Код Безопасности

Сравнение возможностей продуктов АПКШ «Континент» версий 3.5, 3.6, 3.7

Сравнительный анализ средств защиты каналов связи

№	Наименование критерия	АПКШ Континент 3.7	АПКШ Континент 3.6	АПКШ Континент 3.5
Общие сведения				
1.1	Краткое описание решения	АПКШ «Континент» 3.7 позволяет реализовать защиту (шифрование и межсетевое экранирование) каналов связи при передаче информации ограниченного доступа между сегментами сложных распределенных сетей федерального масштаба по публичным (Интернет) и выделенным (ведомственные и корпоративные СПД) каналам связи, обеспечивая резервирование и балансировку имеющихся каналов связи, а также возможность приоритезации сетевого трафика, обеспечивает возможность работы с сетями IPv6. Комплекс содержит интегрированную систему обнаружения вторжений (СОВ). Позволяет строить как L3, так и L2 VPN	АПКШ «Континент» 3.6 позволяет реализовать защиту (шифрование и межсетевое экранирование) каналов связи при передаче информации ограниченного доступа между сегментами сложных распределенных сетей федерального масштаба по публичным (Интернет) и выделенным (ведомственные и корпоративные СПД) каналам связи, обеспечивая резервирование и балансировку имеющихся каналов связи, а также возможность приоритезации сетевого трафика	АПКШ «Континент» 3.5 позволяет реализовать защиту (шифрование и межсетевое экранирование) каналов связи при передаче информации ограниченного доступа между сегментами сложных распределенных сетей федерального масштаба по публичным (Интернет) и выделенным (ведомственные и корпоративные СПД) каналам связи
1.2	Тип решения	Программно-аппаратный комплекс	Программно-аппаратный комплекс	Программно-аппаратный комплекс
Сертификаты АПКШ Континент				
2.1	Сертификаты ФСБ России СКЗИ, МЭ	СКЗИ класса КС3; МСЭ 4-го класса защищенности	СКЗИ класса КС3; МСЭ 4-го класса защищенности	СКЗИ класса КС2; МСЭ 4-го класса защищенности
2.2	Сертификаты ФСТЭК России МЭ, НДВ	МСЭ 2; НДВ 2. Возможность использования в ИСПДн до 1 категории включительно, АС до 1Б включительно	МСЭ 3; НДВ 3. Возможность использования в ИСПДн до 1 класса включительно, в АС до 1В включительно	МСЭ 3; НДВ 3. Возможность использования в ИСПДн до 1 класса включительно, в АС до 1В включительно
2.3	Сертификаты ФСТЭК России СОВ	СОВ 3 класса защищенности	-	-

