Защита информации в компьютерных сетях

Цели и задачи защиты

Цели защиты информации в сетях ЭВМ общие для всех автоматизированных систем обработки данных (АСОД), а именно: **обеспечение целостности** (физической и логической) **информации**, а также предупреждение несанкционированной ее модификации, несанкционированного получения и размножения.

Функции защиты также носят общий для всех АСОД характер.

Задачи защиты информации в сетях ЭВМ определяются теми угрозами, которые потенциально возможны в процессе их функционирования.

Угрозы безопасности

- Прослушивание каналов, т. е. запись и последующий анализ всего проходящего потока сообщений. Прослушивание в большинстве случаев не замечается легальными участниками информационного обмена.
- Умышленное уничтожение или искажение (фальсификация) проходящих по сети сообщений, а также включение в поток ложных сообщений. Ложные сообщения могут быть восприняты получателем как подлинные.
- Присвоение злоумышленником своему узлу или ретранслятору чужого идентификатора, что дает возможность получать или отправлять сообщения от чужого имени.
- Преднамеренный разрыв линии связи, что приводит к полному прекращению доставки всех (или только выбранных злоумышленником) сообщений.
- Внедрение сетевых вирусов, т. е. передача по сети тела вируса с его последующей активизацией пользователем удаленного или локального узла.

Задачи защиты в сетях передачи данных

1. Аутентификация одноуровневых объектов, заключающаяся в подтверждении подлинности одного или нескольких взаимодействующих объектов при обмене информацией между ними.
2. Контроль доступа, т. е. защита от несанкционированного использования ресурсов сети.
3. Маскировка данных, циркулирующих в сети.
4. Контроль и восстановление целостности всех находящихся в сети данных.
5. Арбитражное обеспечение, т. е. защита от возможных отказов от фактов отправки, приема или содержания отправленных или принятых данных.

Задачи защиты на уровнях протоколов передачи данных

- Физический уровень — контроль электромагнитных излучений линий связи и устройств, поддержка коммутационного оборудования в рабочем состоянии. Защита на данном уровне обеспечивается с помощью экранирующих устройств, генераторов помех, средств физической защиты передающей среды.
- Канальный уровень — увеличение надежности защиты (при необходимости) с помощью шифрования передаваемых по каналу данных. В этом случае шифруются все передаваемые данные, включая служебную информацию.

Задачи защиты на уровнях протоколов передачи данных

- Сетевой уровень — наиболее уязвимый уровень с точки зрения защиты. На нем формируется вся маршрутизирующая информация, отправитель и получатель фигурируют явно, осуществляется управление потоком. Кроме того, протоколами сетевого уровня пакеты обрабатываются на всех маршрутизаторах, шлюзах и других промежуточных узлах. Почти все специфические сетевые нарушения осуществляются с использованием протоколов данного уровня (чтение, модификация, уничтожение, дублирование, переориентация отдельных сообщений или потока в целом, маскировка под другой узел и др.). Защита от подобных угроз осуществляется протоколами сетевого и транспортного уровней и с помощью средств криптозащиты. На данном уровне может быть реализована, например, выборочная маршрутизация.

Задачи защиты на уровнях протоколов передачи данных

- **Транспортный уровень** — осуществляет контроль за функциями сетевого уровня на приемном и передающем узлах (на промежуточных узлах протокол транспортного уровня не функционирует).

  Механизмы транспортного уровня проверяют целостность отдельных пакетов данных, последовательности пакетов, пройденный маршрут, время отправления и доставки, идентификацию и аутентификацию отправителя и получателя и другие функции. Все активные угрозы становятся видимыми на данном уровне.

  Гарантом целостности передаваемых данных является криптозащита как самих данных, так и служебной информации. Никто, кроме имеющих секретный ключ получателя и/или отправителя, не может прочитать или изменить информацию таким образом, чтобы изменение осталось незамеченным.

Задачи защиты на уровнях протоколов передачи данных

Анализ трафика предотвращается передачей сообщений, не содержащих информацию, которые, однако, выглядят как реальные сообщения. Регулируя интенсивность этих сообщений в зависимости от объема передаваемой информации, можно постоянно добиваться равномерного трафика. Однако все эти меры не могут предотвратить угрозу уничтожения, переориентации или задержки сообщения. Единственной защитой от таких нарушений может быть параллельная доставка дубликатов сообщения по другим путям.

