Основы информационной безопасности в Российской Федерации

Сомов Юрий Иванович
Лашков Александр Евгеньевич

Цель дисциплины:

обучение студентов соблюдению установленных требований по обеспечению информационной безопасности при осуществлении профессиональной деятельности должностными лицами таможенных органов Российской Федерации.

Задачи изучения дисциплины:

- освоение основных понятий в сфере обеспечения информационной безопасности;
- изучение основ организации обеспечения информационной безопасности в Российской Федерации;
- ознакомление с основами организации обеспечения информационной безопасности в таможенных органах Российской Федерации;
- изучение основных методов обеспечения информационной безопасности.

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВПО по специальности 036401.65 «Таможенное дело»:

профессиональных (ПК):

способен понимать сущность и значение информации в развитии современного информационного общества, соблюдать основные требования информационной безопасности (ПК-3);

умение оценить угрозы экономической и иных видов национальной безопасности Российской Федерации и реализовать меры по их предупреждению или устранению (ПК-26);

По завершении изучения дисциплины студент должен:

знать:

- основные требования руководящих документов по обеспечению информационной безопасности Российской Федерации;
- основные угрозы информационной безопасности;
- основные методы обеспечения информационной безопасности и защиты информации;
- основы организации обеспечения информационной безопасности в РФ;

По завершении изучения дисциплины студент должен:

уметь:
анализировать угрозы информационной безопасности и выявлять уязвимости информационных систем;
применять на практике модель нарушителя информационной безопасности;

По завершении изучения дисциплины студент должен:

владеть навыками и приемами: управления политикой безопасности информационной системы.

ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы	Всего часов	Семестр 7
Аудиторные занятия	28	28
в том числе:		
Лекции (Л)	8	8
Практические занятия (С+ПЗ)	16+4	16+4
в том числе в интерактивной форме	12	12
Самостоятельная работа	44	44
Подготовка к контрольным работам	12	12
Работа с источниками	8	8
Выполнение и защита практических заданий	24	24
Форма промежуточной аттестации (зачет)		
Общая трудоемкость: часы	72	72
зачетные единицы	2	2

- Зачем нужна информационная безопасность?
- И нужна ли она вообще?
- Почему нужно выполнять дополнительные к основной работе мероприятия по информационной безопасности , неудобные и неприятные?

	До	После
Знания о материале		
Полезность материала		

Основные положения обеспечения информационной безопасности в Российской Федерации

лекция

Учебные вопросы

1. Государственная политика Российской Федерации в области обеспечения информационной безопасности.
2. Основные понятия в сфере обеспечения информационной безопасности
3. Государственная тайна, коммерческая тайна, банковская тайна, служебная тайна
4. Лицензирование и сертификация в области защиты информации.
5. Особенности организации обеспечения информационной безопасности в таможенных органах Российской Федерации.

1. Государственная политика Российской Федерации в области обеспечения информационной безопасности.

Роль и значение информационных революций

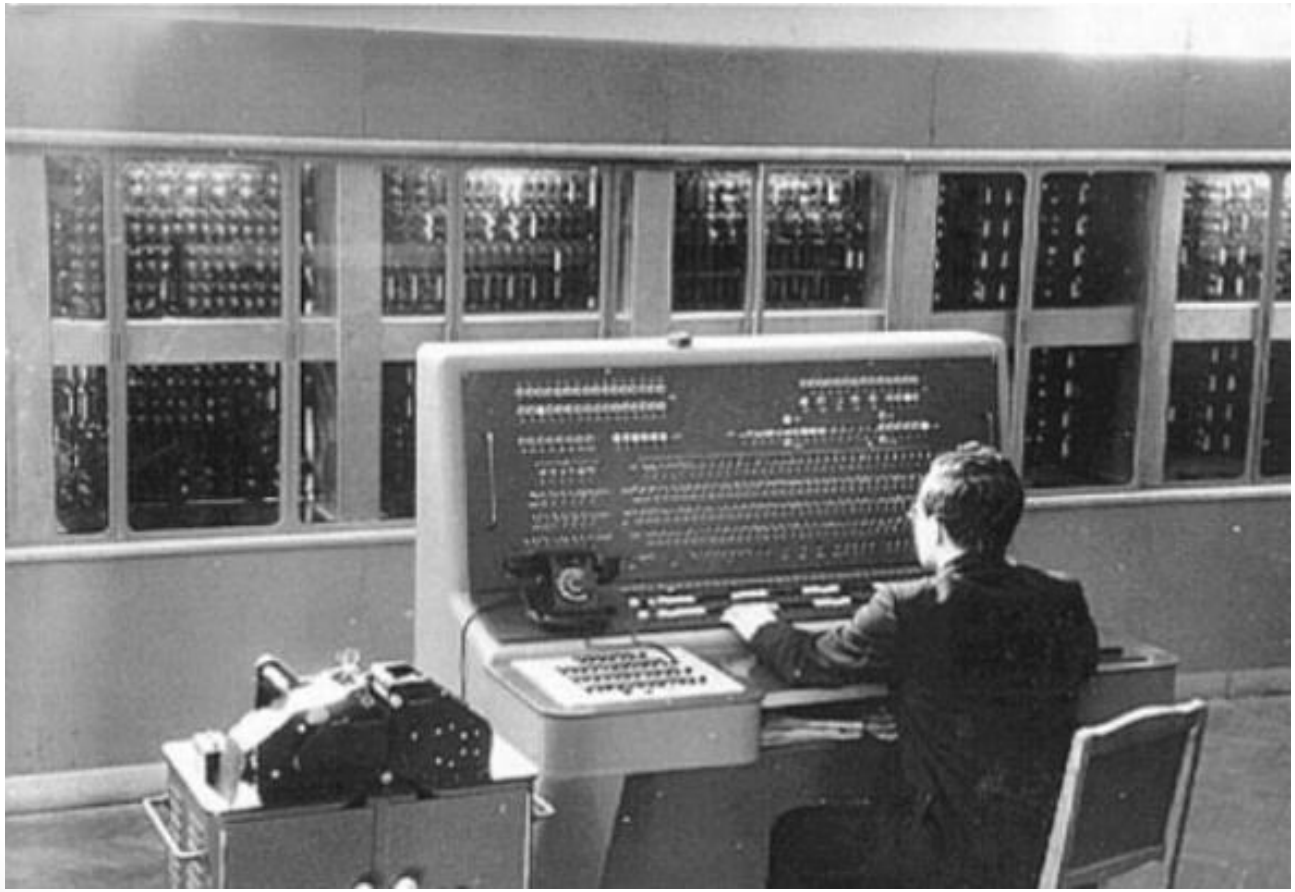
- **Первая революция** связана с изобретением письменности, что привело к гигантскому качественному и количественному скачку. Появилась возможность передачи знаний от поколения к поколениям.
- **Вторая** (середина XVI в.) вызвана изобретением книгопечатания, которое радикально изменило индустриальное общество, культуру, организацию деятельности.
- **Третья** (конец XIX в.) обусловлена изобретением электричества, благодаря которому появились телеграф, телефон, радио, позволяющие оперативно передавать и накапливать информацию в любом объеме.

