

# ***Общие вопросы защиты информации***

***Тема:***

***Правовые и организационные основы защиты информации ограниченного доступа***

# **Основные понятия в области защиты информации**

**Информация** — сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления

**Угроза безопасности информации** — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации

**Атака** — попытка реализации угрозы

**Злоумышленник** — субъект, который незаконным путем пытается добыть, изменить или уничтожить информацию законных пользователей

## **Основные понятия в области**

**Источник угрозы информации** – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности.

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

**Безопасность информации (информационная безопасность)** – состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность.

# Основные понятия в области

## **защиты информации**

*Конфиденциальность информации* – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

*Целостность информации* – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

*Доступность информации* - состояние информации, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно.

# Основные понятия в области

## защиты информации

**Кибербезопасность** - совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.

**Киберпространство** - сфера деятельности, в которой осуществляется функционирование и взаимодействие киберобъектов посредством их использования **ЧЕЛОВЕКОМ**.

**Киберобъект** - любой объект, функционирующий с использованием программных средств.

# Основные понятия в области

## **защиты информации**

*Обеспечение кибербезопасности включает в себя информационную безопасность, сетевую безопасность, интернет безопасность, безопасность критически важных систем.*

***Киберугроза (Cybersecurity threat)** – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность причинения вреда киберпространству;*

***Уязвимость киберпространства** – это потенциальная или реально существующая возможность реализации киберугрозы.*

## **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 и других форм незаконного вмешательства в информационные ресурсы и информационные системы;*

## **Цели защиты информации:**

- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных;
- сохранение государственной тайны, конфиденциальности документированной информации;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем и технологий.



# **Объекты и применяемые меры защиты информации**

## **Правовые меры защиты**

*Защита информации правовыми методами, включающая разработку законодательных и нормативных правовых документов, применение этих документов, надзор и контроль за их исполнением.*

## **Организационные меры защиты**

*Меры, предназначенные для организации функционирования ИС, персонала и взаимодействия пользователей с системой. Базовые организационные меры включают:*

- формирование политики безопасности;*
- организацию доступа в помещения;*
- организация доступа сотрудников к информационным ресурсам;*
- определение ответственности за нарушение требований информационной безопасности.*

## **Применяемые меры защиты информации**

**- Техническая и программно-аппаратная защита информации:**

*Защита информации с применением технических, программных, программно-технических средств.*