№	Наименование критерия	АПКШ Континент 3.7	АПКШ Континент 3.6	АПКШ Континент 3.5
2.4	Сертификаты ФСБ России Континент АП	СКЗИ класса КС1/КС2/КС3; МСЭ 4-го класса защищенности	СКЗИ класса КС1/КС2; МСЭ 4-го класса защищенности	СКЗИ класса КС1/КС2; МСЭ 4-го класса защищенности
2.5	Сертификаты ФСТЭК России. Континент АП	МСЭ 3; НДВ 3. Возможность использования в ИСПДн до 1 категории включительно, АС до 1Б включительно	МСЭ 3; НДВ 3. Возможность использования в ИСПДн до 1 класса включительно, в АС до 1В включительно	МСЭ 4; НДВ 3. Возможность использования в ИСПДн до 2 класса включительно, в АС до 1Г включительно
Реализация МСЭ				
3.1	Возможность идентификации и аутентификации пользователей, работающих на компьютерах в защищаемой сети КШ	**+** Идентификация и аутентификация пользователей предназначена для более тонкой настройки доступа сотрудников к корпоративным ресурсам. Идентификация и аутентификация пользователей, работающих на компьютерах в защищенной сети КШ, выполняется с помощью специальной программы «Клиент аутентификации пользователя», установленной на компьютере пользователя	- Не поддерживается	- Не поддерживается
3.2	Возможность централизованного управления правилами фильтрации сетевого трафика и настройками межсетевого экрана	+ Объекты в Программе управления ЦУС можно объединять в группы. Возможность группировки предусмотрена для следующих объектов: сетевые объекты; сервисы; криптографические шлюзы. Имеется возможность создавать иерархию групп криптографических шлюзов	+ Объекты в Программе управления ЦУС можно объединять в группы. Возможность группировки предусмотрена для следующих объектов: сетевые объекты; сервисы; криптографические шлюзы. Имеется возможность создавать иерархию групп криптографических шлюзов	+
3.3	Производительность МСЭ: • IPC-10 • IPC-25 • IPC-100 • IPC-400 • IPC-1000x • IPC-3000F	 • 100 Мбит/сек; • 100 Мбит/сек; • 400 Мбит/сек; • 600 Мбит/сек; • 1 Гбит/сек; • 3,5 Гбит/с	 • 100 Мбит/сек; • 30 Мбит/сек; • 300 Мбит/сек; • 400 Мбит/сек; • 950 Мбит/сек; • не поддерживается	 • не поддерживается; • 25 Мбит/сек; • 250 Мбит/сек; • 300 Мбит/сек; • 800 Мбит/сек; • не поддерживается
3.4	Фильтрация трафика на сетевом уровне по адресам отправителя/получателя	+	+	+
3.5	Фильтрация трафика на канальном уровне (поддержка VLAN)	+	+	+
3.6	Фильтрация по протоколам в заголовке IP-пакета	+	+	+
3.7	Фильтрация по портам протоколов UDP/TCP	+	+	+

№	Наименование критерия	АПКШ Континент 3.7	АПКШ Континент 3.6	АПКШ Континент 3.5
3.8	Фильтрация с учетом даты/времени	+	+	+
3.9	Возможность Network Address Translation	+	+	+
3.10	Поддержка настройки правил по принципу «белого» и «черного» списков	+	+	+
3.11	Возможность просмотра средствами локального управления КШ таблицы состояний (keep-state), отображающей коли-чество установленных соединений	Да	- Не поддерживается	- Не поддерживается
3.12	Защита от DoS-атак типа SYN-флуд	Да При обращении клиента к серверу криптографический шлюз сначала устанавливает TCP-соединение с клиентом от имени сервера, а затем с сервером от имени клиента. После этого клиент с сервером могут беспрепятственно обмениваться сетевыми пакетами. Полуоткрытые соединения с просроченным временем ожидания автоматически удаляются из таблицы состояния	- Не поддерживается	- Не поддерживается
3.13	Возможность автоматического блокирования всех незащищенных соединений	Да Добавлен режим замкнутой криптографической сети, запрещающий хождение незащищенного трафика	- Не поддерживается	- Не поддерживается
Реализация VPN				
4.1	Возможность организации защищенного VPN соединения через IPv6-сети провайдеров	Да Реализована поддержка работы с каналами связи общих сетей передачи данных, использующих протоколы IPv6	- Не поддерживается	- Не поддерживается
4.2	Возможность организации VPN между сетями с пересекающимися диапазонами IP адресов	Да Возможность обмена информацией по защищенному каналу между подсетями, защищенными разными КШ и использующих одинаковое адресное пространство. Для этого реализован механизм виртуальной адресации	- Не поддерживается	- Не поддерживается
4.3	Возможность централизованного управления ключами криптографической защиты информации	+	+	+

