Перечень инф сост комтайну включает в себя следующие свед:

1 Свед о структуре и масштабах производства, производственных мощностях и размещения оборудования, запасах сырья, материалах, комплектующих и готовой продукции.

2 Сведения о применяемых оригинальных методах управления предприятием, свед о подготовке, принятии и исполнении отдельных решение руководства предприятия по комерческим, организационным, науч-тех и иным вопросам.

3 Свед о планах расширения или свёртывания производств различных видов продукции и их технико-экономических обоснований, свед о планах инвестиций закупок и продаж.

4 Свед о фактах проведения целях предмете и результатах совещаний и заседаний органов управления предприятия

5 Свед о кругообороте средств организации, операций организ., состояние банковских счетов, уровне дохода предприятия, о состоянии кредита предприятия (пассивы и активы).

6 Свед о применяемых предприятием оригинальных методов изучения рынка(маркетинг), свед о результате изуч рынка , содерж оценки состояния и перспектив рыночной коньюктуры, свед о рыночной стратегии предприятия, о примен предприят ориг методов продаж, об эффективности комерч деят предприятия.

7 Обобщённые свед о внутр и зарубежных заказчиках, подрядчиках, ростовщиках, потребителях, покупателях, компоньёнах, спонсорах, посредниках, клиентах и др портнёрах сост в деловых отношениях с предприятием.

8 Обобщ свед о внутр и зарубеж предприятиях как потонцеальных конкурентах в деятельности предприятия , оценки качества деловых отношений с конкурирующ предприятием в различ сферах деловой активности.

9 Свед о подготовки, проведении и результатах переговоров с деловыми партнёрами.

10 Свед об условия конфиденциальности из кот можно установить порядок соглашения и другие обязательства предприятия с партнёрами (клиентами или контрагентами)

11 Свед о методах расчёта, структуре, уровне реальных цен на продукцию и размеры скидок

12 Свед о подготовки к участию, торгах и аукционах, результатах преобретений или продаж на них товаров

13 Свед о целях, задачах , программах перспективных научных исследований, ключевые идеи научных разработок, точные значения конструкционных характеристик, содаваемых изделий, оптимальных параметрах разрабатываемых технологич процессов (размеры, объёмы, конфигурация, процентное соотношение элементов, температура, давление, время и тд), аналитические и графические зависимости отражающие найденный закономерности и взаимосвязи, данные об условии эксперементов и оборудовании, свед о матенриалах из которых изготовлены отдельные детали, об особенностях контрукторско-технологического-художественно-технич дающ положит эффект. Свед о методах защиты от подделки товарных и фирменных знаках, о состоянии парка ПЭВМ и ПО

14 Свед об особенностях и использ и разрабатываемых технологий, специфики их применений, об условиях их производства и транспортировки продукции

15 Свед о порядке и состоянии организации защиты комтайны,

О порядки и состоянии организаци охраны сис сигнализации, пропускном режиме

16 Свед состовляющие комтайну предприятия, предприятий партнёров и передаваемых ими пользовани на доверительной основе и другие сведения

**Организация доступа и допуска персонала   
к конфиденциальной информации**

Осн положения допуска персонала предприятия  
к конфиденц инф

В соответствии с законом №149фз вопросы огранич доступа, опред порядка и условий такого доступа отнесены к компетенции обладателя информации. Обладатель инф при осущ своих прав обязяан ограничивать доступ к инф и принимать еры по её защите, если такая обязанность установлена ФЗ

Доступ граждан к сведениям или инф в установленном порядке отнесённым к комтайне осуществляется в соответствии со статьями ФЗ (7 и 10). С момента установления в отшении информации состовляющ комтайну , режима комтайны , полномочия по принятию решения о доступе к ней переходят к обладателю инф.

Определения порядка доступа лиц к комерческой тайне и учёт лиц получивших такой допуск являются одними из мер по охране такой конфиденциальности такой инф, принятие которых для обладателя инф является обязательным.

Меры по охране конфиденциальности инф признаются   
разумно-достаточными если исключается доступ к инф состовляющ комтайну любых лиц без согласия её обладателя.

Иные меры не противоречащее законодательству РФ по ограничению порядка доступа к комтайне могут быть дополнительно приняты её обладателем.

Основной вопрос государственного регулирования в сфере защиты гостайны является порядок допуска и доступа должностных лиц и граждан к сведениям состовляющ гостайну.

Допуск и непосредственный доступ должностных лиц и граждан к сведениям составляющ гостайну и их носителям выполняется в соответствии с положением и на основании Инструкции о порядке доступа должностных лиц и граждан РФ к гостайне

Допуск граждан к гостайне выполняется соответсвующими руководителями органами госвласти предприятий и организаций.

Допуск граждан производится в добровольном порядке и предусматривает:

1. Принятие на себя допущенными к гостайне лицами обязательств перед государством по нераспростронению доверенных им сведений состовляющ гостаюйну
2. Согласие на временные частичные ограничения их прав в соответствии с законом «о гостайне»
3. Письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий
4. Определение видов и размеров , порядка предоставления льгот предусмотренных РФ
5. Ознакомление с нормами законодательства РФ   
   «о гостайне» предусматривающими ответственность за их нарушение
6. Принятия соответсвующего решения руководителя предприятия о допуске лица к гостайне

Должностное лицо или гражданин допускающийся или ранее допускавшийся к гостайне может быть ограничен в своих правах:

1. Ограничен на выезд на период прописанный в контракте при оформлении допуска к гостайне
2. Распространение свед сост гостайну и использование открытий и изобретений содержащие такие сведения
3. Праве на прикосновенность личной жизни при проведении проверочных мероприятий период составления допуска к гостайне

Праве выезда гражданина за границу осущ в соответствии с ФЗ

«О порядке выезда и въезда в РФ» в целях частичной конпенсации в правах для должностных лиц и граждан допущенных к гостайне на постоянной основе установлены льготы:

1. Процентная надбавка в зависимости от сведений к которым они имеют доступ
2. Преимущественное право при прочих равных условия на остановление на работе при проведении органами госвласти, предприятиями и организациями организационных мер , нештатных ситуаций

Для сотрудников подразделения по защите гостайны дополнительно к вышеперечисленным льготам устанавливается процентная надбавка к заработной плате за стаж работы в указанных структурах, подразделениях.

Граждане коорым по характеру занимаемым должности необходим доступ к гостайне , могут быть назначены на эти должности или приняты на работу только после оформления в установленным порядке допуска по соответствующей форме.

Перечень должностей при назначении на которые граждане обязаны оформлять допуск к сведениям состовляющими гостайну в связи с наложанными на них должностными обязанности определяетс номенклатурой должностей

Номенклатура должностей разрабатывается предприятием и согласовывается с ФСБ РФ и после этого утверждается руководителем предприятия или его представителем возглавляющим работу в этой области (по защ гостайны)

Изменения в Номенклатуру вносят по мере необходимости,

А полная переработка раз в 5 лет

Порядок разработки , сотовления, согласования и утверждение номенклатурой внесение в неё изменений и дополнений определяется Инструкцией допуска должностных лиц и гражданам РФ к гостайне.

С целью подтверждения и ознакомления фактической работы сотрудников со свед сост гостайну подразделение защ гостайны ведёт учёт о осведомлённости их этими сведениями

**Порядок оформления и   
переоформления допуска  
к гостайне  
формы допуска**

Допуск гостайне – это процедура оформления права граждан на попуск к сведения состовлющ гостаюну в соответствии со степенями секретности сведений и грифами секретности их носителей, установлены такие формы допуска:

1. Для гражданам допускаемых к сведениям особой важности
2. Для граждан допускаемых к совершенно секретным свед
3. Для граждан допускаемых к секретным сведениям

Проверочные мероприятия допуска граждан к гостайне выполняется соответствующими органами безопасности во взаимодействия с органами осуществляющими оперативно розыскную деятельность.

Уровень необходимого допуска личного состава опред степенью секретности сведений или грифом их носителей с которыми они знакомятся или работают в пределах своих должностных обязанностей.

Уровень допуска для каждого из должностных лиц отражается в номенклатуре должностей.

Для непосредственного оформления допуска к гостайне лицам принимаемым на работу на должности включённые в намеклатуру должностей кадровый орган предприятия выполняет подготовку необходимых документов.

Основным документом отражающим анкетные автобиографические и другие данные оформляемого лица является анкета собственноручно заполненная им.

Основным документом (учётным) содержащим отметки о согласовании допуска лица с органом безоп, решением руководителя этого предприятия к носителям сведений и любую другую информацию является учётная карточка

В карточку также вносится инф о трудовой деятельности лица , его семейное положения и инф характерезующее это лицо, форма карточки определяется в зависимости от формы допуска гостайне, на которое оформляется лицо.

Напрвление вышеперечичленных и други документов в орган безопасности выполняется письмом в орган безопасности содержащим обоснование необходимости допука лица к сведениям соответствующим сведениям секретностиё.

Согласование допуска к гостайне оформляется в карточке о допуске, которая обязательно должна быть на предприятии и хранится в структурном подразделении по защите гостайны,

Отношения между допущеным лицом и руоководителя предприятия является договор или контракт об оформлении допуска гостайне и является приложением к основному трудовому договору.

Хранение договоров или контрактов (составляются в нескольких договоров) о допуске к гостайне и соответствующих карточек выполняется в установленном порядке в структкрном подразделении о защите гостайны; переоформление лиц по первой и второй формам производится через определённое количество времени (10-15 лет) только в случае перехода граждан на другое место работы, переоформление допуска постоянно работующим лицам не производится если не повышается форма допуска.