Четвертая (70-е гг. XX в.) связана с изобретением микропроцессорной технологии и появлением персонального компьютера. На микропроцессорах и интегральных схемах создаются компьютеры, компьютерные сети, системы передачи данных (информационные коммуникации).

Этот период характеризуют три фундаментальные инновации:

- переход от механических и электрических средств преобразования информации к электронным;
- миниатюризация всех узлов, устройств, приборов, машин;
- создание программно-управляемых устройств и процессов.

ЭВМ 1-е поколение (начало 50-х гг.). Элементная база – электронные лампы. ЭВМ отличались большими габаритами, большим потреблением энергии, малым быстродействием, низкой надежностью, программированием в кодах



2-е поколение (с конца 50-х гг.). Элементная база – полупроводниковые элементы. Улучшились по сравнению с ЭВМ предыдущего поколения все технические характеристики. Для программирования используются алгоритмические языки

3-е поколение (начало 60-х гг.). Элементная база – интегральные схемы, многослойный печатный монтаж. Резко снижение габаритов ЭВМ, повышение их надежности, увеличение производительности. Доступ с удаленных терминалов

4-е поколение (с середины 70-х гг.). Элементная база – микропроцессоры, большие интегральные схемы. Улучшились технические характеристики. Массовый выпуск персональных компьютеров. Направления развития: мощные многопроцессорные вычислительные системы с высокой производительностью, создание дешевых микроЭВМ

5-е поколение (с середины 80-х гг.). Началась разработка интеллектуальных компьютеров, пока не увенчавшаяся успехом. Внедрение во все сферы компьютерных сетей и их объединение, использование распределенной обработки данных, повсеместное применение компьютерных информационных технологий.

- Проблемой обеспечения информационной безопасностью человечество занималось всегда.
- Но! Обострилась она с приходом в нашу жизнь информационной коммуникационных технологий!

Сущность проблемы информационной безопасности общества обусловлена противоречием между объективным развитием информационных технологий и информационных систем и их стремительно возрастающей ролью для развития общества, с одной стороны, и столь же стремительным увеличением как объективных, так и субъективных угроз для общественной жизни, связанных с их использованием.

Отправной точкой для определения роли информационной безопасности в системе национальной безопасности России является **Доктрина информационной безопасности Российской Федерации,** утвержденная Президентом Российской Федерации 9 сентября 2000 г.

В **Стратегии национальной безопасности Российской Федерации до 2020** года подчеркивается, что в современном мире усиливается глобальное информационное противоборство, а также совершенствуются формы противоправной деятельности в кибернетической областях и в сфере высоких технологий, способные повлиять на развитие всех сфер общественной жизни.

Информационная безопасность в силу её значительного влияния на ключевые сферы общественной жизни и функционирование государственных органов становится в современных условиях одной из самостоятельных составляющих национальной безопасности РФ, содержание которой связано с необходимостью обеспечить защиту информационных ресурсов, систем их формирования, распространения и использования, информационной инфраструктуры, право на

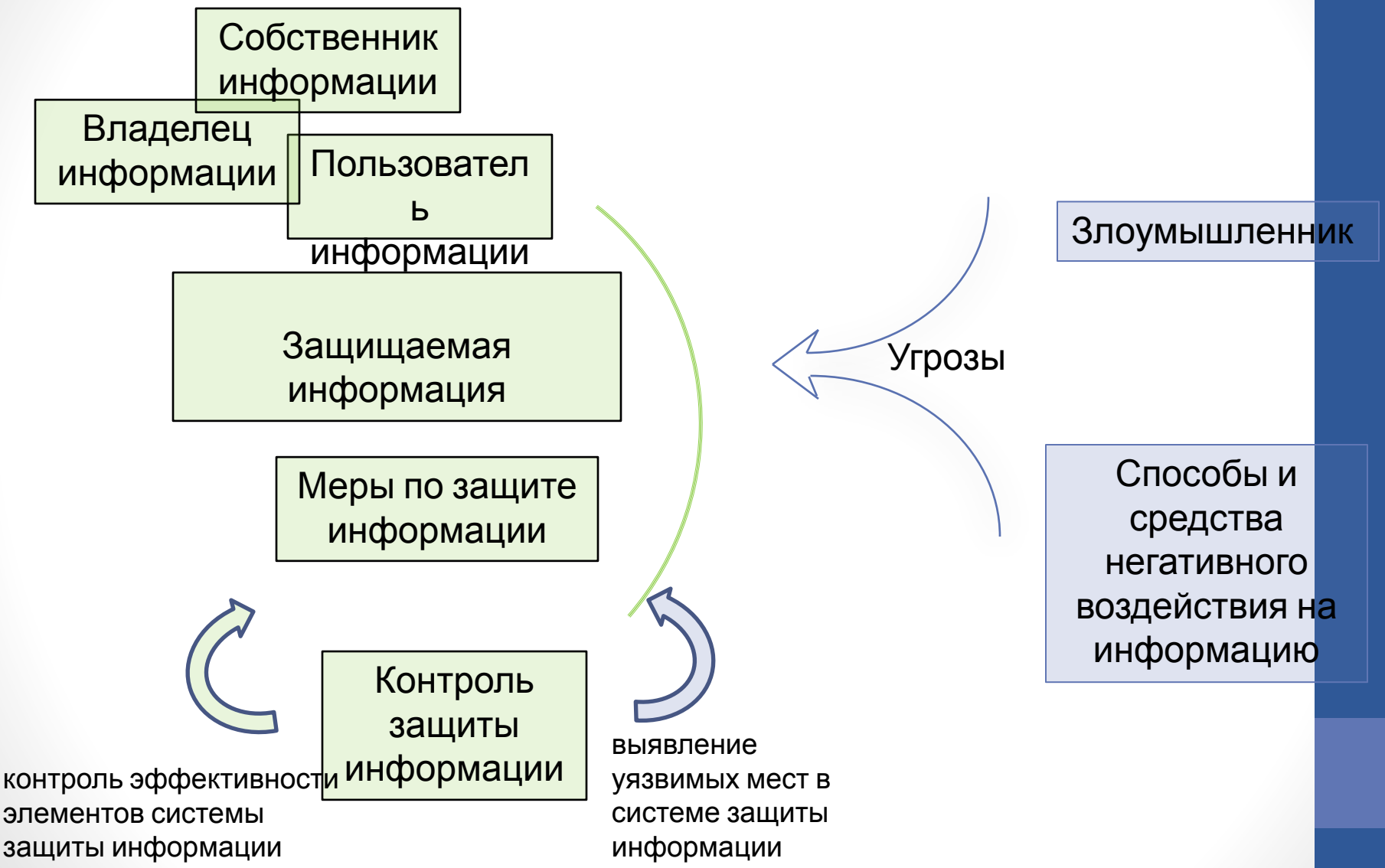
- В ФТС России разработана **Концепция обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года**, целью которой является совершенствование созданной в Федеральной таможенной службе ведомственной системы обеспечения информационной безопасности при реализации политики Российской Федерации в сфере обеспечения информационной безопасности и защиты информации и при выполнении предписаний правовых актов Российской Федерации в сфере таможенной деятельности, обеспечения информационной безопасности и защиты информации, а также при выполнении правовых актов Таможенного союза

