



Защита информации в Пенсионном фонде Российской Федерации

Управление по защите информации



Содержание презентации

- *Нормативно-правовая база защиты информации в ПФР*
- *Задачи, направления и основные мероприятия защиты*
- *Архитектура корпоративной сети ПФР*
- *Схема защиты корпоративной сети ПФР*
- *Информационное взаимодействие ПФР*
- *Иерархия органов защиты информации ПФР*
- *Структура подразделений по защите информации ПФР*



Федеральные законы

- **Об информации, информационных технологиях и о защите информации**
(от 27 июля 2006 года № 149-ФЗ)
- **О персональных данных**
(от 27 июля 2006 года № 152-ФЗ)
- **Об электронной цифровой подписи**
(от 10 января 2002 года № 1-ФЗ)
- **Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования**
(от 1 апреля 1996 года № 27-ФЗ)
- **О дополнительных страховых взносах на накопительную часть трудовой пенсии и государственной поддержке формирования пенсионных накоплений**
(от 30 апреля 2008 года № 56-ФЗ)
- **О страховых взносах в Пенсионный фонд Российской Федерации, ФСС Российской Федерации, Федеральный ФОМС и территориальные ФОМС**
(от 24.07.2009 №212-ФЗ)



Нормативные акты органов исполнительной власти

- **Положение об обеспечении безопасности персональных данных при их обработке в ИСПД**
(постановление Правительства Российской Федерации от 17 ноября 2007 года № 781)
- **Положения о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами**
(постановление Правительства Российской Федерации от 29 декабря 2007 года № 957)
- **Порядок проведения классификации ИСПД**
(приказ ФСТЭК, ФСБ и Мининформсвязи от 13 февраля 2008 года № 55/86/20)
- **Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)**
(приказ Гостехкомиссии России от 30 августа 2002 года № 282)
- **Положение о разработке, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (ПКЗ-2005)**
(приказ Директора ФСБ от 9 февраля 2005 года № 66)
- **Положение о методах и способах защиты информации в информационных системах персональных данных**
(приказ ФСТЭК России от 05 февраля 2010 г. № 58)
- **Методические рекомендации ФСБ России по защите ИСПД**
(№ 149/54-144 от 2008 года)



Нормативные акты ПФР

- *Концепция безопасности информации автоматизированной информационной системы ПФР*
- *Инструкция по организации защиты информации автоматизированной информационной системы ПФР*
- *Инструкция по организации криптографической защиты информации в Пенсионном фонде Российской Федерации*
- *Модель угроз безопасности персональных данных при их обработке в информационной системе ПФР*
- *Акт классификации информационной системы персональных данных ПФР*
- *Положение о порядке работы с документированной информацией конфиденциального характера в системе ПФР*
- *Перечень сведений ограниченного доступа, не составляющих государственной тайны*
- *Порядок формирования списков лиц, допущенных к сведениям о плательщиках страховых взносов и к персональным данным*



Задачи защиты информации

- ***Сохранение конфиденциальности данных***
- ***Сохранение целостности данных***
- ***Обеспечение аутентичности (легитимности) данных***
- ***Обеспечение доступности данных***



Направления защиты информации

- **Санкционирование доступа к ресурсам**
(конфиденциальность, целостность, доступность, аутентичность)
- **Криптографическая защита**
(конфиденциальность, аутентичность)
- **Защита от вредоносных программ**
(конфиденциальность, целостность, доступность)
- **Резервное копирование информационных ресурсов** (целостность, доступность)
- **Мониторинг состояния ресурсов**
(анализ эффективности защиты и разработка направлений её совершенствования)