Задачи защиты на уровнях протоколов передачи данных

Протоколы верхних уровней обеспечивают контроль взаимодействия принятой или переданной информации с локальной системой. Протоколы **сеансового** и **представительного** уровня функций защиты не выполняют.

В функции защиты протокола **прикладного уровня** входит управление доступом к определенным наборам данных, идентификация и аутентификация определенных пользователей, а также другие функции, определяемые конкретным протоколом. Более сложными эти функции являются в случае реализации полномочной политики безопасности в сети.

Сервисы безопасности

Идентификация / аутентификация.

Современные средства идентификации / аутентификации должны удовлетворять двум условиям:

- быть устойчивыми к сетевым угрозам (пассивному и активному прослушиванию сети);
- поддерживать концепцию единого входа в сеть.

Сервисы безопасности

- Первое требование можно выполнить, используя криптографические методы. В настоящее время общепринятыми являются подходы, основанные на системе Kerberos или службе каталогов с сертификатами в стандарте X.509.
- Единый вход в сеть — это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной.

Сервисы безопасности

Разграничение доступа. Разграничение доступа является самой исследованной областью информационной безопасности.

Динамичность современной программной среды в сочетании со сложностью отдельных компонентов существенно сужает область применимости самой употребительной - *дискреционной модели* управления доступом (называемой также моделью с произвольным управлением). При определении допустимости доступа важно не только (и не столько) то, кто обратился к объекту, но и то, какова семантика действия. Без привлечения семантики нельзя выявить троянские программы, противостоять которым произвольное управление доступом не в состоянии.

Сервисы безопасности

Протоколирование/аудит. Протоколирование и аудит традиционно являлись рубежом обороны, обеспечивающим анализ последствий нарушения информационной безопасности и выявление злоумышленников. Такой аудит можно назвать пассивным.

В современный арсенал защитных средств вошел активный аудит, направленный на выявление подозрительных действий в реальном масштабе времени. Активный аудит включает два вида действий:

- выявление нетипичного поведения (пользователей, программ или аппаратуры);
- выявление начала злоумышленной активности.

Сервисы безопасности

Экранирование. Экранирование как сервис безопасности выполняет следующие функции:

- разграничение межсетевого доступа путем фильтрации передаваемых данных;
- преобразование передаваемых данных.

Современные межсетевые экраны фильтруют данные на основе заранее заданной базы правил, что позволяет, по сравнению с традиционными операционными системами, реализовывать гораздо более гибкую политику безопасности. При комплексной фильтрации, охватывающей сетевой, транспортный и прикладной уровни, в правилах могут фигурировать сетевые адреса, количество переданных данных, операции прикладного уровня, параметры окружения (например, время) и т.п.

Сервисы безопасности

Туннелирование. Его суть состоит в том, чтобы «упаковать» передаваемую порцию данных, вместе со служебными полями, в новый «конверт». Данный сервис может применяться для нескольких целей:

- осуществление перехода между сетями с разными протоколами;
- обеспечение конфиденциальности и целостности всей передаваемой порции, включая служебные поля.

Сервисы безопасности

Шифрование. Шифрование — важнейшее средство обеспечения конфиденциальности и одновременно самое конфликтное место информационной безопасности. У компьютерной криптографии две стороны — собственно криптографическая и интерфейсная, позволяющая сопрягаться с другими частями информационной системы.

Сервисы безопасности

Контроль целостности. В современных системах контроль целостности должен распространяться не только на отдельные порции данных, аппаратные или программные компоненты. Он обязан охватывать распределенные конфигурации, защищать от несанкционированной модификации потоки данных.

В настоящее время существует достаточно решений для контроля целостности и с системной, и с сетевой направленностью (обычно контроль выполняется прозрачным для приложений образом как часть общей протокольной активности). Стандартизирован программный интерфейс к этому сервису.