Не зависимо от сроков действия переоформления допуска по первой и второй форме производится в случаях:

1. Перевода или приёма гражданина на работу ,назначение на должность подразделение по защите гостайны
2. Вступление гражданина в брак, за исключением особо оговореных в нормативных документах случаев
3. Возвращение из длительных командировок сроком свыше 6 месяцев
4. Выезда близких родственников лица допущеного к гостайне на пмж заграницу
5. Возникновение обстоятельств, являющихся в соответсвии с закон о гостайне основанием для отказа гражданину в допуске к гостайне (привлекался к административной ответственности)

Перечень направляемых в орган безопасности документов определён в инструкции о порядке допуска должностных лиу и граждан РФ к гостайне. При несоответствии формы допуска лица степени секретности сведений, к которым он фактически имеет доступ форма допуска должна быть изменена.

Снижение формы допуска с первой на вторую или третью или со второй на третью, оформляется по распоряжению руководителя с соответствующей отметкой в карточке о допуске к гостайне; при необходимости руководитель предприятия может вернуть ранее присвоеную форму допуска без проведения проверочных мероприятий.

Предприятие обязано в установленном порядке письменно информировать орган безопасности, о состоянии работы допуска лиц к гостайне и предоставлять соответсвующую отчётную документацию.

**Основание для отказа   
должностному лицу или   
гражданину в допуске к гостайне  
и условия прекращения допуска**

При оформлении должностного лица или гражданина допуска к гостайне в установленном порядке, уполномоченные органы проводя проверочные работы, объём проверочных мероприятий зависит от степени секретности сведений к которым оформляется допускаемое лицо. Цель проведения проверочных мероприятий, выявление оснований в соответствии с законом о гостайне в отказе гражданину в допуске к гостаййне.

Основаниями могут быть:

1. Признание гражданина не дееспособным, ограничено недееспособным или особо опасным рецедивистом, Нахождение его под судом или следствием за государственные или иные преступления, наличие у него не снятых судимостей за эти преступления
2. Наличие у гражданина медецинских противопоказаний для работы с использованием сведений сост гостайну
3. Постоянное проживание его самого и/или ближайших родственников за границей и/или оформления указанными лицами документов для выезда за границу на пмж.
4. Выявление в результате проверки действий проверяемого лица создающих угрозу безопасности РФ
5. Уклонение от проверочных мероприятий и/или сообщение заведомо ложных анкетных данных.

Решение об отказе гражданина в допуске к гостайне принимается руководителем предприятия в индивидуальном порядке с учётом результатов проверочных мероприятий.

После оформления должностному лицу или гражданину допуска к гостайне в процессе выполнения им своих должностных обязанностей в зависимости отличных или иных обстоятельств могут возникать условия, являющиеся препядствием наличия такого допуска.

Допуск к гостайне может быть прекращён в случае:

1. Расторжение с ним трудового договора в связи с проведением организационных и/или штатных мероприятий
2. Однократного нарушения им предусмотренным трудовым договором обязательств связанных с сохранением гостайны
3. Возникновение обстоятельств явл основанием для отказа гражданину в допуске к гостайне
4. Прекращения допуска к гостайне осуществляется по решению руководителя предприятия в котором он работает, это решение оформляется в виде письменного мотивированного заключения

Если заключение о прекращении допуска гражданина к свед сост гостайну вынесено решением органа безопасности, то оно является обязательным основанием прекращения гражданина от работы с данными сведениями

Прекращение допуска гражданина не освобождает от обязанностей связ с неразлашением свед сост гостайну

Решение руководителя о прекращении допуска к гостайне и растожение на этом основании договора или договора, может быть обжалавоно в выше стоящем органе или в суде

Указанные лица предупреждаются о неразглашении гостайны ставшей им известной в связи с исполнением их обязанностей и о привлечении их к ответственности в случае её разглашения (берётся соответствующая расписка).

**Организация доступа персонала  
предприятия к сведения  
составляющую  
гостайну**

Допуск к сведениям сост гостайну это санционированное полномочным должностным лицом ознакомление конкретного лица со сведениями составляющ гостайну.

Организацие доступа должностного лица и гражданина к свед гостайну возлагается на руководителя органа гос власти , а так же на структурные подразделения по защите гостайны, руководитель предприятия обязан осуществлять постоянный контроль вза соотвествием формы допуска граждан к которым они фактически имеют доступ.

Руководитель несёт персональную ответсвенность за создание таких условий при которых должностное лицо или гражданин знакомится только с теми сведениями сост гостайну и в таких объёмах которые необходимы ему для выполнения своего функционала.

После приняятия решения о допуске гражданина или должностного лица это лицо изучает соответсвующие документы , внутрераспорядительные документы , дополнительно могут проводиться занятия с привлечением структурных подразделений по защите гостайны.  
Завершающий этап сдача зачёта по знанию нормативно правовой документации и способности решения задач на предприятии.

Приём зачётов выполняет комисия из сотрудников подразделения по защите гостайны, представители профилирующих подразделений, включая подразделение куда назначен гражданин, результаты зачёта оформляются в виде акта, которые хранятся в подразделении по защите гостайны.

В дальнейшем ежегодно обязанности и права ежегодно доводятся до всех сотрудников имеющих допуск к гостайне.

Порядок допуска к инф командированных лиц комерческой тайне.

Доступ командированных лиц на предприятии выполняется в порядке установленном обладателем.

Доступ командированных лиц к сведениям сост гостайну выполняется в соответствии с положениями нормативных документов по защите гостайны.

Основаниями командированного лица к гостайне и их носителям являются документы:

1. Паспорт или документ удостоверяющий личность командированного
2. Справка о допуске соответствующего уровня подтверждающая наличие у командированного лица на подразделении или работу со сведениями соответствующей степени секретности
3. Предписание по выполнению работы

Справка о допуске и предписание на выполнение задания оформляются в соответствии с инструкцией о допуске должностных лиц и граждан РФ к гостайне; данная справка подписывается руководителем подразделения по защите гостайны или кадрового органа, заверяется печатью руководителя организации, выдаётся для посещения только одной организации, в предписании кратко указывается командирования и определяется с какими сведениями надо ознакомить командированного для выполнения задания, если необходимо указать сведения сост гостайну , то предписание отправляется спец почтой в порядке установленном для секретных документов.

Прямой доступ командированного выполняется с письменного разрешения руководителя принимающей стороны, которое оформляется в соответствующей графе предписания на выполнение задания.

По завершении командировки лица на предприятии выполняется оформление документов , производится отметка о степени секретности сведений , с которыми фактически знакомилось лицо, отметку подтверждает командированный, после чего предписание передаётся для хранения, подразделения по защите гостайны предприятия, командированному выдаётся справка о допуске с указанием степени секретности сведений и дата, запись заверяется подписью руководителя подразделения по защите гостайны и печатью. По возвращению командированного , справка сдаётся на хранение в подразделение по защите гостайны предприятия.

Руководитель организации и подразделения по защите гостайны следит за созданием условий по работе командрованных лиц для отслежевани работы со сведения и их носителями равного уровня секретности.

**Федеральный закон  
«О персональных данных» №152**

Впервые был принят 27.01.2006

Гос-во регулирует сферу персональных данных с помощью целого ряда законодательно-правовых актов:

1. Конституция РФ
2. ФЗ №152 о перс данных
3. Гражданский кодекс
4. Уголовный кодекс

ФЗ №152 закон разъясняет что такое персональные данные, что к ним относится и область применения;

персональные данные по сути это сведения напрямую или косфено характиризующее физ лицо – субъекта п/д (перс данных)

В конституции РФ тоже есть рассмотрение персональных данных и дают право на тайну частной жизни её непрекосновенность и защиту, всё что входит в понятие персональные данные, пренадлежит только их носителю и не может контролироваться правительством или третьими лицами, граждане сами решают как распоряжаться этой информацией, препядствовать распростронению или передавать её другим; гос-во гарантирует защиту этой возможности

ФЗ №152 определяет кто в праве использовать п/д кроме их носителя, на каких условиях, по каким правилам; получать и обрабатывать личную инф о субъекте могут только операторы по согласию.

Операторы получают доступ к определённому объёму данных, которые необходимы для решения их задач, они не имеют право их хранить или использовать после того как цель достигнута, если человек увольняется то работодатель обязан уничтожить перс данные кроме личного дела. По нормам ФЗ №152 особые правила для частных и юр лиц, применяются когда п/д получают для личных или семейных нужд, если это не ущемляет права третьих лиц; персональные данные содержатся в архивах; составляют гостайну или собираются по судебному акту. Другие законодательные акты уточняют положение о п/д применительно к разным ситуациям, вводят в систему и классификацию средств защиты п/д.

Классификация п/д

ФЗ №152 выделяет виды п/д, которые можно расположить по их степени секретностии , сложности в сборе и исп 3 лицами:

1. Обезличиные
2. Общие
3. Биометрические
4. Специальные

Общие п/д

Общие п/д -Это основная инф о человеке, к ним относят:

1. ФИО
2. Место регестрации
3. Паспортные данные
4. Образование
5. ИНН
6. Свед о работе
7. Размер доходов
8. И тд

Не все эти данные можно отнести по отдельности к п/д

Общие п/д содержатся в паспорте, в военном билете, в дипломе, в личной карточке сотрудника, в трудовой книжке и тд

Письменное согласие сотрудника не обязательно для разрешения на их получение, достаточно косфенного согласия.

Личная жизнь гражданина включает в себя различные виды тайн (врачебная , налоговая, тайна усыновления и тп) , защищается от разглашения УкРФ

Биометрические п/д

Это физические и биологические характеристики субъекта

Дактилоскопические изображения, группа крови, рост, вес, цвет глаз, анализ днк и тд

Также к этой относится инф по фото и видео человека

Специальные п/д

Требуюется для полит деят, для поступления к опред рода работу.

