1. ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Основные понятия и определения в области информационной безопасности

Информация

- сведения (сообщения, данные) о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Компьютерная информация

- информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ.

Информационная среда общества

- совокупность информационных ресурсов, система формирования, распространения и использования информации.

Информационная инфраструктура

- совокупность центров обработки и анализа информации, каналов информационного обмена и телекоммуникации, линий связи, систем и средств защиты информации.

Из федерального закона «Об информации, информацонных технологиях и о защите информации» от 27 июля 2006 года

- информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
- обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- доступ к информации - возможность получения информации и ее использования;

Из федерального закона «Об информации, информацонных технологиях и о защите информации» от 27 июля 2006 года

- предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
- распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
- электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
- документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
- оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Информационная безопасность

- состояние защищенности информационной среды общества, обеспечивающее ее формирование и развитие в интересах граждан, организаций и государства.

Угрозы информационной безопасности

- совокупность факторов, создающих опасность функционированию и развитию информационной среды общества.

Несанкционированный (неправомерный) доступ к информации

- это доступ к информации, нарушающий установленные правила ее получения.

Безопасность информации (данных)

- состояние защищенности информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

конфиденциальность — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

целостность — исключение возможности несанкционированной модификации информации;

доступность — исключение возможности временного или постоянного сокрытия информации от пользователей, получивших права доступа;

неотказуемость **неотказуемость или апеллируемость** — невозможность отказа от авторства;

подотчётность — обеспечение идентификации субъекта доступа и регистрации его действий;

достоверность — свойство соответствия предусмотренному поведению или результату;

аутентичность **аутентичность или подлинность** — свойство, гарантирующее, что субъект или ресурс

Из федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года

Защита информации

- это принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2) соблюдение конфиденциальности информации ограниченного доступа;
3) реализацию права на доступ к информации.

Ценная информация, которую необходимо охранять:

- государственная;
- военная;
- техническая;
- коммерческая;
- финансовая;
- юридическая
- и т.д.

Из федерального закона «Об информации, информацонных технологиях и о защите информации» от 27 июля 2006 года

Обладатель информации, оператор информационной системы обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
2) своевременное обнаружение фактов несанкционированного доступа к информации;
3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6) постоянный контроль за обеспечением уровня защищенности информации.

1.2. Информационная безопасность в России

Государственные органы РФ, контролирующие деятельность в области защиты информации:

- Комитет Государственной думы по безопасности;
- Совет безопасности России;
- Федеральная служба по техническому и экспортному контролю (ФСТЭК);
- Федеральная служба безопасности Российской Федерации (ФСБ России);
- Министерство внутренних дел Российской Федерации (МВД России);
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Основы нормативно-правового регулирования информационной безопасности

1. Акты федерального законодательства:
   - Международные договоры РФ;
   - Конституция РФ;
   - Законы федерального уровня (включая федеральные конституционные законы, кодексы);
   - Указы Президента РФ;
   - Постановления правительства РФ;
   - Нормативные правовые акты федеральных министерств и ведомств;
   - Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

Основы нормативно-правового регулирования информационной безопасности

2. Методические документы государственных органов России:

- Доктрина информационной безопасности РФ;
- Руководящие документы ФСТЭК (Гостехкомиссии России);
- Приказы ФСБ;
- Лицензии;
- Сертификаты.

Основы нормативно-правового регулирования информационной безопасности

3. Стандарты информационной безопасности, из которых выделяют:

- Международные стандарты;
- Государственные (национальные) стандарты РФ (ГОСТы);
- Отраслевые стандарты (ОСТы);
- Рекомендации по стандартизации.

Законодательство РФ в сфере защиты информации и охраны прав интеллектуальной собственности

- Федеральный закон № 149-ФЗ «Об информации, информацонных технологиях и о защите информации» от 27 июля 2006 года;
- Федеральный закон № 152-ФЗ «О персональных данных» от 27 июля 2006 года;

Законодательство РФ в сфере защиты информации и охраны прав интеллектуальной собственности

- **Уголовный кодекс РФ** (Глава 28. Преступления в сфере компьютерной информации);
  - Статья 272. Неправомерный доступ к компьютерной информации
  - Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ
  - Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

Законодательство РФ в сфере защиты информации и охраны прав интеллектуальной собственности

- **Конституция РФ** (ст. 44)

  1. Каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом.

- **Гражданский кодекс РФ**
  - Часть 4 раздел VII. Права на результаты интеллектуальной деятельности и средства индивидуализации

1.3. Источники угроз информационной безопасности и их классификация

Внешние источники угроз информационной безопасности :

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- недружественная политика иностранных государств в области глобального информационного мониторинга, распространения информации и новых информационных технологий;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

Внешние источники угроз информационной безопасности :

- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- преступные действия международных групп, формирований и отдельных лиц;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность иностранных разведывательных и специальных служб;

Внешние источники угроз информационной безопасности :

- воздействие космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.
- стихийные бедствия и катастрофы.

