятие - объект оценки.

Важно указание и на различие между функциями (сервисами) безопасности и реализующими их механизмами, а также выделение двух аспектов гарантированности - эффективности и корректности средств безопасности. Руководящие документы (РД) Гостехкомиссии России [13] начали появляться несколько позже, уже после опубликования "Гармонизированных критериев", и, по аналогии с последними, подтверждают разницу между автоматизированными системами (АС) и продуктами (средствами вычислительной техники, СВТ), но в общем и целом они долгое время следовали в фарватере "Оранжевой книги".

Первое примечательное отклонение от этого курса произошло в 1997 году, когда был принят РД по отдельному сервису безопасности - межсетевым экранам (МЭ) [18]. Его основная идея - классифицировать МЭ на основании осуществляющих фильтрацию потоков данных уровней эталонной семиуровневой модели - получила международное признание и продолжает оставаться актуальной.

В 2002 году Гостехкомиссия России приняла в качестве РД русский перевод [19] международного стандарта ISO/IEC 15408:1999 "Критерии оценки безопасности информационных технологий" [53], что послужило толчком для кардинальной и весьма своевременной со всех точек зрения переориентации (вспомним приведенный выше принцип стандартизации из закона "О техническом регулировании"). Конечно, переход на рельсы "Общих критериев" будет непростым, но главное, что он начался.

Среди технических спецификаций на первое место, безусловно, следует поставить документ X.800 "Архитектура безопасности для взаимодействия открытых систем" [78]. Здесь выделены важнейшие сетевые сервисы безопасности: аутентификация, управление доступом, обеспечение конфиденциальности и/или целостности данных, а также невозможность отказаться от совершенных действий. Для реализации сервисов предусмотрены следующие сетевые механизмы безопасности и их комбинации: шифрование, электронная цифровая подпись (ЭЦП), управление доступом, контроль целостности данных, аутентификация, дополнение трафика,

управление маршрутизацией, нотаризация. Выбраны уровни эталонной семиуровневой модели, на которых могут быть реализованы сервисы и механизмы безопасности. Наконец, детально рассмотрены вопросы администрирования средств безопасности для распределенных конфигураций.

Спецификация Internet-сообщества RFC 1510 "Сетевой сервис аутентификации Kerberos (V5)" [64] относится к более частной, но весьма важной и актуальной проблеме - аутентификации в разнородной распределенной среде с поддержкой концепции единого входа в сеть. Сервер аутентификации Kerberos представляет собой доверенную третью сторону, владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности. О весомости данной спецификации свидетельствует тот факт, что клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем. Далее предполагается, что читатель свободно разбирается в особенностях охарактеризованных выше стандартов и спецификаций.

Краткие аннотации подробно рассматриваемых в курсе стандартов и спецификаций

"Гармонизированные критерии Европейских стран" стали весьма передовым документом для своего времени, они подготовили появление международного стандарта ISO/IEC 15408:1999 "Критерии оценки безопасности информационных технологий" (Evaluation criteria for IT security) [53], в русскоязычной литературе обычно (но не совсем верно) именуемого "Общими критериями" (ОК).

На сегодняшний день "Общие критерии" - самый полный и современный оценочный стандарт. На самом деле, это метастандарт, определяющий инструменты оценки безопасности ИС и порядок их использования; он не содержит предопределенных классов безопасности. Такие классы можно строить, опираясь на заданные требования.

ОК содержат два основных вида требований безопасности:

функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям (сервисам) безопасности и реализующим их механизмам;

требования доверия, соответствующие пассивному аспекту; они предъявляются к технологии и процессу разработки и эксплуатации.

Требования безопасности формулируются, и их выполнение проверяется для определенного объекта оценки - аппаратно-программного продукта или информационной системы.

Подчеркнем, что безопасность в ОК рассматривается не статично, а в соответствии с жизненным циклом объекта оценки. Кроме того, последний предстает в контексте среды безопасности, характеризующейся определенными условиями и угрозами.

"Общие критерии" способствуют формированию двух базовых видов используемых на практике нормативных документов - это профиль защиты и задание по безопасности.

Профиль защиты представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса.

Задание по безопасности содержит совокупность требований к конкретной разработке, их выполнение позволит решить поставленные задачи по обеспечению безопасности.

В последующей части курса будут детально рассмотрены как сами "Общие критерии", так и разработанные на их основе профили защиты и проекты профилей.

Криптография - область специфическая, но общее представление о ее месте в архитектуре безопасности и о требованиях к криптографическим компонентам иметь необходимо. Для этого целесообразно ознакомиться с Федеральным стандартом США FIPS 140-2 "Требования безопасности для криптографических модулей" (Security Requirements for Cryptographic Modules) [44]. Он выполняет организующую функцию, описывая внешний интерфейс криптографического модуля, общие требования к подобным модулям и их окружению. Наличие такого стандарта упрощает разработку сервисов безопасности и профилей защиты для них.

Криптография как средство реализации сервисов безопасности имеет две стороны: алгоритмическую и интерфейсную. Нас будет интересовать исключительно интерфейсный аспект,

поэтому, наряду со стандартом FIPS 140-2, мы рассмотрим предложенную в рамках Internet-сообщества техническую спецификацию "Обобщенный прикладной программный интерфейс службы безопасности" (Generic Security Service Application Program Interface, GSS-API) [67].

Интерфейс безопасности GSS-API предназначен для защиты коммуникаций между компонентами программных систем, построенных в архитектуре клиент/сервер. Он создает условия для взаимной аутентификации общающихся партнеров, контролирует целостность пересылаемых сообщений и служит гарантией их конфиденциальности. Пользователями интерфейса безопасности GSS-API являются коммуникационные протоколы (обычно прикладного уровня) или другие программные системы, самостоятельно выполняющие пересылку данных.

Технические спецификации IPsec [IPsec] имеют, без преувеличения, фундаментальное значение, описывая полный набор средств обеспечения конфиденциальности и целостности на сетевом уровне. Для доминирующего в настоящее время протокола IP версии 4 они носят факультативный характер; в перспективной версии IPv6 их реализация обязательна. На основе IPsec строятся защитные механизмы протоколов более высокого уровня, вплоть до прикладного, а также законченные средства безопасности, в том числе виртуальные частные сети. Разумеется, IPsec существенным образом опирается на криптографические механизмы и ключевую инфраструктуру.

Точно так же характеризуются и средства безопасности транспортного уровня (Transport Layer Security, TLS) [42]. Спецификация TLS развивает и уточняет популярный протокол Secure Socket Layer (SSL), используемый в большом числе программных продуктов самого разного назначения.

В упомянутом выше инфраструктурном плане очень важны рекомендации X.500 "Служба директорий: обзор концепций, моделей и сервисов" (The Directory: Overview of concepts, models and services) [49] и X.509 "Служба директорий: каркасы сертификатов открытых ключей и атрибутов" (The Directory: Public-key and attribute certificate frameworks) [51]. В рекомендациях X.509 описан формат сертификатов открытых ключей и атрибутов - базовых элементов инфраструктур открытых ключей и управления привилегиями.

Как известно, обеспечение информационной безопасности - проблема комплексная, требующая согласованного принятия мер на законодательном, административном, процедурном и

программно-техническом уровнях. При разработке и реализации базового документа административного уровня - политики безопасности организации - отличным подспорьем может стать рекомендация Internet-сообщества "Руководство по информационной безопасности предприятия" (Site Security Handbook, см. [47], [45]). В нем освещаются практические аспекты формирования политики и процедур безопасности, поясняются основные понятия административного и процедурного уровней, содержится мотивировка рекомендуемых действий, затрагиваются темы анализа рисков, реакции на нарушения ИБ и действий после ликвидации нарушения. Более подробно последние вопросы рассмотрены в рекомендации "Как реагировать на нарушения информационной безопасности" (Expectations for Computer Security Incident Response) [33]. В этом документе можно найти и ссылки на полезные информационные ресурсы, и практические советы процедурного уровня.

При развитии и реорганизации корпоративных информационных систем, несомненно, окажется полезной рекомендация "Как выбирать поставщика Internet-услуг" (Site Security Handbook Addendum for ISPs) [40]. В первую очередь ее положений необходимо придерживаться в ходе формирования организационной и архитектурной безопасности, на которой базируются прочие меры процедурного и программно-технического уровней.

Для практического создания и поддержания режима информационной безопасности с помощью регуляторов административного и процедурного уровней пригодится знакомство с британским стандартом BS 7799 "Управление информационной безопасностью. Практические правила" (Code of practice for information security management) [31] и его второй частью BS 7799-2:2002 "Системы управления информационной безопасностью - спецификация с руководством по использованию" (Information security management systems - Specification with guidance for use) [32]. В нем разъясняются такие понятия и процедуры, как политика безопасности, общие принципы организации защиты, классификация ресурсов и управление ими, безопасность персонала, физическая безопасность, принципы администрирования систем и сетей, управление доступом , разработка и сопровождение ИС, планирование бесперебойной работы организации.

Можно видеть, что отобранные для курса стандарты и спецификации затрагивают все уровни информационной безопасности, кроме законодательного. Далее мы приступим к их детальному рассмотрению.

Программно-аппаратные средства обеспечения информационной безопасности

История создания и текущий статус "Общих критериев"

В 1990 году Рабочая группа 3 Подкомитета 27 Первого совместного технического комитета (JTC1/SC27/WG3) Международной организации по стандартизации (ISO) приступила к разработке "Критериев *оценки безопасности информационных технологий*" (Evaluation Criteria for IT Security, ECITS). Несколько позже, в 1993 году, правительственные организации шести североамериканских и европейских стран - Канады, США, Великобритании, Германии, Нидерландов и Франции - занялись составлением так называемых "*Общих критериев оценки безопасности информационных технологий*" (Common Criteria for IT Security Evaluation). За этим документом исторически закрепилось более короткое название - "***Общие критерии***", или ОК (Common Criteria, CC).

Рабочая группа ISO, возглавляемая представителем Швеции, функционировала на общественных началах и действовала весьма неторопливо, пытаясь собрать и увязать между собой мнения экспертов примерно из двух десятков стран, в то время как коллектив "Проекта ОК", финансируемый своими правительствами, несмотря на

первоначальное трехлетнее отставание, весьма быстро начал выдавать реальные результаты. Объяснить это нетрудно: в "Проекте ОК" требовалось объединить и развить всего три весьма продвинутых и близких по духу документа - "Гармонизированные критерии Европейских стран", а также "Канадские критерии оценки доверенных компьютерных *продуктов*" и "Федеральные критерии безопасности *информационных технологий*" (США). (Сами разработчики "*Общих критериев*" относят к числу первоисточников еще и "Оранжевую книгу".)

Как правило, круг людей, заседающих в комитетах и комиссиях по информационной безопасности, довольно узок, поэтому нет ничего удивительного в том, что одни и те же представители стран (в частности, США и Великобритании) входили в обе группы разработчиков. Естественно, в таких условиях между коллективом "Проекта ОК" и Рабочей группой 3 установилось тесное взаимодействие. Практически это означало, что группа WG3 стала бесплатным приложением к "Проекту ОК", а сами "*Общие критерии*" автоматически должны были получить статус не межгосударственного, а *международного стандарта*.

В ОС Unix есть утилита tee, создающая ответвления каналов путем копирования стандартного вывода в файлы и довольно точно моделирующая взаимоотношения между коллективом "Проекта ОК" и группой WG3. С 1994 года ранние версии ОК становятся рабочими проектами WG3. В 1996 году появилась версия 1.0 "*Общих критериев*", которая, помимо публикации в Internet для всеобщего свободного доступа, была одобрена ISO и обнародована в качестве Проекта Комитета.

Широкое открытое обсуждение документа и "опытная эксплуатация" привели к его существенной переработке и выходу версии 2.0 ОК в мае 1998 года. Разумеется, эксперты WG3 не могли ее не отредактировать. Их замечания были учтены в версии 2.1 ОК 34-[36], принятой в августе 1999 года. Соответствующий *международный стандарт* ISO/IEC 15408-1999 53-[55] введен в действие с 1 декабря 1999 года. Таким образом, фактически стандарт ISO/IEC 15408-1999 и версия 2.1 ОК совпадают, а если пренебречь описываемыми ниже нюансами, их названия могут считаться взаимозаменяемыми. Однако, строго говоря, "Критерии *оценки безопасности информационных технологий*" и "*Общие критерии оценки безопасности информационных технологий*" - разные документы, поскольку выпущены под эгидой разных организаций, руководствующихся разными правилами распространения и обновления.

ISO не предоставляет свободный доступ к своим стандартам, они относительно статичны, поскольку их обновляют или подтверждают один раз в пять лет (какие-либо

изменения в стандарте ISO/IEC 15408 можно ожидать в 2004 году). Напротив, портал "Проекта ОК" (http://www.commoncriteria.org) открыт для всех желающих, а разработчики "*Общих критериев*" постоянно предлагают и принимают изменения, уточнения, интерпретации отдельных положений и готовят третью версию своего документа. Поэтому, с формальной точки зрения, *международный стандарт* ISO/IEC 15408-1999 по-русски правильнее сокращенно именовать КОБИТ, а не ОК. (Правда, велика вероятность, что рабочая группа ISO любезно согласится и дальше пользоваться плодами "Проекта ОК", естественно, внося в них свои редакторские правки...)

Уточним, что далее, в рамках этой темы, мы будем иметь в виду именно "*Общие критерии*", а не стандарт ISO.

С целью унификации процедуры сертификации по "*Общим критериям*" в августе 1999 года была опубликована "Общая *методология оценки*безопасности *информационных технологий*" (Common Methodology for Information Technology Security Evaluation) [37], описывающая минимальный набор действий при проведении оценки. "Проект ОК" с самого начала носил не только технический, но и экономико-политический характер. Его цель состояла, в частности, в том, чтобы упростить, удешевить и ускорить выход сертифицированных изделий*информационных технологий* (ИТ) на мировой рынок. Для этого в мае 2000 года уполномоченные правительственные организации шести стран-основателей "Проекта ОК", а также Австралии и Новой Зеландии, Греции, Италии, Испании, Норвегии, Финляндии и Швеции подписали ***соглашение "О признании*** *сертификатов* по *Общим критериям* в области безопасности *информационных технологий*" (позднее к нему присоединились Австрия и Израиль).

Участие в соглашении предполагает соблюдение двух независимых условий: признание *сертификатов*, выданных соответствующими органами других стран-участниц, а также возможность осуществления подобной сертификации. Очевидно, от взаимного признания*сертификатов* выигрывают не только производители, но и потребители *изделий ИТ*. Что же касается их выдачи, то соглашение предусматривает жесткий контроль при получении и подтверждении этого права (например, предусмотрено проведение так называемых теневых сертификационных испытаний под контролем независимых экспертов). Таким образом, для полноценного участия в соглашении, помимо желания, государство должно располагать органами сертификации с достаточными ресурсами и штатом специалистов, квалификация которых получила официальное международное признание. По данным на конец 2002 года, правом

выдачи *сертификатов*, признаваемых участниками соглашения, обладали Австралия и Новая Зеландия, Великобритания, Германия, Канада, США и Франция.

К началу 2003 года *сертификаты* по "*Общим критериям*" получили около семидесяти разнообразных *изделий ИТ* ведущих производителей: операционные *системы*, *системы* управления базами данных, межсетевые экраны, коммуникационные средства, интеллектуальные карты и т.п.; еще почти сорок находились в процессе сертификации.

Определяя статус "*Общих критериев*" в России, следует отметить, что отечественные специалисты с самого начала внимательно следили за этим проектом, публиковали аналитические обзоры и переводы (см., например, [JI981K]). В 1999 году была организована работа по подготовке *российского стандарта* и *Руководящего документа* (РД) Гостехкомиссии России на основе аутентичного перевода ОК. Она велась в тесном контакте с зарубежными коллегами и успешно завершена в 2002 году. Именно тогда был официально издан ГОСТ Р ИСО/МЭК 15408-2002 "Критерии *оценки безопасности информационных технологий*" 10-[12] с датой введения в действие 1 января 2004 года. А пока положение регулируется РД Гостехкомиссии России [19], который, как и "*Общие критерии*", по замыслу разработчиков, должен быть динамичнее стандарта, модифицируясь вместе с ОК.

Российские специалисты - активные участники "Проекта ОК", они вносят предложения по доработке "*Общих критериев*", выступают с докладами на конференциях, ведут научно-исследовательские работы, внедряют ОК в практику различных организаций. Следующим логичным шагом стало бы присоединение России к соглашению "О признании *сертификатов*".

Основные понятия и идеи "Общих критериев"

Основным свойством, которым должны обладать действительно *общие критерии оценки безопасности информационных технологий*, является универсальность. Следовательно, они не должны содержать априорных предположений об *объекте оценки*. В ОК данное условие выполнено: под ***объектом оценки*** (ОО) понимается аппаратно-программный *продукт* или информационная *система* с соответствующей документацией.

Система - это специфическое воплощение *информационных технологий* с конкретным назначением и условиями эксплуатации.

Продукт, согласно ОК, есть совокупность средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные *системы*. В качестве собирательного термина для *систем* и *продуктов*применяют словосочетание "***изделие ИТ***". Оно может быть как уже существующим, так и проектируемым. В первом случае - доработано по результатам оценки, во втором - сама перспектива подобного контроля способна дисциплинировать разработчиков; так или иначе проведение оценки должно оказать положительное влияние на безопасность ОО.

Объект оценки рассматривается в определенном контексте - ***среде безопасности***, в которую включаются все, что имеет отношение к его безопасности, а именно:

- законодательная среда - законы и нормативные акты, затрагивающие ОО;
- административная среда - положения политик и программ безопасности, учитывающие особенности ОО;
- процедурная среда - физическая среда ОО и меры физической защиты, персонал и его свойства (знания, опыт и т.п.), принятые эксплуатационные и иные процедуры;
- программно-техническая среда - предназначение *объекта оценки* и предполагаемые области его применения, активы (ресурсы), которые требуют защиты средствами ОО.

Дальнейший этап технологического цикла подготовки к оценке, согласно "*Общим критериям*", - описание следующих аспектов среды ОО:

- ***предположения безопасности***. Они выделяют *объект оценки* из общего контекста, задают границы рассмотрения. Истинность этих предположений принимается без доказательства, а из множества возможных отбирается только то, что заведомо необходимо для обеспечения безопасности ОО;
- ***угрозы безопасности*** ОО, наличие которых в рассматриваемой среде установлено или предполагается. Они характеризуются несколькими параметрами: источник, метод воздействия, опасные с точки зрения злонамеренного использования уязвимости, ресурсы (активы), потенциально подверженные повреждению. При анализе рисков принимаются во внимание вероятность активизации угрозы и ее успешного осуществления, а также размер возможного ущерба. По результатам анализа из множества допустимых угроз отбираются только те, ущерб от которых нуждается в уменьшении;

- положения *политики безопасности*, предназначенные для применения к *объекту оценки*. Для *системы* ИТ такие положения могут быть описаны точно, для *продукта* - в общих чертах.

На основании предположений, при учете угроз и положений *политики безопасности* формулируются *цели безопасности* для *объекта оценки*, направленные на обеспечение противостояния угрозам и выполнение *политики безопасности*. В зависимости от непосредственного отношения к ОО или к среде они подразделяются на две группы. Часть целей для среды может достигаться нетехническими (процедурными) мерами. Все остальные (для объекта и среды) носят программно-технический характер. Для их достижения к объекту и среде предъявляются *требования безопасности*.

"*Общие критерии*" в главной своей части как раз и являются каталогом (библиотекой) *требований безопасности*. Спектр стандартизованных требований чрезвычайно широк - это необходимое условие универсальности ОК. Высокий уровень детализации делает их конкретными, допускающими однозначную проверку, что важно для обеспечения повторяемости результатов оценки. Наличие параметров обусловливает гибкость требований, а дополнительную возможность ее достижения (через расширяемость) привносит использование нестандартных (не входящих в каталог ОК) требований.

Для структуризации пространства требований в "*Общих критериях*" введена иерархия *класс-семейство-компонент-элемент*.

Классы определяют наиболее общую (как правило, предметную) группировку требований.

Семейства в пределах *класса* различаются по строгости и другим характеристикам требований.

Компонент - минимальный набор требований, фигурирующий как целое.

Элемент - неделимое требование.

Между *компонентами* могут существовать зависимости. Они возникают, когда *компонент* сам по себе недостаточен для достижения *цели безопасности*. Соответственно, при включении такого *компонента* необходимо добавить всю "гроздь" его зависимостей.

