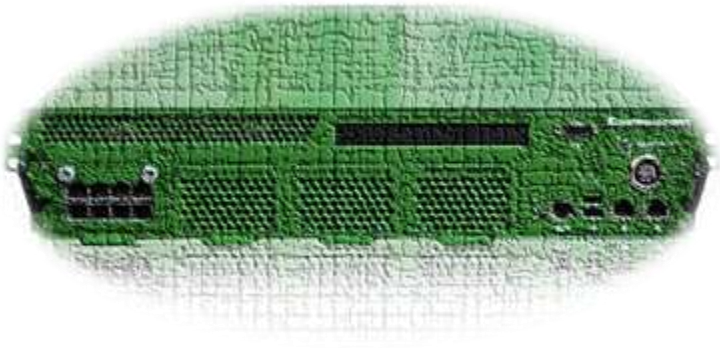
Код безопасности

Аппаратно-программный комплекс шифрования «Континент» 3.7



АПКШ «Континент»

Аппаратно-программный комплекс шифрования «Континент»

Комплекс предназначен для организации защиты сетевого периметра и обеспечения конфиденциальности данных при передаче по общедоступным каналам связи.

- **Межсетевой экран**
- **Маршрутизатор с развитыми сетевыми функциями**
- **Средство построения виртуальных частных сетей (VPN) на основе глобальных сетей общего пользования (Интернет)**
- **Средство обнаружения вторжения (СОВ)**

АПКШ «Континент»

Объединение через Интернет территориально распределённых локальных сетей предприятия в единую сеть VPN

Использование выделенных линии при сохранении высокого уровня безопасности

Безопасное подключение к сетям общего пользования

АПКШ «Континент» может применяться в качестве межсетевого экрана/маршрутизатора для безопасного подключения ЛВС к сетям общего пользования (Интернет). Поддержка технологии NAT, позволяет организовать доступ пользователей ЛВС к ресурсам сети Интернет с одного IP адреса.

Подключение удаленных сотрудников

Подключение удаленный сотрудников возможно при помощи абонентского пункта (АП). Абонентский пункт это программный VPN клиент, который позволяет удаленному пользователю устанавливать защищенное соединение.

АПКШ «Континент»

Защита трафика IP телефонии и видеоконференцсвязи

Использование функции приоритезации трафика QoS.

Защита сегментов беспроводных сетей

Безопасное подключение клиентов беспроводной сети в выделенный сегмент с разграничением прав доступа.

Защита банкоматов (встраиваемое применение)

Отказоустойчивый кластер

Позволяет повысить надежность за счет применения схемы кластера высокой доступности, который состоит из двух криптошлюзов, которые работают по схеме Active/Passive, то есть в случае сбоя активного переключается на пассивный, за счет автоматической синхронизации конфигураций.

Подключение к системе электронного декларирования ФТС

Защита мобильных устройств (платформы iOS, Android)

Сертификаты АПКШ «Континент»

АПКШ «Континент»

- ФСТЭК – МЭ2, НДВ2, СОВ3
- ИСПДн до УЗ1
- ФСБ – СКЗИ КС3, КС2,
- ФСБ – МЭ4

СЗИ/СКЗИ Континент АП

- ФСТЭК – МЭ3, НДВ3
- ИСПДн до УЗ1
- ФСБ – СКЗИ КС1/КС2/КС3
- ФСБ – МЭ4

Новые сертификаты версии 3.7


СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3008


СЕРТИФИКАТ СООТВЕТСТВИЯ

Сертификат ФСТЭК
Подтверждает соответствие требованиям руководящих документов по **3-му классу защиты для систем обнаружения вторжений**, по **2-му классу защищенности для межсетевых экранов** и по **2-му уровню контроля на отсутствие НДВ**

Минкомсвязи России – о соответствие установленным требованиям к оборудованию маршрутизации пакетов информации и возможности применения на сетях связи общего пользования в качестве оборудования коммутации и маршрутизации пакетов информации

Код Безопасности

Модельный ряд

Континент IPC-25 Континент IPC-10 Континент IP-64	Континент IPC-100 Континент IPC-400	Континент IPC-3034F/3034 Континент IPC-3000F Континент IPC-1000 Континент IPC-1000F Континент IPC-1000F2

Модельный ряд

Континент IPC-3000F (S021)	
Форм-фактор	2U
Блок питания	2x отказоустойчивый Hot Swap
Количество, тип сетевых интерфейсов	10x Gigabit Ethernet 10/100/1000 RJ45 4x10Gbit оптические SFP+
Производительность VPN	3 Гбит/с

Континент IPC-3034 (S021)	
Форм-фактор	2U
Блок питания	2x отказоустойчивый Hot Swap
Количество, тип сетевых интерфейсов	34x Gigabit Ethernet 10/100/1000 RJ45
Производительность VPN	3 Гбит/с

Континент IPC-1000F2 (S021)	
Форм-фактор	2U
Блок питания	2x отказоустойчивый Hot Swap
Количество, тип сетевых интерфейсов	10x Gigabit Ethernet 10/100/1000 RJ45 8x1000BASE-X оптические SFP
Производительность VPN	1 Гбит/с

Модельный ряд

Континент IPC-1000F (S021)	
Форм-фактор	2U
Блок питания	2x отказоустойчивый Hot Swap
Количество, тип сетевых интерфейсов	6x Gigabit Ethernet 10/100/1000 RJ45 UTP 4x1000BASE-X оптические SFP
Производительность VPN	1 Гбит/с

Континент IPC-1000 (S021)	
Форм-фактор	2U
Блок питания	2x отказоустойчивый Hot Swap
Количество, тип сетевых интерфейсов	10x Gigabit Ethernet 10/100/1000 RJ45 UTP
Производительность VPN	1 Гбит/с

Континент IPC-400 (S021)	
Форм-фактор	2U
Блок питания	1x (Hot Swap дополнительная опция)
Количество, тип сетевых интерфейсов	6x Gigabit Ethernet 10/100/1000 RJ45 UTP
Производительность VPN	500 Мбит/с

Модельный ряд

Континент IPC-100 (92E3)	
Форм-фактор	1U
Блок питания	1x
Количество, тип сетевых интерфейсов	6x Gigabit Ethernet 10/100/1000 RJ45 UTP 2x1000BASE-X оптические SFP
Производительность VPN	300 Мбит/с

Континент IPC-25 (92D9)	
Форм-фактор	1U
Блок питания	1x внешний
Количество, тип сетевых интерфейсов	4x Gigabit Ethernet 10/100/1000 RJ45 UTP
Производительность VPN	50 Мбит/с

Континент IPC-10 (S088)	
Форм-фактор	Mini-ITX
Блок питания	1x внешний
Количество, тип сетевых интерфейсов	3x Gigabit Ethernet 10/100/1000 RJ45 UTP
Производительность VPN	10 Мбит/с

Обновление модельного ряда

Континент IPC-100 (S102) будет доступна с I квартала 2015	
Форм-фактор	1U
Блок питания	1x
Количество, тип сетевых интерфейсов	6x Gigabit Ethernet 10/100/1000 RJ45 UTP 2x1000BASE-X оптические SFP
Производительность VPN	300 Мбит/с

