



ДЕПАРТАМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Федеральный Закон №152 «О персональных данных» и
компетенции ЗАО «РАМЭК-ВС» по обеспечению их защиты**

Шибков Сергей Ильич
Директор департамента

ТЕХНОЛОГИЧЕСКИЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ

Создание комплексных систем
защиты конфиденциальной
информации

Аттестация объектов
информатизации по
требованиям безопасности
информации

Научно-исследовательские и
опытно-конструкторские
работы

Проведение сертификации по
требованиям безопасности
информации

Проведение специальной экспертизы
предприятий на право деятельности
по созданию СЗИ

СТРУКТУРНЫЕ ПОДРАЗДЕЛЕНИЯ ДЕПАРТАМЕНТА

Директор

Отдел маркетинга и
управления проектами

Отдел разработки и
внедрения
комплексных систем
безопасности
информации

Сектор
проектирования

Сектор внедрения

Отдел научно-
исследовательских и
опытно-
конструкторских
работ

Сектор
системных
решений

Сектор защиты
от НСД

Сектор защиты
от ПЭМИН

Сектор
криптографическ
ой защиты

Отдел аттестации
объектов
информатизации и
объектовых
специальных работ

Сектор
аттестации
объектов
информатизации

Группа
объектовых
специальных
работ

Испытательная
лаборатория

Группа контроля
по НСД

Группа контроля
по НДВ

Группа
тестирования

Отдел
специальных
экспертиз

ЛИЦЕНЗИИ И СЕРТИФИКАТЫ

**В
области
защиты
государс
т-венной
тайны**



**ФС
Б**

Осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (специальные работы)

Осуществление деятельности по выявлению электронных устройств предназначенных для не гласного получения информации в помещениях и технических средствах

~~Осуществление работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну (монтаж, наладка, установка, распространение и ТО шифровальные средства)~~

Осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (монтаж, наладка, установка, распространение и ТО шифровальные средства)



**ФСТЭ
К**

Осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации и ПДИТР)

Проведение работ, связанных с созданием средств защиты информации



**МО
РФ**

Деятельность в области создания средств защиты информации

**В области
защиты
конфиденциальной
информации
и
(в том
числе
защиты
персональ-
ных
данных)**



**ФС
Б**

Осуществление мероприятий и оказание услуг в области шифрования информации с использованием шифровальных (криптографических) средств

Осуществление деятельности по техническому обслуживанию шифровальных (криптографических) средств

Осуществление деятельности по распространению шифровальных (криптографических) средств



**ФСТЭ
К**

Деятельность по разработке и (или) производству средств защиты конфиденциальной информации

Деятельность по технической защите конфиденциальной информации



**МО
РФ**

Деятельность в области создания средств защиты информации



СИСТЕМА ДОБРОВОЛЬНОЙ СЕРТИФИКАЦИИ

ГАЗПРОМСЕРТ

**Научно-испытательный институт систем
обеспечения комплексной безопасности**

СЕРТИФИКАТ СООТВЕТСТВИЯ

**Проектирование , установка, пуско-наладочные
работы и техническое обслуживание
автоматизированных систем в защищенном
исполнении**

ПАРТНЕРЫ



Информзащита
Системный интегратор

s•terra
c s p

Aladdin[®]
SECURITY SOLUTIONS



Microsoft
GOLD CERTIFIED
Partner

2010
Preferred Partner
GOLD
hp



активаторы
КА(ПЕР)КОГО



- **Аудит состояния информационной безопасности** информационных и телекоммуникационных систем, оценка рисков, выработка политик информационной безопасности (ИБ);
- **Проектирование** информационных систем (автоматизированных систем управления производством, географических информационных систем и др.) и объектов в защищенном исполнении;
- **Создание** защищённых информационных и телекоммуникационных систем и объектов любой сложности в соответствии с требованиями по безопасности информации, предъявляемыми руководящими документами ФСБ России, ФСТЭК России и Минобороны России;
- **Специальные проверки и специальные исследования** технических средств и систем, предназначенных для хранения, обработки и передачи информации, составляющей государственную тайну, или предназначенных для размещения в помещениях, предназначенных для проведения мероприятий с обсуждением информации, составляющей государственную тайну;
- **Аттестация объектов информатизации** по требованиям безопасности информации, составляющей государственную тайну и конфиденциальные сведения (в том числе персональные данные);
- **Подбор, поставку, настройку и установку аппаратных и программных средств защиты информации** в соответствии с требованиями заказчика и разработанной политикой безопасности, разработке, созданию и вводу в строй систем защиты информации (СЗИ) эксплуатируемых и создаваемых локальных и глобальных автоматизированных систем, техническое сопровождение СЗИ в течение гарантийного срока эксплуатации, а также послегарантийное обслуживание;
- **Консалтинг** в области информационной безопасности.
- **Сертификация автоматизированных систем, средств и комплексов защиты информации** в системе сертификации МО РФ.
- **Экспертная оценка** предприятий промышленности, организаций и компаний на соответствие требованиям МО РФ на право получения лицензий на деятельность в области защиты информации.

СОТРУДНИКИ



ВУЗЫ базового специального образования:

Военная академия связи, Военно-воздушная академия им.Ю.А.Гагарина, МГТУ им. Баумана, МИФИ, МТУСИ, Высшие военные учебные заведения по командным и инженерным специальностям радиоэлектроники, РЭБ, электросвязи

Характеристика кадрового

Высшее образование в предметной области		100 %
Стаж работы в предметной области	<i>свыше 20 лет-</i>	20 %
	<i>от 10 до 20 лет</i>	30 %
	<i>от 5 до 10 лет</i>	30 %
	<i>менее 5 лет</i>	20 %
Возраст	<i>свыше 50 лет</i>	20 %
	<i>от 35 до 50</i>	70%
	<i>менее 35</i>	10 %

Сертификаты подтверждающие квалификацию (повышение

Зарубежные компании	Cisco Career Certifications, Symantec Expert, Alladin, ICDN Cisco, IBM	20 %
Российские компании (учебные центры)	«ЦБИ», «Маском», «Информзащита», «Форт», «Инфотекс», «Эшелон», «Центрпрограммсистем», «ГАСИС», «ВНИИС» ОКБ «САПР»	100%