Получить доступ к этим данным 3 лицам, можно получить только с разрешения субъекта.

Это расса и национальность, вероисповедание, филосовские убеждения, состояние здоровья, наличие судимости, интимная жизнь, сексуальные предпочтения, эти данные могут содержаться в медецинских справках, личных делах и тд.

**Типы п/д**

Работодатели для организации рабочего процесса обрабатывают 2 типа докуметов:

К первому типу относят задокументированые свед , кот подаёт работник в связи с подписанием договора (трудовая книжка, паспорт, СНИЛС, ИНН, документы военского учёта, диплом, сертификаты, наличие специальных данных и тп)

Второй тип формируется самим работодателем (приказы о поступлении на работу, распоряжение о перемещениях по отделам, поощрение, должностные повышения или понижения, личная карточка, расчётные документы)

Классификация п/д  
критерии классификации:

1. По степени доступа
2. По направлению
3. По содержанию

К каждому критерию классификации относится категория п/д:

По степени доступа – 1А общедоступные (субъект п/д дал согласие на доступ к ним неограниченного круга лиц илиинф общедоступна согласно законодательству)

1Б конфиденциальные (все п/д кроме тех которые законом установлены обратное или в отнощении которык субъект п/д согласился на распространение

1. 2-а специальные (национальная и расовая пренадлежность, полит взгляды, состояние здоровья, религиозные убеждения, судимость, личная жизнь)

2-б обычные (все п/д кроме тех которые отнесены к специальным

1. 3-а биометрические (данные которые характеризуют физиологию человека и позволяют установить его личность)

3-б небиометрические

Правовой основой по защите п/д нормы конституции РФ и   
ФЗ №152, в соответствии с законом(2 практическая) под п/д – понимают инф с ограниченном доступом, трудовой кодекс РФ даёт более узкую трактовку - это свед необходимые работодателю которые касаются конкретного сотрудника, трудовой кодескс выделяет отдельную главу по защите п/д, судебные споры в отношении разглашения личных п/д, как правило заканчиваются в пользу работника, на основании нарастающей необходимости по защите п/д сокращённо именуемых ИСПДн (информационные системы персональных данных) строится работа по их защите, оператор обязан защищать и несёт ответственность за невыполнение ФЗ №152, разрабатываются на предприятия мероприятия по защите п/д документально.

**Аттестация объекта информатизации  
по требованиям безопасности информации**

(практические только по ИБ)

Деятельность по аттестации объекта информатизации по требованиям безопасности инф выполняет ФСТЭК России

Объект информатизации – это совокупность информационных ресурсов, средств и систем обработки используемых в соответсвии заданной информационной технологией , средств обеспечения объекта информатизации , помещений или объектов(зданий, сооружений, технических средств), в которых они установлены или помещения и объекты предназначенные для ведения конфиденциальных переговоров.

Аттестация объектов информатизации – это комплекс организационно-технических мероприятий, в результате которых с помощью специального документа (аттестат соответствия) подтверждает что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности инф утверждённых ФСТЭК РФ.

Наличие аттестата соответствия в организации даёт право организации на право обработки информации с уровнем секретности (конфиденциальности) на переод времени установленный в аттестате.

Аттестация выполняется в порядке установленном «в положении по аттестации объектов информатизации по требованиям безопасности информации».

В первый раз такое положение было принято 25 ноября 1994 года.

Был приказ ВСТЭК от 29 апреля 2021 года приказ №77 об утверждении Порядка организации и проведении работ по аттестации объектов информатизации на соответствии требований ИБ при работе не с гостайной;

Положение №240/24/2087 Об утверждении порядка аттестации объектов информатизации и особенностях его реализации (29.04.2021).

В соответствии с этими документами аттестация должна проводиться до начала обработки информации подлежащей защите, это необходимо в целях подтверждения эффективности использования мер и средств по защите этой инф на определённом объекте информатизации.

Аттестация является обязательной:   
1. В случаях работы с гостайной

2. управлении экологически опасными объектами

3. ведение секретных переговоров

В остальных случаях аттестация производится по желанию владельца объекта информатизации

Аттестация подразумевает комплексную проверку(испытания объекта иформатизации в реальных условиях эксплуатациии)

Целью является проверка соответствия применяемых мер и средств защиты требуемого для защиты инф

К проверяемым требованиям относятся:

1. Защита от НСД и комп вирусов
2. Защита от утечки через ПЭМИН
3. Защита от утечки или воздействия информации за счёт специальных средств, устройств, встроенных в объект информатизации

ПЭМИН- побочные электромагнитные …

Аттестация проводится органом по аттестации в соответствии со схемой выбираемой этим органом и состоит из следующего перечня работ:

1. Анализ исходных данных по аттестуемому объекту информатизации
2. Предварительное ознакомление с аттестуемым объектом информатизации
3. Проведение экспертного обследования объекта информатизации и анализ разработанной документации на этом предприятии органами по защите информации с точки зрения её соответствия требованиям нормативной и методической документации
4. Проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте с помощью специальной контрольной аппаратуры и тестовых средств
5. Проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств по защите информации по требованиям безопасности информации
6. Проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации
7. Анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации

Органы по аттестации должны проходить окредитацию ФСТЭК РФ в соответствии с положением об окредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации.

Все расходы по проведению аттестации возлагается на заказчика в любом случае. Органы по аттестации несут ответственность за выполнение своих функций, за сохранение конфиденциальности информации полученной в ходе аттестации и соблюдения авторских прав заказчика.

В качестве заявителей могут выступать заказчики, владельцы или разработчики аттестуемых объектов информатизации.

Органы по аттестации:

1. Аттестовывают объекты информатизации и выдают аттестаты соответствия
2. Выполняют контроль за безопасностью информации , используемой на аттестуемых объектах и за их эксплуатацией
3. Отменяют и приостанавливают действия выданных аттестатов соответствия
4. Формируют фонд нормативно-методической документации необходимой для аттестации конкретных типов информатизации и участвуют в их разработке
5. Ведут информационную базу об аттестуемых объектах взаимодействуют с ФСТЭК РФ ежеквартально информируют о своей деятельности в области аттестации

Испытательные лаборатории проводят испытания несеретифицырованной продукции используемой на аттестуемом объекте.

Вся информация по аттестации объектов информатизации находится на сайте ФСТЭК.

Заявитель обязан:

1. Провести подготовку объекта для аттестации путём реализации необходимых организационно-технических мероприятий по защите информации
2. Привлекают органы по аттестации для проведения данного мероприятия
3. Предоставляют органам по аттестации необходимые документы и условия для проведения аттестации
4. При необходимости привлекают для проведения испытаний несертифицырованных средств защиты информации этого объекта ипытательные центры (лаборатории) по сертификации
5. выполняют эксплуатацию объекта информатизации в соотвтсвии с условиями и требованиями установленными в аттестате соответсвия
6. извещают орган по аттестации о всех изменениях в информационных технологиях ,составе и размещение средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации
7. предоставляют необходимые документы и условия для контроля и надзора за эксплуатацией объекта информатизации

Для проведения испытаний заявитель должен предоставить документы:

1. Приёмно-сдаточные документы на объект инфоматизации
2. Акты категорирования выделенных помещений и объектов информатизации
3. Инструкции по эксплуатации СЗИ (средства защиты информации)
4. Тех паспорт на испытуемый объект
5. Документы на эксплуатацию (сертификаты соответствия требования безопасности информации):

А. на технические ср-ва защиты информации

Б. ТСОИ (технические средства обрабатываемой мнформации)

В. ВТСС (вспомогательные технические ср-ва и системы)

6. Акты на проведённые скрытые работы

7. сертификации звукоизоляции и эффективность экранирования сооружений если они проводились

8. протоколы измерения величены сопративления заземления

9. протоколы измерения реального затухания до мест возможного размещения средств разверстки

10. данные по уровню подготовки кадров обеспечивающих защиту информации (ЗИ)

11. данные о ТО средствами контроля эффективности защиты информации и их метрологической поверке

12. нормативную и методическую документацию по защите инф и контролю эффективности защиты

Исходные данные и документы могут уточняться заявителем зависимости от особенностей аттестуемого объекта по согласовонию с аттестуемой комиссией.

Порядок проведения аттестации объектов информатизации:

1. Подача и рассмотрение заявки на аттестацию по установленному образцу, заявитель направляет заявку в орган по аттестации где в месячный срок она рассматривается выбирается схема аттестации и согласовывается с заявителем
2. Предварительное ознакомление с объектом аттестации
3. Испытания в испытательных лабораториях несертифицированных средств и систем защиты инф с аттестуемого объекта
4. Разработка программы и методике аттестационных испытаний – орган аттестации определяет перечень работ и их продолжительность, методики испытаний, состав комиссий, использование контрольной аппаратуры, тестовых средств и всё согласовывается с заявителем
5. Составление договора на аттестацию – составляется между заявителем, органом по аттестации и привлекаемыми экспертами, оформляются предписания о допуске аттестационной комиссии к проведению аттестации.
6. Работа аттестационной комиссии, которая выполняет:  
   А) анализ организационной структуры объекта, состава и структуры комплекса технических средств и ПО, системы ЗИ на объекте, разработанной документации и её соответствие  
   Б) определяется правильность категорирывания объектов электронной вычеслительной техники и автоматизированных систем выбора и применения сертифицырованных и несертифицырованных средств и систем ЗИ  
   В) проводятся испытания на аттестуемом объекте и анализ результатов их испытаний в лабораториях  
   Г) проверяется Уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по ИБ  
   Д) проводятся комлексные аттестационные испытания в реальных условиях эксплуатации, путём проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации  
   Е) оформляются протоколы испытаний и заключения по результатам аттестации счётким указанием нарушений и рекомендациями по устранению выявленных нарушений, приведению системы защиты объекта в соответствии с требованиями и совершенствования этих требований

К заключению прилагаются протоколы испытаний с результатами и выводы

В протокол включается:

1. Вид испытаний
2. Объект испытаний
3. Дата и время проведения испытаний
4. Место проведения испытаний
5. Перечень используемой аппаратуры(должна быть вся поверена)
6. Перечень нормативно-методических документов по которым проводились испытания,
7. краткое описание методики испытания
8. результаты расчёта
9. выводы по результатам

Протоколы подписываются экспертами с указанием должности и фамилии с инициалами

Заключение подписывают члены аттестационной комиссии, утверждаются руководителем органа аттестации , как и протоколы испытаний и передаются заявителю

Если заключение по результатам аттестации утверждено, то проводится оформление, регистрация и выдача аттестата соответствия.

