


Основные подходы к обеспечению защиты информационных систем учреждений.



Учебные вопросы:

- 
1. Информационные ресурсы.
 2. Организация обеспечения информационной безопасности.
 3. Защита персональных данных в учреждении.
 4. Ответственность за нарушения требований, правил и мер защиты информации.



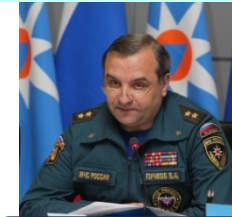
Национальная безопасность - состояние защищенности **личности, общества и государства** от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие РФ, оборону и безопасность государства.

Государственная

Национальная безопасность

Виды безопасности

Экологическая
доктрина РФ



Антитеррористическая
безопасность

Военная

Информационная

Общественная

Техногенная

Экологическая

Стратегия национальной безопасности (Указ Президента РФ от 31.12.2015 N 683)

Концепция
противодействия
терроризму
(утв. 05.10.2009)

Военная доктрина
Российской Федерации
(утв. 25.12.2014)

Доктрина
информационной
безопасности
(утв. 09.09.2000)

Доктрина
продовольственной
безопасности

ФЗ «О транспортной
безопасности»

Экономическая,
энергетическая

Бортников А.В.

Шойгу С.К.

Селин В.В. Нарышкин С.Е. Золотов В.В.



Федеральная целевая программы
 «Национальная система химической и
 биологической безопасности Российской
 Федерации (2015 - 2020 годы)»

Стратегия
Экономической
безопасности

ПОСТАНОВЛЕНИЕ
от 7 октября 2017 г. N 1235

ТРЕБОВАНИЯ
К АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ (ТЕРРИТОРИЙ)
МИНИСТЕРСТВА ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
И ОБЪЕКТОВ (ТЕРРИТОРИЙ), ОТНОСЯЩИХСЯ К СФЕРЕ
ДЕЯТЕЛЬНОСТИ МИНИСТЕРСТВА ОБРАЗОВАНИЯ И НАУКИ РФ

17. Антитеррористическая защищенность объектов (территорий) независимо от их категории опасности обеспечивается путем осуществления комплекса мер, направленных:

д) на **обеспечение защиты служебной информации ограниченного распространения**, содержащейся в паспорте безопасности объекта (территории) и иных документах, в том числе служебной информации ограниченного распространения о принимаемых мерах по АТЗ объектов (территорий).

18. Воспрепятствование неправомерному проникновению на объекты (территории) достигается посредством:

е) организации обеспечения информационной безопасности, разработки и реализации мер, **исключающих несанкционированный доступ информационным ресурсам объектов (территорий)**;

Раздел IX. Дополнительная информация с учетом особенностей объекта

IX. Дополнительная информация с учетом особенностей объекта (территории)

(наличие на объекте (территории) режимно-секретного органа, его численность (штатная и фактическая), количество сотрудников объекта (территории), допущенных к работе со сведениями, составляющими государственную тайну, меры по обеспечению режима секретности и сохранности секретных сведений)

(наличие локальных зон безопасности)

(другие сведения)

1. Информационные ресурсы.

Информация – сведения (сообщения, данные) независимо от формы их представления (ФЗ № 149 2006 г.)

Угроза – возможная причина нежелательного инцидента, которая может нанести ущерб информационной системе или всей организации (ISO/IEC 27000:2014)

Уязвимость - слабость актива или управления, эксплуатация которой приведёт к реализации одной или нескольких угроз.

Угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (ГОСТ Р 53114-2008).

Безопасность информации - состояние защищенности информации (данных), при котором обеспечены ее (их) **конфиденциальность, доступность и целостность** (ГОСТ Р 50922-2006).

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (ГОСТ Р 50922-2006).

Доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно (рекомендации по стандартизации Р 50.1.056-2005)

Целостность информации – состояние информации, при котором обеспечивается ее неизменность в условиях преднамеренного и (или) непреднамеренного воздействия на нее (рекомендации по стандартизации Р 50.1.056-2005)

Информационные ресурсы Российской Федерации

Федеральный Закон от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и о защите информации» ред. от 29.07.2017

государственные

муниципальные

иные

Открытая, общедоступная информация

Информация не подлежащая ограничению в доступе

Информация с ограниченным доступом

Информационные ресурсы – это отдельные документы, массивы документов, которые входят в состав информационных систем.



