Лекция 12

Защита информации

Качество информации является сложным понятием, его основу составляет базовая система показателей, включающая показатели трех классов:

- **класс выдачи** (своевременность, актуальность, полнота, доступность и другие);
- **класс обработки** (достоверность, адекватность и другие);
- **класс защищённости** (физическая целостность информации, логическая целостность информации, безопасность информации).

Одним из наиболее существенных показателей качества информации является её безопасность.

В качестве предмета защиты рассматривается информация, хранящаяся, обрабатываемая и передаваемая в компьютерных системах.
Понятие компьютерные системы (КС) охватывает следующие системы:

- ***ЭВМ всех классов и назначений;***
- ***вычислительные комплексы и системы;***
- ***вычислительные сети (локальные, глобальные).***

Особенностями этой информации являются:

- двоичное её представление внутри системы, независимо от физической сущности носителей исходной информации;
- высокая степень автоматизации обработки и передачи информации;
- концентрация большого количества информации в КС.

Государственную тайну могут содержать сведения, принадлежащие государству. Сведениям, представляющим ценность для государства, могут быть присвоены следующие степени секретности (гриф):

- особой важности;
- совершенно секретно;
- секретно;
- для служебного пользования.

Коммерческую тайну могут содержать сведения, принадлежащие частному лицу, фирме, корпорации и тому подобное. Сведениям, представляющим коммерческую тайну, могут быть присвоены следующие категории:

- коммерческая тайна – строго конфиденциально или строго конфиденциально – строгий учёт;
- коммерческая тайна – конфиденциально или строго конфиденциально;
- коммерческая тайна или конфиденциально.

Безопасность (защищённость) информации в КС – это состояние всех компонент компьютерной системы, обеспечивающее на требуемом уровне защиту информации от возможных угроз.

Безопасность информации в КС (***информационная безопасность***) является одним из основных направлений обеспечения безопасности государства, отрасли, ведомства, государственной организации или частной структуры.

Информационная безопасность достигается проведением руководством соответствующего уровня политики информационной безопасности. Основным документом, на основе которого проводится политика информационной безопасности, является программа информационной безопасности.

Под ***системой защиты информации в КС*** понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищённость информации в КС в соответствии с принятой политикой безопасности.

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Под ***угрозой безопасности информации*** понимается потенциально возможное событие, процесс или явление, которое может привести к уничтожению, утрате целостности, конфиденциальности или доступности информации.

случайные угрозы

- Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называются **случайными** или **непреднамеренными**. К случайным угрозам относятся: стихийные бедствия и аварии, сбои и отказы технических средств, ошибки при разработке АИС или КС, алгоритмические и программные ошибки, ошибки пользователей и обслуживающего персонала.

преднамеренные угрозы

- Угрозы, которые связаны со злоумышленными действиями людей, а эти действия носят не просто случайный характер, а, как правило, являются **непредсказуемыми**, называются **преднамеренными**. К преднамеренным угрозам относятся: традиционный или универсальный шпионаж и диверсии, несанкционированный доступ к информации, электромагнитные излучения и наводки, несанкционированная модификация структур, вредительские программы.

В качестве источников нежелательного воздействия на информационные ресурсы по-прежнему актуальны **методы и средства шпионажа и диверсий**,.

К методам шпионажа и диверсий

- **Подслушивание**
- **Визуальное наблюдение**
- **Хищение документов и машинных носителей информации**
- **Хищение программ и атрибутов систем защиты**
- **Подкуп и шантаж сотрудников**
- **Сбор и анализ отходов машинных носителей информации**
- **Вооруженные нападения диверсионных или террористических групп**

Несанкционированный доступ к информации – это нарушение правил разграничения доступа с использованием штатных средств вычислительной техники или автоматизированных систем.

Несанкционированный доступ возможен:

- при отсутствии системы разграничения доступа;
- при сбое или отказе в компьютерных системах;
- при ошибочных действиях пользователей или обслуживающего персонала компьютерных систем;
- при ошибках в системе распределения доступа;
- при фальсификации полномочий.

