

1. Модель защищенной информационной системы

Проблема защиты информации возникает, когда одновременно существуют информация и потребитель информации. В этом случае может существовать некто (или нечто), кто пытается вмешаться в процесс передачи информации от источника к потребителю, нарушить нормальный ход этого процесса, получить несанкционированный доступ к информации. Это - злоумышленник. Естественно, в такой ситуации должна существовать система или средства защиты. Поэтому можно предложить следующую упрощенную модель этого явления - назовем ее моделью защиты информации

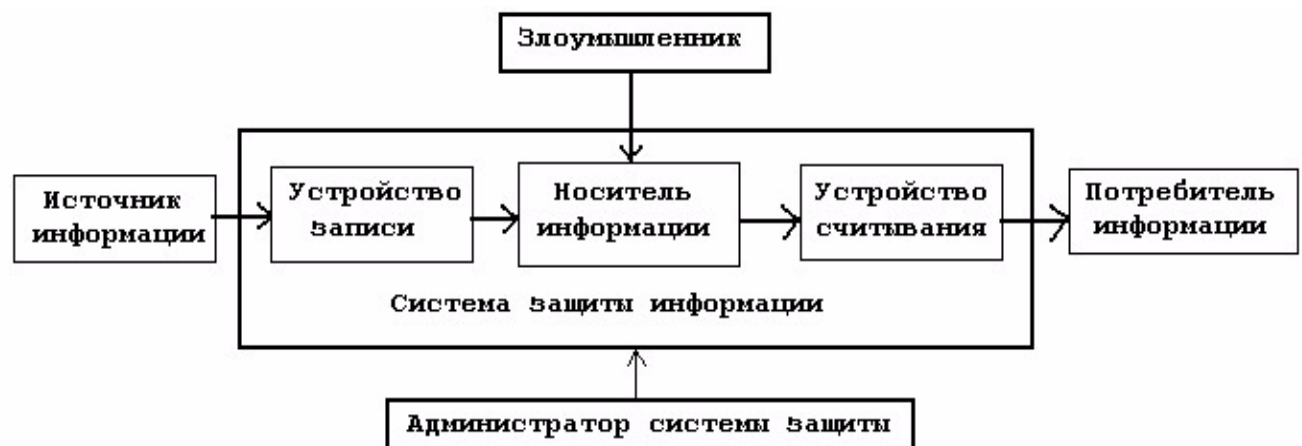


Рис. 1. Модель системы защиты информации.

Злоумышленник может воздействовать и на источник информации, на носитель, на процесс передачи информации на потребителя информации. Нельзя выпускать из внимания систему защиты и другие устройства и процессы, позволяющие злоумышленнику нанести вред информации. Заметим, что злоумышленником может быть источник информации (такая ситуация называется подлогом), либо потребитель.

Средства защиты должны отслеживать и оберегать все элементы и процессы на пути информации от источника к потребителю.

Кроме того, защита должна выполняться различными средствами: программными, аппаратными, программно-аппаратными и по всем направлениям: **правовая, организационная, инженерно-техническая защита.**

В процессе хранения и передачи информационные ресурсы (в нашем случае, документы) подвержены некоторым опасностям, как принято говорить, угрозам. В некоторых литературных источниках под угрозами понимают конкретные события, приводящие к искажению, хищению, уничтожению информации (например, угрозами называются отказы технических устройств, ошибки операторов или программистов, действия хакеров или вирусов). Мы же будем выделять только 5 видов угроз, определяемых *воздействием* на защищаемую информацию и *последствиями*, к которым приводит *реализация* той или иной угрозы. В этом смысле можно выделить следующие основные типы угроз для документов: **уничтожение документов, отказы систем обработки документов, хищение документов, искажение** (подмена, подделка) **документов**, отрицание факта создания **документов**, отрицание факта получения **документов**

А те события, которые приводят к реализации перечисленных угроз, называются источниками угроз. Условно можно выделить три источника угроз:

- природные явления (стихийные бедствия, радиоактивные излучения, магнитные бури и т.п.);
- технические (отказы аппаратуры, отключение электропитания и т.п.);
- люди (ошибочные или преднамеренные действия).

