Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Омский государственный технический университет»
Кафедра «Комплексная защита информации»

Лекция 1: «Основные понятия информационной безопасности. Основы законодательства в сфере информационной безопасности»

Асс. Горохова В.Ф.

Основные определения

В соответствии с Доктриной информационной безопасности РФ:

- **Информационная безопасность Российской Федерации** - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Основные определения

- **Защита информации** – это комплекс мероприятий, направленных на обеспечение информационной безопасности.
- **Средства обеспечения информационной безопасности -** это средства, с помощью которых осуществляются меры по защите информации, систем управления, связи, компьютерных сетей, недопущению подслушивания, маскировке, предотвращению хищения информации и т.д.
- **Объекты системы** — пассивные компоненты системы, хранящие, принимающие или передающие информацию. В качестве объектов могут быть: файлы, данные, информационные или автоматизированные системы.
- **Субъекты системы** — активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту или изменения состояния системы. В качестве субъектов могут выступать пользователи, активные программы и процессы.

Основные определения

Свойства информации с точки зрения ИБ**:**

- **Доступность** – это возможность за приемлемое время получить требуемую информационную услугу любым законным способом.
- Под **целостностью** подразумевается защищенность информации от разрушения и несанкционированного изменения.
- **Конфиденциальность** (информации) – требование не передавать информацию третьим лицам без согласия ее обладателя.

Угрозы и атаки

- **Источник угрозы** - это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.
- **Угроза (действие)** - это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации.
- **Фактор (уязвимость)** - это присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.
- **Последствия (атака)** - это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся факторы (уязвимости). Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку, - злоумышленником. Потенциальные злоумышленники называются источниками угрозы.

Окно опасности

- Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется **окном опасности**, ассоциированным с данным уязвимым местом.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда - недель), поскольку за это время должны произойти следующие события:

- должно стать известно о средствах использования пробела (уязвимости) в защите;
- должны быть выпущены соответствующие заплаты (разработаны средства устранения уязвимостей);
- заплаты должны быть установлены в защищаемой ИС.

Основные критерии классификации угроз ИБ

- **по расположению источника угроз** (внутри/вне рассматриваемой ИС);
- **по компонентам информационных систем**, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- **по способу осуществления** (случайные/преднамеренные, действия природного/техногенного характера);
- **по аспекту информационной безопасности** (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь.

Уровни обеспечения информационной безопасности

- **Законодательный уровень.** Комплекс мер, направленных на создание и поддержание в обществе негативного отношения к нарушителям и нарушениям ИБ. Совокупность законодательных актов и механизм, который позволяет согласовывать разработку законов с постоянным совершенствованием информационных технологий.
- **Административный уровень.** Совокупность документированных решений руководства, которые направлены на защиту информации, а также ресурсов, ассоциированных с ней.
- **Процедурный уровень.** Меры по обеспечению ИБ, реализуемые пользователями.
- **Технический уровень.** Реализация механизмов ИБ аппаратными и программными средствами.

Правовые акты РФ в области ИБ

1. Конституция РФ, международные договоры РФ. Данный уровень представлен рядом конституционных норм.

2. Законы Федерального уровня РФ. Специфика данного уровня законодательной базы состоит в том, что федеральные законы, регулирующие отношения в информационной среде и принятые в соответствии с ними нормативные акты подчинены Конституции и не могут ей противоречить.

3. Постановления правительства, указы президента, нормативные правовые акты федеральных министерств, служб и ведомств. «Подзаконные» нормативные акты не должны противоречить Конституции и Федеральным законам. Наряду с указами Президента РФ и постановлениями Правительства к ним относятся акты центральных органов государственного управления РФ, **приказы ФСБ, руководящие документы ФСТЭК.**

4. Нормативные правовые акты субъектов РФ, органов местного самоуправления. Имеют локальную силу и ограничены вышестоящими уровнями в иерархии.

