АВТОМАТИЗАЦИЯ ДЕЛОПРОИЗВОДСТВА, ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ И ЗАЩИТА ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИИ

«Доктрина информационной безопасности Российской Федерации» (Указ Президента Российской Федерации № 1895 от 09.09.2000 г.)

Одним из главных стратегических национальных ресурсов, основой экономической и оборонной мощи государства становятся информация и информационные технологии.

Информация в современном мире является таким атрибутом, от которого в решающей степени зависит эффективность жизнедеятельности современного общества.

Информационные технологии принципиально изменили объём и важность информации, обращающейся в технических средствах её хранения, обработки и передачи.

Всеобщая компьютеризация основных сфер деятельности привела к появлению широкого спектра внутренних и внешних угроз, нетрадиционных каналов утечки информации и несанкционированного доступа к ней.

Массовое оснащение государственных учреждений, предприятий, организаций и частных лиц средствами вычислительной техники и включение их в мировое информационное пространство таит в себе реальную угрозу создания разветвлённых систем регулярного несанкционированного контроля за информационными процессами и ресурсами, злоумышленного вмешательства в них.

ОСНОВНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ДОКУМЕНТООБОРОТА

1.Автоматизация делопроизводства.
-изготовление, копирование, размножение документов с помощью СВТ;
-применение СВТ для учета, поиска документов.
2.Переход к электронному документообороту.
-создание АС для обмена документами внутри предприятия;
-обмен электронными сообщениями между предприятиями с использованием ЭП.

Система электронного документооборота

Документ **«Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать». ГОСТ Р 51141-98 «Делопроизводство и архивное дело. Термины и определения».**

Гражданский кодекс РФ

ст.160 («Письменная форма сделки») при совершении сделок допустимо применение электронной подписи (а, следовательно, допустим и обмен документами в электронной форме)

В соответствии со ст. 434 ГК РФ («Форма договора») договор в письменной форме может быть заключен путем обмена документами электронной связи, позволяющей достоверно установить, что документ исходит от стороны по договору

Федеральный закон «Об электронной подписи»

Ст. 4 и ст. 19 Электронная цифровая подпись в электронном документе является не просто равнозначной собственноручной подписи на бумажном носителе, но и в ряде случаев признается равнозначной подписи личности, заверенной печатью.

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

Ст.11.п.3 Электронное сообщение, подписанное электронной подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью.

Электронный документооборот (ЭДО) - обмен электронными документами в соответствии с установленным регламентом

Система электронного документооборота (СЭД) - организационно-техническая система, представляющая собой совокупность программного, информационного и аппаратного обеспечения, реализующая электронный документооборот.

Электронный документ - документ, в котором информация представлена в электронно - цифровой форме («Закон об ЭЦП»).

ЭЛЕКТРОННОЕ СООБЩЕНИЕ -
информация, представленная в форме набора состояний элементов электронной вычислительной техники, иных электронных средств обработки, хранения и передачи информации, могущей быть преобразованной в форму, пригодную для однозначного восприятия человеком.

«Обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами». Федеральный Закон 2006 г. № 149 «Об информации, информационных технологиях и о защите информации»

Электронный документооборот

Включает в себя:

- формирование электронного документа;
- отправку и доставку электронного документа;
- проверку электронного документа;
- получение и подтверждение получения электронного документа;
- учет электронных документов (регистрацию входящих и исходящих электронных документов);
- контроль за ходом перемещения (и исполнения) электронного документа;
- хранение электронных документов (ведение архивов электронных документов);

Основные проблемы, которые могут возникнуть в процессе функционирования систем ЭДО

- проверка подлинности электронного документа;
- возможность использования электронных документов в качестве доказательств в судах;
- распределение риска убытков, которые могут возникнуть в процессе функционирования систем ЭДО;
- взаимоотношения юридических лиц, использующих ЭДО, с органами власти и организациями, куда необходимо представлять отчетность о своей деятельности;
- Международные правовые проблемы, которые могут возникнуть, когда участники ЭДО и провайдер находятся в разных странах;
- стандартизация;
- Обеспечение безопасности электронного документооборота

РАСПРОСТРАНЕННЫЕ В РФ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

1. КОДЕКС-документоборот.
2. ЕВФРАТ-документооборот.
3. Комита – документооборот.
4. Босс-референт.
5. Оптима WORK-FLOW/
6. Тайлос.
7. Мегаполис-делопроизводство.

КАНАЛЫ УТЕЧКИ И ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

• электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящими за пределы КЗ;

• несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;

• воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;

• побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих важную информацию, и линий передачи этой информации;

• наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания заземления и линии связи, выходящие за пределы КЗ;
• радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;

- **радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации "закладочных устройств", модулированные информативным сигналом;**
- **радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;**

• просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;
• хищение технических средств с хранящейся в них информацией или отдельных носителей информации.

Перехват информации или воздействие на информацию с использованием технических средств могут вестись:

- **из-за границы КЗ из близлежащих строений и транспортных средств;**
- **из смежных помещений, принадлежащих другим м предприятиям и расположенным в том же здании, что и объект защиты;**
- **при посещении предприятия посторонними лицами;**
- **за счет несанкционированного доступа (несанкционированных действий) к информации, циркулирующей в АС, как с помощью технических средств АС, так и через информационные сети общего пользования.**

В качестве аппаратуры перехвата или воздействия на информацию и технические средства могут использоваться портативные возимые и носимые устройства, размещаемые вблизи объекта защиты либо подключаемые к каналам связи или техническим средствам обработки информации, а также электронные устройства съема информации "закладочное устройство", размещаемые внутри или вне защищаемых помещений.

ОРГАНИЗАЦИЯ РАБОТ ПРИ ОБРАБОТКЕ ЗАКРЫТОЙ ИНФОРМАЦИИ НА СРЕДСТВАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ (СВТ) И В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ (АС)

ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

1.Определения перечня информации подлежащей обработке.

2.Определение технических средств необходимых для обработки информации.

3.Категорирование СВТ /АС/.

4.Формирование перечня пользователей и режима их работы.

5.Разработка системы доступа в помещение и к информационным ресурсам в СВТ /АС/.

ОСНОВНЫЕ МЕРОПРИЯТИЯ

6.Определение порядка приобретения, приемки и режима эксплуатации СВТ и средств защиты информации.
7.Монтаж, установка средств ЗИ.
8.Назначение работников ответственных за БИ.
9.Обучение, переподготовка и повышение квалификации персонала в области защиты информации.
10.Опытная эксплуатация СВТ /АС/.
11.Аттестование объекта информатизации.
12.Ввод в эксплуатацию.