ВЫПОЛНЕННЫЕ ПРОЕКТЫ



**Федеральные
и
региональные
органы
исполнительно
й власти
Коллектив
Департамента –
активно
развивает
направление по
реализации 152
ФЗ «О защите
персональных
данных»**

2009 год

- ❖ Проектно-изыскательские работы по модернизации информационной системы обработки персональных данных Министерства социального развития Саратовской области
- ❖ Проектно-изыскательские работы по модернизации информационной системы обработки персональных данных Государственного комитета социальной поддержки населения Саратовской области
- ❖ Осуществление поставки средств защиты информации и работы по их установке для создания и развития информационной системы для предоставления государственных и муниципальных услуг на основе многофункциональных центров в Тамбовской области.

2007-2008 год

- Разработка технического проекта на создание «Системы защиты информации, обрабатываемой в автоматизированной информационной системе «Государственный заказ» Ханты-Мансийского автономного округа.
- Разработка концепции по Информационной безопасности администрации Ямало-ненецкого автономного округа.
- Модернизация системы защиты информации в Управлении Федерального казначейства по Москве и Московской области, выполнение специальных работ, аттестация локальных вычислительных сетей УФК.
- Выполнение работ по защите выделенных помещений, первых отделов в различных учреждениях, организациях, на предприятиях и компаниях. Аттестация объектов информатизации для обработки сведений составляющих государственную тайну.



**Коллектив
Департамента –
участник
комплексной
целевой
программы
Службы
корпоративной
защиты ОАО
«Газпром» по
безопасности
информации**

2009 год

- ❖ Проектно-изыскательские работы по созданию «Комплексной системы защиты информации информационно-управляющей системы производственно-хозяйственной деятельности ООО «Газпром трансгаз Ставрополь»
- ❖ Проектно-изыскательские работы по созданию «Защищенного узла доступа ООО «Газпром трансгаз Ставрополь»
- ❖ Проектно-изыскательские работы по созданию «Системы управления доступом к сетевому оборудованию ООО «Газпром трансгаз Ставрополь»

2007-2008 год

- Проектно-изыскательские работы по созданию «Системы информационной безопасности Региональной сети передачи данных ООО «Газпром ноябрьск добыча»
- Проектно-изыскательские работы по созданию «Системы информационной безопасности информационно-вычислительной системы Объекта №4 ОАО «Газпром»
- Проектно-изыскательские работы по созданию «Системы информационной безопасности информационно-вычислительной системы Объекта №5 ОАО «Газпром»
- Проектно-изыскательские работы по созданию «Системы информационной безопасности информационно-вычислительной системы Объекта №6 ОАО «Газпром»
- Внедрение Удостоверяющего центра в ООО «Новоуренгойский газохимический комплекс»
- Участие в разработке проекта на создание «Системы защиты информации информационно-управляющей системы производственно-хозяйственной деятельности ООО «Надымгазпром».

Минобороны России



*Коллектив
Департамента –
разработчик
систем
защиты
информации в
АСУ
вооружения и
военной
техники*

2009 год

- ❖ Участие в проектах по созданию автоматизированной системы Вооруженных Сил Российской Федерации в части защиты информации и противодействия иностранным техническим разведкам
- ❖ Выполнение опытно-конструкторских работ по созданию систем защиты информации комплексных систем тренажеров для отработки задач по управлению вооружением и военной техникой
- ❖ Выполнение опытно-конструкторских работ по созданию систем защиты информации информационных и управляющих систем вооружения и военной техники
- ❖ Выполнение объектовых специальных исследований на объектах информатизации органов военного управления Министерства обороны Российской Федерации.

2008-2007 год

- Выполнение опытно-конструкторской работы по созданию системы защиты информации в функциональной системе освещения обстановки в составе интегрированной АСУ Военно-морского флота
- Выполнение опытно-конструкторской работы по созданию системы защиты секретной информации специального назначения
- Выполнение опытно-конструкторской работы по созданию «Системы информационной безопасности оперативно-тактического тренажерного комплекса ВМФ»
- Участие в выполнении опытно-конструкторской работы по созданию системы защиты секретной информации боевого объекта ВМФ
- Проведение сертификации специального программного обеспечения объектов вооружения и военной техники.

***Основные положения Федерального Закона
№152 «О персональных данных»
Правоотношения в сфере защиты
персональных данных***

Нормативно-правовая база обеспечения безопасности персональных данных

Федеральный закон РФ от 27 июля 2006 г. №152-ФЗ



«О персональных данных» с изменениями от 16.12.09 г.

Постановление правительства РФ от 17 ноября 2007 г. № 781
«Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

Приказ ФСТЭК, ФСБ, Мининформсвязи России от 13 февраля 2008 г. №55/86/20 г.

Москва

«Об утверждении порядка проведения классификации информационных систем персональных данных»

Руководящие документы ФСТЭК

«Базовая модель угроз безопасности ПДн при их обработке в информационных системах персональных данных»

«Методика определения актуальных угроз безопасности ПДн при их обработке в информационных системах персональных данных»

«Основные мероприятия по организации и техническому обеспечению безопасности ПДн, обрабатываемых в информационных системах персональных данных»

«Рекомендации по обеспечению безопасности ПДн при обработке в информационных системах персональных данных»

Документы ФСБ

«Методические рекомендации по обеспечению с помощью криптографических средств безопасности ПДн при обработке в информационных системах персональных данных с использованием автоматизации»

«Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащих сведений составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных».

Безопасность персональных данных - состояние защищенности, характеризующее способность пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в информационных системах ПДн.