Однако такое понимание источников угроз мало может помочь в работе по защите информации. Для разработки мер защиты информации необходимы полные перечни источников угроз.

Основные задачи и принципы построения защищенных информационных систем

Если сформулировать кратко, то задача обеспечения информационной безопасности состоит в устранении любой возможности реализации перечисленных выше угроз или устранения всех источников угроз.

Решение этой задачи можно конкретизировать в виде следующих подзадач, которые можно также рассматривать как основные требования к любой защищенной информационной системе:

1. *Целостность.* Система хранения, обработки и передачи информации должна обеспечивать сохранность и целостность информации, то есть не возможность полного или частичного уничтожения информации.

2. *Доступность.* Должна быть обеспечена доступность информации для легальных пользователей: своевременный и беспрепятственный доступ субъектов к интересующей их информации, готовность в любой момент времени, соответствующих средств, к обслуживанию поступающих от субъектов запросов.

3. *Достоверность.* Должна быть обеспечена достоверность информации. Мы будем понимать под достоверностью информации ее существование в неискаженном, неизменном по отношению к некоторому начальному состоянию виде.

4. *Конфиденциальность.* Должна быть обеспечена конфиденциальность информации - субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации. Это свойство обеспечивается системой, которая сохраняет указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней.

5. *Аутентификация источника.* В системе документооборота в качестве источника может выступать документ, подразделение, база данных, процесс и т.п. аутентификация – это подтверждение подлинности перечисленных источников.

6. *Протоколируемость*. Задача протоколирования всех процессов, происходящих в системе.

Как видим, каждая из задач защиты информации фактически является задачей отражения определенной угрозы.

А теперь сформулируем несколько основных принципов, которых необходимо придерживаться на любом этапе работ по проектированию защиты информационной системы.

Принципы построения защищенной информационной системы

Защита информации в системах должна строиться на основе следующих принципов:

- системности;
- комплексности;
- непрерывности защиты;
- разумной достаточности;
- гибкости управления и применения;
- открытости алгоритмов и механизмов защиты;
- простоты применения защитных мер и средств.

Приведем краткие характеристики этих принципов.

Принцип системности. Системный подход к защите информационных систем предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, процессов, условий и факторов окружающих систем.

Принцип комплексности. В распоряжении специалистов по компьютерной безопасности имеется широкий спектр мер, методов и средств защиты компьютерных систем. Комплексное их использование предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающих все существенные каналы реализации угроз. Защита должна вестись по всем направлениям и всеми возможными способами и средствами. Защита должна строиться эшелонировано. Внешняя

защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одной из наиболее укрепленных линий защиты, должна быть операционная система. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж обороны.

Принцип непрерывности защиты. Защита информации - это не разовое мероприятие и даже не определенная совокупность мероприятий и средств защиты, а непрерывный, целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационной системы, начиная с самых ранних стадий проектирования, а не только на этапе её эксплуатации. Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка. Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных “закладок” и других средств преодоления системы защиты.

Принцип разумной достаточности. Принцип разумной достаточности заключается в том, что расходы на предотвращение некоторой угрозы не должны превосходить возможного ущерба от реализации угрозы. Создать абсолютно непреодолимую систему защиты в принципе невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту. Поэтому всегда имеет смысл вести разговор только о некотором приемлемом уровне безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности и ресурсов компьютерной системы и может создать ощутимые неудобства пользователям. Поэтому очень важно выбрать тот приемлемый уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Принцип гибкости управления и применения. Системы защиты на практике чаще всего создаются в условиях большой неопределенности. Поэтому принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Естественно, что для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса её нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких условиях свойство гибкости спасает владельцев от необходимости принятия кардинальных мер по полной замене существующих средств защиты на новые.

Принцип открытости алгоритмов и механизмов защиты. Суть этого принципа состоит в том, что защита не должна обеспечиваться только за счет секретности структуры организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности взломать её даже автору. Однако это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна.

Принцип простоты применения защитных мер и средств. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Механизмы защиты не должны требовать от пользователя выполнения рутинных, малопонятных ему операций, раздражающих действий, чтобы не вызвать ответную, негативную реакцию от пользователя.