Безопасность Электронного документооборота

Под безопасностью электронного документооборота понимается состояние данного процесса, отражающее степень защищенности его участников от противоправных действий и их последствий.

Электронный документооборот

Угрозы

Несанкционированный доступ

Утечка по техническим каналам

Обеспечение безопасности информации в системах ЭДО

Источниками угроз безопасности информации в системах ЭДО являются

- субъекты (нарушители), осуществляющие умышленные незаконные действия в отношении информации, циркулирующей в системах ЭДО;

- субъекты (нарушители), создающие непреднамеренные угрозы безопасности информации, обрабатываемой и хранящейся в системах ЭДО;

технические аварии (отказы оборудования, внезапное отключение электропитания, протечки и т.п.);

стихийные бедствия (пожары, наводнения и т.п.);

Обеспечение безопасности информации в системах ЭДО

Основные объекты воздействия в системах ЭДО при реализации угроз

- средства информатизации (помещения, средства вычислительной техники, автоматизированные системы (подсистемы), сети, средства и системы связи и передачи данных);
- Открытая информация, информация ограниченного доступа, циркулирующая в системах ЭДО в процессе информационного взаимодействия;

общесистемные и прикладные программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение);

средства защиты информации;

средства контроля эффективности защиты информации в системах ЭДО

Обеспечение безопасности информации в системах ЭДО

Угрозы, связанные с возможностью целенаправленного осуществления незаконных действий в отношении систем ЭДО могут осуществляться (способ реализации угроз):

- **путем несанкционированного получения средств аутентификации пользователей с последующим несанкционированным доступом к конкретным ресурсам системы ЭДО;**
- **внедрением программ, обеспечивающих получение контроля над информационными потоками и (или) ресурсами системы ЭДО**
- **путем хищения закрытых ключей или физического вывода из строя технических средств;**
- **с помощью технических средств, позволяющих контролировать сетевой трафик;**
- **путем внедрения технических и программных средств скрытного съема информации с рабочих станций, средств связи и других технических устройств в системах ЭДО, в которых обрабатывается защищаемая информация;**

Обеспечение безопасности информации в системах ЭДО

Угрозы, связанные с возможностью целенаправленного осуществления незаконных действий в отношении систем ЭДО могут осуществляться (способы реализация угроз):

- **путем обхода механизмов разграничения доступа, возникающего вследствие несовершенства общесистемных компонентов программного обеспечения (операционных систем, систем управления базами данных и др.);**
- **путем модификации используемого программного обеспечения систем ЭДО для получения возможности несанкционированного доступа к защищаемой информации.**
- **с применением технических средств съема информации по возможным каналам ее утечки**

Обеспечение безопасности информации в системах ЭДО

Угрозы, связанные с действиями законных пользователей в отношении систем ЭДО могут осуществляться:

- при нарушении технологии хранения, обработки, передачи и защиты информации;

- при нарушении установленных правил обращения с информацией

наибольшую угрозу безопасности информации в системах ЭДО представляют умышленные действия субъектов (нарушителей), в т. ч. законных пользователей, направленные на нарушение конфиденциальности, целостности и доступности информации.

Обеспечение безопасности информации в системах ЭДО

Несанкционированный доступ к электронному документу может быть получен:

Путем физического доступа к носителям информации

- **изъятия носителей информации;**
- **хищения носителей информации;**
- **копирования с носителей информации;**
- **Информация может быть прочитана «через плечо» с экрана монитора при работе зарегистрированного пользователя.**

Методами дистанционного сьема информации

- **программы-шпионы;**
- **специальные аппаратные средства, обеспечивающие неправомерный доступ к информации, в том числе в каналах связи;**
- **использование специальных технических средств для перехвата электромагнитных излучений ПК (с помощью направленной антенны такой перехват возможен в отношении персонального компьютера на расстояниях до 1 км).**

Обеспечение безопасности информации в системах ЭДО

Неправомерный доступ к конфиденциальной информации находящейся на жестком диске может быть осуществлен путем:

Путем физического доступа к информации

- несанкционированного проникновения в помещение, где установлен ПК, с получением дальнейшего доступа к конфиденциальной информации;
- несанкционированного подключения к ПК внешних и (или) съемных носителей с целью копирования информации, несанкционированного копирования конфиденциальной информации на магнитные носители, а также несанкционированного получения печатных копий документа;
- хищения жесткого диска с конфиденциальной информацией или самого ПК;

Методами дистанционного съема информации

- использование заранее загруженных на ПК программных средств(в том числе вирусов);
- получения доступа к ПК при помощи существующей внутренней сети, в том числе через Интернет
- применения технических средств дистанционного съема информации с работающего ПК.

Обеспечение безопасности информации в системах ЭДО

Неправомерный доступ к конфиденциальной информации находящейся на съемных магнитных носителях может быть осуществлен:

Путем физического доступа к информации

- несанкционированного проникновения в помещение, где установлены съемные носители ПК, с получением дальнейшего доступа к конфиденциальной информации;
- несанкционированного подключения съемных носителей к ПК с целью копирования информации;
- хищения съемных носителей с конфиденциальной информацией;

Методами дистанционного сьема информации

получения доступа к подключенным к ПК съемным носителям, используя существующую внутреннюю сеть, в том числе через Интернет;

применения технических средств дистанционного снятия информации с работающего ПК, к которому подключены съемные носители.

Обеспечение безопасности информации в системах ЭДО

Реализации основных угроз безопасности информации способствуют:

- **отсутствие или недостаточность мер по защите информации при работе в Интернете;**
- **бесконтрольное использование флэш-карт;**
- **бесконтрольное использование мобильных телефонов с определенным набором функций;**
- **применение нелицензионного программного обеспечения;**
- **отсутствие или недостаточность организационных и технических мер по предотвращению НСД к информации и физического доступа к системам ЭДО, в т.ч. по каналам связи;**
- **недостаточно развитое чувство ответственности за обеспечение безопасности информации у пользователей.**

Обеспечение безопасности информации в системах ЭДО

Возможные последствия в случае реализации угроз безопасности информации в системах ЭДО

ухудшение качества функционирования системы управления в органах власти и организациях

сбои в работе систем обеспечения жизнедеятельности (транспорт, энергоснабжение,, ПФР, ФНС и др.)

Экономический, финансовый, моральный ущерб обладателям и пользователям систем ЭДО

нарушения конституционных прав граждан;

снижение авторитета, деловой репутации и, соответственно, степени доверия к органам вадасти, организациям

предпосылки к нарушению социальной стабильности.

