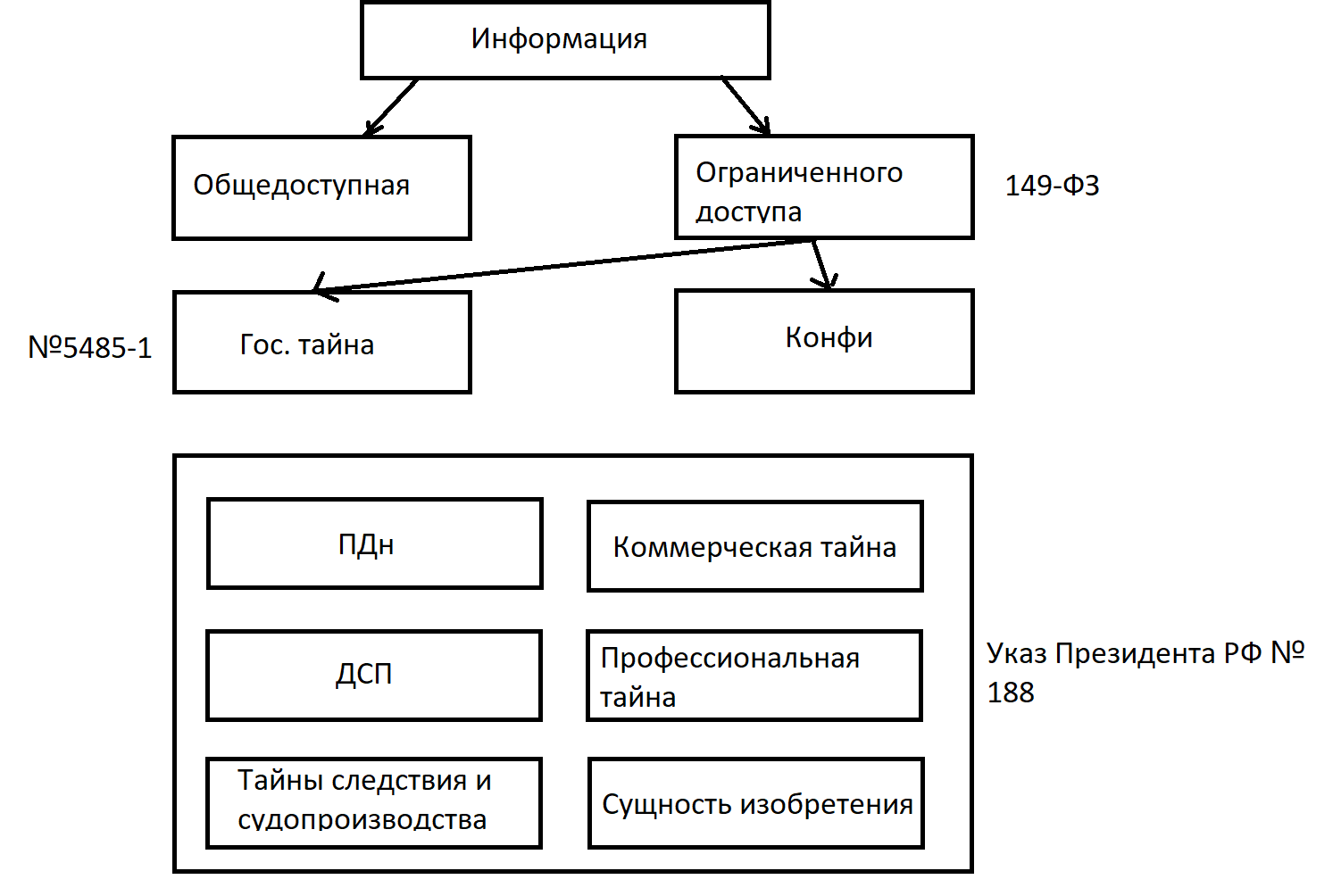
Основы информационной безопасности

# Лекция №1

Информация – любые сведения (данные) независимо от формы их представления.



ФЗ №149 27.07.2006 “Об информации, информационных технологиях и о защите информации” определяет деление информации на общедоступную и информацию, доступ к которой ограничен федеральными законами (ст. 5).

Информация, доступ к которой ограничивать нельзя (149-ФЗ, ст. 10):

* нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина;
* информация о состоянии окружающей среды;
* информация о деятельности гос. органов, а также об использовании бюджетных средств;
* информация библиотек, архивов, музеев и других организаций.