Сведения, составляющие гостайну

Служебная тайна

Профессиональная тайна

Коммерческая тайна

Персональные данные

Отнесение информации к государственной тайне осуществляется в соответствии с Законом РФ «О государственной тайне»

Отнесение информации к конфиденциальной осуществляется в порядке, установленном законодательством РФ

Отнесение информации осуществляется в порядке, установленном Законами РФ

«О коммерческой тайне»

«О персональных данных»

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

Федеральный Закон 149 – ФЗ 2006 г. «Об информации, информационных технологиях и о защите информации»

Документальные формы представления информации

На материальном носителе

Текст

Фото

Рисунок

Скульптурное изображение

Ауди и Видеоматериалы

В электронной форме

Word

Paint

Excel

PowerPoint,

Adobe PDF

Другие

электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, **признается электронным документом**, равнозначным документу, подписанному собственноручной подписью,

Защита информации

Комплекс мер

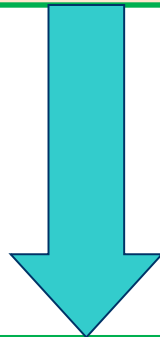
Правовых (Законы и др. нормативные документы)

Организационных (внутренние мер и документы)

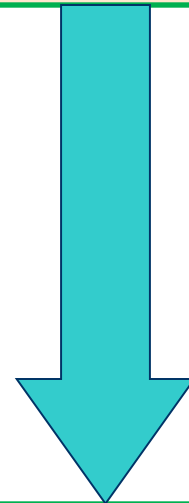
Технических (программные, технические)



Предотвращение НСД



Предотвращение утечки по техническим каналам



Предотвращение программно – математических воздействий

Что делать?

Провести инвентаризацию – определить чем владеешь

Оценить уровень защиты и его соответствие требованиям нормативных документов

Выполнить требования по защите информации, определенные нормативными документами

2. Организация обеспечения информационной безопасности.

В органе власти и организации любой формы собственности видом основной деятельности является организация и обеспечение защиты информации с ограниченным доступом

Решая задачи обеспечения безопасности информации (защиты информации) требуется ответить на пять основных вопросов: **что защищать?, от чего (кого) защищать, кто будет защищать?, как защищать?, чем защищать?**

Что защищать?

Защите подлежит информация, ее носители и физические поля зафиксированные в «**Перечне сведений организации, подлежащих защите**»

Кто будет защищать?

В любой организации к защите сведений причастны: руководитель, его заместитель, начальники отделов: финансового и персонала, начальник подразделения по защите информации, администратор безопасности и пользователь (исполнитель, работник)

Подразделение (Штатный Специалист) по защите информации

От чего (кого) защищать?

Информация (ее носители) защищается от **внешних и внутренних** нарушителей, создающих **угрозы безопасности информации**, ее носителям

Защита информации – это работа и (или) оказание услуг по защите ее **от утечки по техническим каналам, от несанкционированного доступа** к ней (носителям), **от специальных воздействий** на информацию

В органе власти и организации любой формы собственности видом основной деятельности **является** организация и обеспечение защиты информации **с ограниченным доступом**

Как защищать?