Сервисы безопасности

Контроль защищенности. Контроль защищенности по сути представляет собой попытку «взлома» информационной системы, осуществляемого силами самой организации или уполномоченными лицами. Идея данного сервиса в том, чтобы обнаружить слабости в защите раньше злоумышленников. В первую очередь, имеются в виду не архитектурные (их ликвидировать сложно), а «оперативные» бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения.

Сервисы безопасности

Обнаружение отказов и оперативное восстановление. Обнаружение отказов и оперативное восстановление относятся к числу сервисов, обеспечивающих высокую доступность (готовность). Его работа опирается на элементы архитектурной безопасности, а именно на существование избыточности в аппаратно-программной конфигурации.

Международные стандарты X.800 и X.509

Стандарт X.800 предусматривает следующие сервисы безопасности:

- аутентификация (имеются в виду — аутентификация партнеров по общению и аутентификация источника данных);
- управление доступом — обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети;
- конфиденциальность данных. В X.800 под этим названием объединены существенно разные вещи — от защиты отдельной порции данных до конфиденциальности трафика;
- целостность данных. Данный сервис подразделяется на подвиды в зависимости от того, что контролируется — целостность сообщений или потока данных, обеспечивается ли восстановление в случае нарушения целостности;
- неотказуемость. Данный сервис относится к прикладному уровню, то есть имеется в виду невозможность отказаться от содержательных действий таких, например, как отправка или прочтение письма.

Международные стандарты X.800 и X.509

Стандарт X.509 описывает процедуру аутентификации с использованием службы каталогов. Наиболее ценной в стандарте оказалась не сама процедура, а ее служебный элемент — структура сертификатов, хранящих имя пользователя, криптографические ключи и сопутствующую информацию. Подобные сертификаты — важнейший элемент современных схем аутентификации и контроля целостности.

Архитектура механизмов защиты информации в сетях ЭВМ

Архитектуру механизмов защиты информации рассмотрим на примере наиболее распространенной эталонной модели взаимодействия открытых систем (ВОС).

Основные концепции применения методов и средств защиты информации на уровне базовой эталонной модели изложены в международном стандарте ISO/IEC 7498-2 «Базовая эталонная модель взаимодействия открытых систем, часть 2 «Архитектура безопасности». В самом наименовании ВОС термин «открытые» подразумевает, что если вычислительная система соответствует стандартам ВОС, то она будет открыта для взаимосвязи с любой другой системой, которая соответствует тем же стандартам. Это, естественно, относится и к вопросам защиты информации.

Архитектура механизмов защиты информации в сетях ЭВМ

В ВОС различают следующие основные активные способы несанкционированного доступа к информации:

- маскировка одного логического объекта под другой, который обладает большими полномочиями (ложная аутентификация абонента);
- переадресация сообщений (преднамеренное искажение адресных реквизитов);

Архитектура механизмов защиты информации в сетях ЭВМ

- модификация сообщений (преднамеренное искажение информационной части сообщения);
- блокировка логического объекта с целью подавления некоторых типов сообщений (выборочный или сплошной перехват сообщений определенного абонента, нарушение управляющих последовательностей и т. п.).

Архитектура механизмов защиты информации в сетях ЭВМ

Перечень видов услуг, предоставляемых по защите информации

1. аутентификация равнозначного логического объекта — обеспечивается во время установления им соединения или во время нормального обмена данными для гарантии того, что равноправный логический объект, с которым осуществляется взаимодействие, является тем, за кого себя выдает. Для аутентификации равнозначного логического объекта требуется, чтобы лежащий ниже уровень обеспечивал услуги с установлением соединения;
2. аутентификация источника данных — подтверждение подлинности источника (абонента-отправителя) сообщения. Эта услуга не ориентирована на соединение и не обеспечивает защиту от дублирования («проигрывания» ранее перехваченного и записанного нарушителем) блока данных;

Архитектура механизмов защиты информации в сетях ЭВМ

3. управление доступом (разграничение доступа) — обеспечивает защиту от несанкционированного доступа к ресурсам, потенциально доступным посредством ВОС. Доступ может быть ограничен полностью или частично. Например, для информационного ресурса может быть ограничен доступ по чтению, записи, уничтожению информации;
4. засекречивание соединения — обеспечивает конфиденциальность всех сообщений, передаваемых пользователями в рамках данного соединения. Данная услуга направлена на предотвращение возможности ознакомления с содержанием сообщений со стороны любых лиц, не являющихся легальными пользователями соединения. При этом в некоторых случаях нет необходимости в защите срочных данных, а также данных в запросе на установление соединения;