Обеспечение безопасности информации в системах ЭДО

Основные деструктивные действия нарушителей в системах ЭДО

- **нарушение конфиденциальности информации ограниченного доступа путем перехвата техническими средствами разведки, хищения или копирования**
- **блокирование общедоступной информации (нарушение доступности информации);**
- **уничтожение информации;**
- **модификация (искажение) информации;**
- **нарушение адресности при передаче информации по каналам связи;**
- **отрицание подлинности информации;**
- **навязывание ложной информации.**

Угрозы безопасности в системах ЭДО. Угрозы компьютерной преступности

В 2006 по данным МВД России в Российской Федерации выявлено 15 000 преступлений с использованием Интернет

Неправомерный доступ в компьютерные сети органов государственной власти, организацийк	Разглашение сведений, содержащих информацию с ограниченным доступом Компьютерное пиратство Распространение вредоносных программ Телефонное пиратство Неправомерное использование сетевых реквизитов при авторизации в Интернете
Хищение инфоормации	Распространение в “свободной продаже”: сведений, содержащие государственную тайну и др. информацию с ограниченным доступом баз данных МВД, ФНС, других органов государственной власти; данных о финансовых операциях, идентификационных данных платежных карт; кодов сим-карт;.
Распространение информации террористического и экстермисткого характера	Как организовать теракт; Как изготовить взрывное устройство; Как убить человека и.т.д.
Навязывание информации	спам

Более 90% совершается внутренними пользователями. Общий объем ущерба – миллиарды долларов

Обеспечение безопасности информации в системах ЭДО

Вывод: гипотетический злоумышленник (который может быть и сотрудником фирмы) должен получить непосредственный доступ (физический или программный) к носителю информации.

При использовании программ-шпионов или вирусов нужно заставить (тем или иным образом) пользователя загрузить на свой компьютер (или носитель) необходимое для этой цели программное обеспечение.

Задача - защитить доступ (физический и программный) к системам ЭДО и их элементам, в которых хранится и обрабатывается конфиденциальная информация таким образом, чтобы максимально удорожить процесс несанкционированного доступа к защищаемым данным.

Обеспечение безопасности информации в системах ЭДО

Задача решается путем

Обеспечения сохранности документов

Обеспечения безопасного доступа к электронным документам

Обеспечения подлинности документов

Обеспечение безопасности информации в системах ЭДО

Обеспечение сохранности документов

Контролируемый доступ к документам.

Централизованное хранение и резервное копирование документов.

Предотвращение утраты и несанкционированного уничтожения документов.

Обеспечение безопасного доступа к электронным документам

Разграничение доступа к документам.

Шифрование информации на основе паролей.

Шифрование информации на основе сертификатов (электронные ключи).

Гарантированное уничтожение документов

Стирание электронных копий со всех видов носителей.

Уничтожение всех следов пребывания данного документа в организации.

Физическое уничтожение носителей.

Обеспечение безопасности информации в системах ЭДО

Обеспечение подлинности документов,

Наличие у пользователя зарегистрированного сертификата открытого ключа. Секретный закрытый ключ находится только у его владельца и недоступен другим пользователям; ответственность за его сохранность несет владелец ключа.

Протоколирование ЭДО и контроль действий пользователей

Определение ответственности пользователей в должностных инструкциях (регламентах)

Регистрация событий в системе ЭДО

Немедленное реагирование на нарушения, допущенные пользователями установленного порядка работы с применением соответствующих административных и технических мер

Учет электронных документов

Техническая защита объектов информатизации и каналов передачи данных

Система ЭДОи ее отдельные элементы должны быть классифицированы по требованиям безопасности информации

Должны быть выполнены все мероприятия в соответствии с присвоенным классом защищенности

Постоянный контроль за эффективностью мер по защите информации

Наличие подготовленных специалистов, ответственных за защиту информации

Обеспечение функционирования и безопасности средств защиты информации

Учет электронных документов

Осуществляется путем ведения электронных журналов учета. Программные средства ведения электронных журналов учета являются составной частью программного обеспечения, используемого для организации электронного документооборота.

Технология ведения электронных журналов учета включает программно-технологические процедуры заполнения и администрирования электронных журналов и средства хранения этой информации.

Электронный журнал учета подлежит защите от НСД, непреднамеренного искажения или уничтожения учетных данных журнала

Обеспечение безопасности информации в системах ЭДО

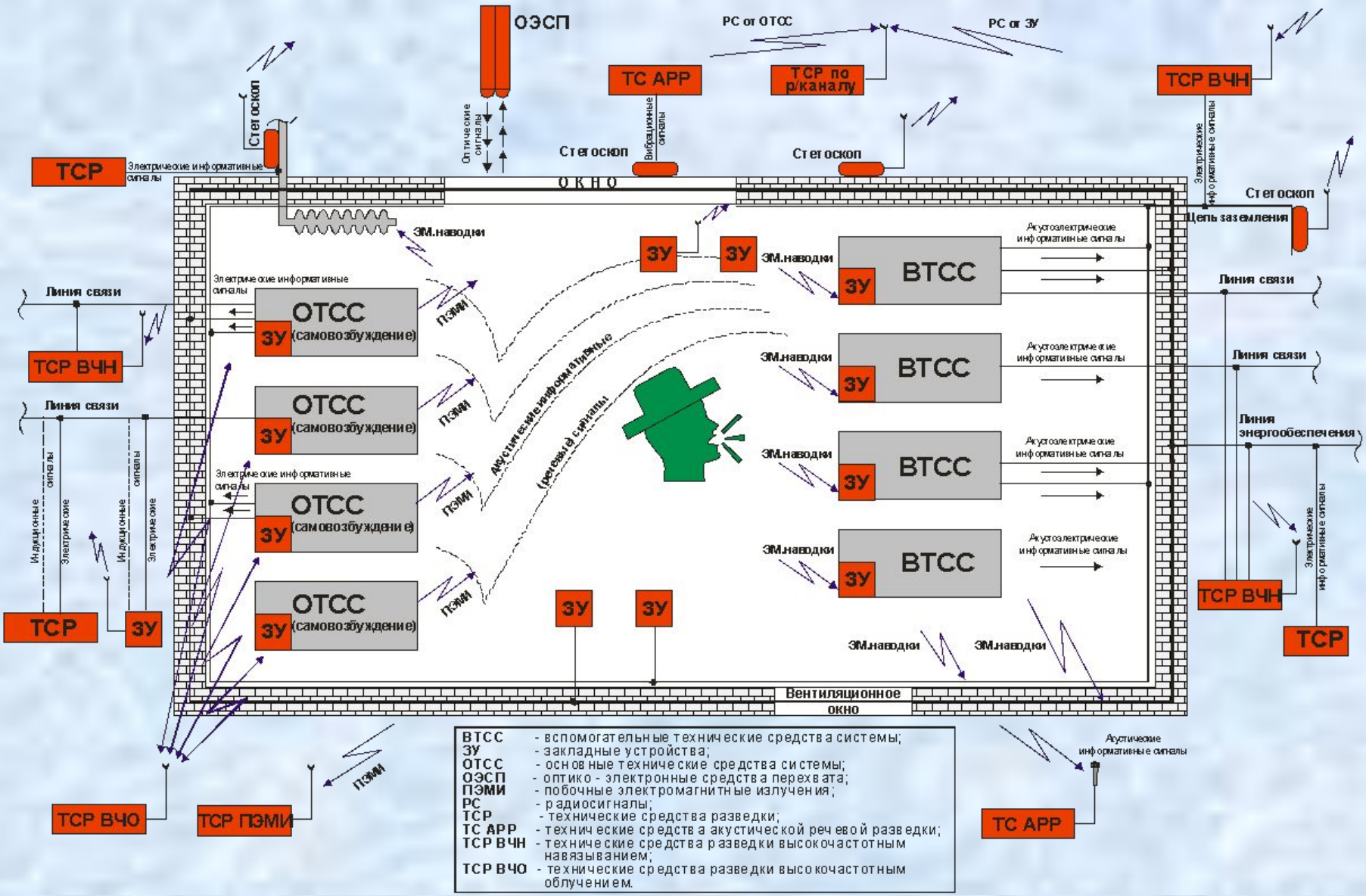
Соблюдение требований безопасности информации при организации электронного документооборота должно обеспечить:

- **конфиденциальность информации (получить доступ к информации может только определенный круг лиц);**
- **целостность передаваемой информации (гарантирование, что данные передаются без искажений и исключается возможность подмены информации);**
- **аутентификацию (когда передаваемую информацию может получить только то лицо, кому она предназначена, а отправителем является именно тот, от чьего имени она отправлена).**
- **Требования к безопасности информации при организации электронного документооборота реализуются посредством применения программно-технических средств защиты информации и организационных мер.**

Обеспечение безопасности информации в системах ЭДО

К программно-техническим средствам относятся:

- **программные средства, специально разработанные для осуществления электронного документооборота;**
- **система паролей и идентификаторов для ограничения доступа пользователей и администраторов к техническим и программным средствам системы электронного документооборота;**
- **средства электронной подписи;**
- **средства криптографической защиты информации;**
- **программно-аппаратные средства защиты от несанкционированного доступа;**
- **средства защиты от программных вирусов;**
- **средства защиты от утечки по техническим каналам , в т.ч. по каналам связи**



Модель технических каналов утечки информации на типовом объекте информатизации

Обеспечение безопасности информации в системах ЭДО

К организационным мерам относятся:

- размещение технических средств в помещениях с контролируемым доступом;
- административные ограничения доступа к этим средствам;
- задание режима использования пользователями и администраторам паролей и идентификаторов;
- допуск к осуществлению документооборота только определенных лиц;
- поддержание программно-технических средств в исправном состоянии;
- резервирование программно-технических средств;
- обучение персонала;
- защита технических средств от повреждающих внешних воздействий (пожар, воздействие воды и т.п.).
- контроль эффективности мер по защите информации

Общие меры по обеспечению безопасности информации в системах ЭДО

Системы ЭДО, содержащие секретную информацию не должны иметь выхода во внешнюю сеть.

Государственные и муниципальные **Системы ЭДО, содержащие другую информацию с ограниченным доступом (персональные данные , служебная информация) не должны иметь выхода во внешнюю сеть.**

На АРМ пользователей должны быть заблокированы порты и разъемы для подключения внешних устройств, в том числе сетевых, а также множительной техники.

АРМ должны находиться в охраняемом помещении с ограниченным контролируемым доступом. К этим компьютерам не должны иметь доступа сотрудники, не допущенные (в соответствии со служебной инструкцией) к работе с информацией с ограниченным доступом.

Официальный запрет для сотрудников проносить на рабочее место телефоны с: встроенными фото- и видеокамерами, возможностью подключения к компьютеру. Запрет на пользование и фото и видеотехникой.

Носители с конфиденциальной информацией должны храниться и использоваться таким образом, который бы не допускал возможности получения к ним доступа извне.

Если носитель больше не будет использоваться для работы с конфиденциальной информацией - он должен быть уничтожен физически.

Общие меры по обеспечению безопасности информации в системах ЭДО

Вся компьютерная техника должна быть учтена.

За эксплуатацию и технико-программное состояние компьютеров должен отвечать специально назначенный сотрудник.

Конфиденциальные электронные документы уничтожаются лично сотрудником, отвечающим за безопасность компании.

Все рабочие места должны быть оборудованы источниками бесперебойного питания с целью недопущения сбоев работы в системе из-за отключения электроснабжения. При таких ситуациях на диске остается часть невидимой для пользователя информации, которая в дальнейшем может быть использована для получения несанкционированного доступа к конфиденциальным данным.

Общие меры по обеспечению безопасности информации в системах ЭДО

Конфиденциальная информация, хранящаяся на магнитных носителях, должна быть зашифрована.

Контроль над доступом сотрудников к закрытой документации и к базам данных.

Распечатки конфиденциальной информации должны проходить через один сетевой принтер и регистрироваться.

Обязательное наличие уничтожителя бумаги для ликвидации ненужных документов (включая использованную копировальную бумагу от пишущих машинок).

Определение установленных для посещения мест, не оставлять посетителей одних в помещениях, где функционирую АРМ и другие элементы ЭДО.

Меры по обеспечению безопасности средств криптографической защиты информации.

Приказом руководителя организации назначены должностные лица, ответственные за разработку и практическое осуществление мероприятий по обеспечению функционирования и безопасности средств криптографической защиты информации.

Разработана и утверждена руководством организации инструкция по обеспечению функционирования и безопасности средств криптографической защиты с учетом эксплуатационной документации на средства криптографической защиты информации.

Для хранения ключей шифрования и электронной цифровой подписи, нормативной и эксплуатационной документации, инсталляционных дискет помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Дубликаты ключей от хранилищ и входных дверей должны храниться в сейфе ответственного лица, назначаемого руководством организации.