"*Общие критерии*" содержат два основных вида ***требований безопасности***:

- ***функциональные***, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности ОО и реализующим их механизмам;
- ***требования доверия***, которые соответствуют пассивному аспекту, предъявляются к технологии и процессу разработки и эксплуатации ОО.

Библиотека *функциональных требований* составляет вторую часть "*Общих критериев*", а каталог *требований доверия* - третью (первая часть содержит изложение основных концепций ОК).

Сформулировав *функциональные требования*, *требования доверия* и требования к среде, можно приступать к *оценке безопасности*готового *изделия ИТ*. Для типовых изделий "*Общие критерии*" предусматривают разработку типовых совокупностей *требований безопасности*, называемых ***профилями защиты*** (ПЗ).

Для проектируемого изделия за выработкой требований следует разработка *краткой спецификации*, входящей в *задание по безопасности*(ЗБ).

(Как вспомогательный *элемент*, упрощающий создание *профилей защиты* и *заданий по безопасности*, могут применяться***функциональные пакеты*** (ФП) - неоднократно используемые совокупности *компонентов*, объединенных для достижения установленных*целей безопасности*.)

Краткая спецификация определяет отображение требований на функции безопасности (ФБ). "*Общие критерии*" не предписывают конкретной методологии или дисциплины разработки *изделий ИТ*, но предусматривают наличие нескольких уровней представления проекта с его декомпозицией и детализацией. За *требованиями безопасности* следует *функциональная спецификация*, затем *проект верхнего уровня*, необходимое число промежуточных уровней, *проект нижнего уровня*, после этого, в зависимости от типа изделия, исходный код или схемы аппаратуры и, наконец, *реализация* в виде исполняемых файлов, аппаратных *продуктов* и т.п. Между уровнями представления должно демонстрироваться соответствие, то есть все сущности более высоких уровней обязаны фигурировать и "ниже", а "внизу" нет места лишним сущностям, не обусловленным потребностями более высоких уровней.

При проведении оценки *изделия ИТ* главными являются следующие вопросы:

- отвечают ли функции безопасности ОО *функциональным требованиям*?
- корректна ли *реализация* функций безопасности?

Если оба ответа положительны, можно говорить о достижении *целей безопасности*.

Основные понятия и идеи "Общей методологии оценки безопасности информационных технологий"

"Общая методология *оценки безопасности информационных технологий*" - второй по важности документ (после "*Общих критериев*"), подготовленный в рамках "Проекта ОК". Основная цель "Общей методологии" - добиться объективности, повторяемости и воспроизводимости результатов оценки.

Следуя принципам структурной декомпозиции, разработчики выделили в процессе оценки три задачи (этапа):

- *входная задача;*
- *задача оценки;*
- *выходная задача.*

Входная задача имеет дело с представленными для оценки свидетельствами (далее для краткости мы будем именовать их свидетельствами оценки). Ее назначение - убедиться, что версии свидетельств корректны и должным образом защищены.

Обычно для оценки представляются стабильные, официально выпущенные версии свидетельств, однако в ситуациях, когда оценка ведется параллельно разработке или доработке ОО, возможно предъявление рабочих версий. Оценщику вместе со спонсором этого процесса необходимо составить каталог и в дальнейшем производить конфигурационный контроль версий. Он обязан обеспечить защиту свидетельств от изменения и утери, а по окончании процесса оценки возвратить их, поместить в архив или уничтожить.

На всех этапах оценки должна обеспечиваться конфиденциальность.

Задача оценки в общем случае разбивается на следующие подзадачи:

- оценка *задания по безопасности*;
- оценка управления конфигурацией ОО;
- оценка документации по передаче ОО потребителю и эксплуатационной документации;
- оценка документации разработчиков;
- оценка руководств;
- оценка поддержки жизненного цикла ОО;
- оценка тестов;
- тестирование;

- оценка анализа уязвимостей.

Нередко проводятся выборочные проверки, когда вместо всего (относительно однородного) множества свидетельств анализируется представительное подмножество, что позволяет сэкономить ресурсы при сохранении необходимого уровня доверия безопасности. Размер выборки должен быть обоснован математически и экономически, но при анализе *реализации* объекта оценки он должен составлять не менее 20%.

Ошибки, обнаруженные при выборочной проверке, подразделяются на систематические и случайные. После исправления систематической ошибки необходимо произвести новую выборку; после случайной этого не требуется.

Допускается выборочная проверка доказательств, тестов, результатов анализа скрытых каналов, выполнения требований к содержанию и представлению свидетельств, выборочное тестирование.

В остальных ситуациях такой способ можно применять только в исключительных случаях, когда полная проверка требует слишком много ресурсов по сравнению с другими действиями в процессе оценки или когда она не существенно увеличивает доверие безопасности. При этом необходимо обосновать допустимость и целесообразность выборочного подхода.

В "Общей методологии" специально подчеркивается, что сами по себе большие размеры и высокая сложность *объекта оценки* не оправдывают замены полных проверок выборочными, поскольку для оценки безопасности подобных объектов заведомо требуется много сил и средств.

Необходимый элемент оценки - проверка внутренней согласованности каждого из представленных свидетельств, а также внешней взаимной согласованности различных свидетельств.

Внутренняя согласованность проверяется в первую очередь для сущностей, имеющих несколько представлений: для спецификаций и проектов всех уровней, а также для руководств.

Проверка внешней согласованности производится для описаний функций, параметров безопасности, процедур и событий, связанных с безопасностью, поскольку эти описания могут содержаться в разных документах.

Внутренняя несогласованность высокоуровневых сущностей может иметь глобальные последствия для процесса оценки. Например, выявление противоречий в целях заставляет заново проанализировать требования и функции безопасности.

Разные подзадачи в процессе оценки могут выполняться в произвольном порядке или параллельно, однако существуют зависимости, накладывающие некоторые ограничения на очередность выполнения. Наиболее очевидное из них состоит в том, что анализ *задания по безопасности* должен выполняться до каких бы то ни было проверок *объекта оценки*.

Задание по безопасности среди других характеристик *объекта оценки* определяет его границы и спектр рассматриваемых угроз. Следовательно, процесс и результат оценки одного и того же *продукта* в сочетании с разными заданиями могут быть разными. Например, если в нем содержатся средства межсетевого экранирования и поддержки виртуальных частных сетей (ВЧС), но в *задании по безопасности* предусмотрена исключительно защита внутренней сети от внешних угроз, то свойства ВЧС-функций важны лишь в контексте возможности обхода средств экранирования. Даже если ВЧС-функции не обеспечивают конфиденциальности сетевых потоков данных, *продукт* с таким заданием получит положительную оценку.

(Заметим, что набор проверяемых требований необходим при сертификации не только по "*Общим критериям*". Нередко производитель в рекламных целях ограничивается кратким "*продукт* сертифицирован", что, по сути, бессодержательно и может ввести в заблуждение потребителя, так как зачастую означает соответствие каким-либо условиям общего характера, вроде отсутствия недекларированных возможностей.)

Важным моментом, обычно вызывающим много вопросов, является анализ уязвимостей и *стойкости функций безопасности*.

Цель обоих видов проверки заключается в выявлении степени устойчивости *объекта оценки* по отношению к атакам, выполняемым нарушителем с определенным (низким, умеренным или высоким) *потенциалом нападения*.

Анализ уязвимостей применяется ко всем функциям безопасности; при этом не делается каких-либо предположений относительно корректности их *реализации*, сохранения целостности, возможности обхода и т.п.

Анализу стойкости подвергаются только функции безопасности, реализованные с помощью вероятностных или перестановочных механизмов, у которых и проверяется

стойкость - базовая, средняя или высокая (базовая означает защищенность от нарушителя с низким*потенциалом нападения*). В принципе, все вероятностные функции можно считать уязвимыми, а подобный анализ классифицировать как анализ уязвимостей специального вида.

Для успешного нападения необходимо сначала идентифицировать, а затем использовать некоторую уязвимость. Оба действия оцениваются с точки зрения временных затрат, необходимой квалификации, уровня знаний об ОО, характера и продолжительности доступа к ОО, необходимых аппаратно-программных и иных ресурсов.

Перечисленные составляющие не являются независимыми. Высокая квалификация может сэкономить время, а специальное оборудование - упростить и ускорить доступ к ОО. Следовательно, если оценивать каждый параметр количественно, то результирующую функцию, характеризующую серьезность уязвимости, естественно сделать аддитивной.

В таблицах 2.1 - 2.5 содержатся условные баллы, присваиваемые параметрам уязвимости в зависимости от того, в какой диапазон или на какой уровень они попадают. Для получения общего рейтинга нужно выбрать по одному значению из обоих числовых столбцов всех таблиц и сложить эти десять чисел. При оценке *стойкости функций безопасности* фаза идентификации не рассматривается (предполагается, что уязвимость известна), поэтому достаточно выбрать и сложить пять чисел из последних столбцов.

Таблица 2.1. Условные баллы, присваиваемые уязвимости в зависимости от времени, которое понадобится для ее идентификации и использования.

Диапазон

Идентификация уязвимости

Использование уязвимости

< 0.5 часа

0

0

< суток

2

3

< месяца

3

5

> месяца

5

8

Таблица 2.2. Условные баллы, присваиваемые уязвимости в зависимости от уровня квалификации, необходимого для ее идентификации и использования.

Уровень

Идентификация уязвимости

Использование уязвимости

Любитель

0

0

Специалист

2

2

Эксперт

5

4

Таблица 2.3. Условные баллы, присваиваемые уязвимости в зависимости от уровня знаний об объекте оценки, необходимого для ее идентификации и использования.

Уровень

Идентификация уязвимости

Использование уязвимости

Отсутствие знаний

0

0

Общедоступные знания

2

2

Конфиденциальные сведения

5

4

Таблица 2.4. Условные баллы, присваиваемые уязвимости в зависимости от времени доступа к объекту оценки, требуемого для ее идентификации и использования.

Диапазон

Идентификация уязвимости

Использование уязвимости

< 0.5 часа или доступ незаметен

0

0

< суток

2

4

< месяца

3

6

> месяца

4

9

Таблица 2.5. Условные баллы, присваиваемые уязвимости в зависимости от аппаратно-программных и иных ресурсов (оборудования), необходимых для ее идентификации и использования.

Уровень

Идентификация уязвимости

Использование уязвимости

Отсутствие оборудования

0

0

Стандартное оборудование

1

2

Специальное оборудование

3

4

Заказное оборудование

5

6

Если уязвимость можно идентифицировать и/или использовать несколькими способами, для каждого из них вычисляется рейтинг и из полученных значений выбирается минимальное, то есть уязвимость характеризуется самым простым методом успешного нападения.

В табл. 2.6 приведены диапазоны рейтинга, которые характеризуют *стойкость функции безопасности*.

Таблица 2.6. Диапазоны рейтинга, характеризующие стойкость функции безопасности.

Диапазон

Стойкость функции безопасности

10 - 17

Базовая

18 - 24

Средняя

> 24

Высокая

Согласно "Общей методологии", *потенциал нападения* оценивается в общем и целом по той же схеме, что и степень риска от наличия уязвимостей, с некоторыми очевидными отличиями (например, из нескольких сценариев нападения выбирается худший, с наибольшим потенциалом). Считается, что он является функцией уровня мотивации злоумышленника, его квалификации и имеющихся ресурсов. Мотивация влияет на выделяемое на атаки время и, возможно, на привлекаемые ресурсы и подбор нападающих.

В табл. 2.7 приведены диапазоны рейтинга, иллюстрирующие определенный *потенциал нападения*.

Таблица 2.7. Диапазоны рейтинга, характеризующие потенциал нападения.

Диапазон

Потенциал нападения

< 10

Низкий

10 - 17

Умеренный

18 - 24

Высокий

> 24

Нереально высокий

Нападение может быть успешным, только если его потенциал не меньше *рейтинга уязвимости*. Отсюда следует, в частности, что уязвимости с рейтингом выше 24 устойчивы к нападению с высоким потенциалом, поэтому их практическое использование злоумышленниками представляется нереальным.

Отметим, что потенциал предполагаемых нападений на ОО выявляется дважды: при анализе *задания по безопасности* для выбора надлежащих мер противодействия и при анализе уязвимостей для определения достаточности выбранных мер и качества их *реализации*.

Рассмотрим пример анализа *стойкости функции безопасности*. Пусть доступ к информационной *системе* осуществляется посредством территориально разнесенных терминалов, работа за которыми не контролируется. Авторизованные пользователи проходят аутентификацию путем введения паролей, состоящих из четырех различных цифр. Если пароль введен неверно, терминал блокируется на одну минуту. Требуется оценить стойкость такой парольной защиты для заданного пользователя с известным нападающему входным именем. Для нападения выбран один терминал, временем ввода можно пренебречь.

Очевидно, число возможных парольных последовательностей составляет

```
10*9*8*7 = 5040
```

Для успешного подбора пароля методом полного перебора требуется примерно 2520 попыток, которые можно произвести за 42 часа, что больше суток, но меньше месяца. Никакой квалификации, знаний и/или оборудования для этого не нужно. Следовательно, чтобы определить стойкость функции, достаточно сложить два числа: 5 из табл. 2.1 и 6 из табл. 2.4. Сумма 11 позволяет сделать вывод, что данная функция безопасности обладает базовой стойкостью и является устойчивой к нападению с низким потенциалом.

Возвращаясь к трем основным задачам процесса оценки, рассмотрим последнюю, *выходную задачу*. Ее цель - сформулировать замечания и получить *технический отчет оценки*.

Текст с замечаниями не является обязательным. Он нужен, если в процессе оценки выявились какие-либо неясности или проблемы.

Технический отчет оценки - это главный выходной документ, от качества которого во многом зависит повторяемость и воспроизводимость результатов оценки, т. е. возможность их многократного использования. "Общая методология" предписывает следующую структуру подобных отчетов:

- введение;
- архитектурное (высокоуровневое) описание *объекта оценки* с рассмотрением основных *компонентов*;
- описание процесса оценки, примененных методов, методологий, инструментальных средств и стандартов;
- представление результатов оценки;
- выводы и рекомендации;
- список представленных свидетельств;
- список сокращений, словарь терминов;
- список замечаний.

Изучение "Общей методологии" полезно не только оценщикам, но и разработчикам, так как дает представление о вопросах, которые могут возникать в процессе оценки. К сожалению, более детальное рассмотрение этого документа выходит за рамки настоящего курса.

Программно-аппаратные средства обеспечения информационной безопасности

◄ Предыдущий элемент курса

Классификация функциональных требований безопасности

Часть 2 "Общих критериев", представляющая собой весьма обширную *библиотеку функциональных требований безопасности*, описывает 11*классов*, 66 *семейств*, 135 *компонентов* и содержит сведения о том, какие цели безопасности могут быть достигнуты при современном уровне информационных технологий и каким образом.

Аналогия между *библиотекой функциональных требований безопасности* и библиотекой программных модулей является в данном случае довольно полной. Функциональные *компоненты* могут быть не до конца конкретизированы, поэтому фактические параметры подставляются не в самих "Общих критериях", а в определенных профилях защиты, заданиях по безопасности и функциональных пакетах. (Правда, в ГОСТ Р ИСО/МЭК 15408-2002 *параметризация* не очень удачно названа "назначением".) В качестве параметров могут выступать весьма сложные сущности, такие, например, как политика безопасности (ПБ).

Некоторые функциональные *компоненты* "Общих критериев" задаются "с запасом", в них включается список возможностей, из которых затем с помощью соответствующей операции выбирается только то, что нужно в конкретной ситуации. Пример - обнаружение и/или предотвращение определенных нарушений политики безопасности. На программистском языке подобный отбор называется частичным применением.

Разумеется, любой функциональный *компонент* допускает многократное использование (например, чтобы охватить разные аспекты объекта оценки), называемое в

ОК ***итерацией***, а также *уточнение* и добавление дополнительных деталей (последнее можно считать еще одной формой частичного применения).

Между *компонентами функциональных требований*, как и между привычными библиотечными функциями, могут существовать зависимости. Они возникают, когда *компонент* не является самодостаточным и для своей реализации нуждается в привлечении других*компонентов*. Очевидно, размещая в ПЗ, ЗБ или ФП подобный *компонент*, нужно включить туда и всю гроздь зависимостей (это похоже на разрешение внешних ссылок при формировании выполняемого модуля).

Классы функциональных требований "Общих критериев" можно разделить в зависимости от того, описывают ли они элементарные сервисы безопасности или производные, реализуемые на основе элементарных, направлены ли они на достижение высокоуровневых целей безопасности или играют инфраструктурную роль.

К первой группе относятся следующие *классы*:

- FAU - *аудит безопасности* (описывает требования к сервису протоколирования/аудита);
- FIA - *идентификация*/*аутентификация*;
- FRU - *использование ресурсов* (прежде всего - обеспечение отказоустойчивости).

Классы второй группы:

- FCO - связь (обслуживает *неотказуемость* отправителя/получателя);
- FPR - *приватность*;

Достичь высокоуровневых целей безопасности помогают два *класса*:

- FDP - защита данных пользователя;
- FPT - защита функций безопасности объекта оценки.

Наиболее многочисленны *классы*, играющие инфраструктурную роль:

- FCS - *криптографическая поддержка* (обслуживает управление криптографическими ключами и *криптографические операции*);
- FMT - *управление безопасностью*;
- FTA - доступ к объекту оценки (управление сеансами работы пользователей);
- FTP - *доверенный маршрут*/*канал*.

Приведенная классификация содержит несколько примечательных моментов. Во-первых, *функциональные требования* ОК довольно разнородны. Трудно объяснить, например, почему протоколированию/аудиту соответствует собственный *класс*, а такой важнейший, без преувеличения, классический сервис безопасности, как *управление доступом*, "спрятан" среди других требований защиты данных пользователя.

Во-вторых, в ОК не выделены архитектурные требования. Правда, некоторые весьма важные архитектурные *компоненты*, в числе которых - посредничество при обращениях (частный случай невозможности обхода защитных средств) и *разделение доменов*, вошли в *класс* FPT (защита функций безопасности).

В-третьих, требования для защиты данных пользователя и функций безопасности объекта оценки разделены, хотя, очевидно, в обоих случаях необходимо применять сходные механизмы. Возможно, такой подход объясняется желанием выделить ядро безопасности и сохранить его компактность.

Далее мы кратко рассмотрим все 11 *классов функциональных требований безопасности* "Общих критериев".

Классы функциональных требований, описывающие элементарные сервисы безопасности

В этом разделе рассматриваются три *класса функциональных требований безопасности*:

- FAU - *аудит безопасности*;
- FIA - *идентификация*/*аутентификация*;
- FRU - *использование ресурсов*.

Класс FAU состоит из шести *семейств*, содержащих требования к отбору, протоколированию (регистрации), хранению и анализу данных о действиях и событиях, затрагивающих безопасность объекта оценки.

Семейство FAU_GEN (*генерация данных аудита безопасности*) включает два *компонента*. Первый, FAU_GEN.1 (генерация данных аудита), специфицирует потенциально подвергаемые протоколированию и аудиту события, вводит понятие уровня протоколирования (минимальный, базовый, детализированный, неопределенный), определяет минимум регистрационных данных о событии (дата, время, тип, результат события, а также идентификатор субъекта). Второй, FAU_GEN.2 (ассоциация идентификатора пользователя), предписывает ассоциировать каждое

потенциально регистрируемое событие с идентификатором пользователя, его инициирующего.

Семейство FAU_SEL (*выбор событий аудита безопасности*) определяет требования к средствам отбора (включения или исключения) событий из числа потенциально регистрируемых, которые будут реально протоколироваться и подвергаться аудиту в процессе функционирования объекта оценки. Отбор может производиться на основе таких атрибутов, как идентификаторы объекта, пользователя, субъекта, узла сети или тип события. Предусматривается задание дополнительных атрибутов.

Семейство FAU_STG (*хранение событий аудита безопасности*) содержит две пары *компонентов*. Первая, FAU_STG.1 (защищенное хранение журнала аудита) и FAU_STG.2 (гарантии доступности данных аудита), специфицирует защиту регистрационного журнала от несанкционированного удаления, модификации, а также от повреждения регистрационных данных при его переполнении, сбое или атаке. Вторая пара, FAU_STG.3 (действия в случае возможной потери данных аудита) и FAU_STG.4 (предотвращение потери данных аудита), определяет последовательность действий, если объем информации в регистрационном журнале превышает заранее заданный порог. В их число входят игнорирование и своевременное запрещение протоколируемых событий, запись поверх самых старых регистрационных данных и т.д.

