ЭЛВИС-ПЛЮС

Комплексные решения вопросов обеспечения безопасности информации для государственных информационных систем (на примере построения СОБИ АИС «НАЛОГ-3»)

Мухортов Юрий Валерьевич

Директор департамента специальных проектов
ОАО «ЭЛВИС-ПЛЮС»

«Infosecurity Russia 2013»
26 сентября 2013 г.

ЭЛВИС-ПЛЮС

Характеристика информационной системы

- Многоуровневая:

Федеральный уровень (решения по организации работы, создание нормативных документов, ведомственных стандартов, взаимодействие между управлениями, министерствами, ведомствами….)

Региональный уровень (контроль и координация местных инспекций, подготовка агрегированных отчетов…)

Местный уровень (основная нагрузка по контролю исполнения налогового законодательства);

- Многопользовательская (более 120 тысяч рабочих мест);
- Территориально распределенная (центр, 82 тер.управления, налоговые инспекции и входящие в их состав территориально-обособленные рабочие места ТОРМ);
- Обеспечивающая информационное взаимодействие как по вертикали, так и по горизонтали (между структурными подразделениями в пределах одного налогового органа; между налоговыми органами ФНС России; между налоговым органом и другими организациями и ведомствами, в т.ч. алогоплательщиков)

ЭЛВИС-ПЛЮС

Недостатки децентрализованной архитектуры АИС (с точки зрения реализации мер ОБИ)

Основной недостаток:

Наличие большого количества ИС, входящих в АИС «Налог». Что, в свою очередь, порождает:

- множественность и фрагментарность распределённых по отдельным ИС информационных ресурсов (БД с информацией, подлежащей защите);

И как следствие:

- радикально увеличивается возможность реализации угроз, связанных с осуществлением несанкционированного доступа (НСД) к информации;
- значительно увеличивается вероятность нанесения ущерба субъектам налогообложения, налоговым органам разного уровня и ФНС России в целом.

Косвенные недостатки:

- Необходимость внедрения большего количества технических средств защиты информации (ТСЗИ) на каждом из объектов ФНС России;
- Необходимость содержания большого штата сотрудников, обеспечивающих БИ на местах для поддержки ТСЗИ;
- Отсутствие возможности сбора событий ИБ, мониторинга показателей БИ в масштабе ФНС России.
- Трудности в реализации единых политик БИ;
- Сложность процедур предоставления доступа и управления доступом к распределённым ИР АИС «Налог» как организационно, так и технически;

ЭЛВИС-ПЛЮС

Цели и задачи построения СОБИ АИС «Налог-3»

✓ Цель:

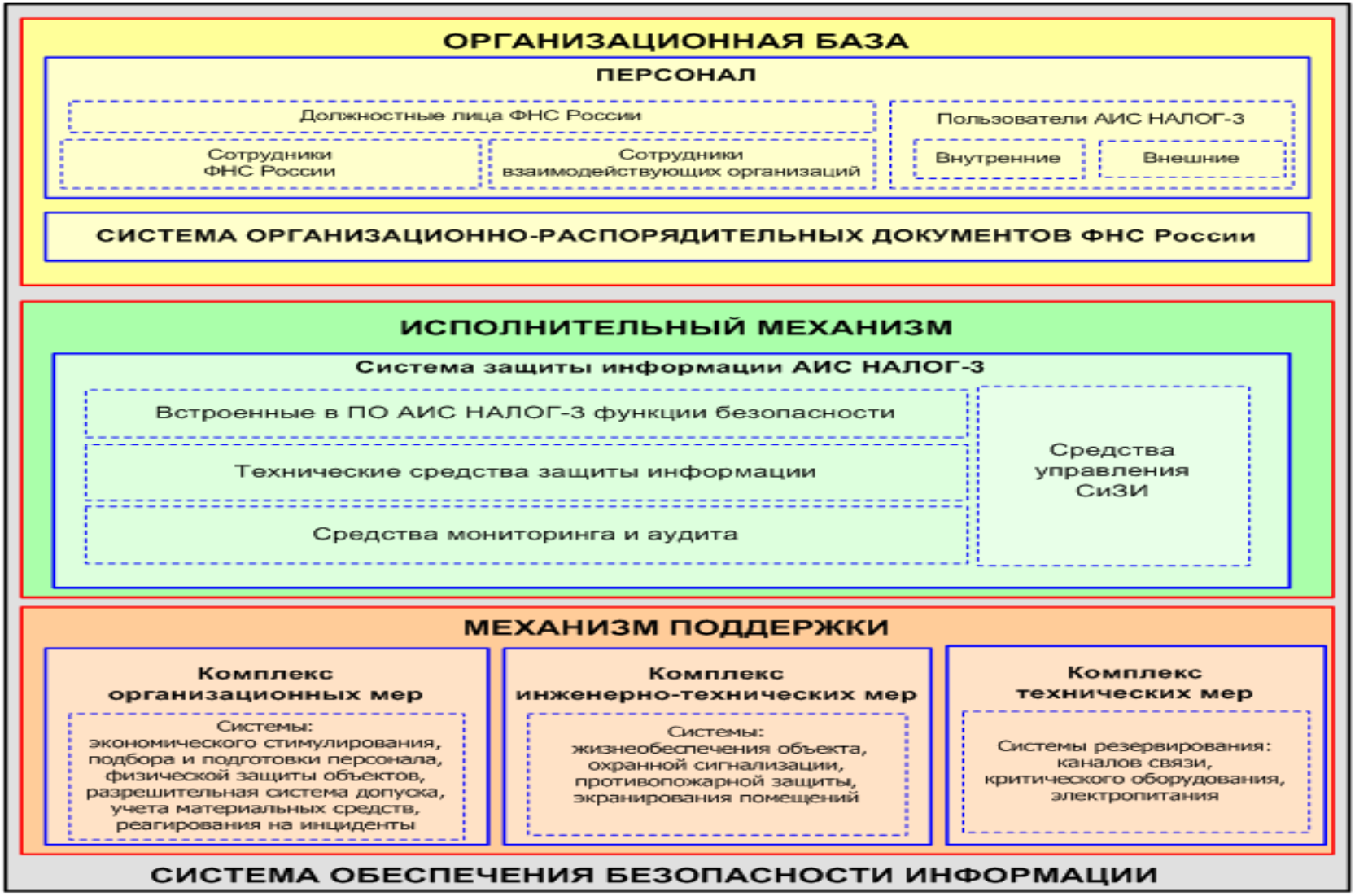
Формирование единой организационно-технической политики обеспечения безопасности информации АИС «Налог-3», достижения требуемого уровня защищенности информационных ресурсов Системы и оперативного реагирования на возникающие угрозы безопасности информации, а также негативные тенденции роста таких угроз.

✓ Задачи:

- Обеспечение соответствия объектов АИС «Налог-3» нормативным требованиям регуляторов (ФСБ, ФСТЭК);
- Учет всех субъектов и всех объектов защиты;
- Контроль всех действий с объектами защиты;
- Обеспечение заданного уровня доверенности среды функционирования АИС;
- Сохранение защитных функций при масштабировании АИС «Налог-3»;
- Обеспечение контроля эффективности принимаемых мер защиты;
- Обеспечение резервирования функций защиты на наиболее критичных участках и др.

ЭЛВИС-ПЛЮС

Общая архитектура СОБИ (на примере ФНС России)



ЭЛВИС-ПЛЮС

Общие требования к разрабатываемой СОБИ

- Архитектура СОБИ должна предусматривать единые технические решения в масштабе ФНС России.
- СОБИ АИС «Налог-3» должна быть структурирована по функциональным подсистемам.
- Архитектура СОБИ в совокупности с механизмом поддержки функциональных подсистем не должна накладывать каких-либо существенных ограничений на ИТ, используемые в АИС «Налог-3».
- Архитектура СОБИ должна обеспечивать реализацию функций безопасности на всех технологических этапах эксплуатации АИС «Налог-3», в том числе при проведении технического обслуживания и ремонта.
- Эффективность СОБИ должна достигаться применением комплекса защитных механизмов.

«По-настоящему безопасной можно считать лишь такую систему, которая выключена, замурована в бетонный бункер, заперта в помещении со свинцовыми стенами и охраняется вооруженным караулом, - но и в этом случае сомнения не покидают меня».

