Московский технологический университет

Институт комплексной безопасности и специального приборостроения

Кафедра КБ-1 «Защита информации»

Специальный курс: Система защиты информации Российской Федерации

Тема 1: Основные составляющие государственной системы защиты информации

2017 год

Цель спец. курса и рассматриваемые темы

Цель курса: **Ознакомить обучаемых с нормативно-правовыми актами государственной системы защиты информации, возможными угрозами информационной безопасности и мерами по их компенсации**

Темы курса:

Тема1: Основные составляющие государственной системы защиты информации.

Тема 2: Угрозы информационной безопасности и меры по компенсации

Вопросы Темы 1:

1. Цель, задачи и содержание специального курса.
2. Информационная безопасность и ее место в системе национальной безопасности РФ.
3. Правовой режим лицензирования и сертификации в сфере информационной безопасности.
4. Современные тенденции в развитии организационно-правового обеспечения информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. **Основы информационной безопасности.** Учебное пособие для вузов. – М.: Горячая линия – Телеком. – 2011.
2. Борисов М.А., Романов О.А. **Основы организационно-правовой защиты информации.** – М.: ЛЕНАНД. – 2015.
3. Коваленко Ю.И. **Правовой режим лицензирования и сертификации в сфере информационной безопасности.** Учебное пособие. – М.: Горячая линия – Телеком. – 2012.
4. Перечень технической документации, национальных стандартов и методических документов. http://fstec.ru/litsenzionnaya-deyatelnost/tekhnicheskaya-zashchita-informatsii/.

1. Цель, задачи и содержание спец. курса

Спец. курс **«Система защиты информации Российской Федерации»** призвана обеспечить освоение слушателями практических навыков работы с нормативно-правовой базой в области обеспечения **информационной безопасности.**

Задачи курса:

- изучение основ организационного и правового обеспечения информационной безопасности;
- изучение правовых основ организации защиты государственной тайны и конфиденциальной информации, задач служб защиты государственной тайны и подразделений защиты информации;
- овладение навыками применения нормативных правовых актов и нормативных методических документов в области обеспечения информационной безопасности;
- овладение навыками разработки проектов нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.

2. Информационная безопасность и ее место в системе национальной безопасности РФ

Конституция Российской Федерации

Конституция РФ является основным источником права в области обеспечения информационной безопасности в России.

Согласно Конституции РФ:

- каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 23);
- сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (статья 24);
- каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, перечень сведений, составляющих государственную тайну, определяется федеральным законом (статья 29);
- каждый имеет право на достоверную информацию о состоянии окружающей среды (статья 42).

- **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.
- **Информация** - сведения (сообщения, данные) независимо от формы их представления.

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ

Предметом регулирования данного Закона являются общественные отношения, возникающие в трех взаимосвязанных направлениях:

- формирование и использование информационных ресурсов;
- создание и использование информационных технологий и средств их обеспечения;
- защита информации, прав субъектов, участвующих в информационных процессах и информатизации.

Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

В Законе также отражены вопросы, связанные с порядком обращения с персональными данными, сертификацией информационных систем, технологий, средств их обеспечения и лицензированием деятельности по формированию и использованию информационных ресурсов.

Федеральный закон "О безопасности" от 28.12.2010 № 390-ФЗ

ФЗ-390 регулирует принципы обеспечения безопасности:

- личной;
- общественной;
- государственной;
- экологической;
- национальной.

Федеральным законом №390 устанавливаются полномочия и функции государственных органов в сфере сохранности.

Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ

Основными принципами обеспечения безопасности являются:

1. соблюдение и защита прав и свобод человека и гражданина;
2. законность;
3. системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности;
4. приоритет предупредительных мер в целях обеспечения безопасности;
5. взаимодействие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности.

Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне»

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.

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.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: "**особой важности**", "**совершенно секретно**" и "**секретно**".

Должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне,
несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне»

Государственную тайну составляют:

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

Не подлежат отнесению к государственной тайне сведения:

1. о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
2. о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
3. о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
4. о фактах нарушения прав и свобод человека и гражданина;
5. о размерах золотого запаса и государственных валютных резервах Российской Федерации;
6. о состоянии здоровья высших должностных лиц Российской Федерации;
7. о фактах нарушения законности органами государственной власти и их должностными

«Доктрина информационной безопасности Российской Федерации»

(Указ Президента Российской Федерации № 646 от 05.12.2016 г.)

1. **Настоящая Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.**
2. **В настоящей Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.**
3. **Правовую основу настоящей Доктрины составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.**
4. **Настоящая Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.**

Составляющие информационной безопасности, согласно Доктрине информационной безопасности (Указ Президента Российской Федерации № 646от 05.12.2016 г.)

Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности. При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

Роль и место информационной безопасности в обеспечении национальной безопасности России

В Ы В О Д

«Доктрина информационной безопасности Российской Федерации» (Указ Президента Российской Федерации № 646 от 05.12.2016 г.)

Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательных решений таких з а д а ч, как:

1. Разработка основных направлений в области обеспечения информационной безопасности, а также мероприятий и механизмов, связанных с реализацией этой политики

2. Развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области

3. Разработка федеральных целевых программ обеспечения информационной безопасности

4. Разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации

5. Совершенствование нормативной базы обеспечения информационной безопасности

6. Установление ответственности должностных лиц органов государственной власти субъектов РФ, органов местного самоуправления, юридических лиц за соблюдением требований информационной безопасности

7. Развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны

Структура государственной системы ПД ТР и ТЗИ

ФСТЭК России

Аппараты органов государственной власти, федеральные органы исполнительной власти

- Технические комиссии
- Структурные подразделения по ПД ТР и ТЗИ

Организации, проводящие работы по оборонной тематике и другие работы с использованием сведений, составляющих государственную или служебную тайну

- Технические комиссии
- Подразделения по ПД ТР и ТЗИ

- Управления ФСТЭК России по федеральным округам
- Головная НИО по проблемам ПД ТР и ТЗИ
- Отраслевые и региональные аттестационные центры
- Головные НИО по проблемам ПД ТР в федеральных органах исполнительной власти
- Органы и испытательные центры (лаборатории) по сертификации
- Органы аттестации
- Головные НИО по ПД отдельным видам ТР
- Учебные заведения
- Организации, оказывающие услуги в области ПД ТР и ТЗИ
- Организации - разработчики средств ПД ТР, ТЗИ и контроля

Аппараты органов государственной власти субъектов РФ, органы исполнительной власти субъектов РФ, органы местного самоуправления

- Технические комиссии
- Структурные подразделения по ТЗИ

Организации, проводящие работы с использованием сведений, составляющих государственную или служебную тайну

- Технические комиссии
- Подразделения по ТЗИ

- - - - координация и функциональное регулирование

——— - ведомственное управление

Организационная структура системы обеспечения информационной безопасности Российской Федерации

3. Правовой режим лицензирования и сертификации в сфере информационной безопасности

Основные формы государственного регулирования деятельности в области защиты информации

Лицензирование - комплекс мер по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну, деятельностью по защите информации конфиденциального характера, а также с созданием средств защиты информации.

Обязательное лицензирование деятельности, связанной с защитой государственной тайны; деятельности по технической защите конфиденциальной информации;

Лицензионные и другие требования, в том числе:

- Требования к уровню подготовки руководителей организаций, наличию в структуре организации специальных подразделений
- Требования к процедуре назначения руководителей
- Требования по категорированию объектов органов управления, предприятий ОПК, образцов ВиВТ, объектов информатизации, информационных систем
- Закрепленная в Законах Российской Федерации обязательность принятия мер по защите информации, ответственности за нарушение требований законов и другие

Сертификация средств защиты информации

Сертификация представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам (далее именуется - система сертификации). (В Постановлении Правительства Российской Федерации №608-95года). Сертификация средств защиты информации осуществляется на основании требований государственных стандартов, нормативных документов, утверждаемых Правительством Российской Федерации и федеральными органами по сертификации в пределах их компетенции.

