ПРОБЛЕМА 01.01.10

№152-ФЗ «О персональных данных»

Основное содержание закона №152-ФЗ о персональных данных

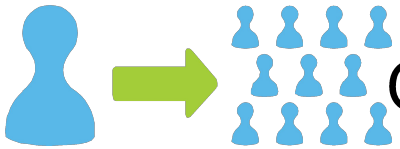
СУБЪЕКТ ПДн

1. САМОСТОЯТЕЛЬНО РЕШАЕТ вопрос передачи кому -либо своих ПДн
2. ИМЕЕТ ПОЛНОЕ ПРАВО на доступ к своим ПДн
3. Оформляет согласие на передачу ПДн ДОКУМЕНТАЛЬНО

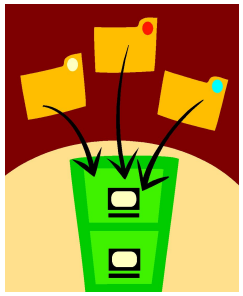
Персональные данные

Специальные категории персональных данных

Биометрические персональные данные



Оператор ПДн



Обработка ПДн

Использование ПДн

Распространение ПДн

Блокирование ПДн

Уничтожение ПДн

Обезличивание ПДн

Контроль и надзор

ФСБ ФСТЭК

РОСКОМНАДЗОР

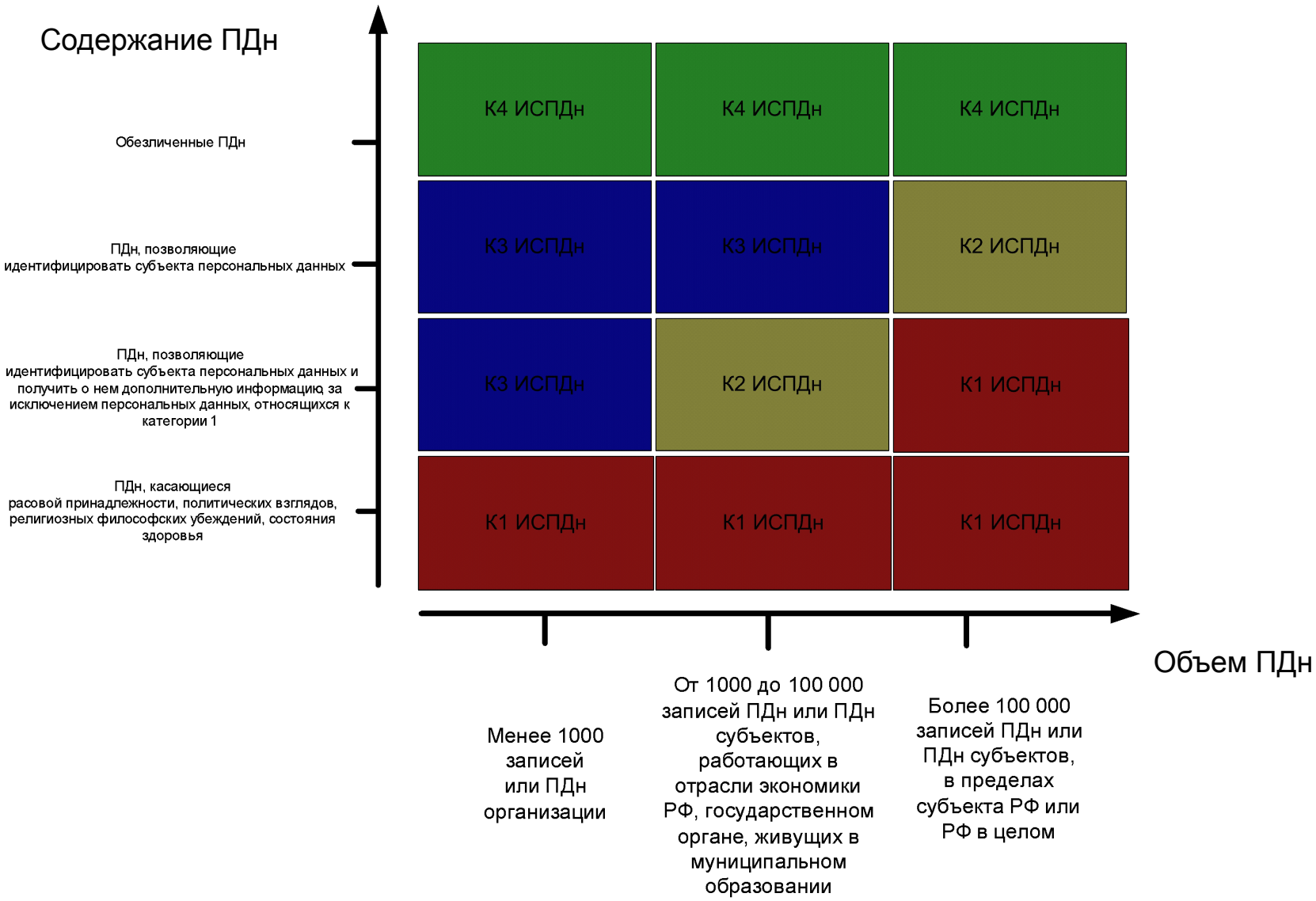
Защита субъектов ПДн

Ответственность за нарушение

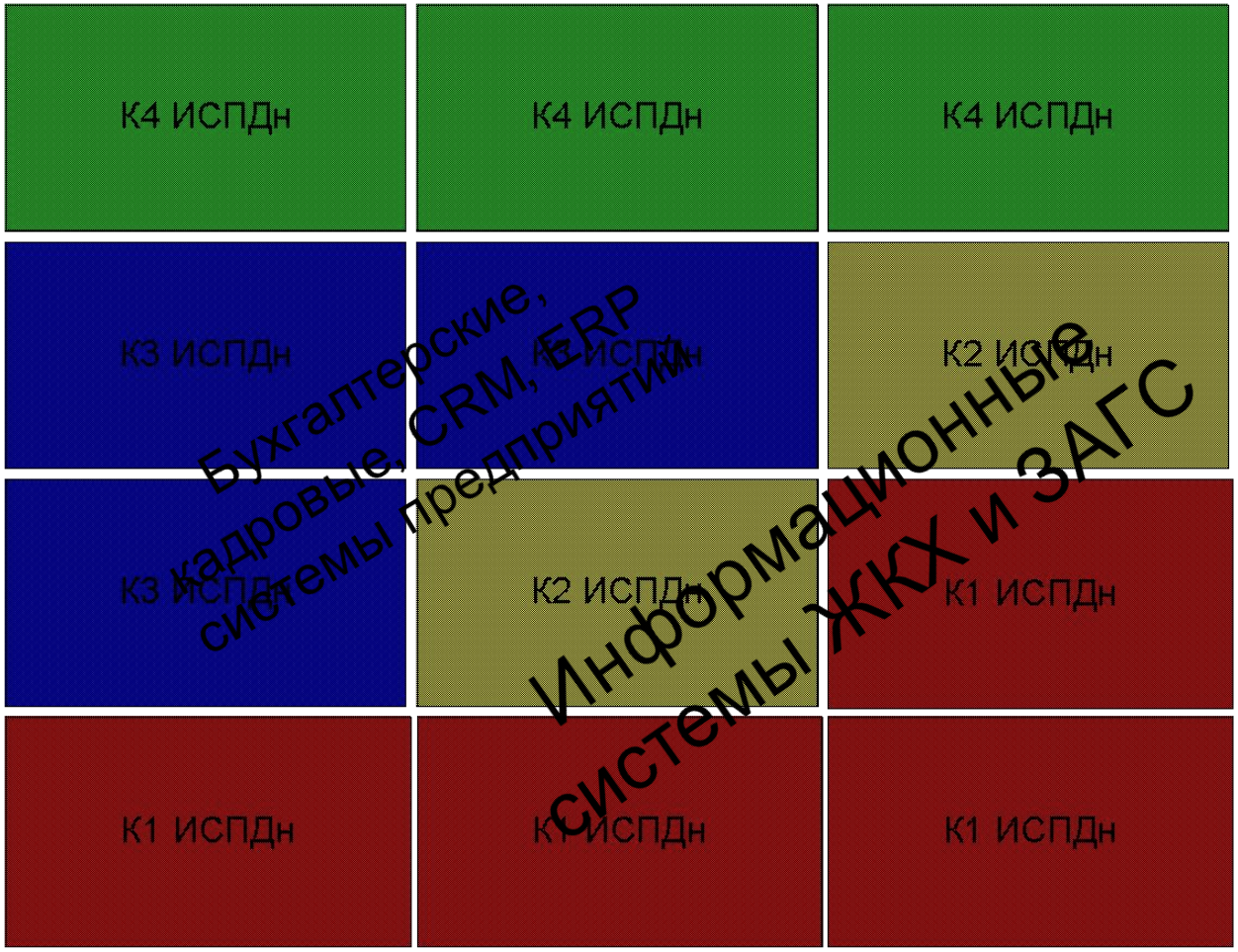
Постановление Правительства РФ от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"