Основные направления практической деятельности таможенных органов по обеспечению информационной безопасности и технической защиты информации

- Обеспечение регулируемого доступа к информационным ресурсам таможенных органов;
- Управление и контроль пользования должностными лицами электронной подписью:
- Выполнение комплексных мер по защите информации, включая антивирусную защиту;
- Контроль соблюдения мер защиты информации.

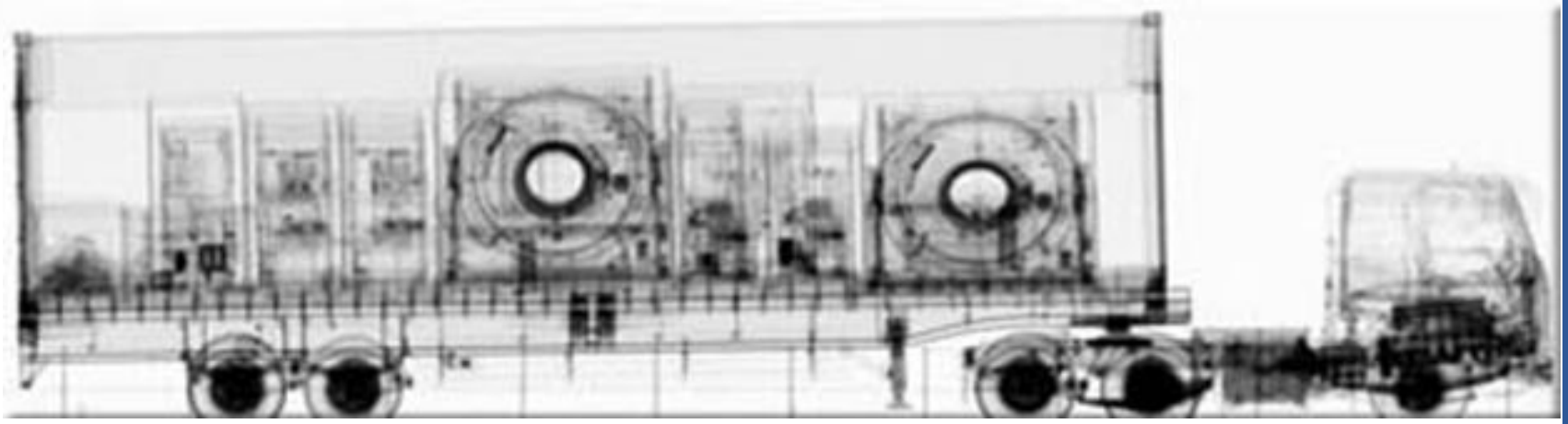
Модель защиты информации

Модель защиты информации




Субъект, имеющий легальный доступ к информации
Защищаемая информация
Носители защищаемой информации
Угрозы защищаемой информации
Способы и средства защиты информации, включая контроль
Характеристики субъекта, имеющего легальный доступ к информации
Мониторинг ценности защищаемой информации
Учёт этапов жизненного цикла носителя защищаемой информации
Ранжирование угроз защищаемой информации по степени опасности
Выбор достаточных способов и средств защиты от угроз за минимальную цену

Рентгеновское изображение загруженного кузова автомобиля, полученное с применением ИДК



2. Основные понятия в сфере обеспечения информационной безопасности

ГОСТ Р 50922-2006
Защита информации
ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1 Область применения

Настоящий стандарт устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации.

Термины, установленные настоящим стандартом, рекомендуется использовать в правовой, нормативной, технической и организационно-распорядительной документации, научной, учебной и справочной литературе.

Защита информации; ЗИ
(определение)

Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита информации

- правовая
- техническая
- криптографическая
- физическая

Правовая защита информации

- Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Техническая защита информации; ТЗИ:

- Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Криптографическая защита информации

- Защита информации с помощью ее криптографического преобразования.

Физическая защита информации

- Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Способ защиты информации

- Порядок и правила применения определенных принципов и средств защиты информации.

Защита информации от утечки

- Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.
- Примечание - Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации от несанкционированного воздействия; ЗИ от НСВ:

- Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

Защита информации от разглашения

- Защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа; ЗИ от НСД

- Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Замысел защиты информации

- Основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Цель защиты информации

Заранее намеченный результат защиты информации.

Примечание - Результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Система защиты информации

- Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

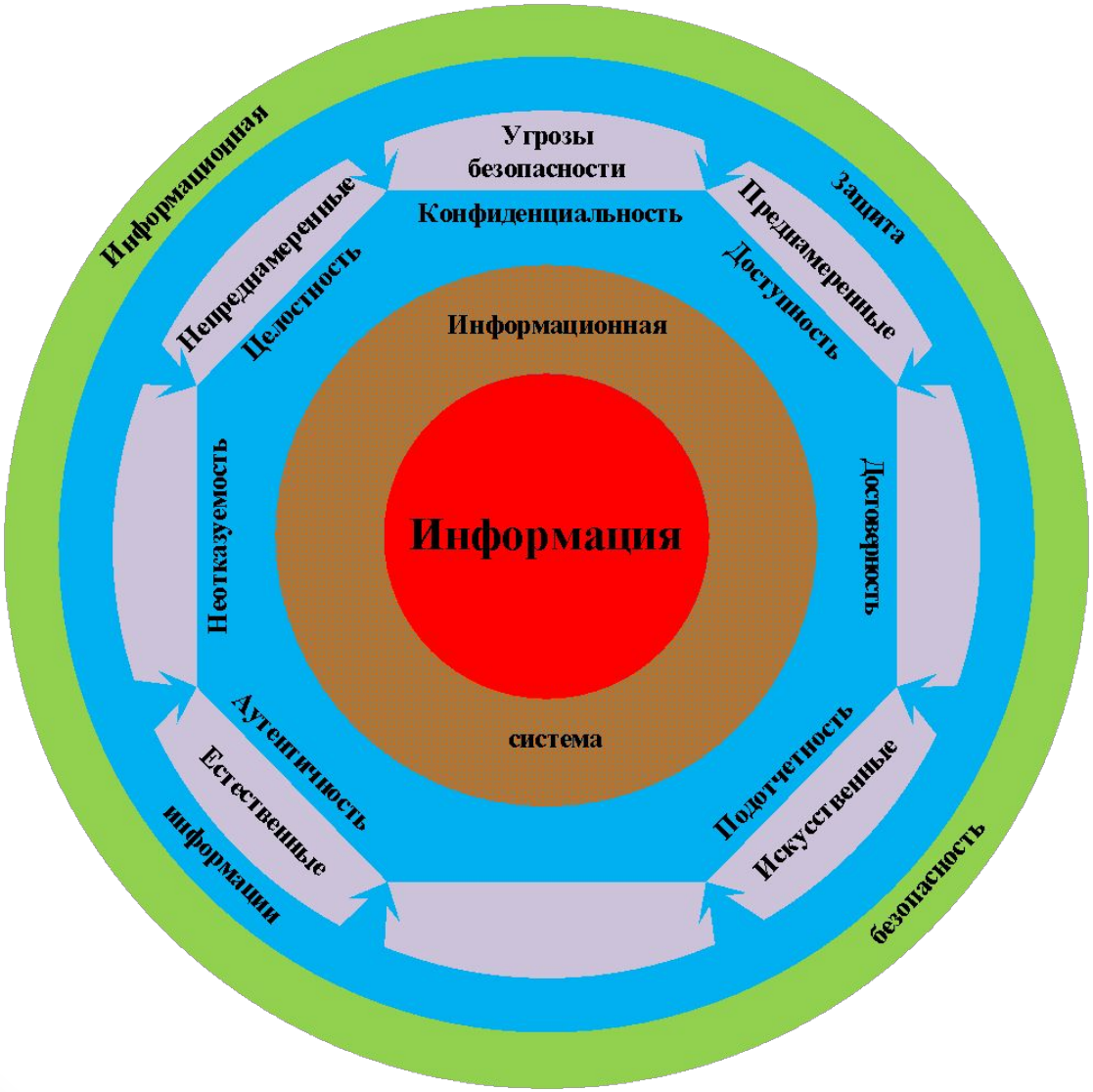
Политика безопасности (информации в организации)

Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Безопасность информации [данных]

- Состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

Соотношение понятий информационная безопасность и защита информации



Доступность информации – это свойство информации или информационной услуги, характеризующее возможность её получения за определенное время или по мере необходимости.

Целостность информации – свойство информации, характеризующее её существование в исходном виде (заданном владельцем или пользователем), то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Конфиденциальность информации – свойство информации, характеризующее её доступность только авторизованным пользователям или процессам.

Неотказуемость – свойство информации или информационной системы, характеризующее её способность удостоверить имевшее место событие или действие, а также авторство так, чтобы эти события или действия, равно как и авторство, не могли быть позже поставлены под сомнение ни одной из сторон.

Подотчетность – свойство информационной системы, включая и информацию, характеризующее её способность идентифицировать субъект информационной системы и регистрировать его действия.

Аутентичность – свойство информации и субъектов информационной системы, характеризующее их идентичность заявленным.

Достоверность информации – свойство информации, характеризующее степень её соответствия реальному событию, состоянию или поведению.

Защищаемая информация

- Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
- Примечание - Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Носитель защищаемой информации:

- Физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Угроза (безопасности информации)

- Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Источник угрозы безопасности информации

- Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Уязвимость (информационной системы); *брешь*

- Свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.
- **Примечания:**

I. Условием реализации угрозы безопасности обрабатываемой в системе информации может быть недостаток или слабое место в информационной системе.

II. Если уязвимость соответствует угрозе, то существует риск.

Вредоносная программа

- Программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы.

Модель угроз (безопасности информации)

Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Примечание - Видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ.

Техника защиты информации

Средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Средство защиты информации

Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

3. Государственная тайна, коммерческая тайна, банковская тайна, служебная тайна

Понятие тайны

Законодатель достаточно часто оперирует термином «тайна» и семантически созвучными с ним терминами «конфиденциальный», «секретный» и т.п. . Используемый в текстах нормативно-правовых актов термин «тайна» с прилагательными типа «коммерческая», «служебная», «банковская», «аудиторская», «врачебная», «государственная» и т. п., употребляется как синоним сведений, которые неизвестны или должны быть неизвестны третьим лицам. К **секретной информации** в настоящее время принято относить сведения, содержащие **государственную тайну**.

Информации, находящейся в тайне и относимой в разряд как конфиденциальной, так и государственной тайны, присущ ряд признаков, в числе которых выделяются:

- важность (ценность) скрываемых сведений, которая обусловлена спецификой их содержания и/или фактором их неизвестности третьим лицам;
- отсутствие свободного доступа к сведениям на законных к тому основаниях;
- наличие превентивных мер, принимаемых обладателем сведений к охране их от доступа третьих лиц.

Федеральный закон «О коммерческой тайне», например, использует такое понятие: «Разглашение информации, составляющей коммерческую тайну, – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной ферме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору».

Государственная тайна

Мера важности отдельных групп сведений, которые прямо влияют на безопасность государства, предопределяет необходимость выделения их в отдельный блок информации, подлежащей нахождению в режиме государственной тайны.

Установление подобного режима является одним из существенных факторов обеспечения безопасности страны.

Согласно Закону РФ «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». Перечень сведений, отнесенных к государственной тайне, определен специальным Указом Президента Российской Федерации от 30.11.1995 № 1203 (действует в последней редакции от 26.09.2013).

