**Лекция 1.**

**Понятие информации, информационного ресурса, информационной системы. Основные особенности информационной системы.**

1. Понятие информации
2. Понятие информационного ресурса, информационной системы
3. Основные особенности информационной системы
4. Понятие предмета и объекта защиты

Объектом защиты информации является компьютерная система или автоматизированная система обработки данных. И представляет собой **комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки и получения информации.**

Предметом защиты выступает информация. Наряду с термином «информация» применительно к КС часто используются такие термины как «данные» и «информационные ресурсы».

В соответствии с законом об информации, информатизации и защите информации» под **информационными ресурсами понимаются отдельные документы и отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и других информационных ресурсах).**

2. Понятие компьютерной системы

Понятие КС охватывает следующие понятия:

- ЭВМ всех классов и назначений;

- вычислительные комплексы и системы;

- вычислительные сети (глобальные, региональные, локальные)

Предметом защиты является информация.

***Материальной основой существования информации в КС являются электронные и электромеханические устройства, а также машинные носители.***

С помощью устройств ввода или систем передачи данных информация попадает в КС. В системе информация хранится в запоминающих устройствах различных уровней, преобразуется (обрабатывается) процессорами и выводится из системы с помощью устройств вывода или систем передачи данных. В качестве машинных носителей вступает бумага, диски, флешки.

Большинство типов машинных носителей являются сьемными и могут храниться отдельно от устройств.

Таким образом для защиты информации (обеспечения безопасности) информации в КС необходимо защищать устройства и машинные носители от несанкционированных воздействий от них.

Далее, КС обслуживаются специалистами (обслуживающим персоналом) в интересах пользователей, которые так же являются носителями информации, поэтому от несанкционированных воздействий необходимо защищать не только устройства и носители, но также обслуживающий персонал.

***Т.е. получается с позиции обеспечения безопасности такие системы рассматриваются как единство трех компонентов: информации, технических и программных средств и обслуживающего персонала.***

Обслуживающий персонал и **пользователи могут быть** как объектом, так и источником несанкционированного воздействия на информацию.

**Одними из основных понятий теории защиты информации являются понятия «безопасности информации», т.е. это такое состояние всех компонент компьютерной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне. Компьютерные системы, в которых обеспечивается безопасность информации, называются защищенными.**

Безопасность информации в КС является одним из основных направлений обеспечения безопасности государства, а также государственной организации или частной фирмы.

Информационная безопасность достигается проведением руководством соответствующего уровня политики информационной безопасности.

Основным документом такой политики является программа информационной безопасности. Этот документ разрабатывается и принимается как официальный руководящий документ высшими органами управления государством. В документе приводятся цели политики информационной безопасности и основные направления решения задач защиты информации в кс. В программах ИБ содержатся также общие требования и принципы построения систем защиты информации в КС.

3. Система защиты как комплекс правовых, организационных и других средств

Система защиты представляет комплекс правовых, организационных и технических , криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности.

При смене способа хранения информации с бумажного вида на цифровой, появился главный вопрос - как эту информацию защитить, ведь очень большое количество факторов влияет на сохранность конфиденциальных данных. Для того чтобы организовать безопасное хранение данных, первым делом нужно провести анализ угроз, для правильного проектирование схем информационной безопасности.

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

4. Общие понятия угроз информации

[Угрозы](http://click01.begun.ru/click.jsp?url=4vrJyDTR1jJVvk-mOwkg5OTmMVD4DXo*PdqbSTIIX7wXRd2M*l8LoIvOmPE*qTxYC1aZJpzDOsTLeJySlvd*DTIrKe0P08*zKx*6mPbiG1aaVgVP0fpd1lYp01yQ-tPnyE4Jyq2E0jmmxDzboIobfZbY-4GsQQeDZqt4xqQbwnymK63CVlcNEqV6VdvPChyIwDjfdap1THEzYMjZyDpgyRO9w6QasKqJomuGtI26W4U6CndIxWMxPikxq1eRoCYzjDL-KefWNQ0ViRmuwH-oqNcaP2tjYAV9fEzNF44e0P7vfoi4KwRnUtl071ncFyjBv88qpVd4ViZWjVy2WibR7FKyCWQrdzXarz9gYz0k44-0luSJDWmrJftrDNOFqtKvvTFk-*9blcyerLUoJKrsqpPDRnJ9tvs-VV82dAwmm3AAJOb96awa5Zhk3yaBLyoRrUPYB*ttqbeEZE8onpK3*kKxA4tntjx8bkz0EXLFKfhmnR5BhB7HTaEUv4LLv7VcDyusXs472hNvducQII2oluUJECnWe4dq44z-5f17jV0) информационной безопасности делятся на два основных типа - это случайные и преднамеренные угрозы.