Постановление Правительства РФ от 15 сентября 2008 г. N 687 Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации

Информационные системы персональных данных (ИСПДн)



Примеры информационных систем ПДн



Создание ИСПДн с СЗПДн

Эффективные технические подходы к реализации требований Закона о защите ПДн

1. Обезличивание персональных данных – уменьшение «периметра» защиты

2. Доступ к персональным данным с использованием терминалов, ограничивающих возможности физического съема информации в совокупности с контролем сессии и физическим наблюдением за действием персонала

3. Использование специализированного сертифицированного оборудования и ПАК для формирования VPN каналов, защиты от интернет-угроз (вирусы, черви, DDOS – атаки, хакеров и пр.), использование устройств DPI для выявления внешних и внутренних угроз, использование сертифицированного ПО (ОС, ПП, антивирусов и пр.)

4. ……..

X

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

X

Специальные категории персональных данных – данные о расовой и национальной принадлежности, политических взглядах, философских и религиозных убеждениях, состоянии здоровья и др.

X

Биометрические персональные данные - сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность

X

Оператор ПДн - государственный, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных

X

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных

X

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц

X

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом

X

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи

X

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных

X

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных

X

Направление в органы прокуратуры, другие правоохранительные органы материалов для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПДн

Приостановка действия или лишение лицензий , без которых деятельность по обработке персональных данных становится незаконной

Конфискация несертифицированных средств защиты информации (в т.ч. основного оборудования и программного обеспечения ИС, т.к. персональные данные обрабатываются непосредственно в ИС, а средства защиты интегрированы в стандартное оборудование и программное обеспечение ИС)

Конфискация используемых средств шифрования

Привлечение к административной и уголовной ответственности лиц, виновных в нарушении соответствующих статей уголовного и административного кодекса

X

Основные мероприятия по организации и техническому обеспечению безопасности персональных данных , обрабатываемых в ИСПДн

- Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн

Рекомендации по обеспечению безопасности персональных данных при их обработке в ИСПДн

- Базовая модель угроз безопасности персональных данных при их обработке в ИСПДн

Документы распространяются по запросу в в территориальные органы ФСТЭК
www.fstec.ru

X

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

**по обеспечению с помощью криптосредств
безопасности персональных данных при их обработке
в информационных системах персональных данных
с использованием средств автоматизации**

УТВЕРЖДЕНЫ
руководством 8 Центра
ФСБ России
21 февраля 2008 года
№ 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**

УТВЕРЖДЕНЫ
руководством 8 Центра
ФСБ России
21 февраля 2008 года
№ 149/6/6-622

www.fsb.ru

X

Типовые информационные системы обработки персональных данных - в которых требуется обеспечение только конфиденциальности персональных данных

X

Специальные информационные системы обработки персональных данных - в которых вне зависимости от необходимости обеспечения конфиденциальности требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

X

класс 1 (К1) - ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

для ИСПДн 1 и 2 классов - обязательная сертификация (аттестация) по требованиям безопасности информации;