Семейство FAU_SAR (*просмотр аудита безопасности*) предоставляет право на чтение (полное или выборочное, на основе критериев с логическими отношениями) регистрационного журнала уполномоченным пользователям и запрет на доступ к журналу для прочих пользователей.

Семейство FAU_SAA (*анализ аудита безопасности*) устанавливает требования к средствам автоматического анализа функционирования объекта оценки, позволяющим выявлять возможные нарушения безопасности. Базовым *компонентом семейства* является FAU_SAA.1 (анализ потенциального нарушения), регламентирующий применение набора правил, основанных на накоплении или объединении событий, сигнализирующих о вероятном нарушении безопасности. В рамках *семейства* этот *компонент* усилен по двум направлениям. В FAU_SAA.2 (выявление аномалий, опирающееся на профиль) вводится понятия профиля поведения, рейтинга подозрительной активности для каждого пользователя, чьи действия отражены в профиле, а также порога, превышение которого указывает на ожидаемое нарушение политики безопасности. FAU_SAA.3 (простая эвристика атаки) и FAU_SAA.4 (сложная эвристика атаки) содержит понятие сигнатуры атаки (разной

степени сложности) и специфические функции выявления сигнатур в реальном масштабе времени.

Шестое *семейство класса* FAU - FAU_ARP (*автоматическая реакция аудита безопасности*) - определяет действия, которые необходимо предпринять при выявлении возможных нарушений безопасности. Действия эти характеризуются как "наименее разрушительные".

Можно сделать вывод, что в "Общих критериях" нашли отражение такие важные достижения относительно недавнего прошлого, как разработка и применение методов активного аудита.

Шесть *семейств класса* FIA (*идентификация*/*аутентификация*) содержат требования к функциям установления и проверки подлинности заявленного идентификатора пользователя, а также связывания атрибутов безопасности с уполномоченным пользователем.

Семейство FIA_UID (*идентификация* пользователя) включает два *компонента* и определяет набор действий (например, получение справочной информации), которые разрешается выполнять до идентификации. Обычно применяют более сильный *компонент* FIA_UID.2 -*идентификация* до любых действий, выполняемых пользователем при посредничестве функций безопасности.

Семейство FIA_UAU (*аутентификация пользователя*) устроено сложнее. Оно специфицирует типы механизмов аутентификации и используемые при этом атрибуты. Два первых *компонента*, FIA_UAU.1 (выбор момента аутентификации) и FIA_UAU.2 (*аутентификация* до любых действий пользователя), играют (применительно к аутентификации) ту же роль, что и *компоненты семейства* FIA_UID. На реализацию надежной аутентификации, устойчивой к сетевым угрозам, направлены *компоненты* FIA_UAU.3 (*аутентификация*, защищенная от подделок), FIA_UAU.4 (*механизмы одноразовой аутентификации*) и FIA_UAU.5 (*сочетание механизмов аутентификации*). После периода неактивности пользователя и в ряде других ситуаций уместно применение *компонента* FIA_UAU.6 (повторная *аутентификация*). Наконец, FIA_UAU.7 (аутентификация с защищенной обратной связью) указывает, как отображать пароль при вводе.

Семейство FIA_ATD (*определение атрибутов пользователя*) предусматривает наличие у пользователей не только идентификаторов, но и других атрибутов безопасности, предписываемых политикой безопасности.

Обычно после успешной идентификации и аутентификации от имени пользователя начинает действовать некий процесс (субъект).*Семейство* FIA_USB (*связывание пользователь-субъект*) содержит требования по ассоциированию атрибутов безопасности пользователя с этим субъектом.

Выявлением и реагированием на неудачи аутентификации ведает *семейство* FIA_AFL (*отказы аутентификации*). Разумеется, и число допустимых неудачных попыток, и действия, выполняемые при превышении порога неудач, - все это параметры единственного *компонентасемейства*.

Обычно пользователь доказывает свою подлинность, сообщая нечто, что знает только он (**"секрет"** в терминологии ОК). *Семейство*FIA_SOS (спецификация секретов) вводит понятие метрики качества секретов и содержит требования к средствам проверки качества и генерации секретов заданного качества. Примеры подобных средств - проверка выполнения технических ограничений на пользовательские пароли в ОС Unix и программные генераторы паролей.

В целом *класс* FIA, по сравнению с FAU, менее конкретен, его *компоненты* слишком параметризованы. Вероятно, это связано с тем, что криптография, без которой надежная и удобная для пользователя *аутентификация* невозможна, находится вне рамок "Общих критериев".

Класс FRU (*использование ресурсов*) включает три *семейства*, призванные разными способами поддерживать высокую доступность.

Выполнение требований *семейства* FRU_FLT (*отказоустойчивость*) должно обеспечить корректную работу всех или хотя бы некоторых функций объекта оценки даже в случае сбоев.

FRU_PRS (*приоритет обслуживания*) регламентирует действия по защите высокоприоритетных операций от препятствий или задержек со стороны операций с более низким приоритетом.

Семейство FRU_RSA (*распределение ресурсов*) для достижения высокой доступности ресурсов привлекает механизм *квот*.

Обращение к вопросу высокой доступности - несомненное достоинство "Общих критериев", которое, к сожалению, несколько проигрывает из-за отсутствия системного подхода. По неясным причинам в качестве сущностей одного уровня выделен один из

трех высокоуровневых аспектов доступности и два механизма, способствующих ее поддержанию.

За пределами рассмотрения остались надежность и обслуживаемость, да и *отказоустойчивость* может достигаться очень разными способами - от использования многопроцессорных конфигураций до организации резервных вычислительных центров.

Помимо двух рассмотренных механизмов поддержания доступности существуют и другие, не менее важные, например, балансировка загрузки, проактивное управление и т.п. На наш взгляд, было бы целесообразным обобщить требования к доступности регистрационного журнала (см. выше *семейство* FAU_STG) на случай произвольных ресурсов.

Отметим также, что включение в *класс* FRU конкретных механизмов еще резче обозначает излишнюю обобщенность требований *класса*FIA.

Классы функциональных требований, описывающие производные сервисы безопасности

Мы приступаем к рассмотрению двух следующих *классов функциональных требований безопасности*:

- FCO - связь;
- FPR - *приватность*.

Класс FCO состоит из двух *семейств*, FCO_NRO и FCO_NRR, ведающих *неотказуемостью* (невозможностью отказаться от факта отправки или получения данных), которая достигается путем избирательной или принудительной генерации допускающих верификацию свидетельств, позволяющих ассоциировать атрибуты отправителя (получателя) с элементами передаваемых данных.

Класс FPR (*приватность*) содержит четыре *семейства функциональных требований*, обеспечивающих защиту пользователя от раскрытия и несанкционированного использования его идентификационных данных.

Семейство FPR_ANO (*анонимность*) дает возможность выполнения действий без идентификатора пользователя. *Анонимность* может быть полной или выборочной. В первом случае функции безопасности обязаны предоставить заданный набор услуг без запроса идентификатора пользователя. Во втором предусмотрено более слабое

требование, в соответствии с которым идентификатор может запрашиваться, но должен скрываться от заранее указанных пользователей и/или субъектов.

Семейство FPR_PSE (*псевдонимность*) обеспечивает условия, когда пользователь может использовать ресурс или услугу без раскрытия своего идентификатора, оставаясь в то же время подотчетным за свои действия. Базовый *компонент семейства*, FPR_PSE.1, предписывает выборочную *анонимность*, а также наличие средств генерации заданного числа *псевдонимов* и определения или принятия*псевдонима* от пользователя с верификацией соответствия некоторой метрике *псевдонимов*. Эти требования дополняются в *компоненте*FPR_PSE.2 (обратимая *псевдонимность*) возможностью определения доверенными субъектами идентификатора пользователя по представленному *псевдониму*, а в *компоненте* FPR_PSE.3 (альтернативная *псевдонимность*) - возможностью оперативного перехода на новый *псевдоним*, связь которого со старым проявляется лишь в заранее оговоренных ситуациях.

Семейство FPR_UNL (*невозможность ассоциации*) содержит единственный *компонент*, предусматривающий неоднократное применение пользователем информационных сервисов, не позволяя заданным субъектам ассоциировать их между собой и приписывать одному лицу.*Невозможность ассоциации* защищает от построения профилей поведения пользователей (см. выше *компонент* FAU_SAA.2).

Самым сложным в *классе* FPR является *семейство* FPR_UNO (*скрытность*). Его требования направлены на то, чтобы пользователь мог незаметно для кого бы то ни было работать с определенными информационными сервисами. Наиболее интересны два из четырех имеющихся *компонентов семейства*. FPR_UNO.2 (*распределение информации*, влияющее на *скрытность*) предписывает рассредоточить соответствующие данные по различным частям объекта оценки. Это одно из немногих архитектурных требований "Общих критериев" (правда, выраженное в очень общей форме). В некотором смысле противоположную роль играет *компонент* FPR_UNO.4 (открытость для уполномоченного пользователя), согласно которому уполномоченные пользователи должны иметь возможность наблюдать за тем, как употребляются заданные ресурсы и/или услуги. (Как сказал один пессимист: "Я так и знал, что этим все кончится!")

Требования приватности ставят очень серьезную проблему *многоаспектности информационной безопасности*, заставляют искать баланс конфликтующих интересов субъектов информационных отношений. Разработчики заданий по безопасности должны учесть и конкретизировать эти требования с учетом действующего законодательства и специфики систем ИТ.

Защита данных пользователя

Мы переходим к рассмотрению *классов функциональных требований*, направленных на достижение высокоуровневых целей безопасности.

К высокоуровневым целям безопасности относятся защита данных пользователя и защита функций безопасности объекта оценки. Соответствующие *классы функциональных требований* характеризуются большим числом входящих в них *семейств* и разнородностью*компонентов*.

Класс FDP (защита данных пользователя) включает тринадцать *семейств*, которые можно разбить на четыре группы:

- политики защиты данных пользователя;
- виды защиты данных пользователя;
- *импорт* и *экспорт данных пользователя*;
- защита данных пользователя при передаче между доверенными изделиями ИТ.

В первую группу входят два *семейства* - FDP_ACC (политика *управления доступом*) и FDP_IFC (политика *управления информационными потоками*), - играющие, по сути, формальную роль именования политик, распространяющихся на определенные множества субъектов, объектов (потоков) и операций. Управление может быть ограниченным и полным. В последнем случае требуется, чтобы все операции всех субъектов на любом объекте (потоке) из области действия функций безопасности были охвачены некоторой политикой.

Вторая группа объединяет семь *семейств*. Содержательные аспекты управления доступом (информационными потоками) регламентируются*семействами* FDP_ACF (функции управления доступом) и FDP_IFF (функции управления информационными потоками). Первое устроено очень просто, состоит из одного *компонента* и требует наличия политик, основанных на атрибутах безопасности, а также дополнительных правил, явно разрешающих или запрещающих доступ.

Требования к функциям управления информационными потоками, представленные шестью *компонентами*, существенно сложнее и многообразнее. *Компонент* FDP_IFF.1 аналогичен FDP_ACF.1. Усиливающий его *компонент* FDP_IFF.2 требует поддержки многоуровневых политик, основанных на *иерархических атрибутах (метках) безопасности*. FDP_IFF.3, FDP_IFF.4 и FDP_IFF.5 направлены, соответственно, на ограничение пропускной способности, частичное или полное устранение *скрытых*

каналов. Наконец, FDP_IFF.6 требует осуществления мониторинга скрытых каналов, пропускная способность которых превышает заданный порог.

Семейство FDP_DAU (*аутентификация данных*) обслуживает один из видов статической *целостности* данных. В соответствии с его требованиями функции безопасности должны предоставить возможность генерировать и верифицировать свидетельства правильности определенных объектов или типов информации (*компонент* FDP_DAU.1), а также (усиливающий *компонент* FDP_DAU.2) идентификатора пользователя, создавшего свидетельство.

Отметим, что *компонент* FDP_DAU.2 ведает *неотказуемостью* авторства, а рассмотренный выше *класс* FCO - *неотказуемостью* отправки и получения данных, что можно считать разновидностью динамической целостности.

Семейство FDP_ITT (передача в пределах ОО) содержит требования, связанные с защитой данных пользователя при их передаче по*внутренним каналам* объекта оценки. Предусматривается базовая защита внутренней передачи (FDP_ITT.1), направленная на предотвращение раскрытия, модификация ситуаций недоступности, а также мониторинг целостности данных (FDP_ITT.3). При обнаружении ошибок целостности должны выполняться заданные действия. Эти требования усиливаются, соответственно, *компонентами*FDP_ITT.2 и FDP_ITT.4 за счет раздельной передачи данных, обладающих разными атрибутами безопасности.

Согласно требованиям *семейства* FDP_RIP (*защита остаточной информации*), унаследованным от "Оранжевой книги", функции безопасности должны обеспечить уничтожение любого предыдущего содержания ресурсов при их выдаче и/или освобождении.

Семейство FDP_ROL (*откат*) предусматривает возможность отмены последней операции и возврат к предшествующему состоянию с сохранением целостности данных пользователя.

Последнее *семейство* второй группы, FDP_SDI (*целостность* хранимых данных), содержит требования мониторинга целостности всех контролируемых объектов и выполнения заданных действий при обнаружении ошибок целостности хранимых данных.

В третью группу *семейств класса* FDP, обслуживающую импорт и экспорт данных пользователя в/за пределы области действия функций безопасности объекта оценки,

мы включили, как и следовало ожидать, два сходных по структуре двухкомпонентных *семейства*: FDP_ETC (экспорт) и FDP_ITC (импорт). Они различаются по наличию или отсутствию (использованию или игнорированию) ассоциированных с данными атрибутов безопасности. Согласованная интерпретация атрибутов оговорена экспортером и импортером.

В последнюю, четвертую группу (защита данных пользователя при передаче между доверенными изделиями ИТ) входят два *семейства*, ведающих обеспечением конфиденциальности (FDP_UCT) и целостности (FDP_UIT). Имеется в виду, что одним из доверенных изделий является объект оценки, а для передачи используются *внешние (по отношению к ОО) каналы*.

FDP_UCT состоит из одного *компонента*, требующего защиты от несанкционированного раскрытия.

В *семейство* FDP_UIT включены более содержательные требования. Во-первых, предусматривается всеобъемлющая защита от модификации, удаления, вставки и повторения данных. Во-вторых, обнаруженная ошибка целостности может быть восстановлена как с помощью отправителя, доверенного изделия ИТ, так и силами самого объекта оценки.

Обратим внимание на различие требований к защите данных пользователя при передаче по внутреннему (*семейство* FDP_ITT) и внешнему (*семейства* FDP_UCT и FDP_UIT) каналам, что можно считать проявлением гибкости "Общих критериев". Для внешних каналов требования заданы более детально (особенно это касается целостности), однако не предусматривается обеспечение высокой доступности данных.

Отметим также, что за различные аспекты целостности данных пользователя отвечают пять *семейств*: FDP_DAU, FDP_ITT (точнее,*компонент* FDP_ITT.3), FDP_ROL, FDP_SDI и FDP_UIT. Первое контролирует аутентичность избранных наборов данных, *компонент* FDP_ITT.3 и *семейство* FDP_UIT отвечают за (динамическую) *целостность* передаваемых данных, FDP_ROL - за восстановление целостности после сбоев или ошибок, а FDP_SDI предусматривает тотальный мониторинг статической целостности.

На практике эти варианты целостности контролируются и восстанавливаются разными методами (например, для выполнения требований FDP_DAU естественно воспользоваться криптографическими хэш-функциями или цифровой подписью, для FDP_SDI - обычными контрольными суммами), поэтому разнесение требований,

относящихся к одному аспекту ИБ, представляется в данном случае оправданным, хотя, на наш взгляд, предпочтительнее было бы ограничиться уровнем *компонентов*, а не *семейств*. Примером могут служить рассмотренные выше *компоненты* FAU_SAA.2 и FAU_SAA.4, обслуживающие различные методы выявления подозрительной активности.

Защита функций безопасности объекта оценки

Мы продолжаем рассмотрение *классов функциональных требований*, направленных на достижение высокоуровневых целей безопасности.

Класс FPT (защита функций безопасности объекта оценки) включает шестнадцать *семейств* (больше, чем какой-либо другой *класс функциональных требований*), которые можно разбить на четыре группы:

- *архитектурная безопасность*;
- защита реализации функций безопасности;
- защита данных функций безопасности;
- инфраструктурные требования.

Важнейший принцип *архитектурной безопасности* - *невозможность обхода защитных средств*. *Семейство* FPT_RVM (*посредничество при обращениях*) предназначено для достижения этой цели. Входящий в него единственный *компонент* FPT_RVM.1 (невозможность обхода политики безопасности ОО) предписывает, чтобы функции, проводящие в жизнь политику безопасности, вызывались и успешно выполнялись прежде любого другого действия, предусмотренного ПБ.

Еще один фундаментальный принцип *архитектурной безопасности* поддерживается *семейством* FPT_SEP (*разделение доменов*). Минимально необходимо отделение домена функций безопасности (*компонент* FPT_SEP.1), то есть функции безопасности должны поддерживать домен безопасности, который защищает их от вмешательства не облеченных доверием субъектов и искажений с их стороны (кроме того, должно быть реализовано *разделение доменов* безопасности субъектов). Максимальный уровень потребует реализации полного монитора обращений (*компонент* FPT_SEP.3), то есть предоставление отдельного домена той части функций безопасности, которая проводит в жизнь политики управления доступом и/или информационными потоками.

Защитой реализации функций безопасности занимаются четыре *семейства*. Самое простое из них (по формулировке, но не по воплощению и/или проверке), FPT_FLS

(*безопасность при сбое*), содержит требование, чтобы политика безопасности не нарушалась при сбоях заданных типов.

Обеспечения высокой доступности и корректной работы функций безопасности вопреки возможным сбоям добивается и более сложное*семейство* FPT_RCV (*надежное восстановление*). FPT_RCV.4 (восстановление функции) предписывает, что функция безопасности либо нормально завершается, либо, для предусмотренных сценариев сбоев, восстанавливается ее устойчивое и безопасное состояние. Первые три его *компонента* отвечают за восстановление - ручное, автоматическое и автоматическое без недопустимой потери. Для ручного восстановления требуется, чтобы после сбоя функции безопасности перешли в режим аварийной поддержки, оставляющего возможность возврата ОО к безопасному состоянию. Автоматическое восстановление без недопустимой потери означает следующее:

- при сбоях заданных типов возврат к безопасному состоянию обеспечивается автоматическими процедурами;
- безопасное состояние восстанавливается без превышения заранее определенной меры потери данных;
- функции безопасности помогают выяснить, какие объекты могут быть восстановлены, а какие нет.

Семейство FPT_PHP (*физическая защита*) требует наличия средств выявления и реагирования на несанкционированный физический доступ к частям ОО, участвующим в реализации функций безопасности. *Компонент* FPT_PHP.1 (пассивное обнаружение физического нападения) можно отнести к средствам контроля целостности, так как он требует однозначного обнаружения физического воздействия, которое может угрожать выполнению функций безопасности; информация о наличии или отсутствии подобного воздействия предоставляется по запросу. Усиливающий *компонент* FPT_PHP.2 (оповещение о физическом нападении) предусматривает постоянный контроль за определенными элементами и оповещение назначенного пользователя о подобных происшествиях. Наконец, *компонент*FPT_PHP.3 (противодействие физическому нападению) требует автоматической реакции, предотвращающей нарушение политики безопасности.

Семейство FPT_TST (*самотестирование функций безопасности*) состоит из одного *компонента*, но служит сразу двум целям: выполняет собственно самотестирование (при запуске, периодически, по запросу уполномоченного пользователя и т.п.), а также осуществляет контроль целостности данных и выполняемого кода функций.

Объединение в одном *компоненте* двух существенно разных видов требований представляется странным (тестирование имеет мало общего с контролем целостности кода и, тем более, изменяемых данных), но позволяет плавно перейти к третьей группе *семейств класса* FPT (защита данных функций безопасности). В эту группу входят шесть *семейств*, три из которых, FPT_ITA, FPT_ITC и FPT_ITI, отвечают, соответственно, за доступность, конфиденциальность и *целостность* экспортируемых данных функций безопасности. Отметим, что доступность должна быть обеспечена с заданной вероятностью, а контроль целостности в общем случае предусматривает возможность восстановления поврежденных данных удаленным доверенным изделием ИТ.