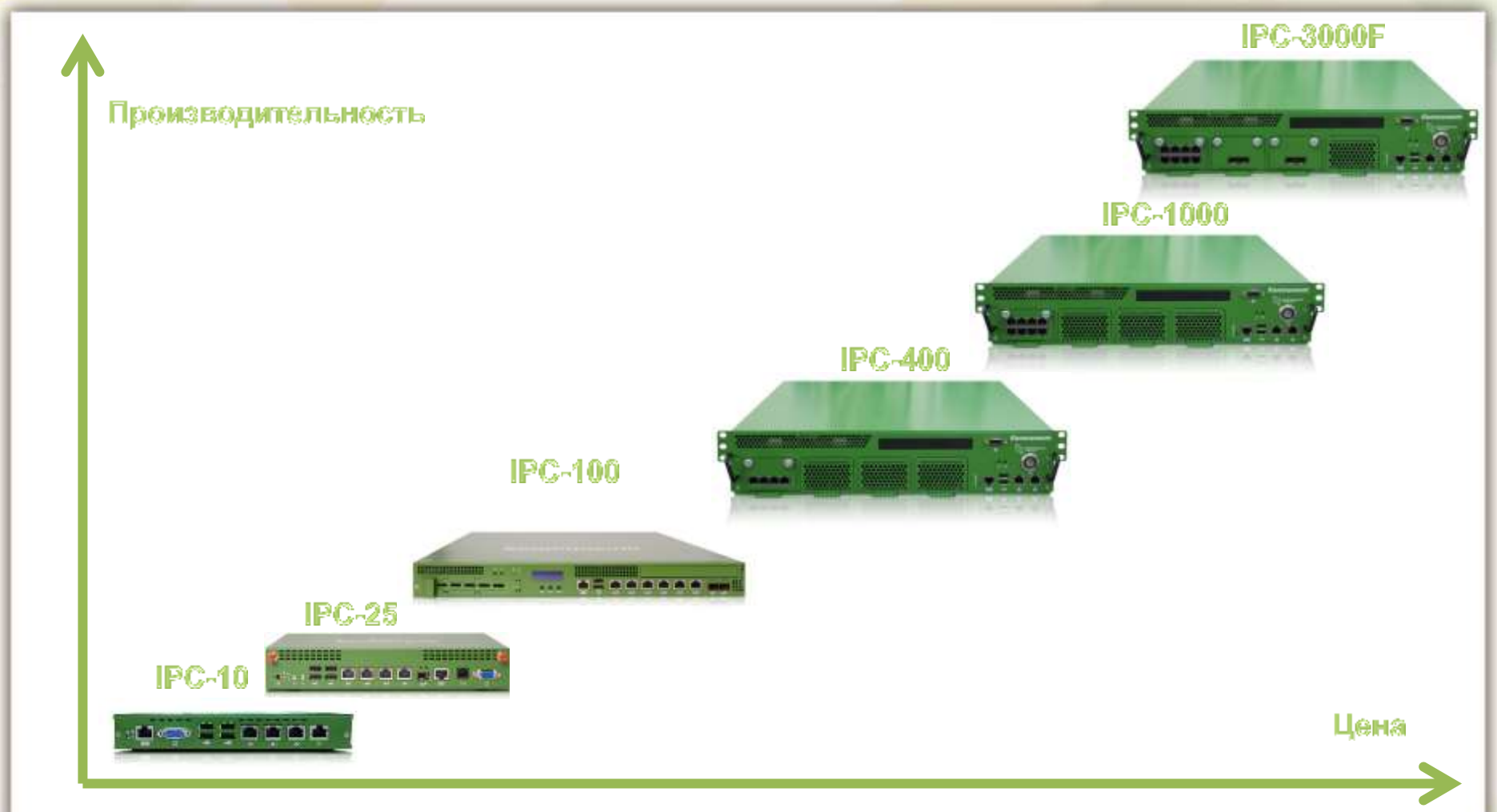
Континент IPC-25 (S115) будет доступна с I квартала 2015	
Форм-фактор	1U
Блок питания	1x внешний
Количество, тип сетевых интерфейсов	4x Gigabit Ethernet 10/100/1000 RJ45 UTP 1x1000BASE-X оптические SFP
Производительность VPN	50 Мбит/с

Континент IP-64 защита от влаги и пыли	
Форм-фактор	1U
Блок питания	1x внешний
Количество, тип сетевых интерфейсов	3x Gigabit Ethernet 10/100/1000 RJ45 UTP 1x1000BASE-X оптические SFP
Производительность VPN	10 Мбит/с

Модельный ряд

	Континент IPC-10	Континент IPC-25	Континент IPC-100	Континент IPC-400	Континент IPC-1000/1000F/10000F2	Континент IPC-3000F
Форм-фактор	Mini-ITX	Mini-ITX	1U	2U rack	2U rack	2U rack
Пропускная способность VPN	10 Мбит/с	50 Мбит/с	300 Мбит/с	500 Мбит/с	950 Мбит/с	2,7 Гбит/с
Пропускная способность МЭ	100 Мбит/с	100 Мбит/с	400 Мбит/с	1 Гбит/с	1 Гбит/с	3 Гбит/с
Максимальное количество конкурирующих TCP keep-state сессий	5 000	10 000	250 000	350 000	1 000 000	3 000 000
Количество, тип сетевых интерфейсов	3x Ethernet 10/100	4x Gigabit Ethernet 10/100/1000	6x Gigabit Ethernet 10/100/1000 2xSPF оптический	6x Gigabit Ethernet 10/100/1000	10x Gigabit Ethernet / 6x Gigabit Ethernet 4x 1000 BASE-X SPF оптический /10x Gigabit Ethernet 8x 1000 BASE-X SPF оптический	10x Gigabit Ethernet 10/100/1000 4x10Gigabit оптические SPF+Fiber
Режим кластера высокой доступности (горячее резервирование)	Нет	Нет	Да (активно-пассивный кластер)	Да (активно-пассивный кластер)	Да (активно-пассивный кластер)	Да (активно-пассивный кластер)
Производительность Сервера Доступности (Количество абонентов Континент АП)	Не поддерживается	До 25	До 500	До 1000	До 3000	
Производительность ЦУС (Количество КШ в сети с одним ЦУС)	Не поддерживается	До 25	До 500	До 1000	До 3000	

АПКШ «Континент» 3.7



Код Безопасности

Возможности «Континент»

Поддержка QoS

Реализована возможность централизованного управления приоритезацией трафика. Теперь комплекс поддерживает работу следующих механизмов управления QoS **:**

- классификация трафика;
- маркировка IP-пакетов;
- управление перегрузками с помощью очередей;
- предупреждение перегрузок.

Управление полосой пропускания

Traffic shaping**:**

- Резервирование полосы пропускания;
- Ограничение полосы пропускания.

Поддержка режимов «Multi-WAN»

Реализована возможность одновременного подключения криптографического шлюза к нескольким внешним сетям (Multi-WAN). Имеются следующие режимы Multi-WAN:

- Передача трафика в соответствии с таблицей маршрутизации;
- Обеспечение отказоустойчивости канала связи;
- Балансировка трафика между внешними интерфейсами КШ.

Криптографический шлюз может функционировать только в одном из выбранных режимов. Управление режимами Multi-WAN осуществляют средствами централизованного управления.

Возможности «Континент»

Multicast - маршрутизация

Реализована поддержка multicast маршрутизации – групповая передача данных (сетевой пакет одновременно направляется определенной группе адресатов).