Аттестат соответствия содержит в себе:

1. регистрационный номер
2. дату выдачи
3. срок действия
4. наименование, адрес и местоположение объекта
5. категория объекта информатизации
6. класс защищённости автоматизированной системы
7. гриф секретности информации обрабатываемой на объекте информатизации
8. организационная структура и вывод об уровне подготовки специалистов по ЗИ
9. номера и даты утверждения программы и методик, по которым проводились аттестационные испытания
10. перечень руководящих документов в соответствии с которыми проводилась аттестация
11. номер и дата утверждения заключения проверки
12. состав комплекса технических средств обработки информации ограниченного доступа, перечень вспомогательных технических средств и систем, перечень технических средств ЗИ, схемы их размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств
13. организационные мероприятия при проведении которых разрешается обработка информации ограниченного доступа
14. перечень действий, которые запрещаются при эксплуатации объекта информатизации объекта информатизации
15. список лиц на которых возлагается обеспечение требований по защите информацией, контроль за эффективностью реализованных мер и средств ЗИ

Аттестат соответствия выдаётся на период, в течении которого организация не изменяет условия прописанные в условиях, но не более чем на 3 года

При любом изменении на объекте информатизации аттестация проводится заново

**Допуск предприятий к проведению работ с конфиденциальной инф  
  
Основные положения лицензирования деятельности предприятий связанной с использованием сведений составляющие гостайну**

В соответствии с законом о гостайне допуск предприятия к гостайне – это оформление договора на проведение работ с использованием сведений гостайну

Каждому предприятию или организации при осуществлении работ с использованием свед сост гостайну необходимо в установленном порядке в соответствии с нормативно-правовыми актами и методическими документами получить лицензию на осуществление этого вида деятельности в сфере защиты гостайны установлены следущие виды деятельности подлежащие лицензированию:

1. проведение работ связанных с использованием свед сост гостайну
2. проведение работ связанных с созданием средств защиты инф
3. проведение работ связанных с осуществлением мероприятий и/или оказания услуг в области защиты гостайны в части технической защиты инф

Незаконная в области з/и без наличии соответствующей лицензии ровно как и нарушение условий работы предусмотренной в лицензии , является наказуемым деянием и рководители и частные лицы ведут административную ответственность в соответствии с административным кодексом статьи 13.13 и 13.12

1 вид Описание лицензии выдаваемой предприятиям выполняющую работы с использ свед сост гостайну (имеющие режимно-секретные органы):

бланк имеет основной цвет салатовый из плотной специальной бумаги; герб, орёл чёрного цвета на жёлтом фоне; водные знаки темно-зелёного цвета ,гербовая печать синего цвета, серия и номер красного цвета  
  
2 вид выдаётся предприятиям связанных с созданием средств защиты информации  
описание:  
бланк выполнен с фоном светло-серым фоном из плотной специальной бумаги, герб орёл чёрного цвета на щите из триколора; водные знаки синего цвета , гербовая печать синяя ; буквы серии красного цвета цифры чёрного, номер чёрного цвета; на обороте листа расшифровка перечня разрешённых работ

3 вид лицензия выдаваемая организации на осущ мероприятия и/или услуг в обл защиты гостайны в части тзи(тех защиты инф)  
выдаётся на бланке светло-серого цвета из плотной специальной бумаги; герб чёрный орёл ,на щите триколор; водные знаки голубые, гербовая печать синего цвета, буквы серии красного цвета, цифры чёрного; на обороте расшифровка перечня работ

Порядок организации и проведения работ по лицензированию деятельности предприятий определены «Положением о лицензировании деятельности предприятий учреждений и организаций по проведению работ связанных с использованием сведений сост гостайну, созданием средств защиты инф, а также осуществлением мероприятий и/иди оказанием услуг по защите гостайны»

Основные мероприятия лицензирования и общие требования к алгоритму лицензирования, функции и задачи решаемые лицензирующими органами права и обязанности соискателя лицензии и лицензиата определены в ФЗ «о лицензировании отдельных видов деятельности»

Органами уполномочинами на ведение лицензионной деят в сфере гостайны являются:

1. на право проведение работ связанных с использованием свед сост гостайну – ФСБ РФ её территориальные органы (на территории РФ) и СВР РФ (за рубежом)
2. на право проведение работ связанных с созданием средств защиты инф – ФСТЭК , СВР, мин обороны РФ, ФСБ в пределах её компетенции
3. право на проведение работ связанных с осуществлением мероприятий и/или оказания услуг в области защиты гостайны в части технической защиты инф – ФСБ и её территориальные органы, ФСТЭК, СВР(служба внешней разведки) в пределах её компетенции

Лицензирование деятельности предприятий ФСБ, мин обороны, СВП, ФСТЭК по допуску к проведению работ связанных с сведсост гостайну выполняется руководителями минестерств и ведомств к которым подчиняются указанные предприятия

**Алгоритм работы органа по лицензированию деятельности предприятия**

Лицензии выдаются предприятиям на основании результатов специальных экспертиз и гос аттестации их руководителей, ответственных за защиту свед сост гостайну

Лицензии оформляются на спец бланках на предъявителя со степенью защиты, подписывается руководителем органа уполномоченного на ведение лицензионной деятельности и заверяется печатью этого органа, копия лицензии хранится в органе выдавшем её

Срок действия лицензии не может быть меньше 3 лет , но не более 5 лет, но по желанию заявителя может выдаваться менее чем на 3 года.

Соискатель лицензии предоставляет заявление о выдачи лицензии с приложением копий уставных и учредительных документов и другие материалы характерезующие деятельность предприятия

1. Орган выполняет организацию лицензирования предприятия
2. Организацию и проведение специальных экспертиз
3. Рассмотрение заявлений
4. Принятие решений о выдаче или отказе выдачи лицензии
5. Выдача лицензии
6. Принятие решений о преостановлении дейсвия лицензии или её онулирование
7. Разработка номативно-метод документов по вопр лиценз
8. Привлечение по необходимости представиелей ведомсв для провед спец экспертиз
9. Ведение реестра выданных приостановленных или онулированных лицензий

Одним из важных вопросов при проверке является проверка наличия в структуре организации необходимого числа специально подготовленных сотрудников для работы по защите гостайны и уровня их квалификации, оценивается готовность сотрудников предприятия выполнять специальные виды работ

Определения по теме лицензирование  
основные понятия:

1. Лицензия – специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий выданное лицензирующим органом юр лицу или ип
2. Лицензируемый вид деятельности – вид деятельности на территории РФ требуется получение лицензии
3. Лицензирование – мероприятие связанное с предоставлением лицензии переоформлением документов подтверждающих наличие лицензии, приостановление деятельности лицензиатов за нарушение лицензионных требований и условий, возобновлением или прекращением действия лицензии , контролем лицензирующих органов, за соблюдением лицензиатами при осуществлении лицензирующих видов деятельности соответствующих лицензионных требований и условий ведением реестров лицензий предоставлением в установленном порядке заинтересованным лицам сведений из реестров лицензий и иной инф о лицензировании
4. Лицензионные требования и условия – совокупность установленных положениями о лицензировании конкретных видов деятельности требований и условий выполнение которых лицензиатом обязательны
5. Лицензирующие органы – федеральные органы исполнительной власти , органы исп власти субъектов РФ (полный перечень был в предыдущей лекции)
6. Лицензиат – юр лицо или ип имеющий лицензию на осуществление конкретного вида деятельности
7. Соискатель лицензии – юр лицо или ип обратившийся в лицензионный орган с заявлением о предоставлении лицензии на осуществление конкретного вида деятельности
8. Реестр лицензий – совокупность данных о предоставлении лицензий переоформление документов подтверждающие наличие лицензии, приостановление и восстновление лицензий и онулирование лицензии (есть реестр для конкретной деятельности; у нас по ИБ)
9. Виды деятельности относящиеся относящиесе к з/и на которые нужна лицензия:  
   1. Шифровальных (криптографических) ср-в  
   2. Деятельность по техническому обслужеванию (ТО) шифровальных (криптографических) ср-в  
   3. Предоставление услуг в облачти шифровальной инф  
   4. Разработка, производство, шифровальных (криптографических) ср-в, защищённых с использованием шифровальных ср-в информационных систем, телеком систем  
   5. Деятельность по выявлению электронных устройств, предназначенных для негласного получения инф. В помещениях и тех ср-вах (за исключением случая, если указанная деятельность обесп для собственных нужд юр лица или ип)  
   6. Деятельность по разработке и/или производству ср-в защиты конфиденциальной инф  
   7. Деятельность по технической защите конфиденциальной инф  
     
   8. Разработка производства реализация и приобретение в целях продажи специальных технических ср-в предназначенных для негласного получения инф ип и юр лицам, осуществляющим предпринемательскую деятельность

