Тема 4.1. Идентификация и аутентификация

1 Понятия «идентификация» и «аутентификация»

Идентификация и аутентификации применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

Общий алгоритм работы таких систем заключается в том, чтобы получить от субъекта (например, пользователя) информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

Наличие процедур аутентификации и/или идентификации пользователей является обязательным условием любой защищенной системы, поскольку все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами информационных систем.

Дадим определения этих понятий.

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

При построении систем идентификации и аутентификации возникает проблема выбора идентификатора, на основе которого осуществляются процедуры идентификации и аутентификации пользователя. В качестве идентификаторов обычно используют:

– набор символов (пароль, секретный ключ, персональный идентификатор и т. п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи);

– физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т. п.) или особенности поведения (особенности работы на клавиатуре и т. п.).

Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на паролях – конфиденциальных идентификаторах субъектов. В этом случае при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам системы.

Парольные методы аутентификации по степени изменяемости паролей делятся на:

– методы, использующие постоянные (многократно используемые) пароли;

– методы, использующие одноразовые (динамично изменяющиеся) пароли.

Использование одноразовых или динамически меняющихся паролей является более надежным методом парольной защиты.

В последнее время получили распространение комбинированные методы идентификации и аутентификации, требующие, помимо знания пароля, наличие карточки (token) – специального устройства, подтверждающего подлинность субъекта.

Карточки разделяют на два типа:

– пассивные (карточки с памятью);

– активные (интеллектуальные карточки).

Самыми распространенными являются пассивные карточки с магнитной полосой, которые считываются специальным устройством, имеющим клавиатуру и процессор. При использовании указанной карточки пользователь вводит свой идентификационный номер. В случае его совпадения с электронным вариантом, закодированным в карточке, пользователь получает доступ в систему. Это позволяет достоверно установить лицо, получившее доступ к системе и исключить несанкционированное использование карточки злоумышленником (например, при ее утере). Такой способ часто называют двухкомпонентной аутентификацией.

Интеллектуальные карточки кроме памяти имеют собственный микропроцессор. Это позволяет реализовать различные варианты парольных методов защиты, например, многоразовые пароли, динамически меняющиеся пароли.

Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают почти 100 % идентификацию, решая проблемы утери или утраты паролей и личных идентификаторов. Однако эти методы нельзя использовать при идентификации процессов или данных (объектов данных), они только начинают развиваться, требуют пока сложного и дорогостоящего оборудования. Это обусловливает их использование пока только на особо важных объектах.

Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, по почерку, по тембру голоса и пр.

Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный защитный механизм основан на использовании системы космической навигации, типа GPS (Global Positioning System). Пользователь, имеющий аппаратуру GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, может с точностью до метра определить месторасположение пользователя. Высокая надежность аутентификации определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что исключает их перехват. Такой метод аутентификации может быть использован в случаях, когда авторизованный удаленный пользователь должен находиться в нужном месте.

2 Механизм идентификации и аутентификации пользователей

Общая процедура идентификации и аутентификации пользователя при его доступе в защищенную информационную систему заключается в следующем.

Пользователь предоставляет системе свой личный идентификатор (например, вводит пароль или предоставляет палец для сканирования отпечатка). Далее система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентифика-

торами. Если результат сравнения успешный, то пользователь получает доступ к системе в рамках установленных полномочий. В случае отрицательного результата система сообщает об ошибке и предлагает повторно ввести идентификатор. В тех случаях, когда пользователь превышает лимит возможных повторов ввода информации (ограничение на количество повторов является обязательным условием для защищенных систем) система временно блокируется и выдается сообщение о несанкционированных действиях (причем, может быть, и незаметно для пользователя).

Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

В целом аутентификация по уровню информационной безопасности делится на три категории:

1) Статическая аутентификация.
2) Устойчивая аутентификация.
3) Постоянная аутентификация.

Первая категория обеспечивает защиту только от несанкционированных действий в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию. Примером средства статической аутентификации являются традиционные постоянные пароли. Их эффективность преимущественно зависит от сложности угадывания паролей и, собственно, от того, насколько хорошо они защищены.

Устойчивая аутентификация использует динамические данные аутентификации, меняющиеся с каждым сеансом работы. Реализациями устойчивой аутентификации являются системы, использующие одноразовые пароли и электронные подписи. Устойчивая аутентификация обеспечивает защиту от атак, где злоумышленник может перехватить аутентификационную информацию и использовать ее в следующих сеансах работы.

Однако устойчивая аутентификация не обеспечивает защиту от активных атак, в ходе которых маскирующийся злоумышленник может оперативно (в течение сеанса

аутентификации) перехватить, модифицировать и вставить информацию в поток передаваемых данных.

Постоянная аутентификация обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки. Примером реализации указанной категории аутентификации является использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.