№	Наименование критерия	АПКШ Континент 3.7	АПКШ Континент 3.6	АПКШ Континент 3.5
4.4	Возможность централизованного управления созданием парных связей между криптографическими шлюзами (КШ)	+	+	+
4.5	Возможность централизованной внеплановой смены ключевой информации для всей сети КШ или выборочно для отдельных КШ	+	+	- Выполняется администратором локально на каждом КШ
4.6	Исходный ключевой блокнот	В качестве источника исходной ключевой информации для инициализации ЦУС может быть использован ПАК «Соболь», ключевой блокнот РДП-006 или АРМ генерации ключей	В качестве источника исходной ключевой информации для инициализации ЦУС может быть использован ПАК «Соболь» или ключевой блокнот РДП-006	В комплекте ЦУС поставляется тестовый ключевой блокнот, необходимость заказа РДП-006 в в/ч 43573
4.7	Периодичность смены ключей парной связи КШ	До 3-х лет К режиму управления ключами по схеме однолетнего хранения ключевой информации добавлен режим управления по схеме трехлетнего хранения ключевой информации. По схеме трехлетнего хранения генерация ключей выполняется на отдельном, не имеющем сетевых соединений АРМ ГК. Средствами АРМ ГК сгенерированные ключи записываются на отчуждаемые носители (USB-ключи). Ключевые носители передаются администраторам для загрузки в БД ЦУС и КШ. Срок действия/хранения ключей составляет три года. В качестве носителя используется USB-ключ Rutoken ЭЦП. Ключи записывают в его защищенную область	1 раз в год	1 раз в год
4.8	Возможность создания виртуальных каналов VPN, представляющих независимые очереди шифратора с возможностью приоритезации трафика и выбора внешнего интерфейса	+ До 32-х виртуальных каналов на одну парную связь	+ До 32-х виртуальных каналов на одну парную связь	- Однопоточное шифрование

№	Наименование критерия	АПКШ Континент 3.7	АПКШ Континент 3.6	АПКШ Континент 3.5
4.9	Возможность организации межсетевого взаимодействия между несколькими ЦУС	+ Организация защищенного соединения между КШ, принадлежащими разным криптографическим сетям и управляемыми разными ЦУС, возможна средствами централизованного управления. Для установления доверительных отношений между ЦУС используется собственная инфраструктура открытых ключей. Генерацию ключевой пары и издание сертификата открытого ключа для своей сети выполняет ЦУС. Администраторы обмениваются этими сертификатами до начала процедуры организации связи между сетями	- Только между КШ разных ЦУС, требует локальной настройки на КШ	- Только между КШ разных ЦУС, требует локальной настройки на КШ
4.10	Производительность шифрования трафика VPN: • IPC-10 • IPC-25 • IPC-100 • IPC-400 • IPC-1000x • IPC-3000F	• 10 Мбит/сек; • 35 Мбит/сек; • 300 Мбит/сек; • 500 Мбит/сек; • 950 Мбит/сек; • 2,7 Гбит/с	• 10 Мбит/сек; • 30 Мбит/сек; • 300 Мбит/сек; • 400 Мбит/сек; • 950 Мбит/сек; • не поддерживается	• не поддерживается; • 25 Мбит/сек; • 250 Мбит/сек; • 300 Мбит/сек; • 800 Мбит/сек; • не поддерживается
4.11	Алгоритм шифрования и длина симметричного ключа	ГОСТ 28147–89, 256 бит	ГОСТ 28147–89, 256 бит	ГОСТ 28147–89, 256 бит
4.12	Поддержка стандарта хэширования ГОСТ Р 34.11-2012	Да	- Не поддерживается	- Не поддерживается
Система обнаружения вторжений (СОВ)				
5.1	Наличие подсистемы обнаружения атак	Да Отдельный модуль, ПАК «Детектор Атак»	- Не поддерживается	- Не поддерживается
5.2	Сигнатурный анализ	Да	- Не поддерживается	- Не поддерживается
5.3	Эвристический анализа, выявление скрытых каналов передачи данных	Да	- Не поддерживается	- Не поддерживается
5.4	Производительность: • IPC-25 • IPC-100 • IPC-1000 • IPC-1000F	• 25 Мбит/сек; • 250 Мбит/сек; • 5 Гбит/сек; • 5 Гбит/сек.	- Не поддерживается	- Не поддерживается
L2VPN				
6.1	Возможность организации L2-VPN	+ Отдельный модуль, ПАК «Криптографический коммутатор»	- Не поддерживается	- Не поддерживается