На носители сведений, составляющих государственную тайну, «в обязательном порядке наносятся реквизиты о степени секретности содержащихся в носителе сведений». В соответствии с нормами Закона «О государственной тайне» установлены три степени секретности сведений, находящихся в режиме государственной тайны: **«Особой важности»** – наивысшая степень секретности, **«Совершенно секретно»** и **«Секретно»,** и три соответствующие этим степеням секретности грифа для носителей сведений, составляющих государственную тайну (материальных объектов, в том числе физических полей, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов). **Использование грифов секретности, установленных Федеральным законом «О государственной тайне», для засекречивания сведений, не отнесенных к государственной тайне, не допускается.**

По общему правилу, должностные лица и граждане знакомятся только с теми сведениями, составляющими государственную тайну, которые необходимы им для выполнения должностных (функциональных) обязанностей.

«Доступ к сведениям, составляющим государственную тайну, – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну». Обязательным условием доступа к сведениям, составляющим государственную тайну, является наличие у лица оформленного допуска по форме, соответствующей степени секретности сведений.

При этом соответствующие сведения могут считаться государственной тайной (могут быть засекречены), если они отвечают следующим требованиям:

– соответствуют перечню сведений, составляющих государственную тайну, перечню сведений, не подлежащих засекречиванию, и законодательству Российской Федерации о государственной тайне (принцип законности);

– целесообразность их засекречивания установлена путем экспертной оценки вероятных экономических и иных последствий, возможности нанесения ущерба безопасности Российской Федерации, исходя из баланса жизненно важных интересов государства, общества и личности (принцип

– ограничения на распространение этих сведений и на доступ к ним установлены с момента их получения (разработки) или заблаговременно (принцип своевременности);
– компетентные органы и их должностные лица приняли в отношении конкретных сведений решение об отнесении их к государственной тайне и засекречивании и установили в отношении этих сведений соответствующий режим правовой охраны и защиты (принцип обязательной защиты).

Исходя из конституционных прав и законных интересов граждан и общества, устанавливаются и изъятия из этого перечня, а именно не подлежат отнесению к государственной тайне и засекречиванию следующие 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

- о привилегиях, компенсациях и социальных гарантиях, 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.

Конфиденциальная информация

В действующем сегодня российском законодательстве отсутствует единое понятие конфиденциальной информации, равно как и четкое определение ее структурного состава. Так, согласно Федеральному закону «Об информации, информатизации и защите информации» и Федерального закона «Об участии в международном информационном обмене», в качестве конфиденциальной признается «документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации».

Указом Президента Российской Федерации от 06.03.1997 № 188 (ред. от 23.09.2005) был утвержден перечень сведений «конфиденциального характера» , где указаны 6 видов такой информации:

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, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20.08.2004 № 119ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации (в ред. Указа Президента

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).
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

Служебная тайна

По Указу Президента РФ от 06.03.1997 № 188 доступ к служебным сведениям ограничивается органами государственной власти.

В действующих законах определены некоторые категории, которые по своему характеру приближены к понятию «служебная тайна», например, Федеральный закон от 21.07.1997 № 114ФЗ (ред. от 02.07.2013) «О службе в таможенных органах Российской Федерации» (ст. 7, 17 служебная тайна – служебная информация сотрудника таможенного органа).

Банковская тайна

Банковская тайна – это защищаемые банками и иными кредитными организациями сведения о банковских операция по счетам и сделкам в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также сведения о клиентах и корреспондентах, разглашение которых может нарушить их право на неприкосновенность частной жизни.

4. Лицензирование и сертификация в области защиты информации.

Лицензирование в области защиты информации

Деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ.

Лицензия - специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.

Лицензиат - юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности.

Соискатель лицензии - юридическое лицо или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии на осуществление конкретного вида деятельности.

Лицензирующие органы - федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с настоящим Федеральным законом.

В соответствии с законом, к ***лицензируемым видам деятельности*** относятся, виды деятельности, осуществление которых может повлечь за собой ***нанесение ущерба*** правам, законным интересам, здоровью граждан, обороне и безопасности государства, культурному наследию народов Российской Федерации и регулирование которых не может осуществляться иными методами, кроме как лицензированием.

Основным законодательным актом, регулирующим отношения, возникающие между федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, юридическими лицами и индивидуальными предпринимателями в связи с осуществлением лицензирования отдельных видов деятельности, является Федеральный закон от 8 августа 2001 года № 128-ФЗ «О лицензировании отдельных видов деятельности».

Лицензирование - мероприятия, связанные с:

- предоставлением лицензий;
- переоформлением документов, подтверждающих наличие лицензий;
- приостановлением действия лицензий в случае административного приостановления деятельности лицензиатов за нарушение лицензионных требований и условий;
- возобновлением или прекращением действия лицензий;
- аннулированием лицензий;
- контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий;
- ведением реестров лицензий;
- предоставлением в установленном порядке заинтересованным лицам сведений из реестров лицензий и иной информации о лицензировании.

Перечень видов деятельности, на осуществление которых требуются лицензии в сфере обеспечения информационной безопасности :

- деятельность по распространению шифровальных (криптографических) средств;
- деятельность по техническому обслуживанию шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

Перечень видов деятельности, на осуществление которых требуются лицензии:

- деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

- деятельность по разработке и (или) производству средств защиты конфиденциальной информации;

- деятельность по технической защите конфиденциальной информации;

- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Перечень федеральных органов исполнительной власти, осуществляющих лицензирование определяется Постановлением Правительства Российской Федерации от 26 января 2006 г. № 45 «Об организации лицензирования отдельных видов деятельности».

