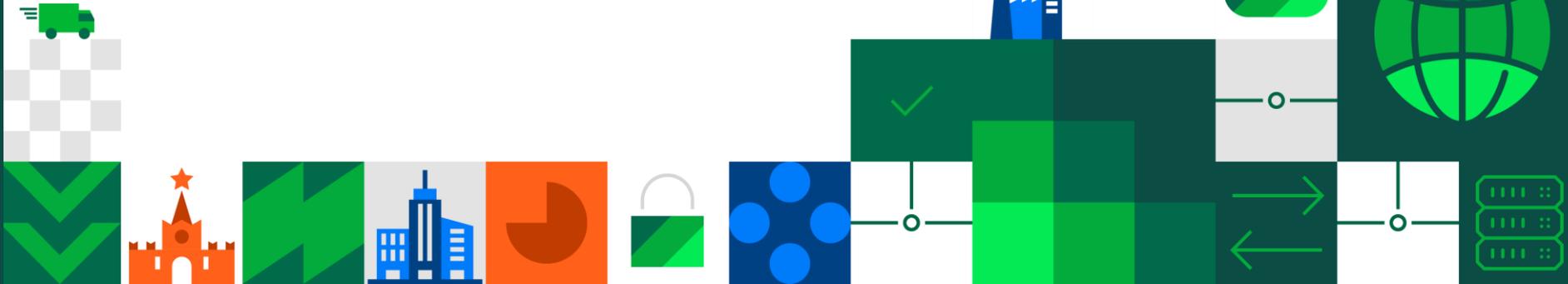




Практика миграции с иностранных NGFW: Документация, сценарии, кейсы

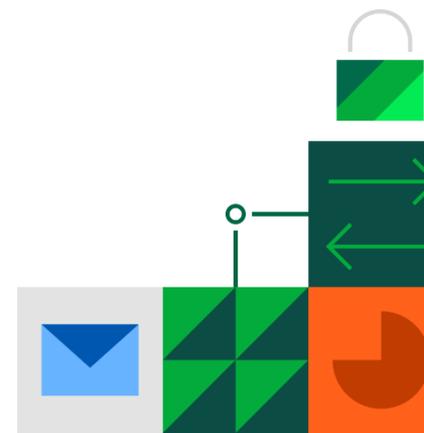


1. Код Безопасности:

- Проблема импортозамещения на рынке сетевой безопасности
- Континент 4
- Рекомендации по тестированию и внедрению Континент 4

2. ТС Солюшен:

- Почему заказчики выбирают Континент 4
- Варианты миграции с иностранных NGFW на Континент 4
- Демонстрации миграции с Check Point на Континент 4