№	Наименование критерия	АПКШ Континент 3.7	АПКШ Континент 3.6	АПКШ Континент 3.5
Аудит сетевой активности				
7.1	Наличие журнала IP-пакетов на криптошлюзе	+	+	+
7.2	Интегрированная система централизованного сбора и хранения журналов в СУБД	+ MSSQL 2005 Server x32; SQL Express 2008 x32/x64; MSSQL 2008 Server x32/x64; Oracle 11g x32	+ MSSQL 2005 Server x32; SQL Express 2008 x32/x64; MSSQL 2008 Server x32/x64; Oracle 11g x32	+ MS SQL Server 2000 SP3; MSDE 2000 SP3; MS SQL Server 2005; MSDE 2005; Oracle 11g
7.3	Формат журнала IP-пакетов	Внутренний	Внутренний	Внутренний
7.4	Возможность экспорта внутреннего журнала IP-пакетов, хранящегося на криптошлюзе	Возможен экспорт в XML	Возможен экспорт в XML	Возможен экспорт в XML
7.5	Сортировка и фильтрация сообщений в журнале IP-пакетов	+	+	+
7.6	Поддерживаемые ОС для установки ПУ ЦУС	ОС Windows: • Windows XP Professional SP3 x86/ x64; • Windows 2003 Server SP2 x86/x64; • Windows 2003 Server R2 SP2 x86/x64; • Windows Vista SP2 x86/ x64 (кроме всех выпусков Starter и • Home Edition); • Windows 2008 Server SP2 x86/x64; • Windows 2008 Server R2 SP1 x64; • Windows 7 SP1 x86/x64 (кроме всех выпусков Starter и • Home Edition); • Windows 8 x86/x64	ОС Windows • Windows XP Professional SP3 x86/x64; • Windows 2003 Server SP2 x86/x64; • Windows 2003 Server R2 SP2 x86/x64; • Windows Vista SP2 x86/ x64 (кроме всех выпусков Starter и Home Edition); • Windows 2008 Server SP2 x86/x64; • Windows 2008 Server R2 SP1 x64; • Windows 7 SP1 x86/x64 (кроме всех выпусков Starter и Home Edition)	ОС Windows • Windows XP Professional SP3; • Windows Vista SP1 (Business / Enterprise / Ultimate Edition); • Windows 2000 Professional SP4, Windows 2000 Server SP4; • Windows Server 2003 SP2; • Windows Server 2003 R2
Надежность				
8.1	Возможность работы в отказоустойчивом режиме кластера «горячего резервирования» с обеспечением автоматической синхронизации конфигураций и таблиц соединений между элементами кластера	+ Возможность назначения резервных интерфейсов синхронизации конфигураций элементов кластера	+ Возможность назначения резервных интерфейсов синхронизации конфигураций элементов кластера	+ Нет резервирования интерфейса синхронизации конфигураций элементов кластера
8.2	Резервирование внешнего канала связи с возможностью мониторинга состояния канала связи и автоматическим переключением на резервный канал в случае сбоя основного	+	+	--

№	Наименование критерия	АПКШ Континент 3.7	АПКШ Континент 3.6	АПКШ Континент 3.5
8.3	Среднее время наработки на отказ криптошлюза	40 000 ч.	40 000 ч.	10 000 ч.
8.4	Наличие у криптошлюза резервирования по питанию (2-х блоков питания)	+	+	+
Эксплуатационные характеристики				
9.1	Возможность работы в режиме замкнутой криптографической сети	**+** Добавлен режим замкнутой криптографической сети, запрещающий хождение незащищенного трафика	- Не поддерживается	- Не поддерживается
9.2	Возможность выполнения функций маршрутизатора (в т.ч. поддержка современных протоколов динамической маршрутизации OSPF, BGP, RIP)	+ OSPF, BGP, RIP. Централизованная настройка и мониторинг	+ OSPF, BGP, RIP. Централизованная настройка и мониторинг	- Ограниченная поддержка OSPF, требуется локальная настройка на КШ
9.3	Поддержка одновременной работы по нескольким каналам связи с возможностью разделения сетевого трафика для маршрутизации через разные (заранее заданные в настройках) внешние интерфейсы	+	+	-- Не поддерживается конфигурация мульти WAN, внешний интерфейс всегда один
9.4	Поддержка одновременной работы по нескольким каналам связи с возможностью балансировки исходящего сетевого трафика между внешними интерфейсами	+	+	-- Не поддерживается
9.5	Поддержка технологии NAT с гибкой настройкой правил (DNAT, NAT 1:1, PAT)	+	+	+/- С ограничениями
9.6	Поддержка мультикаст-маршрутизации (для обеспечения защиты трафика потоковой видеотрансляции)	+	+	- Не поддерживается
9.7	Поддержка QoS с возможностью классификации трафика (создание профилей трафика), маркировки IP-пакетов, управления и предупреждения перегрузок каналов связи с помощью очередей	+ Классификация трафика (максимальное количество классов 32); маркировка IP-пакетов; поле ToS (сохранение, заполнение классификатором DSCP, заполнение классификатором IPP); управление перегрузками с помощью очередей (методы PRIQ, CBQ, HFSC); защита от перегрузок (методы RED, RIO, ECN)	+ Классификация трафика (максимальное количество классов 32); маркировка IP-пакетов; поле ToS (сохранение, заполнение классификатором DSCP, заполнение классификатором IPP); управление перегрузками с помощью очередей (методы PRIQ, CBQ, HFSC); защита от перегрузок (методы RED, RIO, ECN)	- Ограничено (перенос IP TOS на зашифрованные пакеты)