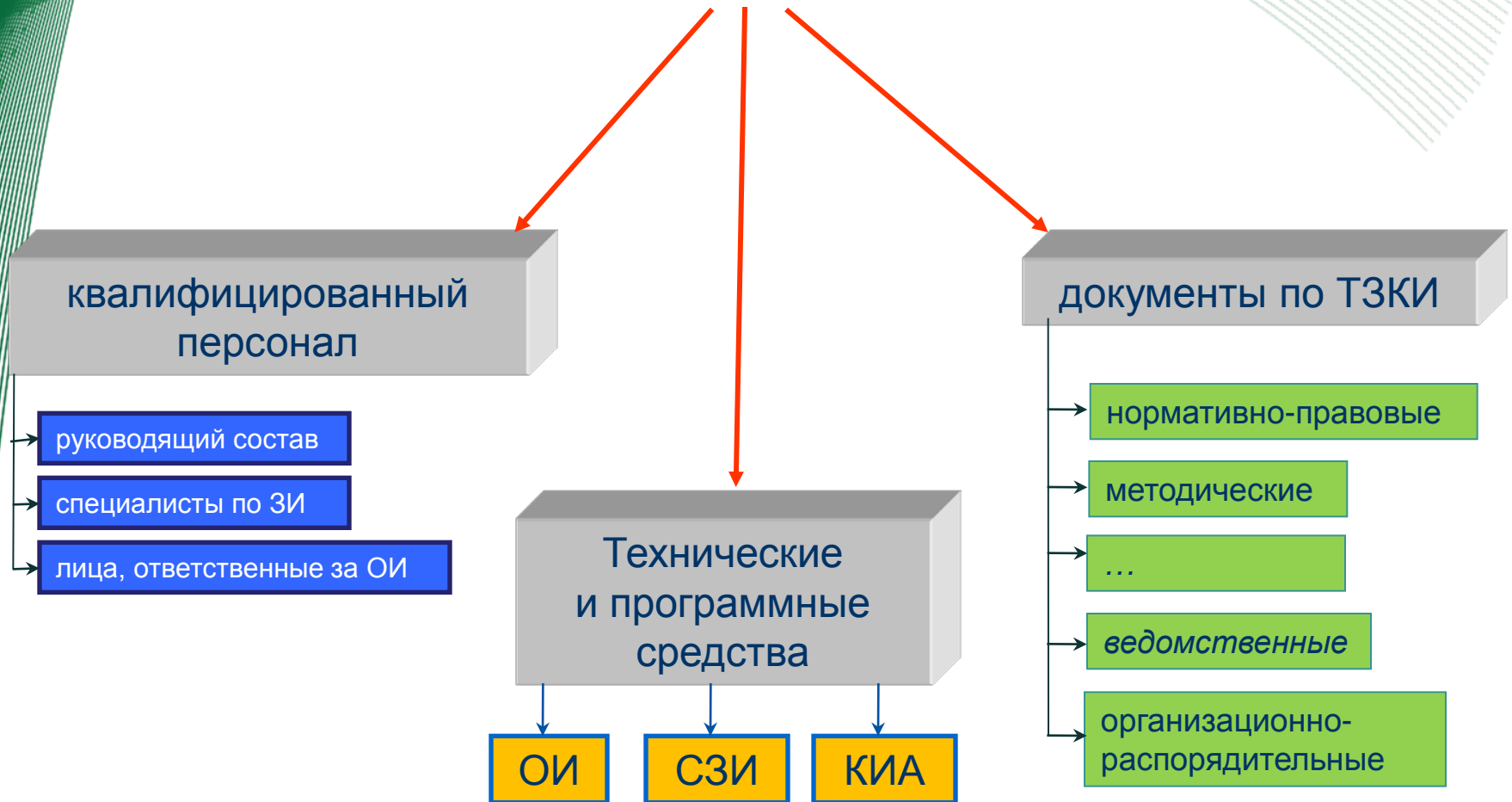
Информация (ее носители) защищаются на объектах информатизации и в линиях (каналах) связи. Защита информации – вид деятельности подлежащий лицензированию. Для защиты информации необходимо создать объекты информатизации – режимные, выделенные (защищаемые) помещения, автоматизированные системы и средства изготовления и размножения документов. Эксплуатация объектов информатизации возможна после проведения аттестационных испытаний и ввода их в эксплуатацию

Чем защищать?

Информация (ее носители) защищаются организационными мероприятиями и техническими мерами.

Защита информации – принятие организационных и технических мер, направленных на выполнение правовых требований по **предотвращению НСД к информации, утечки по техническим каналам и специальных воздействий на нее**

Система защиты информации (обобщенно)











РД. АС. Защита от НСД к информации. Классификация АС и требования по защите информации

Организационные мероприятия:

выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите;

определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;

установление и оформление правил разграничения доступа, т.е. совокупности правил, регламентирующих права доступа субъектов к объектам;

ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;

получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;

обеспечение охраны объекта, на котором расположена защищаемая АС, (территория, здания, помещения, хранилища информационных носителей);

выбор класса защищенности АС в соответствии с особенностями обработки информации и уровнем ее конфиденциальности;

организация службы безопасности информации (ответственные лица, администратор АС), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД, приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т.д.;

разработка СЗИ НСД, включая соответствующую организационно-распорядительную и эксплуатационную документацию.

Требования по технической защите коммерческой тайны на ОИ

- документальное **оформление Перечня** сведений;
- реализация **разрешительной системы допуска** исполнителей;
- **ограничение доступа персонала** и посторонних лиц на ОИ и в помещения;
- **разграничение доступа пользователей** и обслуживающего персонала к информационным ресурсам и информационным сетям (АС), к программным средствам обработки (передачи) и защиты информации;
- **регистрация действий пользователей** и обслуживающего персонала, контроль (обнаружение) НСД к информационным ресурсам и НСД со стороны пользователей, обслуживающего персонала и посторонних лиц;
- **учет и надежное хранение** конфиденциальной информации, исключающее хищение, подмену и уничтожение;
- **контроль доступа к ОТСС**, носителям конфиденциальной информации и их защита путем использования специальных защитных знаков и сертифицированных по требованиям безопасности информации;

Требования по технической защите коммерческой тайны на ОИ (продолжение)