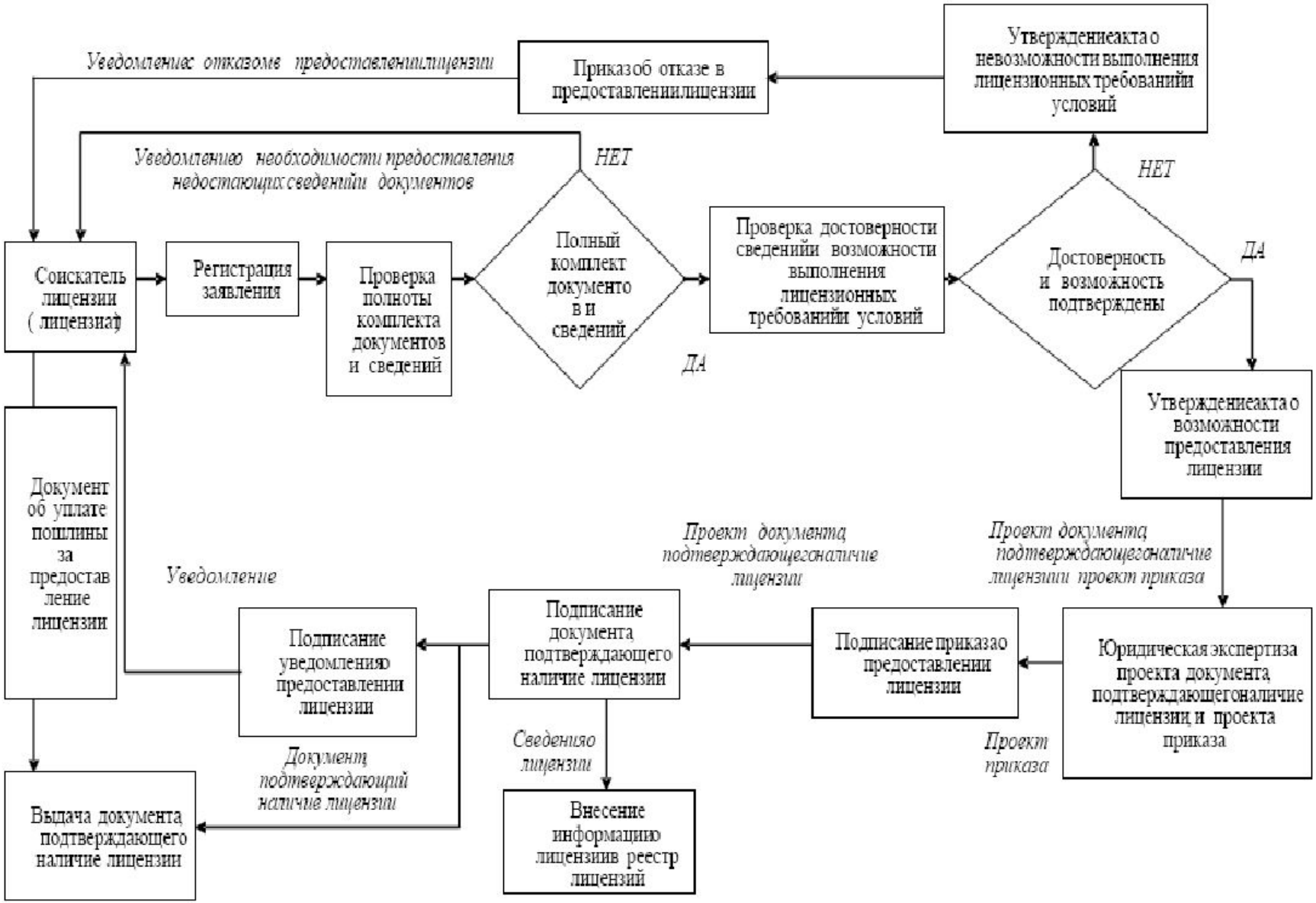
Порядок лицензирования отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами

- ✔ «Положение о лицензировании деятельности по распространению шифровальных (криптографических) средств»;
- ✔ «Положение о лицензировании деятельности по техническому обслуживанию шифровальных (криптографических) средств»;
- ✔ «Положение о лицензировании предоставления услуг в области шифрования информации»;
- ✔ «Положение о лицензировании разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем».

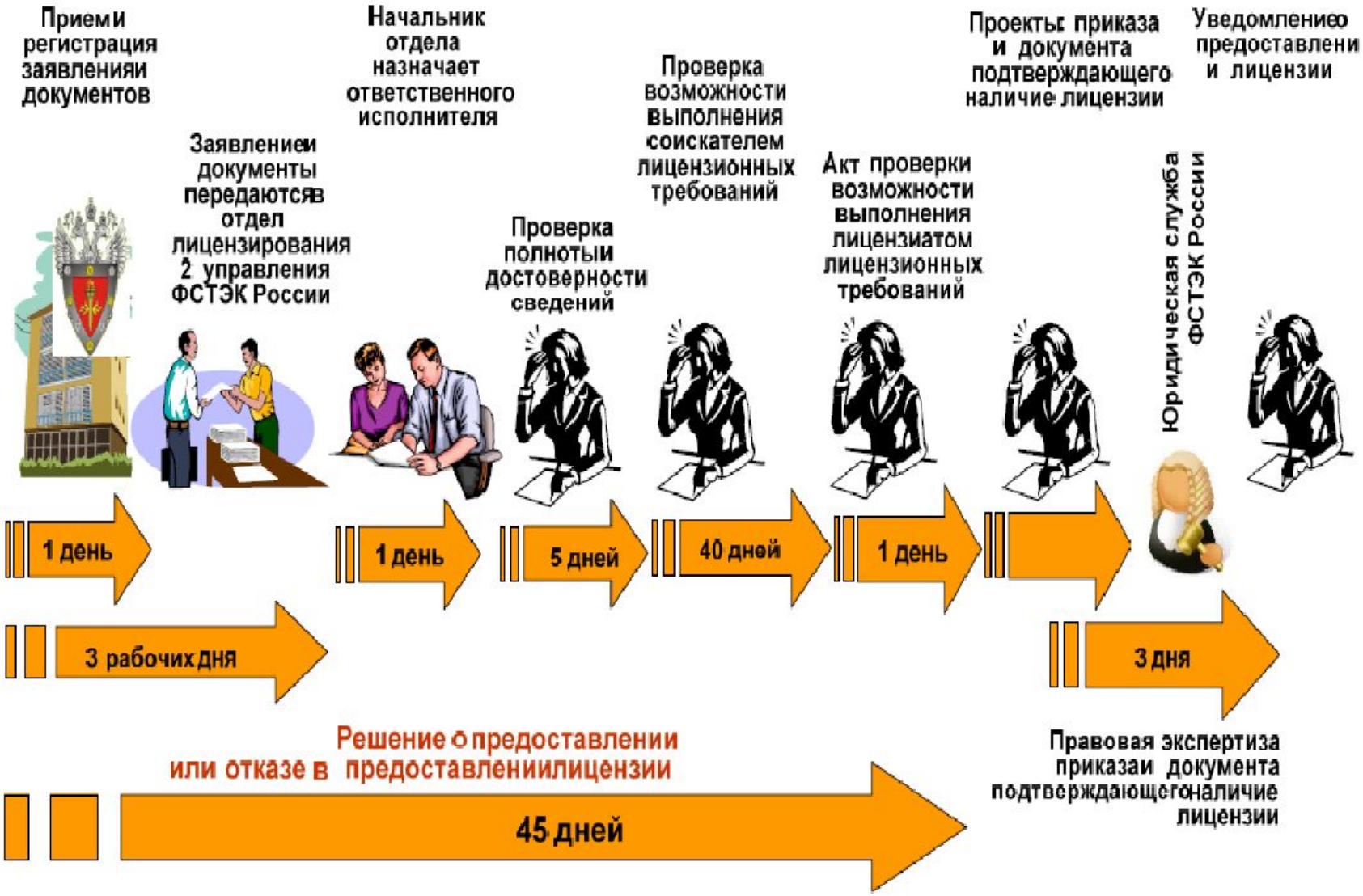
Лицензирование деятельности по технической защите конфиденциальной информации

«Положение о лицензировании деятельности по технической защите конфиденциальной информации», утвержденным постановлением Правительства Российской Федерации от 15 августа 2006 года № 504.