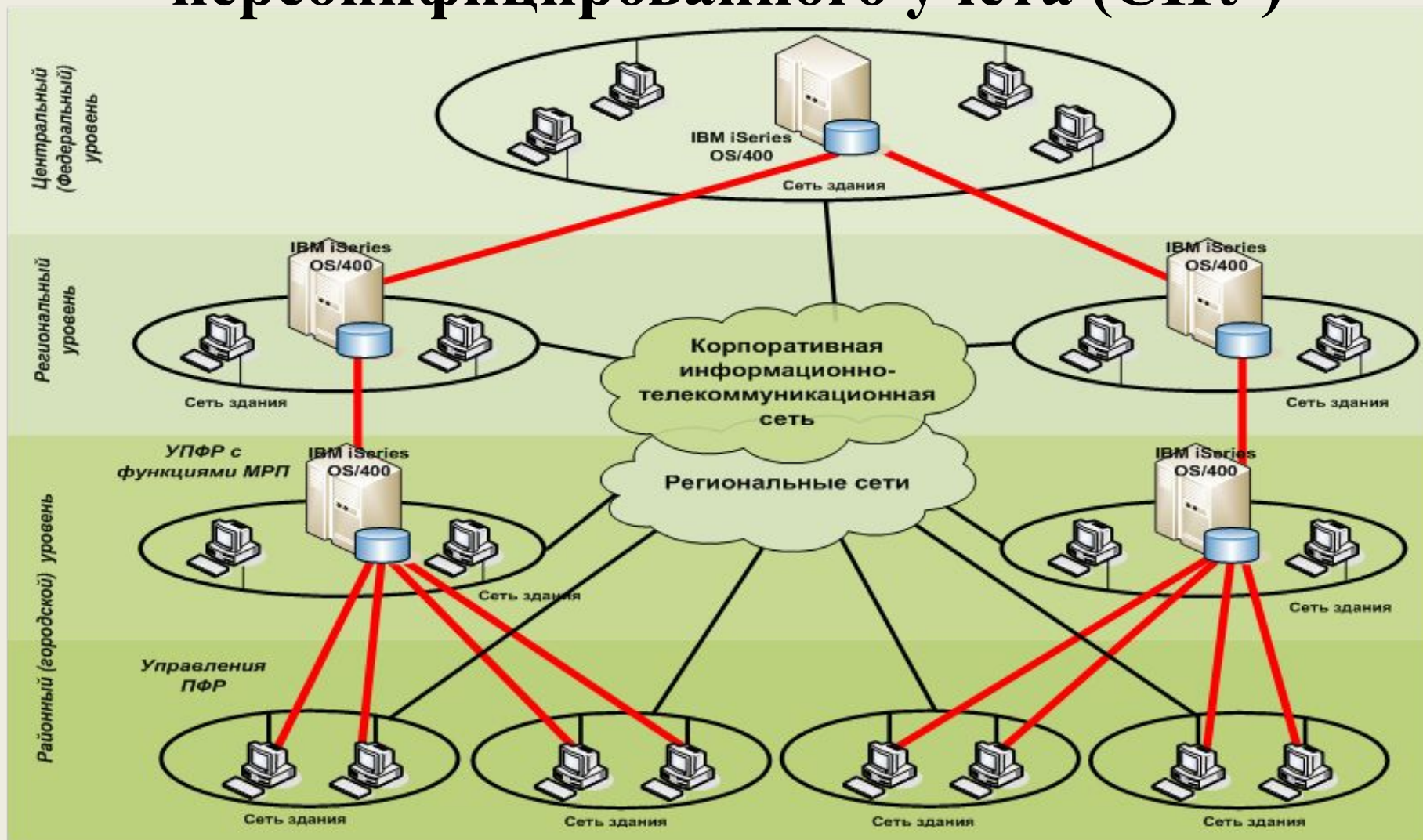


Санкционирование доступа к ресурсам

- **Допуск к работе с ресурсами** (перечень ресурсов; таблица допуска к ресурсам; списки лиц, допущенных к ПДн и сведениям о ПСВ)
- **Санкция на вход в систему** (пароль, загрузка только с НМЖД, минимизация прав пользователя, опечатывание системного блока, доверенная загрузка)
- **Санкция на доступ к сетевым ресурсам** (пароль, сертификат)
- **Безопасное хранение аутентифицирующих данных** (электронные ключи)
- **Блокирование портов ввода-вывода** (программное или механическое)



Архитектура Системы персонифицированного учёта (СПУ)