Большую угрозу безопасности информации в компьютерных системах представляет несанкционированная модификация *алгоритмической, программной и технической структуры системы* (вирусные программы).

Методы защиты информации

Защита информации в компьютерных системах обеспечивается созданием **комплексной системы защиты**.

Комплексная система защиты включает:

- правовые методы защиты;
- организационные методы защиты;
- методы защиты от случайных угроз;
- методы защиты от традиционного шпионажа и диверсий;
- методы защиты от электромагнитных излучений и наводок;
- методы защиты от несанкционированного доступа;
- криптографические методы защиты;
- методы защиты от компьютерных вирусов.

Среди методов защиты имеются и универсальные, которые являются **базовыми** при создании любой системы защиты.

Методы защиты от случайных угроз разрабатываются и внедряются на этапах проектирования, создания, внедрения и эксплуатации компьютерных систем.

К их числу относятся:

- создание высокой надёжности компьютерных систем;
- создание отказоустойчивых компьютерных систем;
- блокировка ошибочных операций;
- оптимизация взаимодействия пользователей и обслуживающего персонала с компьютерной системой;
- минимизация ущерба от аварий и стихийных бедствий;
- дублирование информации.

При **защите информации в компьютерных системах от традиционного шпионажа и диверсий** используются те же средства и методы защиты, что и для защиты других объектов, на которых не используются компьютерные системы.

К их числу относятся:

- создание системы охраны объекта;
- организация работ с конфиденциальными информационными ресурсами;
- противодействие наблюдению и подслушиванию;
- защита от злоумышленных действий персонала.

Все **методы защиты от электромагнитных излучений и наводок** можно разделить:

1) **Пассивные методы** обеспечивают уменьшение уровня опасного сигнала или снижение информативности сигналов.
2) **Активные методы** защиты направлены на создание помех в каналах побочных электромагнитных излучений и наводок, затрудняющих приём и выделение полезной информации из перехваченных злоумышленником сигналов.

Для защиты **информации от несанкционированного доступа** создаются:

- система разграничения доступа к информации;
- система защиты от исследования и копирования программных средств.

Исходной информацией для создания системы разграничения доступа является решение администратора компьютерной системы о допуске пользователей к определённым информационным ресурсам. Так как информация в компьютерных системах хранится, обрабатывается и передаётся файлами (частями файлов), то доступ к информации регламентируется на уровне файлов.

Различают следующие операции с файлами: чтение (R); запись; выполнение программ (E).

Операции записи имеют две модификации: субъекту доступа может быть дано право осуществлять запись с изменением содержимого файла (W); разрешение дописывания в файл без изменения старого содержимого (A).

Система защиты от исследования и копирования программных средств включает следующие методы: методы, затрудняющие считывание скопированной информации; методы, препятствующие использованию информации.

Под **криптографической защитой информации** понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий.

По виду воздействия на исходную информацию методы криптографического преобразования информации разделяются на следующие группы:

- шифрование;
- стенография;
- кодирование;
- сжатие.

Вредительские программы и, прежде всего, вирусы представляют очень серьёзную опасность для информации в компьютерных системах. Знание механизмов действия вирусов, методов и средств борьбы с ними позволяет эффективно организовать противодействие вирусам, свести к минимуму вероятность заражения и потерь от их воздействия.

Компьютерные вирусы - это небольшие исполняемые или интерпретируемые программы, обладающие свойством распространения и самовоспроизведения в компьютерных системах. Вирусы могут выполнять изменение или уничтожение программного обеспечения или данных, хранящихся в компьютерных системах. В процессе распространения вирусы могут себя модифицировать.

Профилактика заражения вирусами компьютерных систем

Правило первое. Обязательное использование программных продуктов, полученных законным путём. Так как в пиратских копиях вероятность наличия вирусов во много раз выше, чем в официально полученном программном обеспечении.

Правило второе. Дублирование информации, то есть создавать копии рабочих файлов на съёмных носителях информации (дискеты, компакт-диски и другие) с защитой от записи.