Dr. Eugene Spafford
Director of the Center for Education and Research in Information Assurance and Security (CERIAS)

ЭЛВИС-ПЛЮС

СТРУКТУРА ВЫПОЛНЕНИЯ РАБОТ

на основе «лучших практик» создания систем обеспечения ИБ

- Анализ нормативной базы. Классификация информационных ресурсов АИС Налог-3
- Разработка модели угроз и модели нарушителя. Разработка функционально-технических требований к СОБИ
- Разработка концепции СОБИ. Разработка ТЗ на создание СОБИ. Разработка ЧТЗ на подсистемы СОБИ и схемы их интеграции.
- Разработка общесистемных проектных решений по функциональным подсистемам СОБИ и их макетирование в рамках пилотных проектов.
- Разработка типовых проектных решений (ТПР) по подсистемам СОБИ по типам объектов. Разработка методик привязки ТПР к объектам.
- Разработка техно-рабочих проектов на подсистемы СОБИ. Проведение СМР и ПНР. Проведение ПСИ. Аттестация объектов защиты.

Разработка и внедрение прикладных компонент АИС Налог-3

Проектирование и создание инфраструктуры АИС Налог-3

Разработка комплекса организационно-распорядительной и нормативно-методической документации по АИС Налог-3

ЭЛВИС-ПЛЮС

ПРАВОВАЯ ОСНОВА СОБИ АИС НАЛОГ-3

структура требований нормативных документов регуляторов в области ИБ

Анализ нормативной базы. Классификация информационных ресурсов АИС Налог-3	Разработка модели угроз и модели нарушителя. Разработка функционально-технических требований к СОБИ	Разработка концепции СОБИ. Разработка ТЗ на создание СОБИ. Разработка ЧТЗ на подсистемы СОБИ и схемы их интеграции.	Разработка общесистемных проектных решений по функциональным подсистемам СОБИ и макетирование в рамках пилотных проектов.	Разработка типовых проектных решений (ТПР) по подсистемам СОБИ по типам объектов. Разработка МУ по привязке ТПР к объектам.	Разработка техно-рабочих проектов на подсистемы СОБИ. Проведение СМР и ПНР. Проведение ПСИ. Аттестация объектов защиты.

- Положения Конституции Российской Федерации, Кодексов Российской Федерации, Федеральных законов, указов Президента Российской Федерации, постановлений и распоряжений Правительства Российской Федерации;
- Нормативные документы ФСТЭК России и ФСБ России по вопросам защиты информации и обеспечения её безопасности;
- «Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года», распоряжение Правительства РФ от 27.09.04 г. №1244-р.

ЭЛВИС-ПЛЮС

ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

на основании анализа угроз безопасности информации АИС Налог-3

Анализ нормативной базы. Классификация информационных ресурсов АИС	Разработка модели угроз и модели нарушителя. Разработка функционально-технических требований к СОБИ	Разработка концепции СОБИ. Разработка ТЗ на создание СОБИ. Разработка ЧТЗ на подсистемы СОБИ и схемы их интеграции.	Разработка общесистемных проектных решений по функциональным подсистемам СОБИ и макетирование в рамках пилотных проектов.	Разработка типовых проектных решений (ТПР) по подсистемам СОБИ по типам объектов. Разработка МУ по привязке ТПР к объектам.	Разработка техно-рабочих проектов на подсистемы СОБИ. Проведение СМР и ПНР. Проведение ПСИ. Аттестация объектов защиты.

- Криминальные элементы, террористы;
- Компьютерные злоумышленники;
- подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования АИС и его ремонт;
- Сотрудники ФНС России, являющиеся легальными участниками процессов в АИС и действующие вне рамок предоставленных полномочий;
- ***Сотрудники (группы сотрудников) ФНС России, являющиеся легальными участниками процессов в АИС и действующие в рамках предоставленных полномочий, но в личных интересах.***

