Лабораторное занятие № 1

Тема № 1. Российское законодательство по защите компьютерной информации. Компьютерные преступления

Цель занятия: закрепить знания о Российском законодательстве по защите компьютерной информации. Изучить компьютерные преступления.

Учебные вопросы

2.1.Основные понятия защиты компьютерной информации.

2.2.Компьютерные преступления и особенности их раскрытия.

2.3.Законодательство РФ в области информационной безопасности.

2.1.Основные понятия защиты компьютерной информации

Защита информации - это комплекс мероприятий, направленных на обеспечение информационной безопасности.

В качестве **предмета защиты** рассматривается информация, хранящаяся, обрабатываемая и передаваемая в компьютерных системах. Особенностями этой информации являются;

- двоичное представление информации внутри системы, не зависимо от физической сущности носителей исходной информации;
- высокая степень автоматизации обработки и передачи ин формации;
- концентрация большого количества информации в КС.

Объект защиты информации

Объектом защиты информации является компьютерная система или автоматизированная система обработки данных (АСОД). В работах, посвященных защите информации в автоматизированных системах, до последнего времени использовался термин АСОД, который все чаще заменяется термином КС. Что же понимается под этим термином?

Компьютерная система это комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации. Наряду с термином «информация» применительно к КС часто используют термин «данные».

Используется и другое понятие -«информационные ресурсы». В соответствии с законом РФ «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 системах).

Понятие КС очень широкое и оно охватывает следующие системы:

* ЭВМ всех классов и назначений;
* вычислительные комплексы и системы;

вычислительные сети (локальные, региональные и глобальные).

2.2.Компьютерные преступления и особенности их раскрытия

Уголовный кодекс Российской Федерации. Глава 28 - "Преступления в сфере компьютерной информации" - содержит три статьи:

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.

Первая имеет дело с посягательствами на конфиденциальность, вторая – с вредоносным ПО, третья - с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ. Включение в сферу действия УК РФ вопросов доступности информационных сервисов представ-1яется нам очень своевременным.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Интересы государства в плане обеспечения конфиденциальности деформации нашли наиболее полное выражение в Законе "О государственной тайне" (с изменениями и дополнениями от 6 октября 1997 года). В нём гостайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств зашиты информации. Согласно данному Закону, это технические,

криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации. Подчеркнем важность последней части определения.

2.3.Законодательство РФ в области информационной безопасности

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информационных технологиях и о защите информации" 2006 года. В нём даются основные определения и намечаются направления развития законодательства в данной области.

Вот некоторые из этих определений:

- **информация** — сведения о лицах, предметах, фактах, событиях, явлениях и процессах **независимо** от формы их представления;
- **документированная информация (документ) –** зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- **информационные процессы** — процессы сбора, обработки, накопления, хранения, поиска и распространения информации;
- **информационная система** — организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том **числе** с использованием средств вычислительной техники и связи, реализующих информационные процессы;
- **информационные ресурсы** - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
- **информация о гражданах (персональные данные)** - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
- **конфиденциальная информация** — документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;
- **пользователь (потребитель) информации** - субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Закон выделяет следующие цели защиты информации:

- 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;
- зашита 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.

Закон на первое место ставит сохранение конфиденциальности информации. Целостность представлена также достаточно полно, хотя и на втором месте. О доступности ("предотвращение несанкционированных действий по ... блокированию информации") сказано довольно мало.

"Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику владельцу, пользователю и иному лицу".

По сути, это положение констатирует, что зашита информации направлена на обеспечение интересов субъектов информационных отношений.

Далее. "Режим защиты информации устанавливается:

- в отношении сведений, отнесенных к государственной тайне, -

уполномоченными органами на основании Закона Российской

Федерации "О государственной тайне";

- в отношении конфиденциальной документированной информации —

собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального

закона;

- в отношении персональных данных - федеральным законом.

Здесь выделены три вида защищаемой информации, ко второму из которых

принадлежит, в частности, коммерческая информация.

Поскольку защите подлежит только документированная информация, необходимым условием является фиксация коммерческой информации на материальном носителе и снабжение ее реквизитами. Отметим, что в данном месте Закона речь идет только о конфиденциальности.

Защиту государственной тайны и персональных данных берет на себя государство; за другую конфиденциальную информацию отвечают ее собственники.

Как же защищать информацию? В качестве основного закон предлагает для этой цели мощные универсальные средства: лицензирование и сертификацию. Рассмотрим статью 19.

1.Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации "О сертификации продукции и услуг".

2. Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации.

3.Организации, выполняющие работы в области проектирования производства средств зашиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Федерации.

4.Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации. Рассмотрим пункты следующей статьи 22.

2. Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.

3.Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике

(владельце) этих систем и средств. Риск, связанный с использованием информации, полученной из несертифицированной системы лежит на потребителе информации.

4.Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств зашиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер зашиты его ресурсов и систем и получения консультаций.

5.Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации.

Статья 23 "Защита прав субъектов в сфере информационных процессов и информатизации" содержит следующий пункт:

2.Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба.

Очень важными являются пункты статьи 5, касающиеся юридической силы электронного документа и электронной цифровой подписи:

3.Юридическая сила документа, хранимого, обрабатываемого и пере даваемого с помощью автоматизированных информационных

систем, может подтверждаться электронной цифровой подписью.

Юридическая сила электронной цифровой подписи признается приналичии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.

4.Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии. Порядок выдачи лицензий определяется законодательством Российской Федерации.

Таким образом, Закон предлагает действенное средство контроля целостности и решения проблемы "неотказуемости" (невозможности отказаться от собственной подписи).

Таковы важнейшие, положения Закона "Об информации, информационных технологиях и о защите информации".