3 Выводы по теме 4.1

1) Идентификация и аутентификации применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

2) Общий алгоритм работы таких систем заключается в том, чтобы получить от субъекта (например, пользователя) информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

3) Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

4) Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

5) В качестве идентификаторов в системах аутентификации обычно используют набор символов (пароль, секретный ключ, персональный идентификатор и т. п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи). В системах идентификации такими идентификаторами являются физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т. п.) или особенности поведения (особенности работы на клавиатуре и т. п.).

6) В последнее время получили распространение комбинированные методы идентификации и аутентификации, требующие, помимо знания пароля, наличие карточки (token) – специального устройства, подтверждающего подлинность субъекта.

7) Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

8) В целом аутентификация по уровню информационной безопасности делится на три категории: статическая аутентификация, устойчивая аутентификация и постоянная аутентификация.

9) Постоянная аутентификация является наиболее надежной, поскольку обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки.

Тема 4.2. Криптография и шифрование

1 Структура криптосистемы

Самый надежный технический метод защиты информации основан на использовании криптосистем. Криптосистема включает:

– алгоритм шифрования;

– набор ключей (последовательность двоичных чисел), используемых для шифрования;

– систему управления ключами.

Криптосистемы решают такие проблемы информационной безопасности как обеспечение конфиденциальности, целостности данных, а также аутентификацию данных и их источников.

Криптографические методы защиты являются обязательным элементом безопасных информационных систем. Особое значение криптографические методы получили с развитием распределенных открытых сетей, в которых нет возможности обеспечить физическую защиту каналов связи.

Общая схема работы криптосистемы показана на рисунке 4.2.1.

2 Классификация систем шифрования данных

Основным классификационным признаком систем шифрования данных является способ их функционирования. По способу функционирования системы шифрования данных делят на два класса:

– системы «прозрачного» шифрования;

– системы, специально вызываемые для осуществления шифрования.

Рисунок 4.2.1 – Общая схема работы криптосистемы

В системах «прозрачного» шифрования (шифрование «налету») криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя. Например, пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование. Системы второго класса обычно представляют собой утилиты (программы), которые необходимо специально вызывать для выполнения шифрования.

Как уже отмечалось, особое значение криптографические преобразования имеют при передаче данных по распределенным вычислительным сетям. Для защиты данных в распределенных сетях используются два подхода: канальное шифрование и оконечное (абонентское) шифрование.

В случае канального шифрования защищается вся информация, передаваемая по каналу связи, включая служебную. Этот способ шифрования обладает следующим достоинством – встраивание процедур шифрования на канальный уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы.

Оконечное (абонентское) шифрование позволяет обеспечить конфиденциальность данных, передаваемых между двумя абонентами. В этом случае защищается только содержание сообщений, вся служебная информация остается открытой.

3 Симметричные и асимметричные методы шифрования

Классические криптографические методы делятся на два основных типа: симметричные (шифрование секретным ключом) и асимметричные (шифрование открытым ключом).

В симметричных методах для шифрования и расшифровывания используется один и тот же секретный ключ. Наиболее известным стандартом на симметричное шифрование с закрытым ключом является стандарт для обработки информации в государственных учреждениях США DES (Data Encryption Standard). Общая технология использования симметричного метода шифрования представлена на рисунке 4.2.2.

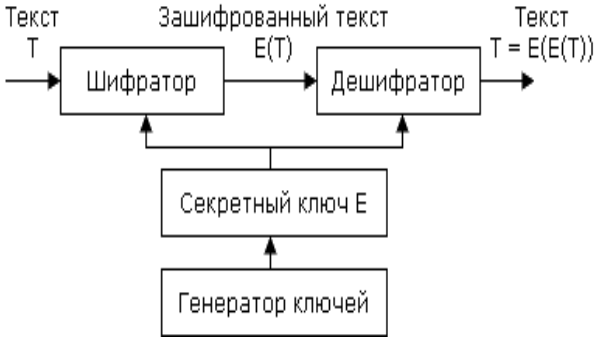

Рисунок 4.2.2 – Общая технология симметричного метода шифрования

Основной недостаток этого метода заключается в том, что ключ должен быть известен и отправителю, и получателю. Это существенно усложняет процедуру назначения и распределения ключей между пользователями. Указанный недостаток послужил причиной разработки методов шифрования с открытым ключом – асимметричных методов.

Асимметричные методы используют два взаимосвязанных ключа: для шифрования и расшифрования. Один ключ является закрытым и известным только получателю. Его используют для расшифрования. Второй из ключей является открытым, т. е. он может быть общедоступным по сети и опубликован вместе с адресом пользователя. Его используют для выполнения шифрования. Схема функционирования данного типа криптосистемы показана на рисунке 4.2.3.