Блок-схема последовательности действий при исполнении государственной функции
по лицензированию деятельности по технической защите конфиденциальной информации



Административные процедуры



Основными правовыми и нормативными документами в области сертификации являются:

- Федеральный закон от 27 декабря 2002 года № 184-ФЗ «О техническом регулировании»;
- Постановление Правительства РФ от 26 июня 1995 года № 608 «О сертификации средств защиты информации»;
- «Положение о сертификации средств защиты информации по требованиям безопасности информации», утверждённое приказом Председателя Гостехкомиссии России от 27 октября 1995 года № 199.

Сертификация на соответствие требованиям по безопасности информации –

форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации.

Сертификат соответствия

- документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;

Система сертификации

- совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом;

Подтверждение соответствия

документальное удостоверение соответствия продукции или иных объектов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров

Структура Системы сертификации средств защиты информации по требованиям безопасности информации, функции субъектов сертификации, порядок сертификации, государственного контроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации, общие требования к нормативным и методическим документам по сертификации средств защиты информации определяются «Положением о сертификации средств защиты информации по требованиям безопасности информации», утверждённым приказом Председателя Гостехкомиссии России от 27 октября 1995 года № 199.

Организационную структуру Системы сертификации образуют:

- ФСТЭК России (федеральный орган исполнительной власти, уполномоченный проводить работу по обязательной сертификации);
- органы по сертификации средств защиты информации - органы, проводящие сертификацию определенной продукции;
- испытательные лаборатории - лаборатории, проводящие сертификационные испытания (отдельные виды этих испытаний) определенной продукции;
- заявители - изготовители, продавцы или потребители продукции.

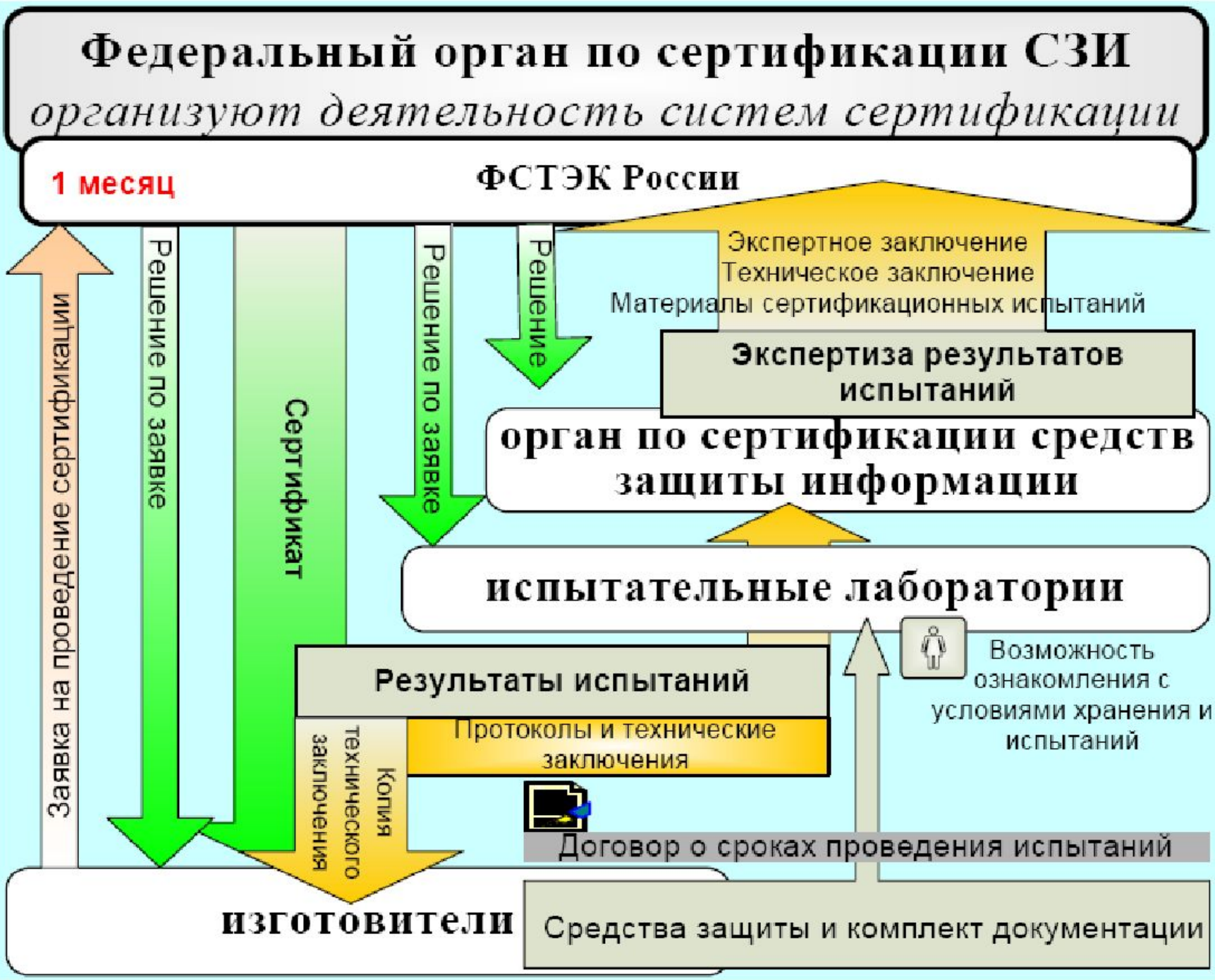

Система сертификации средств защиты информации по требованиям безопасности информации
Подсистема аттестации объектов информатизации и
Подсистема подготовки и аттестации экспертов

Органы по сертификации средств защиты информации и испытательные лаборатории проходят аккредитацию на право проведения работ по сертификации, в ходе которой ФСТЭК России определяет возможности выполнения этими органами и лабораториями работ по сертификации средств защиты информации.

Аккредитация проводится только при наличии у указанных органов и лабораторий лицензии на проведение мероприятий и (или) оказание услуг в области защиты государственной тайны в части технической защиты информации по сертификации и сертификационным испытаниям.