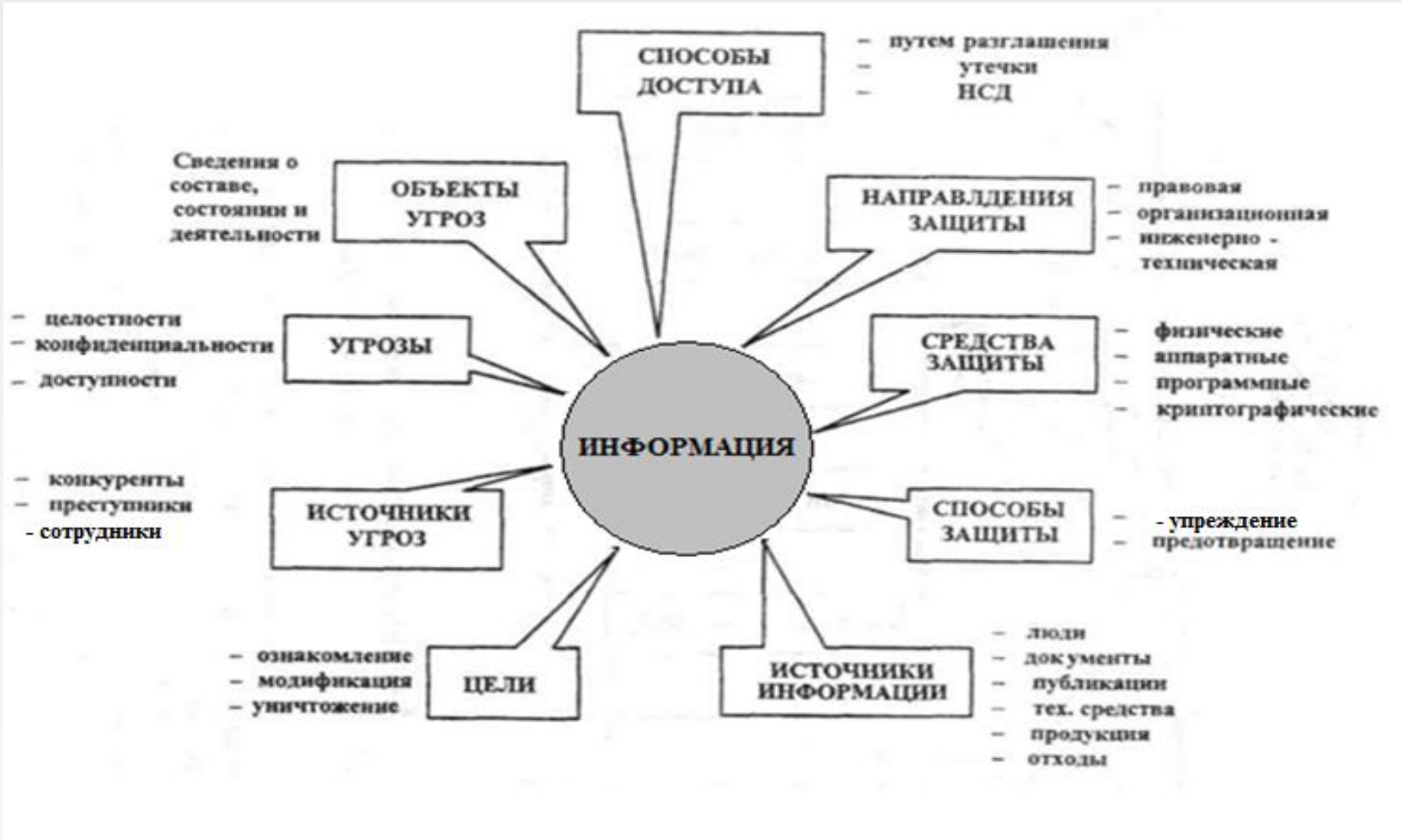
**- Физическая защита:**

*Совокупность средств, препятствующих проникновению потенциального злоумышленника на территорию контролируемой зоны.*

# Принципы построения системы защиты информации

- Комплексность;
- Своевременность;
- Непрерывность;
- Активность;
- Законность;
- Обоснованность;
- Экономическая целесообразность и сопоставимость;
- Специализация;
- Взаимодействие и координация;
- Совершенствование;
- Централизация управления;

# Концептуальная модель компонентов



# **Правовые основы обеспечения информационной безопасности**

- *Законы Российской Федерации;*
- *Указы Президента Российской Федерации;*
- *Концептуальные документы;*
- *Постановления правительства Российской Федерации;*
- *Руководящие документы регуляторов (ФСБ, ФСТЭК, Роскомнадзор и др.);*
- *Локальные нормативные документы ;*
- *Инструкции.*

## **Правовые основы обеспечения информационной безопасности**

- Закон РФ «О безопасности» от 28.12.2010 № 390-ФЗ;
- Закон РФ «О государственной тайне» от 21.07.93 № 5485-1;
- Закон РФ «О коммерческой тайне» от 29.07.2004 № 98-ФЗ;
- Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;
- Закон РФ «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ;
- Закон РФ «О техническом регулировании» от 27.12.2002 №184-ФЗ;
- Закон РФ «О стандартизации» от 29.06.2015 № 162-ФЗ;
- Закон РФ «Об электронной подписи» от 06.04.2011 № 63-ФЗ;
- Закон РФ «О связи» от 07.07.2003 № 126-ФЗ;
- Закон РФ «О персональных данных» от 27.07.2006 № 152-ФЗ;
- Закон РФ «О федеральной службе безопасности» от 03.04.95 № 40-ФЗ;
- Закон РФ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ;

## **Правовые основы обеспечения информационной безопасности**

**Закон РФ «О безопасности» от 28.12.2010 № 390-ФЗ**

*Закон определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общества, личности, экологической безопасности и иных видов, предусмотренных законодательством Российской Федерации, полномочия и функции федеральных органов государственной власти, субъектов Российской Федерации, местного самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации.*

# **Правовые основы обеспечения информационной безопасности**

## **Закон РФ «О государственной тайне» от 21.07.93 № 5485-1**

*В законе используются следующие понятия:*

**Государственная тайна** – защищаемые государством сведения в области 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 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, их носителей, а также мероприятий, проводимых в этих целях;

*Государственную тайну составляют сведения:*

- в военной области;
- в области экономики, науки и техники;
- в области внешней политики и экономики;
- в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.