В настоящее время наиболее известным и надежным является асимметричный алгоритм RSA (Rivest, Shamir, Adleman).

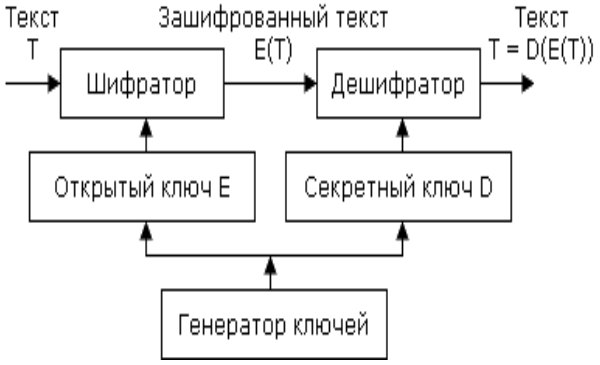

Рисунок 4.2.3 – Общая технология асимметричного метода шифрования

4 Механизм электронной подписи

Для контроля целостности передаваемых по сетям данных используется электронная подпись, которая реализуется по методу шифрования с открытым ключом.

Электронная подпись представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом. Отправитель формирует цифровую подпись, используя секретный ключ отправителя. Получатель проверяет подпись, используя открытый ключ отправителя.

Идея технологии электронной подписи состоит в следующем. Отправитель передает два экземпляра одного сообщения: открытое и расшифрованное его закрытым ключом (т. е. обратно шифрованное). Получатель шифрует с помощью открытого ключа отправителя расшифрованный экземпляр. Если он совпадет с открытым вариантом, то личность и подпись отправителя считается установленной.

При практической реализации электронной подписи также шифруется не все сообщение, а лишь специальная контрольная сумма – хэш, защищающая послание от нелегального изменения. Электронная подпись здесь гарантирует как целостность сообщения, так и удостоверяет личность отправителя.

Безопасность любой криптосистемы определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в системе или сети. Различают следующие виды функций управления ключами: генерация, хранение и распределение ключей.

Способы генерации ключей для симметричных и асимметричных криптосистем различны. Для генерации ключей симметричных криптосистем используются аппаратные и программные средства генерации случайных чисел. Генерация ключей для асимметричных криптосистем более сложна, так как ключи должны обладать определенными математическими свойствами.

Функция хранения предполагает организацию безопасного хранения, учета и удаления ключевой информации. Для обеспечения безопасного хранения ключей применяют их шифрование с помощью других ключей. Такой подход приводит к концепции иерархии ключей. В иерархию ключей обычно входит главный ключ (т. е. мастер-ключ), ключ шифрования ключей и ключ шифрования данных. Следует отметить, что генерация и хранение мастер-ключа является наиболее критическим вопросом криптозащиты.

Распределение – самый ответственный процесс в управлении ключами. Этот процесс должен гарантировать скрытность распределяемых ключей, а также быть оперативным и точным. Между пользователями сети ключи распределяют двумя способами:

- с помощью прямого обмена сеансовыми ключами;
- используя один или несколько центров распределения ключей.

5 Выводы по теме

1) Любая криптосистема включает: алгоритм шифрования, набор ключей, используемых для шифрования и систему управления ключами.

2) Криптосистемы решают такие проблемы информационной безопасности как обеспечение конфиденциальности, целостности данных, а также аутентификация данных и их источников.

3) Основным классификационным признаком систем шифрования данных является способ их функционирования.

4) В системах прозрачного шифрования (шифрование «на лету») криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя.

5) Классические криптографические методы делятся на два основных типа: симметричные (шифрование секретным ключом) и асимметричные (шифрование открытым ключом).

6) В симметричных методах для шифрования и расшифровывания используется один и тот же секретный ключ.

7) Асимметричные методы используют два взаимосвязанных ключа: для шифрования и расшифрования. Один ключ является закрытым и известным только получателю. Его используют для расшифрования. Второй из ключей является открытым, т. е. он может быть общедоступным по сети и опубликован вместе с адресом пользователя. Его используют для выполнения шифрования.

8) Для контроля целостности передаваемых по сетям данных используется электронная подпись, которая реализуется по методу шифрования с открытым ключом.

9) Электронная подпись представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом. Отправитель формирует цифровую подпись, используя секретный ключ отправителя. Получатель проверяет подпись, используя открытый ключ отправителя.

10) При практической реализации электронной подписи также шифруется не все сообщение, а лишь специальная контрольная сумма – хэш, защищающая послание от нелегального изменения. Электронная подпись здесь гарантирует как целостность сообщения, так и удостоверяет личность отправителя.

11) Безопасность любой криптосистемы определяется используемыми криптографическими ключами.