Важна не сама технология, а закрываемые потребности



Функции

Централизованное управление

Эргономика

Контроль приложений

Защита от вторжений и вредоносного ПО

Масштабируемость и отказоустойчивость

VPN и удаленный доступ

Расшифровка трафика

Сетевые функции

Сценарии использования

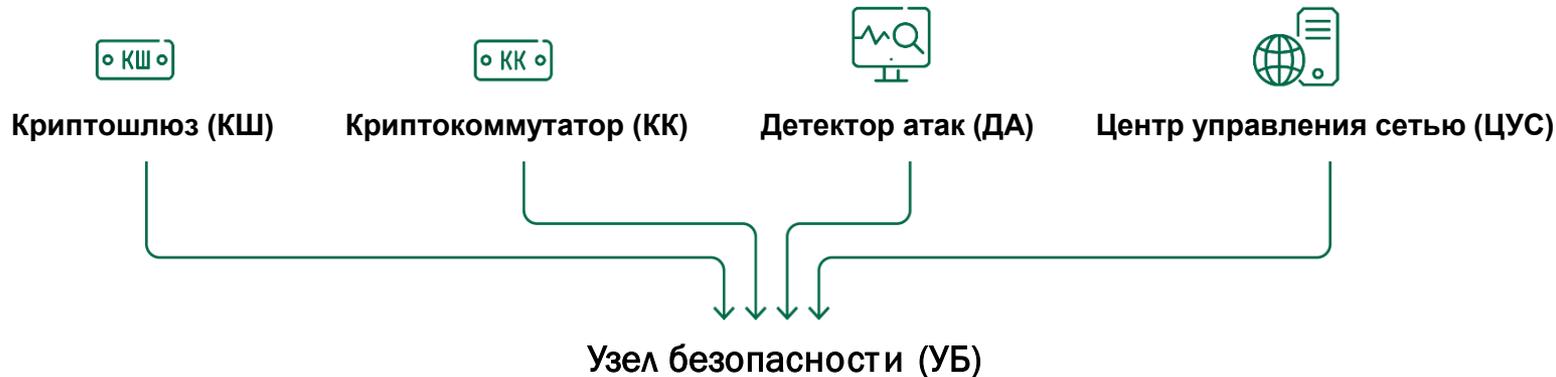
В датацентре организации

На периметре организации

В геораспределенной сети

Для малого и среднего
бизнеса

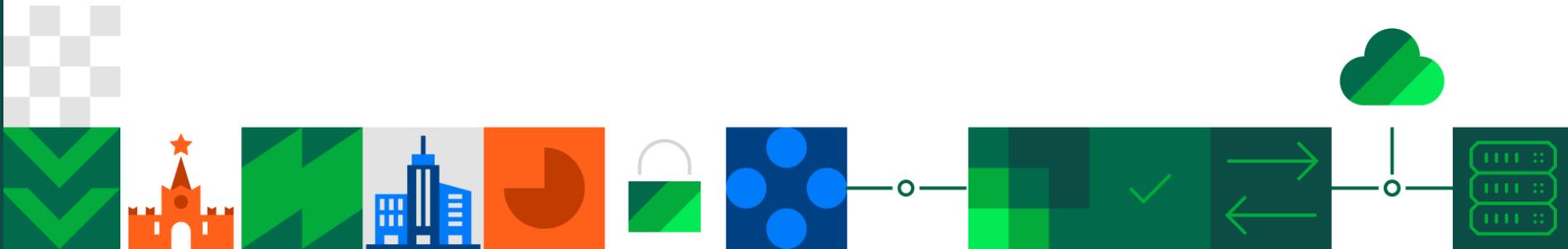


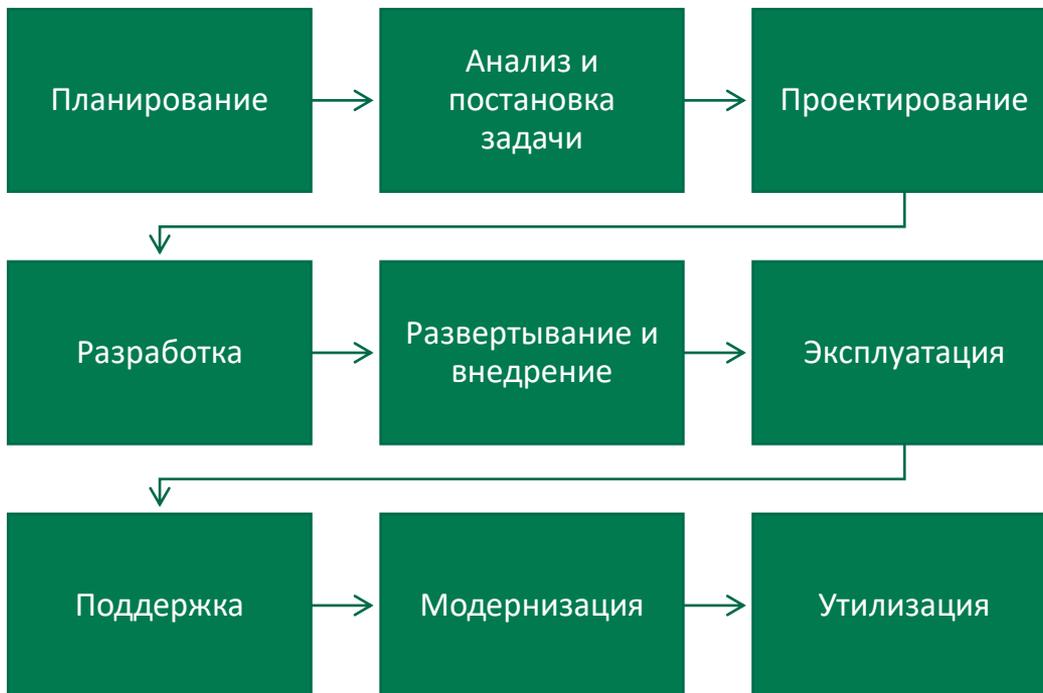


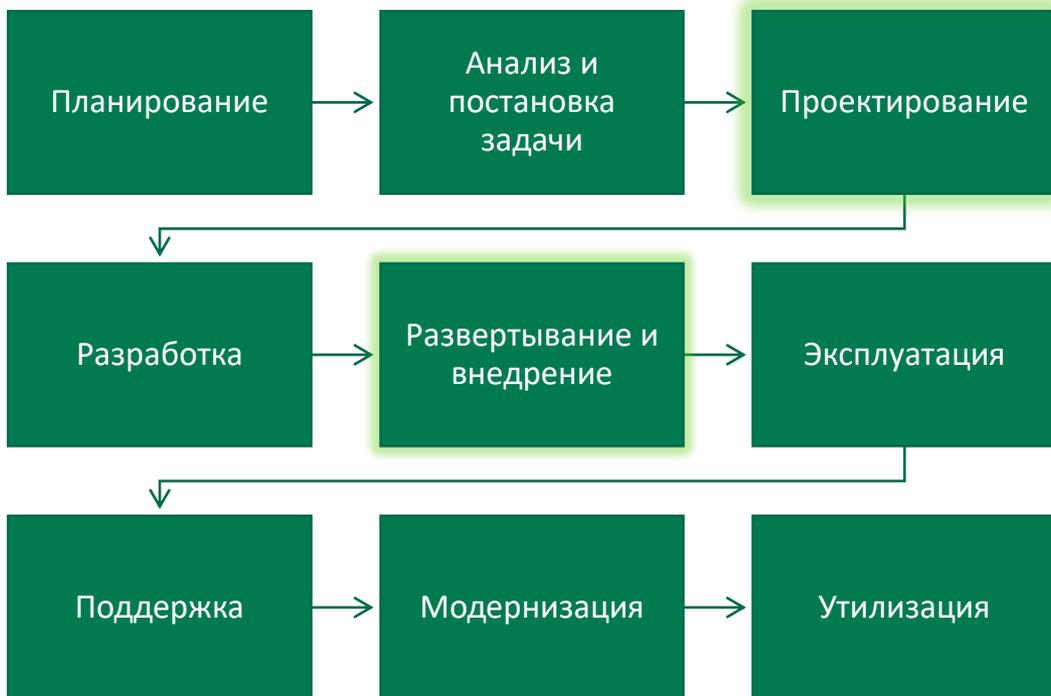
- FW
- IPS
- App control
- L2 VPN
- L3 VPN
- MGMT
- Threat Intelligence
- Log
- URL Filtering
- User Identity
- Antivirus
- GeoIP



Процессы внедрения и тестирования







Проектирование:

1. Пояснительная записка
2. Входные и выходные данные системы
3. Схема функциональной структуры
4. Описание автоматизируемых функций
5. Постановка задач и алгоритмы решения
6. Программное обеспечение
7. Информационное обеспечение
8. Комплекс технических средств системы

Развертывание и внедрение:

1. Закупка и настройка требуемой ИТ-инфраструктуры
2. Обучение пользователей
3. Развертывание системы на рабочих местах
4. Основные виды тестирования
5. Опытно-промышленная эксплуатация
6. Приемо-сдаточные испытания

Проектирование:

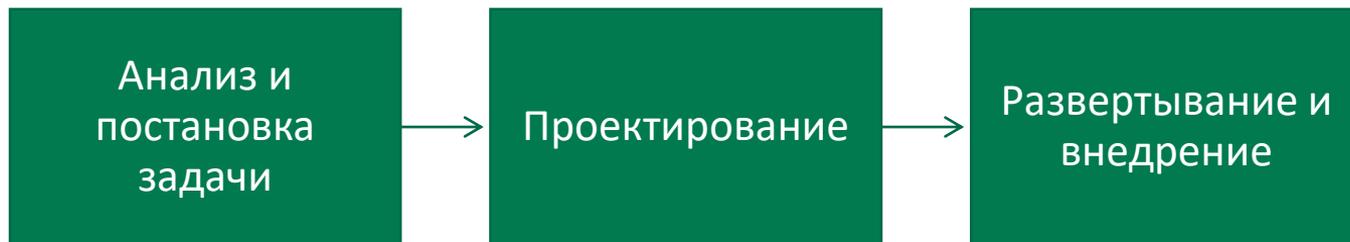
1. Пояснительная записка
2. Входные и выходные данные системы
3. Схема функциональной структуры
4. Описание автоматизируемых функций
5. Постановка задач и алгоритмы решения
6. Программное обеспечение
7. Информационное обеспечение
8. Комплекс технических средств системы

Развертывание и внедрение:

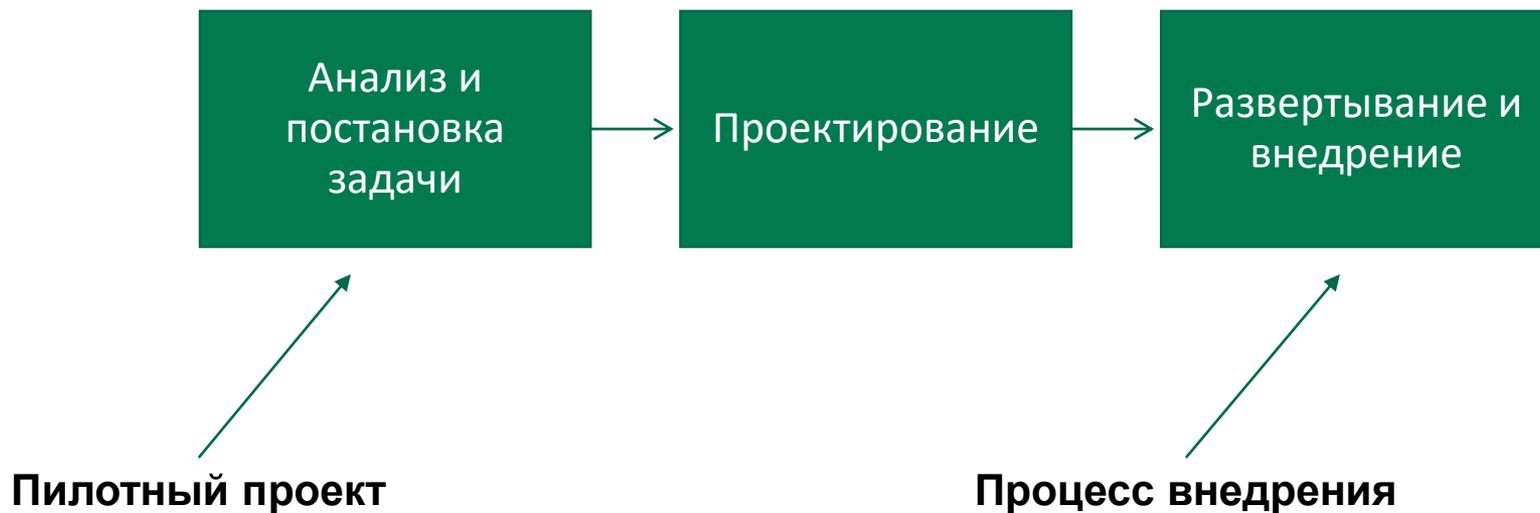
1. Закупка и настройка требуемой ИТ-инфраструктуры
2. Обучение пользователей
3. Развертывание системы на рабочих местах
4. Основные виды тестирования
5. Опытно-промышленная эксплуатация
6. Приемо-сдаточные испытания

Что если что-то пойдет не так?