Система защиты персональных данных

Организационные меры и средства защиты информации (в том числе криптографические)

Средства предотвращающие несанкционированный доступ к информации

Средства предотвращающие утечку по техническим каналам

Средства предотвращающие программно-техническое воздействие на ПДн

Свойства используемых программно-технических информационных технологий ПДн

Функции органов государственной системы защиты ПДн

ФСТЭК
ФСБ

Разработка методов и способов защиты информации в информационных системах ПДн в пределах полномочий

Государственный контроль достаточности принятых мер по обеспечению безопасности ПДн

Оператор *

Обеспечение безопасности ПДн при их обработке путем выполнения требований системы защиты.
**Выполнение требований может быть поручена уполномоченному лицу, имеющему разрешительные документы на этот вид деятельности*

Основные участники правоотношений в сфере персональных данных

Субъект персональных данных

Принимает решение о предоставлении своих ПДн и дает согласие на их обработку

Оператор персональных данных

Государственный орган, муниципальный орган, юридическое, или физическое лицо, организующее и (или) осуществляющее обработку ПДн

Имеет право:

- ❖ **Ознакомления со сведениями*:**
 1. **Об операторе (местонахождении, наличии сведений ПДн субъекта);**
 2. **О ПДн, относящимся к субъекту и требовать уточнения, а при необходимости уничтожения или блокирования;**
 3. **О процессе обработки ПДн субъекта (при запросе).**
- ❖ **На принятие (непринятие) решения на основании информации по ПДн на основании исключительно автоматизированной обработки его персональных данных;**
- ❖ **Обжалование действий (бездействия) оператора по обеспечению безопасности ПДн.**

**Право на ознакомление ограничивается:*

1. **Если обработка осуществляется в целях обороны страны, безопасности государства, охраны правопорядка;**
2. **Если обработка осуществляется органами,**

Обязан:

- ❖ **Оставлять субъекту ПДн по его просьбе информацию по подтверждению обработки ПДн, способах обработки, сведения о лицах, допущенных к обработке, о перечне ПДн, сроках хранения, юридические последствия обработки;**
- ❖ **Разъяснять юридические последствия в случаях отказа представления ПДн ;**
- ❖ **Обеспечивать меры безопасности ПДн;**
- ❖ **Безвозмездно представлять субъекту возможность ознакомления со своими ПДн, внесения изменений, уточнений, а в случае необходимости уничтожения или блокирование**
- ❖ **В случае отказа в представлении ПДн, принадлежащий субъекту –мотивировать отказ;**
- ❖ **Сообщать в уполномоченный орган по защите прав субъектов ПДн по его запросу, информацию необходимую для осуществления его деятельности.**

Требования к оператору (уполномоченному лицу) осуществляющему



Федеральный закон РФ №128-ФЗ от 8 августа 2001 года
«О лицензировании отдельных видов деятельности»

Постановления правительства РФ

- ❖ от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»
- ❖ от 31 августа 2006 г. № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»
- ❖ от 29 декабря 2007 г. № 957 «О лицензировании отдельных видов деятельности связанных с шифровальными (криптографическими) средствами»

Лицензии ФСТЭК

На деятельность по технической защите конфиденциальной информации
На проведение работ, связанных с созданием средств защиты информации

Лицензии ФСБ

На осуществление технического обслуживания шифровальных (криптографических) средств
На осуществление распространения шифровальных (криптографических) средств
На предоставление услуг в области шифрования информации

Наличие специалистов имеющих профильное образование или прошедших обучение (повышение квалификации)

Наличие необходимой нормативно-методической и руководящей документации

Наличие необходимого материально-технического обеспечения

Определение класса информационной системы



RAMES

ПДн Этапы классификации

Сбор и анализ исходных данных

Определение категории (Хпд)

Определение объема Пдн (Хн пд)

Анализ заданных оператором характеристик безопасности Пдн

Анализ структуры информационной системы Пдн

Определение наличия подключения к сетям общего пользования и международного обмена

Анализ режима обработки Пдн

Анализ режима разграничения прав доступа

Анализ размещения (местоположения) технических средств обработки Пдн

Классификация

Типовые (по классам)

К1-значительные негативные последствия

К2-негативные последствия

К3-незначительные негативные последствия

К4-без негативных последствий

Специальные

по результатам анализа исходных данных определяется класс специальной информационной системы, а на основе модели угроз безопасности персональных данных в соответствии с методическими документами, уточняются требования по безопасности

Документальное оформление

Акт оператора о присвоении класса ИС

Акт оператора о присвоении статуса специальной системы

Специальные информационные системы*

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

К специальным информационным системам должны быть отнесены:

- информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;
- информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

****Класс специальной информационной системы определяется на основе анализа исходных данных, а на основе модели угроз безопасности персональных данных при обработке в информационных системах ПДн уточняются требования по защите.***

ФЗ 152 «Лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность»

Кодексы РФ	Статьи	Максимальное наказание
Кодекс об административных правонарушениях (КоАП РФ)	13.11, 13.12, 13.13, 13.14, 5.27, 5.39, 19.4, 19.5, 19.6, 19.7, 19.20, 20.25	<p>! Штраф до 500 тыс. руб.; Конфискация; ! Приостановление деятельности на срок до 90 суток; ! Дисквалификация должностного лица на срок от одного года до трех лет</p>
Трудовой кодекс (ТК РФ)	237, 195, 90, 81	<p>! Денежная компенсация за причиненный моральный вред; ! Увольнение</p>
Уголовный кодекс (УК РФ)	137, 140, 171	<p>! Штраф до 300 тыс. руб.; ! Арест до 6-ти месяцев; ! Лишение права занимать должность на срок до 5-ти лет</p>

***Услуги и решения ЗАО «РАМЭК-ВС» по
созданию системы защиты
персональных данных на объектах
обработки информации предприятий и
организаций***

Технологические направления по созданию систем защиты ИСПДн

А. Разработка, научные

исследования:

Разработка проектных решений по созданию информационных систем в защищенном исполнении

Проведение научно-исследовательских и опытно-конструкторских работ

Сертификация программно-аппаратных комплексов по требованиям безопасности

Разработка моделей, методологии (концепций) защиты

Б. Практическая реализация:

Внедрение систем защиты от несанкционированного доступа

Оборудование объектов информатизации (выделенных, защищаемых помещений) средствами защиты от утечки по техническим каналам

Разработка организационно-распорядительной документации по защите информации



Аттестация объектов информатизации по требованиям безопасности информации

ЗАО «РАМЭК-ВС» выполняет полный комплекс работ по созданию систем защиты ИСПДн и руководствуется экономической целесообразностью и эффективностью мер, обеспечивающих выполнение требований безопасности информации.