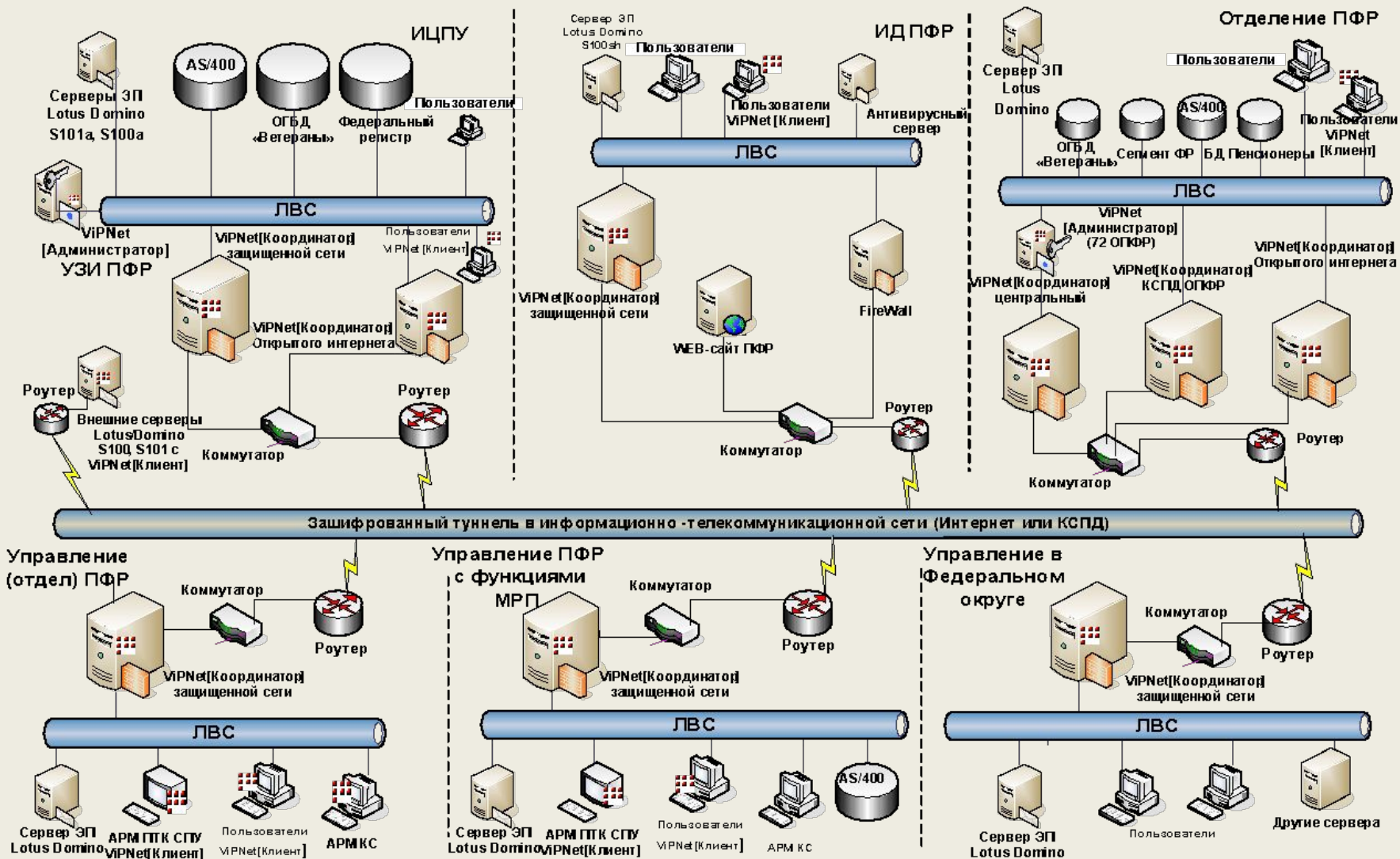


Криптографическая защита

- **Шифрование информации, передаваемой по информационно-телекоммуникационным сетям (ViPNet; Вербa):**
 - абонентское шифрование;
 - канальное шифрование;
 - центр управления ViPNet-сетью.
- **Шифрование хранимой информации (Safe Disk, Secret Disk);**
- **Применение электронной цифровой подписи (применение Домен-К, Вербa-OW; понимание Крипто-Про,):**
 - Удостоверяющий центр ПФР (ViPNet, Вербa);
 - регистрационные центры в отделениях ПФР;
 - доверенные Удостоверяющие центры (ИнфоТекС Интернет Трaст, МО ПНИЭИ, ТУСУР);