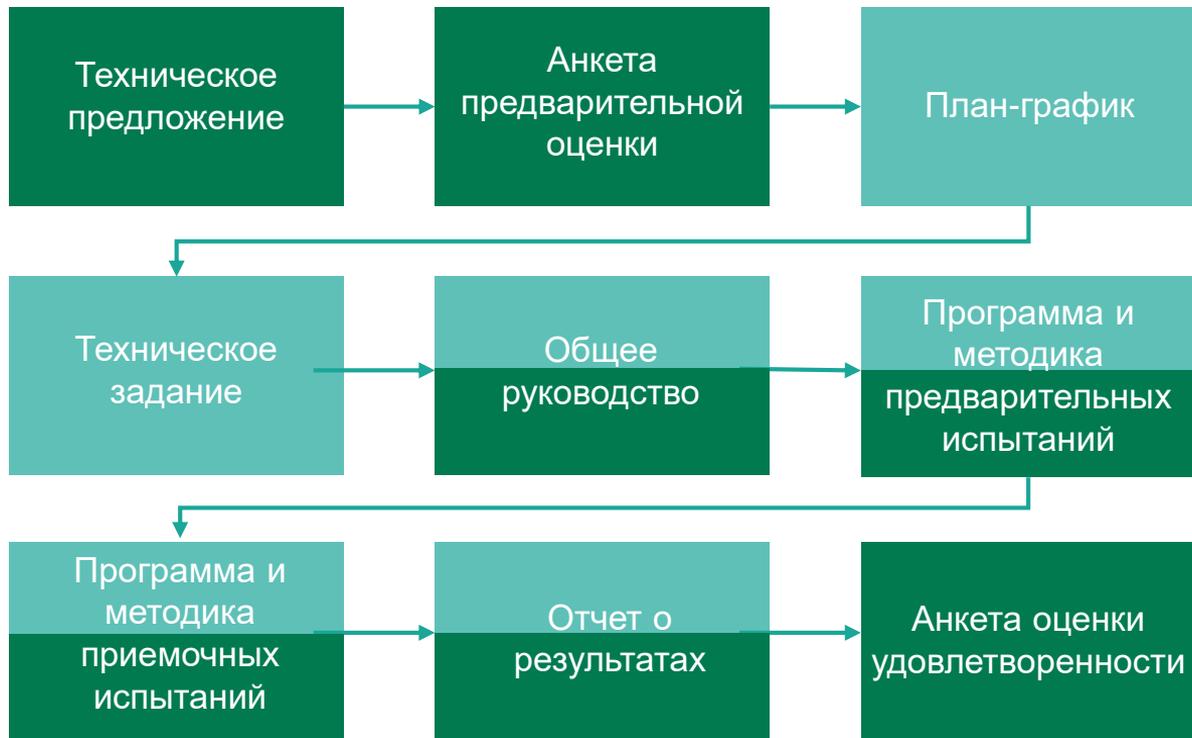
Оценка применимости решения
должна происходить здесь