Внутренние источники угроз информационной безопасности :

- критическое состояние отечественных отраслей промышленности;
- противозаконная деятельность политических и экономических структур в области формирования, распространения и использования информации;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищённости законных интересов граждан, общества и государства в информационной сфере;

Внутренние источники угроз информационной безопасности :

- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

Внутренние источники угроз информационной безопасности :

- неправомерные действия государственных структур, приводящие к нарушению законных прав граждан и организаций в информационной сфере;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

Внутренние источники угроз информационной безопасности :

- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Информационные способы воздействия:

- нарушения установленных регламентов сбора, обработки и передачи информации;
- нарушения адресности и своевременности информационного обмена, противозаконный сбор и использование информации;
- несанкционированный доступ к информационным ресурсам;
- незаконное копирование данных в информационных системах;
- использование средств массовой информации с позиций, противоречащих интересам граждан, организаций и государства;
- хищение информации из библиотек, архивов, банков и баз данных;
- преднамеренные действия и непреднамеренные ошибки персонала информационных систем.

Программно-математические способы воздействия:

- внедрение программ-вирусов;
- установку программных и аппаратных закладных устройств;
- сбои программного обеспечения в информационных и телекоммуникационных системах.
- уничтожение или модификацию данных в информационных системах.

Физические способы воздействия:

- отказы технических средств в информационных и телекоммуникационных системах.
- уничтожение или разрушение средств обработки информации и связи;
- уничтожение, разрушение или хищение машинных или других оригиналов носителей информации;
- хищение программных или аппаратных ключей и средств криптографической защиты информации;
- воздействие на персонал;
- поставку «зараженных» компонентов информационных систем.

Радиоэлектронные способы воздействия:

- перехват информации в технических каналах ее утечки;
- внедрение электронных устройств перехвата информации в технических средствах и помещениях;
- перехват, дешифрование и навязывание ложной информации в сетях передачи данных и линиях связи;
- воздействие на парольно-ключевые системы;
- радиоэлектронное подавление линий связи и систем управления.

Организационно-правовые способы воздействия:

- закупки несовершенных или устаревших информационных технологий и средств информатизации;
- невыполнение требований законодательства и задержки в принятии необходимых нормативно-правовых положений в информационной сфере;
- неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.

Категории злоумышленников:

- случайные любопытные пользователи, не применяющие специальных технических средств;
- члены организации, занимающиеся компьютерным хулиганством;
- преступники, которые совершают попытки личного обогащения;
- профессионалы, занимающиеся коммерческим и военным шпионажем.

Айрэ Винклер

Взломщик

Причины случайной потери данных:

- ***Форс-мажор***: пожары, наводнения, землетрясения, войны, восстания, крысы, изгрызшие ленты, насекомые, замкнувшие контакты микросхем и т.д.
- ***Аппаратные и программные ошибки***: сбои центрального процессора, нечитаемые диски или ленты, ошибки при передаче данных, ошибки в программах и т.д.
- ***Человеческий фактор***: неправильный ввод данных, неверные установленные диск или лента, запуск не той программы, случайное повреждение носителей информации или устройств компьютера, потерянные диск или лента и т.д.

1.4. Основные мероприятия по обеспечению информационной безопасности

Ответственность за выполнение мер защиты лежит не только на собственнике, но и на пользователе информации

Комплекс мероприятий по обеспечению информационной безопасности объектов электронно-вычислительной техники:

- организационно-административные мероприятия;
- технические мероприятия и методы;
- программные методы.

1.4.1. Организационно-административные мероприятия по обеспечению защиты информации

Политика безопасности

- совокупность документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов.

Направления организационно-административных мероприятий:

- физическая защита информации;
- управление персоналом, имеющим доступ к системам, в том числе его обучение и практическая подготовка;
- реагирование на нарушения информационной безопасности.

Организационно-административные мероприятия:

- привлечение к проведению работ по защите информации организаций, имеющих лицензию на деятельность в области защиты информации, выданную соответствующими органами;
- категорирование и аттестация объектов ТСПИ и выделенных для проведения закрытых мероприятий помещений;
- использование на объекте сертифицированных ТСПИ и ВТСС;
- установление контролируемой зоны вокруг объекта;
- организация контроля и ограничение доступа на объекты ТСПИ и в выделенные помещения;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- отключение на период закрытых мероприятий технических средств, имеющих элементы, выполняющие роль электроакустических преобразователей, от линий связи и т.д.

1.4.2. Технические мероприятия и методы по обеспечению защиты информации

Технические средства обеспечения защиты информации:

- аппаратные средства защиты компьютерных систем и систем передачи данных;
- аппаратура активной защиты от побочных электромагнитных излучений и наводок;
- аппаратура маскирования телефонных переговоров;
- средства выявления радиозакладных устройств;
- аппаратура защиты служебных помещений от акустического, виброакустического и оптического несанкционированного снятия информации.

1.4.3. Программные методы по обеспечению защиты информации

Главные задачи компьютерной системы по обеспечению информационной безопасности:

- конфиденциальность данных;
- целостность данных;
- доступность системы.

Защите подлежит только документированная информация

Документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

Государственные стандарты РФ в сфере защиты информации:

- ГОСТ 28147-89 «Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;
- ГОСТ Р 34.10-2001. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
- ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

Международной организацией по стандартизации (ISO) был разработан стандарт по компьютерной безопасности **ISO/IEC 15408, ИСО/МЭК 15408-2002 «Общие критерии оценки безопасности информационных технологий»** — (англ. Common Criteria for Information Technology Security Evaluation). Общеизвестным является более короткое название «Общие критерии» (Common Criteria, CC, или ОК).

Вывод:

Ценной становится та информация, обладание которой позволит ее существующему и потенциальному владельцам получить какой-либо выигрыш: материальный, политический, военный и т.д. Таким образом, проблемы информационной безопасности и защиты информации, циркулирующей в различных компьютерных информационно-телекоммуникационных системах, приобретают в настоящее время все большее значение.