Тема 4.3. Методы разграничение доступа

1 Методы разграничения доступа

После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы.

Обычно полномочия субъекта представляются: списком ресурсов, доступным пользователю и правами по доступу к каждому ресурсу из списка.

Существуют следующие методы разграничения доступа:

1) Разграничение доступа по спискам.
2) Использование матрицы установления полномочий.
3) Разграничение доступа по уровням секретности и категориям.
4) Парольное разграничение доступа.

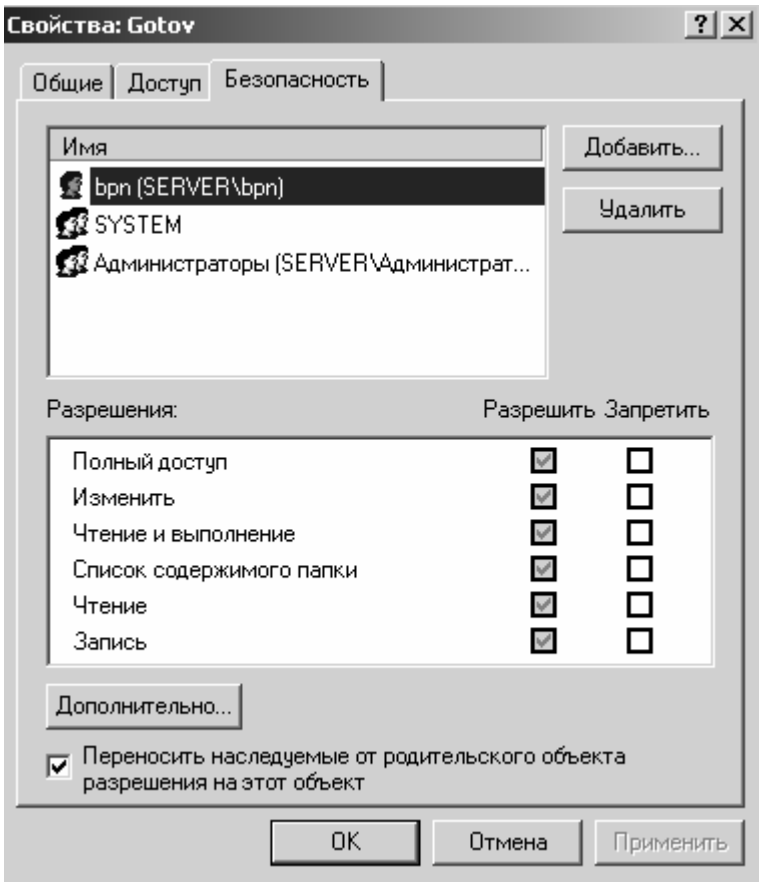

Рисунок 4.3.1 – Пример разграничения доступа

При разграничении доступа по спискам задаются соответствия: каждому пользователю – список ресурсов и прав доступа к ним или каждому ресурсу – список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Пример (операционная система Windows 2010) разграничения доступа по спискам для одного объекта показан на рисунке 4.3.1.

Использование матрицы установления полномочий подразумевает применение матрицы доступа (таблицы полномочий). В указанной матрице строками являются идентификаторы субъектов, имеющих доступ в информационную систему, а столбцами – объекты (ресурсы) информационной системы. Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа (чтение, запись и пр.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа и пр.

Данный метод предоставляет более унифицированный и удобный подход, т. к. вся информация о полномочиях хранится в виде единой таблицы, а не в виде разнотипных списков. Недостатками матрицы являются ее возможная громоздкость и неоптимальность (большинство клеток – пустые).

Фрагмент матрицы установления полномочий показан в таблице 4.3.1

Таблица 4.3.1 – Фрагмент матрицы установления полномочий.

Субъект	**Диск c:**	**Файл d:\prog. exe**	**Принтер**
Пользователь 1	Чтение Запись Удаление	Выполнение Удаление	Печать Настройка параметров
Пользователь 2	Чтение	Выполнение	Печать с 9:00 до 17:00
Пользователь 3	Чтение Запись	Выполнение	Печать с 17:00 до 9:00

Разграничение доступа по уровням секретности и категориям заключается в разделении ресурсов информационной системы по уровням секретности и категориям.

При разграничении по степени секретности выделяют несколько уровней, например: общий доступ, конфиденциально, секретно, совершенно секретно. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен. Пользователь имеет доступ ко всем данным, имеющим уровень (гриф) секретности не выше, чем ему определен, например, пользователь имеющий доступ к данным «секретно», также имеет доступ к данным «конфиденциально» и «общий доступ».

