Лекция 8. Вопросы безопасности в ЛВС

Лока́льная вычисли́тельная сеть — **компьютерная сеть**, покрывающая обычно относительно небольшую территорию или небольшую группу зданий.

Характерными особенностями ЛВС являются распределенное хранение файлов, удаленная обработка данных (вычисления) и передача сообщений (электронная почта), а также сложность проведения контроля за работой пользователей и состоянием общей безопасности ЛВС.

Средства защиты информации должны располагаться на каждом узле ЛВС вне зависимости от того, обрабатывается ли на нем конфиденциальная информация. Каждый администратор и пользователь ЛВС должен иметь уникальный пароль, идентификатор и , в случае использования криптографических средств защиты, ключ шифрования.

Класс защищенности ЛВС определяется в соответствии с рассмотренной выше классификацией АС.

Состав пользователей ЛВС должен утверждаться руководителем организации и строго контролироваться. Все изменения состава пользователей, их прав и привилегий должны регистрироваться.

Защита информации при межсетевом взаимодействии

Межсетевое взаимодействие подразумевает под собой взаимодействие ЛВС, ни одна из которых не имеет выхода в Интернет.

В данном случае коммуникационное оборудование (маршрутизаторы, коммутаторы, концентраторы и пр.) и все соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах контролируемой зоны. При конфигурировании коммуникационного оборудования) и прокладке кабельной системы ЛВС рекомендуется учитывать разделение трафика по отдельным сетевым фрагментам на производственной основе и видам деятельности предприятия.

При подключении ЛВС к АС с другим классом защищенности необходимо использовать межсетевой экран в соответствии с Руководящим Документом

Гостехкомиссии России "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации".

Для защиты конфиденциальной информации при ее передаче по каналам связи из одной АС в другую необходимо использовать:

- в АС класса 1Г - МЭ не ниже класса 4;
- в АС класса 1Д и 2Б, 3Б - МЭ класса 5 или выше.

Если каналы связи выходят за пределы контролируемой зоны, необходимо использование защищенных каналов связи, волоконно-оптических линии связи либо сертифицированных криптографических средств защиты.

Защита информации при работе с системами управления базами данных

При работе с системами управления базами данных (СУБД) и базами данных (БД) необходимо учитывать следующие особенности защиты информации от НСД:

- в БД может накапливаться большой объем интегрированной информации по различным тематическим направлениям, предназначенной для различных пользователей;
- БД могут быть физически распределены по различным устройствам и узлам сети;
- БД могут включать информацию различного уровня конфиденциальности;
- разграничение доступа пользователей к БД средствами операционной системы и/или СЗИ НСД может осуществляться только на уровне файлов БД;
- разграничение доступа пользователей к объектам БД: таблицам, схемам, процедурам, записям, полям записей в базах данных и т.п., может осуществляться только средствами СУБД, если таковые имеются;
- регистрация действий пользователей при работе с объектами БД может осуществляться также только средствами СУБД, если таковые имеются;

- СУБД могут обеспечивать одновременный доступ многих пользователей (клиентов) к БД с помощью сетевых протоколов, при этом запросы пользователя к БД обрабатываются на сервере и результаты обработки направляются пользователям (клиентам).

С учетом указанных особенностей при создании БД рекомендуется:

- при выборе СУБД ориентироваться на операционные системы и СУБД, включающие либо штатные сертифицированные средства защиты информации от НСД, либо имеющие соответствующие сертифицированные дополнения в виде СЗИ НСД;
- при использовании СУБД, не имеющих средств разграничения доступа, производить разбиение БД на отдельные файлы, разграничение доступа к которым можно проводить средствами ОС и/или СЗИ НСД;
- при использовании современных СУБД, основанных на модели клиент-сервер, использовать их штатные средства защиты информации от НСД, применять средства регистрации (аудита) и разграничение доступа к объектам БД на основе прав, привилегий, ролей, представлений (VIEW), процедур и т.п.[11.1]

Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

Приведенные ниже рекомендации определены для АС, обрабатывающих конфиденциальную информацию, не относящихся к государственным информационным ресурсам.