Системные блоки ЭВМ с установленными средствами криптографической защиты информации оборудованы средствами контроля их вскрытия

Все поступающие для использования ключи шифрования и электронной цифровой подписи и инсталляционные дискеты берутся в организации на поэкземплярный учет в специальных журналах.

Для учета и хранение магнитных носителей ключевой информации и инсталляционных дискет, непосредственной работы с ними приказом руководителя назначается специально выделенный работника организации, которые в соответствии с его должностными обязанностями несет персональную ответственность за сохранность ключей шифрования, электронной подписи и функционирование средств криптографической защиты информации

Руководитель организации, а также работник, ответственный за сохранность ключей шифрования, электронной подписи и функционирование средств криптографической защиты информации должны пройти обучение на специальных курсах.

Меры по обеспечению безопасности информации в системах ЭДО

Модель нарушителя автоматизированной системы и степень риска (НСД)

Категория пользователя	Степень риска	Элементы ЭДО					
		I	II	III	IV	V	VI
		A B C	A B C	A B C	A B C	A B C	A B C
Пользователи ПЭВМ	Средняя				5 5 5		5 5
Специалисты отдела информационных технологий	Повышенная				5 5 5	4 4	4 5
Прикладные программисты	Повышенная	3 3 3	2 2 2		5 5 5	5 5 5	4 4 5
Специалисты по ремонту и техническому обслуживанию ПЭВМ	Наибольшая	4 4 4	2 2 2	1 1 1	5 5 5	5 5 5	5 5 5
Администратор телекоммуникационных ресурсов	Наибольшая	5 5 5	5 5 5	5 5 5	5 5 5	5 5 5	5 5 5
Администратор ЛВС	Наибольшая	5 5 5	5 5 5	5 5 5	5 5 5	5 5 5	5 5 5
Администратор информационной безопасности	Наибольшая	5 5 5	5 5 5	5 5 5	5 5 5	5 5 5	5 5 5

Компоненты системы, наиболее уязвимые при попытках НСД:
I - внутренние данные; **II** - внутренние прикладные программы; **III** - внутренние системные модули; **IV**- внешние данные; **V** - внешние системные модули; **VI** - элементы компьютера и др. аппаратура.
Виды ущерба: **A** - модификация; **B** – разрушение; **C** – компрометация информации, D – копирование больших объемов информации.
Степень угрозы: **1** – до 20%; **2** – до 40%; **3** – до 60%; **4** – до 80%; **5** – до 100%.

Определение требований по обеспечению безопасности персональных данных

Правительство Российской Федерации готовит требования к обеспечению безопасности персональных данных при их обработке в информационных системах.

В настоящий момент времени требования к обеспечению безопасности персональных данных при их обработке в информационных системах устанавливается СТР-К:

- п.5.2.3 АС, обрабатывающие персональные данные, должны иметь класс защищенности не ниже 3Б,2Б и 1Д.

РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования по защите информации.

Подсистемы и требования	Классы		
	1Д	2Б	3Б
1. Подсистема управления доступом			
1.1. Идентификация, проверка подлинности и контроль доступа субъектов в систему	+	+	+
2. Подсистема регистрации и учета			
Регистрация и учет:			
входа (выхода) субъектов доступа в (из) систему (узел сети).	+	+	+
Учет носителей информации	+	+	+
3. Криптографическая подсистема	-	-	-
4. Подсистема обеспечения целостности			
Обеспечение целостности программных средств и обрабатываемой информации	+	+	+
Физическая охрана средств вычислительной техники и носителей информации	+	+	+
Периодическое тестирование СЗИ НСД	+	+	+
Наличие средств восстановления СЗИ НСД	+	+	+

Типовые требования по обеспечению безопасности информации в системах ЭДО

При работе в системе электронного документооборота запрещается:
-осуществлять несанкционированное копирование магнитных носителей ключевой информации;
-разглашать содержимое магнитных носителей ключевой информации, а также передавать их лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер, за исключением случаев, предусмотренных эксплуатационной документацией;
-записывать на магнитные носители ключевой информации любую другую информацию;
-оставлять без контроля АРМ АС при включенном питании и загруженном программном обеспечении;
-вносить какие-либо изменения в программное обеспечение АРМ АС;
-использовать бывшие в работе магнитные носители ключевой информации для записи новой информации, без предварительного уничтожения на дискетах ключевой информации путем их переформатирования при помощи программы, входящей в состав средств криптографической защиты информации;
-оставлять монитор в непогашенном состоянии. При длительном или кратковременном перерыве в работе с программой необходимо производить гашение экрана, а возобновление активности экрана производить с использованием пароля доступа, задаваемого в конфигурации АРМ АС; осуществлять несанкционированное вскрытие системных блоков АРМ АС.

В случае обнаружения факта НСД к системным блокам, работа на этих АРМ АС должна быть прекращена. По данному факту должно проводиться служебное расследование и организовываться работа по анализу и ликвидации негативных последствий данного нарушения.

-Все поступающие от юридических и физических лиц электронные документы с электронной подписью должны помещаться в архив и храниться в соответствии с требованиями Федеральной архивной службы России,, с указанием сроков хранения,

Необходимые функции системы ТЗИ в системах ЭДО по обеспечению безопасности информации

- Механизмы контроля доступа к информационным ресурсам в соответствии с заданными параметрами безопансоти.
- Идентификация пользователей.
- Контроль целостности программ и данных.
- Контроль за состоянием и гарантированное восстановление функций системы защиты информации
- Аудит и регистрация доступа к информационным ресурсам.
- Гарантированное удаление информационных ресурсов.
- Контроль вывода на печать для различных приложений.
- Контроль запуска процессов.
- Контроль ввода и вывода на отчуждаемый физический носитель информации.
- Локальное и удаленное администрирование подсистем безопансоти.

Комплект документов для регистрации юридического лица в системе ЭДО ПФР России

Включает в себя;

- Соглашение об обмене электронными документами в системе электронного документооборота ПФР, подписанное юридическим или физическим лицом;
- контрольный лист с образцами печати юридического лица и личной подписью руководителя (контрольный лист физического лица также представляется с образцом его личной подписи);
- выписку из приказа о назначении администратора информационной безопасности и его заместителя у юридического лица, заверенную печатью и подписью руководителя;
- Акт о готовности к работе в системе электронного документооборота Пенсионного фонда Российской Федерации (1 экз.);
- Акт об изготовлении криптографических ключей (1 экз.);
- Акт о готовности к эксплуатации программно-аппаратного комплекса, защищенного СКЗИ (1 экз.);
- открытые ключи шифрования и электронной подписи;
- сертификаты открытых ключей (регистрационные карточки, 1 экз. остается в органе ПФР);
- справочник открытых ключей.