# **Правовые основы обеспечения информационной безопасности**

## **Закон РФ «О коммерческой тайне» от 29.07.2004 № 98-ФЗ**

*Закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны.*

***Коммерческая тайна** – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.*

*Ст. 10 настоящего закона устанавливает меры по охране конфиденциальности информации, принимаемые ее обладателем:*

- определение перечня информации, составляющей коммерческую тайну;*
- ограничение доступа к информации, составляющей коммерческую тайну;*
- учет лиц, получивших доступ к информации, составляющей коммерческую тайну;*
- регулирование отношений по использованию информации работниками на основании трудовых и гражданско-правовых договоров;*
- нанесение на материальные носители, содержащие информацию, составляющей коммерческую тайну грифа «Коммерческая тайна».*

## **Правовые основы обеспечения информационной**

**безопасности**  
Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ

*Закон регулирует отношения, возникающие при:*

- поиске, получении, передаче, производстве и распространении информации;*
- применении информационных технологий;*
- обеспечении защиты информации.*

Закон не распространяется на отношения при правовой охране интеллектуальной деятельности.

*Правовое регулирование основывается на:*

- свободе поиска, получения, передачи, производства и распространения информации любым законным способом;*
- установление ограничений доступа к информации только федеральными законами;*
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации;*
- обеспечение безопасности Российской Федерации при создании информационных систем и их эксплуатации;*
- достоверность информации и своевременность ее представления;*

# **Правовые основы обеспечения информационной безопасности**

**Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ**

*Обладатель информации, оператор информационной системы обязаны обеспечить:*

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;*
- своевременное обнаружение фактов несанкционированного доступа к информации;*
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;*
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;*
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;*
- постоянный контроль за обеспечением уровня защищенности информации;*

## **Правовые основы обеспечения информационной безопасности**

### **Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ**

#### *Ст. 16 Защита информации*

*Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:*

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий в отношении такой информации;*
- соблюдение конфиденциальности информации ограниченного доступа;*
- реализацию права на доступ к информации.*

#### *Ст. 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации*

*Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.*

# **Правовые основы обеспечения информационной безопасности**

**Закон РФ «О лицензировании отдельных видов деятельности»  
от 04.05.2011 № 99-ФЗ**

*В соответствии с законом лицензированию подлежат следующие виды деятельности:*

- разработка, производство, распространение шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств ;*
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;*
- деятельность по выявлению электронных устройств, предназначенных для негласного получения информации;*
- разработка и производство средств защиты конфиденциальной информации;*
- деятельность по технической защите конфиденциальной информации;*
- производство и реализация защищенной от подделок полиграфической продукции;*

## **Правовые основы обеспечения информационной безопасности**

### **Закон РФ «О техническом регулировании»**

**от 27.12.2002 №184-ФЗ;**

*Закон регулирует отношения, возникающие при:*

- разработке, принятии, применении и исполнении обязательных требований к продукции, в том числе зданиям и сооружениям, процессам проектирования, производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации;*
- разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам проектирования, производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;*

## **Правовые основы обеспечения информационной безопасности**

**Закон РФ «О техническом регулировании»  
от 27.12.2002 №184-ФЗ;**

*Статья 5. Особенности в отношении:*

- оборонной продукции (работ, услуг), поставляемой по государственному оборонному заказу; продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа;
- продукции (работ, услуг), сведения о которой составляют государственную тайну;

***обязательными требованиями наряду с требованиями технических регламентов являются требования, установленные:***

- государственными заказчиками;
- федеральными органами исполнительной власти;
- уполномоченными в области обеспечения безопасности, обороны, внешней разведки, противодействия техническим разведкам и технической защиты информации.

