XV международная конференция
«РусКрипто’ 2013»

конференция
РусКрипто’2013

http://www.ruscrypto.ru/conference/

Защита каналов связи между участниками единой платёжно-сервисной системы «Универсальная электронная карта»

Юрий Авраменко

ОАО «ИнфоТеКС»
+7 (495) 737-61-92
avramenko@infotecs.ru

ViPNet® Virtual Private Network

infotecs®

Участники ЕПСС УЭК

- ФУО (ОАО «УЭК»)
- УОС (государственные учреждения и коммерческие организации в субъектах РФ)
- Более 200 банков
- Сервис-партнёры
  - Центры персонализации и изготовления карт
  - Поставщики коммерческих услуг
  - Операторы сервисных сетей и др.

Требования к защите каналов связи

- В ЕПСС УЭК обрабатываются ПДн большого числа субъектов (граждан)
- К ЕПСС УЭК подключены информационные системы многих банков
- В процессе работы ЕПСС УЭК осуществляется деятельность УЦ и передача ключевой информации СКЗИ по каналам связи
- Информационные системы участников ЕПСС УЭК взаимодействуют с СМЭВ
- В ЕПСС УЭК может обрабатываться коммерческая тайна ОАО «УЭК»

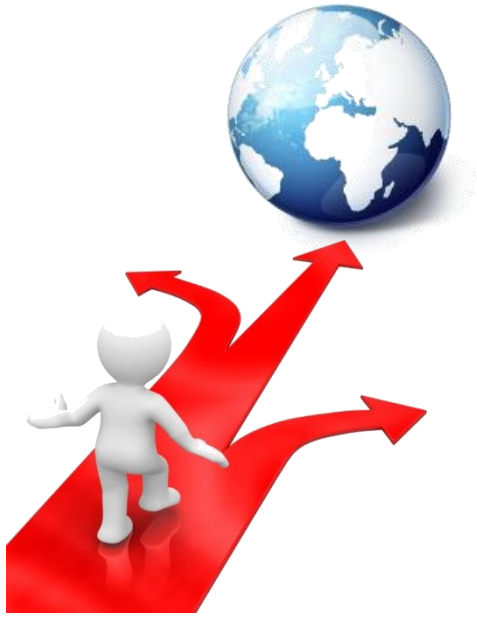
Модель угроз и нарушителя ЕПСС УЭК

- 17 ролей участников ЕПСС УЭК
- ЕПСС УЭК рассматривается как АСЗИ, в которой обрабатываются ПДн
- Различные классы нарушителей для разных ролей участников ЕПСС (от Н5 для центров выпуска карт до Н1 для терминалов операторов канала обслуживания)
- Модель предусматривает необходимость разработки частных моделей угроз и нарушителя для систем участников ЕПСС УЭК

Модель угроз нарушителя информационной безопасности ЕПСС УЭК согласована с ФСБ России в 2011 г.

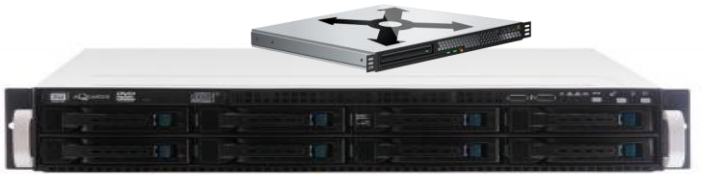
Типовые решения для защиты каналов связи ЕПСС УЭК

- ПАК ViPNet Coordinator KB2
- ПАК ViPNet Coordinator HW1000 в кластерном исполнении
- ПАК ViPNet Coordinator HW100
- ПО ViPNet Client
- ПО ViPNet Administrator КС3



Характеристики комплексов защиты каналов связи ЕПСС УЭК

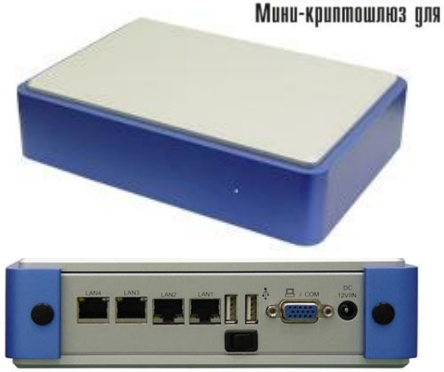
ПАК ViPNet Coordinator HW2000



- Криптошлюз и межсетевой экран для ЦОД
- Эффективная поддержка 10G сетевых интерфейсов;
- Работа в кластерной схеме с резервированием каналов и резервированием ПАК
- Производительность: 3,5 Гбит/с ;
- встроенные средства удалённого управления и мониторинга
- Сертификаты ФСТЭК (3 класс МЭ и 3 уровень контроля НДВ) и ФСБ России (КС3 для СКЗИ и 4 класс МЭ)

ПАК ViPNet Coordinator HW100

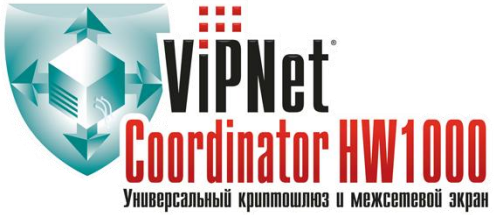
Компактный криптошлюз и межсетевой экран для защиты трафика удаленных сетевых устройств или небольших локальных сетей.