Федеральный закон от 04.05.2011 N 99-ФЗ (ред. от 29.07.2017) «О лицензировании отдельных видов деятельности»

Лицензирование - деятельность лицензирующих органов по предоставлению, переоформлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, осуществлению лицензионного контроля, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса, а также по предоставлению в установленном порядке информации по вопросам лицензирования.

Лицензируемый вид деятельности - вид деятельности, на осуществление которого на территории Российской Федерации и на иных территориях, над которыми Российская Федерация осуществляет юрисдикцию в соответствии с законодательством Российской Федерации и нормами международного права, требуется получение лицензии в соответствии с настоящим Федеральным законом, в соответствии с федеральными законами

Лицензия - специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается документом, выданным лицензирующим органом на бумажном носителе или в форме электронного документа, подписанного электронной подписью, в случае, если в заявлении о предоставлении лицензии указывалось на необходимость выдачи такого документа в форме электронного документа;

Федеральный закон от 04.05.2011 N 99-ФЗ (ред. от 29.07.2017) «О лицензировании отдельных видов деятельности»

В перечень лицензионных требований с учетом особенностей осуществления лицензируемого вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности) могут быть включены следующие требования:

1) наличие у соискателя лицензии и лицензиата помещений, зданий, сооружений и иных объектов по месту осуществления лицензируемого вида деятельности, технических средств, оборудования и технической документации, принадлежащих им на праве собственности или ином законном основании, соответствующих установленным требованиям и необходимых для выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности;
2) наличие у соискателя лицензии и лицензиата работников, заключивших с ними трудовые договоры, имеющих профессиональное образование, обладающих соответствующей квалификацией и (или) имеющих стаж работы, необходимый для осуществления лицензируемого вида деятельности;
3) наличие у соискателя лицензии и лицензиата необходимой для осуществления лицензируемого вида деятельности системы производственного контроля;
4) соответствие соискателя лицензии и лицензиата требованиям, установленным федеральными законами и касающимся организационно-правовой формы юридического лица, размера уставного капитала, отсутствия задолженности по обязательствам перед третьими лицами;
5) иные требования, установленные федеральными законами.

Статья 5. Полномочия Правительства Российской Федерации в области лицензирования и полномочия лицензирующих органов

К полномочиям Правительства Российской Федерации в области лицензирования относятся:

1) определение федеральных органов исполнительной власти, осуществляющих лицензирование конкретных видов деятельности;

2) утверждение положений о лицензировании конкретных видов деятельности и принятие нормативных правовых актов по вопросам лицензирования;

3) утверждение порядка предоставления документов по вопросам лицензирования в форме электронных документов, подписанных электронной подписью, с использованием информационно-телекоммуникационных сетей общего пользования, в том числе единого портала государственных и муниципальных услуг;

4) утверждение типовой формы лицензии;

5) утверждение показателей мониторинга эффективности лицензирования, порядка проведения такого мониторинга, порядка подготовки и представления ежегодных докладов о лицензировании.

Статья 5. Полномочия Правительства Российской Федерации в области лицензирования и полномочия лицензирующих органов

К полномочиям лицензирующих органов относятся:

1) осуществление лицензирования конкретных видов деятельности;

2) проведение мониторинга эффективности лицензирования, подготовка и представление ежегодных докладов о лицензировании;

3) утверждение форм заявлений о предоставлении лицензий, переоформлении лицензий, а также форм уведомлений, предписаний об устранении выявленных нарушений лицензионных требований, выписок из реестров лицензий и других используемых в процессе лицензирования документов;

4) предоставление заинтересованным лицам информации по вопросам лицензирования, включая размещение этой информации в информационно-телекоммуникационной сети "Интернет" на официальных сайтах лицензирующих органов с указанием адресов электронной почты, по которым пользователями этой информацией могут быть направлены запросы и получена запрашиваемая информация.

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВа РОССИЙСКОЙ ФЕДЕРАЦИИ ПОСТАНОВЛЕНИЕ от 15 апреля 1995 г. № 333 «О ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ, УЧРЕЖДЕНИЙ И ОРГАНИЗАЦИЙ ПО ПРОВЕДЕНИЮ РАБОТ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОЗДАНИЕМ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, А ТАКЖЕ С ОСУЩЕСТВЛЕНИЕМ МЕРОПРИЯТИЙ И (ИЛИ) ОКАЗАНИЕМ УСЛУГ ПО ЗАЩИТЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ»

Органами, уполномоченными на ведение лицензионной деятельности, являются:

1. по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну, - Федеральная служба безопасности Российской Федерации и ее территориальные органы (на территории Российской Федерации), Служба внешней разведки Российской Федерации (за рубежом);

2. на право проведения работ, связанных с созданием средств защиты информации, - Федеральная служба по техническому и экспортному контролю, Служба внешней разведки Российской Федерации, Министерство обороны Российской Федерации, Федеральная служба безопасности Российской Федерации (в пределах их компетенции);

3. на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны - Федеральная служба безопасности Российской Федерации и ее территориальные органы, Федеральная служба по техническому и экспортному контролю, Служба внешней разведки Российской Федерации (в пределах их компетенции).

Постановление Правительства РФ от 16.04.2012 № 313 (ред. от 18.05.2017)

ПОЛОЖЕНИЕ

О ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ ПО РАЗРАБОТКЕ, ПРОИЗВОДСТВУ, РАСПРОСТРАНЕНИЮ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ, ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ, ЗАЩИЩЕННЫХ С ИСПОЛЬЗОВАНИЕМ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ, ВЫПОЛНЕНИЮ РАБОТ, ОКАЗАНИЮ УСЛУГ В ОБЛАСТИ ШИФРОВАНИЯ ИНФОРМАЦИИ, ТЕХНИЧЕСКОМУ ОБСЛУЖИВАНИЮ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ, ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ, ЗАЩИЩЕННЫХ С ИСПОЛЬЗОВАНИЕМ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ (ЗА ИСКЛЮЧЕНИЕМ СЛУЧАЯ, ЕСЛИ ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ, ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ, ЗАЩИЩЕННЫХ С ИСПОЛЬЗОВАНИЕМ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ, ОСУЩЕСТВЛЯЕТСЯ ДЛЯ ОБЕСПЕЧЕНИЯ СОБСТВЕННЫХ НУЖД ЮРИДИЧЕСКОГО ЛИЦА ИЛИ ИНДИВИДУАЛЬНОГО ПРЕДПРИНИМАТЕЛЯ)

Постановление Правительства РФ от 16.04.2012 № 313 (ред. от 18.05.2017)

К шифровальным (криптографическим) средствам (средствам криптографической защиты информации), включая документацию на эти средства, относятся:

1. средства шифрования;
2. средства имитозащиты
3. средства электронной подписи;
4. средства кодирования;
5. средства изготовления ключевых документов;
6. ключевые документы;
7. аппаратные шифровальные (криптографические) средства;
8. программные шифровальные (криптографические);
9. программно-аппаратные шифровальные (криптографические) средства.

Лицензирование деятельности, определенной настоящим Положением, осуществляется Федеральной службой безопасности Российской Федерации.

Постановление Правительства РФ от 16.04.2012 № 314 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»

Электронное устройство, предназначенное для негласного получения информации - специально изготовленное изделие, содержащее электронные компоненты, скрытно внедряемое (закладываемое или вносимое) в места возможного съема защищаемой акустической речевой, визуальной или обрабатываемой информации (в том числе в ограждения помещений, их конструкции, оборудование, предметы интерьера, а также в салоны транспортных средств, в технические средства и системы обработки информации).

Средства выявления электронных устройств, предназначенных для негласного получения информации - технологическое, испытательное, контрольно-измерительное оборудование, а также средства вычислительной техники и программное обеспечение, позволяющие осуществлять поиск электронных устройств, предназначенных для негласного получения информации.

Лицензирование деятельности, определенной настоящим Положением, осуществляется Федеральной службой безопасности Российской Федерации

Постановление Правительства РФ от 03.02.2012 № 79 (ред. от 15.06.2016) «О лицензировании деятельности по технической защите конфиденциальной информации»

Под **технической защитой конфиденциальной информации** понимается выполнение работ и (или) оказание услуг по ее защите от несанкционированного доступа, от утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Лицензирование деятельности по технической защите конфиденциальной информации осуществляет **Федеральная служба по техническому и экспортному контролю**.