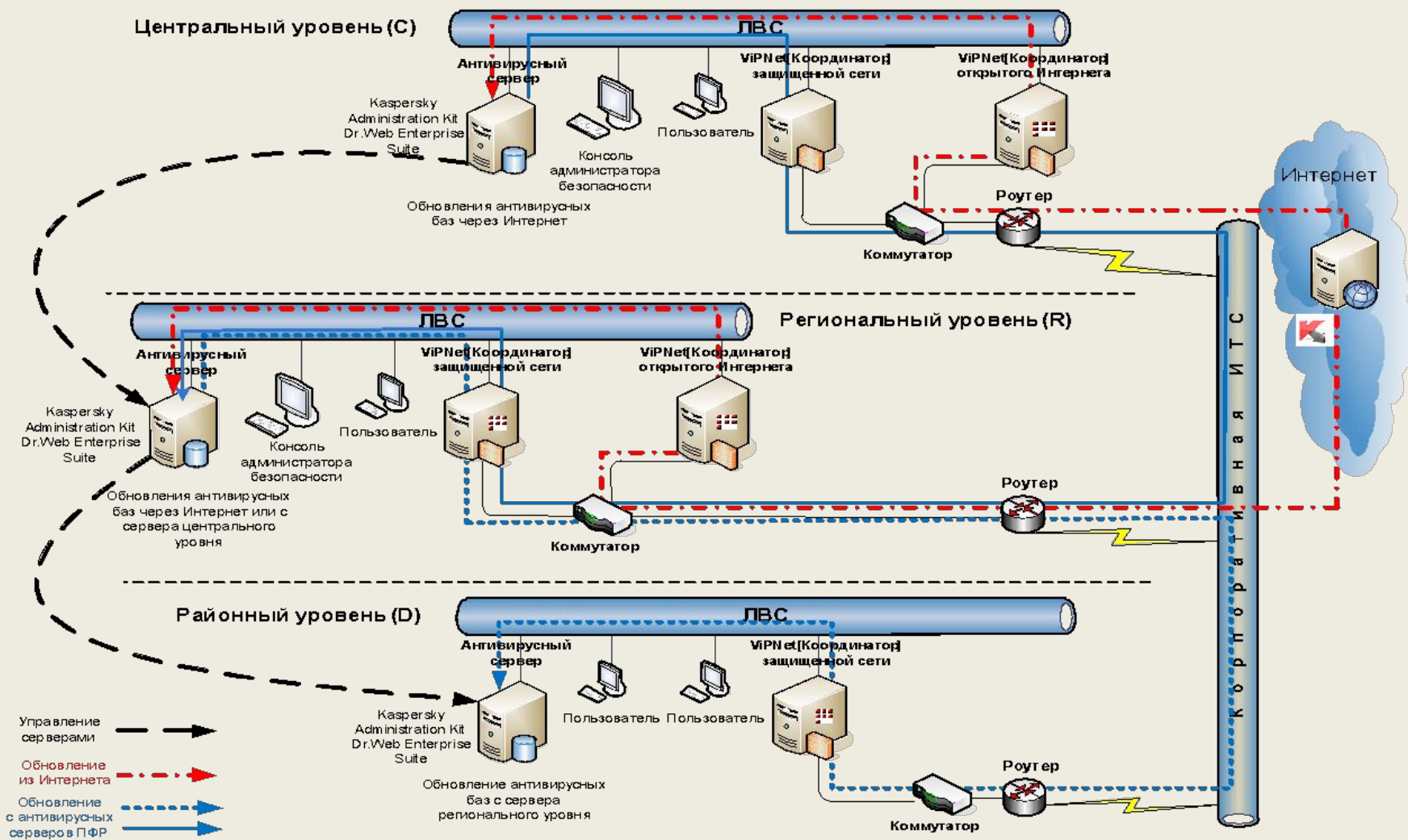


Общая схема защиты корпоративной ИТС ПФР





Защита от вредоносных программ





Резервное копирование информационных ресурсов

- **Копирование на съёмные носители** (различная периодичность, учёт процедур копирования, комплект носителей; раздельное хранение копий, назначение ответственных, их дублёров);
- **Дублирование ресурсов на уровне вычислительных средств** (рассредоточение мест положения средств);
- **Дублирование на уровне функциональных систем** (СПУ на базе серверов iSeries дублируется на уровне отделений системой на базе Intel-серверов);
- **Процедура восстановления ресурса из резервной КОПИИ** (коллегиальность, документальное оформление)