Семейство FPT_TDC содержит требование согласованной интерпретации данных, совместно используемых функциями безопасности ОО и другим доверенным изделием ИТ. Явных требований к контролю импортируемых данных в *классе* FPT (в отличие от FDP) нет, хотя из соображений симметрии они, безусловно, должны присутствовать (см. выше *семейства* FDP_ETC и FDP_ITC).

Пятое *семейство* группы, FPT_ITT (передача данных функций безопасности в пределах объекта оценки), аналогично рассмотренному ранее *семейству* из *класса* защиты данных пользователя FDP_ITT (передача в пределах ОО), но не предусматривает обеспечения доступности и разделения по атрибутам при контроле целостности. Справедливости ради укажем, однако, что в *компоненте* FPT_ITT.3 более детально специфицированы обнаруживаемые виды нарушений целостности: модификация, подмена, перестановка, удаление данных.

Семейство FPT_TRC отвечает за *согласованность данных функций безопасности* при дублировании в пределах ОО. Здесь следует обратить внимание на требования элемента FPT_TRC.1.2: если части ОО, содержащие дублируемые данные, были разъединены, необходимо обеспечить согласованность таких данных после восстановления соединения перед обработкой запросов к заданным функциям безопасности. Отметим, что к взаимодействию с удаленным доверенным изделием ИТ требование согласованности данных не предъявляется. В целом же остается неясным смысл разнесения по разным *классам* требований защиты данных пользователя и функций безопасности. Последние, кроме того, трактуются как одноуровневые, для них не предусмотрено разделение по атрибутам, что для сложных систем может оказаться неприемлемым.

Требования, которые мы назвали инфраструктурными, вошли в состав четырех *семейств*. *Семейство* FPT_AMT (тестирование *базовой абстрактной машины*)

определяет требования к тестированию, демонстрирующему правильность предположений, обеспечиваемых абстрактной машиной (аппаратно-программной платформой), лежащей в основе функций безопасности.

Семейство FPT_RPL (*обнаружение повторного использования*) нацелено на выявление повторного использования сущностей различных типов (например, сообщений, запросов на обслуживание и ответов на запросы) и выполнение заданных ответных действий.

Семейство FPT_SSP (протокол *синхронизации состояний*) на самом деле содержит требования одностороннего или взаимного надежного подтверждения при обмене данными между функциями безопасности в распределенной среде.

Наконец, *семейство* FPT_STM (метки времени) требует предоставления *надежных меток времени* в пределах объекта оценки. Подобные метки необходимы, например, функциям протоколирования и управления.

Классы функциональных требований, играющие инфраструктурную роль

Криптографические механизмы - обязательный элемент защищенных систем. *Класс* FCS (*криптографическая поддержка*) состоит из 2*семейств*, где в самом общем виде (точнее, в виде параметризованных шаблонов) рассматриваются *генерация*, *распределение*, *доступ* и*уничтожение ключей*, а также *криптографические операции*. Смысл требований состоит в том, что необходимо действовать в соответствии с некими алгоритмами, длинами ключей и стандартами; какие-либо содержательные спецификации отсутствуют.

Класс FMT (*управление безопасностью*), включающий шесть *семейств*, регламентирует управление функциями безопасности и их данными, атрибутами и ролями безопасности.

Семейство FMT_MOF (управление отдельными функциями) содержит единственное требование: только уполномоченные пользователи (точнее, уполномоченные идентифицированные роли) могут управлять режимами выполнения, подключением и отключением функций безопасности.

К управлению атрибутами безопасности (*семейство* FMT_MSA) предъявляется больше требований. Во-первых, оно должно быть доступно только определенным ролям. Во-вторых, необходимо контролировать безопасность присваиваемых значений. В-третьих,

при создании объектов должна существовать возможность задания значений, отличных от подразумеваемых.

Аналогичным образом устроено *семейство* FMT_MTD (управление данными функций безопасности), только вместо переопределения подразумеваемых значений в *компоненте* FMT_MTD.2 специфицируются граничные значения и действия, предпринимаемые в случае выхода за допустимые границы.

FMT_REV (отмена) предусматривает возможность отмены (отзыва) атрибутов безопасности пользователей, субъектов и объектов.

FMT_SAE позволяет устанавливать *сроки действия атрибутов безопасности*. Для каждого атрибута могут задаваться действия, выполняемые по истечении срока.

Наконец, *семейство* FMT_SMR (*роли управления безопасностью*) предназначено для управления назначением различных ролей пользователям. Предусмотрено наличие правил, управляющих отношениями между ролями.

Шесть *семейств* простой структуры содержит и *класс* FTA (доступ к объекту оценки), куда вошли требования *управления сеансами работы пользователей* (помимо идентификации и аутентификации).

Семейство FTA_LSA определяет требования по ограничению атрибутов безопасности сеанса, которые может выбирать пользователь.

Семейство FTA_MCS *ограничивает количество параллельных сеансов*, предоставляемых пользователю. Оно может быть как общим, так и индивидуальным (с учетом атрибутов безопасности).

Семейство FTA_SSL (*блокирование сеанса*) определяет возможность блокирования или завершения интерактивного сеанса как по инициативе пользователя, так и по инициативе функций безопасности (если пользователь неактивен заданное время). Действия, осуществляемые при блокировании, описаны весьма детально:

- очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида;
- блокирование любых действий по доступу к данным пользователя и устройствам отображения, кроме необходимых для разблокирования сеанса.

Еще три однокомпонентных *семейства* содержат некоторые подробности открытия сеанса.

Семейство FTA_TAB (предупреждения перед предоставлением доступа к ОО) предписывает, чтобы перед открытием сеанса отображалось предупреждающее сообщение относительно несанкционированного использования объекта оценки. Это одно из весьма немногих*функциональных требований* без управляющих конструкций назначения или выбора.

Семейство FTA_TAH (*история доступа* к ОО) при успешном открытии сеанса определяет требования к отображению истории попыток получить доступ от имени пользователя, выполняющего вход в систему. Здесь проявлена просто-таки трогательная забота о пользователе: оговаривается, что справочная информация не должна исчезать с экрана до того, как пользователь успеет ее просмотреть.

Кроме того, функции безопасности могут отказать пользователю в открытии сеанса, основываясь на атрибутах безопасности, такая возможность с обманчивым названием "Открытие сеанса с ОО" предусмотрена *семейством* FTA_TSE.

Если сопоставить степень детализации требований к криптографической поддержке и к управлению сеансами, то различие представляется слишком большим. Впрочем, выдержать единый уровень в столь большом и сложном документе, как "Общие критерии", едва ли возможно.

Привычные, традиционные требования предъявляет *класс* FTP (*доверенный маршрут*/*канал*), состоящий из двух *семейств*, содержащих по одному *компоненту* в каждом. Доверенный маршрут (*семейство* FTP_TRP) позволяет выполнять определенные действия в режиме прямого взаимодействия с функциями безопасности (например, при начальной аутентификации). Доверенные каналы (*семейство* FTP_ITC) предназначены для передачи критичных по безопасности данных между функциями безопасности с другими доверенными изделиями ИТ.*Доверенный маршрут*/*канал* должен быть логически отличим от других маршрутов (каналов), обеспечивать уверенную идентификацию взаимодействующих сторон, а также конфиденциальность и *целостность* передаваемых данных.

На этом мы завершаем рассмотрение *функциональных требований безопасности*.

Методические указания по выполнению лабораторных работ

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Проблема защиты информации не нова. Она появилась еще задолго до появления компьютеров. Стремительное совершенствование компьютерных технологий сказалось и на принципах построения защиты информации.

Актуальность проблемы защиты информации связана с ростом возможностей вычислительной техники. Развитие средств, методов и форм автоматизации процессов обработки информации, многообразие и массовость применения средств вычислительной техники резко повышают уязвимость информации. Основными факторами, способствующими повышению этой уязвимости, являются резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ и других средств автоматизации, сосредоточение в единых базах данных информации различного назначения и различной принадлежности, резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и находящимся в ней массивам данных, автоматизация межмашинного обмена информацией, в том числе и на больших расстояниях.

В этих условиях возникает возможность несанкционированного использования или модификации информации, что может нанести серьезные убытки широкому кругу пользователей. Автоматизация финансовых расчетов, развитие электронных платежных систем создают благоприятные условия для осуществления мошеннических операций.

Сегодня на рынке представлен большой спектр продуктов, позволяющих построить надежную, хорошо эшелонированную систему защиты информации, обрабатываемой в автоматизированных системах.

Однако недостаточно просто приобрести и установить некоторую совокупность разнообразных средств защиты компьютерной информации. Для того, чтобы применение подобных средств было эффективным для обеспечения надежной защиты конфиденциальной информации, необходимо иметь четкое понимание функционального назначения каждого продукта, твердые знания принципов его работы и их правильную настройку, выполнить которую можно только имея, оценив имеющиеся угрозы безопасности информации.

Предлагаемое издание знакомит с практическими приемами настройки и использования наиболее распространенных средств защиты компьютерной информации. Лабораторный практикум состоит из пяти работ, которые охватывают основные рубежи защиты информации, обрабатываемой в автоматизированных системах.

В первой работе производится знакомство с принципами настройки современных межсетевых экранов на примере межсетевого экрана *D-link DFL-800*T. Многочисленные устройства данного класса имеют аналогичный интерфейс и принципы работы, поэтому навыки работы с *D-link DFL-800*T помогут легко организовать работу с другими устройствами.

Вторая работа дает навыки организации обмена данными через защищенные беспроводные сети. Технология Wi-Fi получает все большее распространение среди пользователей, поэтому умение правильно настроить

устройства для беспроводного доступа в сеть, параметры защиты канала связи приобретает на сегодняшний день все большее значение.

Третья работа носит исследовательский характер и предназначена для формирования более глубокого понимания способов перехвата конфиденциальной информации и актуальности задачи её защиты.

Четвертая работа позволяет освоить один из наиболее эффективных способов защиты информации – шифрование. В процессе выполнения работы студенты знакомятся со способами получения сертификатов, используемых для выполнения криптографических преобразований. Для шифрования и цифровой подписи может использоваться электронный ключ *ruToken*. В результате выполнения работы формируются знания и умения организации защищенного информационного обмена между корпоративными пользователями.

Пятая работа знакомит с одним из эффективных способов защиты данных на локальной машине – использование защищенных виртуальных дисков. Одним из преимуществ виртуальных дисков является то, что доступ к данным может получить только владелец электронного ключа *eToken*, который практически невозможно подделать и можно хранить в надежном месте. В данной работе отрабатывается выполнение всех основных операций с виртуальными защищенными дисками: создание, изменение параметров, перешифрование, удаление и восстановление, проверка возможности использования.

Таким образом, добросовестное выполнение предложенных работ, а также твердое знание лекционного материала создает хорошие предпосылки для становления настоящего специалиста по защите информации.

ЛАБОРАТОРНАЯ РАБОТА №1. ЗАЩИТА ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ С ПОМОЩЬЮ МЕЖСЕТЕВОГО ЭКРАНА

Цель работы

Научиться конфигурированию межсетевого экрана *D-link DFL-800*T для приобретения навыков защиты локальной вычислительной сети предприятия от угроз информационной безопасности со стороны пользователей глобальной сети Интернет.

Краткие теоретические сведения

Межсетевой экран (firewall) - это устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных. Этим оно отличается от маршрутизатора, функцией которого является доставка трафика в пункт назначения в максимально короткие сроки.

Кроме того, межсетевые экраны, как правило, обладают большим набором настроек. Прохождение трафика на межсетевом экране можно настраивать по службам, IP-адресам отправителя и получателя, по идентификаторам пользователей, запрашивающих службу. Межсетевые экраны позволяют осуществлять централизованное управление безопасностью. В одной конфигурации администратор может настроить разрешенный входящий трафик для всех внутренних систем организации. Это не устраняет потребность в обновлении и настройке систем, но позволяет снизить вероятность неправильного конфигурирования одной или нескольких систем, в результате которого эти системы могут подвергнуться атакам на некорректно настроенную службу.

Межсетевой экран использует один или более наборов "правил" для проверки сетевых пакетов при их входе или выходе через сетевое соединение, он или позволяет прохождение трафика или блокирует его. Правила межсетевого экрана могут проверять одну или более характеристик пакетов, включая, но не ограничиваясь типом протокола, адресом хоста источника или назначения и портом источника или назначения.

Межсетевые экраны представляют собой программные пакеты, базирующиеся на операционных системах общего назначения (таких как Windows и Unix) или на аппаратной платформе межсетевых экранов. Межсетевой экран обладает несколькими интерфейсами, по одному на каждую из сетей, к которым он подключен. Набор правил политики определяет, каким образом трафик передается из одной сети в другую. Если в правиле отсутствует явное разрешение на пропуск трафика, межсетевой экран отклоняет или аннулирует пакеты.

Существуют два основных типа межсетевых экранов: межсетевые экраны прикладного уровня и межсетевые экраны с пакетной фильтрацией. В их основе лежат различные принципы работы, но при правильной настройке оба типа устройств обеспечивают правильное выполнение функций безопасности, заключающихся в блокировке запрещенного трафика.

При использовании межсетевого экрана прикладного уровня все соединения проходят через него. Как показано на рисунке 1.1, соединение начинается на системе-клиенте и поступает на внутренний интерфейс межсетевого экрана. Межсетевой экран принимает соединение, анализирует содержимое пакета и используемый протокол и определяет, соответствует ли данный трафик правилам политики безопасности. Если это так, то межсетевой экран инициирует новое соединение между своим внешним интерфейсом и системой-сервером.

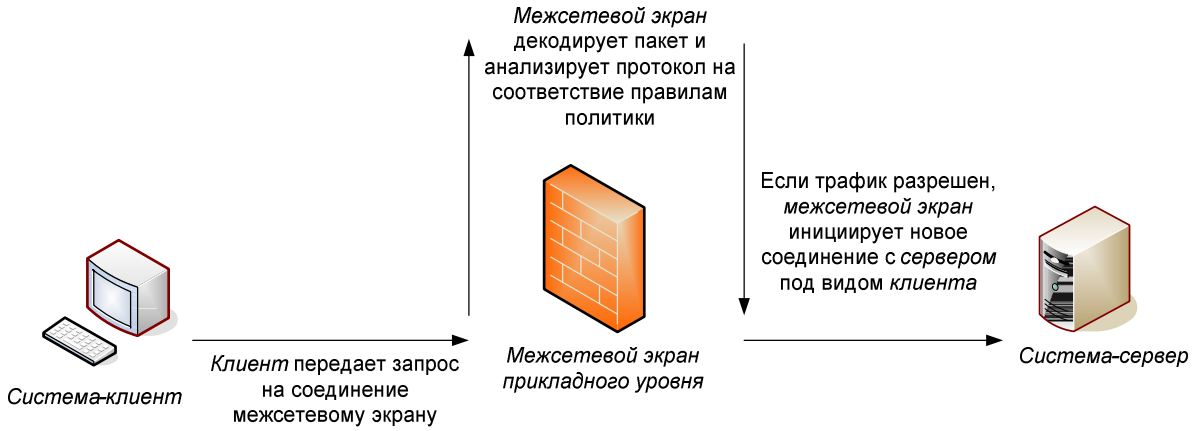

Рис. 1.1. Соединения модуля доступа межсетевого экрана прикладного уровня

Межсетевые экраны прикладного уровня используют модули доступа для входящих подключений. Модуль доступа в межсетевом экране принимает входящее подключение и обрабатывает команды перед отправкой трафика получателю. Таким образом, межсетевой экран защищает системы от атак, выполняемых посредством приложений.

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.

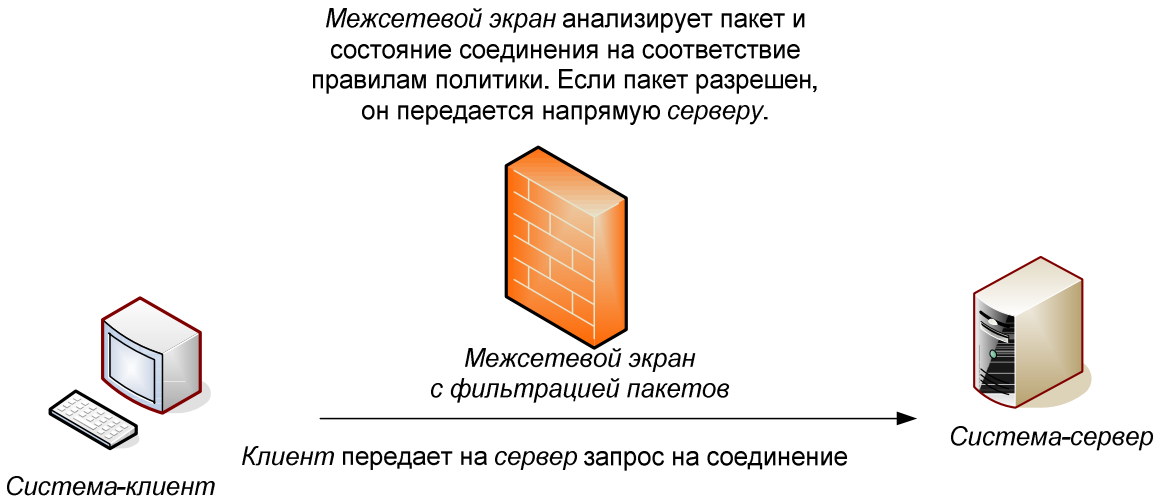

Рис. 1.2. Передача трафика через межсетевой экран с фильтрацией пакетов

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, работающие только посредством фильтрации пакетов, не используют модули доступа, и поэтому трафик передается от клиента непосредственно на сервер. Если сервер будет атакован через открытую службу, разрешенную правилами политики межсетевого экрана, межсетевой экран никак не отреагирует на атаку. Межсетевые экраны с пакетной фильтрацией также позволяют видеть извне внутреннюю структуру адресации. Внутренние адреса скрывать не требуется, так как соединения не прерываются на межсетевом экране.

Как и многие другие устройства, межсетевые экраны изменяются и совершенствуются с течением времени, т. е. эволюционируют. Производители межсетевых экранов прикладного уровня в определенный момент пришли к выводу, что необходимо разработать метод поддержки протоколов, для которых не существует определенных модулей доступа. Вследствие этого увидела свет технология модуля доступа Generic Services Proxy (GSP). GSP разработана для поддержки модулями доступа прикладного уровня других протоколов, необходимых системе безопасности и при работе сетевых администраторов. В действительности GSP обеспечивает работу межсетевых экранов прикладного уровня в качестве экранов с пакетной фильтрацией.

Производители межсетевых экранов с пакетной фильтрацией также добавили некоторые модули доступа в свои продукты для обеспечения более высокого уровня безопасности некоторых широко распространенных протоколов. На сегодняшний день многие межсетевые экраны с пакетной фильтрацией поставляются с модулем доступа SMTP.

В то время как базовая функциональность межсетевых экранов обоих типов осталась прежней, (что является причиной большинства "слабых мест" этих устройств), сегодня на рынке присутствуют гибридные межсетевые экраны. Практически невозможно найти межсетевой экран, функционирование которого построено исключительно на прикладном уровне или фильтрации пакетов. Это обстоятельство отнюдь не является недостатком, так как оно позволяет администраторам, отвечающим за безопасность, настраивать устройство для работы в конкретных условиях.

Межсетевые экраны могут серьезно повысить уровень безопасности хоста или сети. Они могут быть использованы для выполнения одной или более нижеперечисленных задач:

- Для защиты и изоляции приложений, сервисов и машин во внутренней сети от нежелательного трафика, приходящего из внешней сети интернет.
- Для ограничения или запрещения доступа хостов внутренней сети к сервисам внешней сети интернет.
- Для поддержки преобразования сетевых адресов (network address translation, NAT), что дает возможность задействовать во внутренней сети приватные IP адреса и совместно использовать одно подключение к сети Интернет (либо через один выделенный IP адрес, либо через адрес из пула автоматически присваиваемых публичных адресов).

Характеристика работы

Работа выполняется бригадой студентов из двух человек, каждый из которых имеет свое рабочее место. Для выполнения работы следует использовать рабочие места *WS23* и *WS26*, находящиеся в разных подсетях, разделенных межсетевым экраном *D-link DFL-800*.

Перед началом работы следует уточнить IP-адрес межсетевого экрана *D-link DFL-800* и учетные данные, используемые для входа в интерфейс администрирования. Каждый из участников сообщает IP-адрес своего рабочего места другому участнику бригады.

