ЭЛВИС-ПЛЮС

Архитектура системы защиты персональных данных. Подсистема межсетевого экранирования

Ростислав Рыжков
ОАО «ЭЛВИС-ПЛЮС»

2010 год

ЭЛВИС-ПЛЮС

ВОПРОСЫ ПРЕЗЕНТАЦИИ

- Регуляторы о системе защиты персональных данных.
- Требования к средствам ИБ, применяемых в подсистемах
- Примеры решений
- Подсистема межсетевого экранирования, ее специфика и место в СЗПДн
- Как традиционно выглядит подсистема МЭ, и почему
- Проблемы ПМЭ для малых и больших ИС
- Управление ПМЭ, инфраструктура и обеспечивающие сервисы.
- Практика решений.

Презентация нацелена на операторов персональных данных, в том числе и не имеющих достаточного опыта в вопросах информационной безопасности

ЭЛВИС-ПЛЮС

Регуляторы о системе защиты персональных данных

Подсистемы СЗПДн

Предусмотрены однопользовательский и многопользовательский режимы обработки данных в ИСПДн, во втором случае – с равными либо разными правами доступа

ПОДСИСТЕМЫ:

- Подсистема управления доступом
- Подсистема регистрации и учета
- Подсистема обеспечения целостности
- Подсистема антивирусной защиты
- Подсистема обнаружения вторжений
- Подсистема криптографической защиты
- Подсистема защиты ПДн от утечки за счет ПЭМИН

Требования регуляторов ясно определяют состав ИСПДн и требования к ее подсистемам

ЭЛВИС-ПЛЮС

Требования к средствам ИБ, применяемых в подсистемах, и примеры решений

Рекомендации регуляторов по архитектуре СЗПДн. Подсистемы СЗПДн

Подсистемы	Требования
Регистрации и учета	Регистрация запросов на получение ПДн и их предоставления в электронном журнале, защита данных регистрации
Обеспечения целостности	Резервное копирование ПДн на отчуждаемые носители в ИСПДн К1 иК2, с разными правами пользователей
Антивирусной защиты	Антивирусное ПО должно быть сертифицировано по требованиям соответствующего уровня контроля НДВ, а также на соответствие ТУ с требованиями не ниже соответствующего класса ИСПДн
Обнаружения вторжений	Мероприятия по обнаружению вторжений в ИСПДн в соответствии с требованиями НД ФСБ. Для ИСПДн 3 класса рекомендуются СОВ, использующие сигнатурные методы, для ИСПДН 1 и 2 класса – СОВ, использующие также методы выявления аномалий.

ЭЛВИС-ПЛЮС

Требования к средствам ИБ, применяемых в подсистемах, и примеры решений

Рекомендации регуляторов по архитектуре СЗПДн. Подсистемы СЗПДн

Подсистемы	Требования
Защиты ПДн от утечки за счет ПЭМИН	К2- в соответствии стандартам по ЭМС и санитарным нормам, К1- по СТР-К
Криптографической защиты	Шифрование ПДн в каналах связи и на съёмных носителях, в ИСПДн К1, с равными и разными правами пользователей
Управления доступом	Межсетевые экраны от 5 до 3 класса

Далее - о двух последних подсистемах

ЭЛВИС-ПЛЮС

Подсистема криптографической защиты

Когда использовать криптографию?

в криптографической подсистеме……. должны использоваться сертифицированные средства криптографической защиты

- **В системах, где АРМ или ЛВС объединены средствами связи. Необходимость криптографической защиты возникает при передаче информации в среду, в которой она может оказаться доступной нарушителю (незащищенные от НСД средства хранения информации, каналы связи)**
- **В системах, в которых в соответствии с моделью угроз возможно наличие инсайдера, а безопасность хранения и обработки не может быть гарантированно обеспечена другими средствами**
  - **Шифрование файлов и папок не проблема – имеется много инструментов**
  - **Шифрование баз данных – также решаемо.**

