Лекция 2
Программно-аппаратные средства защиты информации в сети

1. Аппаратные средства защиты информации
2. Программные средства защиты информации
3. Сервисы безопасности
4. Вопросы

Аппаратные средства защиты информации

Программно-аппаратные средства защиты информации — это сервисы безопасности, встроенные в сетевые операционные системы.

К **аппаратным средствам защиты информации** относятся электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к аппаратным, а не к инженерно-техническим средствам защиты является обязательное включение в состав технических средств КС.

К основным **аппаратным средствам** защиты информации относятся:

- устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т. п.);
- устройства для шифрования информации;
- устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы).

Примеры вспомогательных аппаратных средств защиты информации:

- устройства уничтожения информации на магнитных носителях;
- устройства сигнализации о попытках несанкционированных действий пользователей КС и др.

Программные средства защиты информации

Под **программными средствами защиты информации** понимают специальные программы, включаемые в состав программного обеспечения КС исключительно для выполнения защитных функций. К основным **программным средствам** защиты информации относятся:

- программы идентификации и аутентификации пользователей КС;
- программы разграничения доступа пользователей к ресурсам КС;
- программы шифрования информации;
- программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования.

Примеры **вспомогательных программных средств** защиты информации:

- программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т. п.);
- программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий;
- программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации);
- программы тестового контроля защищенности КС и др.

Сервисы безопасности

К **сервисам безопасности** относятся: идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование.

Под **идентификацией,** применительно к обеспечению информационной безопасности компьютерной сети, понимают однозначное распознавание уникального имени субъекта компьютерной сети. Идентификация предназначена для того, чтобы пользователь или вычислительный процесс, действующий по команде определенного пользователя, могли идентифицировать себя путем сообщения своего имени.

Аутентификация означает подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта). С помощью аутентификации вторая сторона убеждается, что пользователь, пытающийся войти в операционную систему, действительно тот, за кого себя выдает.

Средства управления доступом позволяют специфицировать и контролировать действия, которые пользователи и вычислительные процессы могут выполнять над информацией и другими компьютерными ресурсами, то есть речь идет о логическом управлении доступом, который реализуется программными средствами.

Логическое управление доступом обеспечивает конфиденциальность и целостность объектов путем запрещения обслуживания неавторизированных пользователей. Контроль прав доступа осуществляется посредством различных компонент программной среды — ядром сетевой операционной системы, дополнительными средствами безопасности, системой управления базами данных, посредническим программным обеспечением.

Протоколированием называется процесс сбора и накопления информации о событиях, происходящих в компьютерной сети.

Возможные события принято делить на три группы:

- внешние события, вызванные действиями других сервисов;
- внутренние события, вызванные действиями самого сервиса;
- клиентские события, вызванные действиями пользователей и администраторов.

Аудитом называется процедура анализа накопленной в результате протоколирования информации. Этот анализ может осуществляться оперативно в реальном времени или периодически.

Экран это средство разграничения доступа клиентов из одного сетевого множества к серверам, принадлежащим другому сетевому множеству. Функция экрана заключается в контроле всех информационных потоков между двумя множествами систем. Примерами экранов являются межсетевые экраны (брандмауэры (firewalls)), устанавливаемые для защиты локальной сети организации, имеющей выход в открытую среду.

Метод криптографии — одно из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Основной элемент криптографии шифрование (или преобразование данных в нечитабельную форму ключей шифрования расшифровки). В состав криптографической системы входят: один или нескольких алгоритмов шифрования, ключи, используемые этими алгоритмами шифрования, подсистемы управления ключами, незашифрованный и зашифрованный тексты.

При использовании метода криптографии на первом этапе к тексту, который необходимо шифровать, применяются алгоритм шифрования и ключ для получения из него зашифрованного текста. На втором этапе зашифрованный текст передается к месту назначения, где тот же самый алгоритм используется для его расшифровки.

Ключом называется число, используемое криптографическим алгоритмом для шифрования текста.

В криптографии используется два **метода шифрования** симметричное и асимметричное.

При **симметричном шифровании** для шифрования и для расшифровки отправителем и получателем применяется один и тот же ключ, об использовании которого

они договариваются заранее. Основной недостаток симметричного шифрования состоит в том, что ключ должен быть известен как отправителю, так и получателю, откуда возникает новая проблема безопасной рассылки ключей.

Существует также вариант симметричного шифрования, основанный на использовании составных ключей, когда секретный ключ делится на две части, хранящиеся отдельно. Таким образом, каждая часть сама по себе не позволяет выполнить расшифровку.

Асимметричное шифрование характеризуется тем, что при шифровании используются два ключа: первый ключ делается общедоступным (публичным) и используется для шифровки, а второй является закрытым (секретным) и используется для расшифровки

Дополнительным методом защиты шифруемых данных и проверки их целостности является **цифровая подпись.**

Вопросы

1. Что относится к сервисам безопасности?
2. Что является наиболее эффективным средством для защиты от сетевых атак?
3. Что называется утечкой информации?
4. Защита информации обеспечивается применением антивирусных средств?
5. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на …
6. Сервисы безопасности, встроенные в сетевые операционные системы, это…
7. Устройства для ввода идентифицирующей пользователя информации, устройства для шифрования информации; устройства для воспрепятствования несанкционированному включению рабочих станций и серверов, относятся к …
8. Устройства уничтожения информации на магнитных носителях; устройства сигнализации о попытках несанкционированных действий пользователей компьютерных сетей относятся к…
9. Программы идентификации и аутентификации пользователей КС; программы разграничения доступа пользователей к ресурсам КС; программы шифрования информации; программы защиты информационных от несанкционированного изменения, использования и копирования относятся к …
10. Программы уничтожения остаточной информации; программы аудита событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий; программы имитации работы с нарушителем программы тестового контроля защищенности КС относятся к…
11. Однозначное распознавание уникального имени субъекта компьютерной сети – это…
12. Подтверждение подлинности субъекта – это…
13. Процесс сбора и накопления информации о событиях, происходящих в компьютерной сети – это…
14. Процедура анализа накопленной в результате протоколирования информации – это…
15. Средство разграничения доступа клиентов из одного сетевого множества к серверам, принадлежащим другому сетевому множеству – это…
16. Число, используемое криптографическим алгоритмом для шифрования текста – это…
17. Назовите дополнительный метод защиты шифруемых данных и проверки их целостности.
18. Назовите вид шифрования, при котором используются два ключа, один ключ.