- **дублирование (резервирование)** отдельных категорий информационных ресурсов и носителей защищаемой информации;
- **резервирование технических средств**, обрабатывающих защищаемую информацию;
- **использование сертифицированных**, выпускаемых в защищенном исполнении **технических средств обработки, передачи и хранения информации** (АС или СВТ в защищенном от утечки информации исполнении);
- **использование сертифицированных** по требованиям безопасности информации **систем гарантированного электропитания** (источников бесперебойного питания);
- **использование** для передачи (обмена) защищаемой информации **защищенных линий и каналов связи**;
- **безопасное размещение** средств отображения информации, составляющей коммерческую тайну, исключающее ее несанкционированный просмотр;
- **использование лицензионных программных продуктов.**

Статья 11. Охрана конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений

1. ... работодатель обязан:

- 1) **ознакомить под расписку** работника, ... с **перечнем информации, составляющей коммерческую тайну**;
- 2) **ознакомить под расписку** работника с **установленным работодателем режимом коммерческой тайны** и с мерами ответственности за его нарушение;
- 3) **создать работнику** необходимые **условия** для соблюдения им установленного работодателем режима коммерческой тайны.

2. **Доступ работника** к информации, составляющей коммерческую тайну, **осуществляется с его согласия**, если это не предусмотрено его трудовыми обязанностями.

Статья 11. Охрана конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений

3. ... работник обязан:

- 1) **выполнять** установленный работодателем **режим КТ**;
- 2) **не разглашать** эту информацию, обладателями которой являются работодатель и его контрагенты, и **без их согласия не использовать** эту информацию в личных целях в течение всего срока действия режима КТ, **в том числе после прекращения действия трудового договора**;
- 3) **возместить причиненные работодателю убытки**, если работник виновен в разглашении информации, составляющей КТ и ставшей ему известной в связи с исполнением им трудовых обязанностей;
- 4) **передать работодателю** при прекращении или расторжении трудового договора **материальные носители информации**, имеющиеся в пользовании работника и содержащие информацию, составляющую КТ.

Статья 11. Охрана конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений

4. **Работодатель вправе потребовать возмещения убытков**, причиненных ему разглашением информации, составляющей КТ, от лица, получившего доступ к этой информации в связи с исполнением трудовых обязанностей, но **прекратившего трудовые отношения с работодателем**, если эта информация разглашена в течение срока действия режима коммерческой тайны.
5. **Причиненные** работником или прекратившим трудовые отношения с работодателем лицом **убытки не возмещаются**, если разглашение информации, составляющей коммерческую тайну, произошло **вследствие несоблюдения работодателем мер по обеспечению режима КТ**, действий третьих лиц или непреодолимой силы.
6. **Трудовым договором с руководителем** организации должны предусматриваться его **обязанности по обеспечению охраны конфиденциальности составляющей КТ информации**, обладателем которой являются организация и ее контрагенты, и **ответственность за обеспечение охраны конфиденциальности этой информации**.

3. Защита персональных данных в учреждении.

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

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.



Федеральный закон от 27.07.2006 г. № 152-ФЗ
«О персональных данных»

Постановление Правительства РФ № 1119 от 01.11.2012
«Об утверждении требований к защите персональных
данных при их обработке в информационных системах
персональных данных»

Постановление Правительства РФ № 687 от 15.09.2008 г.
«Об утверждении Положения об особенностях обработки
ПДн, осуществляемой без использования средств
автоматизации»

Постановление Правительства РФ №512 от 06.07.2008 г. «Об
утверждении требований к материальным носителям
биометрических ПДн и технологиям хранения таких данных
вне ИСПДн»

Законодательство нормативные документы ФСТЭК

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 года.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14 февраля 2008 года.

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Приказ ФСТЭК России от 18.02.2013 № 21.

Законодательство нормативные документы ФСБ

«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 г., №149/54-144.

«Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», ФСБ России, №149/6/6-622.

Постановление Правительства РФ № 1119 от 01.11.12 г.

документ устанавливает **требования к защите персональных данных при их обработке в информационных системах ПДн и уровни защищенности таких данных.**

Под актуальными угрозами безопасности ПДн понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПДн при их обработке в информационной системе, результатом которого могут стать **уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия.**

При обработке персональных данных в информационных системах **устанавливаются 4 уровня защищенности ПДн.**

Типы информационных систем

ИС является информационной системой, обрабатывающей **специальные категории ПДн**, если в ней обрабатываются ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, **состояния здоровья**, интимной жизни субъектов ПДн.

ИС является информационной системой, обрабатывающей **биометрические ПДн**, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность **и которые используются оператором для установления личности субъекта ПДн**, и не обрабатываются сведения, относящиеся к специальным категориям ПДн.

