



Код безопасности
ГК «Информзащита»

Сравнение функций МЭ, входящих в состав SSEP и АПКШ Континент, и МЭ TrustAccess

Как правильно выбрать продукт в линейке «Кода Безопасности», подходящий для решения задач организации?

Введение

Компания «Код Безопасности» – российский разработчик средств защиты информации. В продуктовой линейке «Кода Безопасности» присутствуют продукты, осуществляющие техническую защиту информации в информационных системах на основе технологии межсетевого экранирования. Это продукты Security Studio Endpoint Protection (SSEP),

TrustAccess и АПКШ «Континент». Целью данного документа является оказание помощи специалистам по информационным технологиям и специалистам по информационной безопасности при выборе решений «Кода Безопасности» на основе технологии межсетевого экранирования, подходящего для задач организации.

Различные задачи информационной безопасности, решаемые с помощью SSEP, TrustAccess и АПКШ «Континент»

Задача	Решение «Кода Безопасности»
Комплексная защита АРМ и серверов от внешних угроз (Firewall+HIPS+AV)	SSEP
Фильтрация интернет-трафика АРМ	SSEP
Проактивная защита АРМ	SSEP
Разграничение доступа к сетевым ресурсам в условиях терминальной среды	SSEP, TrustAccess, АПКШ «Континент»
Защищенное межсетевое взаимодействие в клиент-серверных и многозвенных системах	TrustAccess, АПКШ «Континент»
Защита виртуальных машин	SSEP, TrustAccess
Защита внутренних сегментов сети от несанкционированного доступа извне	АПКШ «Континент»
Межсетевое экранирование в виртуальной среде	TrustAccess, SSEP
Объединение через Интернет локальных сетей предприятия в единую сеть VPN	АПКШ «Континент»
Подключение удаленных и мобильных пользователей к VPN по защищенному каналу	АПКШ «Континент»
Организация защищенного взаимодействия со сторонними организациями	АПКШ «Континент»
Скрытие внутренней структуры защищаемых сегментов сети	АПКШ «Континент»
Разграничение сетевого доступа пользователей к серверу	АПКШ «Континент», TrustAccess
Сегментирование АС	АПКШ «Континент», TrustAccess

Решения Security Studio Endpoint Protection (SSEP), TrustAccess и АПКШ «Континент» основаны на следующих технологиях:

Технология	Решение «Кода Безопасности»
Межсетевой экран	SSEP, TrustAccess, АПКШ «Континент»
HIPS/IDS	SSEP
VPN шлюз	АПКШ «Континент»
Antivirus	SSEP
Маршрутизатор	АПКШ «Континент»

Как видно из таблицы эти решения объединяет наличие межсетевого экрана (МЭ) в составе. Если в решениях SSEP и АПКШ «Континент» МЭ – это одна

из функциональных частей, то TrustAccess – это полнофункциональное решение класса МЭ.

Сравнительная характеристика функциональных возможностей МЭ в продуктах SSEP, TrustAccess и АПКШ «Континент»

Таблица 2

В таблице приведена сравнительная характеристика функциональных возможностей МЭ в составе продуктов SSEP, TrustAccess и АПКШ «Континент».

Функции межсетевого экрана	Security Studio Endpoint Protection 6	TrustAccess 1.1	АПКШ Континент 3.5	Континент -АП
Настройка правил фильтрации				
Настройка режима (политики) безопасности	√	√	√	√
Настройка правил для пакетов	√	√	√	√
Типовые наборы правил фильтрации	√	√	√	√
Контроль активности ICMP	√	√	√	√
Механизм защиты от сетевых сбоев		√	√	
Настройка правил для прикладных протоколов		√	√	√
Фильтрация на транспортном уровне запросов на установление виртуальных соединений		√	√	√
Расписание применения правил	√*	√	√	√
Возможность задания реакции на срабатывание правил		√		
Режим обучения	√			
Настройка правил для приложений	√			
Криптографическая защита				
Сжатие передаваемых пакетов			√	
Имитозащита пакетов в VPN			√	
Криптографическое преобразование пакетов			√	
Аутентификация				
Аутентификация абонентов. Поддержка правил для пакетов на основе ID-отправителя		√	√	√
Группы пользователей. Поддержка групп пользователей в правилах	√*	√	√	√
Сетевая защита				
Правила трансляции сетевых адресов (NAT) для входящих и исходящих пакетов			√	
Скрытие внутренней структуры защищаемого сегмента сети методом инкапсуляции передаваемых пакетов			√	
Защита сетевых пакетов от модификации		√	√	
Защита сетевых пакетов от перехвата		√	√	
Защита сетевых пакетов от replay атак		√		
Система обнаружения сетевых атак (IDS)	√			
Система предотвращения вторжений на хост (HIPS)	√			
Централизованное управление клиентскими компьютерами				
Парольная защита администрирования	√	√	√	√
Гранулярность удаленной настройки до уровня шаблона правил	√	√	√	