Архитектура механизмов защиты информации в сетях ЭВМ

5. засекречивание в режиме без установления соединения — обеспечивает конфиденциальность всех данных пользователя в сообщении (единственном сервисном блоке данных), передаваемом в режиме без установления соединения;
6. засекречивание поля данных — обеспечивает конфиденциальность отдельных полей данных пользователя на всем соединении или в отдельном сервисном блоке данных;
7. засекречивание трафика — препятствует возможности извлечения информации из наблюдаемого трафика;

Архитектура механизмов защиты информации в сетях ЭВМ

8. целостность соединения с восстановлением — позволяет обнаружить попытки вставки, удаления, модификации или переадресации в последовательности сервисных блоков данных. При нарушении целостности предпринимается попытка ее восстановления;
9. целостность соединения без восстановления — обеспечивает те же возможности, что и предыдущая услуга, но без попытки восстановления целостности;
10. целостность поля данных в режиме с установлением соединения — обеспечивает целостность отдельного поля данных пользователя во всем потоке сервисных блоков данных, передаваемых через это соединение, и обнаруживает вставку, удаление, модификацию или переадресацию этого поля;

Архитектура механизмов защиты информации в сетях ЭВМ

11. целостность блока данных в режиме без установления соединения — обеспечивает целостность единственного сервисного блока данных при работе без установления соединения и позволяет обнаружить модификацию и некоторые формы вставки и переадресации;
12. целостность поля данных в режиме без установления соединения — позволяет обнаружить модификацию выбранного поля в единственном сервисном блоке данных;

Архитектура механизмов защиты информации в сетях ЭВМ

13. информирование об отправке данных — позволяет обнаружить логические объекты, которые посылают информацию о нарушении правил защиты информации. Информирование об отправке предоставляет получателю информацию о факте передачи данных в его адрес, обеспечивает подтверждение подлинности абонента-отправителя. Услуга направлена на предотвращение отрицания отправления, т.е. возможности отказа от факта передачи данного сообщения со стороны отправителя;
14. информирование о доставке — позволяет обнаружить логические объекты, которые не выполняют требуемых действий после приема информации, предоставляет отправителю информацию о факте получения данных адресатом. Услуга направлена на предотвращение отрицания доставки, т.е. обеспечивает защиту от попыток получателя отрицать факт получения данных.

Архитектура механизмов защиты информации в сетях ЭВМ

Механизм управления доступом, предназначенный для реализации соответствующего вида перечисленных выше услуг, основан на идентификации логического объекта (или информации о нем) для проверки его полномочий и разграничения доступа. Если логический объект пытается получить доступ к ресурсу, использование которого ему не разрешено, механизм управления доступом (в основе которого также наиболее эффективными средствами являются криптографические) отклонит эту попытку и сформирует запись в специальном системном журнале для последующего анализа.

Архитектура механизмов защиты информации в сетях ЭВМ

Механизмы управления доступом могут быть основаны на:

1. информационных базах управления доступом, где содержатся сведения о полномочиях всех логических объектов;
2. системах управления криптографическими ключами, обеспечивающими доступ к соответствующей информации;
3. идентифицирующей информации (такой, как пароли), предъявление которой дает право доступа;
4. специальных режимах и особенностях работы логического объекта, которые дают право доступа к определенным ресурсам;
5. специальных метках, которые, будучи ассоциированы с конкретным логическим объектом, дают ему определенные права доступа;
6. времени, маршруте и продолжительности доступа.

Межсетевые экраны — брандмауэры (FireWall)

Гостехкомиссией при Президенте РФ разработан Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

Межсетевые экраны — брандмауэры (FireWall)

В указанном документе межсетевой экран (МЭ) определяется как локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и /или выходящей из АС.

Межсетевые экраны

Межсетевой экран располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети).