К случайным угрозам относятся: стихийные бедствия и аварии, сбои и отказы технических средств, ошибки при разработке КС, алгоритмические и программные ошибки, ошибки пользователей и обслуживающего персонала.

**Остановимся на естественных угрозах** и попытаемся выделить основные из них. К естественным угрозам относятся пожары, наводнения, ураганы, удары молний и другие стихийные бедствия и явления, которые не зависят от человека. Наиболее частыми среди этих угроз являются пожары. Для обеспечения безопасности информации, необходимым условием является оборудование помещений, в которых находятся элементы системы (носители цифровых данных, серверы, архивы и пр.), противопожарными датчиками, назначение ответственных за противопожарную безопасность и наличие средств пожаротушения. Соблюдение всех этих правил позволит свести к минимуму угрозу потери информации от пожара.

Если помещения с носителями ценной информации располагаются в непосредственной близости от водоемов, то они подвержены угрозе потери информации вследствие наводнения. Единственное что можно предпринять в данной ситуации - это исключить хранение носителей информации на первых этажах здания, которые подвержены затоплению.

Еще одной естественной угрозой являются молнии. Очень часто при ударах молнии выходят из строя сетевые карты, электрические подстанции и другие устройства. Особенно ощутимые потери, при выходе сетевого оборудования из строя, несут крупные организации и предприятия, такие как банки. Во избежание подобных проблем необходимо соединительные [сетевые кабели](http://click01.begun.ru/click.jsp?url=4vrJyIr05AhvhHXcATMa3t7cC2rCN0AEB*ChcwgyZYZa98RJfmvJv77inU2TF*Wv-KFu0Ws0zTO7wC2NL9HkReKWCDwTwWw387ElYm1*dVE99sDtRJ*5WNinXdIecF1pRsCHRCMKXLcoSrJVLgSV8y1tF4*u4hLfRrqrGG2O-Tzma*2CFhdNUva2ooV-yEDwuECnDdINNAlLGLChsEIYsWvFu9xiyNLx2hP*zPXCI-1Ccg8wvRtJRlFJ0y-p2F5L9EqHUZ*uTXVt8WHWuAeQ0K9iRxMbGH0FBDS1b-ZmqIaXBvDAU3wfKqEMlyGkb1C5FpjZp48BCTQXfGFKKwvcoEttpxXL77LH476GE05Qi8MNSbWSasVY1gDlD4g*AO6LgMPbvvFwGOgXaYZn5lZjH0Nb*aRnkQcjzltj2fbAT8idRxqVmT9wmglqhKwdLUo5wx15NvV84LTuQPwmHW882dB6RvGr4GcmZ*UNVad9pK98ymRKapbK4A) были экранированы (экранированный сетевой кабель устойчив к электромагнитным помехам), а экран кабеля следует заземлить. Для предотвращения попадания молнии в электрические подстанции, следует устанавливать заземленный громоотвод, а компьютеры и серверы комплектовать источниками бесперебойного питания.

**Сбои и отказы сложных систем неизбежны**. Выходят из работы транзисторы, теристоры, процессоры, схемы, нарушается работоспособность технических средств, уничтожаются данные и программы, нарушается алгоритм работы устройств.

Нарушение алгоритмов работы отдельных узлов и устройств могут привести к нарушению конфиденциальности информации. Например, сбои и отказы средств выдачи информации могут привести к несанкционированному доступу к информации путем несанкционированной выдачи её в канал связи, на печатающее устройство.

**Ошибки при разработке КС алгоритмические и программные ошибки также приводят к сбою и отказу технических средств.**

Но 65% случаев нарушения безопасности информации происходит в результате **ошибок пользователей и обслуживающего персонала**. Это ошибки, которые совершают люди по неосторожности, незнанию, невнимательности или из любопытства. К такому типу относят установку программных продуктов, которые не входят в список необходимых для работы, и в последствии могут стать причиной нестабильной работы системы и как следствие потеря информации. Сюда же можно отнести и другие «эксперименты», которые не являлись злым умыслом, а люди, совершавшие их, не осознавали последствий. К сожалению, этот вид угроз очень трудно поддается контролю, мало того, чтобы персонал был квалифицирован, необходимо чтобы каждый человек осознавал риск, который возникает при его несанкционированных действиях.

**Обязательное резервирование информации позволяет значительно снизить потери от реализации угроз этого класса.**

**Вопросы:**

**1. Что представляет из себя объект защиты?**

**2. Что такое информационные ресурсы?**

**3. Что входит в понятие КС?**

**4. Что понимается под материальной основой существования информации?**

**5. Безопасность информации**

**6. Что такое угроза безопасности информации**

**7. Назовите виды случайных угроз.**

**8. В чем заключается анализ случайных угроз.**