***Особенности технического регулирования устанавливаются Президентом Российской Федерации и Правительством Российской Федерации.***

# **Правовые основы обеспечения информационной безопасности**

**Закон РФ «О стандартизации» от 29.06.2015 № 162-ФЗ;**

*Стандартизация направлена на достижение цели обеспечения обороны страны и безопасности государства.*

*Статья 6.*

***Порядок стандартизации** в отношении оборонной продукции (товаров, работ, услуг) по государственному оборонному заказу, продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции, сведения о которой составляют государственную тайну, а также процессов и иных объектов стандартизации, связанных с такой продукцией, устанавливается **Правительством Российской Федерации.***



# **Правовые основы обеспечения информационной безопасности**

**Закон РФ «Об электронной подписи» от 06.04.2011 № 63-ФЗ;**

*1. Видами электронных подписей, отношения в области использования которых регулируются настоящим Федеральным законом, являются:*

- простая электронная подпись;*
- усиленная электронная подпись.*

*Различаются усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись.*

*2. Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.*

## **Правовые основы обеспечения информационной безопасности**

**Закон РФ «Об электронной подписи» от 06.04.2011 № 63-ФЗ;**

*3. Неквалифицированной электронной подписью является электронная подпись, которая:*

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;*
- позволяет определить лицо, подписавшее электронный документ;*
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;*
- создается с использованием средств электронной подписи.*

*4. Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:*

- ключ проверки электронной подписи указан в квалифицированном сертификате;*
- для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.*

## **Правовые основы обеспечения информационной безопасности**

**Закон РФ «О персональных данных» от 27.07.2006 № 152-ФЗ;**

*Закон регулирует деятельность физических и юридических лиц по обработке и использованию персональных данных.*

*В законе определяются требования и правила по защите персональных данных ко всем организациям, государственным и частным компаниям, которые хранят, обрабатывают и собирают персональные данные своих сотрудников, посетителей или клиентов.*

*Закон обязывает операторов персональных данных уведомлять об обработке персональных данных субъекта, получать его письменное разрешение и уведомлять об уничтожении персональных данных при прекращении отношений.*

## **Правовые основы обеспечения информационной безопасности**

**Закон РФ «О персональных данных» от 27.07.2006 № 152-ФЗ;**

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

- обработке персональных данных физическими лицами исключительно для личных и семейных нужд;*
- организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов;*
- обработке персональных данных, отнесенных к сведениям, составляющим государственную тайну;*
- предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации.*

## **Правовые основы обеспечения информационной безопасности**

**Закон РФ «О безопасности критической информационной инфраструктуры  
Российской Федерации» от 26.07.2017 N 187-ФЗ;**

*Действие настоящего Федерального закона распространяется на государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы (объекты КИИ), информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сферах:*

*здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.*

## **Правовые основы обеспечения информационной безопасности**

**Закон РФ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ;**

*Критическая информационная инфраструктура (КИИ) – совокупность всех объектов КИИ и используемых ими сетей электросвязи;*

*Объекты КИИ подразделяются на значимые (три категории) и незначимые;*

*Субъекты КИИ сами определяют категории значимости своих объектов. Критерии для категорирования значимых объектов КИИ определяются постановлением Правительства.*

*Регулирование и надзор осуществляет ФСТЭК (федеральная служба по техническому и экспортному контролю), ФСБ (федеральная служба безопасности), Минкомсвязь, Банк России;*

## **Правовые основы обеспечения информационной безопасности**

**Закон РФ «О безопасности критической информационной  
инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ;**

**Субъект КИИ обязан:**

- *обеспечивать выполнение порядка, технических условий установки и эксплуатации технических средств ГосСОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак), если они устанавливаются на объектах КИИ;*
- *соблюдать требования по обеспечению безопасности и выполнять предписания регуляторов об устранении выявленных нарушений;*
- *оказывать содействие должностным лицам ФСТЭК, ФСБ и прочим регуляторам в деятельности, связанной с предупреждением, обнаружением и ликвидацией последствий инцидентов;*
- *незамедлительно информировать регуляторов об инцидентах нарушения информационной безопасности.*