В соответствии с положениями Федерального закона от 8 августа 2001 г. № 128 «О лицензировании отдельных видов деятельности» и требованиями постановления Правительства Российской Федерации от 16 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации» Операторы ИСПДн для проведения мероприятий по обеспечению безопасности ПДн (конфиденциальной информации) при их обработке в ИСПДн 1, 2 классов и в распределенных информационных системах 3 класса **должны получить лицензию на осуществление деятельности по технической защите конфиденциальной информации**

X

класс 2 (К2) - ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к негативным последствиям для субъектов ПД;

для ИСПДн 1 и 2 классов - обязательная сертификация (аттестация) по требованиям безопасности информации;

В соответствии с положениями Федерального закона от 8 августа 2001 г. № 128 «О лицензировании отдельных видов деятельности» и требованиями постановления Правительства Российской Федерации от 16 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации» Операторы ИСПДн для проведения мероприятий по обеспечению безопасности ПДн (конфиденциальной информации) при их обработке в ИСПДн 1, 2 классов и в распределенных информационных системах 3 класса **должны получить лицензию на осуществление деятельности по технической защите конфиденциальной информации**

X

класс 3 (К3) - ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

для ИСПДн 3 класса - декларирование соответствия требованиям безопасности информации;

В соответствии с положениями Федерального закона от 8 августа 2001 г. № 128 «О лицензировании отдельных видов деятельности» и требованиями постановления Правительства Российской Федерации от 16 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации» Операторы ИСПДн для проведения мероприятий по обеспечению безопасности ПДн (конфиденциальной информации) при их обработке в ИСПДн 1, 2 классов и в распределенных информационных системах 3 класса **должны получить лицензию на осуществление деятельности по технической защите конфиденциальной информации**

X

класс 4 (К4) - ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, не приводит к негативным последствиям для субъектов ПД.

для ИСПДн 4 класса оценка соответствия проводится по решению оператора.

X

определение необходимости обработки ПДн в ИСПДн;
определение перечня ПДн, подлежащих защите от НСД;
определение конфигурации ИСПДн;
определение технических средств и систем, использующихся в ИСПДн;
определение класса ИСПДн, проработка вопроса оптимизации класса;
определение модели действий персонала в обработке ПДн;
разработка модели угроз информационной безопасности ИСПДн.

X

Разработка технического решения СЗПДн на основе ТЗ;
Разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;
Разработка и реализация системы доступа пользователей к обрабатываемой на ИСПДн информации;
Определение подразделений и назначение лиц , ответственных за эксплуатацию СЗПДн;
Разработка эксплуатационной документации на ИСПДн и СЗИ, а также организационно-распорядительной документации по защите информации .

X

инсталляция и ввод в действие программно-технических и организационных мероприятий по защите ПДн в соответствии с разработанным графиком;
опытная эксплуатация СЗИ в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн и отработки ПДн;