1 Аудит информационной системы персональных данных, анализ соответствия нормативным требованиям

- получение исходных качественных и количественных параметров для организации проектирования
- оценка состояния системы по параметрам соответствия с требованиями руководящих документов ФСТЭК и ФСБ России



Отчет об обследовании
(концепция)

2 Разработка требований безопасности информационной системы персональных данных

- классификация ИСПДн
- формирование модели угроз безопасности
- разработка требований по безопасности
- проведение экспертизы в регулирующих органах (по желанию заказчика)



Техническое задание на проектирование

3 Разработка системы защиты персональных данных

- проектирование системы защиты
- разработка организационно-распорядительной документации
- отработка процессов функционирования системы, проведение испытаний и доводка на макетах и стендах (по желанию заказчика)



Технический проект

ЗАО «РАМЭК-ВС» предлагает Технические решения по защите персональных данных разработанных на базе собственных аппаратно-программных комплексов и сертифицированных продуктов ведущих российских и зарубежных компаний.



4 Внедрение проектных решений
(установка, пуско-наладка аппаратных средств, инсталляция и настройка СПО)



Действующая система защиты информации

- подготовка к аттестации, включая разработку разрешительной документации системы доступа, организационно-распорядительной документации, технической документации на объект в части касающейся ЗПДн

- проведение аттестационных испытаний на соответствие требований безопасности информации, включая экспертное обследование объекта информатизации, исследований на предмет утечки по техническим каналам, комплексные исп



5 Аттестация объектов информатизации

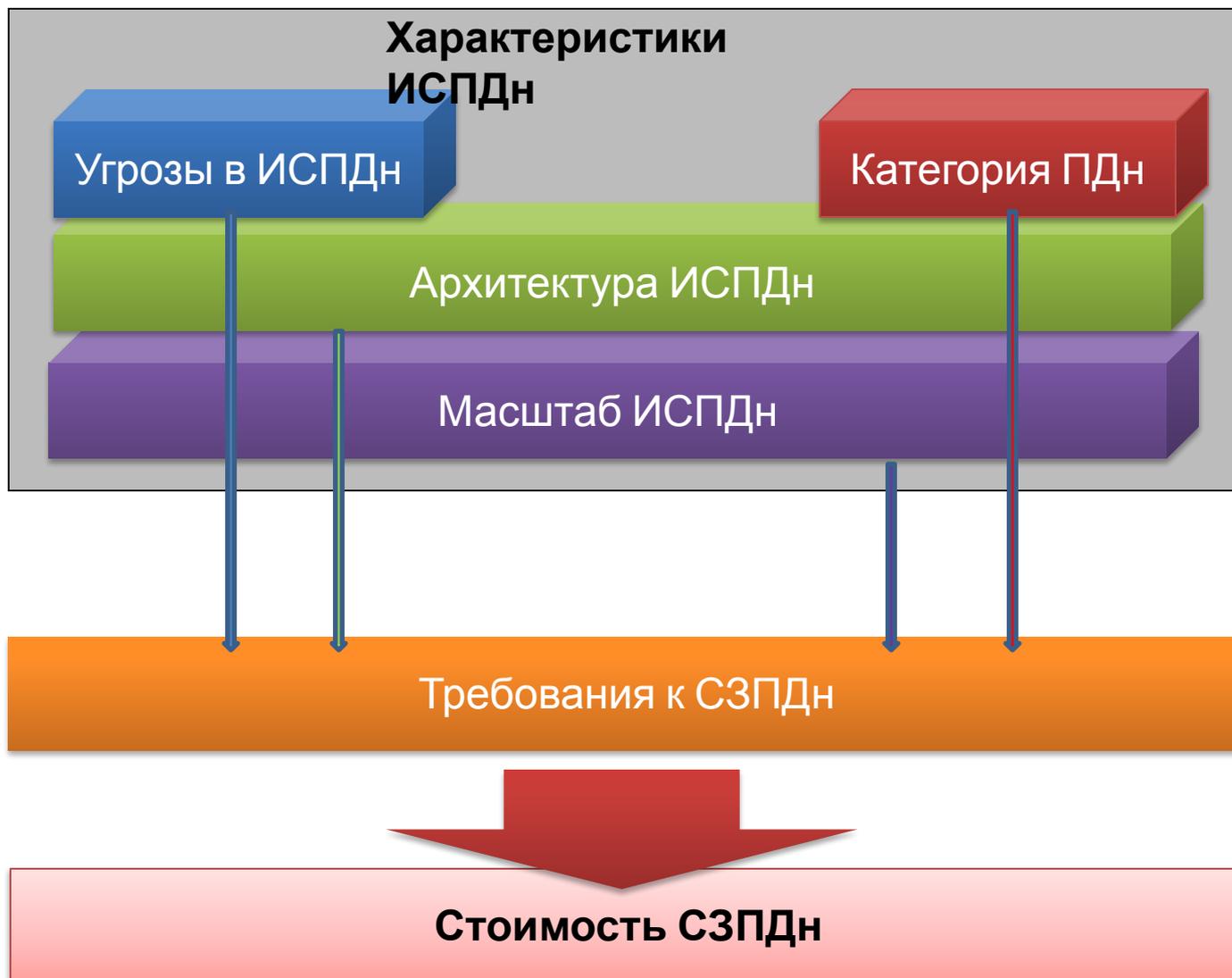
Аттестат соответствия

6 Сервисное обслуживание



Оперативное восстановление системы, периодический контроль

Факторы, влияющие на стоимость СЗПДн

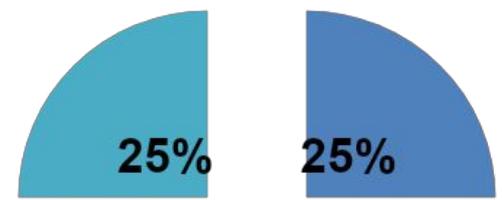


СТОИМОСТЬ РАБОТ ПО ЗАЩИТЕ ИСПДН
 приближенно-типового объекта в составе 20 АРМ (ПЭВМ
 стандартной конфигурации) + 1 сервер + 4 СКЗИ

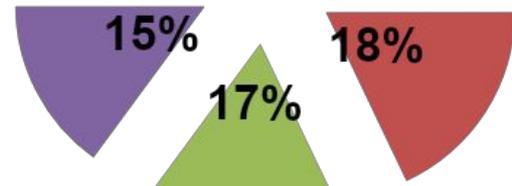
120 000-200 000 руб.