4. Современные тенденции в развитии организационно-правового обеспечения информационной безопасности

Понятие системы защиты информации

Система защиты информации – совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно - распорядительными и нормативными документами в области защиты информации.

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения

Правовое обеспечение государственной системы защиты информации в Российской Федерации

Извлечения из Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам утвержденное постановлением Совета Министров-Правительства РФ от 15.09.1993 года № 912-51. **(Положение – 93)**

Является обязательным для выполнения при проведении работ защите информации, содержащей сведения, составляющие государственную или служебную тайну в органах представительной, исполнительной и судебной властей РФ, республик в составе РФ, автономной области, автономных округов, краев, областей, городов Москва и Санкт-Петербург, в органах местного самоуправления, на предприятиях и в их объединениях, учреждениях и организациях независимо от их форм собственности

Определяет структуру государственной системы защиты информации в РФ, ее задачи и функции, основы защиты организации сведений, отнесенных в установленном порядке к государственной или служебной тайне от иностранных технических разведок и от ее утечки по техническим каналам

Главные направления работ по защите информации

- Обеспечение эффективного управления системой ЗИ
- Определение охраняемых сведений, и демаскирующих признаков
- Анализ и оценка реальной опасности угроз безопасности информации, каналов утечки
- Разработка и реализация организационно-технических мероприятий
- Организация и проведение контроля состояния ЗИ

- Лицензирование деятельности предприятий в области защиты информации
- Аттестование объектов по выполнению требований обеспечения безопасности информации
- Сертификация средств защиты информации и контроля за ее эффективностью, средств информатизации с вязи в части ЗИ от утечки по техническим каналам
- Категорирование вооружения и военной техники, предприятий по степени важности ЗИ в оборонной, экономической, политической, научно-технической и др. сферах деятельности
- Обеспечение условий для ЗИ при подготовке и реализации международных договоров
- Оповещение о полетах космических воздушных летательных аппаратов, кораблях и судах, ведущих разведку объектов на территории РФ
- Введение территориальных, частотных, энергетических , пространственных и временных ограничений в режимах использования технических средств, подлежащих защите.
- Создание и применение информационных и автоматизированных систем в защищенном исполнении
- Разработка и внедрение технических решений и элементов ЗИ при создании и эксплуатации военной техники, при проектировании, строительстве и эксплуатации объектов, систем и средств автоматизации и связи и другие.

Основное содержание «Положения-93»

Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам утвержденное постановлением Совета Министров-Правительства РФ от 15.09.1993 года № 912-51. (Положение – 93)

1. **Состав, структуру, функции и задачи государственной системы защиты информации**
2. **Организацию защиты информации в системах и средствах информатизации и связи**
3. **Организацию защиты информации о вооружении и военной техники от технических средств разведки**
4. **Организацию защиты информации об объектах органов управления, военных и промышленных объектах системах и средства информатизации и связи**
5. **Контроль состояния защиты информации**
6. **Финансирование мероприятий по защите информации**

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Государственная система защиты информации - **совокупность органов защиты информации, используемых ими средств и методов защиты информации и ее носителей, а также мероприятий, проводимых в этих целях.**

ОСНОВНЫЕ ЗАДАЧИ

- **Проведение единой технической политики, организация и координация работ по защите информации в различных сферах деятельности государственных структур**
- **Нормативно-методическое обеспечение деятельности государственной системы защиты информации**
- **Оценка возможностей технической разведки, формирование модели угроз информационной безопасности**
- **Проведение организационно-технических мероприятий по противодействию технической разведке и технической защите информации**
- **Организация сил, создание средств защиты информации и средств контроля эффективности принятых мер защиты**
- **Контроль состояния защищенности информации в органах государственной власти и организациях**

Основные органы государственной системы защиты информации

п. **11 «Положения о государственной системе защиты информации в Российской Федерации от ИТР и от ее утечки по техническим каналам», утвержденное Постановлением Совета министров – Правительства Российской Федерации от 15 сентября 1993 г. № 912- 51 («Положение - 93»)**

ГОСУДАРСТВЕННУЮ СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ ОБРАЗУЮТ:

Федеральная служба по техническому и экспортному контролю России

Федеральная служба безопасности России и подразделения по защите информации

Министерство внутренних дел России и подразделения по защите информации

Министерство обороны России и подразделения по защите информации

Служба внешней разведки России и подразделения по защите информации

Федеральная служба охраны и подразделения по защите информации

Структурные и межотраслевые подразделения органов государственной власти

Головные НИИ, предприятия ОПК, ВУЗы и институты повышения квалификации

Предприятия, специализирующиеся на проведении работ в области защиты информации

ОБЪЕКТЫ МЕЖОТРАСЛЕВОЙ КООРДИНАЦИИ И ФУНКЦИОНАЛЬНОГО РЕГУЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

- Аппараты органов государственной власти Российской Федерации
- Федеральные органы исполнительной власти
- Органы местного самоуправления
- Аппараты органов государственной власти субъектов Российской Федерации
- Органы исполнительной власти субъектов Российской Федерации
- Предприятия, организации, учреждения

Основные объекты ТЗИ ограниченного доступа, не содержащей сведений составляющих государственную тайну и открытой информации

Информационные системы.

Государственные ИС. | **Муниципальные ИС.** | **Иные ИС**

СТРК
Рекомендации по обеспечению безопасности ПД в ИСПДн, КСИИ

1 Информационные системы, средства информатизации, содержащие:

- Информацию ограниченного доступа, не содержащую сведений, составляющих государственную тайну
- Открытую информацию

КСИИ – ключевая система инфор. Инфраструк. | ИСПД | ЛВС | АРМ | Средства печати, копирования | Средства связи, коммутации и др.

2 Технические средства и системы обработки открытой информации в помещениях, где обрабатывается закрытая информация

Бытовые устройства | Средства пожарной и охранной сигнализации | Средства связи. | Телефоны и др.

3 Помещения для ведения переговоров с использованием сведений ограниченного доступа

Особенности подключения государственных информационных систем к ИТКС (Интернет) установлены Указом Президента РФ от 17 марта 2008 г. № 351)

Информация с ограниченным доступом

КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ

Конфиденциальной является информация, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничен в соответствии с законодательством Российской Федерации.

Конфиденциальность информации – состояние защищённости информации, характеризуемое способностью объектов информатизации обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К)

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам **без согласия ее обладателя;**

Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

Федеральный закон от 27 07 2006 «Об информации, информационных технологиях и о защите информации»

Защита информации конфиденциального характера

Техническая защита конфиденциальной информации- защита информации не криптографическими методами, направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования (СТР-К)

Субъекты деятельности по защите информации

Органы власти, уполномоченные органы власти, организации, обрабатывающие информацию на объектах информатизации, организации - лицензиаты

Что подлежит защите → **Объекты информатизации, ИС, в т.ч. программные средства, в которых обрабатывается и хранится информация, на доступ к которой установлены ограничения федеральными законами, средства защиты информации, общедоступная информация**

От каких угроз → **От утечки по техническим каналам, неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.**

Как защищать → Комплекс правовых, организационных и технических мер

Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) «О персональных данных»

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.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Причины повышения эффективности и наращивания усилий по созданию и развитию систем защиты информации в органах власти и организациях федерального округа

- осуществление иностранными разведывательными службами наращивания и модернизации сил и средств ИТР в пределах ФО и на территории сопредельных государств, а также расширение возможностей использования этих средств;

- недостаточность нормативной правовой базы субъектов Российской Федерации, находящихся в пределах ФО, в отношении закрепления ответственности и возложения обязанностей на должностных лиц по обеспечению безопасности информации с ограниченным доступом на объектах защиты;

- увеличение количества и масштабов использования в органах власти и организациях информационных систем, недостаточно защищенных от вероятных угроз безопасности информации, имеющих выход в сети связи общего пользования, международные информационные сети;

- широкомасштабное использование в каналах передачи (обмена) информацией, в открытых каналах связи органами власти и организациями радиоустройств, применение которых увеличивает возможности технических разведок и в значительной мере упрощает доступ к защищаемой информации, в том числе к технологической информации КСИИ.

