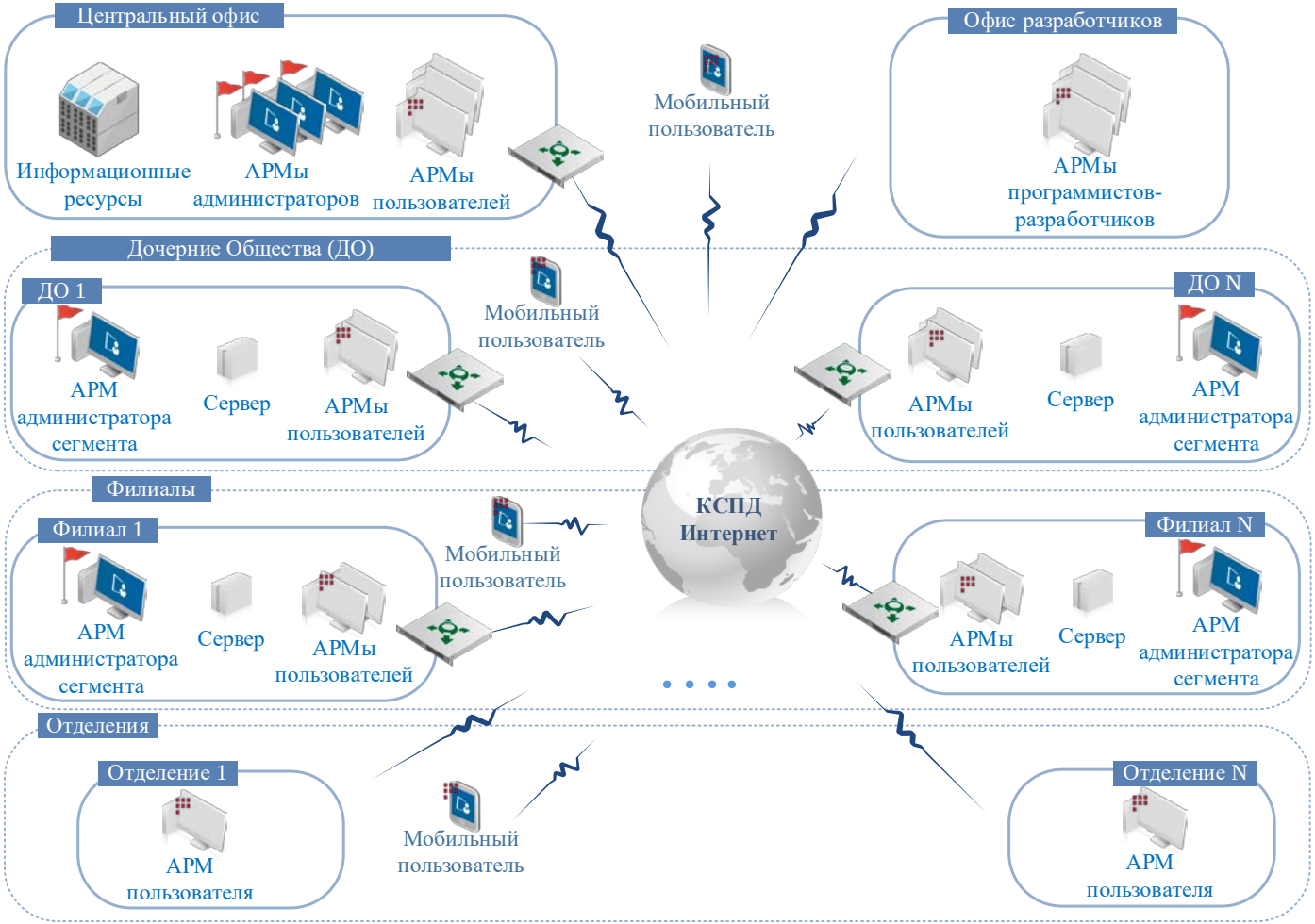
Защита персональных данных в организации при межсетевом взаимодействии