Задания работы участниками бригады выполняются поочередно, со своих рабочих мест. Правильность составления каждого правила следует проверять. Например, если было добавлено правило, ограничивающее доступ в Интернет для определенной машины, то следует сделать соответствующую попытку и убедиться, что для этой машины доступ действительно ограничен.

Порядок выполнения работы

ВНИМАНИЕ!

1. Запрещается «сбрасывать» настройки межсетевого экрана в *factory defaults*.
2. В настройках браузера отключить использование прокси-сервера при соединении с Интернетом (или добавить адрес межсетевого экрана с список исключений).

Перед началом работы Участник №1 занимает рабочее место WS23, Участник №2 – WS26. Используя полученные учетные данные, оба Участника авторизуются в конфигурационной оболочке межсетевого экрана *D-link DFL-800*.

Обоим Участникам необходимо выполнить следующие действия:

1. Участник №1 создает правило, запрещающее доступ в сеть Интернет Участнику№2;
2. Участник №2 создает правило, которое разрешает прохождение ICMP-трафика через межсетевой экран для своего рабочего места;
3. Участник №2 корректирует набор правил межсетевого экрана так, чтобы открыть себе доступ в сеть Интернет;
4. Участник №1 создает правило, ограничивающее объем трафика для подсети *umk-net2*;

5. Участник №2 корректирует созданное на предыдущем шаге правило, изменяя лимит трафика для подсети *umk-net2*;
6. Участник №1 создает правило, запрещающее доступ к FTP-серверу Участнику №2. При этом другие компьютеры из подсети *umk-net2* имеют доступ к FTP-серверу (IP-адрес FTP-сервера следует уточнить у лаборанта);
7. Участник №2 корректирует созданное на предыдущем шаге правило, открывая себе доступ к FTP-серверу;
8. Участник №2 вводит настройки, с помощью которых запрещается доступ к конфигурационной оболочке межсетевого экрана для компьютеров из другой подсети. При этом, с рабочих мест своей подсети (*umk-net2*) конфигурировать разрешено.

Требования к содержанию и оформлению отчета

В отчет следует помещать экранные снимки окон оболочки конфигурирования межсетевого экрана *D-link DFL-800*. В тексте отчета следует приводить названия редактируемых параметров правил (например, имя правила, выполняемое действие, служба и т.п.) и введенные значения (наример, *AllowICMP*, *Allow*, *all_icmp* и т.п. соответственно). Таким образом, смысл правил должен быть понятен без разглядывания экранных снимков.

Контрольные вопросы

1. В чем состоит принцип работы межсетевого экрана?
2. Выделите два основных типа межсетевых экранов.
3. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика?
4. Является ли один из типов межсетевых экранов более безопасным, нежели другой?
5. Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?
6. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора?
7. Что проверяет межсетевой экран с фильтрацией пакетов, помимо набора правил, для принятия решения о блокировке или передаче пакета?
8. От каких угроз безопасности информации защищает межсетевой экран?
9. В каком месте вычислительной сети целесообразна установка межсетевого экрана?
10. Каким образом производится настройка параметров межсетевого экрана?
11. Какова структура правил настройки межсетевого экрана?

ЛАБОРАТОРНАЯ РАБОТА №2. ОРГАНИЗАЦИЯ ЗАЩИЩЕННОЙ БЕСПРОВОДНОЙ КОМПЬЮТЕРНОЙ СЕТИ

Цель работы

Изучить порядок настройки беспроводной точки доступа и организации беспроводных сетей по технологии Wi-Fi.

Краткие теоретические сведения

Повсеместное распространение беспроводных сетей, развитие инфраструктуры хот-спотов, появление мобильных технологий со встроенным беспроводным решением (Intel Centrino) привело к тому, что конечные пользователи (не говоря уже о корпоративных клиентах) стали обращать все большее внимание на беспроводные решения. Такие решения рассматриваются, прежде всего, как средство развертывания мобильных и стационарных беспроводных локальных сетей и средство оперативного доступа в Интернет. Однако конечный пользователь, не являющийся сетевым администратором, как правило, не слишком хорошо разбирается в сетевых технологиях, поэтому ему трудно сделать выбор при покупке беспроводного решения, особенно учитывая многообразие предлагаемых сегодня продуктов. Бурное развитие технологии беспроводной связи привело к тому, что пользователи, не успев привыкнуть к одному стандарту, вынуждены переходить на другой, предлагающий еще более высокие скорости передачи. Речь, конечно же, идет о семействе протоколов беспроводной связи, известном как IEEE 802.11, куда входят следующие протоколы: 802.11, 802.11b, 802.11b+, 802.11a, 802.11g. В последнее время стали говорить и о расширении протокола 802.11g.

Различные типы беспроводных сетей отличаются друг от друга и радиусом действия, и поддерживаемыми скоростями соединения, и технологией кодирования данных. Так, стандарт IEEE 802.11b предусматривает максимальную скорость соединения 11 Мбит/с, стандарт IEEE 802.11b+ - 22 Мбит/с, стандарты IEEE 802.11g и 802.11a - 54 Мбит/с.

На самом деле все спецификации Wi-Fi являются стандартом в стандарте. С одной стороны, они все должны удовлетворять стандарту беспроводных сетей 802.11, а с другой – они входят в состав крупнейшего стандарта локальных сетей IEEE 802. И преимущества такого подхода сложно недооценивать. Так, спецификации 802.11 затрагивают лишь два нижних уровня (физический и канальный) общей модели ISO/OSI, состоящей из семи уровней. На практике это означает, что любое приложение, равно как и операционная система, не почувствует никакой разницы, будет ли оно работать, например, в проводной локальной сети Ethernet, или беспроводной Wi-Fi, а следовательно, затраты на переход с проводной технологии на беспроводную будут определяться лишь стоимостью оборудования и его установки, и никакая разработка и замена программного обеспечения не потребуется.

Оборудование, предназначенное для работы в стандарте 802.11, в основном делится на два класса – это клиенты и точки доступа (Access Point). Роль клиентов могут играть настольные компьютеры, ноутбуки, КПК,

телефоны, принтеры, игровые приставки и прочая портативная и стационарная бытовая техника, оборудованная Wi-Fi-модулем. Если в ПК или КПК изначально отсутствует поддержка беспроводных сетей, то в большинстве случаев это можно с легкостью восполнить приобретением соответствующего адаптера, который может быть реализован в форме практически любой платы расширения. Точки доступа обычно выполнены в виде отдельного внешнего устройства, подключаемого непосредственно к кабелю проводной сети Ethernet или к любому другому совместимому источнику широкополосного доступа в Интернет. Иногда точки доступа комбинируют с каким-либо другим устройством, например, весьма распространены ADSL-модемы, совмещенные с точкой доступа Wi-Fi. На точку доступа возлагается львиная часть работы по обслуживанию беспроводной сети: она должна не только поддерживать радиопередачу со всеми клиентами и связывать сеть с внешним миром, но и регулировать трафик, обрабатывать данные и совершать массу других операций. Также в некоторых случаях может потребоваться и дополнительное оборудование: например, при недостаточном уровне сигнала нужны антенны, а при необходимости соединения между собой двух сетей – мосты.

Существует два основных способа организации беспроводной сети – это клиент-сервер (*Infrastructure Mode*) и точка-точка (*Ad-hoc*). В первом случае сеть состоит из одной или нескольких точек доступа и произвольного количества клиентов. Это стандартная модель построения локальной сети, которая принципиально отличается от проводной разве что отсутствием тех самых проводов. Во втором случае связь устанавливается непосредственно между несколькими клиентами, минуя точку доступа. Такая модель удобна для соединения между собой нескольких портативных устройств, например, для моментальной печати фотографий с Wi-Fi-камеры на Wi-Fi-принтер или многопользовательской игры на портативных консолях (Sony PSP, Nintendo DS и других).

Точка доступа может использовать DHCP – протокол динамической конфигурации хоста. По протоколу DHCP один компьютер в сети назначается сервером BOOTP, все остальные – по крайней мере те, кому нужен IP-адрес – становятся клиентами DHCP (компьютеры, уже имеющие постоянный IP-адрес, могут не приниматься в расчет). Администратор точки доступа должен вначале сконфигурировать DHCP-сервер. Частью процесса конфигурации является выделение блока IP-адресов для последующего присвоения клиентам.

При появлении нового узла в сети DHCP-сервер посылает широковещательный запрос с просьбой о назначении IP-адреса (если, конечно, этот узел может быть клиентом DHCP). В ответ на запрос сервер DHCP находит в таблице адресов свободный адрес и посылает ответ запрашивающему узлу.

Необходимое оборудование и программное обеспечение

Для выполнения работы используется DWL-2100AP – многофункциональная беспроводная точка доступа для сетей предприятий. Точка доступа разработана для установки в помещениях и предоставляет

расширенные функции, включая режим *Turbo*, со скоростью соединения до 108 Мбит/с, функции безопасности и качества обслуживания (QoS), а также поддержку нескольких режимов работы, позволяя развертывать управляемые и надежные беспроводные сети.

В качестве клиентов беспроводной сети используются персональные компьютеры, оснащенные адаптерами Wi-Fi. Как минимум один компьютер должен быть подключен к точке доступа через кабельную систему.

Характеристика работы

Работа выполняется бригадой студентов из двух человек, каждый из которых имеет свое рабочее место. Для выполнения работы следует использовать рабочие места *WS28* и *WS27*, оснащенные беспроводными адаптерами.

На подсеть, в которой находится точка доступа, выделен диапазон адресов в подсети **192.168.2.0/240**. Точке доступа должен быть присвоен адрес **192.168.2.7**.

В ходе выполнения работы следует настроить точку доступа для организации защищенной беспроводной сети, к которой необходимо подключить рабочие места *WS28* и *WS27*.

Конфигурирование точки доступа выполняется студентами совместно, с любого компьютера, подключенного к сети. Настройка каждого рабочего места, оснащенного беспроводным адаптером выполняется одним из студентов индивидуально.

Перед началом работы лаборант загружает в точку доступа исходную конфигурацию.

Порядок выполнения работы

1. Запретить доступ к конфигурационному интерфейсу точки доступа для всех компьютеров, кроме того, с которого осуществляется доступ в данный момент.
2. Разрешить доступ к конфигурационному интерфейсу точки доступа для компьютера с IP-адресом **192.168.2.24**.
3. Задать идентификатор точки доступа. В качестве идентификатора использовать фамилии студентов, выполняющих задание. Например – *Ivanov_Petrov*.
4. Включить DHCP-сервер на точке доступа.
5. Определить пул из свободных IP-адресов в подсети **192.168.2.0/240**, начиная с **192.168.2.11.** Ввести соответствующие параметры в конфигурацию точки доступа.
6. Включить режим шифрования радиосигнала, задать ключ.
7. Задать фильтры MAC-адресов, разрешающие доступ в беспроводную сеть только с рабочих мест *WS28* и *WS27*.
8. На рабочих местах *WS28* и *WS27* включить адаптеры беспроводной сети.
9. Ввести необходимые настройки и подключиться к беспроводной сети.
10. Убедиться, что с каждого рабочего места, подключенного к беспроводной сети, доступны другие рабочие места, подключенные к этой сети.

11. Сохранить полученную конфигурацию точки доступа в файле.
12. Загрузить в точку доступа исходную конфигурацию из файла «Точка доступа2.cfg».

Требования к содержанию и оформлению отчета

В ходе выполнения задания необходимо делать экранные снимки окон настройки точки доступа и помещать их в отчет. Текст отчета должен содержать пояснения, в которых детально рассматриваются задаваемые параметры конфигурации.

После выполнения первого пункта задания необходимо сделать попытку доступа к конфигурационному интерфейсу с другого компьютера и убедиться, что эта попытка безуспешна.

В случае успешного подключения к беспроводной сети следует открыть окно параметров соединения и поместить в отчет соответствующий экранный снимок.

Контрольные вопросы

1. Что такое DHCP-сервер и для чего он используется?
2. В чем заключается принцип работы DHCP-сервера?
3. Для чего используется шифрование данных, передаваемых по радиоканалу?
4. Назовите алгоритмы шифрования, поддерживаемые точкой доступа *DWL-2100AP*. В чем их отличие?
5. В чем заключается необходимость использования фильтров MAC-адресов?
6. Каков порядок настройки устройств для подключения к точке доступа по беспроводному каналу?

ЛАБОРАТОРНАЯ РАБОТА №3. ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ПЕРЕХВАТА ТРАФИКА В КОМПЬЮТЕРНОЙ СЕТИ

Цель работы

Смоделировать попытку несанкционированного доступа к информации, которой обмениваются пользователи сети через FTP-сервер. Получить навыки перехвата и анализа пакетов компьютерной сети с помощью программы-монитора.

Основные возможности утилиты Microsoft Network Monitor

Анализатор протоколов *Microsoft Network Monitor* это инструмент, используемый для просмотра содержимого сетевых пакетов, отправляемых или получаемых через активное сетевое соединение, или из полученного файла данных. Этот инструмент предоставляет возможность фильтрации для сложного анализа сетевых данных.

Вообще, анализаторы протоколов предназначены для поиска «узких мест» в сети и повышения ей производительности. Однако, как будет показано ниже, анализатор протоколов может использоваться для несанкционированного доступа к информации, передаваемой по компьютерной сети.

Рассмотрим основные функции *Microsoft Network Monitor*, необходимые для выполнения лабораторной работы. На рисунке 3.1 показан фрагмент окна программы, на котором отмечены используемые закладки.

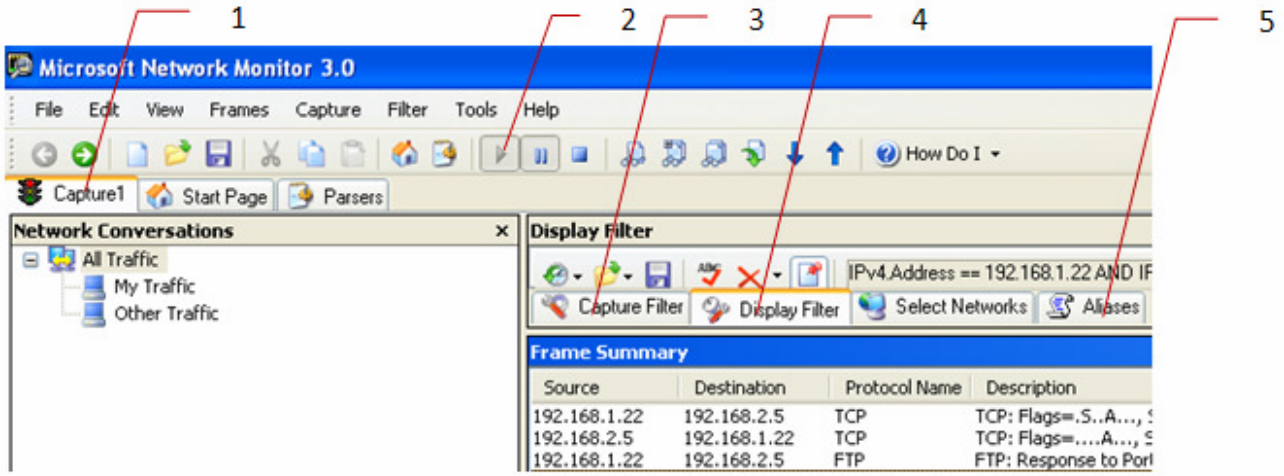

Рис. 3.1 Фрагмент окна программы *Network Monitor*

Закладка 1 содержит окно выбора вида трафика, который следует перехватывать. Целесообразно активизировать значение *All Traffic*. Закладка 3 позволяет сконфигурировать фильтр перехватываемых пакетов. Закладка 4 позволяет сконфигурировать фильтр пакетов, отображаемых в окне *Frame Summary*. Закладка 5 содержит список псевдонимов, которые могут быть использованы для удобства анализа перехваченных пакетов. Для запуска процесса прослушивания трафика необходимо нажать на кнопку 2.

Окно *Frame Summary* является основным экранным элементом, в котором отображается содержимое перехваченных пакетов. В ходе работы следует внимательно изучать перехватываемые пакеты в поисках конфиденциальной

информации, а также учетных данных пользователей, передаваемых в открытом (нешифрованном) виде. Например, на рисунке 3.2 показано *Frame Summary*, в котором синим цветом выделены пакеты, содержащие имя пользователя и пароль, необходимые для подключения к FTP-серверу.

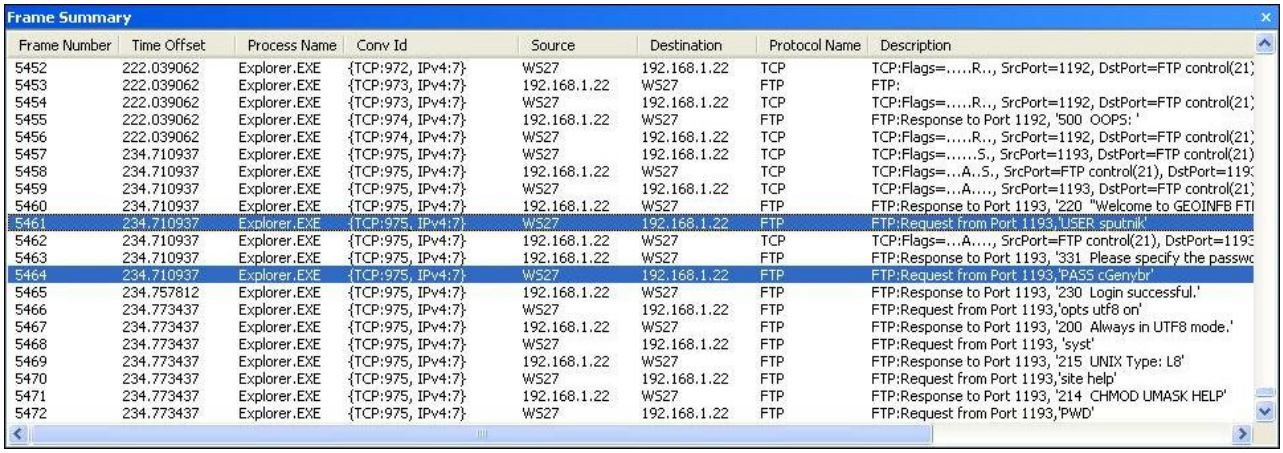

Рис. 3.2. Окно *Frame Summary* с перехваченными учетными данными пользователя

Фильтрация пакетов представляет собой логическое выражение, задающее критерии отбора пакета по выбранным параметрам. Рисунок 3.3 иллюстрирует использование фильтра пакетов по IP-адресу.

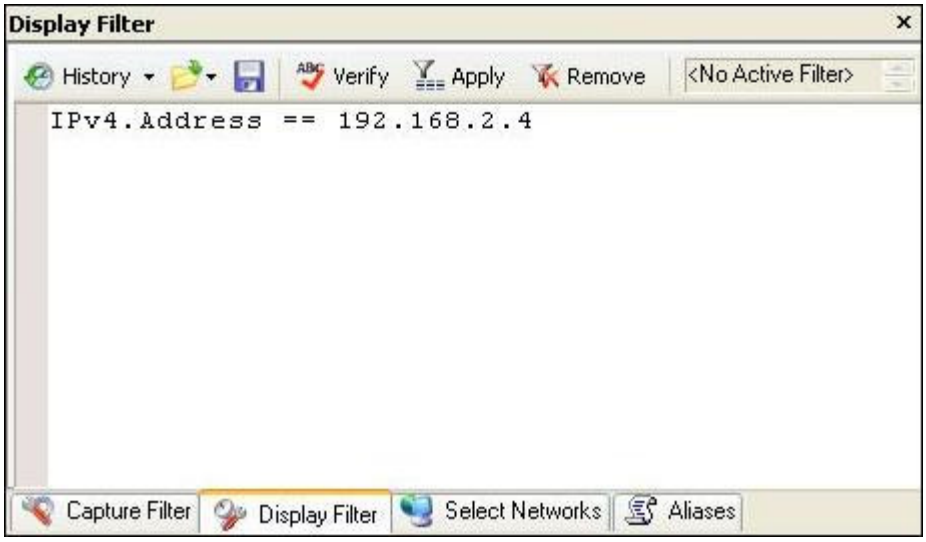

Рис. 3.3 Окно конфигурирования фильтра отображаемых пакетов

Порядок выполнения работы

Работа выполняется бригадой студентов из трех человек, каждый из которых имеет свое рабочее место. В ходе работы производится моделирование обмена текстовыми файлами между двумя пользователями сети через FTP-сервер. Третий участник бригады, имитируя действия злоумышленника, должен перехватить учетные данные пользователей, используемые для авторизации на FTP-сервере, и исказить передаваемые файлы.