При разграничении по категориям задается и контролируется ранг категории пользователей. Соответственно, все ресурсы информационной системы разделяются по уровням важности, причем определенному уровню соответствует категория пользователей. В качестве примера, где используются категории пользователей, приведем операционную систему Windows 2010, подсистема безопасности которой по умолчанию поддерживает следующие категории (группы) пользователей: «администратор», «опытный пользователь», «пользователь» и «гость». Каждая из категорий имеет определенный набор прав. Применение категорий пользователей позволяет упростить процедуры назначения прав пользователей за счет применения групповых политик безопасности.

Парольное разграничение, очевидно, представляет использование методов доступа субъектов к объектам по паролю. При этом используются все методы парольной защиты. Очевидно, что постоянное использование паролей создает неудобства пользователям и временные задержки. Поэтому указанные методы используют в исключительных ситуациях. На практике обычно сочетают различные методы разграничения доступа. Например, первые три метода усиливают парольной защитой.

Разграничение прав доступа является обязательным элементом защищенной информационной системы. Напомним, что еще в «Оранжевой книге США» были введены понятия: произвольное управление доступом; принудительное управление доступом.

2 Мандатное и дискретное управление доступом

В ГОСТе Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах ФСТЭК РФ определены два вида (принципа) разграничения доступа:

1) Дискретное управление доступом представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.

2) Мандатное управление доступом основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах (файлы, папки, рисунки) и официального разрешения (допуска) субъекта к информации соответствующего уровня конфиденциальности.

При внимательном рассмотрении можно заметить, что дискретное управление доступом есть ничто иное, как произвольное управление доступом (по «Оранжевой книге США»), а мандатное управление реализует принудительное управление доступом.

3 Выводы по теме 4.3

1) Определение полномочий (совокупность прав) субъекта для последующего контроля санкционированного использования им объектов информационной системы осуществляется после выполнения идентификации и аутентификации подсистема защиты.

2) Существуют следующие методы разграничения доступа:

- разграничение доступа по спискам;
- использование матрицы установления полномочий;
- разграничение доступа по уровням секретности и категориям;
- парольное разграничение доступа.

3) При разграничении доступа по спискам задаются соответствия: каждому пользователю – список ресурсов и прав доступа к ним или каждому ресурсу – список пользователей и их прав доступа к данному ресурсу.

4) Использование матрицы установления полномочий подразумевает применение матрицы доступа (таблицы полномочий). В указанной матрице строками являются идентификаторы субъектов, имеющих доступ в информационную систему, а столбцами – объекты (ресурсы) информационной системы.

5) При разграничении по уровню секретности выделяют несколько уровней, например: общий доступ, конфиденциально, секретно, совершенно секретно. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен. Пользователь имеет доступ ко всем данным, имеющим уровень (гриф) секретности не выше, чем ему определен.

6) Парольное разграничение основано на использовании пароля доступа субъектов к объектам.

7) В ГОСТе Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах ФСТЭК РФ определены два вида (принципа) разграничения доступа: дискретное управление доступом и мандатное управление доступом.

8) Дискретное управление доступом представляет собой разграничение доступа между поименованными субъектами и поименованными объектами.

9) Мандатное управление доступом основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах (файлы, папки, рисунки) и официального разрешения (допуска) субъекта к информации соответствующего уровня конфиденциальности.

Тема 4.4. Регистрация и аудит

1 Определение и содержание регистрации и аудита информационных систем

Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности, такие как:

- вход и выход субъектов доступа;
- запуск и завершение программ;
- выдача печатных документов;
- попытки доступа к защищаемым ресурсам;
- изменение полномочий субъектов доступа;
- изменение статуса объектов доступа и т. д.

Для сертифицируемых по безопасности информационных систем список контролируемых событий определен рабочим документом ФСТЭК РФ: «Положение о сертификации средств и систем вычислительной техники и связи по требованиям безопасности информации».

Эффективность системы безопасности принципиально повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, анализировать закономерности системы, оценивать работу пользователей и т. д.

1) Аудит – это анализ накопленной информации, проводимый оперативно в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация механизмов регистрации и аудита позволяет решать следующие задачи обеспечения информационной безопасности:

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

Рассматриваемые механизмы регистрации и аудита являются сильным психологическим средством, напоминающим потенциальным нарушителям о неотвратимости наказания за несанкционированные действия, а пользователям – за возможные критические ошибки.

Практическими средствами регистрации и аудита являются:

- различные системные утилиты и прикладные программы;
- регистрационный (системный или контрольный) журнал.

Первое средство является обычно дополнением к мониторингу, осуществляемого администратором системы. Комплексный подход к протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

2) Регистрационный журнал – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

Фрагмент журнала безопасности подсистемы регистрации и аудита операционной системы показан на рисунке 4.4.1.

Обнаружение попыток нарушений информационной безопасности входит в функции активного аудита, задачами которого является оперативное выявление подозрительной активности и предоставление средств для автоматического реагирования на нее.