* С помощью Administration Center

Функции межсетевого экрана	Security Studio E n d p o i n t Protection 6	TrustAccess 1.1	АПКШ Континент 3.5	Континент -АП
Журнал сетевой активности	√	√	√	√
Гранулярность удаленной настройки до уровня правила		√	√	
Развертывание клиентской части через Active Directory	√	√		
инструмент для централизованного развертывания клиентской части	√			
Сертификаты ФСТЭК России				
МЭ4/НДВ4	√			√
МЭ2/НДВ4		√		
МЭ3/НДВ3			√	
МЭ4/НДВ3				√
МЭ2/НДВ2		√		
HIPS (ТУ/НДВ4)	√			
Antivirus (ТУ/НДВ4)	√			
Сертификаты ФСБ России				
КС1				√
КС2			√	√
КВ2			√	
МЭ4			√	√
ГОСТ Р (РОСТЕСТ)				
ГОСТ Р МЭК 60950-1-2005; ГОСТ Р 5131822-99; ГОСТ Р 51318.24-99; ГОСТ Р 51317.3.2-2006 (Разд. 6. 7.)			√	
Подтверждение совместимости				
Сертификация ПО в Microsoft		√		
Сертификация ПО в VMware (VMware Ready!)		√		
Поддерживаемые платформы				
Windows 2000	√	√	√	√
Windows 2000 Server		√	√	√
Windows XP	√	√	√	√
Windows 2003	√	√	√	√
Windows Vista	√	√	√	√
Windows 2003 R2		√	√	√
Windows 7		√		
Windows 2008	√	√		
Windows 2008 R2		√		

Использование SSEP, TrustAccess и АПКШ «Континент» в ИСПДн и АС разного класса

Таблица 3

В таблице показано, какой именно стоит выбрать продукт в зависимости от вида информации, которую необходимо защитить:

Виды защищаемой информации	Security Studio Endpoint Protection 6	TrustAccess 1.1	АПКШ «Континент»	Континент-АП
Персональные данные				
К1	√*	√	√	√
К2	√	√	√	√
К3	√	√	√	√
Сведения, составляющие государственную тайну				
Секретно		√	√	
Совершенно секретно		√		
Конфиденциальная информация (ДСП)	√	√	√	√

Выполнение требований ФСТЭК к ИСПДн с помощью SSEP, TrustAccess и АПКШ «Континент»

Таблица 4

В следующей таблице показано, какие именно классы требований к системе защиты персональных данных (на основании приказа ФСТЭК 58) можно закрыть с помощью соответствующего продукта:

Классы требований защиты ПДн	Security Studio Endpoint Protection 6	TrustAccess 1.1	АПКШ «Континент»	Континент-АП
Подсистема межсетевого экранирования	√	√	√	√
Подсистема управления доступом		√	√	√
Подсистема регистрации и учета	√	√	√	√
Подсистема антивирусной защиты	√			
Подсистема обнаружения вторжений	√			

Использование SSEP, TrustAccess и АПКШ «Континент» в АС разного класса

Таблица 5

Выбор продукта в зависимости от классификации АС:

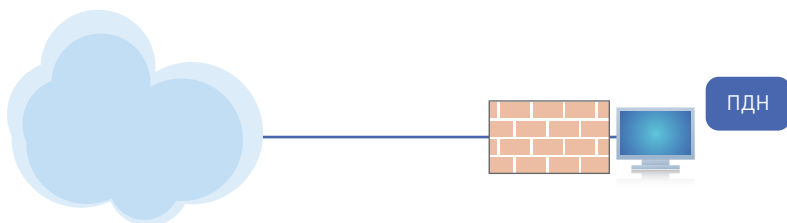
Класс АС	Security Studio Endpoint Protection 6	TrustAccess 1.1	АПКШ «Континент»	Континент-АП
1Д	√	√	√	√
1Г	√	√	√	√
1В		√	√	
1Б		√		

* Может применяться для защиты ИСПДн К1 с ограничением: при подключении к сетям общего пользования в ИСПДн К1 необходимо использовать «Континент» на периметре организации. В этом случае SSEP МЭ обеспечивает защиту от сотрудников, которые не имеют прав доступа к ИСПДн.