Перед началом работы участники бригады распределяют между собой роли участников сетевого обмена, которые можно обозначить: Абонент1, Абонент2 и Злоумышленник. В процессе выполнения работы Абонент1 и

Абонент2 обмениваются текстовыми файлами, а Злоумышленник реализует несанкционированный доступ к ним.

Внимание! Для успешного выполнения работы сканер пакетов должен быть запущен на сервере ***S10***, через который проходит трафик к FTP-серверу.
Если на сервере ***S10*** установлена операционная система из семейства *Linux*, то следует использовать сканер пакетов *WireShark* или его аналог.
Запуск сканера пакетов следует осуществлять от пользователя **root**.

Ход работы состоит из перечисленных ниже действий.

1. Каждый из Абонентов создает на локальном диске текстовый файл, в который помещает сообщение произвольного содержания для другого Абонента. Размер файла должен быть более 1 кб. Тексты сообщений помещаются в отчет.
2. Злоумышленник запускает программу Network Monitor и начинает отслеживать входящий и исходящий трафик FTP-сервера.
3. Абоненты устанавливают связь с FTP-сервером кафедры и копируют созданные файлы в общедоступную папку. После окончания копирования, соединения с FTP-сервером должны быть разорваны.
4. Анализируя трафик, Злоумышленник определяет учетные данные, использованные Абонентами для установления соединения с FTP-сервером.
5. Используя полученные учетные данные, Злоумышленник устанавливает соединение с FTP-сервером и модифицирует текстовые файлы Абонентов.
6. Абоненты вновь устанавливают связь с FTP-сервером и копируют с него на свои локальные диски загруженные ранее текстовые файлы.
7. Сопоставляя исходный и загруженный файлы, каждый из Абонентов должен убедиться, что содержание текстового сообщения изменено Злоумышленником.
8. Указанные выше действия выполняются еще два раза так, чтобы каждый из участников бригады выполнил роль Злоумышленника.

Методические указания по выполнению работы

Перед началом работы участники бригады должны уточнить у преподавателя или лаборанта наименования используемых рабочих мест в компьютерном классе, IP-адрес FTP-сервера. Абонентам также сообщаются параметры соединения с FTP-сервером.

Примечание. В настоящее время следует использовать следующие параметры FTP-соединения: IP – 192.168.1.22, учетная запись – *sputnik*, пароль *cGenybr*.

Для удобства анализа трафика с помощью программы Network Monitor следует использовать фильтры и псевдонимы. Доступны фильтры двух типов: фильтр захвата (Capture Filter) фильтр отображения (Display Filter). При использовании только фильтра отображения, программа Network Monitor перехватывает все пакеты в сети, но в рабочем окне Frame Summary отображаются только те, которые удовлетворяют условиям фильтрации. Поэтому в данной работе целесообразно использовать фильтр отображения,

поскольку применение различных вариантов фильтрации к накопленному множеству пакетов позволит быстро найти нужные данные. При использовании же фильтра захвата часть пакетов, в которых возможно нахождение нужной информации, будет недоступна.

Требования к содержанию отчета

В отчете по работе следует документировать выполнение каждого этапа задания. Словесное описание выполненных действие следует иллюстрировать экранными снимками. Отчет должен обязательно содержать следующую информацию:

1. тексты исходного и искаженного сообщений;
2. скрипты использованных фильтров пакетов в программе Network Monitor;
3. экранные снимки рабочего окна программы Network Monitor, в котором видны перехваченные учетные данные соединения с FTP-сервером, а также имена передаваемых Абонентами файлов.

Контрольные вопросы

1. Каким способом возможен перехват учетных данных пользователей FTP-сервера?
2. Каково основное функциональное назначение программы Network Monitor?
3. Какими возможностями располагает программа Network Monitor для оптимизации анализа перехваченных пакетов?
4. Какие меры могу предпринять пользователи сети для противодействия попыткам ознакомления и искажения передаваемой информации?

ЛАБОРАТОРНАЯ РАБОТА №4. ЗАЩИТА ПЕРЕДАВАЕМЫХ ДАННЫХ С ПОМОЩЬЮ ШИФРОВАНИЯ И ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Цель работы

Приобрести навыки защиты и верификации передаваемых данных с помощью механизма шифрования и электронной цифровой подписи, используя программный продукт КриптоАРМ.

Основные сведения о программе *КриптоАРМ*

Продуктовая линейка «КриптоАРМ» предназначена для решения задач защиты и обеспечения юридической значимости любых видов электронного документооборота.

Программа *КриптоАРМ* предназначена для надежной защиты (шифрования) и аутентификации авторства (электронной цифровой подписи) документов и файлов, передаваемых по открытым незащищенным каналам связи (по Интернету).

Криптопровайдер (CSP, Cryptographic Service Provider) — независимый программный модуль, интегрированный в MS Windows и содержащий библиотеку криптографических функций со стандартизованным интерфейсом. CSP выполняет следующие криптографические функции:

- формирование/проверка электронной цифровой подписи (ЭЦП),
- шифрование информации,
- хранение ключей всех типов.

Криптопровайдер предназначен для авторизации, обеспечения конфиденциальности и юридической значимости электронных документов при обмене ими между пользователями, контроля целостности информации и др.

В составе ОС Windows пользователь получает несколько CSP, которые реализуют наиболее часто используемые методы шифрования. Наряду со стандартными криптопровайдерами, поставляемыми Microsoft, можно использовать CSP собственной разработки, предварительно сертифицировав его.

Использование MS Windows CSP иногда бывает неприемлемо по разным причинам (например, государственными органами или организациями). Если организация использует стандартные криптопровайдеры Windows (несертифицированные в России криптографические алгоритмы шифрования и ЭЦП данных), согласно действующему на территории России законодательству она не может вести обмен документами с государственными учреждениями. Для этого фирме требуется использовать сертифицированный ФСБ (ФАПСИ) криптопровайдер, который позволит обеспечить юридическую значимость электронных документов при обмене ими между пользователями.

Вы можете работать с программой *КриптоАРМ* через главное окно, представленное в двух видах:

1. Вид "Пользователь" – режим предназначен для выполнения базовых операций по шифрованию, подписи данных и работе с цифровыми сертификатами
2. Вид "Эксперт" – режим предназначен для выполнения всех криптоопераций и управления криптопровайдерами, сертификатами и настройками программы

Для выполнения работы не следует изменять никакие настройки программы, заданные по умолчанию.

С помощью программы *КриптоАРМ* вы можете управлять сертификатами и запросами в УЦ, списками отзыва сертификатов и ключевыми носителями.

Так как в цифровом сертификате, наряду с открытым ключом, присутствует также другая информация, имеющая определенный срок действия, жизненный цикл сертификата имеет ряд отличий от жизненного цикла ключа. Он включает в себя следующие основные фазы:

1. Создание запроса в Удостоверяющий Центр на выпуск сертификата открытого ключа,
2. Верификация запроса (проверка Удостоверяющим центром корректности данных),
3. Выпуск сертификата в соответствии с данными, указанными в запросе, и действующей политикой сертификации,
4. Распространение сертификата среди участников информационной системы,
5. Хранение и выдача сертификата по запросу пользователей и владельцев сертификатов,
6. Приостановка и возобновление действия сертификата,
7. Обновление информации, содержащейся в сертификате, и ключевой пары
8. Отзыв сертификата по запросу владельца или уполномоченного органа

В ходе выполнения лабораторной работы необходимо создать самоподписанный сертификат.

Самоподписанный сертификат – сертификат, изданный самим пользователем, без обращения к доверенной стороне Удостоверяющему центру. Самоподписанный сертификат является одновременно личным и корневым (устанавливается в Личное хранилище сертификатов и «Доверенные корневые центры сертификации»).

Самоподписанные сертификаты используются для обмена зашифрованными или подписанными документами между людьми, доверяющими друг другу, например, друзьями, коллегами. Обменявшись такими сертификатами между собой, они могут пересылать друг другу подписанные и зашифрованные электронные данные, не беспокоясь при этом, что информация может быть перехвачена, искажена и использована против их интересов.

Важно помнить, что использование самоподписанных сертификатов не позволяет решать конфликтные ситуации, возникающие при обмене конфиденциальными данными, с помощью суда. Законодательно

регламентировано получение сертификатов в доверенных Удостоверяющих центрах РФ (Федеральный закон «Об электронной цифровой подписи» от 10.01.2002 №1-ФЗ): «…сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи…»

Самоподписанный сертификат может использоваться и для криптографической защиты собственной информации. В этом случае вам не потребуется помнить пароль, который вы должны были бы применять при использовании программ для защиты дискового пространства, упаковки файлов с паролем и в иных ситуациях.

Программа *КриптоАРМ* позволяет экспортировать сертификат из хранилища в файл.

Экспорт сертификата может понадобиться для выполнения следующих задач:

- архивирование сертификата;
- архивирование сертификата и связанного с ним закрытого ключа;
- копирование сертификата для использования на другом компьютере;
- удаление сертификата и его закрытого ключа с компьютера владельца сертификата для установки на другом компьютере.

Когда сертификат экспортируется, он копируется из хранилища сертификатов в файл, использующий стандартный формат хранения сертификатов.

Для того чтобы установить сертификат в хранилище сертификатов, необходимо выполнить импорт сертификата. Импорт сертификатов может понадобиться для выполнения следующих задач:

- установка сертификата, который был отправлен вам в файле другим пользователем, компьютером или центром сертификации
- восстановление поврежденного или утерянного сертификата, заархивированного ранее
- установка сертификата и связанного с ним закрытого ключа с компьютера, на котором владелец сертификата его использовал ранее

Первичная установка в хранилище личного сертификата ГОСТ может выполняться как средствами криптопровайдера *КриптоПро CSP*, так и средствами ПО *КриптоАРМ*.

Хранение секретных ключей в тайне является главным требованием при эксплуатации системы электронной цифровой подписи. Одним из эффективных способов хранения секретных ключей является использование отчуждаемых носителей.

Отчуждаемые носители - это портативные устройства, выполненные в форме USB-брелка или смарт-карты, обеспечивающие хранение конфиденциальной ключевой информации и аутентификацию пользователя.

Наиболее функциональным, перспективным, удобным и эргономичным носителем ключевой информации в настоящее время считается USB брелок.

Для получения доступа к защищённым на компьютере и в сети данным он не требует никаких дополнительных устройств считывания информации и подключается к компьютеру через usb-порт. USB-брелки удобно и просто использовать. Нужно всего лишь вставить идентификатор в USB-порт, а затем набрать на клавиатуре PIN-код. USB-брелок удобно носить на связке ключей.

Краткая характеристика работы

Работа выполняется бригадой, состоящей не менее чем из двух студентов.

В процессе работы участники бригады создают собственные самоподписанные сертификаты, причем каждый участник передает свой сертификат остальным коллегам. Это позволяет в дальнейшем производить обмен зашифрованными и подписанными с помощью электронной цифровой подписи сообщениями. Тем самым каждый участник может удостовериться, что благодаря шифрованию содержание сообщения будет недоступно для ознакомления посторонним лицам. При этом подлинность автора подтверждается электронной цифровой подписью.

После создания и распространения самоподписанных сертификатов, каждый участник создает текстовый файл с сообщением, шифрует и подписывает его, используя свой сертификат. Защищенный таким способом файл сообщения передается другим участникам бригады любым доступным способом.

Получив шифрованные и подписанные файлы сообщений, каждый участник бригады расшифровывает и знакомится с их содержанием, используя при этом свой сертификат.

Для выполнения лабораторной работы следует использовать ПО *КриптоАРМ*.

Порядок выполнения работы

Перед началом работы каждый участник занимает отдельное рабочее место с установленной программой *КриптоАРМ*. Если на рабочем месте установлен криптопровайдер, поддерживающий USB-ключ, то его следует получить у преподавателя или лаборанта.

Выполнение работы проходит в три этапа. **Каждый участник бригады**, находясь на своем рабочем месте, самостоятельно выполняет перечисленные ниже действия.

Этап I. Обмен сертификатами

1. Создать самоподписанный сертификат. При создании сертификата следует указать наиболее полную идентификационную информацию о себе. В качестве идентификатора задать свою фамилию с инициалами.

2. Экспортировать свой сертификат в файл. Передать созданный файл сертификата остальным участникам своей бригады любым способом, например через общую сетевую папку.

3. Получить файлы сертификатов от остальных участников своей бригады.

4. Импортировать сертификаты других участников своей бригады в хранилища сертификатов своего рабочего места:

а) импортировать сертификаты в «Доверенные корневые центры сертификации»;

б) импортировать сертификаты в «Сертификаты других пользователей».

Этап II. Обмен защищенными сообщениями

5. С помощью текстового редактора *Блокнот* создать текстовый документ, содержащий сообщение участникам своей бригады.

6. В программе *КриптоАРМ* зашифровать созданный файл и подписать его электронной цифровой подписью, используя свой сертификат. В списке получателей указать свой сертификат, а также сертификаты других участников своей бригады.

7. Передать зашифрованный и подписанный файл другим участникам бригады любым способом, например через общую сетевую папку.

8. Получить зашифрованные и подписанные файлы сообщений от других участников бригады.

Этап III. Расшифрование сообщений и проверка подлинности

9. Расшифровать полученные сообщения.

10. Просмотреть информацию о сертификатах отправителей.

11. Открыть расшифрованные файлы в текстовом редакторе *Блокнот* и ознакомиться с их содержанием.

Методические указания по выполнению работы

Перед тем, как приступить к работе с ПО *КриптоАРМ*, следует изучить основные термины и понятия криптографии, порядок работы с цифровыми сертификатами, ознакомиться с установленными в системе криптопровайдерами.

Запустив ПО *КриптоАРМ*, следует изучить интерфейс главного окна в режимах *Пользователя* и *Эксперта*. При этом целесообразно использовать справочную систему программы.

Для хранения рабочих файлов следует создать папку на локальном диске. По окончании оформления и сдачи отчета созданную папку можно удалить.

Требования к содержанию отчета

Каждый участник бригады самостоятельно готовит и оформляет свой отчет по работе, описывая проделанную им работу.

В отчете следует документировать выполнение каждого этапа задания. Словесное описание выполненных действий следует иллюстрировать экранными снимками. Отчет должен обязательно содержать следующую информацию:

1. регистрационные данные своего сертификата;

2. имя созданного файла сообщения и его текст;
3. параметры шифрования и электронной цифровой подписи;
4. имя своего зашифрованного и подписанного файла с сообщением;
5. порядок экспорта своего сертификата для последующего распространения;
6. порядок импорта сертификатов остальных участников бригады, название хранилища сертификатов, в которое они были импортированы;
7. содержимое полученных от остальных участников бригады шифрованных файлов;
8. расшифрованные сообщения;
9. функциональное описание опций меню ПО *КриптоАРМ*, которые были использованы при выполнении заданий.

Контрольные вопросы

1. Что называется шифрованием?
2. Что такое электронная цифровая подпись?
3. Что такое запрос в Удостоверяющий центр, как он создается и передается?
4. Что такое криптопровайдер? Как просмотреть список криптопровайдеров, доступных для работы в системе и свойства каждого криптопровайдера?
5. Что представляют собой электронные ключи и в чем их преимущества?
6. Что такое самоподписанный сертификат и в чем его отличие от сертификата, полученного в Удостоверяющем центре?
7. Каковы основные фазы жизненного цикла сертификата?

ЛАБОРАТОРНАЯ РАБОТА №5. РАБОТА С ЗАЩИЩЕННЫМИ ДИСКАМИ

Цель работы

Приобрести навыки работы с защищенными дисками на локальной рабочей станции с помощью программного пакета *Secret Disk NG*.

Краткие теоретические сведения

Программно-аппаратный комплекс *Secret Disk NG* защищает конфиденциальную информацию на персональном компьютере. С его помощью вы можете создавать на рабочей станции так называемые защищённые диски (*секретные диски*) – диски с зашифрованным содержимым, работать с которыми можете только вы и ваши доверенные лица. Любой другой пользователь, пусть даже наделённый административными полномочиями на данном компьютере, не может получить доступ к защищённым дискам.

Защита конфиденциальной информации обеспечивается шифрованием данных «на лету» с помощью надежных алгоритмов шифрования. При чтении данных с защищенного диска происходит их расшифрование, при записи на диск — зашифрование. Находящиеся на защищенном диске данные всегда зашифрованы.

Secret Disk NG позволяет превращать существующие диски, в том числе съёмные, в защищённые тома, а также создавать так называемые защищённые виртуальные диски. Всё содержимое защищённого виртуального диска хранится в одном файле в зашифрованном виде. Подключенный защищённый виртуальный диск операционная система воспринимает как обычный диск. Удаление файла подключенного защищённого виртуального диска невозможно.

Управление *Secret Disk NG* тесно интегрировано с операционной системой Windows 2000/XP и предоставляет возможность удаленного администрирования защищенных дисков. Непосредственная работа с защищенными дисками предполагается только с локального компьютера.

Для доступа к защищённым дискам используется персональный USB-ключ или смарт-карта *eToken*. По умолчанию работа с защищёнными дисками возможна только при наличии *eToken*. Если вы отключаете *eToken*, то все защищённые диски автоматически становятся недоступными. Отключенные защищённые тома операционная система воспринимает как неформатированные.

Secret Disk NG не имеет встроенных средств шифрования. В *Secret Disk NG* применяются установленные в данной операционной системе криптопровайдеры. В качестве криптопровайдера *Secret Disk NG* может использовать:

- *Microsoft Enhanced CSP* (стандартный поставщик криптографии, для шифрования дисков по умолчанию можно применять алгоритмы DES, RC2 и Triple DES);

- *Signal-COM CSP* (для шифрования дисков используется алгоритм, соответствующий ГОСТ 28147-89 «Система обработки информации. Защита криптографическая»);
- *КриптоПро CSP 2.0* (для шифрования дисков применяется алгоритм, соответствующий ГОСТ 28147-89).

Использование Secret Disk NG

При обращении к инструментам управления *Secret Disk NG* необходимо подключить к компьютеру свой *eToken* с лицензией *Secret Disk NG*, указать свой сертификат. Если на рабочем месте используется несколько криптопровайдеров, то в процессе аутентификации можтно применять любой из сертификатов, связанных в системе *Secret Disk NG* с вашей учётной записью.

Подключив eToken и указав сертификат, вы вводите PIN-код, подтверждая тем самым владение соответствующим закрытым ключом. Таким образом, аутентификация пользователя в Secret Disk NG 3.1.2 основана на двух факторах:

1. владение *eToken*;
2. знание PIN-кода.

Ярлыки *Secret Disk NG* в меню *Пуск/Start* располагаются в группе *Все программы (Программы)/All Programs (Programs) > Secret Disk NG*.

В группу *Secret Disk NG* входят следующие ярлыки:

- *Secret Disk NG* – открывает сеанс пользователя *Secret Disk NG*. Если *eToken* с лицензией *Secret Disk NG*, принадлежащий пользователю, зарегистрированному на данной рабочей станции, подключен к компьютеру, то после того как вы выберете этот пункт, на панели задач появится значок Secret Disk NG.
- *Новый пользователь* – открывает диалоговое окно для регистрации нового пользователя *Secret Disk NG* на данном компьютере;
- *Помощь по Secret Disk* – открывает файл справки *Secret Disk NG*;
- *Удалить Secret Disk NG* – вызывает программу удаления системы *Secret Disk NG*.

В *Secret Disk NG* наборы операций, которые можно совершать над тем или иным диском, различаются у разных пользователей. У защищённого диска может быть только один владелец. Другие пользователи *Secret Disk NG* на данном компьютере не могут форматировать, перешифровывать этот защищённый диск и выполнять ряд других операций. Более того, подключать защищённый диск могут не все пользователи *Secret Disk NG*, а только те, кому владелец предоставил соответствующие права.

Режим работы *Secret Disk NG*, при котором один из пользователей может реализовывать свои полномочия для подключения и отключения защищённых дисков, зашифрования, перешифрования, расшифрования, выполнения операций с резервными копиями мастер-ключей и настройки параметров работы *Secret Disk NG*, называется сеансом данного пользователя.

Поскольку в *Secret Disk NG* в качестве идентификаторов пользователя используются его сертификаты, добавление пользователя – это регистрация имени пользователя, комментария и сертификатов в защищённом хранилище.

Для добавления нового пользователя учетная запись, под которой выполнен вход в систему, должна иметь полномочия администратора.

Для того чтобы зарегистрировать пользователя, необходимо выполнить следующие действия.