Под подозрительной активностью понимается поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям). Например, подсистема аудита, отслеживая процедуру входа (регистрации) пользователя в систему подсчитывает количество неудачных попыток входа. В случае превышения установленного порога таких попыток подсистема аудита формирует сигнал о блокировке учетной записи данного пользователя.

Безопасность 13 событий

Тип	Дата	Время	Источник	Категория	Событие	Пользователь	Компьютер
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	562	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	562	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Учетные записи	643	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	560	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	560	admin	GHJ
Аудит успехов	26.04.2004	5:34:49	Security	Доступ к объектам	562	admin	GHJ

Рисунок 4.4.1 – Фрагмент журнала безопасности подсистемы регистрации и аудита

2 Этапы регистрации и методы аудита событий информационной системы

Организация регистрации событий, связанных с безопасностью информационной системы включает как минимум три этапа:

1) Сбор и хранение информации о событиях.
2) Защита содержимого журнала регистрации.
3) Анализ содержимого журнала регистрации.

На первом этапе определяются данные, подлежащие сбору и хранению, период чистки и архивации журнала, степень централизации управления, место и средства хранения журнала, возможность регистрации шифрованной информации и пр.

Регистрируемые данные должны быть защищены, в первую очередь, от несанкционированной модификации и, возможно, раскрытия.

Самым важным этапом является анализ регистрационной информации. Известны несколько методов анализа информации с целью выявления несанкционированных действий.

1) Статистические методы основаны на накоплении среднестатистических параметров функционирования подсистем и сравнении текущих параметров с ними. Наличие определенных отклонений может сигнализировать о возможности появления некоторых угроз.

2) Эвристические методы используют модели сценариев несанкционированных действий, которые описываются логическими правилами или модели действий, по совокупности, приводящие к несанкционированным действиям.

3 Выводы по теме 4.4

1) Эффективность системы безопасности принципиально повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защите, анализировать закономерности системы, оценивать работу пользователей.

2) Механизм регистрации основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности.

3) Аудит системных событий – это анализ накопленной информации, проводимый оперативно в реальном времени или периодически (например, раз в день).

4) Механизмы регистрации и аудита являются сильным психологическим средством, напоминающим потенциальным нарушителям о неотвратимости наказания за несанкционированные действия, а пользователям – за возможные критические ошибки.

5) Регистрационный журнал – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

6) Регистрация событий, связанных с безопасностью информационной системы, включает как минимум три этапа: сбор и хранение информации о событиях, защита содержимого журнала регистрации и анализ содержимого журнала регистрации.

7) Методы аудита могут быть статистические и эвристические.

8) Для сертифицируемых по безопасности информационных систем список контролируемых событий определен рабочим документом ФСТЭК РФ: «Положение о сертификации средств и систем вычислительной техники и связи по требованиям безопасности информации».

Тема 4.5. Межсетевое экранирование

1 Классификация межсетевых экранов

Одним из эффективных механизмом обеспечения информационной безопасности распределенных вычислительных сетях является экранирование, выполняющее функции разграничения информационных потоков на границе защищаемой сети.

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым, обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет межсетевой экран или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Межсетевые экраны классифицируются по следующим признакам:

– по месту расположения в сети – на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети;

– по уровню фильтрации, соответствующему эталонной модели OSI/ISO.

Внешние межсетевые экраны обычно работают только с протоколом TCP/IP глобальной сети Интернет. Внутренние сетевые экраны могут поддерживать несколько протоколов, например, при использовании сетевой операционной системы Novell Netware, следует принимать во внимание протокол SPX/IPX.

2 Характеристика межсетевых экранов

Работа всех межсетевых экранов основана на использовании информации разных уровней модели OSI. Как правило, чем выше уровень модели OSI, на котором межсетевой экран фильтрует пакеты, тем выше обеспечиваемый им уровень защиты.

Таблица 4.5.1 – Типы межсетевых экранов и уровни модели ISO OSI

	Уровень модели OSI	**Протокол**	**Тип межсетевого экрана**
1	Прикладной	Telnet, FTP, DNS, NFS, SMTP, HTTP	– шлюз прикладного уровня; – межсетевой экран экспертного уровня.
2	Представления данных		
3	Сеансовый	TCP, UDP	– шлюз сеансового уровня.
4	Транспортный	TCP, UDP	
5	Сетевой	IP, ICMP	– межсетевой экран с фильтрацией пакетов.
6	Канальный	ARP, RAP	
7	Физический	Ethernet	

Межсетевые экраны разделяют на четыре типа:

1) Межсетевые экраны с фильтрацией пакетов представляют собой маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Поэтому такие экраны называют иногда пакетными фильтрами. Фильтрация осуществляется путем анализа IP-адреса источника и приемника, а также портов входящих TCP- и UDP-пакетов и сравнением их со сконфигурированной таблицей правил. Эти межсетевые экраны просты в использовании, дешевы, оказывают минимальное влияние на производительность вычислительной системы. Основным недостатком является их уязвимость при подмене адресов IP. Кроме того, они сложны при конфигурировании: для их установки требуется знание сетевых, транспортных и прикладных протоколов.