Оценка применимости решения
должна происходить здесь

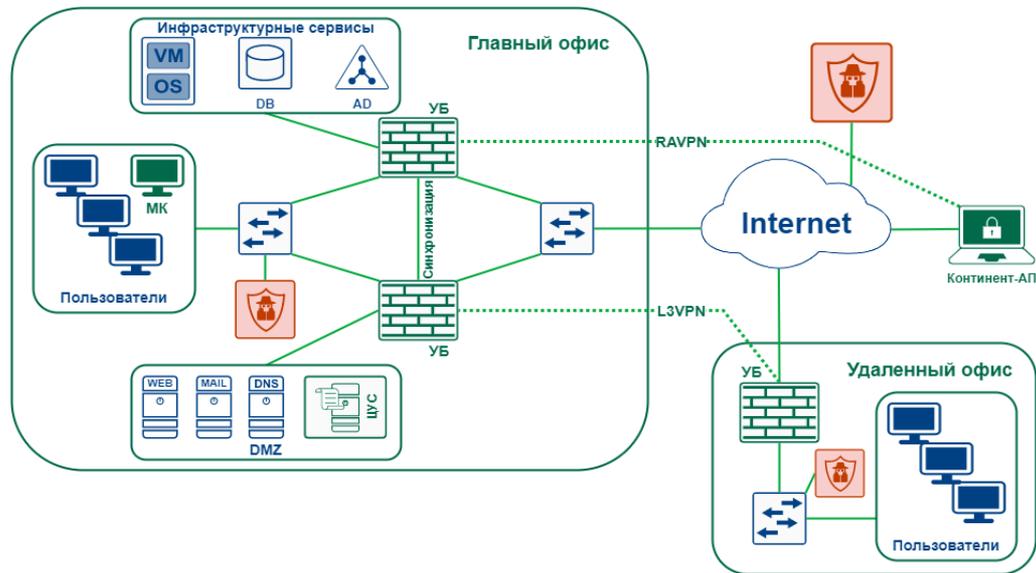


Внедрение
Пилотный проект



Цель – предоставить Заказчику информацию по проведению пилотного проекта

- Цели пилотного проекта
- Задачи в рамках пилотного проекта
- Описание комплекса Континент 4
- Этапность пилотного проекта
- Рекомендации по организации
- Сбор требований и согласование варианта использования
- Описание пилотной зоны



Цель – сбор информации, требующейся при подготовке к проведению пилотного проекта:

- Сведения об организации
- Планируемые сроки проведения проекта
- Цели и задачи
- Сведения об инфраструктуре
- Техническая информация

Цели и задачи		
1	Демонстрация функциональности продукта на стенде	<input type="checkbox"/> Требуется
2	Интеграция продукта в пилотной зоне с реальной инфраструктурой	<input type="checkbox"/> Требуется
3	Имитация в пилотной зоне угроз безопасности и их предотвращение с помощью продукта	<input type="checkbox"/> Требуется
4	Подтверждение количественных характеристик продукта	<input type="checkbox"/> Требуется
5	Иное	



Цель – сбор информации, требующейся при подготовке к проведению пилотного проекта:

- Сведения об организации
- Планируемые сроки проведения проекта
- Цели и задачи
- Сведения об инфраструктуре
- Техническая информация

Цели и задачи		
1	Демонстрация функциональности	
Основные параметры		
1	Предполагаемый вариант использования	<input type="checkbox"/> Сегментация внутренней сети <input type="checkbox"/> Контроль доступа в интернет <input type="checkbox"/> Построение VPN
2	Исполнение	<input type="checkbox"/> Аппаратное <input type="checkbox"/> Виртуальное
3	Отказоустойчивость	<input type="checkbox"/> Узлов безопасности <input type="checkbox"/> Сетевых портов <input type="checkbox"/> Серверов управления <input type="checkbox"/> Блоков питания <input type="checkbox"/> Внешних каналов связи
4	Сетевые порты	1000Base-T – ____ шт. <input type="checkbox"/> Трансиверы 1000Base-SX – ____ шт. <input type="checkbox"/> Трансиверы 10GBase-SR – ____ шт. <input type="checkbox"/> Трансиверы
5	Кабели питания	<input type="checkbox"/> Евровилка <input type="checkbox"/> IEC-320-C14



Цель – сбор информации, требующейся при подготовке к проведению пилотного проекта:

- Сведения об организации
- Планируемые сроки проведения проекта
- Цели и задачи
- Сведения об инфраструктуре
- Техническая информация

Цели и задачи		
1	Демонстрация функциональности	
Основные параметры		
1	Предполагаемый вариант использования	<input type="checkbox"/> Сегментация внутренней сети <input type="checkbox"/> К...
Функциональные возможности		
1	Межсетевое экранирование	<input type="checkbox"/> Расширенный DPI <input type="checkbox"/> URL-фильтрация <input type="checkbox"/> Антивирус
		<input type="checkbox"/> Geo Protection <input type="checkbox"/> IPS <input type="checkbox"/> Защита от DDoS
2	Криптографическая защита передаваемых данных	<input type="checkbox"/> L3VPN <input type="checkbox"/> L2VPN <input type="checkbox"/> Удаленный доступ
3	Сетевая функциональность	<input type="checkbox"/> QoS <input type="checkbox"/> NAT <input type="checkbox"/> Идентификация пользователей <input type="checkbox"/> DHCP <input type="checkbox"/> ICAP
		<input type="checkbox"/> Динамическая маршрутизация <input type="checkbox"/> SNMP <input type="checkbox"/> NetFlow <input type="checkbox"/> Syslog <input type="checkbox"/> Multi-WAN