## **Правовые основы обеспечения информационной безопасности**

**Закон РФ «О безопасности критической информационной  
инфраструктуры Российской Федерации» от 26.07.2017 N  
187-ФЗ;**

### ***Ответственность за невыполнение обязанностей:***

- *невыполнение требований по обеспечению безопасности КИИ («нарушение правил эксплуатации») – до 6 лет лишения свободы (до 8 лет в случае «группы лиц по предварительному сговору»);*
- *невыполнение требований по обеспечению безопасности КИИ в случае инцидента с тяжкими последствиями или угрозой таких последствий – до 10 лет лишения свободы.*



## **Правовые основы обеспечения информационной безопасности**

### **Указы Президента РФ**

- *«Стратегия национальной безопасности Российской Федерации» от 31.12.2015 № 683;*
- *«О некоторых вопросах информационной безопасности Российской Федерации» от 22.05.2015 № 260;*
- *Доктрина информационной безопасности, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646*
- *Стратегия развития информационной общества в Российской Федерации на 2017 -2030 от 9 мая 2017 г. N 203*
- *«О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 №351;*
- *«О Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия» от 12.03.2007 №320;*

## **Правовые основы обеспечения информационной безопасности**

### **Указы Президента РФ**

- *«Вопросы Федеральной службы по техническому и экспортному контролю» от 16.08.2004 №1013;*
- *«Вопросы Федеральной службы безопасности Российской Федерации» от 11.08.2003 №960;*
- *«Об утверждении перечня сведений, отнесенных к государственной тайне» от 30.11.1995 № 1203;*
- *«Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 № 188;*
- *«О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» от 03.04.1995 № 334;*
- *«Об основах государственной политики в сфере информатизации» от 20.01.1994 № 1701;*

## **Правовые основы обеспечения информационной безопасности**

**«Стратегия национальной безопасности Российской  
Федерации» от 31.12.2015 № 683;**

*обеспечение национальной безопасности - реализация органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов;*

*система обеспечения национальной безопасности - совокупность осуществляющих реализацию государственной политики в сфере обеспечения национальной безопасности органов государственной власти и органов местного самоуправления и находящихся в их распоряжении инструментов*

## **Правовые основы обеспечения информационной безопасности**

**«Стратегия национальной безопасности Российской  
Федерации» от 31.12.2015 № 683;**

*Обеспечение национальных интересов осуществляется посредством реализации следующих стратегических национальных приоритетов:*

- оборона страны;*
- государственная и общественная безопасность;*
- повышение качества жизни российских граждан;*
- экономический рост;*
- наука, технологии и образование;*
- здравоохранение;*
- культура;*
- экология живых систем и рациональное природопользование;*
- стратегическая стабильность и равноправное стратегическое партнерство.*

## **Правовые основы обеспечения информационной безопасности**

### **«Доктрина информационной безопасности» от 5 декабря 2016 г. № 646**

*Доктрина предусматривает пять основных сфер, в которых необходимо обеспечение информационной безопасности РФ:*

- оборона;*
- государственная безопасность;*
- экономика;*
- наука, технологии и образование;*
- стратегическая стабильность.*

## **Правовые основы обеспечения информационной безопасности**

**«Доктрина информационной безопасности» от 5 декабря 2016 г.  
№ 646**

***Основные информационные угрозы национальной безопасности  
России:***

- стремление «отдельных государств» использовать технологическое превосходство для доминирования в информационном пространстве;*
- наращивание зарубежными странами возможностей по оказанию «информационно-психологического воздействия» на российское население с целью внутривнутриполитической дестабилизации и подрыва суверенитета РФ;*
- увеличение в зарубежных СМИ числа материалов, содержащих «предвзятую оценку государственной политики РФ», дискриминация российских средств массовой информации за рубежом нормативам.*

## **Правовые основы обеспечения информационной безопасности**

**«Доктрина информационной безопасности» от 5 декабря 2016 г.  
№ 646**

- технологическое отставание РФ в сфере информационных технологий, высокий уровень зависимости от зарубежной компонентной базы и программного обеспечения, недостаточная эффективность отечественных научных исследований;
- рост киберпреступности, в первую очередь в кредитно-финансовой сфере.

