Лекция 7
Тема: Средства защиты информации в компьютерных системах.

Задание 1. Прочитайте текст, составьте краткий конспект. Делайте записи в тетради аккуратно. Конспект будет проверен при выходе на очное обучение.

Существование и развитие информационного общества на современном этапе невозможно без использования информационных сетей, глобальных компьютерных сетей и сетей связи — радио, телевидения, фиксированных и мобильных телефонных сетей, *Internet* и т.д. В связи с этим в вычислительной системе понятие безопасности является весьма широким. Оно подразумевает и надежность работы компьютера, и сохранность ценных данных, и защиту информации от внесения в нее изменений неуполномоченными лицами, и сохранение тайны переписи в электронной связи.

Информационная безопасность *(в широком смысле)* – это состояние защищенности интересов субъектов информационных отношений от нежелательных действий в отношении принадлежащей им информации и информационных процессов, в которых они принимают участие.

Информационной безопасностью называют комплекс организационных, технических и технологических мер по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе.

Информационная безопасность дает гарантию того, что достигаются следующие цели:

- *конфиденциальность* информации (свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц);
- *целостность* информации и связанных с ней процессов (неизменность информации в процессе ее передачи или хранения);
- *доступность* информации (свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц).

Защита информации – это применение различных средств и методов, использование мер и осуществление мероприятий для того, чтобы обеспечить систему надежности передаваемой, хранимой и обрабатываемой информации.

Угроза безопасности компьютерной системы – это потенциально возможное происшествие (преднамеренное или нет), которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

Политика безопасности – это комплекс мер и активных действий по управлению и совершенствованию систем и технологий безопасности, включая информационную безопасность.

Источники угроз:

Известны следующие источники угроз безопасности информационных систем:

I. антропогенные источники, вызванные случайными или преднамеренными действиями субъектов. Антропогенные источники угроз делятся:

1. внутренние (воздействия со стороны сотрудников компании) и внешние (несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения) источники;

2. непреднамеренные (случайные) и преднамеренные действия субъектов. Существует достаточно много возможных направлений утечки информации и путей несанкционированного доступа к ней в системах и сетях:

3. перехват информации;

4. модификация информации (исходное сообщение или документ изменяется или подменяется другим и отсылается адресату);
5. подмена авторства информации (кто-то может послать письмо или документ от вашего имени);
6. использование недостатков операционных систем и прикладных программных средств;
7. копирование носителей информации и файлов с преодолением мер защиты;
8. незаконное подключение к аппаратуре и линиям связи;
9. маскировка под зарегистрированного пользователя и присвоение его полномочий;
10. введение новых пользователей;
11. внедрение компьютерных вирусов и так далее.

II. техногенные источники, приводящие к отказам и сбоям технических и программных средств из-за устаревших программных и аппаратных средств или ошибок в ПО;

III. стихийные источники, вызванные природными катаклизмами или форс-мажорными обстоятельствами.

Основные методы обеспечения информационной безопасности:

Авторизация. Этот метод позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.

Идентификация и аутентификация. Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам. Аутентификация- проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д. Последние годы активно внедряются следующие методы аутентификации:

- Биометрия. Используется аутентификация по геометрии руки, радужной оболочки сетчатки глаза, клавиатурный почерк, отпечатки глаза и т.п.
- SMART-карты (интеллектуальные карты). Их удобство заключается в портативном и широком спектре функций, которые могут быть легко модифицированы. Недостатком SMART-карты является их дороговизна, так как требуют определенных устройств для считывания информации.
- e-Token (электронный ключ) – аналог SMART-карты, выполненный в виде брелка, подключающегося через USB-порт. Достоинство e-Token заключается в том, что он не требует специальных, дорогостоящих карт -reader.

Обеспечение безопасности информации в вычислительных сетях и в автономно работающих ПЭВМ достигается комплексом организационных, организационно-технических и программных мер.

