Глава 1

Многие слышали словосочетание «Информационная безопасность», но не все понимают, что это словосочетание обозначает. «Информационная безопасность» — это процесс обеспечения доступности (обеспечение доступа к информации), целостности (обеспечение достоверности и полноты информации) и конфиденциальности (обеспечение доступа к информации только авторизованным пользователям) информации. Чтобы найти необходимые и оптимальные средства защиты информации, нужно знать виды угроз информационной безопасности.

Компоненты, на которые угрозы нацелены:

1. Данные
2. Программы
3. Аппаратура
4. Поддерживающая инфраструктура

К основным угрозам **доступности** можно отнести:

1. Внутренний отказ информационной системы;
2. Отказ поддерживающей инфраструктуры.

Основными источниками внутренних отказов являются:

1. Нарушение (случайное или умышленное) от установленных правил эксплуатации
2. Выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.)
3. Ошибки при (пере) конфигурировании системы
4. Вредоносное программное обеспечение
5. Отказы программного и аппаратного обеспечения
6. Разрушение данных
7. Разрушение или повреждение аппаратуры

К основным угрозам **целостности** можно отнести:

1. Угрозы статической целостности (злоумышленник может ввести неверные данные, изменить данные).
2. Угрозы динамической целостности (кража, дублирование данных).

К основным угрозам **конфиденциальности** можно отнести:

1. Злоупотребление полномочиями
2. Нанесение ущерба при сервисном обслуживании

Принимая все вышесказанное во внимание, можно приступить к выбору *средств защиты* информации.

*Средства защиты* информации принято делить: неформальные и формальные.

**Неформальными средствами защиты информации** – являются *законодательные, административные и морально-этические**средства*, к которым можно отнести: документы, правила, мероприятия.

* *Законодательные средства* информационной безопасности обеспечивает государство. Защита информации регулируется международными конвенциями, Конституцией, всевозможными разными федеральными законами и различными подзаконными актами. Также государство определят меру ответственности за нарушение положений законодательства в сфере информационной безопасности.
* *Административные мероприятия* играют огромную и очень важную роль в создании механизма защиты данных. Злоумышленник может действовать благодаря небрежности, халатности пользователей или охранников – персонала защиты. Чтобы предотвратить халатность пользователей, необходимы мероприятия, которые исключали бы или намного уменьшали возможность проникновения угрозы. Например: архитектурные и планировочные решения, которые позволяют защитить переговорные комнаты от утечки информации.
* *К морально-этическим средствам* можно отнести сложившиеся в обществе или данном коллективе моральные, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе. Грубо говоря, человек сам должен понимать, какую информацию ему можно рассказать, а какую нет. Не соблюдение этих правил не несет никакой ответственности, но, рассказав информацию, ты можешь подорвать свой статус или авторитет в обществе.

**Формальные средства защиты информации** – это специальные технические средства и программное обеспечение, которые можно разделить на *физические, аппаратные, программные и криптографические.*

* К *физическим средствам защиты информации* относятся: замки, жалюзи и занавески. Также это камеры и всевозможные видеорегистраторы.
* К *аппаратным средствам защиты информации* относятся: генераторы шума, сетевые фильтры и другие устройства, которые встраиваются в информационные системы.
* *Программные средства защиты информации*– это простые и комплексные программы, предназначенные для решения задач, связанных с обеспечением информационной безопасности. Примером комплексных решений служат DLP-системы и SIEM-системы. **DLP-системы** («*Data Leak Prevention*» дословно «предотвращение утечки данных») соответственно служат для предотвращения утечки, переформатирования информации и перенаправления информационных потоков. **SIEM-системы** («*Security Information and Event Management*», что в переводе означает «Управление событиями и информационной безопасностью») обеспечивают анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений. SIEM представлено приложениями, приборами или услугами, и используется также для и генерации отчетов в целях совместимости с прочими бизнес данными. Программные средства требовательны к мощности аппаратных устройств, и при установке необходимо предусмотреть дополнительные резервы.
* *Криптографический метод защиты информации* - внедрение криптографических методов защиты данных для безопасной передачи по сети. Криптография считается одним из самых надежных способов защиты данных, ведь она охраняет саму информацию, а не доступ к ней. Внедрение криптографической защиты информации предусматривает создание программно-аппаратного комплекса, архитектура и состав которого определяется, исходя из потребностей конкретного заказчика, требований законодательства, поставленных задач и необходимых методов, и алгоритмов шифрования.