## **Правовые основы обеспечения информационной безопасности**

### **«Доктрина информационной безопасности» от 5 декабря 2016 г. № 646**

#### ***Основные направления противостояния информационным угрозам:***

- *нейтрализация информационно-психологического воздействия, «направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества» (оборона);*
- *повышение защищенности критически важной информационной инфраструктуры, противодействие экстремизму и размыванию «традиционных российских духовно-нравственных ценностей» (госбезопасность);*



## **Правовые основы обеспечения информационной безопасности**

### **«Доктрина информационной безопасности» от 5 декабря 2016 г. № 646**

#### ***Основные направления противостояния информационным угрозам:***

- *инновационное развитие электронной промышленности, импортозамещение (экономика);*
- *разработка перспективных технологий (наука);*
- *развитие национальной системы управления российским сегментом интернета (стратегическая стабильность).*

## **Правовые основы обеспечения информационной безопасности**

**«О некоторых вопросах информационной безопасности Российской Федерации»  
от 22.05.2015 № 260;**

*В целях противодействия угрозам информационной безопасности Российской Федерации при использовании информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации предусмотрены следующие мероприятия:  
Преобразование сегмента международной компьютерной сети "Интернет" для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, находящийся в ведении Федеральной службы охраны Российской Федерации, в российский государственный сегмент информационно-телекоммуникационной сети "Интернет», являющийся элементом российской части сети "Интернет»*

## **Правовые основы обеспечения информационной безопасности**

**«О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 №351;**

*В целях обеспечения информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей, позволяющих осуществлять передачу информации через государственную границу Российской Федерации, в том числе при использовании международной компьютерной сети «Интернет» предусмотрены следующие мероприятия:*

*- подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие **государственную тайну**, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие **служебную тайну**, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети "Интернет" **не допускается**;*

## **Правовые основы обеспечения информационной безопасности**

**«О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 №351;**

*- При необходимости подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю.*

## **Правовые основы обеспечения информационной безопасности**

### **«Вопросы Федеральной службы по техническому и экспортному контролю» от 16.08.2004 №1013;**

*Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти и осуществляет реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:*

- 1) обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;*
- 2) противодействия иностранным техническим разведкам на территории Российской Федерации;*

## **Правовые основы обеспечения информационной безопасности**

### **«Вопросы Федеральной службы по техническому и экспортному контролю» от 16.08.2004 №1013;**

- 3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;*
- 4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;*
- 5) осуществления экспортного контроля.*

## **Правовые основы обеспечения информационной безопасности**

**«Вопросы Федеральной службы безопасности Российской Федерации» от  
11.08.2003 №960;**

***Одними из основных задач ФСБ России являются:***

- обеспечение в пределах своих полномочий защиты сведений, составляющих государственную тайну, и противодействия иностранным организациям, осуществляющим техническую разведку;*
- формирование и реализация в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности;*
- организация в пределах своих полномочий обеспечения криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях за рубежом.*

## **Правовые основы обеспечения информационной безопасности**

**«Об утверждении перечня сведений, отнесенных к  
государственной тайне» от 30.11.1995 № 1203;**

*К сведениям, отнесенных к государственной тайне относятся:*

- 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, в области противодействия терроризму и обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты;*



## **Правовые основы обеспечения информационной безопасности**

**«Об утверждении перечня сведений конфиденциального характера» от  
06.03.1997 № 188;**

- 1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.*
- 2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну.*
- 3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).*

## **Правовые основы обеспечения информационной безопасности**

**«Об утверждении перечня сведений конфиденциального характера» от  
06.03.1997 № 188;**

4. *Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).*
5. *Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).*
6. *Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.*
7. *Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц.*

# **Правовые основы обеспечения информационной безопасности**

## **Постановления Правительства РФ:**

- *Постановление Правительства РФ от 17.02.2018 N 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;*
- *Постановление Правительства РФ от 08.02.2018 N 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;*
- *«Об утверждении правил организации и осуществления федерального государственного контроля за обеспечением защиты государственной тайны» от 22.12.2012 №1376;*

# **Правовые основы обеспечения информационной безопасности**

## **Постановления Правительства РФ:**

- *«Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных» от 01.11.2012 № 1119*
- *«О видах электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг» от 25.06.2012 № 634;*
- *«О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных и телекоммуникационных систем ...» от 16.04.2012*

