СОДЕРЖАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 1

Понятие "информационная безопасность"

- С понятием "информационная безопасность" в различных контекстах связаны различные определения.
- Так, в Законе РФ "Об участии в международном информационном обмене" информационная безопасность определяется как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.
- Подобное же определение дается и в Доктрине информационной безопасности Российской Федерации, где указывается, что информационная безопасность характеризует состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.
- Оба эти определения являются широкими и рассматривают информационная безопасность в национальных масштабах. Применительно к различным сферам деятельности так или иначе связанным с информацией понятие "информационная безопасность" принимает более конкретные очертания.

- В "Концепции информационной безопасности сетей связи общего пользования Российской Федерации" даны два достаточно узких определения этого понятия.

- 1. Информационная безопасность – это свойство сетей связи общего пользования противостоять возможности реализации нарушителем угрозы информационной безопасности.

- 2. Информационная безопасность – свойство сетей связи общего пользования сохранять неизменными характеристики информационной безопасности в условиях возможных воздействий нарушителя.

- Необходимо иметь в виду, что при рассмотрении проблемы информационной безопасности нарушитель необязательно является злоумышленником. Нарушителем информационной безопасности может быть сотрудник, нарушивший режим информационной безопасности или внешняя среда, например, высокая температура, может привести к сбоям в работе технических средств хранения информации и т. д.

- Сформулируем следующее общее определение "информационной безопасности" – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.
- Рассматривая информацию как товар можно сказать, что нанесение ущерба информации в целом приводит к материальным затратам и потерям.
- Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и, как следствие, владелец технологии, а может быть и автор, потеряют часть рынка и т. д.
- С другой стороны, рассматривая информацию как субъект управления (технология производства, расписание движения транспорта и т.д.), можно утверждать, что изменение ее может привести к катастрофическим последствиям в объекте управления – производстве, транспорте и др.
- Именно поэтому при определении понятия "информационная безопасность" на первое место ставится защита информации от различных воздействий.
- Согласно ГОСТу 350922-96 защита информации - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

- Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем.
- Это обусловлено тем, что для разных категорий субъектов характер решаемых задач может существенно различаться. Например, задачи решаемые администратором локальной сети по обеспечению информационной безопасности, в значительной степени отличаются от задач, решаемых пользователем на домашнем компьютере, не связанном сетью.
- Исходя из этого, отметим следующие важные выводы:
- – задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;
- – информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации – это принципиально более широкое понятие.

- При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами.
- В области информационной безопасности важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие, как минимум, адекватно реагировать на угрозы информационной безопасности или предвидеть новые угрозы и уметь им противостоять.
- В ряде случаев понятие "информационная безопасность" подменяется термином "компьютерная безопасность". В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информационных систем.
- Несмотря на это, в рамках изучаемого курса особое внимание будет уделяться изучению вопросов, связанных с обеспечением режима информационной безопасности применительно к вычислительным системам, в которых информация хранится, обрабатывается и передается с помощью компьютеров.
- Согласно определению, компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал.

Содержание информационной безопасности

- Информационная безопасность предполагает **комплекс** организационных, правовых и технических мер по предотвращению угроз и устранению их последствий.
- Эти меры заключаются в выявлении, устранении или нейтрализации негативных источников, причин и условий воздействия на информацию, которые составляют угрозу безопасности.
- Информационная безопасность направлена:
- – на предупреждение угроз как превентивных мер по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;
- – на выявление угроз, которое выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;
- – на обнаружение угроз, целью которого является определение реальных угроз и конкретных преступных действий;
- – на локализацию преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;
- – на ликвидацию последствий угроз и преступных действий и восстановление статус-кво.

- *Предупреждение возможных угроз* и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами.
- Важным является учет путей получения информации о готовящихся противоправных актах, планируемых хищениях, подготовительных действиях и других элементах преступных деяний.
- *Выявление* имеет целью проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий информационных и других со стороны криминальных структур или конкурентов на рынке.
- *Обнаружение угроз* – это действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба.
- К таким: действиям можно отнести обнаружение фактов хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированного доступа к источникам коммерческих секретов.
- *Пресечение или локализация угроз* – это действия, направленные на устранение действующей угрозы и конкретных преступных действий.
- Например, пресечение подслушивания конфиденциальных переговоров за счет акустического или электронного канала утечки информации.
- *Ликвидация последствий* имеет целью восстановление состояния, предшествовавшего наступлению угрозы. Например, восстановление информации, очистка компьютеров от вирусов и т.п.

- **Защищаемая информация** включает сведения, составляющие государственную, коммерческую, служебную и иные охраняемые законом тайны.
- Каждый вид защищаемой информации имеет свои особенности в области регламентации, организации и осуществления этой защиты.
- Наиболее общими признаками защиты любого вида охраняемой информации являются следующие:

– защиту информации организует и проводит собственник или владелец информации или уполномоченные им на то лица (юридические или физические);

– защитой информации собственник охраняет свои права на владение и распоряжение информацией, стремится оградить ее от незаконного завладения и использования в ущерб его интересам;

– защита информации осуществляется путем проведения комплекса мер по ограничению доступа к защищаемой информации и созданию условий, исключающих или существенно затрудняющих несанкционированный, незаконный доступ к защищаемой информации и ее носителям.

- Защищаемая информация, являющаяся государственной или коммерческой тайной, как и любой другой вид информации, необходима для управленческой, научно-производственной и иной деятельности.
- В настоящее время перед защитой информации ставятся более широкие задачи, чем обеспечение безопасности информации.
- Это обусловлено рядом обстоятельств, и в первую очередь тем, что все более широкое распространение в накоплении и обработке защищаемой информации получают ЭВМ, в которых может происходить не только утечка информации, но и ее разрушение, искажение, подделка, блокирование и иные вмешательства в информацию и информационные системы.

- **Основными целями защиты информации** являются:

– 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 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.

- Из анализа угроз безопасности информации, целей и задач ее защиты следует, что достичь максимального (требуемого) уровня защищенности можно только за счет комплексного использования существующих методов и средств защиты.
- Комплексность является одним из принципов, которые должны быть положены в основу разработки, как концепции защиты информации, так и конкретных систем защиты.

- Цели защиты информации на объектах защиты могут быть достигнуты при проведении работ **по следующим направлениям**:

– определению охраняемых сведений об объектах защиты;

– выявлению и устранению (ослаблению) демаскирующих признаков, раскрывающих охраняемые сведения;

– оценке возможностей и степени опасности технических средств разведки;

– выявлению возможных технических каналов утечки информации;

– анализу возможностей и опасности несанкционированного доступа к информационным объектам;

– анализу опасности уничтожения или искажения информации с помощью программно-технических воздействий на объекты защиты;

– разработке и реализации организационных, технических, программных и других средств и методов защиты информации от всех возможных угроз;

– созданию комплексной системы защиты;

– организации и проведению контроля состояния и эффективности системы защиты информации;

– обеспечению устойчивого управления процессом функционирования системы защиты информации.

- Реализация непрерывного процесса защиты информации возможна только на основе систем концептуального подхода и промышленного производства средств защиты, а создание механизмов защиты и обеспечение их надежного функционирования и высокой эффективности может быть осуществлено только специалистами высокой квалификации в области защиты информации.

СПАСИБО ЗА ВНИМАНИЕ!