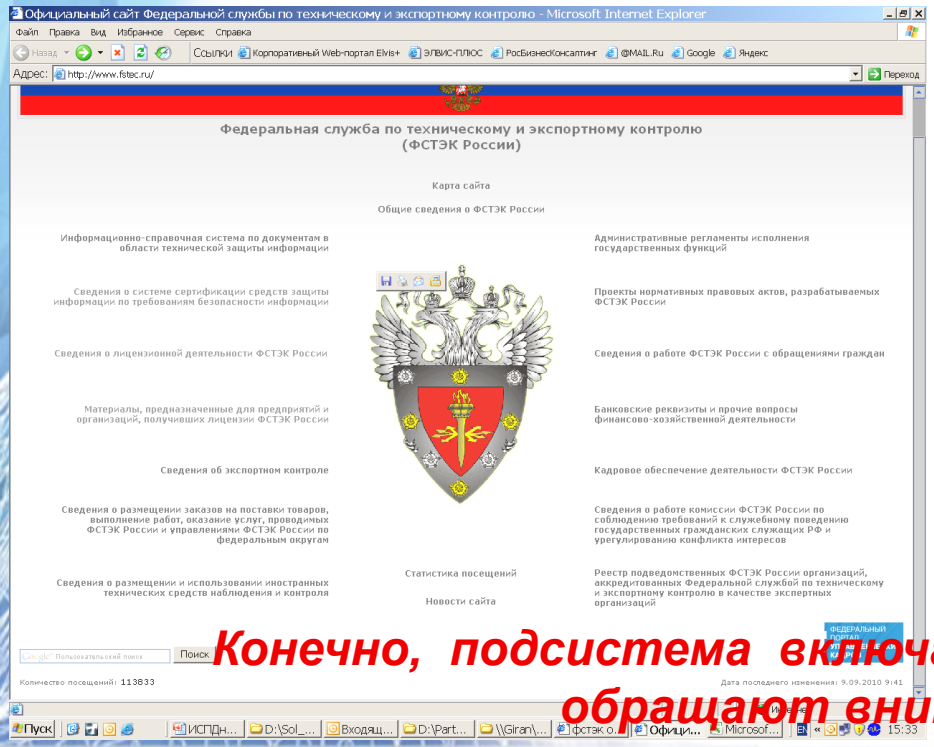
Решение о необходимости защиты ПДн с использованием криптографических средств принимается оператором

ЭЛВИС-ПЛЮС

Подсистема управления доступом

Межсетевые экраны

В зависимости от класса ИСПДн (1- 4 классы) и режима обработки данных (однопользовательский, многопользовательский) должны использоваться межсетевые экраны, сертифицированные ФСТЭК по классам от 5 до 3 (для межсетевых экранов)



Пример текста в сертификате:

«…по 3 классу для МЭ и по 3 уровню НДВ (может использоваться для защиты информации в ИСПДн до 1 класса включительно)»

ПОДРОБНОСТИ

http://www.fstec.ru/_doc/reestr_sszi/_reestr_sszi.xls

Конечно, подсистема включает не только МЭ, но регуляторы обращают внимание именно на них

ЭЛВИС-ПЛЮС

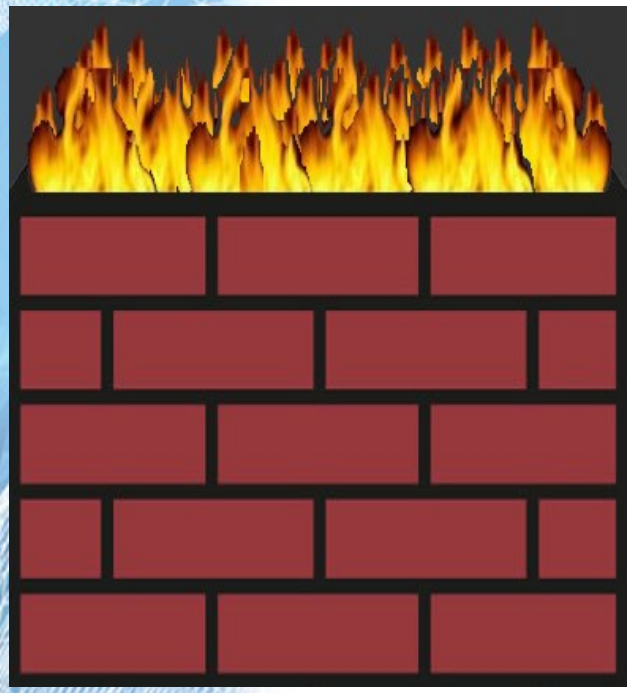
Fire wall, он же – Брандмауэр 200 лет назад

Сегодня так называют межсетевой экран

БРАНДМАУЭР Стена из несгораемого материала, разделяющая смежные строения или части одного строения в противопожарных целях

ЭЛВИС-ПЛЮС

Традиционные средства межсетевого экранирования



Firewalls D-Link

Cisco Secure Private Internet Exchange (PIX) Firewall

CheckPoint Connectra

Даже если снаружи все горит – у нас покой и порядок.
В чем же проблема?