X

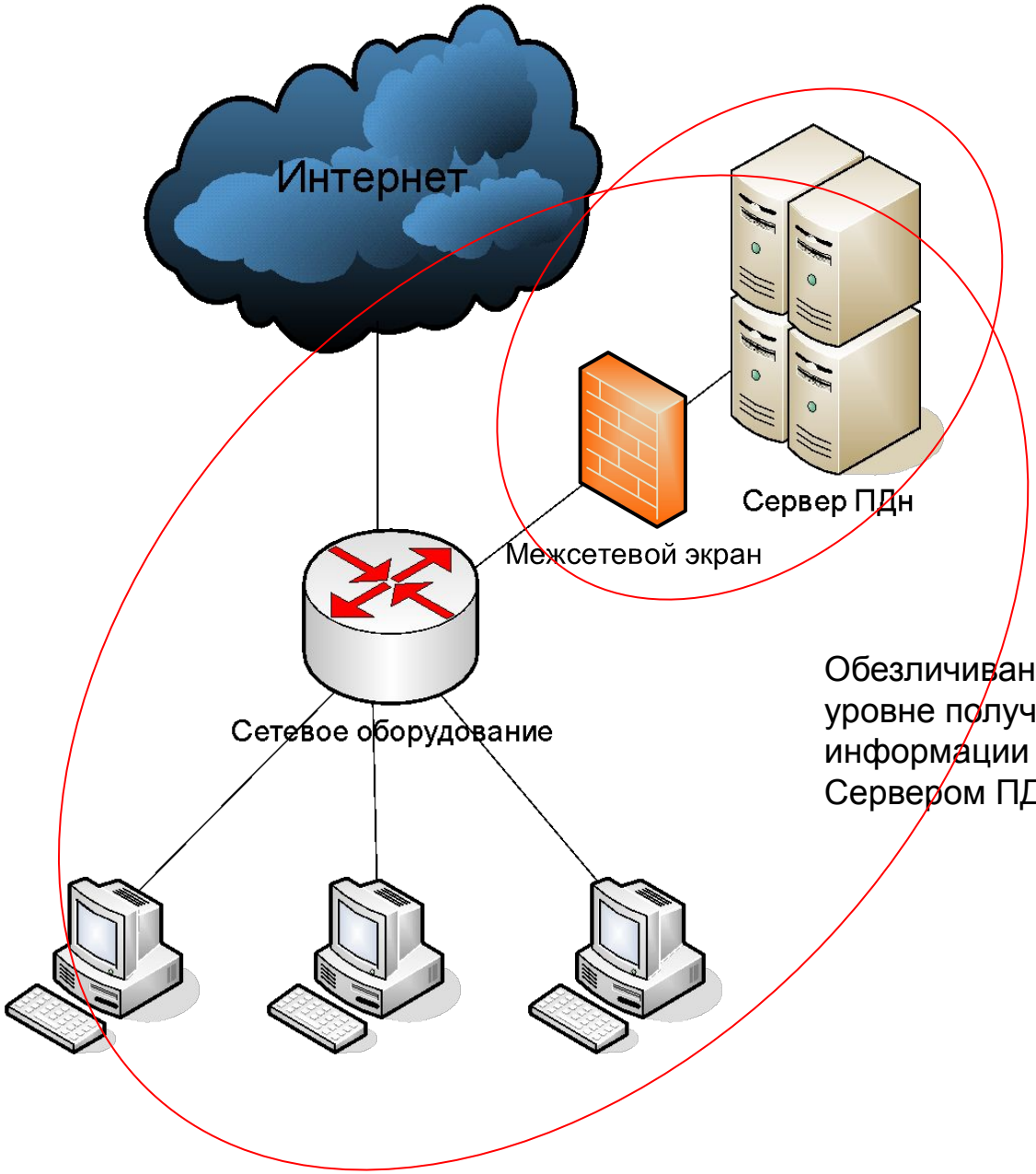
приемо-сдаточные испытания СЗИ по результатам опытной эксплуатации;
оценка соответствия ИСПДн требованиям безопасности ПДн.