Механизм трансляции NAT

Реализован режим NAT 1:1. Инициатор соединения — любая сторона. В исходящих IP-пакетах внутрисетевой IP-адрес отправителя заменяется на указанный публичный. Во входящих IP-пакетах публичный IP-адрес получателя заменяется на указанный внутрисетевой.

Работа КШ за NAT

- КШ Континент может располагаться за любым типом NAT;
- ЦУС выполняет роль координирующего сервера, сообщает КШ их реальные IP;
- ЦУС всегда должен иметь «белый» IP –адрес.

Смена ключей КШ

Управление сменой ключей производится средствами централизованного управления (главного ключа КШ и ключа связи с ЦУС):

- автоматически в соответствии с заданным расписанием;
- вручную.

Возможности «Континент»

Аппаратное резервирование КШ

- Поддержка аппаратного резервирования (создания кластера высокого доступа) для криптографических шлюзов, подключенных к внешней сети по протоколу PPPoE.
- Возможность задать два интерфейса резервирования.

IP адрес внешнего интерфейса ЦУС

- Возможность назначение нескольких IP-адресов на внешнем интерфейсе ЦУС, что делает возможным безболезненную смену IP-адреса ЦУС при смене провайдера.

Средства управления

- Интегрированные средства централизованного управления всеми функциями комплекса (включая настройки функций VPN и межсетевого экранирования).
- Графический пользовательский интерфейс настройки и управления.

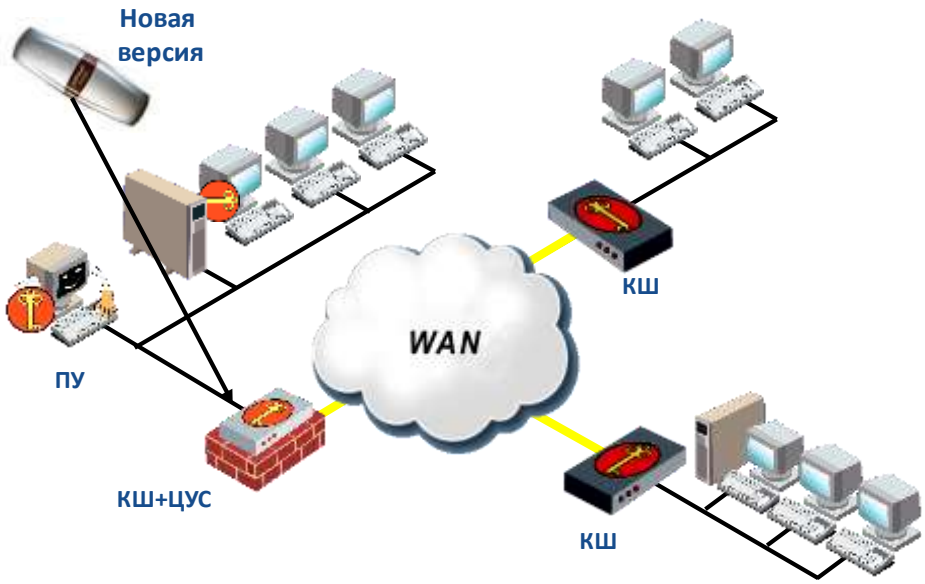
Средства мониторинга

- Оперативный мониторинг состояния комплекса в режиме реального времени, из ПУ ЦУС;
- Уведомление администратора о критических событиях по e-mail;
- Мониторинг состояния КШ по SNMP;
- Хранение журналов в СУБД MS SQL Server;
- Экспорт событий в xml формат для импорта во внешние системы SIEM.

Возможности «Континент»

Централизованное-дистанционное управление

Удаленное обновление версии ПО криптошлюзов



Удобство управления

Для удобства просмотра и управления объекты можно объединять в группы. Возможность группировки предусмотрена для следующих объектов:

- сетевые объекты;
- сервисы;
- криптографические шлюзы.

Новые возможности «Континент» 3.7

Удобное межсетевое взаимодействие между разными сетями «Континент»

- Возможность организации защищенного соединения между КШ, принадлежащими разным криптографическим сетям и управляемыми разными ЦУС, установка доверительных отношений между ЦУС разных сетей и возможность централизованного управления созданием парных связей между КШ разных сетей и управление их параметрами.

Поддержка протокола IPv6

- Поддержка работы с каналами связи общих сетей передачи данных, использующих протоколы IPv6. Протокол IPv6 используются для организации защищенных связей через IPv6 сети провайдеров.

Возможность использования NAT внутри VPN

- Возможность создания VPN связей между КШ с пересекающимися диапазонами IP адресов в защищаемых сетях, с использованием механизма виртуальной адресации.

Возможность балансировки шифрованного трафика между фермой криптошлюзов для достижения производительности свыше 10Гбит/с

Новое высокопроизводительное криптоядро

- Новая технология ускорения криптографических операций на выделенных ядрах ЦПУ, обеспечивает увеличение предельной пропускной способности. Максимальная производительность криптографической обработки трафика (режим VPN + МЭ) до 3Гбит/с на платформе Континент IPC-3000F.

Новые возможности «Континент» 3.7

АРМ ГК

- В составе комплекса создано автоматизированное рабочее место генерации ключей (АРМ генерации ключей)

Срок жизни ключей КШ до 3-х лет

- Возможность использования для КШ не извлекаемых ключей хранящихся на внешнем защищенном носителе Rutoken со сроком жизни до трех лет

Поддержка NTP на ЦУС

- Автоматическая синхронизация времени ЦУС с заданным сервером точного времени по протоколу NTP.

Режим повышенной безопасности

- Позволяет создавать группы КШ с политиками безопасности исключающими попадание незашифрованного трафика во внешние сети.

Функционал DHCP сервера на КШ

- Позволяет назначать динамические IP адреса клиентским устройствам
- DHCP relay

L2 VPN

- Криптографический коммутатор – позволяет объединять сети прозрачно на уровне L2

Программный VPN клиент

СКЗИ "Континент-АП" является программным VPN-клиентом и предназначено для предоставления сотрудникам, работающим на ОС семейства MS Windows, удаленного доступа к ресурсам корпоративной информационной системы.

Поддерживаемые операционные системы:

- *Windows XP SP3;*
- *Windows Vista 32/64;*
- *Windows 7 32/64;*
- *Windows 8 x86/64;*
- *Windows 8.1 x86/64;*
- *Windows Server 2003;*
- *Windows Server 2008;*
- *Windows Embedded Standard 7*