Подключение к сети абонентского пункта должно утверждаться руководителем организации на основании обоснования необходимости данного подключения. **Абонентский пункт (АП)** - средства вычислительной техники учреждения (предприятия), подключаемые к Сетям с помощью коммуникационного оборудования. Обоснование подключения должно содержать:

- наименование Сети, реквизиты организации-владельца Сети и провайдера Сети;

- состав технических средств для оборудования АП;
- предполагаемые виды работ и используемые прикладные сервисы Сети (E-Mail, FTP, Telnet, HTTP и т.п.) для АП в целом и для каждого абонента, в частности:
  - режим подключения АП и абонентов к Сети (постоянный, в т.ч. круглосуточный, временный);
  - состав общего и телекоммуникационного программного обеспечения АП и абонентов (ОС, клиентские прикладные программы для сети - Browsers и т.п.);
  - число и перечень предполагаемых абонентов (диапазон используемых IP-адресов);
  - меры и средства защиты информации от НСД, которые будут применяться на АП, организация-изготовитель, сведения о сертификации, установщик, конфигурация, правила работы с ними;
  - перечень сведений конфиденциального характера, обрабатываемых (хранимых) на АП, подлежащих передаче и получаемых из Сети.

Если АП обрабатывает открытую информацию и представляет собой автономную ПЭВМ с модемом, то можно не использовать средства защиты информации от НСД. АП, на которых обрабатывается не открытая информация, должны быть оборудованы средствами защиты и удовлетворять требованиям законодательства.

Подключение ЛВС организации к Сети должно осуществляться через межсетевой экран, сертифицированный по требованиям безопасности информации. Доступ к МЭ и его конфигурированию должен быть только у выделенных администраторов. МЭ должен быть сконфигурирован так, чтобы запросы пользователей ЛВС обрабатывались, а внешние запросы отбрасывались и не проникали в ЛВС.

Почтовый сервер и Web-сервер не должны входить в состав ЛВС и должны подключаться к Сети по отдельному сетевому фрагменту (через маршрутизатор).

На технических средствах АП должно находится только то ПО, которое необходимо для выполнения работ в соответствии с обоснованием необходимости подключения. Установка и конфигурирование ПО осуществляется назначенным администратором, абонент АП не должен иметь на это прав.

СЗИ НСД, устанавливаемая на автономную ПЭВМ, рабочие станции и серверы внутренней ЛВС организации при обработке на них конфиденциальной информации, должна осуществлять:

- идентификацию и аутентификацию пользователей при доступе к автономной ПЭВМ, рабочим станциям и серверам внутренней ЛВС по идентификатору и паролю;
- контроль доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС на основе дискреционного принципа;
- регистрацию доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС, включая попытки НСД;
- регистрацию фактов отправки и получения абонентом сообщений (файлов, писем, документов).

При этом СЗИ НСД должна запрещать запуск абонентом произвольных программ, не включенных в состав программного обеспечения АП.

Модификация конфигурации программного обеспечения АП должна быть доступна только со стороны администратора, ответственного за эксплуатацию АП.

Средства регистрации и регистрируемые данные должны быть недоступны для абонента. СЗИ НСД должна быть целостной, т.е. защищенной от несанкционированной модификации и не содержащей путей обхода механизмов контроля.

Тестирование всех функций СЗИ НСД с помощью специальных программных средств должно проводится не реже одного раза в год.

При создании АП рекомендуется:

- при предоставлении абонентам прикладных сервисов исходить из принципа минимальной достаточности. То есть, если абоненту нужна только электронная почта, предоставить доступ только к ней.
- использовать операционные системы со встроенными средствами защиты от НСД (например, Windows) или использовать сертифицированные СЗИ от НСД.
- максимально использовать имеющиеся у маршрутизаторов средства фильтрации.
- контролировать исходящую и входящую во внутреннюю сеть информацию. Копии исходящей почты (файлов) хранить в отдельном месте с целью дальнейшего анализа со стороны администратора (службы безопасности).
- контролировать информацию, публикуемую на Web-серверах;
- приказом по организации назначаются абоненты, лица, ответственные за эксплуатацию АП и его защиту(например, администраторы безопасности);
- вопросы обеспечения безопасности информации на АП должны быть отражены в инструкции, определяющей порядок подключения абонентов, конфигурирования программного обеспечения, работы с почтой и т.п.

К работе с Сетью допускаются люди, ознакомленные с требованиями взаимодействия с другими абонентами. При этом абоненты сети обязаны:

- знать порядок регистрации и взаимодействия в Сети;
- знать инструкцию по обеспечению безопасности информации на АП;
- знать правила работы со средствами защиты информации от НСД, установленными на АП (серверах, рабочих станциях АП);
- уметь пользоваться средствами антивирусной защиты;
- после окончания работы в Сети проверить свое рабочее место на наличие "вирусов".

Ведение учета абонентов, имеющих доступ в Сеть, организуется в соответствии с установленном в конкретной организации порядке.

Вопросы для самопроверки:

1. Характерные особенности ЛВС
2. Требования к абонентам сети