Органы управления
 Промышленные предприятия



Государственные образовательные учреждения



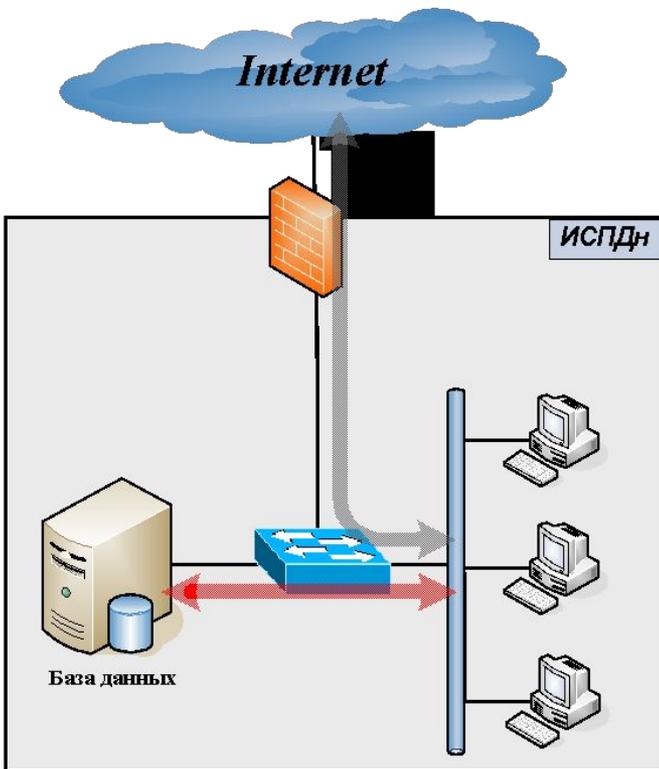
Условные обозначения

-  Оборудование
-  Сбор и анализ исходных данных
-  Проектирование
-  Установка и настройка СЗИ и СКЗИ
-  Аттестация

***Решения ЗАО «РАМЭК-ВС» по снижению
стоимости при создании системы
защиты персональных данных на объектах
обработки информации предприятий и
организаций***