**Сертификация средств заиты информации(СЗИ)**

Общий порядок сертификации СЗИ

выполняется в соответствии с сертификацией СЗИ

Сертификация – форма осуществляемого органом по сертификации подтверждения соответсвия объектов требованиям технических регламентов, положением стандартов, сводов правил или условия договора

Сертификат соответствия – документ удоставеряющий соотвтесвие объекта требованиям тех регламентов, положениям стандартов, сводам правил или условиям договоров

Ср-вами з/и являются технические, криптографические, программные и другие ср-ва предназначенные для защиты сведений сост гостайну, средствах в которых они реализованны, атакже средства контроля эффективности з/и

Указанные ср-ва подлежат обязательной сертификации

Система сертификации сзи которая проводится в рамках контроля представляет собой совокупность участников сертификации:

1. Федеральный орг по сертификации
2. Орган возглавляющий сис сертификации однородной продукции
3. Органы по сертификации СЗИ – органы проводящие сертификацию опред продукции
4. Испытательные лаборатории – лаборатории проводящие сертификационные испытания продукции или отдельные виды этих испытаний
5. Изготовители – продавцы исполнители продукции

Центральные органы сис сертификации, органы по сертификации СЗИ и испытательные лаборатории проходя окредитацию на право проведения работ по сертификации. Целью окредитации является проверка возможности выполнения работ по сертификации СЗИ

По результатам контроля федеральный орган по сертификации может приостановить или онулировать сертификат в случаях:

1. Изменения на законодательном уровне, касающиеся требований к СЗИ, методы испытаний и контроля
2. Изменение технологий изготовления,   
   конструкции (состава), комплектности СЗИ и системы контроля их качества
3. Невыполнение требований технологии изготовления, контроля и испытаний СЗИ
4. Несоответствие сертифицированных СЗИ техническим условия или формуляру, выявленное в ходе государственного или инспекционного контроля
5. Отказ заявителя в допуске или приёме лиц уполномоченных осуществлять госконтроль и надзор, инспекционный контроль за соблюдением правил сертификации и за сертифицированными СЗИ

Сроки проведения испытаний при сертификации устанавливаются договором между изготовителем и испытательной лабораторией

Экспертиза результатов испытаний оформление, регистрацию и выдачу сертификата и лицензии на право пользования знака соответствия включает в себя процедура соответствия на основании заключения испытательной лаборатории делает закючение и отправляет в орган по сертификации после получения регистрационного номера заявитель получает сертификат

Сертификат дают сроком не менее 5 лет

По результатам контроля фед орган по сертификации может преостановить или онулировать сертификат в случаях:

Читать выше

Сертификация импотрных СЗИ проводится по тем же правилам что и отечественный

Основными схемами проведения сертификации СЗИ являются:

1. Единичных образцов СЗИ – проведение испытаний образцов на соответствие требований по ЗИ
2. Для серийного производства СЗИ – проведение типовых испытаний образцов СЗИ на соответствии требований по ЗИ и последующий инспекционный контроль за стабильностью характериристик сертифицированных СЗИ выполняющих требования

В отдельных случаях по согласованию с органом по сертификации СЗИ допускается проведение испытаний на базе изготовителя сроки таких испытаний устанавливаются договором между изготовителем и испытательной лабораторией

Если соискатель не согласен с отказом в выдаче сертификата, он имеет право обратиться в центральный орган по сертификации или в федеральный орган по сертификации или в межведомственную комиссию для дополнительного рассмотрения полученных результатов

Оплата работ по сертификации осущетвляется по договору между участниками по сертификации

Порядок сертификации  
во ФСТЭК РФ

Заявитель на сертификацию должен иметь лицензию ФСТЭК на соответствующий вид деятельности и может подать заявку во ФСТЭК РФ

В заявке указывается:

1. Наименование заявителя
2. Адрес заявителя
3. Наименование продукции (в соответствии с паспортом)
4. Перечень нормативных и методических документов на соответствие требований которые заявителю нужно просертифицировать
5. схема сертификации (на единичный образец или на серийное производство)
6. испытательная лаборатория в которой заявитель хотел бы провести испытания
7. дополнительные условия или требования

в заявке заявитель обязуется выполнять требования, обеспечивать стабильность сертифицированных характеристик продукции, маркерованные знаком соответствия и оплатить все расходы по проведению работ

Решение на проведение сертификационных испытаний

ФСТЭК в течении месяца после получения заявки направляет заявителю и испытательной лаборатории решение на проведение испытаний которое содержит:

1. наименование заявителя и адрес
2. наименование сертифицируемой продукции
3. схему проведения образца
4. назначенная испытательная лаборатория и её адрес
5. перечень нормативных и правовых документов на соответствие которых будет проводиться сертификация
6. испытательная лаборатория назначенная для последующего инспекционного котроля
7. орган сертификации назначенный для проведения экспертизы
8. способ оплаты работ

Испытательная лаборатория может быть изменена по согласию

Заключение договора с испытательной лобаротрией в таком договоре устанавливаются сроки, порядок, стоимость; сначала испытательная лаборатория готовит комерческое предложение с обоснованием сроков, стоимости работ и проект договора

В комплект договорных документов входит:

1. договор
2. техническое задание на проведение работ
3. ведомость исполнения
4. протокол согласования цены

также включается в случае порчи испытательных образцов

Подготовка исходных данных

Этот этап включает в себя согласование и методики сертификационных испытаний

Предаёт инф заявителю о том какие данные необходимы для испытаний

В орган по сертификации лаборатория направляет программу и методику для утверждения

Заявитель получает эти же документы для согласования и подготовки исходных данных, он предоставляет лаборатории СЗИ в комплектации по техническим условиям или формуляру

Сертификационные испытания

Лаборатория отбирает образцы сертифицируемой продукции, идентифицирует её, проводит испытания, по утверждённой методике и программе

Заявитель готовит и настраивает стенд для проведения сертификационных испытаний

Запрещается вносить изменения в состав или конструкцию объектов по сертификации или документацию во время испытаний – это ведёт к остановке испытаний, их перезапуску что влияет на стоимость и сроки проведения работ

Оформление результатов испытаний

Оформляются в виде протоколов сертификационных испытаний и технических заключений, эти документы направляются в орган по сертификации, а копии заявителю

Заключение договора   
с органом по сертификации

Испытательная лаборатория заключает договор с органом по сертификации на проведение экспертизы где оговариваются сроки, порядок и стоимость (проводится в течении месяца)

Иногда орган по сертификации требует заключить договор с заявителем и это необходимо изначально обговаривать с испытательной лабораторией

Орган по сертификации проводит экспертизу результатов испытаний, технических и эксплутационных документов на сертифицированную продукцию, затем делают экспертное заключение которое вместе с техническим заключением предаётся во ФСТЭК РФ на основании этих документов оформляется сертификат

Если ФСТЭК выявит в результате проверки несоответсвии результатов то заявителю направляется матевированное письмо и заявитель имеет право обратиться в апеляционный совет федерального органа, апелляция рассматривается в месячный срок

ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ

СОВЕЩАНИЙ, В ХОДЕ ИЗДАТЕЛЬСКОЙ И РЕКЛАМНОЙ ДЕЯТЕЛЬНОСТИ 9.1. Планирование мероприятий по защите информации

при подготовке к проведению совещания В ходе повседневной деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну, и конфиденциальной информации, планируются и проводятся служебные совещания\*, в ходе которых рассматриваются

или обсуждаются вопросы, содержащие конфиденциальную информацию. Это могут быть вопросы, отнесенные к государственной тайне, касающиеся проводимых предприятием научно-исследовательских, опытноконструкторских и иных видов работ, предусмотренных уставом предприятия, или вопросы, носящие конфиденциальный характер, отражающие коммерческую сторону деятельности

предприятия. Вышеперечисленные мероприятия могут быть внутренними (к участию в них привлекается только персонал данного предприятия) или внешними (с участием

представителей сторонних организаций-партнеров). Решение на проведение совещания во всех случаях принимается непо- средственно руководителем предприятия или его заместителем по ходатайству

руководителя подразделения, в чьих интересах оно будет проведено. Принимаемые должностными лицами предприятия (структурным подраз- делением, его организующим) меры по защите конфиденциальной информации в ходе подготовки и проведения совещания должны носить как организационный, так и

технический характер.

Мероприятия по защите информации проводятся при подготовке, в ходе

проведения и по окончании совещания. Одним из важных элементов в работе руководства и должностных лиц предприятия по защите информации при проведений совещания является этап планирования конкретных организационно-технических мер, направленных на

исключение утечки конфиденциальной информации и на ее защиту.

Планирование мероприятий по защите информации включает выработку

конкретных мер, определение ответственных за их реализацию

Должностных лиц

(структурных подразделений) предприятия и сроков их выполнения (проведения). Планирование мероприятий по защите информации, проводимых в ходе совещания с участием представителей сторонних организаций, осуществляется под руководством руководителя предприятия и при непосредственном участии его заместителя, возглавляющего на предприятии работу по защите информации. При отсутствии в структуре предприятия данного должностного лица, непосредственная

ответственность за проведение планирования мероприятий по защите информации

9.4. Основы организации защиты информации в ходе издательской и

рекламной деятельности предприятия В настоящее время невозможно представить деятельность современного предприятия без его участия в издательской деятельности и рекламных акциях различного характера. Вместе с тем, для предприятий, осуществляющих работу с конфиденциальной информацией, такие его виды деятельности могут привести к распространению охраняемой информации о направлениях его деятельности и

проводимых работах. В связи с этим, в повседневной деятельности предприятия мероприятия по защите информации в процессе подготовки и реализации рекламных и издательских

проектов занимают важное место,

В соответствии с Федеральным законом РФ "О рекламе"43 в сфере рекламы

используются следующие основные понятия: реклама - информация, распространенная любым способом, в любой форме и с использованием любых средств, адресованная неопределенному кругу лиц и направленная на привлечение внимання к объекту рекламирования, формирование или

поддержание интереса к нему и его продвижение на рынке; объект рекламирования - товар, средство его индивидуализации, изготовитель или продавец товара, результаты интеллектуальной деятельности либо мероприятие (в том числе спортивное соревнование, концерт. конкурс, фестиваль, основанные на

риске игры, пари), на привлечение внимания к которым направлена реклама:

товар - продукт деятельности (в том числе работа, услуга), предназначенный

для продажи, обмена или иного введения в оборот;

рекламодатель - изготовитель или продавец товара либо иное определившее

объект рекламирования и (или) содержание рекламы лицо;

рекламопроизводитель - лицо, осуществляющее полностью или частично

приведение информации в готовую для распространения в виде рекламы форму;

рекламораспространитель - лицо, осуществляющее распространение рекламы

любым способом, в любой форме и с использованием любых средств.

