Лекция 1
ИТСЗИ
ВВЕДЕНИЕ

Преподаватель

Ерофеева Ольга Геннадьевна

Значение информации в жизни любого цивилизованного общества непрерывно возрастает.

С незапамятных времен сведения, имеющие важное военно-стратегическое значение для государства, тщательно скрывались и защищались.

В настоящее время информация, относящаяся к *технологии производства* и сбыта продукции, стала рыночным товаром, имеющим большой спрос как на внутреннем так и на внешнем рынках.

Информационные технологии постоянно совершенствуются в направлении их

Развитие новых информационных технологий сопровождаются такими негативными явлениями, как **промышленный шпионаж, компьютерные преступления и несанкционированный доступ (НСД) к секретной и конфиденциальной информации.**

Поэтому защита информации является важнейшей государственной задачей в любой стране.

Острая необходимость в защите информации в России нашла выражение в создании *Государственной системы защиты информации* (ГСЗИ) и в развитии правовой базы информационной безопасности.

Приняты и введены в действие законы

«О государственной тайне», «Об информации, информатизации и защите информации»,

«О правовой охране программ для электронных вычислительных машин и баз данных», «Доктрина информационной безопасности Российской Федерации» и др.

Задачи систем защиты информации

Защита информации представляет собой комплекс целенаправленных мероприятий ее собственников по предотвращению утечки, искажения, уничтожения и модификации защищаемых сведений.

Под системой защиты информации можно понимать государственную систему защиты информации и систему защиты информации на конкретных объектах.

Государственная система защиты информации включает в себя:

- *систему государственных нормативных актов, стандартов, руководящих документов и требований;*
- *разработку концепций, требований, нормативно-технических документов и научно-методических рекомендаций по защите информации;*
- *порядок организации, функционирования и контроля за выполнением мер, направленных на защиту информации, являющейся собственностью государства, а также рекомендаций по защите информации, находящейся в собственности физических и юридических лиц;*
- *организацию испытаний и сертификации*

- *создание ведомственных и отраслевых координационных структур для защиты информации;*
- *осуществление контроля за выполнением работ по организации защиты информации;*
- *определение порядка доступа юридических и физических лиц иностранных государств к информации, являющейся собственностью государства, или к информации физических и юридических лиц, относительно распространения и использования которой*

Цели защиты информации от технических средств разведки на конкретных объектах информатизации определяются конкретным перечнем потенциальных угроз.

В общем случае **цели защиты информации** можно сформулировать как:

- *предотвращение утечки, хищения, утраты, искажения, подделки информации;*
- *предотвращение угроз безопасности личности, общества, государства;*
- *предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;*
- *предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;*

- *защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;*
- *сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;*
- *обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения*.

В целом ***средства обеспечения защиты*** **информации** в части предотвращения преднамеренных действий в зависимости от способа реализации **можно разделить на следующие** ***группы*****.**


КЛАССИФИКАЦИЯ
ИТС
по функциональному назначению
ФИЗИЧЕСКИЕ
Устройства, инженерные сооружения, затрудняющие или исключающие проникновение злоумышленников к источникам конфиденциальной информации
АППАРАТНЫЕ
Механические, электрические, электронные и др. устройства, предназначенные для защиты информации от утечки и разглашения и противодействия техническим средствам промышленного шпионажа
ПРОГРАММНЫЕ
Система специальных программ, включаемых в состав общего и специального обеспечения, реализующих функции защиты информации и сохранения целостности и конфиденциальности
КРИПТОГРАФИЧЕСКИЕ И стеганографические
Технические и программные средства шифрования и скрытия информации
КОМБИНИРОВАННЫЕ
Совокупная реализация аппаратных и программных средств, криптографических и стеганографических методов защиты информации

Технические (аппаратные) средства.

Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации.

Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки.

Первую часть *задачи решают замки, решетки на окнах, защитная сигнализация и* др.

Вторую –*генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, "перекрывающих" потенциальные каналы утечки информации* или позволяющих их обнаружить.

Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации.

Слабые стороны – недостаточная гибкость, относительно большие объем и масса, высокая

Программные средства *включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др.*

*Преимущества программных сре*дств – универсальность, гибкость, надежность, простота установки, способность к модификации и развитию.

Недостатки – ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Смешанные аппаратно-программные средства *реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства*.

Организационные средства *складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых* (национальные *законодательства и правила работы, устанавливаемые руководством конкретного предприятия).*

Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития.

Недостатки – высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

Организационные меры защиты – *меры организационного характера, предназначенные для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой.*

Среди *базовых организационных* мер по защите информации можно выделить следующее:

Формирование политики безопасности;

Регламентация доступа в помещения;

Регламентация допуска сотрудников к использованию ресурсов информационной системы и др.

Организационные меры сами по себе не могут решить задачу обеспечения безопасности.

Они *должны работать в комплексе с физическими и техническими средствами защиты информации* в части определения действий людей.

Физическая защита *представляет собой совокупность средств, препятствующих физическому проникновению потенциального злоумышленника в контролируемую зону.*

Ими могут быть механические, электро- или электронно-механические устройства различного типа.

Чаще всего, именно с построения физической защиты начинается обеспечение безопасности в организации, в том числе информационной.

Последним и самым обширным по своему составу эшелоном системы защиты является техническая защита информации.


Объекты защиты
информация
ресурсные объекты
физические объекты
пользовательские объекты
по форме представления:
▪ бумажные носители
▪ цифровые сигналы
▪ аналоговые сигналы
▪ виртуальная форма и т.п.
▪ аппаратное обеспечение
▪ программное обеспечение
▪ процессы и процедуры обработки информации
▪ территории
▪ помещения
▪ здания
▪ техническое оборудование
▪ средства и каналы связи и т.п.
▪ пользователи информации
▪ субъекты информации
▪ собственники и информации
▪ обслуживающий персонал