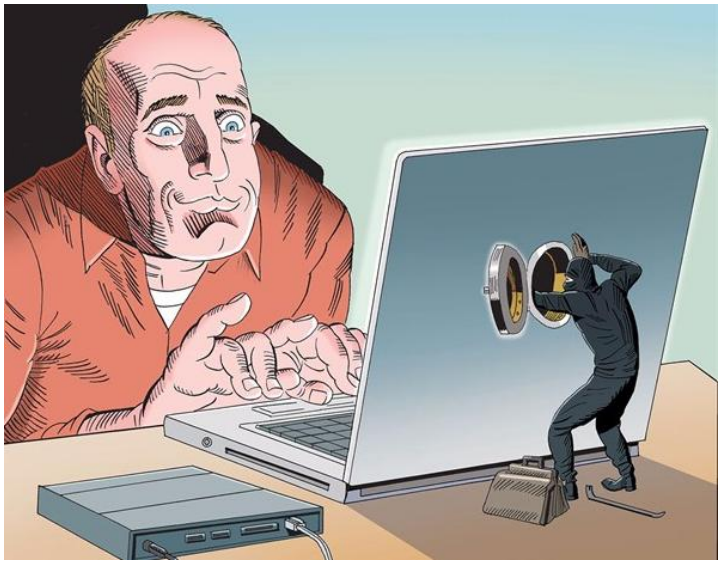
Валентина Миронова
Руководитель спецпроектов, к.т.н.



©2018, ОАО «ИнфоТеКС».

Что требуется

Построить систему защиты информации в ИС

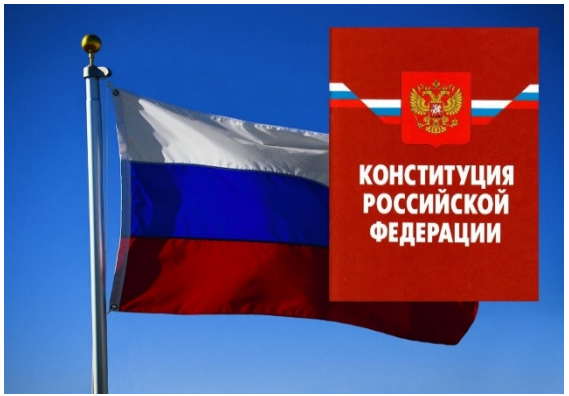


©2018, ОАО «ИнфоТеКС».

Законодательство РФ по защите ПДн

Законодательство РФ в области ПДн основывается на Конституции РФ и международных договорах РФ.

Федеральный закон №152-ФЗ «О персональных данных» от 27 июля 2006г. и другие определяющие случаи и особенности обработки ПДн нормативные документы.



©2018, ОАО «ИнфоТеКС».

Законодательство РФ по защите ПДн

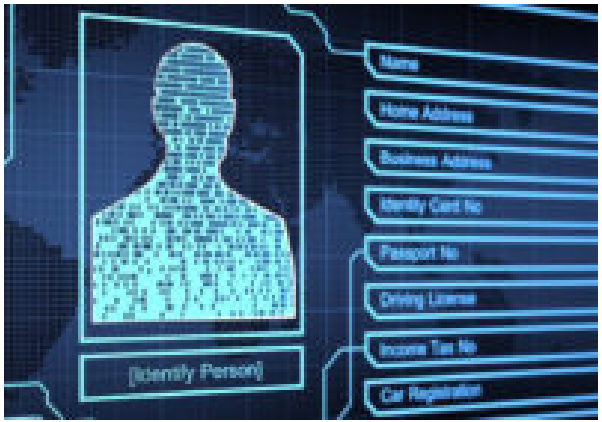
27 июля 2006г. был принят Федеральный закон №152 «О персональных данных».

Целью данного Федерального закона является **обеспечение защиты прав и свобод человека и гражданина** при **обработке его персональных данных**, в том числе **защиты прав на неприкосновенность частной жизни, личную и семейную тайну**.

©2018, ОАО «ИнфоТеКС».

Основные термины и определения

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



©2018, ОАО «ИнфоТеКС».

Основные термины и определения

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

©2018, ОАО «ИнфоТеКС».

Государственные регуляторы по защите персональных данных

Роскомнадзор

ФСБ России

ФСТЭК России

В целях контроля за соблюдением операторами требований защиты ПДн проводятся **плановые** и **внеплановые** проверки.