«Специальные требования и рекомендации по технической защите конфиденциальной информации»

Защите подлежат:

Информационные ресурсы информационных систем

Совокупность файлов данных, составляющих информацию пользователей и программных продуктов, определяющих информационную технологию.

Средства и системы информатизации

СВТ, АС различного уровня и назначения на базе СВТ, в т. ч. информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), средства защиты информации, используемые для защиты конфиденциальной информации

Технические средства и системы,

Не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует);

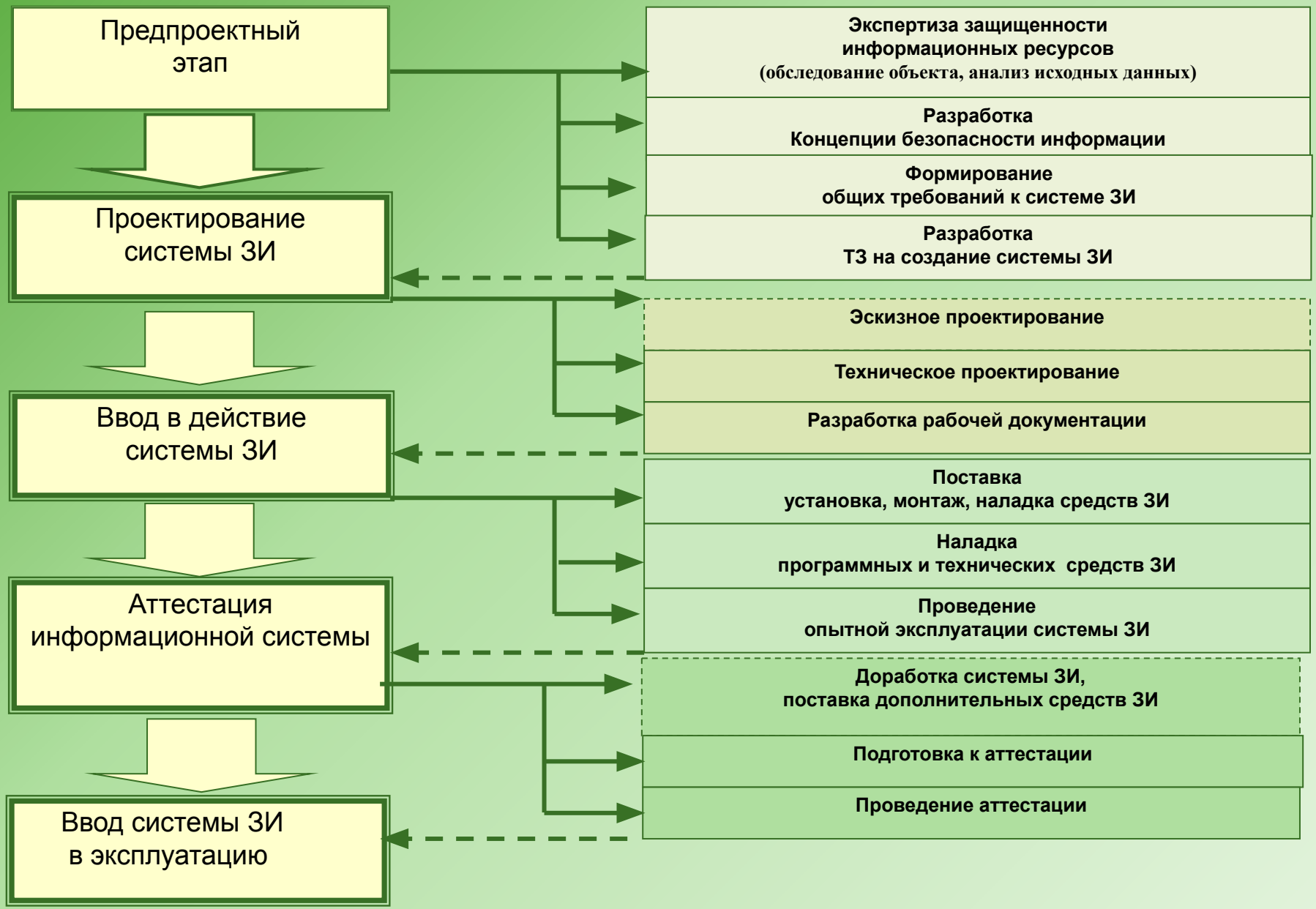
Помещения

для ведения переговоров со сведениями ограниченного доступа

С И С Т Е М А

защиты информации в органе власти (организации)

Основные этапы формирования защищенной информационной системы



Основные этапы и содержание работ по созданию (совершенствованию) системы защиты информации органа власти (организации)

Определение объекта защиты, объектов защиты информации, анализ потоков и хранилищ информации, каналов связи, оценка последствий (ущерба) в случае утечки информации или нарушений в работе ИС , содержащих информацию, отнесенную федеральными законами к информации ограниченного доступа)

Оценка масштаба основных работ, обоснование их необходимости, определение основных требований, предварительная оценка стоимости, выбор исполнителя работ,

Определение требований к системе ЗИ, замысла на ее создание (совершенствование)	**Концепция (политика) защиты информации**
Выработка решения	**Техническое задание на разработку системы ЗИ (информационной системы с разделом по ЗИ)**
Планирование работ	**Программа создания (совершенствования) системы ЗИ (план работ)**
Проведение работ и ввод объектов в эксплуатацию	**Аттестаты соответствия объектов информатизации, сертификаты средств защиты, акт о приемке, приказ о вводе**

Определение объектов защиты, объектов защиты информации, анализ потоков и хранилищ информации, каналов связи, определение угроз, оценка последствий (ущерба) в случаях реализации угроз безопасности, НСД, утечки информации или нарушений в работе ИС , содержащих информацию, отнесенную федеральными законами к информации ограниченного доступа

Анализ информации, обрабатываемой и хранимой на объектах информатизации, определение объектов, подлежащих защите

Оценка условий дислокации объекта, угроз безопасности информации

Оценка возможного ущерба в случаях утечки информации или нарушений в работе ИС

Предпроектное обследование

1.Определение перечня информации с ограниченным доступом, потоков, каналов и хранилищ информации.
2. Определение перечня элементов и ресурсов системы, подлежащих защите.

Определение угроз, модели нарушителя, слабых мест и возможных каналов утечки информации.

Предварительные расчеты (обоснование) ущерба в случаях утечки информации или нарушений в работе ИС основных програмно-технических и организационных мер по ЗИ)

Оценка масштаба основных работ, обоснование их необходимости, определение основных требований, предварительная оценка стоимости, выбор исполнителя работ

Определение основных направлений политики безопасности информации.

Определение основных требований к системе ЗИ.

1. Общесистемные требования
2. Функциональные требования
3. Технические требования
4. Экономические требования
5. Организационно-правовые требования
6. Требования к документации

Определение организационной структуры, целей и основных задач системы защиты информации

Определение перечня и уяснение требований нормативных правовых актов РФ, ведомственных нормативных документов, определение перечня организационно-распорядительных и других документов, регулирующих и определяющих правовой статус и организационный режим системы защиты информации органа власти (организации), подлежащих разработке.

Определение перечня основных организационных, инженерно-технических, технических и аппаратно-программных мер по предупреждению утечки информации или нарушений в работе ИС (по каждой угрозе)

Определение объема финансирования. (Предварительный расчет и обоснование затрат на проведение работ).

Определение формы реализации мероприятий по обеспечению безопасности информации (Целевая программа, годовое планирование и т.д.)

Разработка Концепции (политики) обеспечения безопасности информации в органе власти (организации)

- Целей и задач защиты информации
- Угроз безопасности информации
- Объектов защиты и объектов защиты информации (имущественные комплексы, ресурсы, элементы информационных систем, каналы, в том числе КСИИ). Оценка и обоснование их необходимости
- Состава и структуры системы защиты информации, реализующей цели и задачи
- Основных функций системы защиты информации
- Требований к системе защиты информации и ее функциональным элементам
- Основных работ в области, нормативных, организационных и технических мер по каждому направлению
- Архитектуры (облика) системы защиты информации.
- Показателей эффективности работы системы защиты информации, порядка проведения контроля за ее эффективностью.
- Формы реализации проекта (долгосрочная целевая программа, годовое планирование, финансирование отдельных работ и т. д.).