2) Шлюзы сеансового уровня контролируют допустимость сеанса связи. Они следят за подтверждением связи между авторизованным клиентом и внешним хостом (и наоборот), определяя, является ли запрашиваемый сеанс связи допустимым. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т. е. функционирует на два уровня выше, чем межсетевой экран с фильтрацией пакетов. Кроме того, указанные системы обычно имеют функцию трансляции сетевых адресов, которая скрывает внутренние IP-адреса, тем самым, исключая подмену IP-адреса. Однако в таких меж-

сетевых экранах отсутствует контроль содержимого пакетов, генерируемых различными службами. Для исключения указанного недостатка применяются шлюзы прикладного уровня.

3) Шлюзы прикладного уровня проверяют содержимое каждого проходящего через шлюз пакета и могут фильтровать отдельные виды команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Это более совершенный и надежный тип межсетевого экрана, использующий программы-посредники (proxies) прикладного уровня или агенты. Агенты составляются для конкретных служб сети Интернет (HTTP, FTP, Telnet и т. д.) и служат для проверки сетевых пакетов на наличие достоверных данных. Шлюзы прикладного уровня снижают уровень производительности системы из-за повторной обработки в программе-посреднике. Это незаметно при работе в Интернет при работе по низкоскоростным каналам, но существенно при работе во внутренней сети.

4) Межсетевые экраны экспертного уровня сочетают в себе элементы всех трех описанных выше категорий. Как и межсетевые экраны с фильтрацией пакетов, они работают на сетевом уровне модели OSI, фильтруя входящие и исходящие пакеты на основе проверки IP-адресов и номеров портов. Межсетевые экраны экспертного уровня также выполняют функции шлюза сеансового уровня, определяя, относятся ли пакеты к соответствующему сеансу. И, наконец, брандмауэры экспертного уровня берут на себя функции шлюза прикладного уровня, оценивая содержимое каждого пакета в соответствии с политикой безопасности, выработанной в конкретной организации.

Вместо применения связанных с приложениями программ-посредников, брандмауэры экспертного уровня используют специальные алгоритмы распознавания и обработки данных на уровне приложений. С помощью этих алгоритмов пакеты сравниваются с известными шаблонами данных, что теоретически должно обеспечить более эффективную фильтрацию пакетов.

3 Выводы по теме 4.5

1) Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым, обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа экранирование обеспечивает регистрацию информационных обменов.

2) Функции экранирования выполняет межсетевой экран или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации.

3) Межсетевые экраны классифицируются по следующим признакам: по месту расположения в сети и по уровню фильтрации, соответствующему эталонной модели OSI/ISO.

4) Внешние межсетевые экраны обычно работают только с протоколом TCP/IP глобальной сети Интернет. Внутренние сетевые экраны могут поддерживать несколько протоколов.

5) Межсетевые экраны разделяют на четыре типа:

- межсетевые экраны с фильтрацией пакетов;
- шлюзы сеансового уровня;
- шлюзы прикладного уровня;
- межсетевые экраны экспертного уровня.

6) Наиболее комплексно задачу экранирования решают межсетевые экраны экспертного уровня, которые сочетают в себе элементы всех типов межсетевых экранов.

Тема 4.6. Технология виртуальных частных сетей (VPN)

1 Сущность и содержание технологии виртуальных частных сетей

Технология виртуальных частных сетей (VPN - Virtual Private Network) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности:

– шифрования (с использование инфраструктуры криптосистем) на выделенных шлюзах (шлюз обеспечивает обмен данными между вычислительными сетями, функционирующими по разным протоколам);

– экранирования (с использованием межсетевых экранов);

– туннелирования.

Сущность технологии VPN заключается в следующем (рисунок 4.6.1):

1) На все компьютеры, имеющие выход в Интернет (вместо Интернета может быть и любая другая сеть общего пользования), устанавливается VPN-агенты, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям.

2) Перед отправкой IP-пакета VPN-агент выполняет следующие операции:

– анализируется IP-адрес получателя пакета, в зависимости от этого адреса выбирается алгоритм защиты данного пакета (VPN-агенты могут, поддерживать одновременно несколько алгоритмов шифрования и контроля целостности). Пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится;

– вычисляется и добавляется в пакет его имитоприставка, обеспечивающая контроль целостности передаваемых данных;

– пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию);

– формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента (эта процедура называется инкапсуляцией пакета).