Некоторые системы ЭДО

Система информационного взаимодействия ИОГВ Санкт-Петербурга

Система ЭДО Федерального казначейства. (Приказом Федерального казначейства от 18.08.2005 г. №123 определён типовой порядок организации электронного документооборота органов Федерального казначейства с организациями-клиентами),

Система ЭДО Федерального пенсионного фонда Российской Федерации

Государственные информационные системы: ЕГЭ, ГАС «Выборы»

Социальная карта жителя Москвы

Системы межбанковских расчетов, таможенного декларирования

Системы ЭДО

Министерство экономического развития и торговли РФ

- **Почти 500 рабочих мест на 4 площадках**
- **Обрабатывается около 800 документов в день**
- **Сканируется и оцифровывается вся входящая корреспонденция в главное здание Министерства**
- **Информация по контролю доступна с рабочих мест руководства Министерства**
- **В системе работают сотрудники от уровня руководителя до конечного исполнителя**
- **Доступ на просмотр информации из подведомственных организаций**

Системы ЭДО

Министерство регионального развития РФ

- **20 рабочих мест на 1 площадке**
- **Обрабатывается около 110 документов в день**
- **В системе работают регистраторы и секретари департаментов**

Перспективы развития

1. **Полнофункциональный защищенный межведомственный электронный документооборот**
2. **Построение защищенного долговременного архива электронных документов**
3. **Стандартизация решений**

Обеспечение безопасности информации в системах ЭДО

Доли ведущих компаний на рынке систем защиты электронного документооборота (по данным ассоциации «РусКрипто

“Анкад”	**25%**
“ЛАН Крипто”	**35%**
“ЛАН Крипто” и ЭлиПС	**5%**
“Сигнал-КОМ”	**10%**
“Информзащита”	**15%**
Прочие	**10%**

Средства обеспечения безопасности информации в системах ЭДО

Система автоматизации делопроизводства и электронного документооборота «Дело» Тиражируемый программный продукт, может быть установлен силами заказчика на основе функционирующей в организации ЛВС. Обеспечивает подлинность документов, частично защиту информации (криптографическими средствами). Требует дополнительных мер по технической защите информации при наличии в системе ЭДО информации, доступ к которой ограничен федеральными законами.

«Анкад» семейство плат "Криптон" (программно-аппаратное решение), включающее шифрование данных, подпись данных, контроль доступа к компьютерам (350 долл. и выше); Secret Disk 2000 — создание защищенных разделов диска (от 120 долл.); Crypton Word 2000 — шифрование и подпись (встраивается в Microsoft Word, 20 долл.), Crypton Excel 2000 — шифрование и подпись (встраивается в Microsoft Excel, 20 долл.).

«ЛАН Крипто» систем "Нотариус" — подпись данных (от 60 до 100 долл.), систему "Веста" — шифрование данных (от 30 до 70 долл.), "КриптоБанк" — подпись и шифрование данных (от 80 до 170 долл.), Crypto Office Pro — подпись и шифрование данных, документов Microsoft Office, почтовых сообщений (около 150 долл.), CryptoTrust2000 — центр сертификации (500 долл.). Совместная разработка «ЛАН Крипто» и ЭлиПС», аппаратное решение «Грим диск», обеспечивает аппаратное шифрование содержимого жесткого диска (350 долл. и выше).

«Информзащита» программно-аппаратное решение SecretNet для защиты серверов и рабочих станций в локальных сетях (от 1000 до 4500 долл. за сервер и от 140 до 210 долл. за рабочую станцию).

Некоторые средства защиты информации, сертифицированные ФСТЭК России

Программа фиксации и контроля исходного состояния программного комплекса “ФИКС” (версия 2.0). Является программным средством контроля эффективности применения СЗИ

Анализаторы уязвимостей средств защиты СВТ от НСД “НКВД” (версии 2.2, 2.3). Является программным средством контроля эффективности применения СЗИ.

Программа поиска информации на дисках «TERRIER». Является программным средством контроля эффективности применения СЗИ.

Программа «Ревизор-1». Является программным средством контроля защищенности от НСД в АС под управлением WINDOWS 9x/ME/NT4/2000.

Федеральный Закон от 27.07.06г.№ 149 -ФЗ «Об информации, информационных технологиях и о защите информации»

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

Нарушение требований Закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность соотвествии с законодательством Российской Федерации

Уголовный Кодекс Российской Федерации, Гражданский Кодекс Российской Федерации

Глава 28 УК РФ «Преступления в сфере компьютерной информации»

Три вида преступлений

Незаконный доступ к информации ЭВМ, их носителей и сетей.

Создание, распространение и использование вредоносных программ.

Нарушения правил эксплуатации ЭВМ, их систем и сетей.

статья 139 ГК РФ

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

К нарушениям федеральных норм и правил в области ПД ТР и ТЗИ или условий действия лицензий, выданных ФСТЭК России, согласно КОАП относятся

нарушения *требований* нормативной документации (руководящих документов, стандартов, ведомственных правил и др.), а также *условии действия лицензий, выдаваемых Гостехкомиссией России;*

нарушения, повлекшие за собой утечку охраняемых сведений, в том числе сведений, составляющих государственную тайну;

нарушения установленных руководящими документами Гостехкомиссии России *правил и условий* эксплуатации объектов информатизации;

нарушения, связанные с использованием несертифицированных средств связи, несертифицированных информационных систем, баз и банков данных, а также несертифицированные средств защиты информации, если они подлежат обязательной сертификации;

другие нарушения в случаях, обоснованных должностными лицами Гостехкомиссии России, имеющими право назначать административные наказания

К О Д Е К С
Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ

Глава 13. Административные правонарушения в области связи и информации

Статья 13.12. Нарушение правил защиты информации

п. 2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), влечет наложение административного штрафа на должностных лиц – от 10 до 20 МРОТ, на юридических лиц – от 100 до 200 МРОТ.

п. 4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц – от 30 до 40 МРОТ, на юридических лиц – от 200 до 300 МРОТ.