Основными видами осуществляемой предприятием рекламной деятельности с

учетом положений федерального законодательства о рекламе, являются: 1 - наружная реклама, размещаемая на рекламных конструкциях в местах общего пользования. Под рекламными конструкциями в соответствий с Федеральным законом РФ "О рекламе" понимаются: щиты, стенды, строительные сетки, перетяжки, электронные табло и иные технические средства стабильного территориального размещения, монтируемые и располагаемые на внешних стенах, крышах и иных конструктивных элементах зданий, строений, сооружений или вне их, а также

остановочных пунктов движения общественного транспорта;

возлагастоя

на руководителя режимно-секретного подразделения (службы

безопасности).

Проведенне совещания без приглашения представителей сторонних организаций может проводиться без участия режимно-секретного подразделения (службы безопасности). В этих случаях ответственность за планирование и проведение мероприятий по исключению утечки конфиденциальной информации и по ее защите возлагаются на руководителя структурного подразделения предприятия, организующего данное совещание.

При планировании совещания предусматривается такая очередность рассмотрения вопросов, при которой будет исключено участие в их обсуждении лиц, не имеющих к ним прямого отношения.

Непосредственная разработка плана подготовки и проведения совещания

возлагается на структурное подразделение предприятия, организующее его про-ведение. В этом подразделении назначается должностное лицо, отвечающее за его подготовку, согласование с другими заинтересованными подразделениями предприятия, режимно-секретным подразделением (службой безопасности

и

представление в установленном порядке на утверждение руководителю предприятия (его заместителю). После утверждения плана руководством предприятия он доводится в части касающейся до всех заинтересованных должностных лиц (руководителей подразделений), до лиц, назначенных ответственными за выполнение отдельных мероприятий плана, он доводится под роспись.

Подготовка плана осуществляется заблаговременно до начала совещания и

включает мероприятия, проводимые перед проведением совещания, во время проведения совещания и по его завершении.

В плане указываются время и место проведения совещания, состав участников,

перечень предприятий, участвующих в совещании.

План мероприятий по защите информации при подготовке и в ходе проведения

/ совещания содержит следующие основные разделы:

W 1. Определение состава участников и их оповещение. В разделе отражаются: порядок формирования списка лиц, привлекаемых к участию в совещании, а также перечня предприятий, которым необходимо направить запросы с приглашениями; порядок подготовки и направления таких запросов; формирование содержания запросов.

1. ﻿﻿﻿Подготовка служебных помещений, в которых планируется проведение совещания. В разделе отражаются: работа по выбору служебных помещений; проверка соответствия помещений требованиям по защите информации; необходимость и целесообразность принятия дополнительных организационнотехнических мер, направленных на исключение утечки информации; оборудование рабочих мест участников совещания, в том числе средствами автоматизации, на которых разрешена обработка конфиденциальной информации. Определяется порядок использования средств звукоусиления, кино- и видеоаппаратуры (проекторов).

﻿﻿﻿Определение объема обсуждаемой информации. В данном разделе от ражаются: порядок определения перечня вопросов, выносимых на совещание, и очередности их рассмотрения; порядок оценки степени конфиденциальности вопросов; выделение вопросов, к которым допускается узкий круг лиц, участвующих в совещании.

4. Организация пропускного режима на территорию и в служебные помещения, в которых проводится совещание. В разделе отражаются вопросы организации и осуществления пропускного режима: виды пропусков и проставляемых на них условных знаком (шифров) для прохода в конкретные служебные помещения; порядок учета, хранения, выдачи и выведения их из действия (сроки уничтожения); режим прохода, посещения и пребывания в помещениях участников совещания.

Определяются количество и регламент работы основных и дополнительных контрольно-пропускных пунктов для прохода участников совещания на территорию и в служебные помещения.

5. Организация допуска участников совещания к рассматриваемым вопросам.

Раздел содержит мероприятия, касающиеся непосредственного допуска участников к вопросам, выносимым на совещание, с учетом порядка их обсуждения и степени конфиденциальности информации, к которой допущен каждый участник совещания.

6. Осуществление записи (стенограммы), фото-, кино-, видеосъемки совешания.

В разделе определяются порядок и возможные способы записи, съемки (стенографирования) хода совещания и обсуждаемых вопросов с учетом их кон-фиденциальности, а также должностные лица (подразделения), отвечающие за техническое обеспечение данного процесса.

1. ﻿﻿﻿Меры по защите информации непосредственно при проведении совещания. В разделе отражаются: порядок и способы охраны служебных помещений, меры по исключению прохода (проникновения) в них посторонних лиц, а также участников совещания, не участвующих в рассмотрении конкретных вопросов; мероприятия по предотвращению утечки информации по техническим каналам, силы и средства, задействованные при их проведении. Также определяются конкретные меры, исключающие визуальный просмотр и прослушивание ведущихся переговоров и обсуждения вопросов участниками совещания.
2. ﻿﻿﻿Организация учета, хранения, выдачи и рассылки материалов совещания. В

разделе отражаются порядок учета, хранения, размножения (печатания, ксерокопирования), выдачи, рассылки и уничтожения материалов совещания, а также рабочих тетрадей (блокнотов), предназначенных для записи обсуждаемых вопросов участниками совещания. Определяется порядок обращения с данными носителями информации непосредственно в ходе совещания и после его окончания. Особое внимание уделяется порядку учета, хранения, размножения и использования материалов совещания, зафиксированных на магнитных носителях (исполненных в электронном виде).

9. Оформление документов лип, принимавших участие в совещании. В данном разделе отражается порядок и сроки оформления документов, подтверждающих право доступа участников совещания к конфиденциальной информа- пии, предписаний (доверенностей) на участие в совещании, командировочных удостоверений;

10. Проверка и обследование места проведения совещания после его окончания. Раздел содержит мероприятня по организации и проведению визуальной проверки, а также проверки с непользованием специальных технических средств (аппаратуры) помещений, в которых проводилось совещание с целью выявления оставленных (забытых) технических устройств, носителей конфиденциальной информации и

личных вещей участников совещания. 11. Организация контроля выполнения требований по защите информации. В разделе отражается порядок, способы и методы контроля полноты и качества проводимых мероприятий, направленных на предотвращение утечки сведений конфиденциального характера, разглашения информации, содержащей такие сведения, и утрат (хищений) носителей информации. Указываются структурные подразделения

(должностные лица), на которые возлагаются вопросы контроля. Определяется система и порядок представления ответственными должностными лицами докладов о наличии носителей конфиденциальной информации и выявленных

нарушениях в работе по защите конфиденциальной информации.

Для каждого включаемого в план мероприятия определяются: срок (время) его проведения и ответственное за выполнение мероприятия должностное лицо

(подразделение).

9.2. Организация допуска участников совещания к обсуждаемым

вопросам.

Подготовка места проведения совещания

При использовании в ходе совещания сведений конфиденциального характера

или

обсуждении вопросов, содержащих

такие сведения, руководство предприятия-организатора, осуществляет комплекс мероприятий, направленных на

исключение ознакомления с ней посторонних лиц и сотрудников фирм- конкурентов.

На совещание приглашаются работники, имеющие непосредственное от-

ношением к рассматриваемым (обсуждаемым) вопросам. При обсуждении в ходе совещания вопросов, содержащих сведения, со- ставляющие государственную тайну, его участники должны иметь допуск к этим сведениям по соответствующей форме, а при рассмотрении вопросов, отнесенных к иным видам конфиденциальной информации, в установленном порядке оформленное

решение руководителя предприятия на допуск к данной категории (виду) информации.