Выработка решения на создание (совершенствование) системы защиты информации

Разработка технического задания

Определение целей и задач защиты информации

Уяснение и определение угроз безопасности информации

Определение объектов защиты информации (ресурсы, системы, в том числе КСИИ), предварительная оценка их защищенности

Определение состава и структуры системы защиты информации, реализующей установленные цели и задачи

Определение основных функций системы защиты информации

Определение требований к системе защиты информации и ее функциональным элементам

Определение показателей эффективности работы системы защиты информации

Государственная политика в области обеспечения информационной безопасности

Политика ИБ - отношение государства к вопросам обеспечения своей безопасности в информационной сфере

Государственное регулирование:
- установление требований о защите информации;
- установление ответственности за нарушение Законов.

Законы

Субъекты регулирования органы власти, организации

Условия отнесения к информации с ограниченным доступом

Законы

Ограничение доступа к информации, определение перечня информации, доступ к которой ни при каких обстоятельствах не может быть ограничен

Кто (субъект) государство в соответствии с Конституцией, в части определения предметов ведения

Как: Только Федеральными Законами

Что: Только то, что определено в ФЗ

Цель - защита основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечение обороны страны и безопасности государства

Органы власти и организации Принимают правовые, организационные и технические меры по выполнению требований и соблюдению условий

Уполномоченные органы власти Организуют , обеспечивают и контролируют работу государственной системы защиты информации

Основополагающие принципы государственной политики при осуществлении ТЗИ

- Недопустимость нанесения ущерба безопасности Российской Федерации
- Обязательность указов и распоряжений Президента Российской Федерации по вопросам ТЗИ для исполнения всеми органами государственной власти, органами местного самоуправления и организациями
- Единство государственной политики в области ТЗИ
- Сочетание правовых, организационных, технических, экономических и специальных методов ТЗИ

Роль государственной системы ТЗИ в обеспечении национальной безопасности

Основные задачи по обеспечению национальной безопасности
(Доктрина национальной безопасности РФ)

Основные задачи государственной системы ТЗИ

Прогнозирование и выявление внутренних и внешних угроз

Анализ состояния и прогнозирование возможностей ТР и способов их применения

Реализация долгосрочных и оперативных мер по предупреждению и нейтрализации угроз

Формирование и проведение единой государственной политики по ТЗИ

Нормативное, методическое и информационное обеспечение работ по ТЗИ

Создание средств ТЗИ

Контроль состояния ТЗИ

Поддержание на достаточно высоком уровне военного потенциала государства

Исключение или существенное затруднение добывания информации ТР об образцах ВВТ, военных и оборонно -промышленных объектах, органах государственного и военного управления

Основные положения о государственной системе ТЗИ

(Извлечения из Постановления СМ-правительства РФ от 15.09.1993 г. № 912-51)

Положения обязательны при проведении работ по ЗИ, составляющие государственную или служебную тайну в органах государственной власти, в организациях и на предприятиях, независимо от организационно-правовой формы и формы собственности

Работы по ЗИ проводятся на основе актов законодательства РФ

ЗИ осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, НСД к ней, предупреждению преднамеренных программно-технических воздействий с целью уничтожения или искажения информации

Мероприятия по ЗИ являются составной частью управленческой, научной и производственной деятельности и осуществляются во взаимосвязи с другими мерами по обеспечению режима секретности

Основные задачи государственной системы защиты информации

- **Проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах**
- **Исключение или существенное затруднение добывания информации ТСР, а также предотвращение ее утечки по техническим каналам, НСД к ней, предупреждение программно-технических воздействий**
- **Принятие в пределах компетенции правовых актов, регулирующих отношения в области защиты информации**
- **Анализ возможностей ТСР, организация сил, создание средств ТЗИ и проведение контроля состояния защиты информации в органах государственной власти и на предприятиях**

Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» Утверждено постановлением Совета Министров - Правительства Российской Федерации от "15" сентября 1993 г. № 912-51.

Главные направления работ по защите информации

- Формирование и обеспечение эффективного управления системой защиты информации
- Анализ и оценка реальной возможности перехвата информации ТСР, НСД, выявление тех. каналов утечки.
- Разработка организационно-технических мероприятий по ЗИ и их реализация
- Определение сведений, охраняемых от технических средств разведки
- Организация и проведения контроля состояния ЗИ

Основные объекты защиты

- **Объекты органов государственного управления**
- **Объекты информационных систем**
- **Информационные ресурсы**
- **Органы государственной власти, органы местного самоуправления, организации, их деятельность, производимая в них продукция (работы и услуги) и возникающие при этом физические поля**

Основы организации и управления защитой информации

В основу организации защиты информации ограниченного доступа положен принцип разделения прав и обязанностей между субъектами обеспечения защищенности этой информации: государством; предприятиями, учреждениями и организациями; отдельными гражданами.

Государство как основной субъект обеспечения защиты информации через свои органы законодательной, исполнительной и судебной властей обеспечивает создание условий для осуществления защиты, а именно:

- создание системы правовых норм, регулирующих отношения в области защиты информации;
- проведение единой технической политики в этой области, координация и методическое руководство работами по защите информации, разработка технических норм и рекомендаций;
- разработка государственных программ по защите информации;
- общий контроль за состоянием защиты информации.

Предприятия и их объединения, учреждения и организации независимо от формы собственности, а также отдельные граждане, выполняющие работы, связанные с использованием информации ограниченного доступа, обеспечивают полностью их защиту.

Основы организации и управления защитой информации

Основными формами управления работами по защите информации являются:

- государственный заказ на проведение работ по защите информации;
- лицензирование деятельности предприятий и организаций по вопросам защиты информации;
- сертификация систем и средств информации и связи в части защищенности информации от утечки но техническим каналам, средств защиты и контроля;
- аттестование объектов по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием секретных сведений.

Для непосредственного выполнения функций по обеспечению защиты информации создается Государственная система защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам (ГСЗИ).

Возглавляет ГСЗИ - ФСТЭК России.

Важнейшими элементами ГСЗИ являются ФСБ, Министерство обороны которые в пределах своей компетенции имеют определенные цели к объекты защиты и располагают специфическими способами защиты.

Структура, функции и задачи этой системы, права и обязанности ее органов изложены в Положении о ГСЗИ.

Указ Президента Российской Федерации 16 августа 2004 года № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»

Определить, что Федеральная служба по техническому и экспортному контролю, ее территориальные органы и подведомственные ей организации являются правопреемниками Государственной технической комиссии при Президенте Российской Федерации, ее территориальных органов и подведомственных ей организаций.

ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации

ФСТЭК России является органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну.

ФСТЭК России организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях и руководит ею.

Из Положения о Федеральной службе по техническому и экспортному контролю

ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля.

ФСТЭК России является органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну.

ФСТЭК России организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях и руководит ею.

ФСТЭК России подведомственна Минобороны России.

Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации.

Обеспечение безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере

Организация разработки и представление на утверждение в установленном порядке перечней ключевых систем информационной инфраструктуры, а также требований к обеспечению безопасности информации в этих системах

Организация и осуществление экспертизы тактико-технических и технических заданий на создание ключевых систем информационной инфраструктуры, научно-техническое сопровождение и экспертиза работ по обеспечению безопасности информации в указанных системах в ходе их проектирования, строительства и эксплуатации

Осуществление контроля деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры

Ключевые информационные системы, составляющие критически важные сегменты информационной инфраструктуры Российской Федерации

- Системы органов управления государственной власти
- Системы органов управления правоохранительных структур
- Системы финансово-кредитной и банковской деятельности
- Системы предупреждения и ликвидации чрезвычайных ситуаций
- Географические и навигационные системы
- Сети связи общего пользования на участках, не имеющие резервных или альтернативных видов связи
- Системы специального назначения
- Спутниковые системы, используемые для обеспечения органов управления и в специальных целях
- **Системы управления добычей и транспортировкой нефти, нефтепродуктов и газа**
- Программно-технические комплексы центров управления взаимоувязанной сети связи
- Системы управления водоснабжением
- Системы управления энергоснабжением
- Системы управления транспортом (наземным, воздушным, морским)
- **Системы управления потенциально опасными объектами**
- Другие системы, нарушение штатного режима функционирования которых может привести к нарушению функций управления чувствительными процессами для РФ

Контроль состояния защиты информации в Российской Федерации

Важнейшей задачей организации защиты информации в РФ является контроль ее состояния, *который включает* контроль организации и эффективности проводимых мероприятий.