Процедура сертификации включает:

- подачу и рассмотрение заявки на проведение сертификации (продление срока действия сертификата) средств защиты информации;
- сертификационные испытания средств защиты информации и (при необходимости) аттестацию их производства;
- экспертизу результатов испытаний, оформление, регистрацию и выдачу сертификата и лицензии на право использования знака соответствия;
- осуществление государственного контроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации;
- информирование о результатах сертификации средств защиты информации;
- рассмотрение апелляций.


Федеральный орган по сертификации СЗИ
организуют деятельность систем сертификации
1 месяц
ФСТЭК России
Экспертное заключение
Техническое заключение
Материалы сертификационных испытаний
Экспертиза результатов испытаний
орган по сертификации средств защиты информации
испытательные лаборатории
Возможность ознакомления с условиями хранения и испытаний
Результаты испытаний
Протоколы и технические заключения
Копия технического заключения
Договор о сроках проведения испытаний
изготовители
Средства защиты и комплект документации
Заявка на проведение сертификации
Решение по заявке
Сертификат
Решение по заявке
Решение

По результатам контроля и надзора за эксплуатацией аттестованных объектов в случае нарушения их владельцами условий функционирования объектов информатизации, технологии обработки защищаемой информации и требований по безопасности информации органом, проводившим контроль и надзор, может быть приостановлено или аннулировано действие «Аттестата соответствия»

5. Особенности организации обеспечения информационной безопасности в таможенных органах Российской Федерации

Правовой основной обеспечения информационной безопасности таможенных органов являются Доктрина информационной безопасности Российской Федерации, Федеральные законы, указы Президента Российской Федерации, постановления Правительства Российской Федерации в области обеспечения информационной безопасности и защиты информации, а также Таможенный кодекс Российской Федерации.

Работы по созданию ведомственной системы обеспечения информационной безопасности осуществляются по следующим направлениям:

- Совершенствование ведомственной системы обеспечения информационной безопасности таможенных органов в целом;
- проведение единой политики обеспечения информационной безопасности таможенных органов Российской Федерации;
- совершенствование правовых актов ФТС России, регламентирующих обеспечение информационной безопасности таможенных органов Российской Федерации;
- совершенствование организационно-режимных и технических мероприятий и методов обеспечения информационной безопасности таможенных органов Российской Федерации;
- разработка планов по дооснащению таможенных органов Российской Федерации сертифицированными по требованиям безопасности информации средствами информатизации, а также по их внедрению и эксплуатации в повседневной деятельности таможенных органов Российской Федерации;
- подготовка предложений по совершенствованию ведомственной системы обеспечения информационной безопасности таможенных органов Российской Федерации.

В целях всестороннего обеспечения реализации положений Концепции обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года Главному управлению информационных технологий ФТС России совместно с ЦИТТУ, Управлением собственной безопасности ФТС России, Службой защиты государственной тайны и специальной документальной связи Управлением делами ФТС России, Региональным таможенным управлением радиоэлектронной безопасности объектов таможенной инфраструктуры и другими заинтересованным структурными подразделениями поручено представлять ежегодно на утверждение **План практических мероприятий по обеспечению информационной безопасности таможенных органов на год**.

Направления обеспечения информационной безопасности таможенных органов

Совершенствование ведомственной системы обеспечения ИБ ТО РФ в целом

Соблюдение конституционных прав и свобод человека и гражданина в области получения и использования таможенной информации

Информационное обеспечение государственной политики РФ в области таможенного дела

Развитие современных информационных таможенных технологий, эффективное использование информационных ресурсов ТО РФ

Обеспечение безопасности информационных ресурсов и информации в ЕАИС ТО РФ

Контроль состояния обеспечения ИБ таможенных органов РФ

Состав участников по защите информации

Совет (Техническая комиссия)
министерства, ведомства, органа гос. власти субъекта РФ

Подразделение по защите информации в министерствах и ведомствах, в органах гос. власти субъектов РФ

Подразделение по защите информации на предприятии (в учреждении, организации)

Лицензиаты ФСБ и ФСТЭК России по оказанию услуг в области защиты информации

Федеральные органы исполнительной власти и его территориальные органы

Управления ФСБ в субъектах РФ

Управления ФСТЭК по ФО

Организация работы Совета по информационной безопасности таможенных органов

Совет является постоянно действующим внештатным органом ФТС России по проведению государственной политики в области обеспечения информационной безопасности, в том числе защиты сведений, составляющих государственную тайну, в таможенных органах Российской Федерации и в организациях, находящихся в ведении ФТС России, по рассмотрению и выполнению программ создания и совершенствования системы информационной безопасности таможенных органов и по выработке единой технической политики в области защиты информации в Единой автоматизированной информационной системе таможенных органов. Совет выполняет функции ведомственной постоянно действующей технической комиссии ФТС России по защите государственной тайны.

Штатные подразделения информационной безопасности и технической защиты информации

- Отдел информационной безопасности Главного управления информационных технологий ФТС России;
- должностные лица, ответственные за защиту информации в структурном подразделении ФТС России;
- отделы эксплуатации доменной структуры единой службы каталогов и эксплуатации системы ведомственных удостоверяющих центров таможенных органов ЦИТТУ;
- подразделения (отделы или отделения) информационной безопасности и технической защиты информации региональных таможенных управлений;
- подразделения (отделы или отделения) информационной безопасности и технической защиты

Планирование мероприятий, методическое руководство и координация взаимодействия по вопросам обеспечения информационной безопасности и технической защиты информации

Планирование мероприятий осуществляется в соответствии с Планом практических мероприятий по обеспечения информационной безопасности таможенных органов на текущий календарный год

Контроль и координация взаимодействия подразделений информационной безопасности и технической защиты информации осуществляется в повседневной деятельности в установленные правовыми актами ФТС России сроки и порядке по следующим направлениям:

- разработка нормативно-методических документов по вопросам обеспечения информационной безопасности таможенных органов;
- отчетность таможенных органов о ходе и состоянии выполнения Плана практических мероприятий по обеспечения информационной безопасности таможенных органов на текущий календарный год;
- заслушивание представителей региональных таможенных управлений и таможен, непосредственно подчиненных ФТС России на заседаниях СОИБ ТО РФ;
- проведение расширенных выездных заседаний СОИБ ТО РФ;
- проведение функциональных проверок по вопросам обеспечения информационной безопасности и технической защите;
- организация и проведение семинаров-сборов руководителей подразделений информационной безопасности и технической защиты информации;
- организация и проведение обучения должностных лиц