X

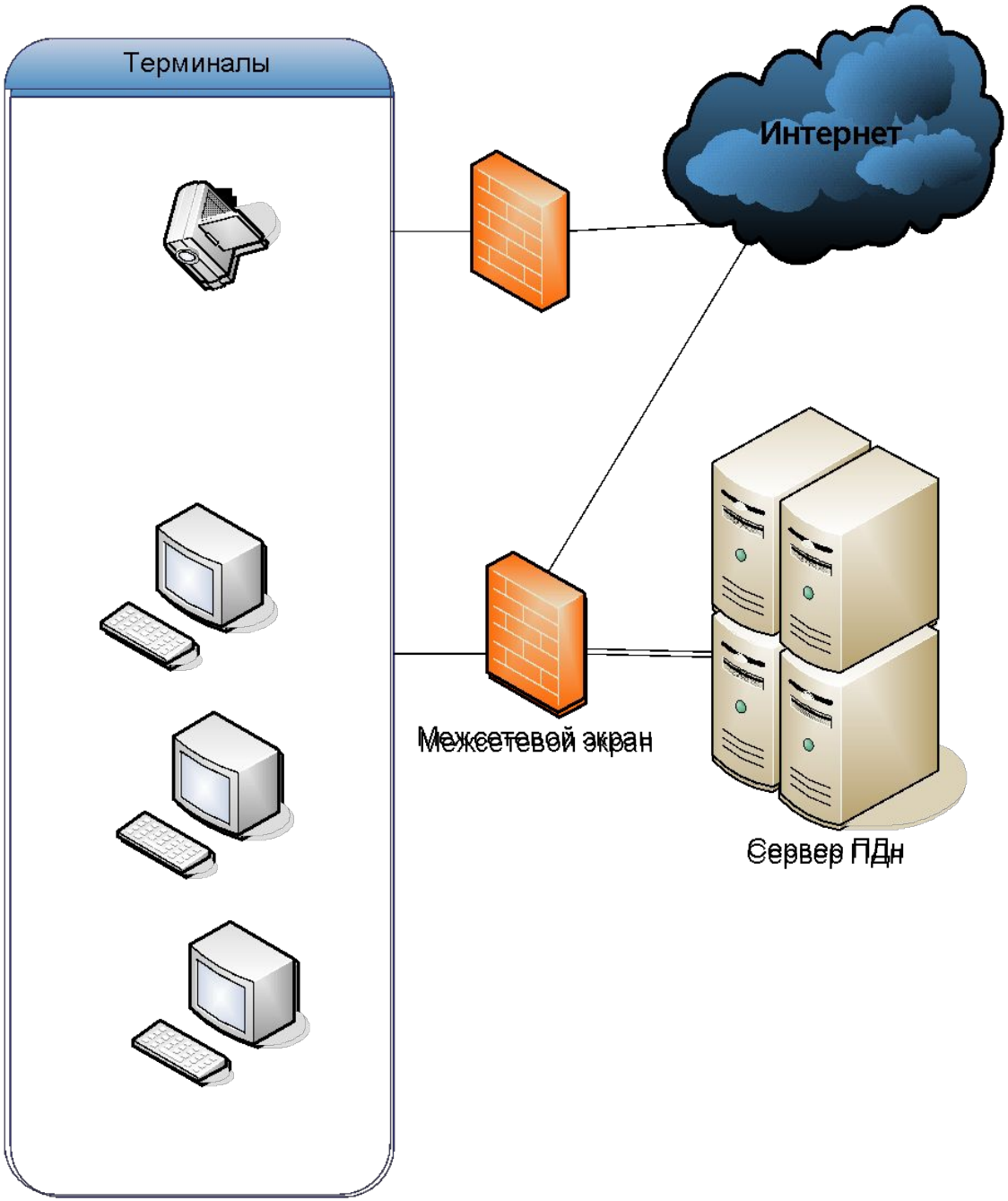
ИСПДн 1 и 2 классов - обязательная сертификация (аттестация) по требованиям безопасности информации;
ИСПДн 3 класса - декларирование соответствия требованиям безопасности информации;
ИСПДн 4 класса оценка соответствия проводится по решению оператора ПДн.

При аттестации объекта информатизации в соответствии с требованиями ФСТЭК подтверждается его соответствие требованиям по защите информации от НСД, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации. Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

X



Обезличивание ПДн на уровне получения информации сразу за Сервером ПДн.


Терминалы
Интернет
Межсетевой экран
Сервер ПДн

X

1. Сертифицированные ОС ПК и Серверов (Windows, Linux, прочие)

2. Сертифицированные антивирусные продукты (Kaspersky, Symantec, …) и специализированные программные продукты обрабатывающие ПДн (1С, SAP, …)

3. Сертифицированные ПАК VPN (VipNet-серия, Застава, Атликс-VPN, CSP VPN, …)

4. Специализированные DPI устройства (Huawei-Symantec, Cisco, Juniper …) для анализа внутреннего и внешнего траффика и защиты от интергент-угроз.

5. Специализированное программное обеспечение мониторинга систем информационной безопасности предприятия в комплексе (MaxPatrol, ArcSight, …)