Программный VPN клиент

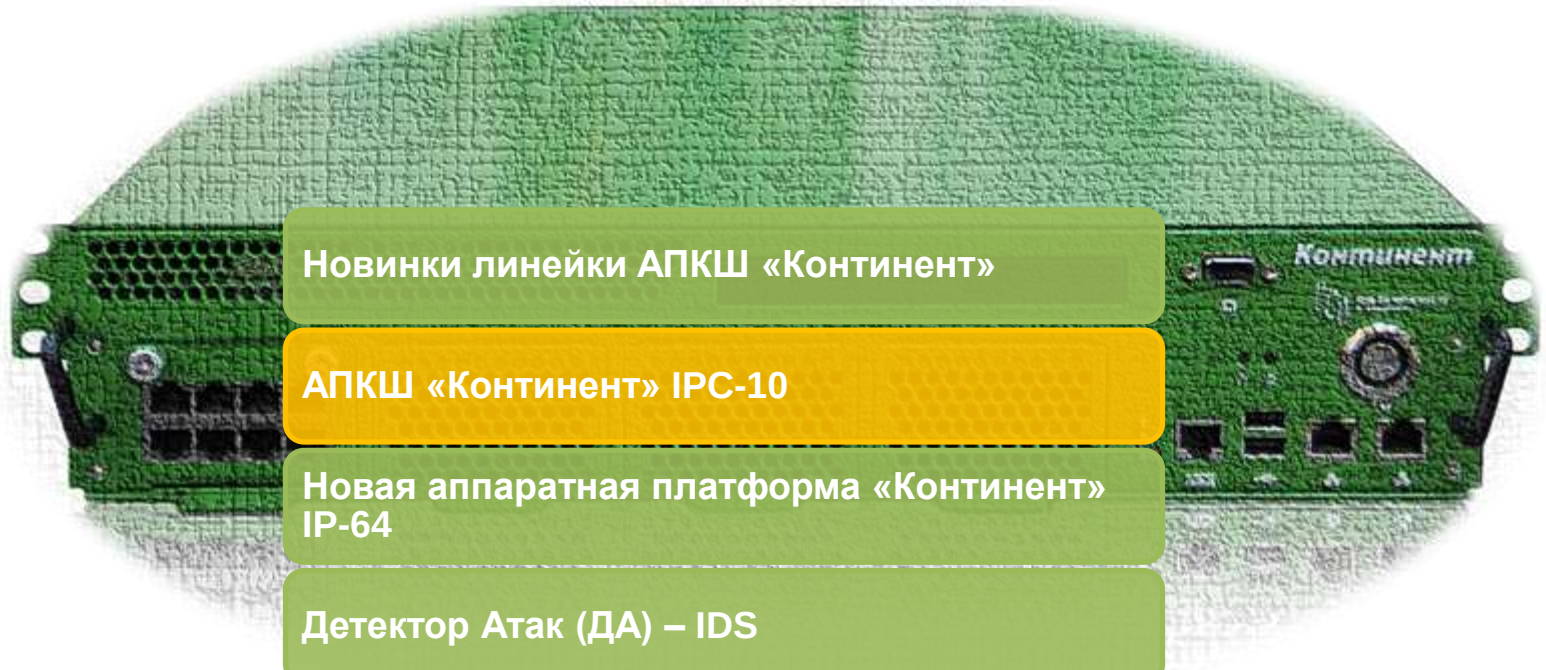
- Встроенный персональный межсетевой экран;
- Строгая двухфакторная аутентификация пользователя;
- Поддержка инфраструктуры PKI;
- Для идентификации и аутентификации пользователя Континент-АП при подключении к СД Континент используется цифровой сертификат X509;
- Возможность использования защищенных отчуждаемых носителей (Token) для хранения цифрового сертификата и ключа;
- Автоматическое восстановление соединения при разрыве связи;
- Возможность работы через различные транспортные среды: выделенное соединение Ethernet, Dial-Up, FDI, GPRS/3G/4G LTE

Новые возможности версии 3.7

- Возможность входа/выхода пользователя МСЭ.
- Возможность определения администратором правил фильтрации, которые действуют до авторизации пользователя.
- Возможность подключения Континент-АП к серверу доступа по DNS-имени.
- Возможность туннелирования трафика Континент-АП в HTTPS тоннель.
- Поддержка авторизации на HTTP-proxy в Континент-АП.
- API интерфейс для взаимодействия Континент-АП с внешними приложениями, возможность автоматического установления VPN соединения на АРМ без участия оператора.
- Возможность установки соединения Континент-АП с сервера доступа до логона пользователя в ОС, позволяет работать рабочим станциям входящим в домен удаленно.

Лицензирование «Континент»

- Лицензия на подключение КШ/ДА/КК к ЦУС, активируется на ЦУС (в комплект каждого ЦУС входит лицензия на подключение 4-х КШ/ДА/КК)
- Лицензия на подключение АП к СД, активируется на СД)
- Обновление ЦУС/КШ/СД с предыдущих версий
  - Право на обновление
  - Установочный комплект с ПО (диск, документация, голограммы)
- Лицензия на обновление БРП Детектора Атак, требуется для каждого используемого детектора атак



Новинки линейки АПКШ «Континент»

АПКШ «Континент» IPC-10

Новая аппаратная платформа «Континент» IP-64

Детектор Атак (ДА) – IDS

Крипто Коммутатор (КК) – L2VPN

АПКШ «Континент» IPC-10. Преимущества

АПКШ «Континент» IPC-10

Криптошлюз для защиты банкоматов и других платежных терминалов.

Выполняет функции криптографической защиты данных, передаваемых по каналам связи, сетевого экранирования и маршрутизации и защищает от атак, направленных на перехват банковских транзакций и получение доступа к счетам владельцев банковских карт, и атак типа «отказ в обслуживании» (Dos-атаки).

АПКШ «Континент» IPC-10. Преимущества

- Высокая устойчивость работы защищенного канала (симметричная ключевая схема), отсутствие необходимости установки соединения, работа по принципу крипто-маршрутизатора.
- Встроенные средства централизованного управления и мониторинга в режиме реального времени.
- Резервирование канала связи, отказоустойчивый VPN.
- Возможность подключения через 3G сети (возможно организовать резервирование каналов связи с банкоматами и обеспечить автоматическое переключение на резервный канал в случае сбоя связи без потери доступности банкомата).
- Сбор и анализ событий, возможен экспорт в ESM ArcSight.
- Предусматривает возможность встраивания.
- Компактные размеры и низкое энергопотребление.
- Корпус реализован в прочном антивандальном исполнении (возможность монтажа на стену или использование замка Кенсингтона).
- Поставляется в готовом для интеграции в ИТ-инфраструктуру виде и не требует затрат на приобретение дополнительных модулей.

Применение, спецификация и возможности системы

«Континент» IPC-10
- не требует локального обслуживания
- централизованная настройка и управления
- умеренная стоимость
- быстрая установка и замена

Применение, спецификация и возможности системы

	Континент IPC-10
Размеры	216mm(W)x 33.4mm(H)x134.2mm(L)
Возможность крепления на стену	Да. Замок Кенсингтона
Процессор	Intel® Atom™ Processor N2600 (1M Cache, 1.6 GHz)
Чипсет	Intel® NM10 Express (Tiger Point)
Память	DDR3 SO DIMM module 2Gb
Дисковая подсистема	1x SATA DOM 2Gb
Видеоадаптер	Intel Cedarview N2600 (640MHz)
Порты USB	4x Front, (4x internal header, 1 via miniPCIE)
Сетевые порты	3x RJ45 Ethernet 10/100
Система охлаждения	Пассивная
Поддерживаемые модули расширения	3G USB модем (внешний), протестированы Huawei E352, E173 (Мегафон) Wi-Fi опционально (для исполнения КС1)
Слоты расширения	MiniPCIE slotx1 (signal USB*1+PCIEx1) совместим с ПАК Соболь miniPCIe
Питание	Внешний адаптер DC 19В, 2,1А, 40Вт, 220В
Индикаторы (LED)	LAN LED, HDD LED, Power LED
Аппаратные кнопки	Reset Button*1, Power Button*1
Антенны	2x разъема SMD на передней панели (опционально)
Консольный порт (COM)	1x RJ485 COM-порт