ИС является информационной системой, обрабатывающей **общедоступные ПДн**, если в ней обрабатываются ПДн субъектов персональных данных, полученные только из общедоступных источников персональных данных.

ИС, обрабатывающая **иные категории** персональных данных, если в ней обрабатываются данные, не указанные выше

ИС является информационной системой, обрабатывающей **ПДн сотрудников оператора**, если в ней обрабатываются ПДн только указанных сотрудников.

Угрозы

1 типа

Актуальны для ИС, если для нее, в том числе, актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в ИС.

2 типа

Актуальны для ИС, если для нее, в том числе, актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в ИС.

3 типа

Актуальны для ИС, если для нее, актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИС.

Оператор самостоятельно определяет тип угроз на основании оценки возможного вреда в соответствии с требованиями уполномоченных органов

Уровни защищенности персональных данных

1
уровень

Для ИС актуальны угрозы 1 типа и в ней обрабатываются либо специальные категории ПДн либо биометрические

Для ИС актуальны угрозы 2 типа и в ней обрабатываются специальные категории ПДн более чем 100 000 субъектов ПДн

Угрозы 1 типа, общедоступные ПДн

Угрозы 2 типа, специальные категории ПДн сотрудников или специальные категории ПДн менее, чем 100 000 субъектов не сотрудн.

Угрозы 2 типа, биометрические ПДн

Угрозы 2 типа, общедоступные ПДн более, чем 100 000 субъектов, не сотрудников

Угрозы 2 типа, иные ПДн более, чем 100 000 субъектов, не сотрудников

Угрозы 3 типа, специальные ПДн более, чем 100 000 субъектов, не сотрудников

Угрозы 2 типа, иные категории ПДн сотрудников оператора или иные категории менее, чем 100 000 субъектов, не сотрудников

Угрозы 3 типа, иные категории ПДн сотрудников оператора или иные категории менее, чем 100 000 субъектов, не сотрудников

Угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

Угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не сотрудников.

2
уровень

3
уровень

4
уровень

Приказ ФСТЭК России от 18.02.2013 № 21.

устанавливает состав и содержание орг. и тех. мер по обеспечению безопасности ПДн при их обработке в ИСПДн **для каждого из уровней защищенности ПДн**, установленных в Требованиях к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119.

п.7. Меры по обеспечению безопасности ПДн при их обработке в государственных ИС принимаются в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, устанавливаемыми ФСТЭК России.

Учебный вопрос № 4



**Ответственность за нарушения
требований,
правил и мер защиты информации.**

Виды юридической ответственности

- Дисциплинарная ответственность — заключается в наложении на виновное лицо дисциплинарного взыскания властью руководителя. Основные нормативно-правовые акты в РФ — Трудовой кодекс, Дисциплинарный Устав ВС, Дисциплинарный Устав Органов Внутренних Дел.
- Административная ответственность — применение органами исполнительной власти мер воздействия к виновным лицам. Основным нормативно-правовой акт — Кодекс РФ об административных правонарушениях.
- Гражданско-правовая ответственность — вытекает из нарушения имущественных и личных неимущественных прав граждан и организаций. Основным нормативный акт — Гражданский кодекс РФ.
- Уголовная ответственность — применяется в судебном порядке к лицу, виновному в совершении преступления. Нормативный акт, устанавливающий уголовную ответственность — Уголовный кодекс РФ.

ОСНОВНЫЕ НАКАЗУЕМЫЕ ДЕЯНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ



Ст. 13.11:

нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

**АДМИНИСТРАТИВНЫЙ
КОДЕКС
Российской
Федерации**

Ст. 13.12:

Нарушение правил защиты информации

Ст. 13.13:

Незаконная деятельность в области защиты информации

Ст. 13.14:

Разглашение информации с ограниченным доступом

"Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 N 51-ФЗ (ред. от 31.01.2016)

Под формой гражданско-правовой ответственности понимается форма выражения тех дополнительных обременений, которые возлагаются на правонарушителя.

Гражданское законодательство предусматривает различные формы ответственности.

Ответственность может наступать в форме:

- возмещения убытков (ст. 15 ГК),
- уплаты неустойки (ст. 330 ГК),
- потери задатка (ст. 381 ГК) и т.д

ДИСЦИПЛИНАРНАЯ ОТВЕТСТВЕННОСТЬ

44

Трудовой кодекс

Статья 192. Дисциплинарные взыскания

За совершение дисциплинарного проступка, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания:

- 1) замечание;
- 2) выговор;
- 3) увольнение по соответствующим основаниям.



СПАСИБО ЗА ВНИМАНИЕ!

**Стручин
Роман Леонидович
т. (931)985-72-05**