Основная цель контроля

обеспечение в субъектах РФ единой дисциплины в организации работ по защите информации, своевременное выявление предпосылок и предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, несанкционированных и непреднамеренных воздействий на защищаемую информацию и средства ее обработки

Контроль и надзор за обеспечением защиты информации ограниченного доступа

Контроль за обеспечением защиты информации ограниченного доступа

Разновидности контроля

Контроль состояния защиты информации

Контроль организации защиты информации

Контроль эффективности защиты информации

Контроль за созданием условий эффективной защиты информации

Надзор за обеспечением защиты информации ограниченного доступа

- Административный
- Прокурорский
- Судебный

Виды контроля

- Межведомственный
- Ведомственный
- Внутренний
- Предварительный
- Текущий
- Устранения недостатков

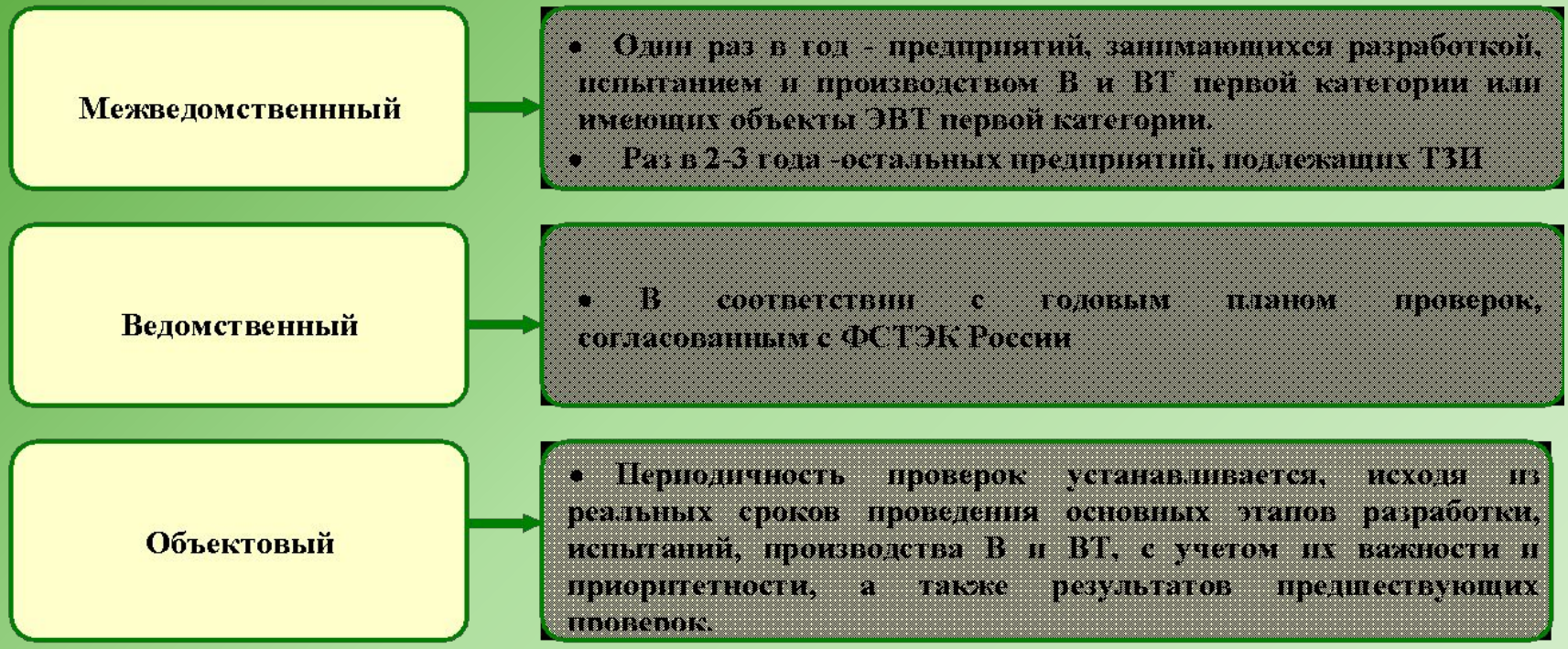
Методы контроля

- Технический
- Организационный

Формы контроля

- Инспектирование
- Экспертиза
- Сертификация
- Аттестация
- Специальные исследования
- Специальные проверки

Периодичность контроля состояния защиты информации



На органы объектового контроля возлагается:

- **проведение постоянного (повседневного) контроля состояния ПД ИТР и ТЗИ на предприятиях и организациях в целях обеспечения установленного порядка функционирования средств ПД ИТР и ТЗИ;**
- **соблюдение установленных режимов работы технических средств, в которых циркулирует защищаемая информация;**
- **выполнение установленных мер защиты и контроля за правильностью реализации правил разграничения доступа к информации на объектах информатизации;**
- **выявление и пресечение нарушений в области ПД ИТР и ТЗИ.**

Критические системы информационной инфраструктуры

- ФЕДЕРАЛЬНЫЙ ЗАКОН №187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» (вступает в силу с 1 января 2018 г.)

ФСТЭК РФ (2007 год):

- «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры»
- «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры»
- «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»

Секретарем Совета Безопасности 08.11.2005 утвержден документ "Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий".

Согласно этим документам Ключевые системы входят в состав следующих сегментов информационной инфраструктуры:

- системы органов государственной власти
- системы органов управления правоохранительных структур
- системы финансово-кредитной и банковской деятельности
- системы предупреждения и ликвидации чрезвычайных ситуаций
- географические и навигационные системы
- сети связи общего пользования на участках, без резервных видов связи
- системы специального назначения
- спутниковые системы для обеспечения органов управления и в спец. целях
- системы управления добычей и транспортировкой нефти, нефтепродуктов и газа
- программно-технические комплексы центров управления
- системы управления водоснабжением и энергоснабжением
- системы управления транспортом (наземным, воздушным, морским)
- системы управления потенциально опасными объектами.

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (2012 год)

Целью государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации является снижение до минимально возможного уровня рисков неконтролируемого вмешательства в процессы функционирования данных систем, а также минимизация негативных последствий подобного вмешательства.

Доктрина информационной безопасности Российской Федерации Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646

33 статья.

…Участниками системы обеспечения информационной безопасности являются: **собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.**

Стратегия развития информационного общества в российской федерации на 2017 - 2030 годы

1 раздел, 4 пункт:

м) **объекты критической информационной инфраструктуры - информационные системы и информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, в сфере здравоохранения, транспорта, связи, в кредитно-финансовой сфере, энергетике, топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленности;**

Утверждена Указом Президента Российской Федерации от 9 мая 2017 г. N 203

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (2012 год)

Критически важный объект инфраструктуры Российской Федерации (далее - критически важный объект) - объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта Российской Федерации либо административно-территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок

УКАЗ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ О СОЗДАНИИ ГОСУДАРСТВЕННОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ (15.01.2013 №31С)

Возложить на Федеральную службу безопасности Российской Федерации полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации - информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.