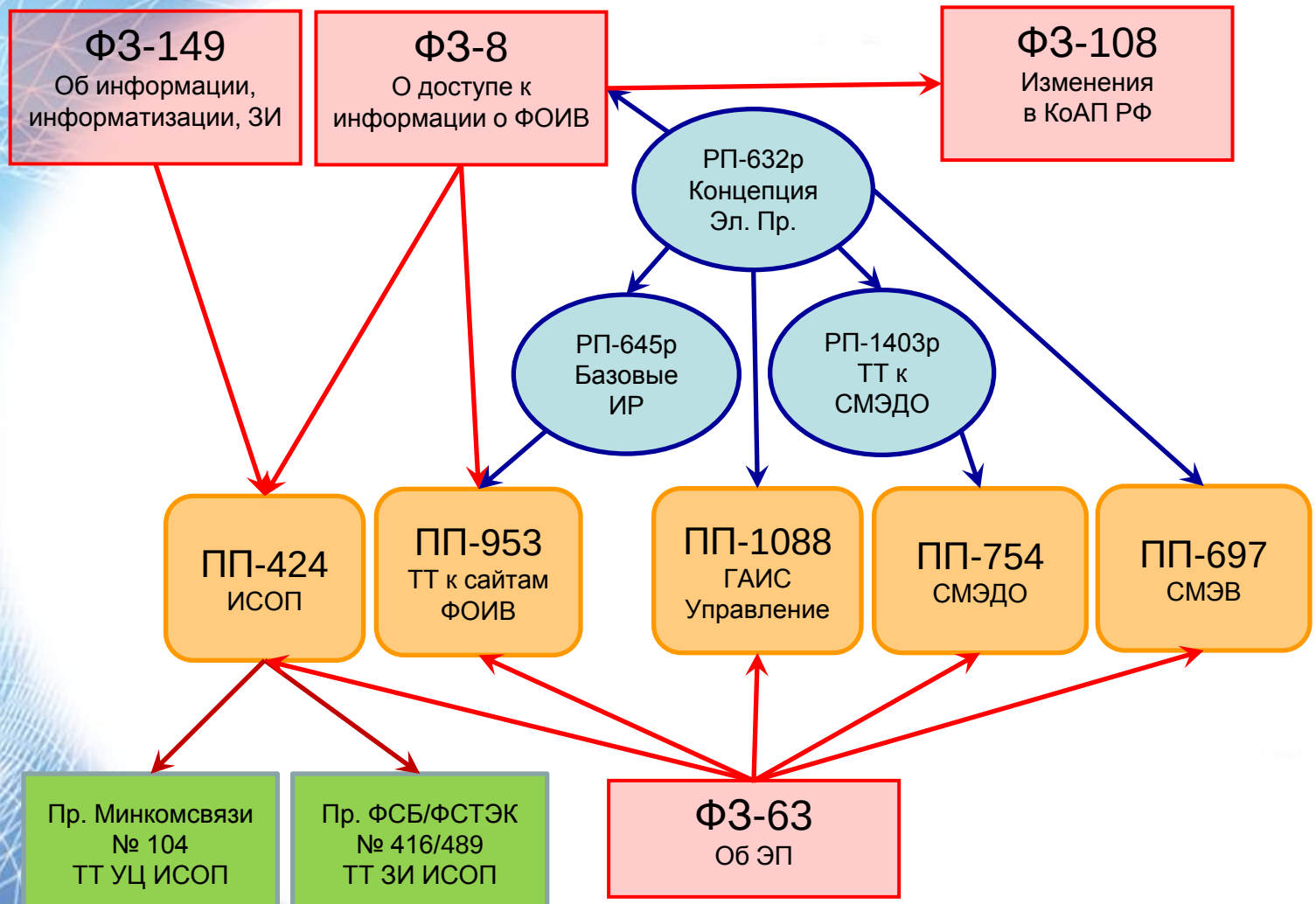
Условия модернизации действующей АИС

В 2007 – 2011 годы законодательство РФ в области информационной безопасности усиленно совершенствовалось.

- «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» № 8-ФЗ, 2009 г.
- «Об электронной подписи», № 63-ФЗ, 2011 г.
- «О персональных данных», № 152-ФЗ, 2006 г. (в ред. ФЗ № 261-ФЗ, 2011 г.)

ЭЛВИС-ПЛЮС

Структура нормативной базы при создании электронного правительства



ЭЛВИС-ПЛЮС

СОСТАВ ПОДСИСТЕМ СОБИ

на основе анализа функциональных требований и механизмов защиты СЗИ

Разработка концепции СОБИ. Разработка ТЗ на создание СОБИ. Разработка ЧТЗ на подсистемы СОБИ и схемы их интеграции.

ЭЛВИС-ПЛЮС

СОСТАВ ТЕХНОЛОГИЧЕСКИХ КОМПОНЕНТ

на примере Подсистемы управления доступом

Разработка концепции СОБИ. Разработка ТЗ на создание СОБИ. Разработка ЧТЗ на подсистемы СОБИ и схемы их интеграции.

ЭЛВИС-ПЛЮС

СтратегиЯ построения СОБИ, технологический процесс реализации СОБИ

ПЛАНЫ ИСПОЛНЕНИЯ РАБОТ

2010	2011	2012-2013

ЭЛВИС-ПЛЮС

Спасибо за внимание !

124498, МОСКВА, Зеленоград,
Центральный проспект, 11
тел. 495-777-42-90,
Факс 499-731-24-03
e-mail: info@elvis.ru
http://www.elvis.ru