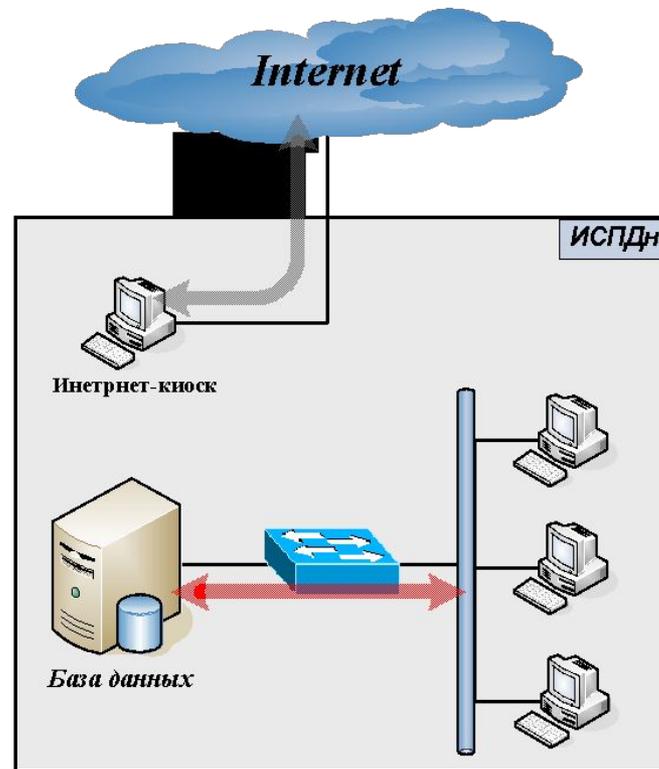
Отключение от сетей общего пользования

до преобразования



 - обработка ПДн

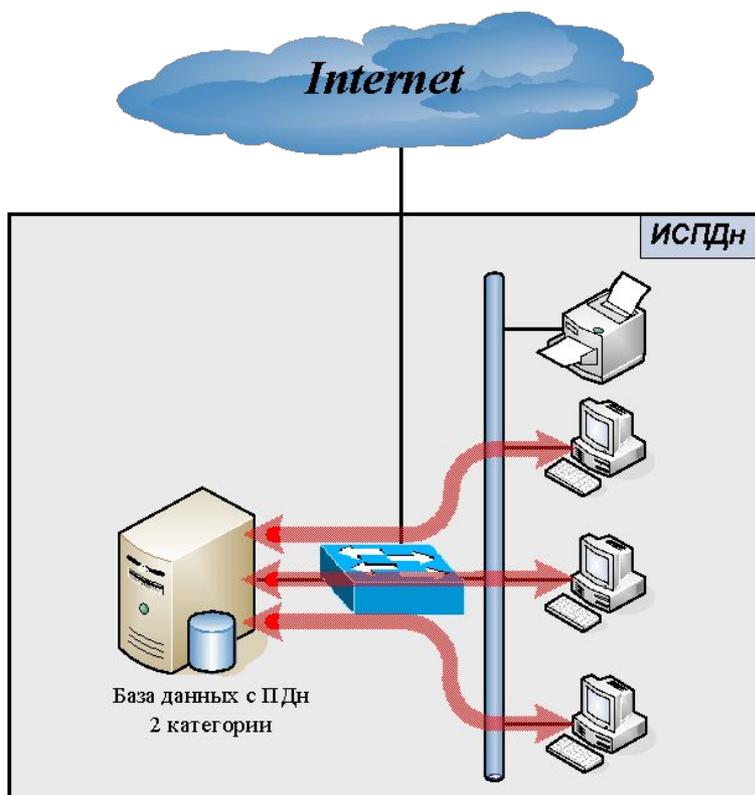
после преобразования



 - информационный обмен с внешними сетями

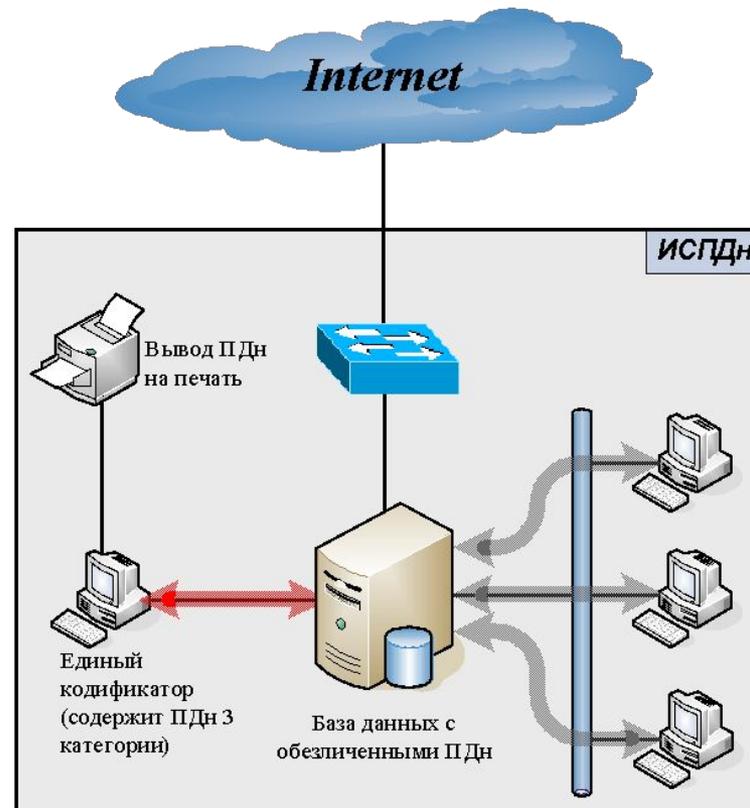
Обезличивание персональных данных обрабатываемых в ИСПДн

до преобразования



 - обработка ПДн

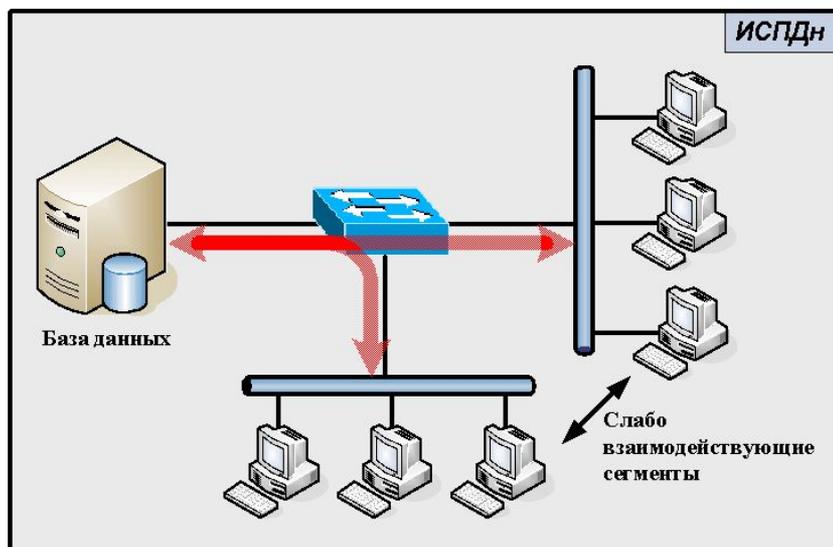
после преобразования



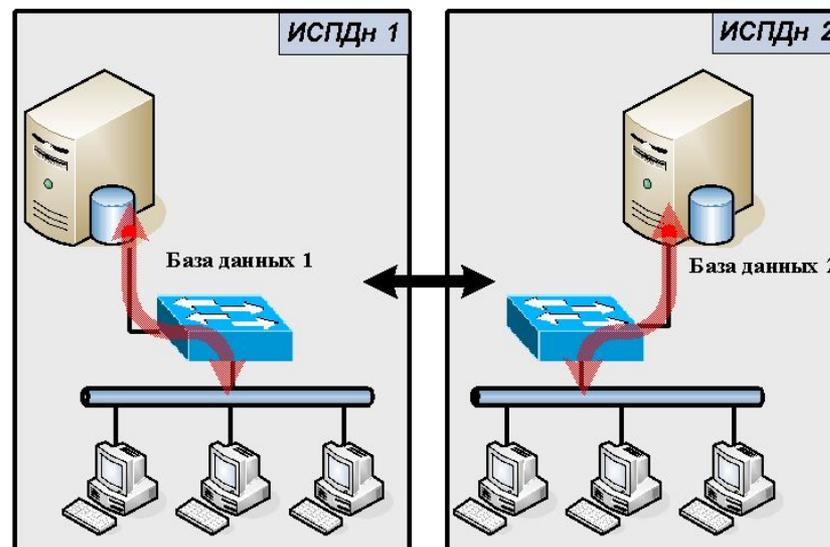
 - обработка обезличенных ПДн

Сегментирование и оптимизация архитектуры ИСПДн.