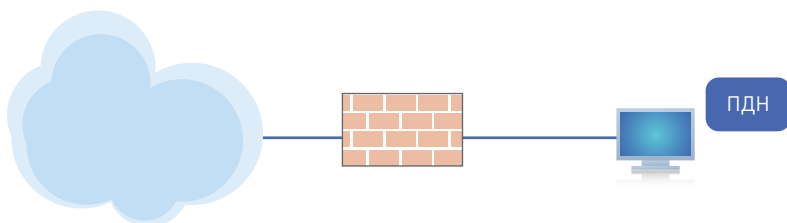
Выбор МЭ по вариантам расположения в сети

Ниже приведены основные варианты расположения продуктов SSEP, TrustAccess и АПКШ «Континент» в ИСПДн.

Security Studio Endpoin Protection: Personal Firewall, установленный на АРМ, на котором обрабатываются ПДн



АПКШ «Континент»: МЭ, отделяющий защищаемый узел от сети общего пользования



TrustAccess: распределенный МЭ, установленный на сервер в ЛВС, содержащий ПДн



Коротко о TrustAccess

TrustAccess – распределенный межсетевой экран с централизованным управлением, агенты которого функционируют непосредственно на защищаемых компьютерах (серверах и рабочих станциях). Решение имеет широкий функционал защиты сетевых соединений, который включает аутентификацию участников сетевых соединений, защиту трафика от подмены пакетов, гибкие настройки правил фильтрации и т.п. TrustAccess можно применять для защиты множества типов данных ограниченного доступа (от персональных данных до гостайны). Защита TrustAccess эффективна в условиях терминальной или виртуальной среды – распределенный межсетевой

экран с централизованным управлением, агенты которого функционируют непосредственно на защищаемых компьютерах (серверах и рабочих станциях). Решение имеет широкий функционал защиты сетевых соединений, который включает аутентификацию участников сетевых соединений, защиту трафика от подмены пакетов, гибкие настройки правил фильтрации и т.п. TrustAccess можно применять для защиты множества типов данных ограниченного доступа (от персональных данных до гостайны). Защита TrustAccess эффективна в условиях терминальной или виртуальной среды.

Коротко о Security Studio Endpoint Protection

Security Studio Endpoint Protection (SSEP) – сертифицированное комплексное программное решение, обеспечивающее полную защиту автоматизированного рабочего места (АРМ) от внешних угроз в соответствии с требованиями ФСТЭК в области защиты персональных данных. SSEP является полноценным

решением, способным решить весь спектр задач по защите компьютера в корпоративной сети от внешних угроз. Входящий в состав SSEP инструмент для централизованного развертывания и управления клиентской частью, позволяет эффективно контролировать систему защиты корпоративной сети.



Код безопасности

ГК «Информзащита»

Почтовый адрес: 127018, Россия, Москва, а/я 55.

Адрес офиса в Москве: ул. Образцова, д. 38.

Адрес офиса в Санкт-Петербурге: Свердловская наб., д. 44.

Тел.: +7 (495) 980-2345 (многоканальный).

Факс: +7 (495) 980-2345.

E-mail: info@securitycode.ru

Запрос дополнительной информации о продуктах: info@securitycode.ru

По вопросам стоимости и покупки продуктов sales@securitycode.ru

По вопросам партнерства и сотрудничества info@securitycode.ru

Вы можете узнать подробную информацию о продуктах на сайте

www.securitycode.ru

О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, коммерческой и государственной тайны, а также среды виртуализации. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

«Код Безопасности» входит в группу компаний «Информзащита», которая уже около 15 лет является лидером российского рынка информационной безопасности.

ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России.