К О Д Е К С
Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ

Глава 19. АДМИНИСТРАТИВНЫЕ ПРАВОНАРУШЕНИЯ ПРОТИВ ПОРЯДКА УПРАВЛЕНИЯ

Статья 19.5. Невыполнение в срок законного предписания (постановления, представления) органа (должностного лица), осуществляющего государственный надзор (контроль)

1. Невыполнение в установленный срок законного предписания (постановления, представления) органа (должностного лица), осуществляющего государственный надзор (контроль), об устранении нарушений законодательства - влечет наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц - от пяти до десяти минимальных размеров оплаты труда; на юридических лиц - от пятидесяти до ста минимальных размеров оплаты труда.

К О Д Е К С
Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ

Глава 19. АДМИНИСТРАТИВНЫЕ ПРАВОНАРУШЕНИЯ ПРОТИВ ПОРЯДКА УПРАВЛЕНИЯ

Статья 19.5. Невыполнение в срок законного предписания (постановления, представления) органа (должностного лица), осуществляющего государственный надзор (контроль)

1. Невыполнение в установленный срок законного предписания (постановления, представления) органа (должностного лица), осуществляющего государственный надзор (контроль), об устранении нарушений законодательства - влечет наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц - от пяти до десяти минимальных размеров оплаты труда; на юридических лиц - от пятидесяти до ста минимальных размеров оплаты труда.

УКАЗ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ «О МЕРАХ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙБЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИВ СФЕРЕ МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА»

(12 мая 2004 года N 611)

В целях обеспечения информационной безопасности Российской Федерации при осуществлении международного информационного обмена посредством информационных систем, сетей и сетей связи, включая международную ассоциацию сетей "Интернет", постановляю:

Субъектам международного информационного обмена в Российской Федерации не осуществлять включение информационных систем, сетей связи и автономных персональных компьютеров, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну, и служебная информация ограниченного распространения, а также для которых установлены особые правила доступа к информационным ресурсам, в состав средств международного информационного обмена, в том числе в международную ассоциацию сетей "Интернет» (далее - сеть "Интернет").

Владельцам открытых и общедоступных государственных информационных ресурсов осуществлять их включение в состав объектов международного информационного обмена только при использовании сертифицированных средств защиты информации, обеспечивающих ее целостность и доступность, в том числе криптографических для подтверждения достоверности информации.

Владельцам и пользователям указанных ресурсов осуществлять размещение технических средств, подключаемых к открытым информационным системам, сетям и сетям связи, используемым при международном информационном обмене, включая сеть "Интернет", вне помещений, предназначенных для ведения закрытых переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну.

Основные положения Федерального Закона от 27.07.06г.№ 149 -ФЗ «Об информации, информационных технологиях и о защите информации»

Федеральный закон регулирует отношения, возникающие при:
1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
2) применении информационных технологий;
3) обеспечении защиты информации.

Основные принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации: - установление ограничений доступа к информации только федеральными законами;
- обеспечение безопасности РФ при создании информационных систем, их эксплуатации и защите содержащейся в них информации;- достоверность информации и своевременность ее предоставления;

Информация подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен ФЗ.

Обладатель информации при осуществлении своих прав обязан:
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена ФЗ

Государственная тайна.
Закон РФ от 21 июля 1993 года №5485-1 **«О государственной тайне».**

Профессиональная тайна),
Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности

К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространения котрой диктуются сл. необх.од. Пост. Правительства РФ от 94 г. №1233

Служебная тайна

Персональные данные.
Федеральный закон №152-ФЗ

Информационные системы.

Государственные информационные системы.

Муниципальные информационные системы.

Ин
информационные системы.

Особенности подключения государственных информационных систем к ИТКС (Интернет) могут быть установлены нормативным правовым актом Президента РФ (611 указ) или Правительства РФ

Обязательны

Требования по защите информации установленные ФСТЭК России.

Рекомендации

Порядок создания и эксплуатации ИС, не являющихся государственными или муниципальными, определяется операторами таких ИС в соответствии с требованиями ФЗ

Основные положения Федерального Закона от 27.07.06г.№ 149 -ФЗ «Об информации, информационных технологиях и о защите информации»

Статья 9. Ограничение доступа к информации

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.
2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

ст. 6 п.3 Обладатель информации при осуществлении своих прав обязан:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Основные положения Федерального Закона от 27.07.06г.№ 149 -ФЗ «Об информации, информационных технологиях и о защите информации»

Обязательность соблюдения конфиденциальности информации, доступ к которой ограничен федеральными законами (ст. 9.2);

Обязательность ввода государственной информационной системы в эксплуатацию в порядке, установленном заказчиком (ст. 14.5);

Методы и способы защиты информации при создании и эксплуатации государственных информационных систем должны соответствовать требованиям, установленным ФОИВ, уполномоченным в области ПДТР и ТЗИ (ст.16.5)

Установленные Федеральным законом от 27.07.06г.№ 149-ФЗ требования к государственным информационным системам, распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации (ст.13.4).

Обязанности обладателя информации, оператора информационной системы *(ст.16.4)*:
- предотвращение несанкционированного доступа к информации, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной в следствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации.

Основные положения Федерального Закона от 27.07.06г. №152-ФЗ «О персональных данных» (вступает в силу с января 2007 г.)

Федеральным законом регулируются отношения, связанные с обработкой персональных данных

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, обезличивания персональных данных и в отношении общедоступных персональных данных

Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.

Меры по обеспечению безопасности персональных данных при их обработке

Оператор при обработке персональных данных обязан **принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных**.

Правительство РФ устанавливает требования к обеспечению безопасности персональных данных.

ФСТЭК России осуществляет контроль выполнения требований обеспечения безопасности

Основные положения Федерального Закона от 27.07.06г. №152-ФЗ «О персональных данных»

Федеральный закон от 27.07.06г. №152-ФЗ «О персональных данных» устанавливает:

обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных, за исключением случаев предусмотренных Законом (ст. 6.1);

операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, предусмотренных настоящим Законом

оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных (ст. 19.1);

Правительство Российской Федерации устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем (ст. 19.2).

Обеспечение безопасности информации в системах ЭДО

Некоторые ведомственные нормативные документы, регулирующие вопросы безопасности информации в системах ЭДО

Временные требования по обеспечению информационной безопасности в системе электронного документооборота Пенсионного фонда Российской Федерации 2001 г.

Временное положение о порядке использования средств криптографической защиты информации и электронной подписи в системе электронного документооборота Пенсионного фонда Российской Федерации 2001 г.

Регламент регистрации и подключения юридических и физических лиц к системе электронного документооборота Пенсионного фонда Российской Федерации.2001 г.