Информация ограниченного доступа делится на гостайну и конфиденциальную информацию (конфи).

Регулирование вопросов, связанных с гостайной возложено на закон РФ №5485-1 21.07.1993 “О государственной тайне”. Перечень сведений, составляющих гостайну, определен в ст. 5, где они группируются по следующим направлениям:

* сведения в военной области;
* сведения в области экономики, науки и техники;
* сведения в области внешней политики и экономики;
* сведения в области разведывательной, контрразведывательной и оперативно-разыскной деятельности, а также в области противодействия терроризму.

Перечень сведений конфиденциального характера опубликован в Указе Президента РФ №188 06.03.1997 “Об утверждении перечня сведений конфиденциального характера”. К ним относятся:

* сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность или персональные данные (ПДн);
* служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и ФЗ РФ (служебная тайна);
* сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах госзащиты (Основной закон №119-ФЗ от 20.02.2004 “О государственной защите потерпевших, свидетелей и участников уголовного судопроизводства”);
* сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и ФЗ “О коммерческой тайне”;
* сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них;

Зачастую одни и те же сведения могут относиться к различным категориям тайн. Например, врачебная тайна часто пересекается с ПДн.

Сложность работы с конфи в том, что каждый ее вид имеет свое законодательство. При обеспечении защиты необходимо рассматривать и прорабатывать большое количество документов, относящихся к данному виду тайны.

Банковская тайна (тайна банковских вкладов) – основное законодательство ФЗ №395-1 “О банках и банковской деятельности”, ГК РФ, Таможенный кодекс РФ, ФЗ “О реструктуризации кредитных организаций”

Служебная тайна – основное законодательство Указ Президента РФ №188, ГК РФ, ФЗ “Об основах государственной службы РФ”, ПП РФ №1233 от 1994 г.

## Понятие комплексной защиты информации

Одним из основных требований к СЗИ является ее комплексность.

При создании и эксплуатации СЗИ следует руководствоваться всеми аспектами ИБ:

* конфиденциальность
* доступность
* целостность

а в ряде случаев дополняется:

* надежность
* подтвержденность авторства
* неотказуемость и т.д.

Комплексность предполагает также использование в активном сочетании различных методов и средств ЗИ: правовых, организационных, физических, технических, криптографических.

Средства ЗИ могут применяться в программном, аппаратном или программно-аппаратном исполнении.

СЗИ должны обладать несколькими уровнями, перекрывающими друг друга, типа матрешка. Для отдельного объекта информатизации можно выделить 6 уровней защиты:

* охрана по периметру территории объекта
* охрана по периметру здания
* охрана помещения
* защита аппаратных средств
* защита программных средств
* защита информации

# Лекция №2

## Требования законодательства в области ИБ

Государственная система защиты информации

Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные конституцией РФ и законодательством РФ. Прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую и безопасность личности.

Обеспечение ИБ осуществляется в рамках обеспечения национальной безопасности. Политика России в области национальной безопасности строится на основе “Стратегии национальной безопасности Российской Федерации”, утвержденной Указом Президента РФ 02.07.2021 №400. В ней определены национальные интересы и стратегические национальные приоритеты России, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление национальной безопасности страны и обеспечение ее устойчивого развития на долгосрочную перспективу.

Так, среди национальных интересов России названы:

* сбережение народа России, развитие человеческого потенциала
* поддержание гражданского мира, укрепление законности, искоренение коррупции
* развитие безопасности информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия

Для достижения экономической безопасности России необходимо сократить использование американского доллара и выпускать свои вакцины.

На основе стратегии разработана доктрина “Информационной безопасности” Российской Федерации, введена в действие Указом Президента РФ от 05.12.2016 №646. Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере. В ней определены стратегические цели и основные направления обеспечения ИБ, проанализированы основные информационные угрозы, дана оценка состоянию ИБ.

Отмечается, что практика внедрения информационных технологий без увязки с обеспечением ИБ существенно повышает вероятность проявления информационных угроз.

Усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских госорганов, научных организаций и предприятий ОПК[[1]](#footnote-1). Отмечается тенденция к увеличению в иностранных СМИ объема материалов отечественной политике, российские СМИ подвергаются откровенной дискриминацией. Различные террористические, экстремистские организации широко используют механизмы информационного воздействия, возрастают масштабы компьютерной преступности. Приводятся основные направления обеспечения ИБ в области обороны, гособщественной безопасности, в экономической сфере, в области науки, технологий и образования, стратегической стабильности и равноправного стратегического партнерства.