# **Правовые основы обеспечения информационной безопасности**

## **Постановления Правительства РФ:**

- *«О лицензировании деятельности по разработке и(или) производству средств защиты конфиденциальной информации» от 03.03.2012 № 171;*
- *«О лицензировании деятельности по технической защите конфиденциальной информации» от 03.02.2012 № 79;*
- *«Об организации лицензировании отдельных видов деятельности» от 21.11.2011 № 957;*
- *«О единой системе межведомственного электронного взаимодействия» от 08.09.2010 № 697;*
- *«Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой.... » от 21.04.2010 № 266;*

# Правовые основы обеспечения информационной безопасности

## Постановления Правительства РФ:

- *«Об утверждении Инструкции о порядке доступа должностных лиц и граждан Российской Федерации к государственной тайне» от 06.02.2010 № 63;*
- *«Об утверждении единого перечня продукции, подлежащей обязательной сертификации, и единого перечня продукции, подтверждение соответствия которой осуществляется в форме принятия декларации о соответствии» » от 01.12.2009 № 982;*
- *«Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям» от 18.05.2009 № 424;*
- *«О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» от 16.03.2009 № 228;*
- *«Об утверждении Положения о лицензировании внешнеэкономических операций с товарами, информацией, работами, услугами, результатами интеллектуальной деятельности (правами на них), в отношении которых установлен экспортный контроль» от 15.09.2008 № 691;*

## **Правовые основы обеспечения информационной безопасности**

### **Постановления Правительства РФ:**

- *«Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687;*
- *«Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» от 06.07.2008 № 512;*
- *«О порядке проведения проверки наличия в заявках на выдачу патента на изобретение или полезную модель, созданные в Российской Федерации, сведений, составляющих государственную тайну» от 24.12.2007 №928;*
- *«О государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий» от 06.11.2007 №758;*

# **Правовые основы обеспечения информационной безопасности**

## **Постановления Правительства РФ:**

- *«О Федеральном агентстве по техническому регулированию и метрологии» от 17.06.2004 №294;*
- *«Об утверждении Положения о создании и деятельности экспертных комиссий по техническому регулированию» от 21.08.2003 №513;*
- *«О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну...» от 15.04.95 № 333;*
- *«Положение о сертификации средств защиты информации» от 26.06.1995 № 608;*
- *«Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 04.09.1995 № 870;*
- *«Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 03.11.1994 №1233.*



## Структура государственной системы защиты информации

**Президент  
Российской Федерации**

**Совет Федерации  
Федерального  
Собрания  
РФ**

**Государственная дума  
Федерального Собрания  
РФ**

**Правительство РФ**

**Совет безопасности  
РФ**

**Федеральные органы  
исполнительной власти**

**Межведомственные и  
государственные  
комиссии**

**Органы  
исполнительной  
власти субъектов  
РФ**

**Органы местного  
самоуправления**

**Органы судебной  
власти**

**Общественные объединения, граждане,  
принимающие участие в решении задач  
обеспечения информационной безопасности РФ**

# Структура государственной системы защиты информации

**В состав системы обеспечения информационной безопасности Российской Федерации также входят:**

- *Федеральная служба по техническому и экспортному контролю (ФСТЭК России);*
- *Федеральная служба безопасности Российской Федерации (ФСБ России);*
- *Служба внешней разведки Российской Федерации (СВР России);*
- *Министерство обороны Российской Федерации (Минобороны России);*
- *Министерство внутренних дел Российской Федерации (МВД России);*
- *Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).*

## Структура государственной системы защиты информации

### Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

- организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации и руководит ею.
- является органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну.
- Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации.
- ФСТЭК России подведомственна Минобороны России. ФСТЭК России и ее территориальные органы входят в состав государственных органов обеспечения безопасности.