№	Наименование критерия	АПКШ Континент 3.7	АПКШ Континент 3.6	АПКШ Континент 3.5
9.8	Поддержка возможности резервирования полосы пропускания (Traffic shaping)	+	+	- Не поддерживается
9.9	Возможность работы криптошлюза за NAT-устройствами	+	+	- КШ должен иметь «белый IP», работа КШ за NAT невозможна
9.10	Работа в режиме сервера IP-адресов для клиентских устройств (DHCP-сервер)	Да	- Не поддерживается	- Не поддерживается
9.11	Работа в режиме ретранслятора DHCP-сервера для конфигурирования IP-адресов клиентских устройств (DHCP relay)	Да	- Не поддерживается	- Не поддерживается
9.12	Возможность синхронизации времени ЦУС с NTP-серверами точного времени	Да	- Не поддерживается	- Не поддерживается
9.13	«Прозрачность» решения для пользовательских прикладных систем	+	+	+
9.14	Поддержка внешних 3G-модемов (USB) для подключения КШ через провайдеров сотовых сетей	Да	- Не поддерживается	- Не поддерживается
Программный VPN клиент (Абонентский пункт)				
10.1	Встроенный персональный МСЭ	+	+	+
10.2	Возможность запрета всех незащищенных соединений	+	+	+
10.3	Подключение по сетевому имени	Да	- Не поддерживается	- Не поддерживается
10.4	Использование протокола HTTPS	Да	- Не поддерживается	- Не поддерживается
10.5	Поддержка авторизации на прокси-сервере (HTTP)	Да	- Не поддерживается	- Не поддерживается
10.6	Возможность подключения до регистрации пользователя в ОС (позволяет рабочим станциям, входящим в домен, работать удаленно)	Да	- Не поддерживается	- Не поддерживается