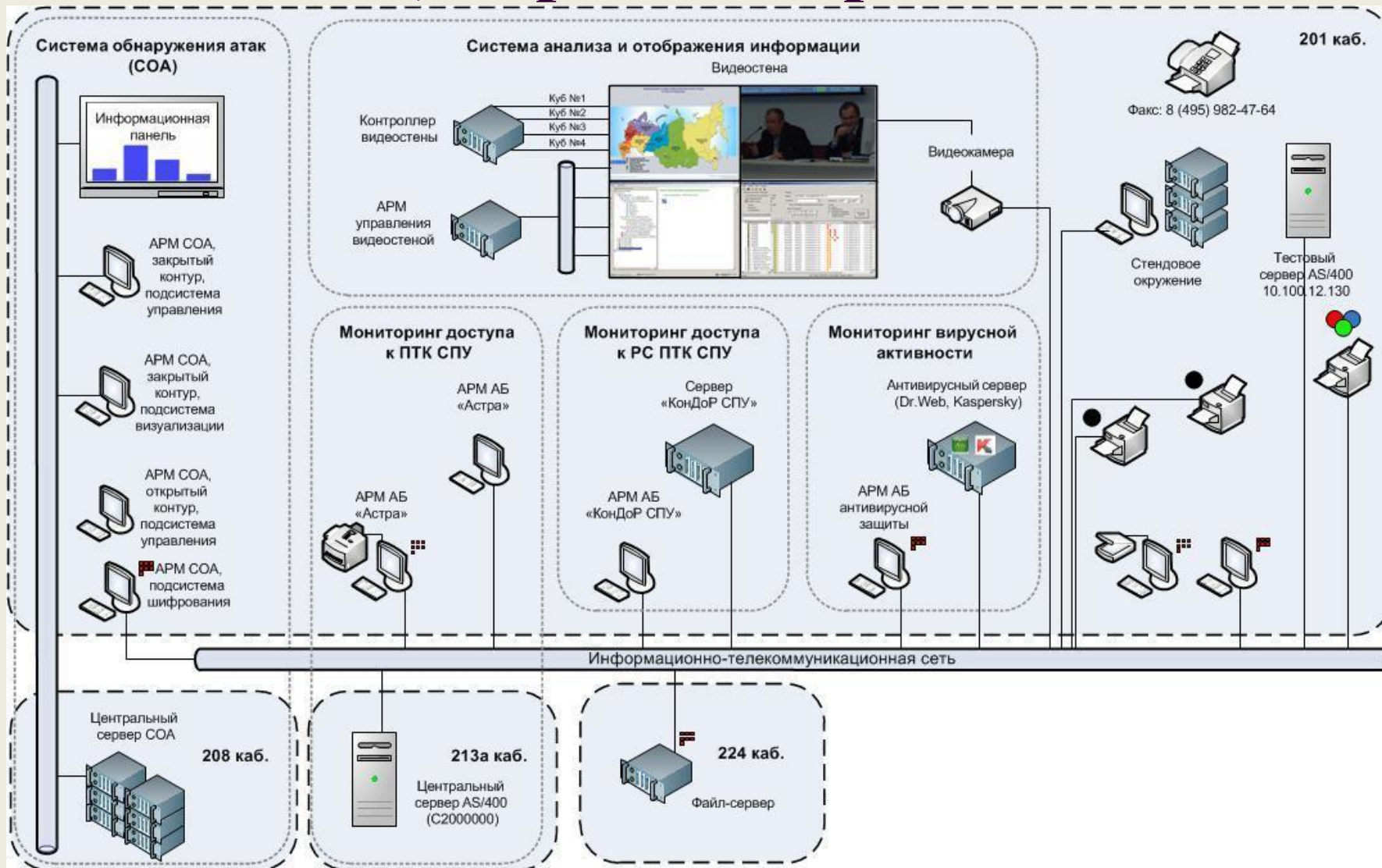


Мониторинг состояния информационных ресурсов

- **Система персонифицированного учёта – комплекс «Астра»**
- **Резервная система персонифицированного учёта – комплекс «КонДоР СПУ»**
- **Антивирусная защита – центр управления средствами «Лаборатории Касперского» и центр управления средствами «Доктор Веб»**
- **Система обнаружения компьютерных атак – специальная система в составе центра анализа и сенсоров в отделениях**



Центр мониторинга





Основные мероприятия защиты

Организационные

- *Разработка системы нормативных документов*
- *Определение перечня защищаемых ресурсов*
- *Ограничение доступа к ресурсам*
- *Персональная ответственность сотрудников за безопасность обрабатываемых данных*
- *Профессиональная подготовка специалистов по защите*
- *Создание контролируемой зоны и организация пропускного режима*
- *Определение порядка информационного взаимодействия*

Технические

- *Разграничение прав доступа к ресурсам*
- *Оборудование зданий и помещений системами безопасности*
- *Применение корпоративной информационно-телекоммуникационной сети*
- *Защита от вредоносных программ*
- *Шифрование (криптозащита) данных*
- *Применение ЭЦП*
- *Автоматизированный мониторинг состояния ресурсов*