ЭЛВИС-ПЛЮС

Требования регуляторов к межсетевым экранам
и другим средствам защиты

«Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия»

Постановление Правительства РФ от 17.11.2007 г. № 781, п.5

Прямой нормы, определяющей понятие «оценка соответствия» применительно к средствам защиты ПДн– нет, это порождает много вопросов, связанных с порядком такой оценки.

Для разрешения проблемы юристы предлагают проверенный метод – применить аналогию закона (ст. 6 ГК РФ)

Наличие сертификата - как будто и не обязательно

ЭЛВИС-ПЛЮС

Требования регуляторов к межсетевым экранам
и другим средствам защиты

Для защиты персональных данных возможно применение не сертифицированных СЗИ, оценка соответствия которых осуществлена в форме декларирования соответствия.

Порядок оценки соответствия устанавливается на основании стандартов (например, ГОСТ 34.601-90), устанавливающих порядок ввода в эксплуатацию ИС, а саму оценку необходимо проводить на соответствие выполняемых средством защиты функций, предусмотренных «Положением о методах и способах защиты информации в информационных системах персональных данных».

Завершить работы по оценке надо проведением экспертизы результатов во ФСТЭК или ФСБ России

НО!

Наличие сертификата позволяет избежать экспертизы результатов оценки соответствия во ФСТЭК или ФСБ России

ЭЛВИС-ПЛЮС

Межсетевые экраны для малых информационных систем

Чего хотят владельцы малых ИСПДн?

Функции

- управление доступом (фильтрация и преобразование фильтруемой информации) на сетевом уровне
- идентификация и аутентификация хостов и пользователей
- регистрация и учет
- администрирование

Дополнительные требования

- Простота установки и администрирования
- невысокая стоимость
- соответствие требованиям регуляторов

Недорогие межсетевые экраны – от 7000 рублей? Вспомним про экспертизу результатов оценки соответствия во ФСТЭК или ФСБ России

Если уж применение межсетевых экранов в ИСПДн обязательно, хотелось бы иметь необходимую функциональность и минимум хлопот.

ЭЛВИС-ПЛЮС

Межсетевое экранирование в крупных информационных системах

Что необходимо в крупных ИСПДН?

Требования

- Соответствие требованиям регуляторов
- Эффективное, желательно централизованное, обновление ПО МЭ
- Простое, желательно централизованное администрирование
- Совместная работа с МЭ разных производителей
- Строгая аутентификация агентов
- Взаимодействие с агентами по защищенному каналу
- Протоколирование и анализ состояния агентов и событий сети

Проблемы

- Наличие значительного числа квалифицированных администраторов
- Большие трудозатраты специалистов на обслуживание МЭ
- Содержательные журналы событий сетевой безопасности и средства их анализа

Серьезная проблема крупных ИСПДн – администрирование сотен и тысяч межсетевых экранов