При рассмотрении любого вопроса, касающегося сетевых технологий, основой служит семиуровневая эталонная модель ISO/OSI. *Межсетевые экраны* также целесообразно классифицировать по уровню *фильтрации* – канальному, сетевому, транспортному или прикладному. Соответственно, можно говорить об **экранирующих концентраторах** (мостах, коммутаторах) (уровень 2), **маршрутизаторах** (уровень 3), о транспортном *экранировании* (уровень 4) и о прикладных *экранах* (уровень 7). Существуют также комплексные *экраны*, анализирующие информацию на нескольких уровнях.

Межсетевые экраны — брандмауэры (FireWall)

МЭ обеспечивает защиту АС посредством фильтрации информации (как минимум на сетевом уровне), т. е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АС к объектам другой АС.

Межсетевые экраны — брандмауэры (FireWall)

Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами и объектами. Как следствие субъекты из одной АС получают доступ только к разрешенным информационным объектам из другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола.

Межсетевые экраны — брандмауэры (FireWall)

Основными компонентами брандмауэра являются:

- политика сетевого доступа
- механизмы усиленной аутентификации
- фильтрация пакетов
- прикладные шлюзы

Межсетевые экраны — брандмауэры (FireWall)

Выделяются пять классов МЭ, где пятый — низший, а первый — высший. Классифицируемый экран должен фильтровать потоки данных, по крайней мере, на сетевом уровне. При умеренных требованиях по защите информации можно ограничиться МЭ пятого или четвертого классов, реализованных в виде маршрутизаторов с включенными средствами фильтрации (экранирующих маршрутизаторов).

Межсетевые экраны — брандмауэры (FireWall)

ПРИМЕР

Брандмауэр FireBox (производства WatchGuard) имеет смешанную архитектуру — динамической фильтрации пакетов и «прозрачного» прокси (proxy) (при этом с глобальной сетью организуется двухсторонняя связь, о proxy-технологии более подробно будет сказано далее). В архитектуре брандмауэра:

- обеспечивается оптимальный баланс между безопасностью и производительностью;
- динамическая фильтрация пакетов отслеживает состояние соединения, что позволяет «отфильтровывать» не только пакеты, но и соединения;

Межсетевые экраны — брандмауэры (FireWall)

- наборы правил являются динамическими и могут быть изменены во время работы (в набор входит 28 стандартных правил типа DNS, Telnet и др. и могут определяться правила пользователями в зависимости от потребностей и угроз безопасности);
- прокси анализирует трафик на сетевом уровне, что дает возможность получить более надежную защиту;
- могут распознаваться подмены сервисов и пакетов;
- имеется функция регистрации пользователей (это позволяет не только повысить безопасность, но и вести мониторинг сети на основе имен пользователей, а не IP-адресов и имен хостов);
- обеспечивается поддержка VPN (Virtual Private Network — виртуальная частная сеть), т. е. безопасный доступ в корпоративную сеть через Internet (для авторизованных удаленных пользователей. При этом используется протокол PPTP (Point-to-Point Tunneling Protocol — туннельный протокол точка-точка), который создает в общей сети безопасный «туннель», через который «прозрачно» проходит весь трафик.

Прокси (Proxy) серверы

Можно использовать специальную программу, которая позволяла бы остальным компьютерам эмулировать выход в Internet, оставаясь при этом «невидимыми» со стороны глобальной сети. Такой компьютер и называется прокси-сервером (proxy — доверенный).

В качестве примера вкратце рассмотрим Microsoft Proxy Server 2.0. Этот продукт, являясь кэширующим сервером (повышает эффективность работы сети — сокращается сетевой трафик), выполняет функции брандмауэра и обеспечивает безопасный доступ в Internet. Серверный компьютер имеет два сетевых адаптера — один соединяет компьютер с сетью, а другой — с Internet.

Прокси (Proxy) серверы

Т.к. локальная сеть «не видна» из Internet, то легальный IP-адрес должен иметь только внешний сетевой интерфейс. IP-адреса внутри сети можно выдавать из пула, зарезервированного для изолированных сетей. Шлюз по умолчанию должен быть указан только для внешнего сетевого интерфейса.