УКАЗ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ О СОЗДАНИИ ГОСУДАРСТВЕННОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ (15.01.2013 №31С)

Определить основными задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации:

а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

б) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

УКАЗ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ О СОЗДАНИИ ГОСУДАРСТВЕННОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ (15.01.2013 №31С)

Федеральная служба безопасности Российской Федерации:

а) организует и проводит работы по созданию государственной системы, осуществляет контроль за исполнением этих работ, а также обеспечивает во взаимодействии с государственными органами функционирование ее элементов;

б) разрабатывает методику обнаружения компьютерных атак на информационные системы и информационно-телекоммуникационные сети государственных органов и по согласованию с их владельцами - на иные информационные системы и информационно-телекоммуникационные сети;

в) определяет порядок обмена информацией между федеральными органами исполнительной власти о компьютерных инцидентах, связанных с функционированием информационных ресурсов Российской Федерации;

г) организует и проводит в соответствии с законодательством Российской Федерации мероприятия по оценке степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

д) разрабатывает методические рекомендации по организации защиты критической информационной инфраструктуры Российской Федерации от компьютерных атак;

е) определяет порядок обмена информацией между федеральными органами исполнительной власти и уполномоченными органами иностранных государств (международными организациями) о компьютерных инцидентах, связанных с функционированием информационных ресурсов, и организует обмен такой информацией.

Органы лицензирования в информационной сфере и область их деятельности

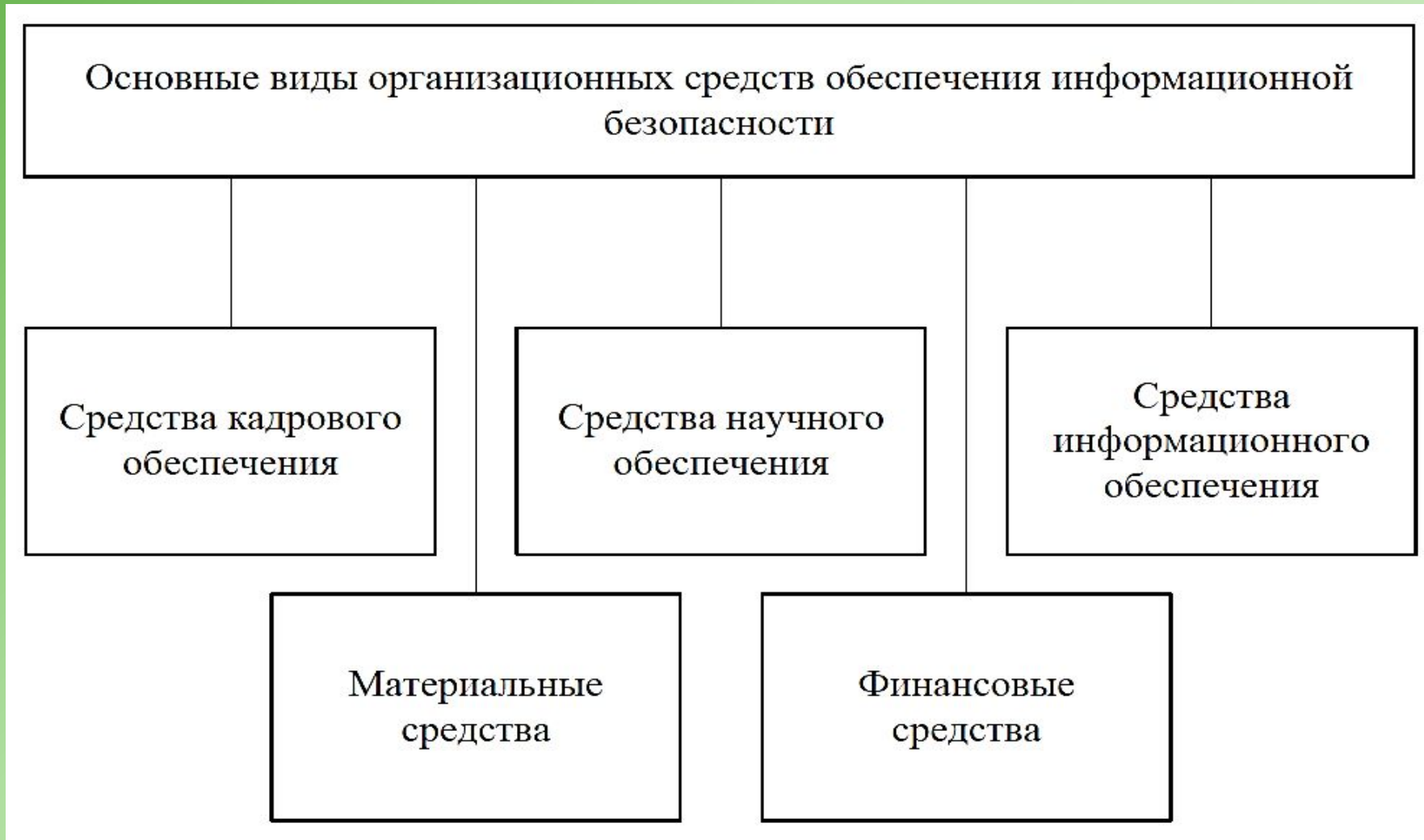
Вид деятельности	Лицензирующие органы России			
	ФСБ	ФСТЭК	ФНС	Роскомнадзор
А	+			
Б	+			
В	+			
Г	+	+		
Д		+		
Е			+	
Ж				+
З				+
И				+

- А – разработка, производство, распространение шифровальных средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных средств.
- Б – разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации.
- В – деятельность по выявлению электронных устройств, предназначенных для негласного получения информации.
- Г – разработка и производство средств защиты конфиденциальной информации.
- Д – деятельность по технической защите конфиденциальной информации.
- Е – производство и реализация защищенной от подделок полиграфической продукции.
- Ж – оказание услуг связи.
- З – телевизионное вещание и радиовещание.
- И – деятельность по изготовлению экземпляров аудиовизуальных произведений, программ для электронных вычислительных машин, баз данных и фонограмм на любых видах носителей.

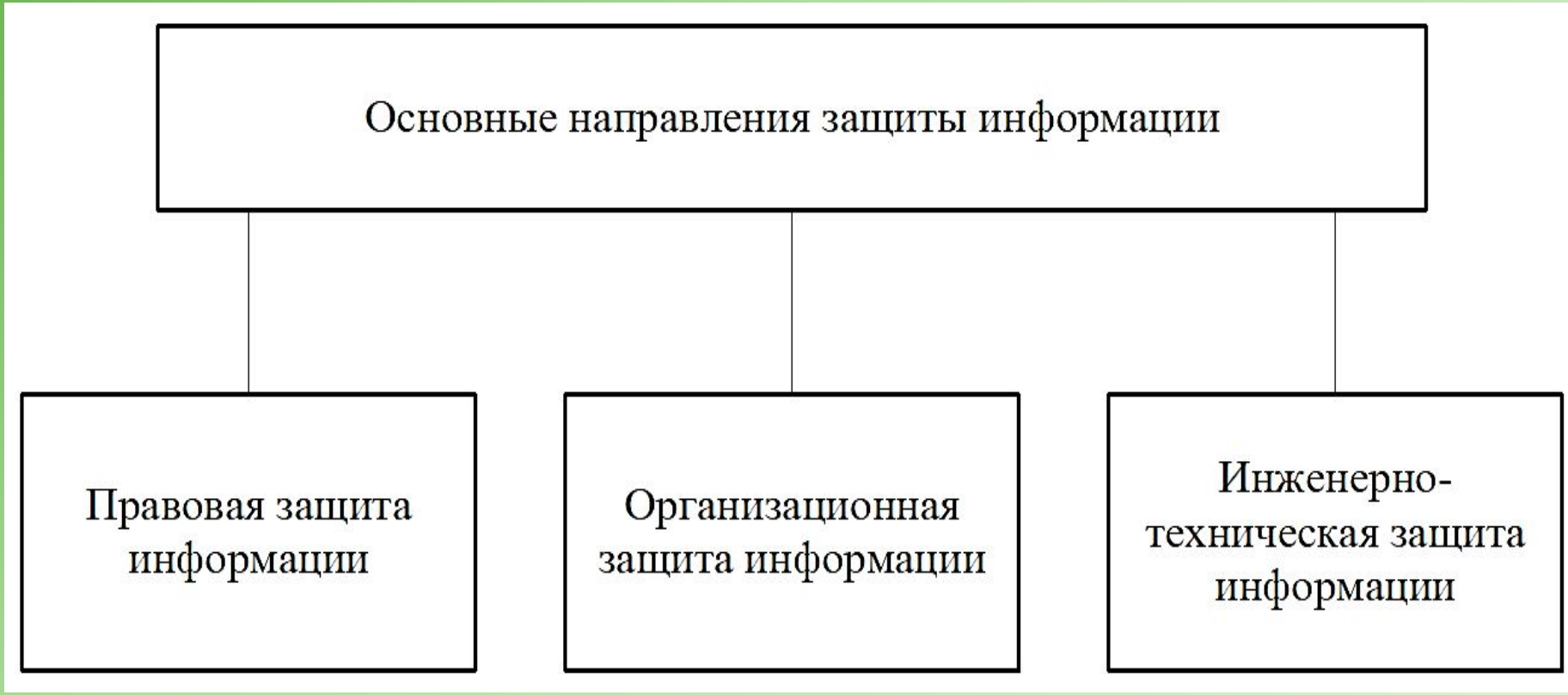
Структура понятия «обеспечение информационной безопасности»