ЭЛВИС-ПЛЮС

Организация работы межсетевых экранов

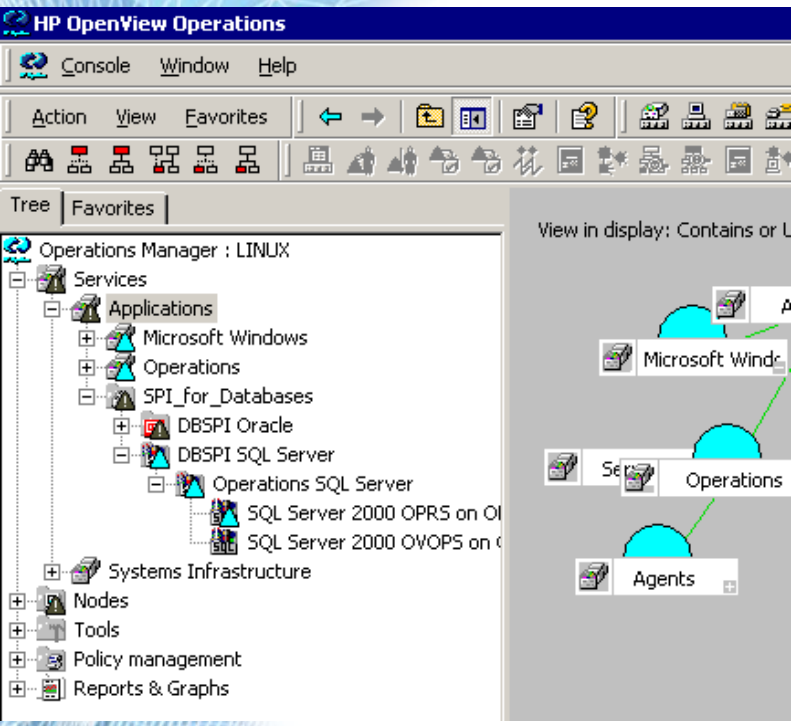
Инфраструктура и обеспечивающие сервисы

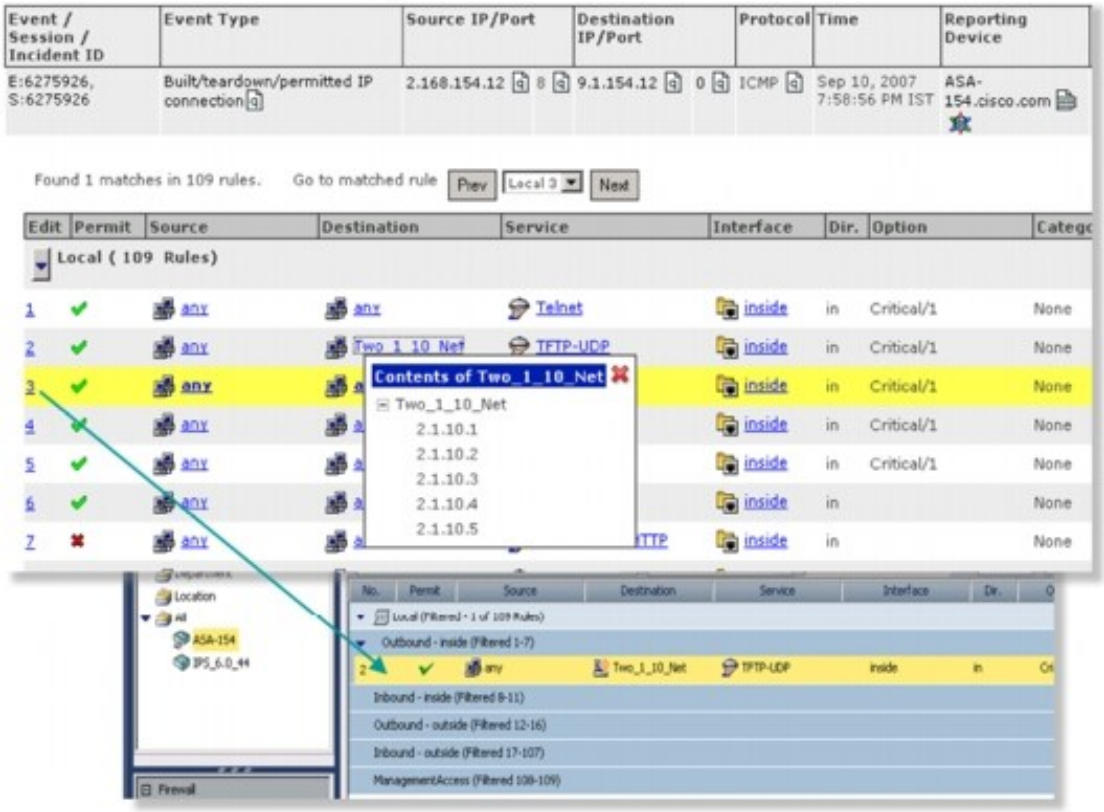
Что понадобится	Как обеспечить
Сертификаты цифрового ключа	Организовать собственный удостоверяющий центр, или получать ключи в стороннем УЦ
Криптопровайдер	Входит в комплект поставки МЭ либо приобретается отдельно
Политики безопасности и правила доступа	Правила доступа определяются владельцами ИСПДн (администраторами), соответствующие политики генерируются программно и устанавливаются на МЭ
Услуги администратора (администраторов)	Силами собственных специалистов, или привлекая сторонних (аутсоурсинг)
Инструменты администрирования и управления	

Проблемы начинаются, когда межсетевых экранов в ИСПДн становится много

ЭЛВИС-ПЛЮС

Инструменты администрирования и управления





Лидеры рынка безопасности решают задачи администрирования и управления сетей и информационных систем с помощью специализированных инструментов