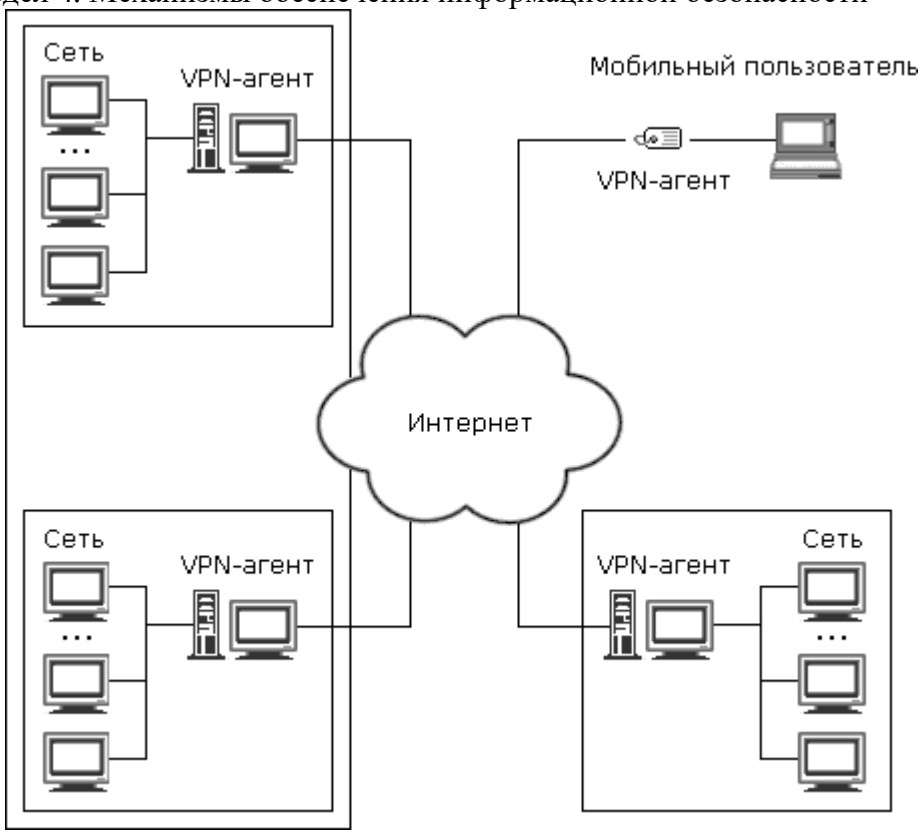

Рисунок 4.6.1 – Сущность технологии VPN

В результате этого обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например, внутренние IP-адреса сети, в этом случае недоступна.

3) При получении IP-пакета выполняются обратные действия:

– из заголовка пакета извлекается информация о VPN-агенте отправителя пакета, если такой отправитель не входит в число разрешенных, то пакет отбрасывается (то же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком);

– согласно настройкам, выбираются криптографические алгоритмы и ключи, после чего пакет расшифровывается и проверяется его целостность (пакеты с нарушенной целостностью также отбрасываются);

– после всех обратных преобразований пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Рисунок 4.6.2 – Понятие «туннеля» при передаче данных

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложной является только настройка VPN-агентов, которая может быть выполнена только очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера, на котором он установлен.

2 Понятие «туннеля» при передаче данных в сетях

Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (такой канал называется «туннелем», а технология его создания называется «туннелированием»). Вся информация передается по туннелю в зашифрованном виде.

Одной из обязательных функций VPN-агентов является фильтрация пакетов. Фильтрация пакетов реализуется в соответствии с настройками VPN-агента, совокупность которых образует политику безопасности виртуальной частной сети. Для повышения защищенности виртуальных частных сетей на концах туннелей целесообразно располагать межсетевые экраны.

3 Выводы по теме 4.6

1) Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности:

- шифрования (с использование инфраструктуры криптосистем);
- экранирования (с использованием межсетевых экранов);
- туннелирования.

2) При реализации технологии виртуальных частных сетей на все компьютеры, имеющие выход в Интернет (вместо Интернета может быть и любая другая сеть общего пользования), устанавливаются VPN-агенты, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям.

3) В виртуальной частной сети обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например, внутренние IP-адреса сети, в этом случае недоступна.

4) Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (такой канал называется «туннелем», а технология его создания называется «туннелированием»).

5) Одной из обязательных функций VPN-агентов является фильтрация пакетов.

6) Фильтрация пакетов реализуется в соответствии с настройками VPN-агента, совокупность которых образует политику безопасности виртуальной частной сети.

7) Для повышения защищенности виртуальных частных сетей на концах туннелей целесообразно располагать межсетевые экраны.