1. В окне *Secret Disk NG: новый пользователь* внесите информацию о пользователе в поля *Имя* и *Комментарий*.

Выберите для добавляемого пользователя *Secret Disk NG* сертификат(ы) для защиты мастер-ключей защищённых дисков и аутентификации. Для каждого из поставщиков криптографии:

- если у вас имеется *eToken* добавляемого пользователя, подключите его к компьютеру, нажмите *Выбрать* и выберите сертификат (а если в памяти *eToken* нет подходящего сертификата – сгенерируйте сертификат с закрытым ключом);
- если вы располагаете копией сертификата, хранящейся в файле .CER, нажмите Выбрать из файла и укажите путь к файлу.

3. Нажмите *Добавить*.

4. В случае успешной регистрации нового пользователя *Secret Disk NG* на данном компьютере, на экране появится окно с сообщением «*Пользователь успешно зарегистрирован на данном компьютере*».

Пользователь может подключить защищённый диск, только если у него есть право доступа к нему, которое возникает в двух случаях:

- если он сам создал этот диск (то есть является его владельцем);
- если владелец диска предоставил данному пользователю право доступа.

Для того чтобы подключить защищённый диск, необходимо выполнить следующие действия.

1. Убедиться в том, что *eToken* с лицензией и сертификатом подключен к компьютеру.

2. Если сеанс пользователя не открыт, то его следует открыть, запустив *Secret Disk NG* из меню *Пуск/Start (Все программы (Программы)/All Programs (Programs) > Secret Disk NG > Secret Disk NG)*.

3. Щёлкнуть правой кнопкой мыши на значке *Secret Disk NG* на панели задач.

4. В меню *Secret Disk NG* выбрать пункт *Подключить*. Появится список доступных отключенных защищённых дисков.

5. Выбрать защищённый диск, который следует подключить, или пункт *Подключить все* для одновременного подключения всех доступных защищённых дисков.

6. При необходимости следует выбирать считыватели (*eToken*) и вводить PIN-код (интерфейс зависит от поставщика криптографии).

В случае успешного подключения защищённого диска над значком *Secret Disk NG* на панели задач появится сообщение: «*Защищённый диск подключен*»

Все защищённые диски отключаются при закрытии сеанса пользователя.

Для того чтобы отключить один или несколько защищённых дисков, не закрывая сеанса пользователя, необходимо выполнить следующее.

Закрыть все приложения, обращающиеся к защищенному диску. Для корректного отключения защищённого диска на нём не должно быть ни одного открытого документа.

Щёлкнуть правой кнопкой мыши на значке *Secret Disk NG* на панели задач.

Выбрать пункт *Отключить*. Появится список подключенных защищённых дисков.

Выберать защищённый диск, который следует отключить, или пункт *Отключить все* для одновременного отключения всех подключенных защищённых дисков.

Если отключаемый диск занят, на экране появится диалоговое окно *Secret Disk NG: отключение диска*. Закройте все приложения, работающие с диском, и нажмите *Да*. Если вы в данный момент отпала необходимость отключать диск, нажмите *Нет*.

В случае успешного отключения диска над значком *Secret Disk NG* на панели задач будет выведено сообщение: «*Защищённый диск отключен*».

Утилита для управления электронным ключом eToken

Для выполнения лабораторной работы используется электронный ключ *eToken PRO* – USB-ключ с аппаратной поддержкой шифрования по алгоритму RSA с ключом 1024 бит. В *eToken PRO*, кроме PIN-кода, может быть задан пароль администратора. С помощью него, например, можно сменить забытый PIN-код. Помимо аппаратной задержки отклика, для защиты от подбора PIN-кода для *eToken PRO* может быть установлено число возможных попыток неправильного ввода PIN-кода подряд, при превышении которого *eToken* блокируется.

Утилита *eToken Properties*, устанавливаемая вместе с *eToken RTE*, служит для настройки параметров *eToken* и его драйверов, просмотра общей информации относительно *eToken*, хранящихся в памяти *eToken* сертификатов и ключевых контейнеров RSA, а также удаления просматриваемых сертификатов вместе с соответствующими закрытыми ключами.

Для того чтобы запустить *eToken Properties*, щёлкните *Пуск/Star t> Все программы (Программы)/All Programs (Programs) > eToken*. В результате этого появится окно, вид которого приведен на рисунке 5.1.

Для того чтобы приступить к настройке общих параметров *eToken RTE*, в окне *eToken Properties* нажмите *Local Machine*.

Подробное описание настройки общих параметров можно прочитать в пользовательской документации к утилите.

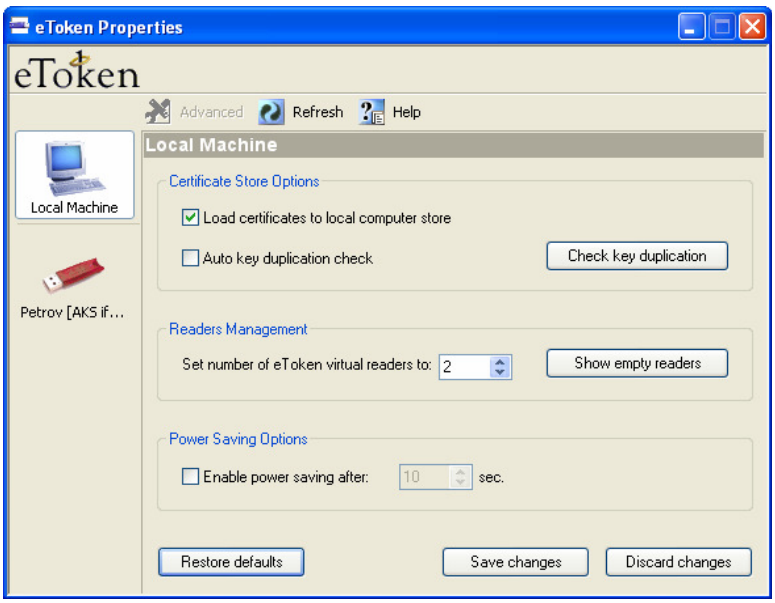

Рис. 5.1 Окно настройки свойств электронного ключа

Для осуществления операций с одним из подключенных *eToken*, отображённым в окне *eToken Properties*, выберите этот *eToken*. В окне *eToken Properties* появится общая информация относительно данного *eToken* (рисунок 5.2).

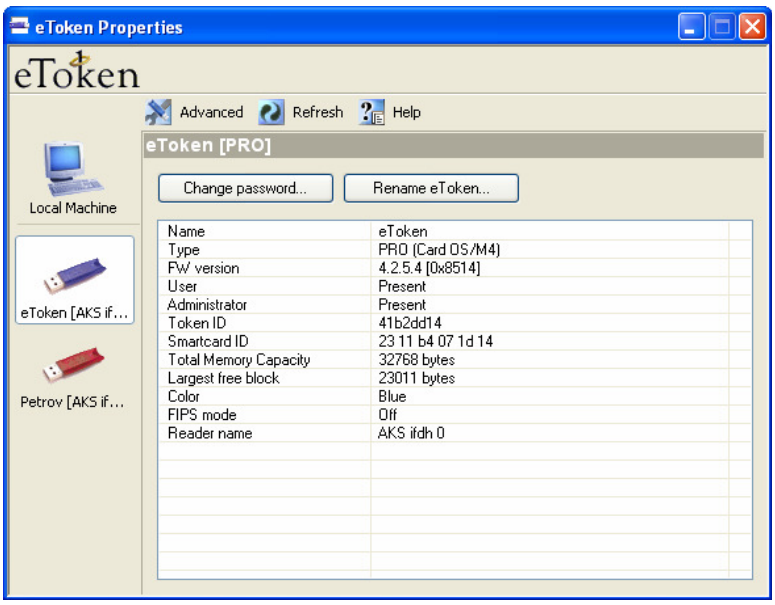

Рис. 5.2 Окно настройки свойств электронного ключа

Настройка выбранного ключа осуществляется нажатием на кнопку *Advanced*. После этого следует ввести пароль для доступа к защищенной области. Если вводится пароль администратора, то необходимо поставить галочку в соответствующем поле окна ввода пароля.

Управление сертификатами и ключами, хранящимися в памяти *eToken*, осуществляется на вкладке *Certificates & keys*. Вид вкладки приведен на рисунке 5.3.

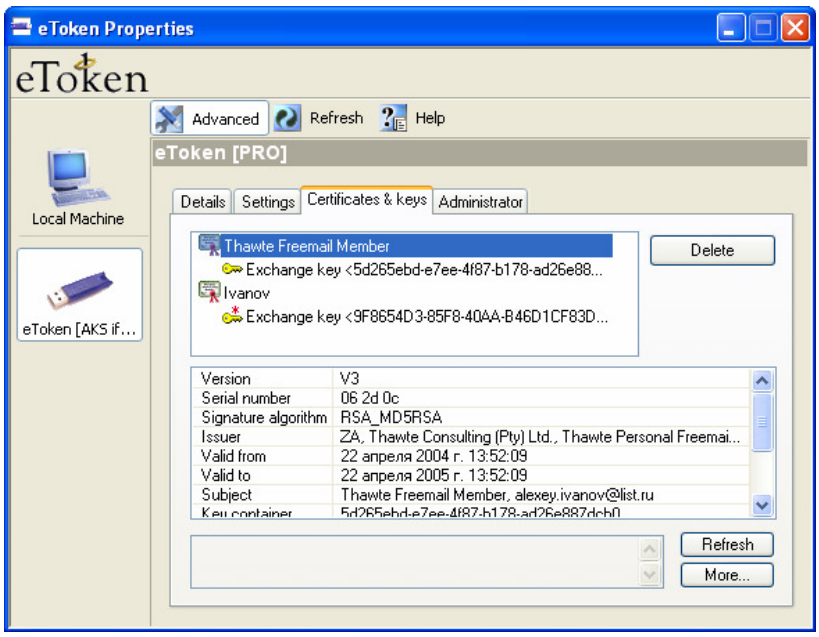

Рис. 5.3 Вид вкладки управления сертификатами и ключами

Как видно из рисунка 5.3, в окне отображается подробная информация о выбранном сертификате или ключе. Для удаления сертификата или ключа следует нажать кнопку *Delete*.

Для выхода из программы необходимо просто закрыть основное окно *eToken Properties*.

Характеристика работы

Работа выполняется в индивидуальном порядке каждым студентом. В ходе работы студент создает в системе *Secret Disk NG* нового пользователя со своими учетными данными, используя электронный ключ *eToken*. Используя свой пользовательский сертификат, следует создать виртуальный защищенный диск, изучить порядок работы с ним, а также назначение и алгоритм выполнения различных сервисных операций.

Для хранения рабочих файлов следует создать папку на локальном диске. По окончании оформления и сдачи отчета созданную папку можно удалить.

Порядок выполнения работы

Приступая к работе с программой *Secret Disk NG*, следует изучить основные термины и понятия криптографии, порядок работы с цифровыми сертификатами, ознакомиться с установленными в системе криптопровайдерами.

Перед началом работы следует получить у лаборанта электронный ключ *eToken*, узнать у него соответствующий PIN-код и занять пользовательское рабочее место с установленной программой *Secret Disk NG*. При использовании, электронный ключ следует вставлять только в тот USB-разъем рабочего места, который указан лаборантом.

Если при попытке записи в память электронного ключа нового сертификата возникает ошибка переполнения, то следует удалить сертификаты и ключи с помощью утилиты управления *eToken* (подробное руководство по работе с сертификатами и ключами см. выше).

При возникновении ошибки во время создания нового пользователя следует убедиться, что текущая учетная запись в системе обладает правами администратора локальной машины.

В ходе работы следует выполнить перечисленные ниже действия.

1. Создать в программе *Secret Disk NG* нового пользователя, введя в соответствующие поля информацию о себе.
2. В процессе создания нового пользователя создать личный сертификат.
3. Начать сеанс работы с *Secret Disk NG* и создать новый защищенный диск объемом 10 Мб. Имя файла защищенного диска и метка тома должны содержать фамилию создателя. При этом обязательно следует сохранить копию мастер-ключа в файле.
4. Подключить защищенный диск и проверить его работоспособность, записав на него один или несколько файлов.
5. Отключить защищенный диск и убедиться в том, что он больше недоступен в системе.
6. Вновь подключить защищенный диск и проверить его работоспособность, создав на нем один или несколько файлов.
7. Удалить защищенный диск из списка доступных дисков. Убедиться, что файл защищенного диска не удален.
8. Добавить свой защищенный диск в список доступных, восстановив его мастер-ключ из файла.
9. Подключить защищенный диск и проверить его работоспособность, прочитав записанные на нем файлы.
10. Выполнить перешифрование защищенного диска, указав другой алгоритм шифрования (например, DES-56 bit). Сохранить мастер-ключ только в памяти *eToken*. Убедиться, что мастер-ключ действительно записан в память *eToken*.
11. Удалить защищенный диск из списка доступных дисков. Убедиться, что файл защищенного диска не удален.
12. Восстановить доступ к диску, используя созданный на шаге 3 файл мастер-ключа. Подключить защищенный диск и сделать попытку прочитать с него файлы. Убедиться, что это невозможно.
13. Удалить защищенный диск из списка доступных дисков и сразу восстановить доступ к нему, используя мастер-ключ только из памяти *eToken*.
14. Проверить работоспособность защищенного диска, создав на нем один или несколько файлов.

После подготовки отчета удалить все резервные копии мастер-ключей.. С помощью утилиты *eToken PRO Properties* удалить из памяти *eToken* все сертификаты пользователей. Удалить созданные в ходе выполнения работы файлы мастер-ключей и защищенных дисков.

Требования к содержанию отчета

В отчете по работе следует документировать выполнение каждого этапа задания. Необходимо указывать, какие пункты меню и элементы управления программного интерфейса были использованы для выполнения задания.

Документальное описание выполненных действий следует иллюстрировать экранными снимками. При этом в тексте отчета должна содержаться исчерпывающая информация о сути выполняемых операций, вводимых параметров и т.п.

Контрольные вопросы

1. В чем суть механизма защиты информации с помощью *Secret Disk NG*?
2. Что называется защищенным томом?
3. Какие средства идентификации и аутентификации используются для доступа к защищенным томам, созданным с помощью *Secret Disk NG*?
4. Какие средства шифрования может использовать *Secret Disk NG*?
5. В чем суть перешифрования защищенного диска?
6. Какая утилита используется для работы с электронными ключами?
7. Перечислите места, в которых можно хранить резервные копии мастер-ключей.

ОБЩИЕ ТРЕБОВАНИЯ К СОДЕРЖАНИЮ И ОФОРМЛЕНИЮ ОТЧЕТА

Отчет, в зависимости от требований задания лабораторной работы, всеми участниками готовится совместно или каждым студентом самостоятельно и индивидуально. Детализированные требования к составу отчета находятся в соответствующем разделе каждой лабораторной работы.

Изложение текста должно быть последовательным и логичным, с правильным использованием специальных технических терминов; не допускается использование жаргонизмов. Текст отчета должен быть кратким, четким и не допускать различных толкований.

В отчете должны применяться научно-технические термины, обозначения и определения, установленные соответствующими стандартами, а при их отсутствии – общепринятые в научно-технической литературе.

Если в отчете используется специфическая терминология, то в конце его (перед списком литературы) должен быть перечень принятых терминов с соответствующими разъяснениями. Перечень включают в содержание документа.

В тексте отчета **не допускается**:

- применять обороты разговорной речи, техницизмы, профессионализмы;
- применять для одного и того же понятия различные научно-технические термины, близкие по смыслу (синонимы), а также иностранные слова и термины при наличии равнозначных слов и терминов в русском языке;
- применять произвольные словообразования;
- применять сокращения слов, кроме установленных правилами русской орфографии, соответствующими государственными стандартами, а также в данном документе;
- сокращать обозначения единиц физических величин, если они употребляются без цифр, за исключением единиц физических величин в головках и боковиках таблицей в расшифровках буквенных обозначений, входящих в формулы и рисунки.

В тексте отчета числовые значения величин с обозначением единиц физических величин и единиц счета следует писать цифрами, а числа без обозначения единиц физических величин и единиц счета от единицы до девяти – словами.

Если в тексте документа приводят диапазон числовых значений физической величины, выраженных в одной и той же единице физической величины, то обозначение единицы физической величины указывается после последнего числового значения диапазона.

Количество иллюстраций должно быть достаточным для пояснения излагаемого текста. Иллюстрации могут быть расположены как по тексту документа (возможно ближе к соответствующим частям текста), так и в конце его. Иллюстрации должны быть выполнены в соответствии с требованиями стандартов ЕСКД и СПДС. Иллюстрации за исключением иллюстраций приложений, следует нуме-ровать арабскими цифрами сквозной нумерацией. Если рисунок один, то он обозначается «Рисунок I».

При ссылках на иллюстрации следует писать «... в соответствии с рисунком 2» при сквозной нумерации и «... в соответствии с рисунком 1.2» при нумерации в пределах раздела.

Иллюстрации, при необходимости, могут иметь наименование и пояснительные данные (подрисуночный текст). Слово «Рисунок» и наименование помещают после пояснительных данных и располагают следующим образом: Рисунок 1 – Детали прибора.

На все рисунки должны быть ссылки в тексте отчета. При этом ссылка должна размещаться перед соответствующим рисунком или таблицей.

Таблицы применяют для лучшей наглядности и удобства представления материала. Название таблицы, при его наличии, должно отражать ее содержание, быть точным, кратким. Название следует помещать над таблицей.

При переносе части таблицы на ту же или другие страницы название помещают только над первой частью таблицы.

Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

На все таблицы документа должны быть приведены ссылки в тексте документа, при ссылке следует писать слово "таблица" с указанием ее номера.

Следует придерживаться следующей структуры отчета:

1. титульный лист;
2. цель работы;
3. краткая информация об изучаемых программно-аппаратных средствах обеспечения безопасности информации;
4. формулировка решаемых задач;
5. поэтапное описание процесса выполнения работы;
6. выводы и рекомендации.

Рассмотрим подробнее содержание разделов отчета.

Отчет следует выполнять в соответствии с ГОСТ 2.105 – 95 «Общие требования к текстовым документам».

Титульный лист должен содержать названия вуза, факультета и кафедры, порядковый номер лабораторной работы и ее тему, фамилии авторов и преподавателя, город и год подготовки отчета.

Цель работы формулируется на основе методических указаний по выполнению работы.

В *теоретическом разделе* следует привести общую характеристику изучаемых программно-аппаратных средств и их назначение. Указать типовые задачи, для решения которых используются указанные средства. Привести описание настраиваемых в ходе выполнения лабораторной работы параметров и их возможных значений.

Формулировки решаемых задач следует взять из методических указаний по выполнению работы.

Основным разделом отчета является *поэтапное описание* проделанной работы с указанием конкретных действий, которые были произведены в целях выполнения поставленной задачи.

Текст отчета должен содержать детальные пояснения хода работы над выполнением задания. Следует указывать, какие опции меню использовались, какие параметры были введены, в чем выразился результат применения введенных настроек.

Для иллюстрации выполненной работы в отчет следует включать экранные снимки окон, в которых выполнялась работа.

По окончании работы необходимо сформулировать *выводы и рекомендации*, которые содержат краткий анализ выполненной работы и подведение итогов.

Выводы должны отражать суть проделанной работы, а также полученные новые знания и навыки.

Целесообразно провести критическую оценку функциональных возможностей изученного аппаратно-программного средства с точки зрения безопасности автоматизированных систем. Следует описать угрозы безопасности информации, противодействие которым может быть организовано с использованием рассматриваемого средства защиты информации, дать оценку его эффективности.

Рекомендации должны содержать описание возможных уязвимостей в системе безопасности, которые могут возникнуть в результате нецелевого или неправильного использования и/или настройки рассматриваемого средства защиты, а также меры, которые следует предпринять для минимизации негативных последствий.

Отчет готовится в электронном виде и помещается в указанную преподавателем папку на сервере. Имя файла отчета должно содержать фамилии его авторов. Целесообразно создать резервную копию отчета на локальном диске и/или съемном запоминающем устройстве.

Распечатка отчета необязательна.

ЗАКЛЮЧЕНИЕ

Рассмотренные в данном издании средства защиты компьютерной информации, конечно же, не закрывают весь спектр угроз безопасности информации. Кроме этого, всегда следует помнить, что методы и средства осуществления угроз безопасности информации постоянно совершенствуются. С развитием систем обработки и передачи данных появляются новые виды угроз. Поэтому постоянное развитие претерпевают и системы защиты информации. Наряду с этим агенты угроз ведут систематический поиск новых уязвимостей в существующих пользовательских приложения, информационных службах и системах защиты.