ЭЛВИС-ПЛЮС

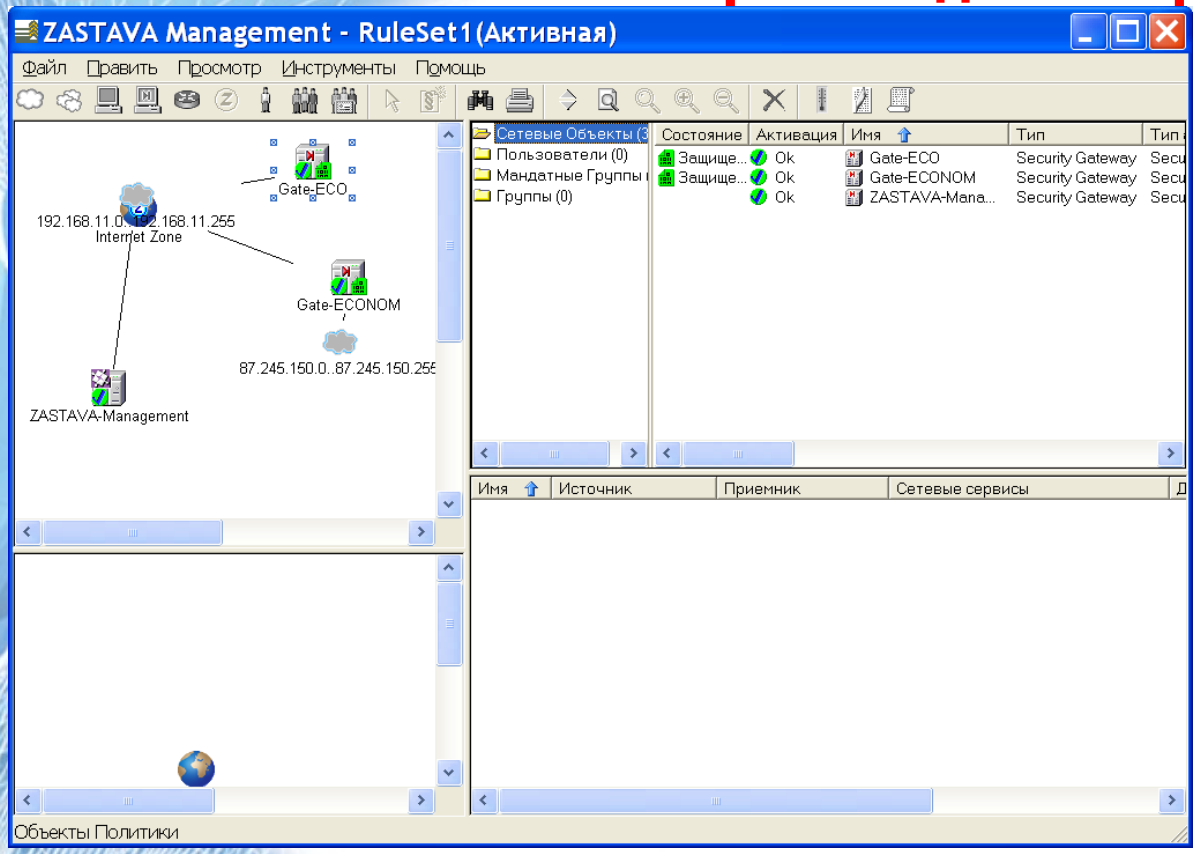
Межсетевые экраны. Задачи администрирования и управления

- Генерация глобальной и локальных политик безопасности (ГПБ, ЛПБ)
- Доставка ЛПБ на управляемые межсетевые экраны, ее активация и дезактивация
- Мониторинг и журналирование событий безопасности на управляемых МЭ
- Мониторинг статуса управляемых устройств и его оперативное изменение в случае необходимости

В больших ИСПДн критически важно централизованное, удаленное управление межсетевыми экранами и средствами безопасности

ЭЛВИС-ПЛЮС

Межсетевые экраны. Администрирование и управление



- Эффективно работает с 1000 -1500 агентами. В перспективе – до 5 000 агентов
- Управляет как собственными Агентами, так и маршрутизаторами Cisco, межсетевыми экранами Cisco PIX, и устройствами Check Point VPN-1/FireWall-1
- Удаленно взаимодействует с агентами через Интернет по защищенному каналу
- Обеспечивает удаленное обновление ПО собственных АгентовАгентов

Подробнее – вчера, 14:40 – 15:00 «Централизованное управление сетевой безопасностью в распределенных информационных системах» и сегодня , здесь.

ЭЛВИС-ПЛЮС

Спасибо за внимание !

124498, Москва, Зеленоград, проезд 4806, д.5, стр.23
тел. (495) 276-0211, факс (499) 731-2403
e-mail: mb@elvis.ru
http://www.elvis.ru