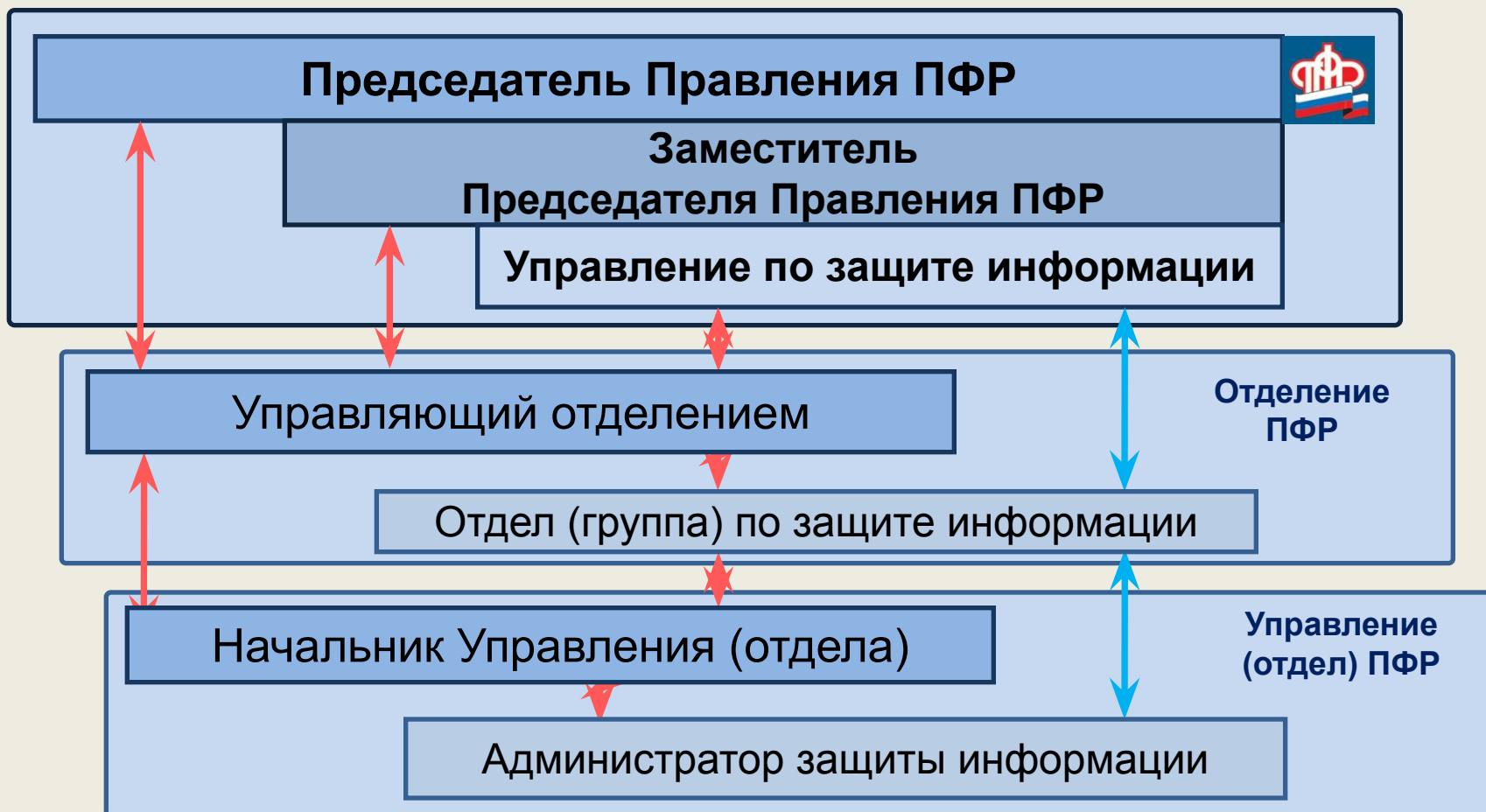


Информационное взаимодействие ПФР





Организационная иерархия защиты информации в ПФР





Концепция безопасности информации АИС ПФР

*Утверждена постановлением Правления ПФР от 26 июля 2008 года
№ 1п ДСП*

Концепция определяет:

- цель и стратегию достижения требуемого уровня безопасности информации АИС ПФР;*
- основные направления достижения безопасности информации;*
- принципы реализации и функционирования системы защиты информации;*
- объекты защиты;*
- меры по обеспечению безопасности информации.*



Инструкция по организации защиты информации АИС ПФР

Утверждена постановлением Правления ПФР от 26 июля 2008 года № 1п ДСП)

Инструкция определяет:

- цели и задачи, объекты, мероприятия и методы защиты информации;*
- порядок руководства защитой и органы защиты информации;*
- задачи подразделений ИД ПФР и отделений ПФР, обязанности должностных лиц по организации защиты информации;*
- основные обязанности пользователя;*
- классификацию ресурсов и особенности их защиты;*
- задачи и мероприятия и средства защиты от НСД;*
- организацию защиты от вредоносных программ;*
- порядок авторизации пользователей;*
- порядок применения машинных носителей информации;*
- порядок копирования информационных ресурсов;*
- требования к прикладным программным продуктам;*
- формы документов.*



Инструкция по организации криптозащиты в ПФР

Утверждена постановлением Правления ПФР от 16 октября 2008 года № 2п ДСП

Определяет:

- организацию и обеспечение безопасности обработки информации с использованием криптосредств;*
- порядок обращения с криптосредствами и криптоключами к ним;*
- мероприятия при компрометации криптоключей;*
- порядок обеспечения безопасности информации с использованием криптосредств при взаимодействии со сторонними организациями и передаче по каналам связи;*
- размещение, оборудование, охрана и организация режима специальных помещений;*
- формы документов.*



Модель угроз безопасности ПДн при их обработке в АИС ПФР

Утверждена Председателем Правления ПФР

Согласована с ФСТЭК России

Определяет для персональных данных:

- *перечень угроз безопасности;*
- *возможные последствия нарушения безопасности;*
- *объекты угроз (основные ресурсы, содержащие ПДн, перечень информации способствующей доступу к ПДн);*
- *основные формы реализации угроз каждой из характеристик безопасности ПДн в АИС ПФР;*
- *модель нарушителя безопасности;*
- *перечень актуальных угроз безопасности.*