©2018, ОАО «ИнфоТеКС».

Постановление Правительства РФ №1119 от 01 ноября 2012г.

При обработке персональных данных в ИС устанавливаются 4 уровня защищенности ПДн.

Уровень защищенности ПДн определяется в зависимости от:

- категории и объема ПДн;
- типа актуальных угроз.

©2018, ОАО «ИнфоТеКС».

Категории ПДн

- специальные
- биометрические
- общедоступные
- иные категории

©2018, ОАО «ИнфоТеКС».

Типы угроз

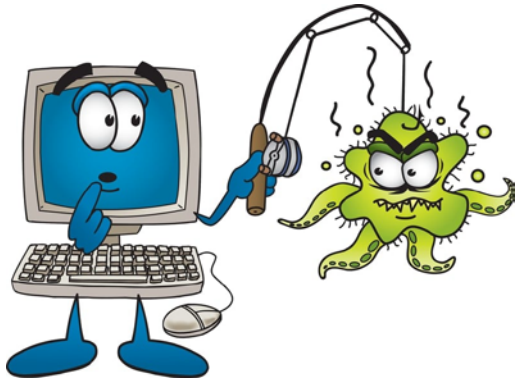
- 1- тип (наличие НДВ в системном ПО)
- 2-тип (наличие НДВ в прикладном ПО)
- 3-тип (не связанные с наличием НДВ в системном и прикладном ПО)

©2018, ОАО «ИнфоТеКС».

МУиН

При разработке МУиН определяются:

- актуальные угрозы безопасности ПДн;
- возможности потенциальных нарушителей безопасности ПДн



Формируются требования к системе защиты ПДн (СЗПДн).

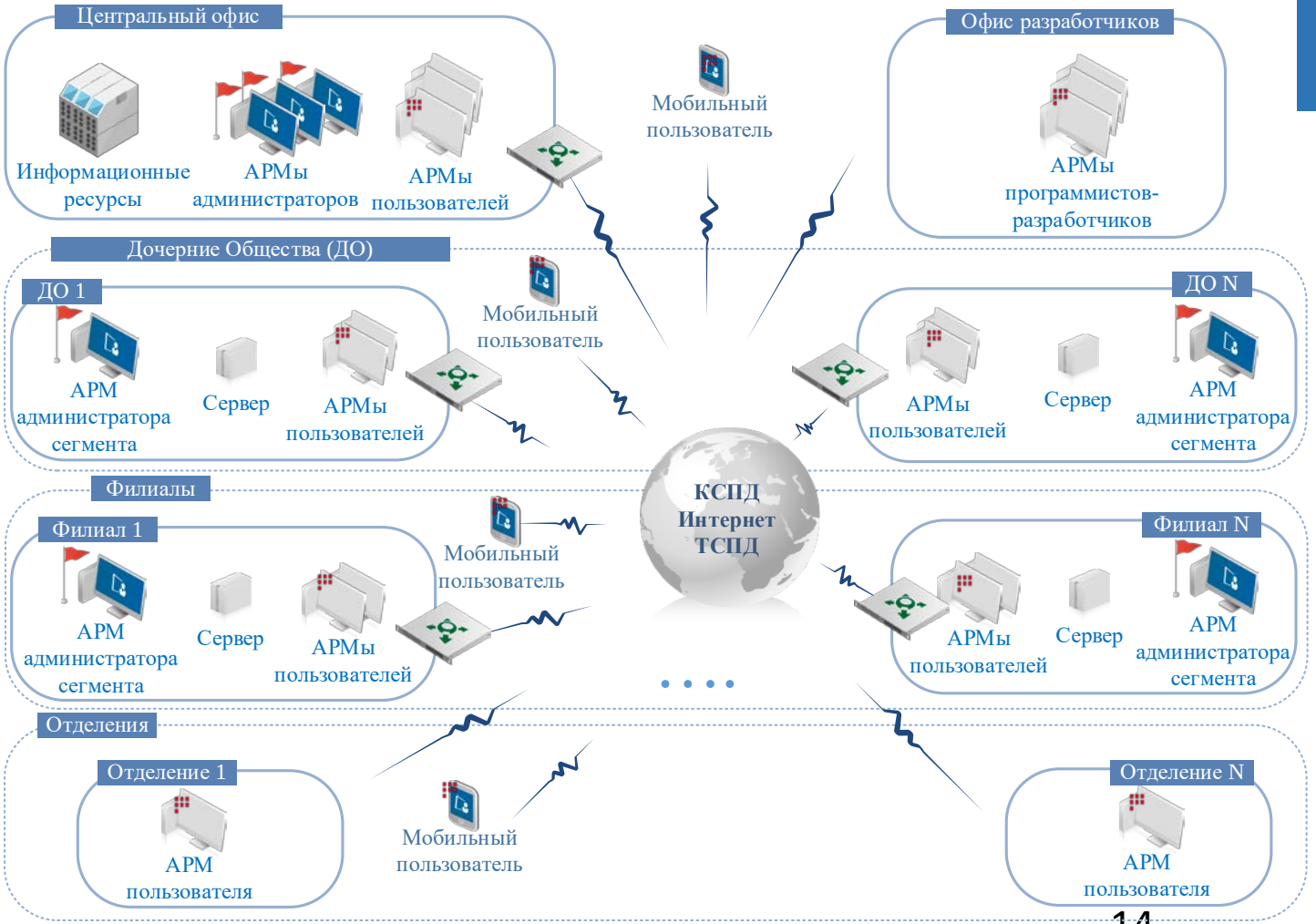
©2018, ОАО «ИнфоТеКС».