до преобразования



после преобразования

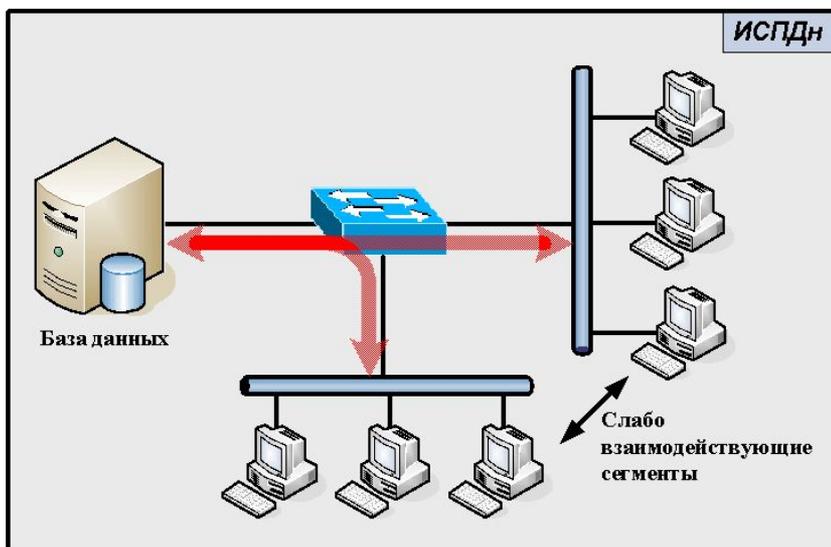


 - обработка ПДн

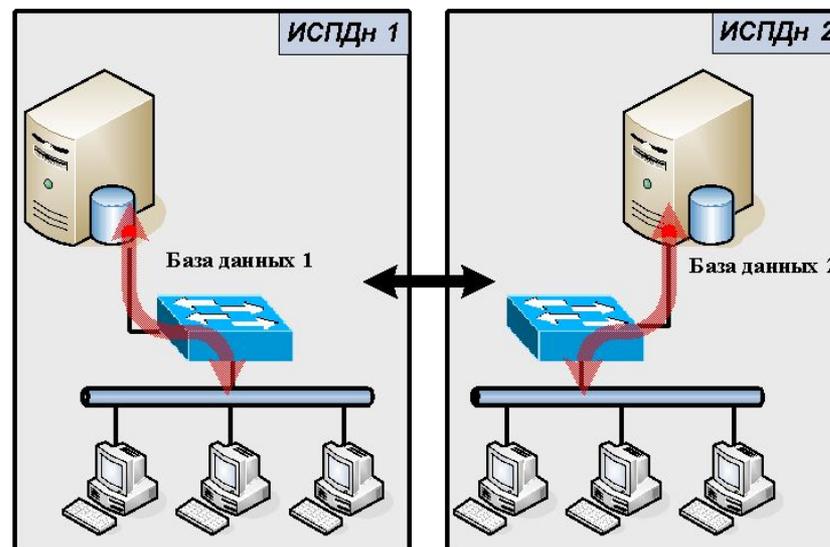
 - обмен информацией с помощью съемных носителей

Сегментирование и оптимизация архитектуры ИСПДн.

до преобразования



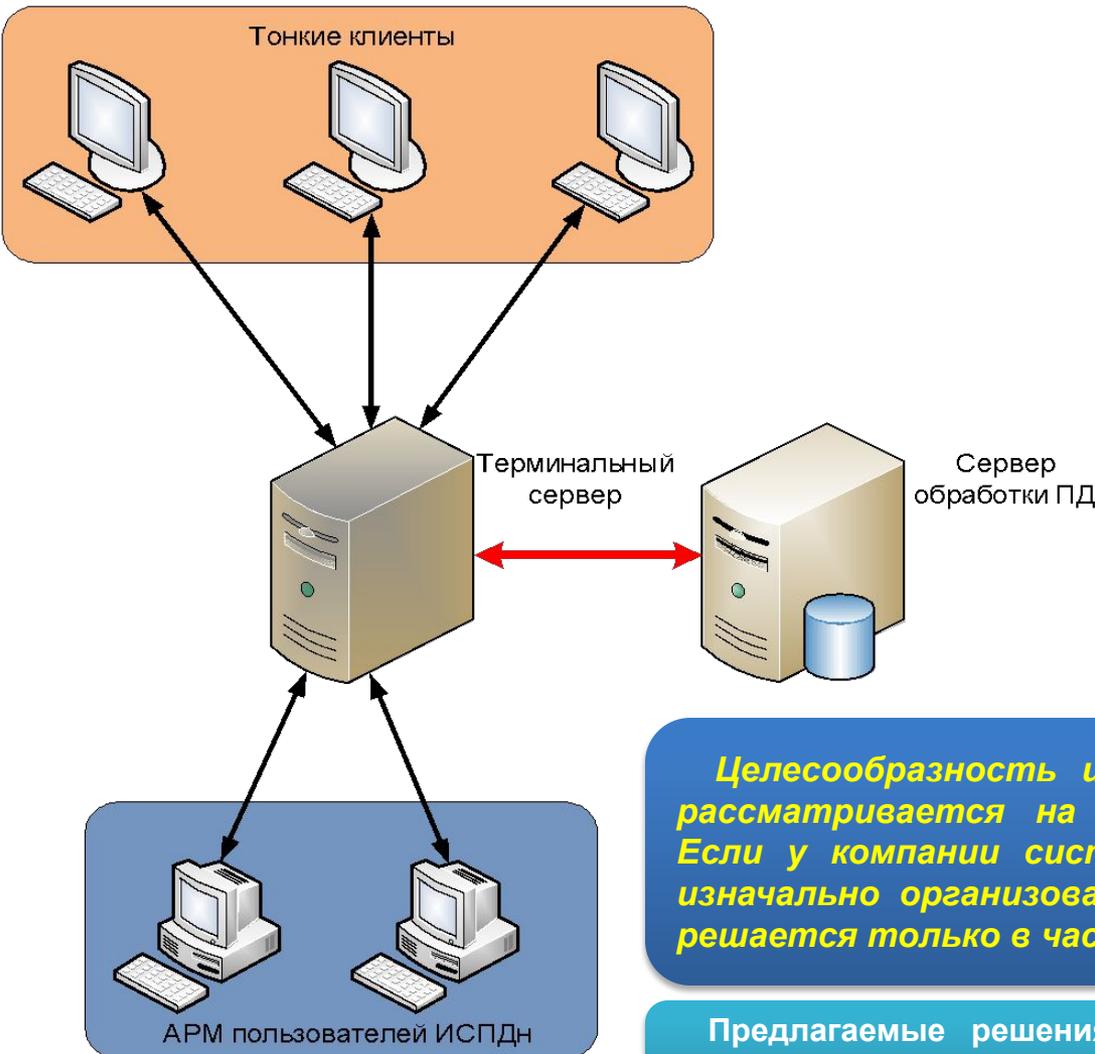
после преобразования



 - обработка ПДн

 - обмен информацией с помощью съемных носителей

Решения ЗАО «РАМЭК-ВС» на базе «тонкого клиента»