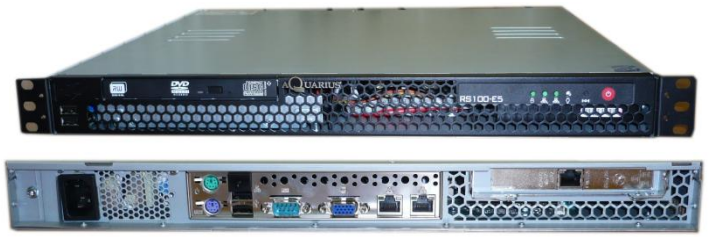


- **Особенности**
  - ✓ Малые размеры и вес, высокая механическая прочность
  - ✓ Безвентиляторное исполнение
  - ✓ 4 сетевых интерфейса Ethernet 10/100/1000
  - ✓ Производительность по шифрованию – до 25 Мбит/с

ПАК ViPNet Coordinator HW1000

Универсальный криптошлюз и межсетевой экран для защиты трафика в любых сценариях защиты информации.

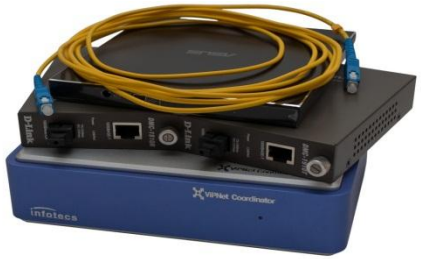




- **Особенности**
  - ✓ Промышленный сервер для установки в стандартную стойку
  - ✓ Поддержка режима failover
  - ✓ Производительность по шифрованию – до 280 Мбит/с
- **Области применения**
  - ✓ Шифрование каналов связи между локальными сетями
  - ✓ Защита локальных сетей от сетевых атак, фильтрации исходящего трафика, сокрытие внутренней структуры сети (DNAT)
  - ✓ Организация защищенного удаленного доступа к корпоративным ресурсам
  - ✓ Защита мультисервисных сетей связи (ip-телефония, видеоконференции)

ПАК ViPNet Coordinator KB100 Q2

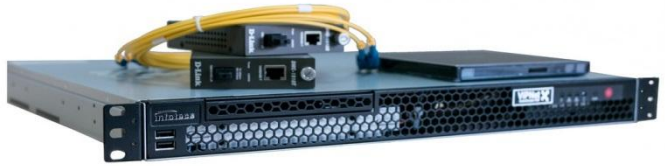
Компактный криптошлюз и межсетевой экран для защиты трафика удаленных сетевых устройств или небольших локальных сетей от нарушителей высокого класса.



- **Особенности**
  - ✓ Защита информации по классу **KB2**
  - ✓ Безвентиляторное исполнение и низкое энергопотребление
  - ✓ Самая низкая стоимость владения среди устройств аналогичного класса

ПАК ViPNet Coordinator KB1000 X2

Универсальный криптошлюз и межсетевой экран для защиты информации от нарушителей высокого класса.



- **Особенности**
  - ✓ Промышленный сервер для установки в стандартную стойку с оптическими конверторами
- **Области применения**
  - ✓ Шифрование каналов связи между локальными сетями по классу **KB2**
  - ✓ Защита территориально-распределённых систем Удостоверяющих центров в сети Интернет
  - ✓ Защита мультисервисных сетей связи (ip-телефония, видеоконференции) высших органов власти

Задачи, требующие решения

- Актуализация модели угроз и нарушителя ЕПСС УЭК
- Разработка частных моделей угроз и нарушителя для систем УОС и других участников ЕПСС УЭК
- Оснащение АСЗИ сертифицированными ФСБ России средствами обнаружения компьютерных атак
- Создание системы мониторинга функционирования защищённой сети ЕПСС УЭК
- Разработка комплексов терминального обслуживания со встроенными средствами криптографической защиты канала связи
- Проведение тематических исследований криптографических компонент УЭК

Перспективы развития

- Стандартизация криптографических алгоритмов (ТК26)
- Завершение работ по созданию бесплатного криптопровайдера с поддержкой УЭК, распространяемого через Интернет (ViPNet CSP)
- Оснащение средствами защиты класса КВ2 центров выдачи карт и регистрации пользователей УЦ
- Модернизация центрального и резервного ЦОД для повышения скорости обработки трафика в сетях свыше 10G
- Проведение инструментального контроля защищённости информационных систем и комплексов ЕПСС УЭК

Спасибо за внимание!
Вопросы?

Юрий Авраменко

ОАО «ИнфоТеКС»
+7 (495) 737-61-92
avramenko@infotecs.ru

ViPNet Virtual Private Network

infotecs