При последовательном рассмотрении вопросов, имеющих различную степень конфиденциальности, к участию в совещании по каждому из рассматриваемых

вопросов допускаются лица, имеющие к ним непосредственное отношение. Должностное лицо, ответственное за проведение совещания, по указанию руководителя предприятия (подразделения, в чьих интересах проводится совещание)

формирует список лиц, участвующих в совещании. Этот список составляется на основании письменных обращений руководителей организаций, приглашенных к участию в совещании, и решений руководителей

подразделений предприятия-организатора по привлечению к участию в совещании своих сотрудников. В списке по каждому участнику указываются: фамилия, имя, отчество; наименование места работы и занимаемая должность; номер допуска к сведениям, составляющим государственную тайну, или номер решения руководителя о допуске к иной конфиденциальной информации; номера вопросов совещания, к обсуждению которых допущен участник. При необходимости в списке могут указываться и другие

сведения. Подготовленный список участников согласовывается с режимносекретным подразделением (службой безопасности) предприятия-организатора совещания и утверждается руководителем этого предприятия, давшим разрешение на его

проведение. Включенные в список участники совещания проходят в служебные помещения, в которых проводится совещание, предъявляя службе охраны (службе безопасности)

документ, удостоверяющий личность. Допускается проход в помещения участников • совещания организовывать по пропускам, выдаваемым им исключительно на период

проведения

совещания

отличающимся

OT

других

используемых

предприятием-организатором видов и образцов пропусков. Проверку документов, подтверждающих наличие у участников совещания допуска к сведениям, составляющим государственную тайну, и разрешений на ознакомление с конфиденциальной информацией, осуществляет служба безопасности

(режимно-секретное подразделение) предприятия-организатора совещания. Участники совещания имеют право посещения только тех служебных по- мещений, в которых будут обсуждаться вопросы, к которым эти участники имеют

непосредственное отношение. Совещания проводятся в служебных помещениях, в которых в установленном порядке разрешено обсуждение вопросов конфиденциального характера, и приняты

предусмотренные нормативными

правовыми

актами

необходимые организационно-технические мероприятия, предотвращающие утечку защищаемой

информации по техническим каналам. В ходе проведения совещания разрешается использование фото-, кино-, видео- и звукозаписывающей аппаратуры, защита которой обеспечивается в соответствии с требованиями по противодействию иностранным техническим разведкам и

технической защите информации. Проверка служебных помещений на предмет возможности обсуждения в них вопросов конфиденциального характера проводится накануне совещания специально

назначаемой комиссией, состоящей

ИЗ специалистов

противодействию иностранным техническим разведкам и технической защите информации

соответствующих подразделений предприятия-организатора.

* 1. **Порядок проведения совещания и использования его материалов**

Непосредственно перед началом совещания руководитель предприятия или

должностное лицо, ответственное за его проведение, обязан проинформировать

участников совещания о степени конфиденциальности обсуждаемых вопросов. В ходе совещания, в том числе и во время перерывов, работник, ответственный за его проведение, совместно со службой безопасности (режимносекретным

подразделением)

осуществляет необходимые организационнотехнические мероприятия, направленные на исключение утечки сведений конфиденциального

характера. Во время перерывов в совещании, а также после завершения обсуждения одного вопроса и перехода к обсуждению следующего, сотрудники службы безопасности (службы охраны) организуют контроль прохода (нахождения) в служебные помещения, в которых проводится совещание, лиц в соответствии с утвержденным

слиском участников. На все время проведения совещания запрещается пронос в служебные по- мешения, в которых оно проводится, индивидуальных видео- и звукозаписывающих устройств, а также средств связи (в том числе мобильных телефонов и приемников

керсонального вызова). В целях обеспечения их сохранности организуется камера

•кранения личных вещей участников совещания.

Звуко- и видеозапись, а также кино- и видеосъемка хода совещания и об- исуждения вопросов совещания проводится с разрешения руководителя предпри-

ия ия-организатора совещания только на учтенных в режимно-секретном подраз- -делении (службе безопасности) носителях. При этом использование в этих целях соответствующей аппаратуры и технических устройств осуществляется при со-

блюдении требований по защите информации. Носители конфиденциальной информации, а также сведений, составляющих государственную тайну, выдаются режимно-секретным подразделением (службой безопасности) участникам совещания под роспись, а после окончания совещания возвращаются. Контроль за своевременным возвратом этих носителей осуществляется

согрудниками вышеуказанных подразделений. Для осуществления записей хода совещания и обсуждаемых вопросов участникам совещания установленным порядком выдаются рабочие тетради или рабочиз блокноты, учтенные в службе безопасности (режимно-секретном под- разделении) и имеющие соответствующий гриф секретности (степень конфи- денциальности). Эти рабочие тетради (блокноты) по окончании совещания воз- вращаются в службу безопасности (режимно-секретное подразделение). При необходимости они могут быть секретной (конфиденциальной) почтой направлены для дальней шего хранения и использования на предприятия, представители которых

производили в них записи на совещании. Игоговые документы совещания, а также материалы выступлений участников, в том числе и оформленные в электронном виде, в установленном порядке высылаются на прецириятия, направлявшие на совещание своих представителей, а также в вышестоящие органы государственной власти (предприятия). Расчет рассылки

материлов определяет руководитель предприятия-организатора.

Лицам, принимавшим участие в совещании, без письменного разрешения

предприятия-организатора совещания запрещается использовать материалы со- вещания и его результаты при взаимодействии (проведении работ, переписке) с

предприятиями, представители которых на него не приглашались.

9.4

Пункт 2 реклама на тв и радио а также в переодических печатных изданиях

1. Реклама распространяемая по сетям электросвязи и размещаемая в почтовых отправлениях
2. Реклама на т/с и их использование
3. Реклама в ходе конференций, симпозиумах проводимых вне предприятиях
4. Рекламав глобальных инф сетях общщего пользования
5. Реклама в ходе проведения внутр предприятий проводимых преприятием с привлечением представителей других организаций, СМИ

Основными направлениями защиты конф инф в ходе осущ предприятием …

1. Подготовка и экспертиза предполагаемых к распростр данных на наличие инф с ограниченным доступом
2. Анализ материалов подготавлеемых рекламопроизводителем и рекламораспространиелям в средствах рекламы
3. Постоянный контроль порядка выхода и содержания рекламных материалов не в зависимости от их формы распространения

**Организация аналитической работы  
состояние защиты конфиденциальной  
информации**

Анализ состояния защиты инф это комплексное органическое взаимосвязанное изучение фактов, событий, процессов, явлений, связанных с проблемами защиты охраняемой инф

Исследование данных путём обработки инф по выявлению каналов утечки и нарушение режима секретности (конфиденциальности) в ходе повседневной деятельности организации , аналитическая работа на предприятии организуется и проводится с целью накопления обобщения и исследования инф, материалов фактов и событий связанных с проблемой защиты конфиденциальной информации

Основное предназначение аналитической работы – выработка эффективных мер предлжений и рекомендаций руководствуу напрвленных на недопущение утечки свед конфидент инф о деят предприятия и проводимых работах в процессе этой работы обязательно должны присутствовать прогнозирования возможных действий противника

Основными направлениями аналитической работы являются:

1. Анализ объекта защиты
2. Анализ внутренних и внешних угроз
3. Анализ возможных каналов НСД
4. Анализ системы комплексной безопасности объекта
5. Анализ имеющих место наруш режима конфид инф
6. Анализ предпосылок к разглашению инф, а также утрате носителей конфидент инф

Аналитической работой занимется специально созданное структурное подразделение укомплектованное квалифиц специалистами в обл ЗИ, эти специалисты в полной мере должны владеть инф по всем направлениям деят организации, знать виды, характер последовательность проведения работ взаимодейст организации, специфику деят структурных подразделений

Как правило аналитическое подразделение входит в состав службы безопасности предприятия

Аналитическое подразделени как правило единое и взаимосвязанное структурой обеспечение руководства предприятия достоверной и аналитически обработанной информации, направленной на полноценную инф поддержку принятия эффективных управленческих решений по всем направлениям ИБ

Основными функциями такого подразделение явл:

1. Обеспечение своевременного поступления достоверной и всесторонней инф по проблемам защиты конфидент инф организации
2. Моделирование реального сценария возможных действий конкурентов в которой могут затрагивать интересы
3. Осущ постоянного мониторинга событий и фактов на рынке продукции товаров и услуг, а также во внешней среде которые могут иметь значение для деят инф
4. Обесп ИБ собственных инф ресурсов
5. Обесп эффективности работы по анализу имеющейся инф, иск дублирования при её сборе, обработки и распространению
6. Подготовка выводов и предположений на основе проводимой работы работы

Одним из осн источников для изучения обобщения и обработки инф, являются материалы контроля состояния защиты конфидент инф на предприятии

Контроль – целенаправленная деятельность руководства и должностных лиц предприятия по проверке состояния защиты конфидент инф в ходе его повседневной деятености при проверке всех видов работ

Эти мероприятия организуются и проводятся с целью определения тстенного состояния дел по вопросам ЗИ оценки эффективности для принемаемых мер для искл утечки инф и тд

Такой контроль выполняется в установленном порядке и в сроки опред нормативно-правов актами и методтческими документами

Плановые проверки распред в течении календарного года и месяца и известны заранее

Внезапные проводятся по указанию руководителя или его зама, могут проводиться масштабно по всему преприятию или в его структурных предприятиях или фелиалах

Комплексные проверки проводятся по всем направлениям ЗИ на предприятии

Основные задачи контроля:

1. Проверка наличия носителей конфидент инф
2. Соблюдение всеми сотрудниками норм и правил устанавливающих порядок обращения с носителямт кофидент инф
3. Анализ состояния дел по вопросам защиты инф
4. Выявление угроз в защите кофид инф и выработка мер по их нейтрализации
5. Оказание практической помощи должностным лицам приведении проверяемых вопросов с нормативно-правовыми актами
6. Принятие мер административной и дисципленарной ответственности к лицам нарушающим требования по порядку обращения с носителями кофид инф

**Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений**

Определения:

Разглашение сведений конфиденциального характера – это придание их огласки работниом который в утановленном порядке имел допуск к данным сведений в процессе выполнения обязанностей в результате чего они стали достоянием посторонних лиц

Под утратой носителей свед конфиденциального характера понимается выход (даже на короткое время) носителей сведений из владения работником который в установленном порядке имел допуск к данным носителям при выполнении своих должностных обязанностей в результате чего они стали достоянием посторонних лиц

За разглашение свед конфид характера и утраты носителей этих свед нарушитель привлекается к административной и уголовной ответственности

О факте утраты таких носителей сведений руководитель структурного подразделения обязан сообщить об этом руководителю предприятия и руководителю службы безопасности вышестоящее предприятие организовывается служебное расследование и розыск утраченных носителей, принемаются меры по локализации возможного ущерба