Применение, спецификация и возможности системы

	Континент IPC-10
Криптография	ГОСТ 28147–89, КС3 (опционально КС1)
Централизованное управление	Да, с ЦУС Континент версии 3.6
Производительность МЭ	10 Мбит/с
Производительность VPN	3 Мбит/с
Максимальное количество конкурирующих keep-state сессий	3000
Общее количество сетевых интерфейсов	3x RJ45 10/100 Ethernet
Поддержка режима мульти-WAN	Да, WAN-failover
Резервирование VPN канала (VPN-failover)	Да
Маршрутизация на основе политик, через разные WAN интерфейсы	Да
Поддержка протоколов динамической маршрутизации	OSPF, BGP, RIP
Приоритизация трафика QoS	Да
Классификация трафика	До 32-х классов
Управление трафиком (Traffic shaping)	Резервирование/ограничение полосы пропускания за отдельными сервисами
Возможность работы КШ за NAT	Да
Динамически назначаемые IP-адреса	Да
Среднее время наработки на отказ (MTBF)	40 000 часов
Работа в необслуживаемом режиме 24x7	Да

Поддерживаемые 3G USB модемы

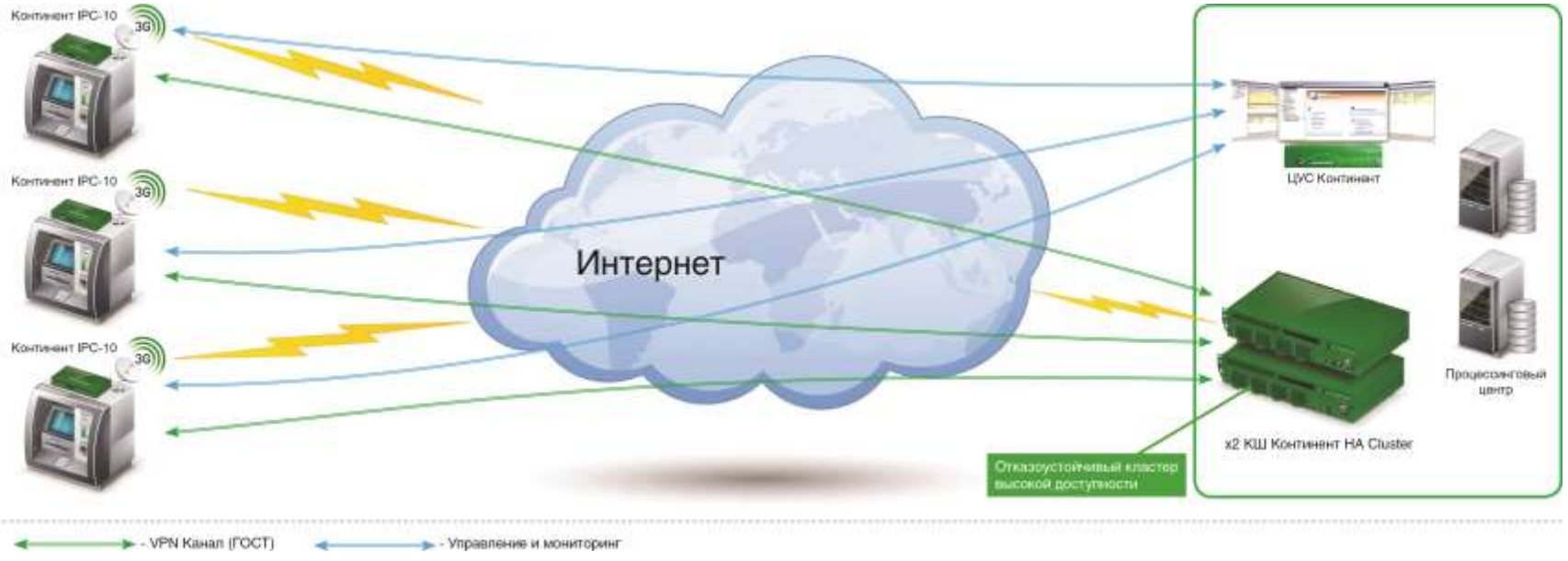
Мегафон
- Huawei E352 возможность подключения внешней антенны.
- Huawei E173.

МТС
- Huawei E171.
- Huawei D420 (он же E3131) возможность подключения внешней антенны.

Билайн
- Huawei E3131.

Без привязки к оператору
- Huawei E369 без привязки к оператору.
- Возможна поддержка других моделей 3G USB модемов.

Пример внедрения



Новинки линейки АПКШ «Континент»

АПКШ «Континент» IPC-10

Новая аппаратная платформа «Континент» IP-64

Детектор Атак (ДА) – IDS

Крипто Коммутатор (КК) – L2VPN

Новая аппаратная платформа «Континент» IP-64

Полное соответствие классу защиты IP65

Возможность применения оборудования Континент на объектах подвергающихся воздействию неблагоприятных условий окружающей среды

- Применение на промышленных объектах;
- Применение на специальных объектах;

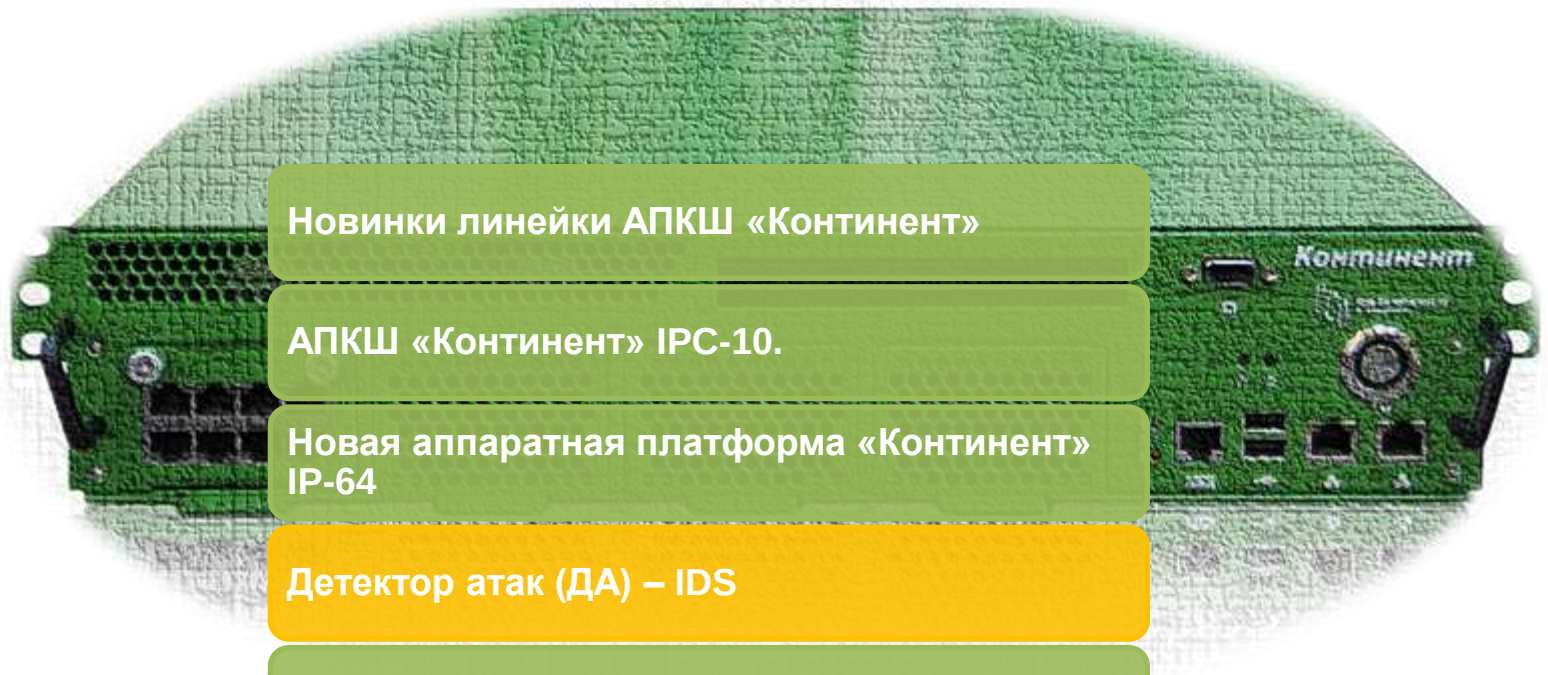
IPxx – рейтинг защиты корпусов электронного оборудования по стандарту IEC-952