Проект документа «Методика определения угроз безопасности информации в информационных системах» ФСТЭК России

Потенциал нарушителя:

- Низкий
- Средний
- Высокий (спецслужбы иностранных государств (блоков государств).

©2018, ОАО «ИнфоТеКС».



©2018, ОАО «ИнфоТеКС».

СЗПДн

СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИС.

©2018, ОАО «ИнфоТеКС».

Основные меры по защите ПДн

Основные меры по защите ПДн, обрабатываемых в негосударственных ИС, приведены в **Приказе №21 от 18 февраля 2013 г.** «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн»

©2018, ОАО «ИнфоТеКС».

Основные меры по защите ГИС

Основные меры по защите информации, обрабатываемых в **государственных информационных системах (ГИС)**, приведены в **Приказе №17 от 11 февраля 2013г.** «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в ГИС»

©2018, ОАО «ИнфоТеКС».

Криптографические методы защиты информации

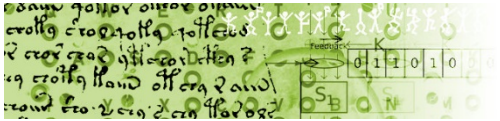
В Приказах № 17 и 21 не рассматриваются требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

©2018, ОАО «ИнфоТеКС».

Необходимость СКЗИ

Использование СКЗИ для безопасности ПДн необходимо:

- если ПДн подлежат криптографической защите **в соответствии с законодательством РФ**;
- если в ИС существуют **угрозы**, которые



могут быть **нейтрализованы только с помощью СКЗИ**.

Кроме того, решение о необходимости криптографической защиты ПДн может быть **принято конкретным оператором на основании технико-экономического сравнения альтернативных вариантов** обеспечения требуемых характеристик безопасности информации, содержащей, в том числе, ПДн.

©2018, ОАО «ИнфоТеКС».

Необходимость СКЗИ

К случаям, когда угрозы могут быть нейтрализованы **только с помощью СКЗИ**, относятся:

- **передача ПДн по каналам связи**, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию;

- **хранение ПДн на носителях информации**, НСД к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

©2018, ОАО «ИнфоТеКС».