Конституция РФ

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

- В соответствии со **статьей 24** Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому **возможность ознакомления с** документами и **материалами**, непосредственно **затрагивающими** его **права и свободы**, если иное не предусмотрено законом.
- **Статья 41** гарантирует **право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей**, **статья 42 - право на знание** достоверной **информации о** состоянии **окружающей среды**.
- **Статья 23** Конституции гарантирует **право на личную и семейную тайну**, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.
- Статья 29 гарантирует **право свободно искать, получать, передавать, производить и распространять информацию** любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации.

Уголовный кодекс РФ

В главе 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 средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Закон «Об информации, информационных технологиях и о защите информации» (149-ФЗ)

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ (принят Государственной Думой 8 июля 2006 года).

Статья 1. Сфера действия

- 1. Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

Закон «Об информации, информационных технологиях и о защите информации» (149-ФЗ)

Для самостоятельного изучения:

- Статья 2. Основные понятия, используемые в настоящем Федеральном законе
- Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации
- Статья 4. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации
- Статья 5. Информация как объект правовых отношений
- Статья 6. Обладатель информации
- Статья 7. Общедоступная информация
- Статья 8. Право на доступ к информации
- Статья 9. Ограничение доступа к информации
- Статья 10. Распространение информации или предоставление информации
- Статья 16. Защита информации.

Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

ФСТЭК России является федеральным органом исполнительной власти России, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

- обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере;
- противодействия иностранным техническим разведкам на территории Российской Федерации;
- обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом;
- защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
- осуществления экспортного контроля.

Федеральная служба безопасности Российской Федерации (ФСБ России)

Федеральная служба безопасности Российской Федерации (ФСБ России) — спецслужба, федеральный орган исполнительной власти Российской Федерации, осуществляющий в пределах своих полномочий решение задач по обеспечению безопасности Российской Федерации.

В соответствии со статьей 8 Федерального закона от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности», деятельность органов ФСБ осуществляется по следующим основным направлениям:

- контрразведывательная деятельность;
- борьба с терроризмом;
- защита конституционного строя;
- борьба с особо опасными формами преступности;
- разведывательная деятельность;
- пограничная деятельность;
- обеспечение информационной безопасности.

Статья 13. Информационные системы. (149-ФЗ) (фрагмент)

1. Информационные системы включают в себя:

1) **государственные** информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

2) **муниципальные** информационные системы, созданные на основании решения органа местного самоуправления;

3) **иные** информационные системы.

2.1. Технические средства информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями, должны размещаться на территории Российской Федерации.

Закон «О государственной тайне» (от 06.10.1997 N 131-ФЗ)

Настоящий Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

- Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.
- Носители сведений, составляющих государственную тайну, - материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.
- Система защиты государственной тайны - совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

Закон «О государственной тайне» (от 06.10.1997 N 131-ФЗ)

- Допуск к государственной тайне - процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений.
- Доступ к сведениям, составляющим государственную тайну, - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.
- Гриф секретности - реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.
- Средства защиты информации - 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.
- Перечень сведений, составляющих государственную тайну, - совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Федеральный закон "О персональных данных" N 152-ФЗ

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

- обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
- организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

Федеральный закон "О персональных данных" N 152-ФЗ

- Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Постановление правительства РФ №1119

Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных.

- Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона "О персональных данных".
- Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Постановление правительства РФ №1119

- Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.
- Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.
- Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Постановление правительства РФ №1119

Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;
- б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Постановление правительства РФ №1119

Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;
- б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;
- г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Постановление правительства РФ №1119

Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;
- д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Постановление правительства РФ №1119

Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;
- б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Постановление правительства РФ №1119

Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

- а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- б) обеспечение сохранности носителей персональных данных;
- в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Приказ ФСТЭК России № 21

Меры по обеспечению безопасности персональных данных:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Приказ ФСТЭК России № 21

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+

Домашнее задание

- Описать какими организационными мероприятиями и техническими средствами выполняются меры по защите информации для объекта информатизации являющимся информационной системой персональных данных. ИСПДн представляет собой 1 АРМ, подключенный к сети Интернет и локальной вычислительной сети организации. Данные передаются по сети Интернет в другую организацию, не передаются на машинных носителях внутри организации.
- Описание ИСПДн: Для ИСПДн актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных менее чем 100000 субъектов персональных данных, являющихся сотрудниками оператора.