ЛЕКЦІЯ №7

Тема: ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

ПЛАН

7.1 Інформаційна безпека та її складові
7.2 Погрози безпеки інформації в комерційних системах
7.3 Методи захисту інформації

Час: 2 год.

7.1 Інформаційна безпека та її складові

С технологической точки зрения информация является продукцией информационных систем. Как и для всякого продукта, для информации большое значение имеет её качество, то есть способность удовлетворять определённые информационные потребности.

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).

Своевременность информации оценивается временем выдачи (получения), в течение которого информация не потеряла свою актуальность.

Актуальность информации – это степень её соответствия текущему моменту времени. Нередко с актуальностью связывают коммерческую ценность информации. Устаревшая и потерявшая свою актуальность информация может приводить к ошибочным решениям и тем самым теряет свою практическую ценность.

Полнота информации определяет достаточность данных для принятия решений или для создания новых данных на основе имеющихся. Чем полнее данные, тем проще подобрать метод, вносящий минимум погрешностей в ход информационного процесса.

Достоверность информации – это степень соответствия между получаемой и исходящей информацией.

Адекватность информации – это степень соответствия реальному объективному состоянию дела. Неадекватная информация может образовываться при создании новой информации на основе неполных или недостаточных данных. Однако и полные, и достоверные данные могут приводить к созданию неадекватной информации в случае применения к ним неадекватных методов.

Доступность информации – мера возможности получить ту или иную информацию. Отсутствие доступа к данным или отсутствие адекватных методов обработки данных приводят к одинаковому результату: информация оказывается недоступной.

Одним из наиболее существенных показателей качества информации является её безопасность.

В качестве предмета защиты рассматривается информация, хранящаяся, обрабатываемая и передаваемая в компьютерных системах. 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.

Понятие компьютерные системы (КС) охватывает следующие системы:

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

Информация доступна человеку, если она содержится на материальном носителе. Поэтому необходимо защищать материальные носители информации, так как с помощью материальных средств можно защищать только материальные объекты.

Информация имеет ценность, которая определяется степенью её полезности для владельца. В свою очередь степень полезности информации зависит от её истинности или достоверности. Истинной информацией является та, которая с достаточной точностью отражает объекты и процессы окружающего мира в определённых временных и пространственных рамках. Если информация искажена, то она является дезинформацией. Если к информации ограничен доступ, то такая информация является конфиденциальной. Такая информация может содержать государственную или коммерческую тайну.

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. Этот документ разрабатывается и принимается как официальный руководящий документ высшими органами управления государством, ведомством, организацией. На основе этого документа создаётся комплексная система защиты информации на уровне соответствующей структуры (государства, отрасли, ведомства, учреждения).

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.

7.2 Погрози безпеки інформації в комерційних системах

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

Всё множество потенциальных угроз безопасности информации в автоматизированных информационных системах (АИС) или в компьютерных системах (КС) может быть разделено на два класса: случайные угрозы и преднамеренные 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.

Реализация угроз этого класса приводит к наибольшим потерям информации (по статистическим данным – до 80% от ущерба, наносимого информационным ресурсам КС любыми угрозами). При этом может происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию. Согласно тем же статистическим данным только в результате ошибок пользователей и обслуживающего персонала происходит до 65% случаев нарушения безопасности информации.

Следует отметить, что механизм реализации случайных угроз изучен достаточно хорошо и накоплен значительный опыт противодействия этим угрозам. Современная технология разработки технических и программных средств, эффективная система эксплуатации автоматизированных информационных систем, включающая обязательное резервирование информации, позволяют значительно снизить потери от реализации угроз этого класса.

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 относятся: 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, поджоги, взрывы, 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.

Процесс обработки и передачи информации техническими средствами компьютерных систем сопровождается электромагнитными излучениями в окружающее пространство и наведением электрических сигналов в линиях связи, сигнализации, заземлении и других проводниках. Всё это получило название: ”побочные электромагнитные излучения и наводки” (ПЭМИН). Электромагнитные излучения и наводки могут быть использованы злоумышленниками, как для получения информации, так и для её уничтожения.

Большую угрозу безопасности информации в компьютерных системах представляет несанкционированная модификация алгоритмической, программной и технической структуры системы.

Одним из основных источников угроз безопасности информации в КС является использование специальных программ, получивших название “вредительские программы”.

В зависимости от механизма действия вредительские программы делятся на четыре класса:

- “логические бомбы”;
- “черви”;
- “троянские кони”;
- “компьютерные вирусы”.

Логические бомбы – это программы или их части, постоянно находящиеся в ЭВМ или вычислительных систем (КС) и выполняемые только при соблюдении определённых условий. Примерами таких условий могут быть: наступление заданной даты, переход КС в определённый режим работы, наступление некоторых событий заданное число раз и тому подобное.

Черви – это программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в вычислительных системах (ВС) или в сети и самовоспроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и блокировке системы.

Троянские кони – это программы, полученные путём явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.

Компьютерные вирусы – это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путём создания своих копий, а при выполнении определённых условий оказывают негативное воздействие на КС.

7.3 Методи захисту інформації

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. Это, прежде всего, правовые методы защиты информации, которые служат основой легитимного построения и использования системы защиты любого назначения. К числу универсальных методов можно отнести и организационные методы, которые используются в любой системе защиты без исключений и, как правило, обеспечивают защиту от нескольких угроз.

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 на пассивные и активные. Пассивные методы обеспечивают уменьшение уровня опасного сигнала или снижение информативности сигналов. Активные методы защиты направлены на создание помех в каналах побочных электромагнитных излучений и наводок, затрудняющих приём и выделение полезной информации из перехваченных злоумышленником сигналов. На электронные блоки и магнитные запоминающие устройства могут воздействовать мощные внешние электромагнитные импульсы и высокочастотные излучения. Эти воздействия могут приводить к неисправности электронных блоков и стирать информацию с магнитных носителей информации. Для блокирования угрозы такого воздействия используется экранирование защищаемых средств.

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. В базах данных доступ может регламентироваться к отдельным её частям по определённым правилам. При определении полномочий доступа администратор устанавливает операции, которые разрешено выполнять пользователю. 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.

Вопросы для самоконтроля

1. Базовая система показателей качества информации.
2. Особенности информации, хранящейся, обрабатываемой и передаваемой в компьютерных системах.
3. Степени секретности государственной тайны.
4. Категории секретности коммерческой тайны.
5. Классы угроз безопасности информации.
6. Классы вредительских программ.
7. Основные правовые документы, регулирующие вопросы защиты информации в компьютерных системах