Типовой порядок организации электронного документооборота органов Федерального казначейства с организациями-клиентами, 2005 г.

С И С Т Е М А

защиты информации на в органе власти (организации)

Система защиты информации

Органы управления Руководитель Органа власти, организации

- Ответственное должностное лицо из числа заместителей руководителя органа власти (организации)
- Структурные подразделения
- Система подготовки кадров
- Подготовленные кадры

Нормативные правовые акты РФ, руководящие документы ФСТЭК (Гостехкомиссии) России и местная система документов

- перечень документов
- Документы по перечню

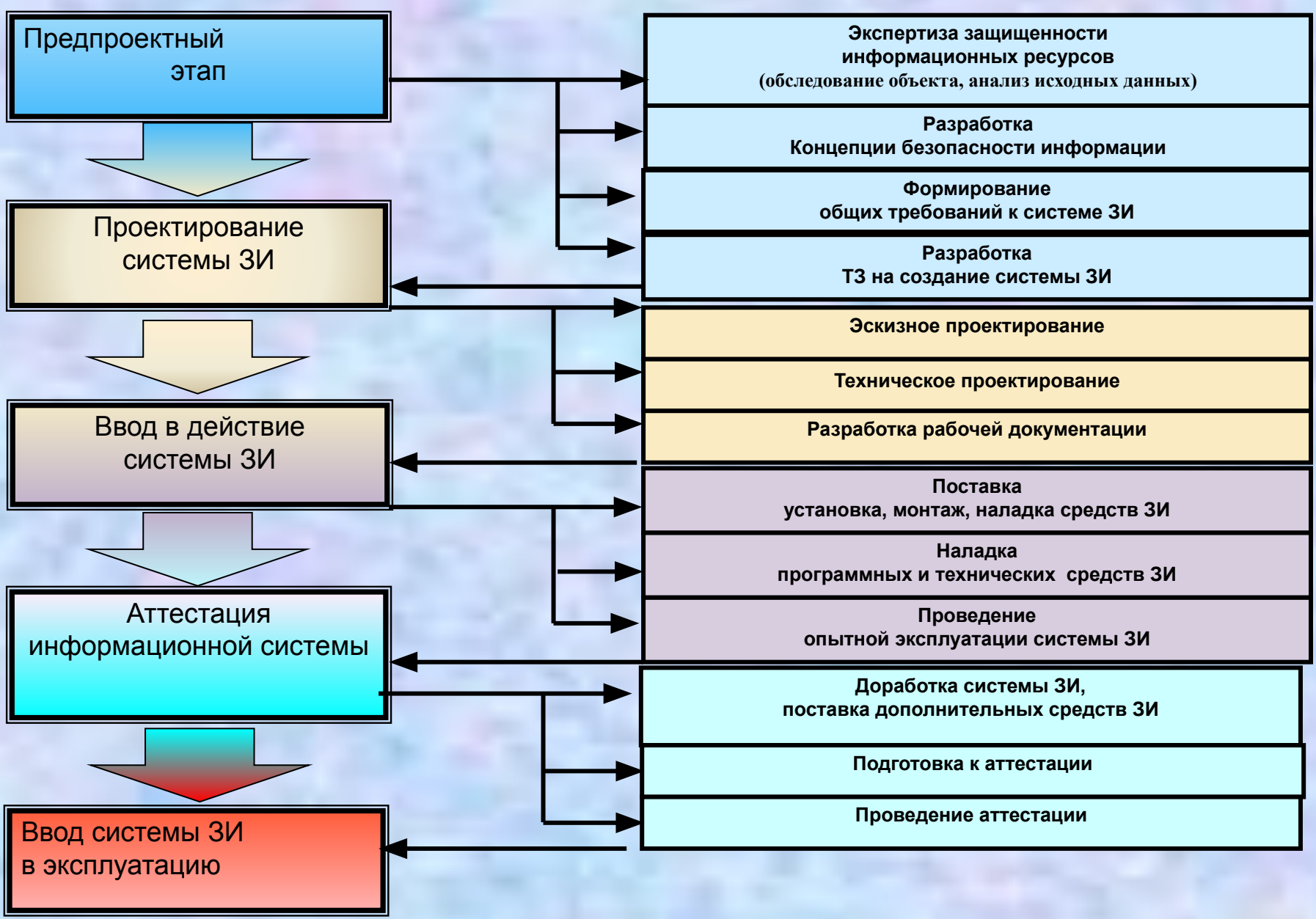
Системы, средства и методы защиты информации

- Система сертификации
- Система аттестования
- Наличие защищенных помещений, состояние их защиты
- Наличие и состояние защиты АС

Организация работ:-по формированию системы защиты информации; - по защите информации.

- Финансирование
- Планирование
- Организация работ, исполнения и контроля

Основные этапы формирования защищенной информационной системы



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

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

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

3. Определение требований к системе ЗИ, замысла на ее создание (совершенствование) → Концепция (политика) защиты информации

4. Выработка решения → Техническое задание на разработку системы ЗИ (информационной системы с разделом по ЗИ)

5. Планирование работ → Программа создания (совершенствования) системы ЗИ (план работ)

6. Проведение работ и ввод объектов в эксплуатацию → Аттестаты соответствия объектов информатизации, сертификаты средств защиты, акт о приемке, приказ о вводе

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

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

1

Предпроектное обследование

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

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

Оценка условий дислокации объекта, угроз безопасности информации

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

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

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

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

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

Определение основных направлений политики безопасности информации.

Определение основных требований к системе ЗИ.

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

- **Определение организационной структуры, целей и основных задач системы защиты информации**
- **Определение перечня и уяснение требований нормативных правовых актов РФ, ведомственных нормативных документов, определение перечня организационно-распорядительных и других документов, регулирующих и определяющих правовой статус и организационный режим системы защиты информации органа власти (организации), подлежащих разработке.**
- **Определение перечня основных организационных, инженерно-технических, технических и аппаратно-программных мер по предупреждению утечки информации или нарушений в работе ИС** (по каждой угрозе)
- **Определение объема финансирования. (Предварительный расчет и обоснование затрат на проведение работ).**
- **Определение формы реализации мероприятий по обеспечению безопасности информации (Целевая программа, годовое планирование и т.д.)**

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

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

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

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

Выработка решения на создание (совершенствование) системы защиты информации

Разработка технического задания

Определение целей и задач защиты информации

Уяснение и определение угроз безопасности информации

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

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

Определение основных функций системы защиты информации

Определение требований к системе защиты информации и ее функциональным элементам

Определение показателей эффективности работы системы защиты информации