Все это говорит о том, что современному специалисту по защите информации необходимо постоянно обновлять и расширять свои знания о существующих угрозах, уязвимостях и современных средствах и методах обеспечения информационной безопасности.

Важно понимать, что защита информации не ограничивается техническими методами. Действительно, системы криптографической защиты, например, будут бессильны, если пользователь использует слишком простые пароли, или хранит их в ненадежном месте. Большое количество угроз несанкционированного доступа к конфиденциальной информации могут быть реализованы по причине неправильной работы пользователей компьютерной системы вследствие незнания основ сетевой безопасности.

Обучение пользователей правилам сетевой безопасности может предотвратить многие сетевые атаки. Защита информации включает в себя кроме технических мер еще и обучение или правильный подбор обслуживающего персонала.

Помимо этого, защита должна постоянно совершенствоваться вместе с развитием компьютерной сети.

Опасно недооценивать и так называемые внутренние ИТ-угрозы, обусловленные действиями легальных пользователей корпоративной системы. При настройке рассмотренных в данном издании систем защиты информации следует учитывать возможные негативные последствия злонамеренных действий легальных пользователей.

Поэтому специалист по защите информации пристально внимание должен уделять также разработке административного регламента работы пользователей с корпоративной информационной системой, информационной политике и документальному сопровождению системы безопасности.

В настоящее время обобщенная теория безопасности информации пока не создана. Применяемые на практике подходы и средства нередко страдают недостатками и не обладают объявленной надежностью. Поэтому необходимо обладать достаточной подготовкой и квалифицированно ориентироваться во всем спектре вопросов обеспечения информационной безопасности, понимая их комплексный и взаимообусловленный характер.

Примерные темы УИРС

1. **Разработка клиент-серверного приложения на основе протокола OpenSSL**
    a. Разработка сервера
    b. Разработка клиента

Краткое описание.
Данная тема направлена на изучение и реализацию возможностей создания распределенной корпоративной информационной системы с защищенными соединениями.
Следует создать два приложения: серверное и клиентское, которые запускаются на разных компьютерах локальной сети. Клиент позволяет отправлять серверу заданные варианты команд, например: запрос системного времени, запрос списка процессов, запрос скриншота и т.п. Сервер соответствующим образом реагирует. Обмен данными осуществляется по протоколу OpenSSL.
Среда разработки – C/C++
Тему выполняют 1-2 студента.
Ссылки по теме:
http://www.ibm.com/developerworks/ru/library/l-openssl3/
http://programmersforum.ru/showthread.php?p=743090

2. **Разработка обфускатора программного кода (или компилированного файла)**

Краткое описание.
В подробном описании не нуждается. Про обфускацию материалов много.
Среда разработки – C/C++
Тему выполняет 1 студент.
Ссылки по теме:
http://www.cyberguru.ru/dotnet/net-framework/net-obfuscation.html
http://www.stunnix.com/prod/cxxo/overview.shtml
http://www.plexaure.de/cobf/index.htm

3. **Реализация алгоритмов шифрования**
    a. Алгоритм Blowfish
    b. Алгоритм IDEA
    c. Алгоритм ГОСТ 28147

Краткое описание.
Написать программу, которая шифрует указанный файл по одному из алгоритмов шифрования.
Среда разработки – C/C++
Ссылки по теме:
http://www.intuit.ru/department/security/networksec/3/1.html
Оценка степени безопасности информационных технологий

Тест по дисциплине

Ф.И.О._____ Группа _____ Дата _____

ИНСТРУКЦИЯ

1. Для каждого вопроса следует выбрать только один, **наиболее правильный**, ответ.
2. Для указания Вашего варианта ответа следует поставить любой символ в соответствующем квадратике.
3. Во время проведения тестирования запрещается использование любых источников информации.

1. Под СВТ понимается:

- совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;
- электронные компоненты, из которых строятся вычислительные системы;
- совокупность программных и технических элементов систем передачи информации, используемая для построения компьютерных систем.

2. Под АС понимается:

- система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;
- локальная ПЭВМ или компьютерная сеть с установленным системным программным обеспечением и средствами коммуникации;
- автоматизированная система управления обработкой информации с целью выполнения производственных функций организации.

3. Под несанкционированным доступом в компьютерной системе понимается:

- доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС;
- доступ к информации с преодолением парольной защиты, фальсификации аутентификационной информации с использованием штатных средств, предоставляемых СВТ или АС;
- реализация угроз безопасности информации с целью ознакомления и/или уничтожения информации с использованием штатных или специальных СВТ.

4. К основным функциям СРД относятся:

- регистрация действий субъекта и активизированного им приложения;
- контроль целостности программной и аппаратной части СРД;
- реакция на попытки НСД;
- управление потоками информации в целях предотвращения записи её на носители несоответствующего уровня конфиденциальности.

5. К основным функциям СРД не относятся:

- реализация правил разграничения доступа субъектов и их процессов к информации и устройствам создания её твердых копий;
- изоляция процесса, выполняемого в интересах субъекта доступа, от других субъектов;
- идентификация и аутентификация субъектов и поддержание привязки субъекта к процессу, выполняемому для него.

6. К функциям обеспечивающих средств для СРД не относятся:

- учет выходных печатных и графических форм и твердых копий в КС;
- очистка оперативной памяти после завершения работы пользователя с защищаемыми данными;
- реализация правил обмена информацией между субъектами в компьютерных сетях.

7. Идентификация это:

- однозначное определение уникального имени, под которым пользователь зарегистрирован в КС;
- генерация уникального имени, под которым пользователь будет зарегистрирован в КС;
- проверка уникальности имени зарегистрированного в КС пользователя при запросе доступа к ресурсам КС;\

8. Аутентификация это:

- подтверждение подлинности имени, предъявленного пользователем;
- подтверждение заявленных пользователем прав доступа к ресурсам КС;
- проверка наличия введенного имени пользователя в регистрационной базе КС.

9. Авторизация это:

- процесс наделения пользователя индивидуальным набором привилегий в системе и определение его прав доступа к объектам КС;
- процесс определения набора информационных ресурсов, доступ к которым разрешен пользователю;
- проверка соответствия введенного пользователем пароля его идентификатору.

10. Аудит безопасности КС это:

- учет возникающих при работе системы событий, связанных с безопасностью информации в ней, и регистрация этих событий в системном журнале;
- учет попыток НСД и регистрация их в системном журнале;
- проверка соответствия защитных функций установленных в АС СЗИ требованиям, предъявляемым к СЗИ в АС;
- учет неудачных попыток ввода пароля и регистрация этих попыток в системном журнале.

11. Укажите наиболее правильную формулировку требований к «идеальной» системе защиты информации (СЗИ).

- СЗИ должна быть прозрачна для легальных пользователей и создавать непреодолимые трудности для реализации НСД.
- СЗИ должна обеспечивать уровень защищенности информации, соответствующий требованиям для данного класса АС.
- СЗИ должна обеспечивать защищенность информации на программном и аппаратном уровне, включать в себя подсистемы, использующие разные технологии ЗИ.

12. Выберите наиболее полное правило, которым следует руководствоваться при выборе паролей:

- пароли должны трудно подбираться и легко запоминаться;
- в паролях следует использовать буквы и цифры, причем длина пароля должна быть не менее 4 символов;
- в качестве паролей не следует использовать простые слова, имена собственные и т.п.

13. Выберите наиболее правильное описание начального этапа модели «рукопожатия».

- Система генерирует случайное значение **x**, вычисляет и сообщает **x** пользователю.
- Пользователь генерирует случайное значение **x**, вычисляет и вводит **x** в ответ на запрос системы.
- Система генерирует случайное значение **x**, вычисляет и сообщает **y** пользователю.
- Система генерирует случайное значение **x**, вычисляет и сообщает **x** и **y** пользователю.

14. К пассивным устройствам аутентификации не относятся:

- пластиковые карты с магнитной полоской
- элементы Touch Memory
- USB-ключи

15. Уязвимость информационной системы это:

- любая характеристика, использование которой нарушителем может привести к реализации угрозы;

- ошибки в программном обеспечении, возникновение которых может привести к реализации угрозы;
- количественная и качественная недостаточность средств ЗИ, которая может привести к реализации угрозы.

16. Угрозой информационной системе называется:

- потенциально возможное событие, действие, процесс или явление, которое может вызвать нанесение ущерба ресурсам системы;
- совокупность программно-аппаратных средств осуществления НСД при наличии методов их использования для нанесения ущерба ресурсам системы;
- возможность использования информации, штатных и нештатных технических средств АС для нанесения ущерба ресурсам системы.

17. Под информационной безопасностью понимается:

- защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры;
- комплекс программно-аппаратных средств направленных на защиту от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры;
- совокупность мер организационно-технического характера, направленных на защиту от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры;

18. Сущность комплексного подхода к ЗИ заключается в:

- сочетании различных мер обеспечения безопасности на законодательном, административном, процедурном и программно-техническом уровнях;
- сочетании различных мер обеспечения безопасности на законодательном и программно-техническом уровнях;
- сочетании различных программно-аппаратных средств защиты АС от НСД.

19. Аспекты обеспечения ИБ:

- формальный и практический;
- общий и частный;
- программный и аппаратный.

20. Укажите, что не является контекстом ЗИ и соответствующих бизнес-процессов:

- конфиденциальность;
- целостность;
- доступность;
- достоверность.

21. Основная цель сетевой ПБ:

- контроль сетевого трафика и его использования;
- противодействие попыткам НСД с использованием сетевой инфраструктуры;
- установка и правильная настройка программно-аппаратных СЗИ.

22. Под доверенными понимаются сети, …

- …над которыми специалисты организации имеют полный административный контроль;
- …на компьютерах которых установлены средства удаленного администрирования;
- оснащенные программно-аппаратными СЗИ и проходящие регулярные проверки на предмет вирусной активности.

23. Ресурсы (в контексте задачи управления рисками) это:

- то, что организация ценит и хочет защитить;
- финансовые и информационные активы организации;
- файлы и бумажные документы.

24. Политика информационной безопасности определяет:

- способы развертывания систем безопасности и поведение пользователей при использовании КС;
- способы настройки межсетевых экранов и антивирусных средств;
- порядок получения доступа пользователей к ресурсам КС организации.

25. Основная цель сетевой ПБ:

- описание топологии ЛВС и определение мест установки МЭ;
- контроль сетевого трафика и его использования;
- формирование требований к настройке МЭ и антивирусных систем;
- разрешить то, что явно не запрещено;
- запретить то, что явно не разрешено.

26. Выберите пункт из перечисленного ниже, который не относится к службам безопасности:

- аутентификация;
- целостность;
- информированность.

27. Под доверенными понимаются сети, …

- …на компьютерах которых установлены средства удаленного администрирования;
- …над которыми специалисты организации имеют полный административный контроль;
- оснащенные программно-аппаратными СЗИ и проходящие регулярные проверки на предмет вирусной активности.

28. Ресурсы (в контексте задачи управления рисками) это:

- информация и поддерживающие средства для ведения бизнеса;
- базы данных корпоративных информационных систем (бухгалтерских, аналитических и т.п.);
- файлы и бумажные документы;
- описания устройств и технологических процессов, являющиеся «ноу-хау» организации.

29. Угроза – это …

- …потенциальная причина нежелательного события, которое может нанести ущерб организации и её объектам;
- …сетевая атака, влекущая нарушение работоспособности КС организации;
- …потенциальная возможность НСД к конфиденциальной информации организации
- …совокупность вредоносного ПО, распространяющаяся по компьютерным сетям.

30. По характеру воздействия угрозы могут быть…

- …против доступности, целостности, конфиденциальности;
- …внутренними, внешними;
- …преднамеренными, случайными.

31. Уязвимость это…

- …ошибка в конфигурации МЭ, позволяющая осуществить НСД к сети организации;

- …ошибка, допущенная при разработке программного обеспечения, исопльзование которой позволяет осуществить НСД;
- …условие или множество условий, которые могут позволить угрозе воздействовать на объект.

32. Риск безопасности это …

- …возможность реализации сетевой атаки на ресурсы КС;
- вероятность преодоления системы защиты за произвольный период времени;
- …возможность данной угрозы реализовать уязвимости для нанесения ущерба организации;
- …вероятность начала вредоносного воздействия на ресурсы КС злоумышленником.

33. Управление риском это …

- …процесс определения риска, применения средств защиты и оценки оставшегося риска;
- …деятельность по выявлению и оценке уязвимостей в программном и аппаратном обеспечении КС;
- … процесс применения средств защиты информационных ресурсов;
- …процесс по выявлению источников угроз БИ.

34. Классы межсетевых экранов по функционированию на уровнях модели OSI:

- пакетный фильтр, программно-аппаратный, программный.
- пакетный фильтр, экранирующий транспорт, прикладной шлюз;
- контроллер состояния протокола, экранирующий транспорт, прикладной шлюз.

35. Список доступа маршрутизатора – это…

- …набор строк, описывающих доверенные адреса хостов;
- …набор строк, определяющих некие образцы, на соответствие которым проверяются пакеты IP;
- …набор строк, описывающих конфигурацию интерфейсов маршрутизатора.

36. Выберите наиболее правильное утверждение.

- Стандартный ACL может проверять адреса отправителей, получателей и ряд параметров;
- Нумерация стандартных ACL выполняется в диапазоне от 100 до 199;
- Стандартный ACL может выполнять контроль состояния соединения;
- Стандартный ACL может проверять только адреса отправителей.

37. Выберите наиболее правильное утверждение.

- Ключевое слово host означает любой IP-адрес хоста;
- Обратная маска 255.255.255.255 определяет единственный IP-адрес;
- Обратная маска 0.0.0.0 определяет единственный IP-адрес;
- Ключевое слово any соответствует WildCard-маске 0.0.0.0.

38. В чем заключается смысл следующего списка доступа?
access-list 45 permit 192.168.20.0 0.0.0.255
access-list 45 deny host 192.168.20.13

- трафику сети 192.168.20.0 разрешено проходить через маршрутизатор, за исключением хоста 192.168.20.13;
- трафику сети 192.168.20.0 разрешено проходить через маршрутизатор;
- трафику сети 192.168.20.0 запрещено проходить через маршрутизатор, за исключением хоста 192.168.20.13;
- трафику хоста 192.168.20.13 запрещено проходить через маршрутизатор, а остальным хостам сети 192.168.20.0 – разрешено.

39. Выберите наиболее правильное утверждение.

- Расширенный ACL может проверять адреса источников, получателей, тип протокола и порты.
- Расширенный ACL обеспечивает более быструю проверку пакетов, чем стандартный ACL.
- Допускается размещать более 1 расширенного ACL на интерфейс, на протокол, на направление.
- Расширенный ACL не может проверить состояние соединения TCP.

40. В чем заключается смысл следующего выражения?

access-list 101 deny ip 0.0.0.0 255.255.255.255 130.120.110.100 0.0.0.0

- запрещение доступа к хосту с IP-адресом 130.120.110.100;
- разрешение доступа к хосту с IP-адресом 130.120.110.100;
- запрещение доступа к подсети 130.120.110.0 0.0.0.255.

41. В чем заключается смысл следующего списка доступа?

access-list 101 permit tcp 0.0.0.0 255.255.255.255 130.120.110.100 0.0.0.0 eq 80
access-list 101 deny ip 0.0.0.0 255.255.255.255 130.120.110.100 0.0.0.0

- разрешен доступ к любому порту хоста и запрещен доступ к протокольному порту HTTP;
- хосту 130.120.110.100 запрещен доступ к другим хостам, за исключением доступа по протоколу http;
- разрешен доступ к подсети 130.120.110.100 0.0.0.255 за исключением хоста 130.120.110.100;
- разрешен доступ к протокольному порту HTTP хоста 130.120.110.100 и запрещен любой другой доступ к хосту.

42. В чем заключается смысл следующего выражения?

ip access-group 101 in

- использование списка доступа номер 101 для входящих пакетов;
- отключение списка доступа номер 101 для входящих пакетов;
- использование списка доступа входящих пакетов для интерфейса номер 101.

43. В чем заключается смысл следующего выражения?

access-list 101 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 established.

- Проверка пакетов отключена полностью.
- Установлен запрет на прохождение пакетов через МЭ.
- Разрешен проход всех пакетов уже установленных сеансов связи.

44. Выберите наиболее правильное утверждение.

- При назначении нового ACL для интерфейса, старый ACL отключается автоматически;
- При назначении нового ACL для интерфейса он добавляется к старому ACL;
- При назначении нового ACL для интерфейса требуется перезагрузка маршрутизатора.

45. Способы удаления остаточной информации с ЖД подразделяются на:

- программные, программно-аппаратные и аппаратные;
- программные, механические и физические;
- низкоуровневые и высокоуровневые.

46. Уровень 0 уничтожения информации на ЖД подразумевает…

- …запись нулей в загрузочный сектор, основную и резервную таблицы разделов;
- …запись последовательности нулей в сектора данных;
- … запись последовательности единиц в сектора данных.

47. Уровень 2 уничтожения информации на ЖД подразумевает…

- …использование нескольких циклов перезаписи информации на ЖД;
- …перестройку структуры магнитного слоя ЖД путем воздействия электромагнитным полем;
- … запись нулей в загрузочный сектор, основную и резервную таблицы разделов и в сектора данных.

48. Свойство универсальности «ОК» состоит в том что они…

- …не должны содержать априорных предположений об объекте оценки;
- …должны быть применимы для оценки средств ЗИ различных производителей;
- …должны быть применимы для оценки различных типов средств ЗИ.

49. Согласно «ОК» система это…

- …программно-аппаратный комплекс для автоматизированной обработки информации;
- …специфическое воплощение информационных технологий с конкретным назначением и условиями эксплуатации;
- …совокупность рабочих мест, объединенная в сеть и имеющая системы защиты от НСД.

50. Под объектом оценки в «ОК» понимается…

- …система разграничения доступа, выполненная в виде программно-аппаратного комплекса;
- …программно-аппаратный продукт или информационная система с соответствующей документацией;
- …операционная система, межсетевой экран или система разграничения доступа.

51. Виды требований безопасности в «ОК»:

- Аппаратные и программные.
- Отраслевые, национальные, международные.
- Функциональные и требования доверия.

52. Профиль защиты в «ОК» это…

- …типовая совокупность требований безопасности;
- …совокупность используемых средств защиты;
- …набор компонентов управления доступом к информационным ресурсам.

ВОПРОСЫ

к экзамену по дисциплине

«Программно-аппаратные средства информационной безопасности»

1. Определение понятий «Автоматизированная система», «Средство вычислительной техники», «Несанкционированный доступ к информации» (НСД). Способы осуществления НСД и основные принципы защиты. Оценка соответствия определения НСД, приведенном в ГОСТ Р 50922-96 современным понятиям об НСД.
2. Уровни возможностей нарушителя. Основные способы реализации НСД.
3. Основные функции СРД. Способы реализации СРД.
4. Подсистемы СЗИ, реализующие механизмы защиты от НСД и решаемые ими задачи.
5. Раскройте понятия идентификация, аутентификация, авторизация, аудит безопасности. Типичная структура учетной записи.
6. Три группы способов аутентификации.
7. Аутентификация пользователей КС на основе паролей: основные требования к политике учетных записей и проблемы парольной аутентификации.
8. Способы назначения начального пароля: преимущества и недостатки.
9. Аутентификация пользователей на основе модели «рукопожатия».
10. Типы устройств аутентификации, примеры. Порядок регистрации пользователя в системах с аутентификацией на основе устройств.
11. Способы удаления остаточной информации с жестких дисков. Алгоритмы удаления остаточной информации.
12. Политика безопасности: основные разделы и их содержание.
13. Цели внедрения систем защиты от внутренних ИТ-угроз. Классификация внутренних нарушителей. Нетехнические меры защиты от внутренних ИТ-угроз.
14. Сущность понятий «угроза» и «уязвимость». Определение риска нарушения безопасности информации для организации. Критерии оценки риска нарушения безопасности информации.
15. История создания и текущий статус «Общих критериев». Основные понятия и идеи «Общих критериев».
16. Основные понятия и идеи «Общей методологии оценки безопасности информационных технологий».
17. Классификация межсетевых экранов.
18. Списки доступа в маршрутизаторах Cisco.
19. Классификация АС. Основные этапы классификации АС
20. Требования к программному обеспечению СЗИ от НСД. Уровни контроля отсутствия НДВ.