Законодательную основу обеспечения безопасности составляют:

1. Конституция РФ;
2. Законы и другие нормативные акты РФ, регулирующие отношения в области безопасности;
3. Конституции, законы и нормативные акты республик в составе РФ, нормативные акты органов власти и управления краёв и областей, принятых в пределах их компетенции;
4. Международные договоры и соглашения , заключенные или признанные РФ.

Основные законы в области защиты информации в правах субъектов, участвующих в информационных процессах и информатизации:

* ФЗ “О безопасности” №390 28.12.2010;
* ФЗ “Об информации, информационных технологиях и защите информации” №149 27.07.2006;
* ФЗ “О государственной тайне” №5485-1
* ФЗ “О персональных данных” №152 27.07.2006
* ФЗ “О средствах массовой информации” №2124-1 27.12.1991
* ФЗ “Об электронной подписи” №66 06.04.2011
* ГК РФ
* УК РФ

Помимо правовых документов в РФ действую нормативно-методические документы:

* Методические документы госорганов России (руководящие документы ФСТЭК[[2]](#footnote-2), ведомственные приказы)
* Стандарты ИБ (международные, государственные рекомендации по стандартизации и методические указания)

Госсистема ЗИ включает:

* Органы законодательной, исполнительной, судебной
* Законодательство, регулирующее отношения в области ЗИ и информационных ресурсов
* Нормативную правовую базу по ЗИ
* Службы (органы) ЗИ, предприятий, организации учреждений

Законодательные органы (госдума) – выпускает законы, регулирующие отношения в области ЗИ.

Основу нормативной базы составляют руководящие документы и стандарты, издаваемые госстандартом.

Органы исполнительной власти (Правительство РФ) контролируют исполнения этих законов. Правительство принимает соответствующие постановления в области ЗИ и издает распоряжения, являющиеся подзаконными нормативными правовыми актами.

К основным ведомствам, регулирующим отношения в области ЗИ относятся:

* Межведомственная комиссия по защите гостайны;
* ФСТЭК;
* ФСБ;
* Госстандарт России;
* Служба внешней разведки (СВР)

Основным органом управления госсистемой ЗИ является ФСТЭК.

## Законодательство в области ИБ

ФЗ “О безопасности” №390 28.12.2010:

Уточняются принципы и содержание деятельности по обеспечению безопасности, закрепляются основные цели международного сотрудничества в данной области.

Президент РФ утверждает стратегию национальной безопасности. Он не только возглавляет, но и формирует Совет Безопасности РФ. СБ РФ готовит решение президента в определенной сфере: оборона, военное строительство, техническое сотрудничество с иностранными государствами и др.

ФЗ “Об информации, информационных технологиях и защите информации” №149 27.07.2006:

Регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации при применении информационных технологий, а также обеспечение ЗИ.

Приводит понятийный аппарат и механизмы регулирования в соответствии с практикой применения информационных технологий, определяет правовой статус различных категорий информации.

Закрепляется принцип свободы поиска, получения, передачи, производства и распространения информации любым законным способом. При этом ограничения доступа к информации могут устанавливаться только ФЗ.

Закон содержит положения, направленные на защиту от недобросовестного использования или злоупотребления возможностями средств распространения информации, при которых пользователям навязывается ненужная информация.

Установлены основные правила и способы защиты прав на информацию, защиты самой информации путем принятия основных правовых, организационных и технических мер по ее защите.

Закреплен прямой запрет на требование от гражданина предоставления информации о его частной жизни, в т.ч. информации, составляющей личную или семейную тайну.

ФЗ “О государственной тайне” №5485-1:

Закон регулирует отношения, возникающие в связи с отнесением сведений к гостайне, их рассекречиванием и защитой в интересах обеспечения безопасности РФ.

Под государственной тайной понимаются защищаемые **государством** сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-разыскной деятельностью, распространение которых может нанести ущерб безопасности РФ.

Устанавливаются 3 степени секретности и соответствующие этим степеням грифы секретности для носителей сведений:

1. Особой важности
2. Совершенно секретно
3. Секретно

Устанавливаются 3 уровня допуска к государственной тайне.