Криптографические методы защиты ПДн

- Приказ ФСБ РФ от 10.07.2014 N 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием СКЗИ, необходимых для выполнения установленных Правительством РФ требований к защите ПДн для каждого из уровней защищенности»
- Методические рекомендации по разработке НПА, определяющих угрозы безопасности ПДн, актуальные при обработке ПДн в ИСПДн, эксплуатируемых при осуществлении соответствующих видов деятельности (утв. рук.8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432)

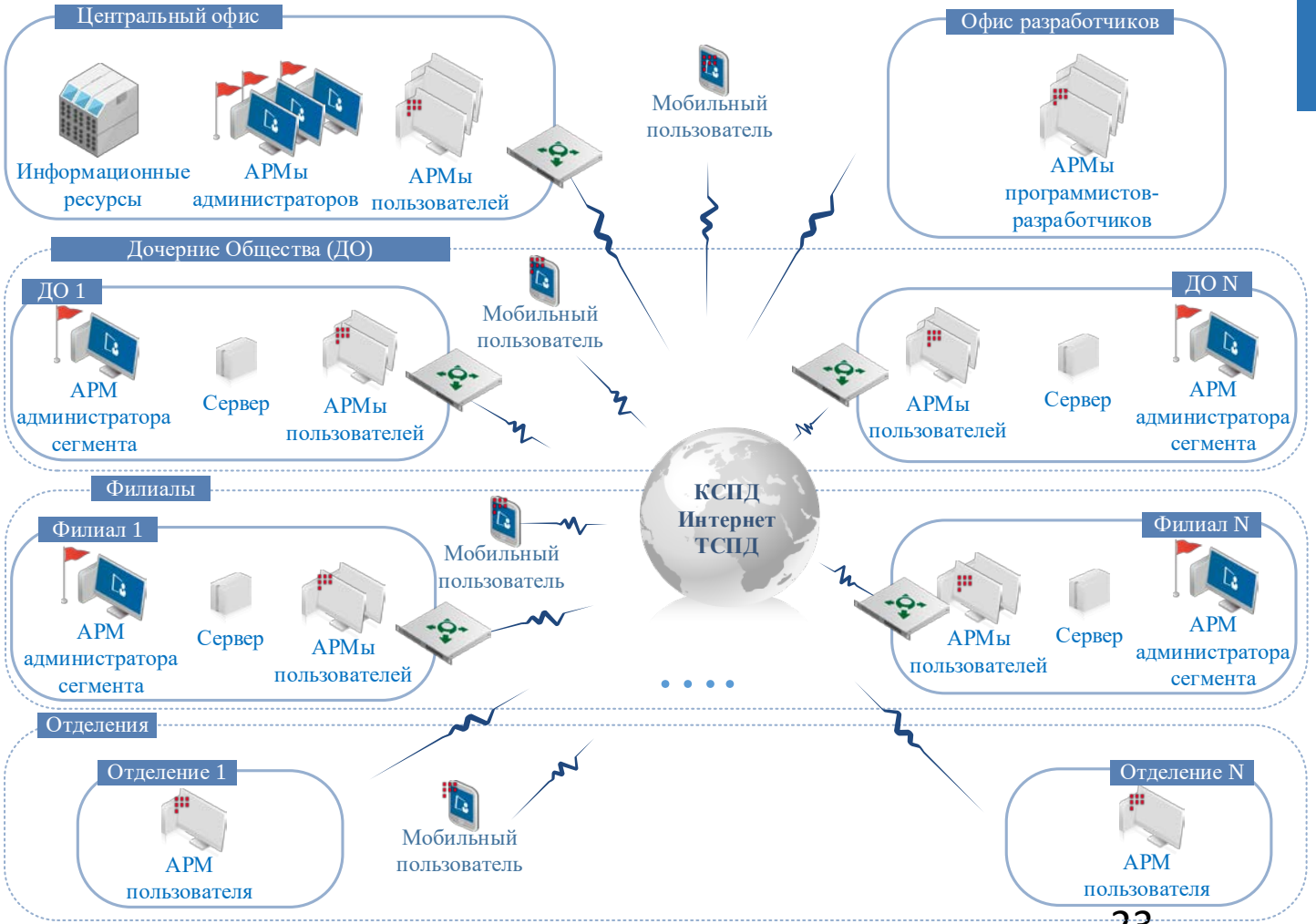
©2018, ОАО «ИнфоТеКС».