Первый индекс – класс защиты корпусов электронного оборудования от проникновения внутрь посторонних тел:
Индекс - Описание

6 - Проникновение пыли предотвращено полностью

Второй индекс – класс защиты корпусов электронного оборудования от воздействия воды:
Индекс - Описание

4 - Вода, разбрызгиваемая на оболочку в любом направлении, не должна оказывать вредного воздействия на изделие



- Новинки линейки АПКШ «Континент»
- АПКШ «Континент» IPC-10.
- Новая аппаратная платформа «Континент» IP-64
- Детектор атак (ДА) – IDS
- Крипто Коммутатор (КК) – L2VPN

Детектор Атак (ДА) - IDS

Программно-аппаратный модуль, входящий в состав сертифицированной системы обнаружения вторжений (СОВ) АПКШ Континент версия 3.7, выполняющий функции сетевого сенсора и предназначен для автоматического обнаружения сетевых атак методом динамического анализа трафика стека протоколов TCP/IP.

Преимущества

- Сертификат соответствия ФСТЭК Россия - СОВ3, НДВ2.
- АПКШ «Континент» Детектор Атак единственное решение на российском рынке, использующее коммерческие сигнатуры. Большое количество правил, база постоянно актуализируется. Для «Континент» ДА актуальные сигнатуры, это одна из главных составляющих успеха (как и для AV).
- Сигнатурные и эвристические методы обнаружения.
- Реализованы наглядные графические представления отчетов.
- Централизованное управление и контроль функционирования. Удобный графический интерфейс программы управления.
- Повышение уровня защищенности АС.
- Оперативное уведомление администратора о выявленных атаках.

Преимущества

- База Решающих правил (БРП) - сигнатуры атак ETPro™ от Emerging Threats, лидирующее решение на рынке разработчиков сигнатур IPS/IDS.
- Более 19 тыс. правил в БРП.
- Актуальная реакция на угрозы - непрерывное ежедневное обновление БРП (ежедневно анализируется 150 - 250 тыс. образцов кода и добавляется в базу 5 - 30 новых правил).
- Низкий уровень ложных срабатываний (False Positives).

Модельный ряд

Континент IPC-100 **Континент IPC-25**	**Континент IPC-1000** **Континент IPC-1000F** **Континент IPC-400**

Модельный ряд

	ДА Континент IPC-25	ДА Континент IPC-100	ДА Континент IPC-400	ДА Континент IPC-1000	ДА Континент IPC-1000F
Форм-фактор	Mini-ITX	1U 19”	2U rack	2U rack	2U rack
Максимальное кол-во анализирующих интерфейсов	1	2	2	3	3
Производительность анализа трафика на одни интерфейс (сенсор) без эвристики	25 Мбит/с	130 Мбит/с	150 Мбит/с	200 Мбит/с	200 Мбит/с
Производительность анализа трафика на одни интерфейс (сенсор) с эвристикой	15 Мбит/с	105 Мбит/с	130 Мбит/с	170 Мбит/с	170 Мбит/с
Совокупная производительность	25 Мбит/с	260 Мбит/с	300 Мбит/с	600 Мбит/с	600 Мбит/с

Ключевые возможности

- **Удобство управления**

  Централизованное управление детекторами с ЦУС Континент, удобный графический интерфейс управления, предусмотрена автоматическая проверка синтаксиса правил, это позволяет упростить администрирование и избежать ошибок в настройке комплекса.

- **Регистрация информации об атаках**

  События, связанные с обнаружением вторжений, регистрируются в журналах. Отображается подробная информация об атаках - субъект/объект компьютерной атаки (IP, port), время и дата события, тип атаки.

- **Возможность обновления Базы Решающих правил БРП в режимах on-line/off-line**

  Обновление решающих правил может выполняться как автоматически по настраиваемому расписанию, так и вручную.

Ключевые возможности

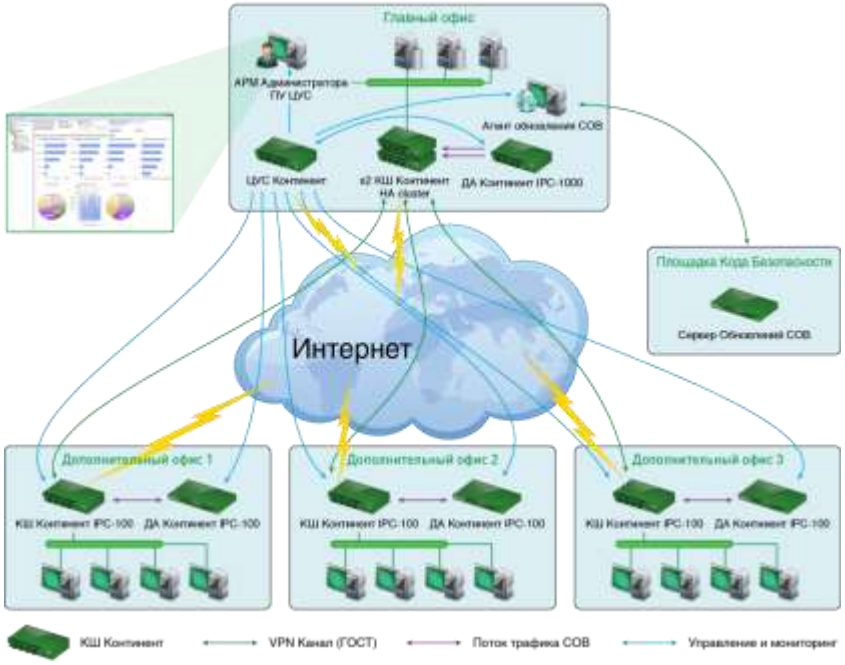
- **Поддержка протоколов различных уровней**
  - сетевого уровня: ICMPv4, ICMPv6, IPv4, IPv6
  - транспортного уровня: TCP, UDP, SCTP
  - канального уровня: PPPoE, PPP
  - прикладного уровня: FTP, HTTP, SMB, SSH, SMTP
  - сеансового уровня: SSL, DCE/RPC
- **Оперативное уведомление администратора**