№	Этап	Работы	Ответственный	Длительность
Подготовительные мероприятия				
...	Анкетирование и интервьюирование	Заполнение Заказчиком анкеты предварительной оценки объема пилотного проекта и рассмотрение ее Исполнителем. Или интервьюирование Заказчика по анкете в рамках очной встречи. Уведомление Исполнителем компании «Код Безопасности» о факте проведения пилотного проекта	Исполнитель и Заказчик	
...
Основные мероприятия				
...	Подготовка инфраструктуры	Согласование адресного плана пилотной зоны. Выделение технических средств, необходимых для пилотной зоны. Подготовка и настройка аппаратного и программного обеспечения в пилотной зоне.	Заказчик	
...
Завершающие мероприятия				
...	Подготовка отчета по результатам пилотного проекта	Подготовка отчета с результатами проверок, проведенных согласно утвержденной методике. Предоставление рекомендаций по внедрению комплекса	Исполнитель	
...

Цель – предоставить
Заказчику требования к
Континент 4 и на состав и
содержание работ.

Составляется на основе
технического предложения.

Содержание	
1 Общие сведения	5
1.1 Полное наименование системы и ее условное обозначение	5
1.2 Наименование предприятий разработчика и заказчика системы и их реквизиты	5
1.3 Перечень документов, на основании которых создается система	5
1.4 Плановые сроки начала и окончания работ по созданию системы	5
1.5 Сведения об источниках и порядке финансирования работ	5
1.6 Порядок оформления и предъявления Заказчику результатов работ	5
2 Назначение и цели создания системы	6
2.1 Назначение системы	6
2.2 Цели создания системы	6
3 Характеристика объекта автоматизации	7
4 Требования к системе	9
4.1 Общие требования	9
4.1.1 Требования к структуре и функционированию системы	9
4.1.2 Требования к численности и квалификации персонала системы и режиму его работы	11
4.1.3 Требования к показателям назначения	11
4.2 Требования к функциям (задачам), выполняемым системой	12
4.2.1 Требования к подсистеме фильтрации	12
4.2.2 Требования к подсистеме обнаружения вторжений	12
4.2.3 Требования к подсистеме шифрования	12
4.2.4 Требования к подсистеме централизованного управления и мониторинга	13
4.3 Требования к видам обеспечения	14
4.3.1 Требования к лингвистическому обеспечению системы	14
4.3.2 Требования к программному обеспечению системы	14
4.3.3 Требования к техническому обеспечению системы	14
5 Состав и содержание работ	15
6 Порядок контроля и приемки системы	17
6.1 Предварительные испытания	17
6.2 Опытная эксплуатация	17
6.3 Приемочные испытания	18
7 Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие	19
8 Требования к документированию	20
9 Источники разработки	21



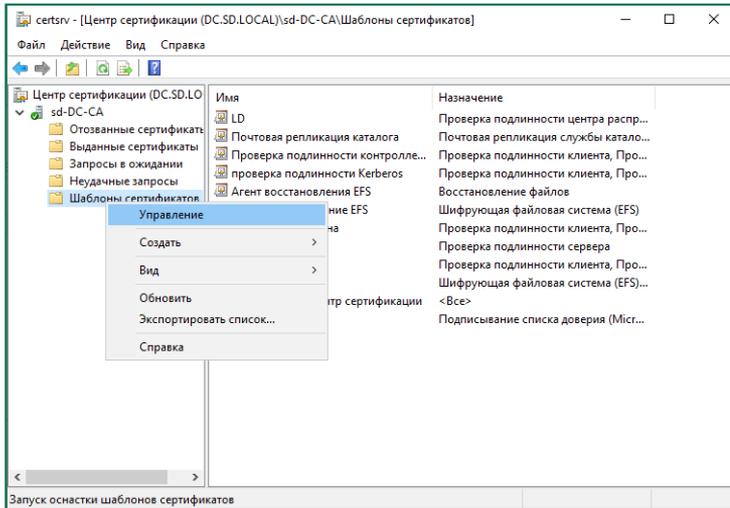
Цель – предоставить описание процесса подготовки и проведения пилотного проекта/ внедрения.