Преимуществами терминального решения являются:

- сокращение стоимости за счет использования централизованной архитектуры защиты и создания рабочих мест сотрудников при помощи терминальных клиентских устройств;
- простота развертывания по сравнению самой ИСПДн и средств ЗИ по сравнению с традиционной архитектурой клиент-сервер;
- масштабируемость архитектуры;
- простота подключения новых пользователей и их сопровождения;
- удобство администрирования и снижение операционных затрат за счет отсутствия необходимости локального развертывания ряда СРЗИ на терминалах ИСПДн.

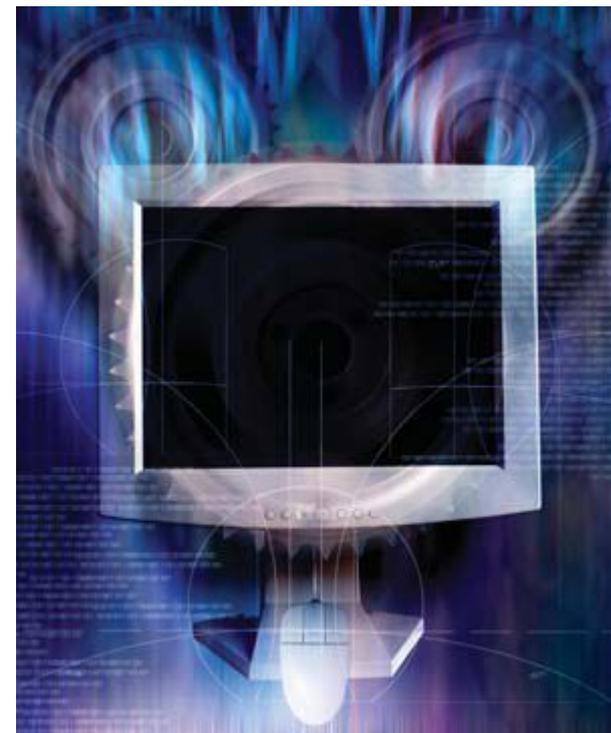
Целесообразность использования терминального доступа рассматривается на этапе предпроектного обследования. Если у компании система обработки персональных данных изначально организована с терминальным доступом, вопрос решается только в части создания защиты.

Предлагаемые решения при внедрении «мягко» адаптируются в существующие информационные системы и не требуют изменения бизнес-процессов пользователей автоматизированной системы.

На базе ПЭВМ RAMEC разработан АРМ, который предназначен для автоматизации процессов обработки конфиденциальной информации. В комплекс входит поставка аппаратной части, системы защиты от НСД, установка и настройка программной части информационной системы (по требованиям заказчика)



- Программная реализация Модуля доверенной загрузки не требует аппаратных средств, дополнительно устанавливаемых в ПЭВМ и проведения повторных СЛП.**
- Применение комплекса обеспечивает защиту многопользовательской АС с разными правами доступа по классу 1Г (обработка конфиденциальной информации).**
- Комплекс позволяет адаптироваться под обработку персональных данных любыми информационными системами, сертифицированными установленным порядком в ФСТЭК России.**



На аппаратной части комплекса проведен полный комплекс специальных работ, включающий лабораторные специальные проверки и исследования.

Что делать сейчас?

- **Закон не отменили!**
- Выполнение работ по защите требует не менее 6 – 8 месяцев!!!!
 - **Необходимо уже сейчас начинать приводить все ИСПДн в соответствие с требованиями ФЗ-152!**

Контакты (Санкт-Петербург)

Центральный офис

Адрес: 195220, Санкт-Петербург,
ул. Обручевых, д. 1

Тел.: (812) 740-38-38

Факс: (812) 327-83-18

[Задать вопрос](#)

Контакты (Москва)

Московское представительство

Адрес: 109316, Москва, Волгоградский пр. 2

Тел.: (495) 221-17-18

Факс: (495) 221-17-18

[Задать вопрос](#)

Директор департамента

ШИБКОВ СЕРГЕЙ ИЛЬИЧ

(495) 221-17-18 * доб. 642, моб. (925)729-9556

◆ Отдел проектирования и внедрения комплексных систем безопасности

◆ Начальник отдела Буянов Александр Иванович
(495) 221-17-18 * доб. 616, моб. (925)011-13-01

[Задать вопрос](#)

◆ Отдел НИОКР

◆ Начальник отдела Варакин Юрий Васильевич
(495) 221-17-18 * доб. 602, моб. (925)294-25-17

[Задать вопрос](#)

◆ Отдел аттестации объектов информатизации

◆ Начальник отдела Морозкин Андрей Борисович
(495) 221-17-18 * доб. 689, моб. (925)010-40-84

[Задать вопрос](#)

◆ Отдел специальной экспертизы

◆ Начальник отдела Букреев Игорь Алексеевич
(495) 221-17-18 * доб.606, моб. (925)010-40-85

[Задать вопрос](#)

◆ Испытательная лаборатория

◆ Главный специалист Остапенко Зоя Федоровна
(495) 221-17-18 * доб.608, моб. (926)106-86-34

[Задать вопрос](#)

СПАСИБО ЗА ВНИМАНИЕ