Приказ ФСБ РФ от 10.07.2014 N 378

В зависимости от предположений о возможностях нарушителя безопасности выделяют следующие классы СКЗИ:

- КС1
- КС2
- КС3
- КВ
- КА

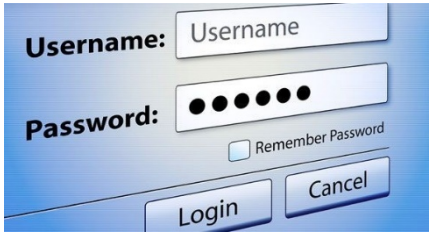
©2018, ОАО «ИнфоТеКС».



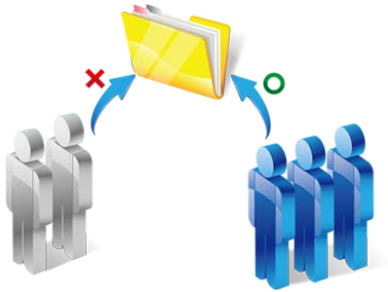
©2018, ОАО «ИнфоТеКС».

Основные меры по защите ПДн

Меры по идентификации и аутентификации субъектов доступа и объектов доступа.



Меры по управлению доступом субъектов доступа к объектам доступа.



©2018, ОАО «ИнфоТеКС».

Основные меры по защите ПДн

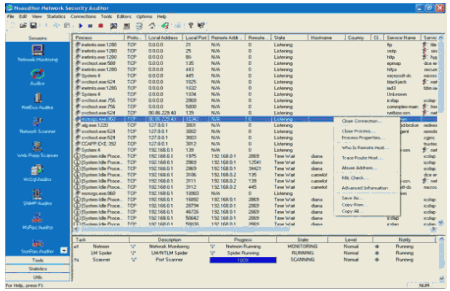
Меры по ограничению программной среды

Меры по защите машинных носителей ПДн (средств обработки (хранения) ПДн, съемных машинных носителей ПДн)

©2018, ОАО «ИнфоТеКС».

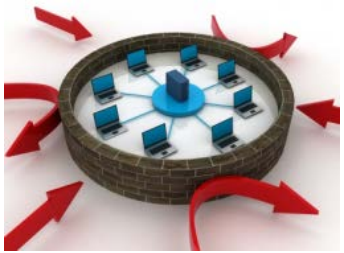
Основные меры по защите ПДн

Меры по регистрации событий безопасности



Меры по антивирусной защите

Меры по обнаружению (предотвращению) вторжений



©2018, ОАО «ИнфоТеКС».

Основные меры по защите ПДн

Меры по обеспечению целостности ИС и ПДн

Меры по обеспечению доступности ПДн

Меры по защите среды виртуализации

©2018, ОАО «ИнфоТеКС».

Основные меры по защите ПДн

Меры по защите ТС

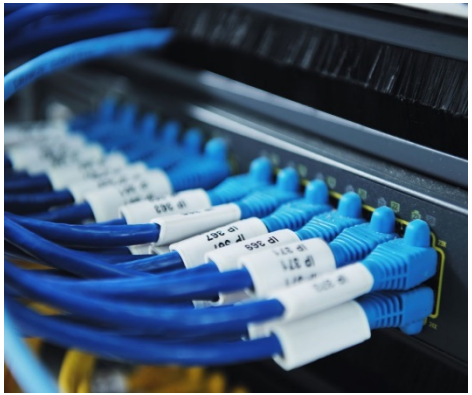
Меры по выявлению инцидентов и реагированию на них

Меры по управлению конфигурацией ИС и СЗПДн

©2018, ОАО «ИнфоТеКС».

Основные меры по защите ПДн

Меры по контролю (анализу) защищенности ПДн



Меры по защите ИС, ее средств, систем связи и передачи данных

©2018, ОАО «ИнфоТеКС».

Приказ №21 от 18 февраля 2013г.

Меры по обеспечению безопасности ПДн реализуются в том числе посредством применения в ИС **средств защиты информации**, прошедших в установленном порядке **процедуру оценки соответствия**, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности ПДн.

©2018, ОАО «ИнфоТеКС».

Приказ №17 от 11 февраля 2013г.

Для обеспечения **защиты информации**, содержащейся в ИС, применяются **средства защиты информации**, прошедшие оценку соответствия в форме **обязательной сертификации** на соответствие требованиям по безопасности информации

©2018, ОАО «ИнфоТеКС».


infotecs
Спасибо за внимание!