  В случае обнаружения вторжений или нарушения безопасности администратору отсылается сообщение по электронной почте, а в программе управления ЦУС появляется визуальное отображение зафиксированного НСД.
- **Повышение уровня защищенности АС**

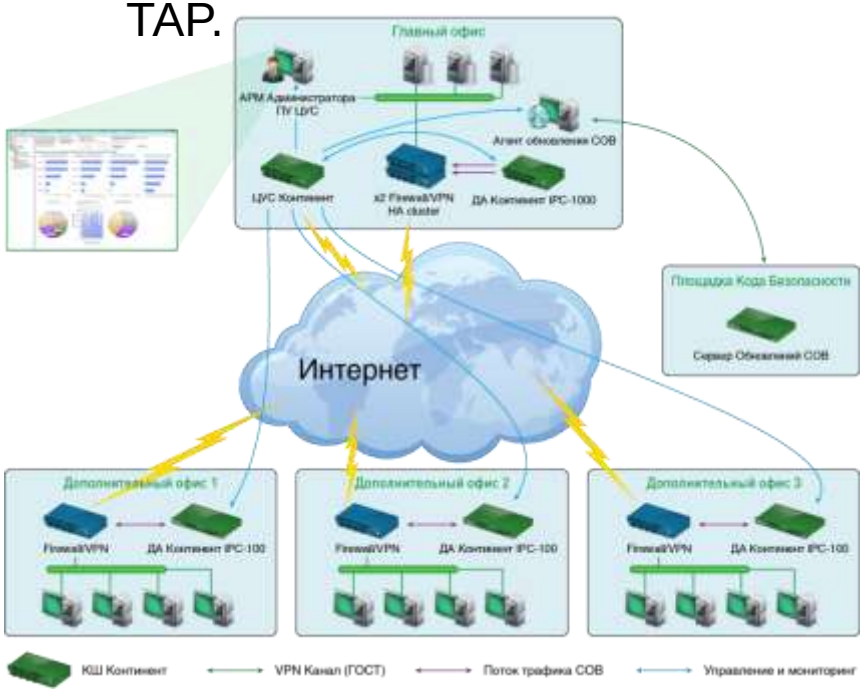
  Возможность работы АПКШ «Континент» ДА со сторонним оборудованием (подключение к SPAN порту маршрутизатора, или включение в сегмент через TAP).
  Возможность расширения защитного функционала существующей криптографической сети «Континент».

Ключевые возможности и пример внедрения

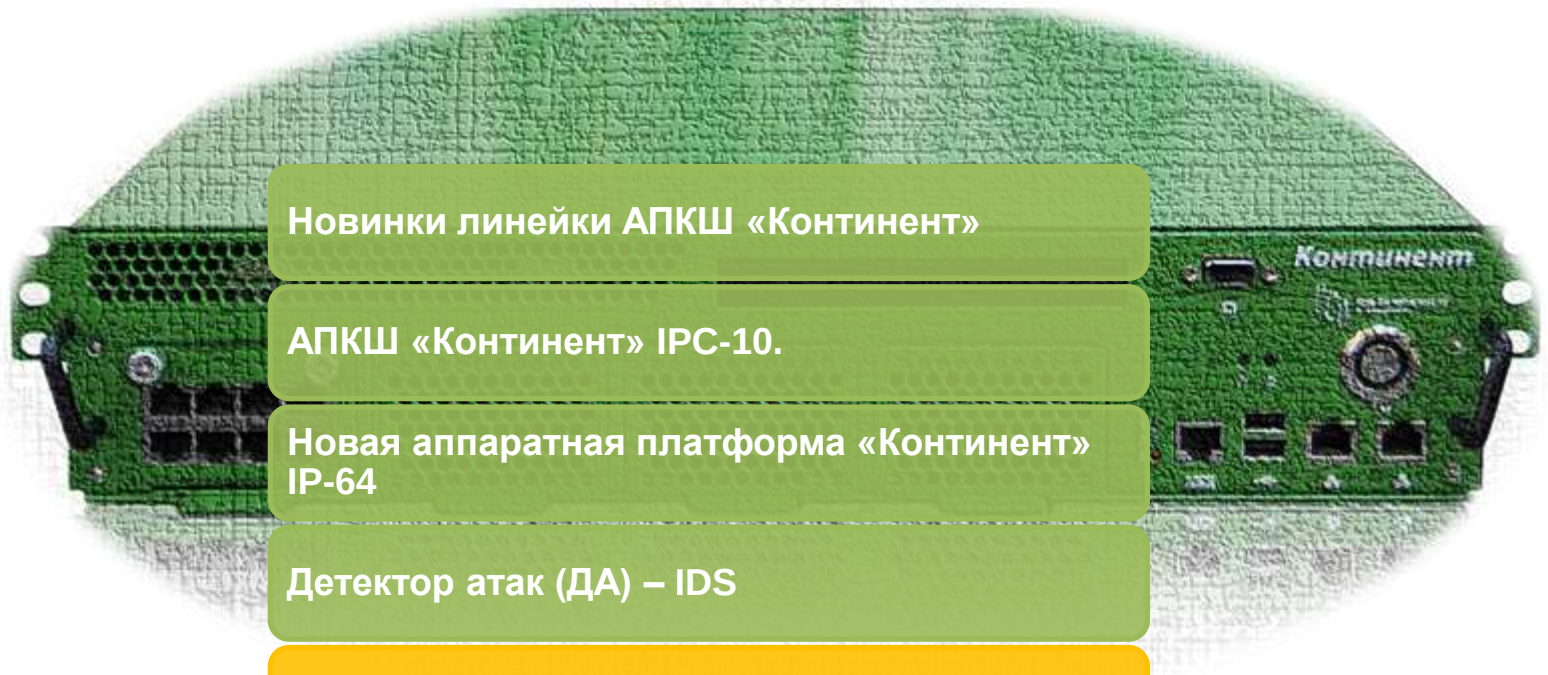
- Возможность применения как в качестве самостоятельного решения, так и для расширения защитного функционала существующей криптографической сети «Континент».



- Возможность работы модуля со сторонним оборудованием – подключение к SPAN-порту маршрутизатора или включение в сегмент через TAP.