- Таким образом, **обеспечение информационной безопасности** есть совокупность деятельности по недопущению вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой, а также средств и субъектов этой деятельности.
- ***Деятельность по обеспечению информационной безопасности*** - комплекс планируемых и проводимых в целях защиты информационных ресурсов мероприятий, направленных на ликвидацию угроз информационной безопасности и минимизацию возможного ущерба, который может быть нанесен объекту безопасности вследствие их реализации.
- Под **субъектами обеспечения информационной безопасности** понимаются государственные органы, предприятия, должностные лица, структурные подразделения, принимающие непосредственное участие в организации и проведении мероприятий по обеспечению информационной безопасности.
- ***Средства, с помощью которых достигаются цели деятельности по обеспечению информационной безопасности***, - это системы, объекты, способы, методы и иные механизмы непосредственного решения задач обеспечения ин-формационной безопасности. Прежде всего, они представляют собой совокупность правовых и организационных средств обеспечения информационной без-опасности.

Основные виды организационных средств обеспечения информационной безопасности



Основные направления защиты информации



Основные направления организационной защиты информации

Основные принципы организационной защиты информации

- Принцип комплексного подхода заключается в использовании сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факто-ров, ослабляющих или усиливающих угрозу возможной утечки конфиденциальной информации.
- Принцип оперативности принятия управленческих решений существенно влияет на эффективность функционирования и гибкость системы защиты ин-формации и отражает целеустремленность должностных лиц на решение задач защиты информации.
- Принцип персональной ответственности заключается в наиболее эффективном и полном распределении сил структурных подразделений предприятия, участвующих в процессе защиты информации.

Структура системы защиты информации

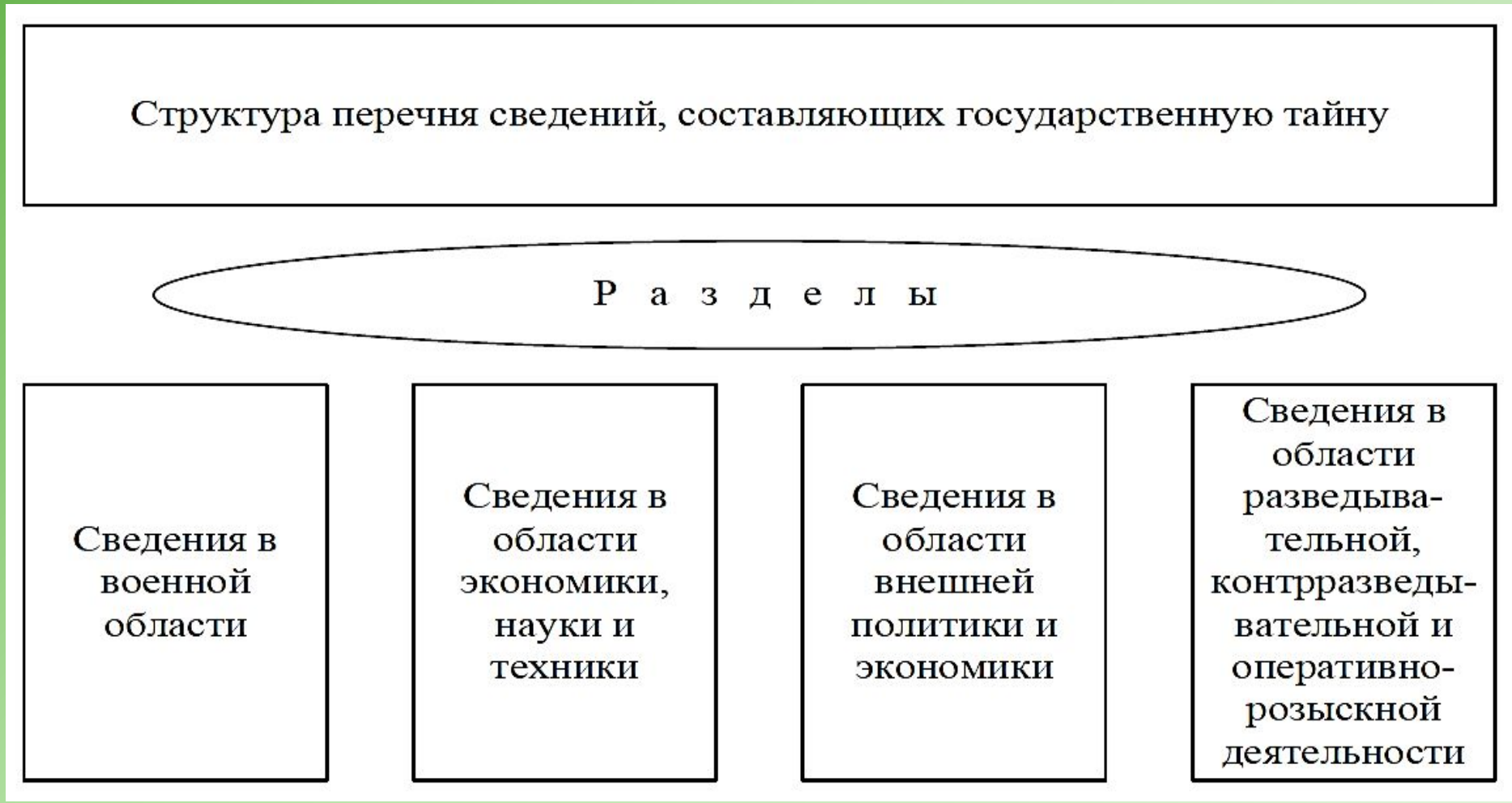
Система защиты информации должна отвечать совокупности следующих основных требований, то есть быть:

- ***централизованной*** - соответствующей эффективному процессу управления системой со стороны руководителя и ответственных должностных лиц по направлениям деятельности предприятия;
- ***плановой*** - объединяющей усилия различных должностных лиц и структурных подразделений при их участии в организации и обеспечении выполнения задач, стоящих перед предприятием;
- ***конкретной и целенаправленной*** - защите должны подлежать абсолютно конкретные информационные ресурсы, представляющие интерес для конкурирующих организаций;
- ***активной*** - обеспечивать защиту информации с достаточной степенью настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия;
- ***надежной и универсальной*** - охватывать весь комплекс деятельности предприятия, связанной с созданием и обменом информацией.

Сведения, отнесенные к государственной тайне, по степени секретности подразделяются на три группы.

- К сведениям ***особой важности*** следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.
- К ***совершенно секретным*** сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.
- К ***секретным*** сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

Структура перечня сведений, составляющих государственную тайну



Вместе с тем, в соответствии со статьей 7 Закона РФ "О государственной тайне", не подлежат отнесению к государственной тайне и засекречиванию сведения:

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

- о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

- о фактах нарушения прав и свобод человека и гражданина;

- о размерах золотого запаса и государственных валютных резервах Российской Федерации;

- о состоянии здоровья высших должностных лиц Российской Федерации;

- о фактах нарушения законности органами государственной власти и их должностными лицами.