К организационным мерам защиты относится:

- ограничение доступа в помещения, в которых происходит подготовка и обработка информации;
- допуск к обработке и передаче конфиденциальной информации только проверенных должностных лиц;
- хранение магнитных носителей и регистрационных журналов в закрытых для доступа посторонних лиц сейфах;
- исключение просмотра посторонними лицами содержания обрабатываемых материалов через дисплей, принтер и т.д.;
- использование криптографических кодов при передаче по каналам связи ценной информации;
- уничтожение красящих лент, бумаги и иных материалов, содержащих фрагменты ценной информации.

Организационно-технические меры включают:

- осуществление питания оборудования, обрабатывающего ценную информацию от независимого источника питания или через специальные сетевые фильтры;
- установку на дверях помещений кодовых замков;
- использования для отображения информации при вводе-выводе жидкокристаллических или плазменных дисплеев, а для получения твердых копий — струйных принтеров и термопринтеров, поскольку дисплей дает такое высокочастотное электромагнитное излучение, что изображение с его экрана можно принимать на расстоянии нескольких сотен километров;
- уничтожение информации, хранящейся в ПЗУ и на НЖМД, при списании или отправке ПЭВМ в ремонт;
- установка клавиатуры и принтеров на мягкие прокладки с целью снижения возможности снятия информации акустическим способом;
- ограничение электромагнитного излучения путем экранирования помещений, где проходит обработка информации, листами из металла или из специальной пластмассы.

Технические средства защиты — это системы охраны территорий и помещений с помощью экранирования машинных залов и организации контрольно-пропускных систем.

Защита информации в сетях и вычислительных средствах с помощью технических средств реализуется на основе организации доступа к памяти с помощью:

- контроля доступа к различным уровням памяти компьютеров;
- блокировки данных и ввода ключей;
- выделения контрольных битов для записей с целью идентификации и др.

Архитектура программных средств защиты информации включает:

- контроль безопасности, в том числе контроль регистрации вхождения в систему, фиксацию в системном журнале, контроль действий пользователя;
- реакцию (в том числе звуковую) на нарушение системы защиты контроля доступа к ресурсам сети;
- контроль мандатов доступа;
- формальный контроль защищенности операционных систем (базовой общесистемной и сетевой);
- контроль алгоритмов защиты;
- проверку и подтверждение правильности функционирования технического и программного обеспечения.

Для надежной защиты информации и выявления случаев неправомочных действий проводится регистрация работы системы: создаются специальные дневники и протоколы, в которых фиксируются все действия, имеющие отношение к защите информации в системе. Фиксируются время поступления заявки, ее тип, имя пользователя и терминала, с которого инициализируется заявка. При отборе событий, подлежащих регистрации, необходимо иметь в виду, что с ростом количества регистрируемых событий затрудняется просмотр дневника и обнаружение попыток преодоления защиты. В этом случае можно применять программный анализ и фиксировать сомнительные события.

Используются также специальные программы для тестирования системы защиты. Периодически или в случайно выбранные моменты времени они проверяют работоспособность аппаратных и программных средств защиты.

К отдельной группе мер по обеспечению сохранности информации и выявлению несанкционированных запросов относятся **программы обнаружения нарушений** в режиме реального времени. Программы данной группы формируют специальный сигнал при регистрации действий, которые могут привести к неправомерным действиям по отношению к защищаемой информации. Сигнал может содержать информацию о характере нарушения, месте его возникновения и другие характеристики. Кроме того, программы могут запретить доступ к защищаемой информации или симулировать такой

режим работы (например, моментальная загрузка устройств ввода-вывода), который позволит выявить нарушителя и задержать его соответствующей службой.

Один из распространенных способов защиты — явное указание **секретности выводимой информации**. В системах, поддерживающих несколько уровней секретности, вывод на экран терминала или печатающего устройства любой единицы информации (например, файла, записи или таблицы) сопровождается специальным грифом с указанием уровня секретности. Это требование реализуется с помощью соответствующих программных средств.