№	Наименование критерия	АПКШ Континент 3.7	АПКШ Континент 3.6	АПКШ Континент 3.5
10.7	Поддерживаемые ОС	<u>ОС Windows</u> • Windows 8 x86/x64; • Windows 8.1 x86/x64; • Windows 7 SP1 x86/x64 (кроме всех выпусков Starter и Home Edition); • Windows Server 2008 R2 SP1 x64; • Windows Server 2008 SP2 x86/x64; • Windows Vista SP2 x86/x64 (кроме всех выпусков Starter и Home Edition); • Windows 2003 Server R2 SP2 x86/x64; • Windows 2003 Server SP2 x86/x64; • Windows XP Professional SP3 x86	<u>ОС Windows:</u> • Windows 7 SP1 x86/x64 (кроме всех выпусков Starter и Home Edition); • Windows 2008 Server R2 SP1 x64; • Windows 2008 Server SP2 x86/x64; • Windows Vista SP2 x86/x64 (кроме всех выпусков Starter и Home Edition); • Windows 2003 Server R2 SP2 x64; • Windows 2003 Server SP2 x86/x64; • Windows XP Professional SP3 x86	<u>ОС Windows:</u> • MS Windows Vista SP2; • MS Windows XP Professional SP3; • MS Windows 2000 Professional SP4
		<u>ОС Linux:</u> • Альт Линукс СПТ 6.0 Рабочая станция x86/x64. Альт Линукс СПТ 6.0 Сервер x86/x64; • Mandriva Spring 2008.1 x86	<u>ОС Linux:</u> • Альт Линукс СПТ 6.0 Рабочая станция x86/x64. Альт Линукс СПТ 6.0 Сервер x86/x64; • Mandriva Spring 2008.1 x86	
		<u>Мобильные ОС:</u> • Android 4.x, 5.x; • Apple iOS 6.x, 7.x, 8.x	<u>Мобильные ОС:</u> • Android 4.0.3; • Apple iOS 6.x, 7.x, 8.x	
Совместимость				
11.1	Возможность интеграции с внешними системами мониторинга по протоколу SNMP	+	+	+/- Трафик SNMP не отправляется в открытом виде, не попадает в VPN-туннель
11.2	Возможность интеграции с системами анализа трафика IPS/IDS в части передачи сетевого трафика на сенсоры систем IPS/IDS	+	+	+
11.3	Возможность интеграции с системами анализа и корреляции событий информационной безопасности (ArcSight)	+	+	+
Области применения				
12.1	Защита удаленного доступа к сети	+	+	+
12.2	Защита внешнего периметра сети	+	+	+

№	Наименование критерия	АПКШ Континент 3.7	АПКШ Континент 3.6	АПКШ Континент 3.5
12.3	Создание отказоустойчивой VPN сети	+ Автоматическое переключение на резервный канал связи с перестроением VPN-связей	+ Автоматическое переключение на резервный канал связи с перестроением VPN-связей	- Нет
12.4	Защита сетевого трафика в мультисервисных сетях (VoIP, Video conference)	+ Профили трафика, приоритезация и управление полосой пропускания	+ Профили трафика, приоритезация и управление полосой пропускания	Нет
12.5	Разделение сети на сегменты с различным уровнем доступа	+	+	+
12.6	Защита персональной рабочей станции (personal firewall)	+	+	+
Стоимость решения*				
13.1	Система лицензирования	Четыре типа лицензий: 1. Лицензия на подключение КШ к ЦУС. 2. Лицензия на подключения Континент АП к СД. 3. Лицензия на обновление версии ПО. 4. Лицензия на обновление БРП ДА. Отсутствуют лицензионные ограничения на количество туннелируемых IP-адресов, число одновременных пользовательских подключений, на количество экземпляров установленных ПУ ЦУС и ПУ СД	Три типа лицензий: 1. Лицензия на подключение КШ к ЦУС. 2. Лицензия на подключения Континент АП к СД. 3. Лицензия на обновление версии ПО. Отсутствуют лицензионные ограничения на количество туннелируемых IP-адресов, число одновременных пользовательских подключений, на количество экземпляров установленных ПУ ЦУС и ПУ СД	Два типа лицензий: 1. Лицензия на подключение КШ к ЦУС. 2. Лицензия на подключения Континент АП к СД. Отсутствуют лицензионные ограничения на количество туннелируемых IP-адресов, число одновременных пользовательских подключений, на количество экземпляров установленных ПУ ЦУС и ПУ СД
13.2	Стоимость административной компоненты ЦУС IPC-100	186 600 руб.	186 600 руб.	EoL
13.3	Стоимость КШ IPC-100	171 600 руб.	171 600 руб.	EoL
13.4	Стоимость КШ IPC-25	82 000 руб.	82 000 руб.	EoL

* Указана стоимость по прайсу производителя. Возможны скидки в зависимости от объема поставки.

Узнать условия приобретения и обновления с предыдущих версий АПКШ «Континент» вы можете в коммерческом отделе компании «Код Безопасности»: buy@securitycode.ru, +7 (495) 982-30-20.