Об этом факте также сообщается в органы безопасности в дальнейшем все мероприятия планируются во взаимодействии с органами безопасности

Для проведения служебного расследования, руководитель организации не позднее следующего дня после обнаружения данного факта назначает комиссию из компетентных и незаинтересованных в исходе дела лиц в составе 3х человек один из которых режимно-сектретного подразделения все они должны иметь прямое отношение к этим сведениям и соответствующий допуск, во время проведения этого расследования эти работники могут освобождаться от своих должностных обязанностей

Комиссия по ведению служебного расследования обязана:

1. Установить обстоятельства разглашения свед/ утраты носителей
2. Проводить розыск утраченных носителей
3. Установить лица виновные в разглашении сведений / утраты носителей
4. Установить причины и условия способствующие разглашению сведений и утраты и выработать рекомендации по их устранению

Комиссия имеет право:

1. Проводить обыск помещения (хранилища столы спец портфели т.п.)
2. Проверять полистно конфиденциальные документы, учётную документацию отражающую их поступление и движение носителей сведений конфиденциальной информации
3. Опрашивать работников предприятия допустивших разглашение этих свед или утрату, а также других работников способных оказать содействие в установлении обстоятельств разглашения конфиденциальных сведений или утраты носителей и получать с них письменные объяснения
4. Привлекать с разрешения руководителя предприятия других работников этой организации незаинтересованных в исходе расследования для проведения отдельных действий в рамках служебного расследования
5. При наличии достаточных оснований и решения органа безопасности по факту этого нарушения возбуждается уголовное дело и проводятся необходимые следственные мероприятия – обыск помещения, изъятие документов и материалов (обыск производится для обыска и фиксации доказательств, а также поиска предметов и ценностей которые могут быть конфискованы по приговору суда)

В результате обыска могут быть обнаружены и изъяты только овеществлённые объекты – орудия преступления; предметы, документы и иные носители инф; ценности

В соответствии со статьёй 182 УК РФ; обыск может быть произведён на основании постановления следователя, судебного решения, если предполагается изымать предметы и материалы составляющие гостайну то это производится по постановления следователя и с санкции прокурора

При этом привлекаются не менее двух сведетелей и экспертна группа, а также сотрудников выполняющую оперативно-розыскную деятельность и всё это отображается в протаколе

Все изъятые предметы упаковываются и опечатываются за подписью понятых

Выемка информации в электронном виде возможна в 2х вариантах:

1 изымается жёсткий диск и другие носители

2 изымается только та часть инф которая имеет отношение к делу если её можно вычленить

Все эти действия обязательно фиксируются электронный носитель опечатывается, а распечатанная в бумажном носителе подписывается понятыми и следователем

Служебное расследование проводится в предельно краткий срок, но не более месяца со дня обнаружения факта разглашения или утраты

Если. Утраченные носители не обнаружены в результате проведения мероприятий но внесена ясность в обстоятельства ураты и выявлены виновный то розыск прекращается мотивированное заключение о прекращении розыска утверждается руководителем предприятия, после чего орно рассматривается и утверждается руководителем вышестоящего предприятия

По оканчанию расследования комиссия обязана представитьь руководителю документы:

1. Заключение о результатах расследования
2. Писменные объяснения лиц которых опрашивали
3. Акты проверок
4. Другие документы имеющие отношения к расследованию

Одновременно с комиссией по проведению служебного расследования, формируется комиссия по уточнению или определению степени секретносити разглашённых документов или утраченных носителей. Комиссия составляется из 3х человек незаинтересованных в исходе дела, но имеющих прямое отношение в исходе дела, результаты работы комиссии отражаются в заключении комиссии которое в предельно короткий срок не больше 10 дней со дня создания комиссии предоставляется руководителю

По результатам работы комиссии руководитель принимает меры по локализации проблемы разглашения или утраты. Если. Комиссия по определению секретности выявила что степень секретности разглашённых или утраченных не соответствует их содержанию, то заключение комисси утверждается руководителем вышестоящего преприятия или органа госвласти наделёнными такими полномочиями по распоряжению такими сведениями

При необходимости проводится дополнительная комиссия или проводится дополнительное служебное расследование

Составляется заключение о степени секретности разглашённых сведений и один материал хранится в службе безопаности и производится списани с учёта утраченных носителей и утверждается руководителем предприятия и подтверждается руководителем в форме акта и фиксируется в Журнале учёта утрат секретных документов и фактов разглашения сведений конфиденциального характера

**Правовая защита конфиденциальной информации**

**Уголовно-правовая защита сведений, составляющих  
коммерческую, налоговую или банковскую тайну**

Характер и объём сведений, составляющих коммерческую, налоговую или банковскую тайну, определяются самим обладателем информации. Им же обеспечивается охрана ее конфиденциальности.

В соответствии с частью 1 статьи 183 УК РФ информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам. Сведения, которые не могут составлять коммерческую тайну, определяются законом и иными нормативными актами.

Налоговую тайну в соответствии со статьей 102 Налогового Кодекса РФ составляют любые полученные налоговым органом, органами внутренних дел, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений: разглашенных налогоплательщиком самостоятельно или с его согласия; об идентификационном номере налогоплательщика; о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения; предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация, о взаимном сотрудничестве между налоговыми, таможенными или правоохранительными органами (в части сведений, предоставленных этими органам).

К банковской тайне в соответствии со статьёй 26 ФЗ РФ «О банках и банковской деятельности» относятся сведения об операциях, счетах и вкладах клиентов банка и его корреспондентов.

Статья 183 УК РФ предусматривает 3 различных состава преступления, которые имеют один предмет посягательства – сведения, составляющие коммерческую, налоговую или банковскую тайну. В части 1 комментируемой статьи предусмотрена ответственность за собирание таких сведений путём похищения, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений. Наказуемы сами действия предусмотренные в части 1 данной статьи, независимо от того, являлись ли их результатом какие-либо последствия. Мотив преступления на квалификацию не влияет.

Субъектом преступления может быть любое лицо, достигшее   
16-летнего возраста, не являющееся владельцем коммерческой, налоговой или банковской тайны и не допущенное к ней в установленном порядке.

Часть 2 коммерческой статьи предусматривает ответственность за незаконные разглашения или использование сведений6 составляющих коммерческую, налоговую или банковскую тайну, без согласия се владельца, совершенные из корыстной или иной личной заинтересованности и причинившие крупный ущерб. Согласно части 2 комментируемой статьи субъектом преступления может быть любой работник организации или иные лица, которым сведения, составляющие коммерческую, налоговую или банковскую тайну, стали известны в связи с профессиональной или служебной деятельностью.

Часть 3 комментируемой статьи предусматривает ответственность за те же деяния. если в результате их совершения причинен крупный ущерб, а равно при наличии корыстной заинтересованности виновного. Обязательные элементы состава преступления – корыстная или иная личная заинтересованность виновного и крупный ущерб как последствие уголовно наказуемых действий.

В соответствии с частью 4 комментируемой статьи ответственность наступает за

деяния, предусмотренные частью 2 или 3 этой статьи, повлекшие тяжкие последствия.

Обязательное условие ответственности виновного лица по части 4 комментируемой статьи – наступление в результате указанных в части 2.3 этой статьи действий виновного лица тяжких последствий. Этот признак оценочный. Он может выражаться как в материальном, так и в ином ущербе.

При определении последствий преступления следует исходить как из стоимости оценки ущерба, так и из других существенных обстоятельств, например материального положения собственника или иного владельца имущества. Тяжкими последствиями могут быть признаны, например, экономическое разорение, дезорганизация работы коммерческого предприятия и т.п. Преступления, предусмотренные комментируемой статьей, совершаются умышленно.

**Уголовно-правовая защита в сфере  
компьютерной информации**

Информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Под компьютерной информацией понимаются не сами сведения, а форма их представления в машиночитаемом виде, т.е. совокупность символов, зафиксированная в памяти компьютера либо на машинном носителе (дискете, оптическом, магнитооптическом диске, магнитной ленте либо ином материальном носителе).

Объективную сторону преступлений в сфере компьютерной информации составляет неправомерный доступ к охраняемой законом компьютерной информации (статья 272 Уголовного кодекса РФ, см. приложение 9), который всегда носит характер совершения определенных действий и может выражаться проникновении компьютерную систему путем:

1. использования специальных технических или программных средств, позволяющих преодолеть установленные системы защиты;
2. незаконного использования действующих паролей или кодов для проникновения в компьютер, либо совершении иных действий в целях проникновения в систему или сеть под видом законного пользователя;
3. хищения носителей информации, при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации.

Неправомерным признается доступ к компьютерной информации лица, не обладающего правами на получение и работу с данной информацией либо компьютерной системой. Причем в отношении этой информации либо системы должны приниматься специальные меры защиты, ограничивать круг лиц, имеющтх к ней доступ. (это вторая фотка)

yf под охраняемой заеоном инф понимается инф для которой в специальных законах установлен специальный режим

а равно выключение реакции какого либо устройства   
сис или сети эвм при сохранении самой инф модификация инф внесение изменений в программы базы данных текстовую инф находящуюся на материальных носителях   
копирование инф – перенос инф на другой материальный носитель при неизменной перваначальной инф   
нарушение работы эвм – системы эвм или их сети что может выразиться как в нарушении работы отдельных программ баз данных выдачи искажённое инф так и внештатно то есть не предусмотренным спец инструкциями функционирование програмно аппаратных средств и перферийных устройств либо нарушение нормального функционирования сети  
важным явл установление причины связи между нсд и наступления последствий при этом следует учитывать что неправомерный доступ может осуществляться с одной компьютерной инф а последствия с другрй  
при функционировании сложных комп сис возможно уничтожение блокирование и нарушение эвм