# Структура государственной системы защиты информации

## Основными задачами ФСТЭК России являются:

- *Организация деятельности государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной государственной системой.*
- *Осуществление самостоятельного нормативно-правового регулирования вопросов организации защиты информации.*
- *Противодействие добыванию информации техническими средствами разведки, техническая защита информации.*
- *Осуществление центральным аппаратом ФСТЭК России организационно-технического обеспечения деятельности Межведомственной комиссии по защите государственной тайны и Комиссии по экспортному контролю Российской Федерации*

# Структура государственной системы защиты информации

**Как преемник деятельности Гостехкомиссии России ФСТЭК наделена следующими полномочиями:**

- *организация и проведение лицензирования деятельности по осуществлению мероприятий и/или оказанию услуг в области защиты государственной тайны (в части, касающейся противодействия техническим разведкам и/или технической защиты информации);*
- *создание средств защиты информации, содержащей сведения, составляющие государственную тайну;*
- *техническая защита конфиденциальной информации;*
- *разработка и/или производство средств защиты конфиденциальной информации, а также лицензирование иных видов деятельности в соответствии с законодательством Российской Федерации.*

Решения ФСТЭК России являются обязательными для исполнения всеми органами государственной власти и местного самоуправления, государственными и негосударственными предприятиями, учреждениями, организациями, должностными лицами и гражданами

## Структура государственной системы защиты информации

### **Федеральная служба безопасности Российской Федерации (ФСБ России):**

- *ФСБ России является федеральным органом исполнительной власти.*
- *Руководит ФСБ Президент.*
- *При ФСБ России действует Академия криптографии Российской Федерации.*
- *Основные цели, задачи и функции ФСБ описаны в "Положении о Федеральной службе безопасности Российской Федерации и ее структуре".*
- *ФСБ определяет порядок осуществления в пределах своих полномочий контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.*

# Структура государственной системы защиты информации

## Федеральная служба безопасности Российской Федерации (ФСБ России):

- *ФСБ осуществляет и организует в соответствии с федеральным законодательством сертификацию средств защиты информации, систем и комплексов телекоммуникаций, технических средств, используемых для выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах;*
- *определяет основные направления деятельности органов федеральной службы безопасности в этих областях;*
- *осуществляет и организует в соответствии с федеральным законодательством лицензирование отдельных видов деятельности.*

## Структура государственной системы защиты информации

**Минобороны России** - федеральный орган исполнительной власти (федеральное министерство), проводящий государственную политику и осуществляющий государственное управление в области обороны, а также координирующий деятельность федеральных министерств, иных федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по вопросам обороны.

**МВД России** - федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, а также по выработке государственной политики в сфере миграции.

**Роскомнадзор** - федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы.



## **Административная и уголовная ответственность за нарушения в области информационной безопасности**

*Статья 13.11 Кодекса РФ об административных правонарушениях (КоАП РФ) регламентирует ответственность за нарушение порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные).*

*Статья 13.12 КоАП РФ составляют:*

- нарушения условий, предусмотренных лицензией на осуществление деятельности в области защиты информации;*
- использование несертифицированных информационных систем, баз и банков данных, несертифицированных средств защиты информации;*
- нарушение условий предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну;*
- использование несертифицированных средств защиты информации, составляющей государственную тайну.*

## **Административная и уголовная ответственность за нарушения в области информационной безопасности**

*Статья 13.13 КоАП РФ регламентирует ответственность за занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения специального разрешения (лицензии), если такое разрешение (лицензия) обязательна.*

*Статья 13.14 регламентирует ответственность на разглашение информации с ограниченным доступом.*

*Статья 13.15 регламентирует ответственность за:*

- изготовление и(или) распространение теле-, видео-, кинопрограмм, документальных, художественных фильмов, а также файлы, программы обработки информации, содержащих скрытые вставки, воздействующие на подсознание людей и(или) оказывающих вредное воздействие на их здоровье;*
- распространение информации об организациях, в отношении которых принято решение о ликвидации или запрете деятельности.*

## **Административная и уголовная ответственность за нарушения в области информационной безопасности**

*Статья 274.1 УК РФ устанавливает наказание за неправомерное воздействие на критическую информационную инфраструктуру:*

*- За нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, ... - лишение свободы на срок до 6 лет*

*- Деяния, приведшие к нарушению эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения - лишение свободы на срок до 8 лет*

*- Деяния, приведшие к нарушению эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, если они повлекли тяжкие последствия - лишение свободы на срок до 10 лет*

***СПАСИБО ЗА ВНИМАНИЕ***