Код Безопасности



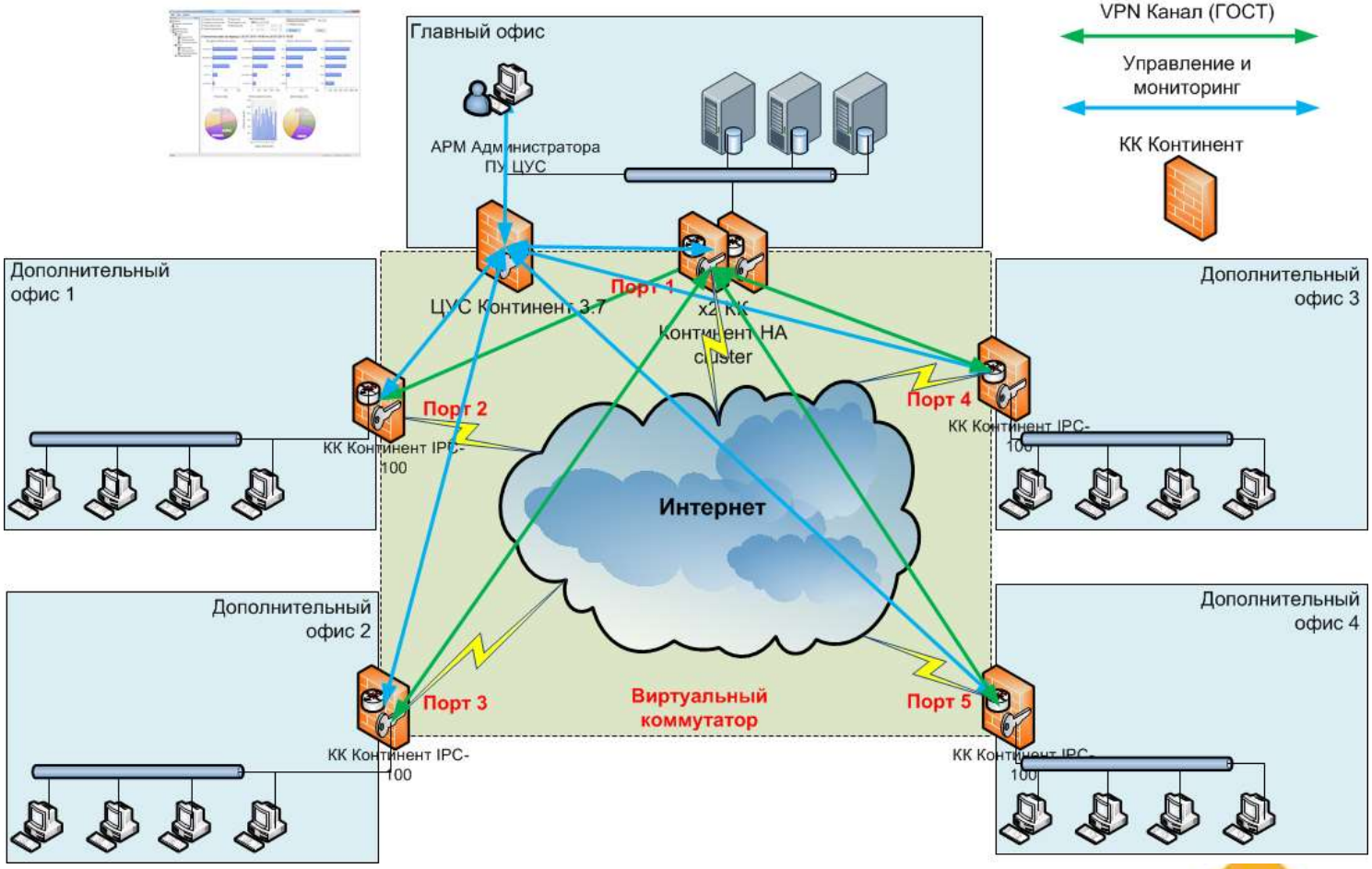
- Новинки линейки АПКШ «Континент»
- АПКШ «Континент» IPC-10.
- Новая аппаратная платформа «Континент» IP-64
- Детектор атак (ДА) – IDS
- Крипто Коммутатор (КК) – L2VPN

Криптографический Коммутатор (КК) – L2VPN

Программно-аппаратный модуль, входящий в состав АПКШ «Континент» версия 3.7, выполняет функции Криптографического Коммутатора, позволяет прозрачно объединять сегменты территориально распределенной сети на уровне L2 (L2VPN).

Криптографический Коммутатор (КК) – L2VPN. Пример внедрения

Виртуальный криптографический коммутатор – L2VPN



Криптографический Коммутатор (КК) – L2VPN. Преимущества

Преимущества

- Объединение территориально-распределенных сетей в один широковещательный домен;
- Передача широковещательных, мультикастовых пакетов, тегированного трафика (VLAN trunk), меток MPLS;
- Соединение двух сетей IPV6 через сеть IPV4;
- Минимальные настройки маршрутизации (настройка внешнего интерфейса подключения к WAN);

Применение

- Организация защищенного канала между ЦОД;
- Простая миграции сетевой инфраструктуры;

Уже используют

- Министерство Финансов Российской Федерации
- ГАС «Выборы»
- Администрация президента России
- Центральный Банк Российской Федерации (ЦБ РФ)
- Федеральная Таможенная Служба России (ФТС)
- Федеральное Казначейство (Казначейство России)
- Объединенная судостроительная корпорация (ОСК)
- Министерство обороны Российской Федерации
- Нефтяные корпорации





АПКШ «Континент» 3.7

- Поддержка ОС Windows 8 (x86/x64) и Windows Server 2012;
- Поддержка работы с каналами связи общих сетей передачи данных, использующих протоколы IPv6;
- Возможность обмена информацией по защищенному каналу между пересекающимися подсетями, защищенными разными КШ, с использованием механизма виртуальной адресации;
- Возможность балансировки шифрованного трафика между фермой криптошлюзов для достижения производительности свыше 10 Гбит/с;
- Добавлено АРМ генерации ключей;
- Реализована поддержка нового стандарта хэширования по ГОСТ Р 34.11–2012;
- В ПО криптошлюзов добавлен криптоусилитель, обеспечивающий увеличение их
- предельной пропускной способности. Максимальная производительностькриптографической обработки трафика (режим МЭ + VPN) до 3 Гбит/с (на платформе IPC-3000F);
- Возможность туннелирования трафика «Континент-АП» в HTTPS–тоннель;
- Поддержка авторизации на HTTP-прокси в «Континент-АП»;
- Реализована возможность использования неизвлекаемых ключей, хранящихся на внешнем защищенном носителе ruToken со сроком жизни до трех лет.

Сертификат ФСБ России – 1-е полугодие 2014 года.

Развитие АПКШ «Континент»

Функциональность

Версия 3.6
- Multi-WAN
- WAN-failover
- VPN- failover
- OSPF, BGP, RIP
- Multicast

Версия 3.7
- Производительность МЭ+VPN – 3Гбит
- IPv6
- Межсетевое взаимодействие ЦУС
- Защита от DOS атак
- СОВ – детектор атак
- L2VPN – Крипто Коммутатор
- DHCP server/DHCP relay
- Диагностические инструменты
- Аутентификация пользователей и возможность применения правил фильтрации к группам пользователей

Версия 4.0
- Новая высокопроизводительная платформа Континент OS на основе архитектуры x64
- Производительность МЭ+VPN – до 10Гбит на одно устройство КШ IPC-3000F
- Активно-активный кластер КШ с балансировкой нагрузки, масштабируемость
- Открытое распределение ключей (PKI)
- Кластеризация ЦУС
- Иерархическое управление ЦУС
- Система IPS в КШ
- DPI – (deep packet inspection)
- URL фильтрация (black листы Роскомнадзора)
- Агрегация портов
- Поддержка GREтоннелей
- Крипто-акселератор FPGA – модуль расширения для IPC-3000F, VPN 80Гбит full duplex
- Интеграция базы пользователей с MS AD

Сроки выпуска

2011	2014	2015

Контакты

Менеджер продукта: Немошкалов Александр, +7 (495) 982-3020 (доб.495)
Тел: +7 (495) 982-3020 (многоканальный)
Сайт компании: **www.securitycode.ru**
Информации о продуктах: info@securitycode.ru
Стоимость и покупка продуктов: buy@securitycode.ru
Служба технической поддержки: support@securitycode.ru

Код Безопасности