В отдельную группу выделены средства защиты от несанкционированного использования **программного обеспечения**. Они приобретают особое значение вследствие широкого распространения персональных компьютеров. Исследования, проведенные зарубежными экспертами, свидетельствуют, что на одну проданную копию оригинальной программы приходится минимум одна нелегальная копия. А для особо популярных программ это соотношение достигает 1:7.

Особое внимание уделяется **законодательным средствам**, регулирующим использование программных продуктов. В соответствии с Законом республики предусматриваются санкции к физическим и юридическим лицам за нелегальное приобретение и использование программных средств.

Большую опасность представляют **компьютерные вирусы.** Если не принимать мер по защите от вируса, то последствия заражения вирусом компьютеров могут быть серьезными.

Компьютерный вирус – это специальная программа, наносящая заведомый вред компьютеру, на котором она запускается на выполнение, или другим компьютерам в сети.

Основной функцией вируса является его размножение.

Классификация компьютерных вирусов:

•по среде обитания;

Файловые вирусы. Наносят вред файлам. Создают файл-двойник с именем оригинала.

Загрузочные вирусы. Внедряются в загрузочный сектор диска. Операционная система при этом загружается с ошибками и сбоями.

Макро-вирусы. «Портят» документы Word, Excel и других прикладных программ операционной системы Windows.

Сетевые вирусы. Распространяются по Internet через электронные письма или после посещения сомнительных сайтов.

•по операционным системам;

Для каждой операционной системы создаются свои вирусы, которые будут «работать» только в ней. Но существуют и универсальные вирусы, которые способны внедряться в различные операционные системы.

•по алгоритму работы;

Резидентность. Вирусы, обладающие этим свойством, действуют постоянно пока компьютер включен.

Самошифрование и полиморфизм. Вирусы-полиморфики изменяют свой код или тело программы, что их трудно обнаружить.

Стелс–алгоритм. Вирусы- невидимки «прячутся» в оперативной памяти и антивирусная программа их не может обнаружить.

Нестандартные приемы. Принципиально новые методы воздействия вируса на компьютер

•по деструктивным возможностям;

Безвредные не наносят никакого вреда ни пользователю, ни компьютеру, но занимают место на жестком диске.

Неопасные наносят моральный ущерб пользователю Вызывают визуальные графические или звуковые эффекты.
Опасные уничтожают информацию в файлах. «Портят» файлы, делают их несчитываемыми и т.д.
Очень опасные сбивают процесс загрузки ОС, после чего требуется ее переустановка; или «портят» винчестер, что его требуется форматировать.

Виды антивирусных программ:

•Детекторы позволяют обнаруживать файлы, заражённые одним из нескольких известных вирусов. Некоторые программы-детекторы также выполняют эвристический анализ файлов и системных областей дисков, что часто (но отнюдь не всегда) позволяет обнаруживать новые, не известные программе-детектору, вирусы.

•Фильтры - это резидентные программы, которые оповещают пользователя о всех попытках какой-либо программы записаться на диск, а уж тем более отформатировать его, а также о других подозрительных действиях.

•Программы-доктора или фаги не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние.

•Ревизоры запоминают сведения о состоянии файлов и системных областей дисков, а при последующих запусках – сравнивают их состояние исходным. При выявлении несоответствий об этом сообщается пользователю.

•Сторожа или фильтры располагаются резидентно в оперативной памяти компьютера и проверяют на наличие вирусов запускаемые файлы и вставляемые USB-накопители.

•Программы-вакцины или иммунизаторы модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже заражёнными.

Недостатки антивирусных программ

•Ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов.

•Антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск. Особенно это может быть заметно на слабых компьютерах.

•Антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания).

•Антивирусные программы загружают обновления из Интернета, тем самым расходуя трафик.

•Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. Однако во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.