## Меры ответственности в области ЗИ

Виды ответственности:

1. Административная
2. Уголовная
3. Дисциплинарная
4. Гражданско-правовая

Контролирующие органы:

* Роскомнадзор
* ФСТЭК (Основной регулятор в сфере гостайны, занимается некриптографическими техническими средствами и экспортным контролем)
* ФСБ (Защита гостайны и конфи с помощью средств криптографической защиты)

# Лекция №3

## Общий порядок действий по созданию СЗИ

Согласно ГОСТ-Р50922 2006 года «Защита информации. Основные термины и определения»:

*Система защиты информации (СЗИ)* – совокупность органов и исполнителей, используемой ими техники ЗИ, а также объектов защиты, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области ЗИ.

В организационную структуру СЗИ входят:

* Руководитель – несет персональную ответственность за обеспечение ИБ.
* Заместитель руководителя – курирует вопросы информационно-технической безопасности.
* Постоянно действующий орган, вырабатывающий предложения по решению проблемных вопросов в области ЗИ
* Подразделение или специалист, ответственные за реализацию мероприятий по технической защите информации (ТЗИ).

Согласно ГОСТ-Р51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»:

*СЗИ* – это совокупность организационных мероприятий, технических программных и программно-технических средств ЗИ и средств контроля эффективности ЗИ.

Задачи, решаемые СЗИ:

1. Исключение неправомерных доступа, копирования, предоставления или распространения информации (конфиденциальность).
2. Исключение неправомерных уничтожения или модифицирования информации (целостность).
3. Исключение неправомерного блокирования информации (доступность).

Жизненный цикл СЗИ объекта обработки информации состоит из стадии создания системы и стадии эксплуатации.

*ЖЦ СЗИ* – совокупность взаимоувязанных процессов последовательного изменения состояния СЗИ конкретного объекта от принятия решения о необходимости защиты, обрабатываемой на нем информации, до окончания его эксплуатации.

*Обладатель информации* – это лицо, создавшее информацию и/или имеющее право разрешать или ограничивать доступ к информации.

*Заказчик* – это лицо, заключившее контракт на создание объекта обработки информации.

*Оператор* – это лицо, эксплуатирующее объект, в т.ч. непосредственно осуществляющее обработку содержащейся в нем информации.

*Уполномоченное лицо –* это лицо, осуществляющее на договорной основес заказчиком или оператором обработку информационного ресурса и/или предоставляющее для этих целей вычислительные ресурсы*.*

Этапы создания СЗИ:

1. Формирование требований к СЗИ (предпроектный этап).
2. Разработка СЗИ (этап проектирования).
3. Внедрение СЗИ (этап установки, настройки, испытаний).
4. Подтверждение соответствия СЗИ (этап оценки).

### Предпроектный этап создания СЗИ

Осуществляется обладателем информации (заказчиком) перечень работ:

1. Принятие решения о необходимости защиты обрабатываемой информации
2. Классификация объекта по требованиям ЗИ (установление уровня защищенности обрабатываемой информации)
3. Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности обрабатываемой информации
4. Определение требований к СЗИ

*Цель защиты информации в информационной системе* – минимизировать (предотвратить) ущерб обладателю информации из-за возможных нарушений свойств ее безопасности.

*Задача защиты информации* – обеспечить необходимый уровень защищенности информации от нарушений ее целостности, доступности и конфиденциальности.

Основные документы, формируемые по результатам работы на предпроектном этапе:

|  |  |  |
| --- | --- | --- |
| 1. | Принятие решения о необходимости ЗИ | Локальный нормативный правовой акт, определяющий необходимость создания СЗИ |
| 2. | Классификация по требованиям ЗИ | Акт классификации по требованиям безопасности информации |
| 3. | Определение актуальных угроз безопасности информации | Частная модель угроз безопасности информации |
| 4. | Определение требований к СЗИ | Техническое задание на создание СЗИ |

### Этап проектирования создания СЗИ

Разработка СЗИ организуется обладателем информации (заказчиком).

Перечень работ:

1. Проектирование СЗИ
2. Разработка эксплуатационной документации на СЗИ

Основные документы, формируемые по результатам работы на этапе проектирования:

|  |  |  |
| --- | --- | --- |
| 1. | Проектирование СЗИ | Технический проект на создание СЗИ |
| 2. | Разработка эксплуатационной документации на СЗИ | 1. Описание структуры СЗИ 2. Техпаспорт с указанием наименования состава и мест установки аппаратных и программных средств 3. Перечень параметров настройки СЗИ 4. Правила эксплуатации СЗИ |

### Этап внедрения по созданию СЗИ

Организуется обладателем информации (заказчиком) с привлечением оператора.