Правило третье. Регулярно использовать антивирусные средства, то есть перед началом работы выполнять программы-сканеры и программы-ревизоры (Aidstest и Adinf). Эти антивирусные средства необходимо регулярно обновлять.

Правило четвертое. Проявлять особую осторожность при использовании новых съёмных носителей информации и новых файлов.

Правило пятое. При работе в системах коллективного пользования необходимо новые сменные носители информации и вводимые в систему файлы проверять на специально выделенных для этой цели ЭВМ.

Правило шестое. Если не предполагается осуществлять запись информации на носитель, то необходимо заблокировать выполнение этой операции.

Порядок действий пользователя при обнаружении заражения вирусами компьютерной системы

О наличии вирусов можно судить по следующим событиям:

- появление сообщений антивирусных средств о заражении или о предполагаемом заражении;
- явные проявления присутствия вирусов (сообщения, выдаваемые на монитор или принтер, звуковые эффекты, уничтожение файлов и другие);
- неявные проявления заражения, которые могут быть вызваны сбоями или отказами аппаратных и программных средств, “зависаниями” системы, замедлением выполнения определённых действий, нарушением адресации, сбоями устройств и другими проявлениями.

Если **заражение действительно произошло**, тогда пользователю следует выполнить следующую последовательность действий:

- выключить ЭВМ для уничтожения резидентных вирусов;
- осуществить загрузку эталонной операционной системы со сменного носителя информации, в которой отсутствуют вирусы;
- сохранить на сменных носителях информации важные файлы, которые не имеют резидентных копий;
- использовать антивирусные средства для удаления вирусов и восстановления файлов, областей памяти. Если работоспособность компьютерной системы восстановлена, то завершить восстановление информации всесторонней проверкой компьютерной системы с помощью всех имеющихся в распоряжении пользователя антивирусных средств. Иначе продолжить выполнение антивирусных действий;

- осуществить полное стирание и разметку (форматирование) несъёмных внешних запоминающих устройств. В персональных компьютерах для этого могут быть использованы программы MS-DOS FDISK и FORMAT. Программа форматирования FORMAT не удаляет главную загрузочную запись на жёстком диске, в которой может находиться загрузочный вирус. Поэтому необходимо выполнить программу FDISKс недокументированным параметром MBR, создать с помощью этой же программы разделы и логические диски на жёстком диске. Затем выполняется программа FORMAT для всех логических дисков;
- восстановить операционную систему, другие программные системы и файлы с резервных копий, созданных до заражения;
- тщательно проверить файлы, сохранённые после обнаружения заражения, и, при необходимости, удалить вирусы и восстановить файлы;
- завершить восстановление информации всесторонней проверкой компьютерной системы с помощью всех имеющихся в распоряжении пользователя антивирусных средств.

Особенности защиты информации в базах данных

Базы данных рассматриваются как надёжное хранилище структурированных данных, снабжённое специальным механизмом для их эффективного использования в интересах пользователей (процессов). Таким механизмом является **система управления базами данных (СУБД)**. Под ***системой управления базами данных*** понимается программные или аппаратно-программные средства, реализующие функции управления данными, такие как: просмотр, сортировка, выборка, модификация, выполнение операций определения статистических характеристик и другие.

Базы данных размещаются:

- на компьютерной системе пользователя;
- на специально выделенной ЭВМ (сервере).

Особенности защиты информации в базах данных:

- необходимость учёта функционирования СУБД при выборе механизмов защиты;
- разграничение доступа к информации реализуется не на уровне файлов, а на уровне частей баз данных.

При создании средств защиты информации в базах данных необходимо учитывать взаимодействие этих средств не только с операционной системой, но с СУБД. При этом возможно встраивание механизмов защиты в СУБД или использование их в виде отдельных компонент. Для большинства СУБД придание им дополнительных функций возможно только на этапе их разработки. В эксплуатируемые системы управления базами данных дополнительные компоненты могут быть внесены путём расширения или модификации языка управления.