Перечень работ:

1. Установка и настройка СЗИ
2. Внедрение организационных мер ЗИ, в т.ч. разработка документов, определяющих правила и процедуры, реализуемые оператором
3. Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению
4. Испытания и опытная эксплуатация СЗИ.

Основные документы, формируемые по результатам работы на этапе внедрения:

|  |  |  |
| --- | --- | --- |
| 1. | Установка и настройка СЗИ | Акт установки средств ЗИ |
| 2. | Внедрение организационных мер ЗИ | Документы по регламентации правил по эксплуатации и вывода из эксплуатации СЗИ |
| 3. | Выявление и анализ уязвимостей | Протокол контроля уязвимостей ПО и технических средств |
| 4. | Испытания и опытная эксплуатация СЗИ | Протоколы контроля оценки эффективности средств ЗИ и оценка защищенности информации |

Состав обязательных организационно-распорядительных документов на этапе внедрения:

1. Порядок администрирования СЗИ
2. Порядок выявления инцидентов, которые могут привести к возникновению угроз безопасности информации (БИ), и реагирование на них
3. Порядок управления конфигурацией объекта и его СЗИ
4. Порядок контроля за обеспечением уровня защиты обрабатываемой информации
5. Порядок защиты информации при выводе из эксплуатации объекта.

### Этап оценки создания СЗИ

Организуется обладателем информации (заказчиком) и оператором.

Перечень работы определяется в программе и методиках аттестационных испытаний (АИ), разрабатываемой до их начала.

ГОСТ-РО0043-004 2013 года «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»:

По итогам АИ оформляются протоколы и заключение по результатам АИ. При оформлении результата АИ разрабатываются рекомендации по обеспечению защищенности информации на аттестуемом объекте и выдается аттестат соответствия соответствующим органом по аттестации.

## Этапы стадии эксплуатации СЗИ

### Ввод СЗИ в постоянную эксплуатацию

Осуществляется оператором. Решение о вводе оформляется локально-нормативным правовым актом, в котором определяются должностные лица, ответственные за эксплуатацию и сопровождение СЗИ (начальник объекта, сисадмины и админы безопасности).

### Промышленная эксплуатация СЗИ

Осуществляется оператором. Происходит непосредственная эксплуатация СЗИ.

### Вывод СЗИ из эксплуатации

На данном этапе производится архивирование информации, уничтожение или стирание данных и остаточной информации с машинных носителей информации, уничтожение машинных носителей информации.

# Лекция №4

## Организационные методы защиты информации. Понятие политики ИБ

### Организационно-административные методы ЗИ

Регламентируют процессы создания и эксплуатации информационных объектов, а также взаимодействие пользователей и систем, таким образом, чтобы НСД к информации становился либо невозможным, либо существенно затруднялся.

Такие методы ЗИ охватывают все компоненты ИС на всех этапах их жизненного цикла: проектирование систем, строительство зданий и сооружений, монтаж и наладка оборудования, эксплуатация и модернизация систем.

К организационно-административным мероприятиям ЗИ относятся:

* выделение специальных защищенных помещений для размещения ЭВМ и средств связи и хранения носителей информации;
* выделение специальных ЭВМ для обработки конфиденциальной информации;
* организация хранения конфи на специальных промаркированных носителях;
* использование в работе с конфи технических и программных средств, имеющих сертификат защищенности и установленных в аттестованных помещениях;
* организация специального делопроизводства для конфи, устанавливающего порядок подготовки использования, хранения, уничтожения и учета документированной информации;
* организация регламентированного доступа пользователей к работе на ЭВМ, средствам связи и к хранилищам носителей конфи;
* установление запрета на использование открытых каналов связи для передачи конфи;
* разработка и внедрение специальных нормативно-правовых и распорядительных документов по организации защиты конфи, которые регламентируют деятельность всех звеньев объекта защиты в процессе обработки информации;
* постоянный контроль за соблюдением установленных требований по ЗИ

### Организационно-технические методы ЗИ

К организационно-техническим мероприятиям ЗИ относятся:

* ограничение доступа посторонних лиц внутрь корпуса оборудования за счет установки механически-запорных устройств или замков;
* отключение ЭВМ от локальной вычислительной сети или сети удаленного доступа при обработке на ней конфи, кроме случаев передачи этой информации по каналам связи;
* использование для отражения конфи ЖК-мониторов, а для печати принтеров с термопечатью с целью снижения утечки информации по электромагнитному каналу;
* при использовании кинескопных мониторов и матричных принтеров рекомендуется включать устройства, создающие дополнительный шумовой эффект – генераторы шума, кондиционеры, вентиляторы и другие шумящие устройства;
* установка клавиатуры и печатающих устройств на мягкие подкладки с целью снижения утечки информации по акустическому каналу;
* организация электропитания ЭВМ от отдельного блока питания;
* использование бесперебойных источников питания;

### Понятие политики ИБ

*Политика ИБ компании* – это совокупность взглядов её руководства на обеспечение ИБ в компании.

*Политика безопасности* – это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерных систем от заданного множества угроз.

*Политика безопасности организации* – это совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политику безопасности нужно построить таким образом, чтобы она устанавливала кто имеет доступ к конкретным активам и приложениям, какие цели и обязанности будут иметь конкретные лица, а также предусмотреть процедуры безопасности, которые четко предписывают как должны выполнятся конкретные задачи безопасности.

##### Структура политики безопасности организации

Обычно политика безопасности включает:

* базовую политику безопасности;
* специализированные политики безопасности;
* процедуры безопасности.

*Базовая политика* устанавливает, как организация обрабатывает информацию, кто может получить к ней доступ и как это можно сделать. Обычно базовая ПБ поддерживается набором специализированных (частных) политик и процедур безопасности.

*Специализированные политики* можно разделить на 2 группы:

* политики, затрагивающие значительное число пользователей (политика удаленного доступа ресурсов к сети, парольная политика и др.)
* политики, связанные с конкретными техническими областями (политика конфигурации межсетевых экранов, политика шифрования и управления крипто-ключами, политика по оборудованию беспроводных сетей и др.)

При разработке частных политик руководствуются следующими принципами:

* принцип невозможности перехода в небезопасное состояние;
* принцип минимизации привилегий (предписывает давать только те права доступа, которые необходимы для выполнения служебных обязанностей);
* принцип разделения обязанностей (критически важными объектами должны управлять как минимум 2 человека);
* принцип эшелонированности обороны (предписывает не полагаться только на один защитный рубеж, каким бы надежным он не казался. За средствами физической защиты должны следовать программно-технические средства, за аутентификацией – управление доступом, затем протоколирование и аудит);
* принцип разнообразия защитных средств;
* принцип простоты и управляемости ИС в целом и защитных средств в особенности;
* принцип всеобщей поддержки мер безопасности;
* принцип адекватности (разумной достаточности);
* принцип прозрачности для легальных пользователей;
* принцип системности (система защиты должна строиться не абстрактно – защита от всего, а на основе анализа угроз, поиска оптимального набора средств и методов защиты);
* равностойкость звеньев (нельзя слабость одних звеньев компенсировать усилением других);

# Термины и определения в области Информационной Безопасности

*Безопасность информации* – защищенность информации от нежелательного ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

*Информационная система* – совокупность содержащейся в БД информации и обеспечивающих ее обработку информационных технологий и технических средств.

*Информационные технологии* – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

*Конфиденциальность информации* – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию 3м лицам без согласия ее обладателя.

*Доступ к информации* – возможность получения информации и ее использования.

*Предоставление информации* – действия, направленные на получение или передачу информации определенным кругом лиц.

*Распространение информации* – действия, направленные на получение или передачу информации неопределенным кругом лиц.

*Защищаемая информация* – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации.

*Защита информации от утечки* – деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

*Защита информации от несанкционированного доступа (НСД)* – деятельность, направленная на предотвращения получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав и/или правил доступа к защищаемой информации.

*Защита информации от несанкционированного воздействия –* деятельность, направленная на предотвращения воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате уничтожению или сбою функционирования носителей информации.

*Комплексная система защиты информации* – совокупность организационно-правовых и инженерно-технических мероприятий, направленных на обеспечение ЗИ от разглашения, утечек, несанкционированного доступа и воздействия.

1. *ОПК* – оборонно-промышленный комплекс [↑](#footnote-ref-1)
2. *ФСТЭК* – федеральная служба технического и экспортного контроля, ранее – гостехкомиссия [↑](#footnote-ref-2)