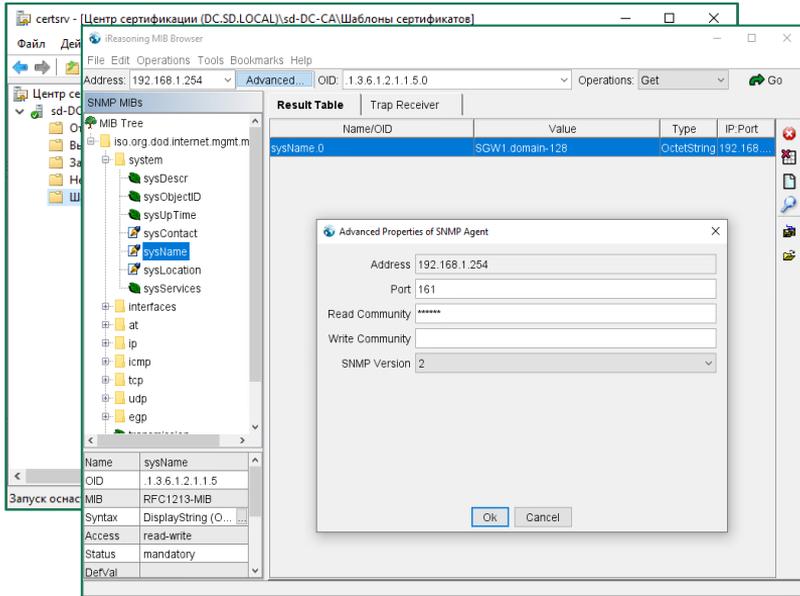
Содержит поэтапное описание настроек Континент 4 и смежного оборудования/ПО для пилотного проекта/внедрения.

Оглавление

Введение	5
Подготовка пилотной зоны	6
Коммутация и маршрутизация.....	8
Серверная инфраструктура	10
Пользовательские рабочие места	14
Узлы комплекса безопасности.....	15
Подготовка общефункциональных тестов	16
Сетевые возможности	16
Регистрация событий	22
Управление системой	24
Подготовка к тестированию безопасности	26
Межсетевое экранирование	26
Обнаружение и предотвращение вторжений	28
Защищенная передача данных.....	30
Подготовка тестов на производительность	33
Рекомендации по профилированию трафика	33
Настройка генератора	37
Настройка профиля трафика на генераторе	38
Фиксация результатов	45
Проведение тестирования и отчетность	46
Предварительные проверки и проведение демонстрации	46
Сопровождение	46
Подготовка отчета	46
Приложение	47
Протоколы и порты	47
Пример конфигурационного файла TRex.....	48
Пример импортируемых пользовательских сигнатур	49







The screenshot shows the iReasoning MIB Browser interface. The main window displays a tree view of SNMP MIBs, with the 'sysName' MIB selected. The 'Result Table' shows the following data:

Name/OID	Value	Type	IP:Port
sysName.0	SGW1.domain-128	OctetString	192.168...

An 'Advanced Properties of SNMP Agent' dialog box is open, showing the following configuration:

- Address: 192.168.1.254
- Port: 161
- Read Community: *****
- Write Community: *****
- SNMP Version: 2

Buttons: Ok, Cancel



Скриншоты интерфейса системы мониторинга. Вверху показаны панели инструментов и меню. В центре — панель «Result Table» с данными о трафике. Внизу — таблица правил мониторинга.

№	Название	Отправитель	Получатель	Сервис	Протокол/приложение	Действие	Профиль	COB	Временной интервал	Лог	Установить	Описание
1	CCM	CCM	NCC	* Любой	* Любое	Пропустить	* Не задан	Выкл	* Всегда	Нет	SGWC	
2	Ping	* Любой	* Любой	ICMP Echo ICMP Echo Reply	* Любое	Пропустить	* Не задан	Вкл	* Всегда	Нет	Безде	
3	DNAT bWAPP	* Любой	10.0.0.254	8080/TCP	* Любое	Пропустить	* Не задан	Выкл	* Всегда	Нет	SGWC	
4	bWAPP	* Любой	bWAPP	* Любой	* Любое	Пропустить	* Не задан	Вкл	* Всегда	Нет	Безде	
5	Block US	* Любой	Соединенные Штаты	* Любой	* Любое	Отбросить	* Не задан	Выкл	* Всегда	Лог	SGWC	
6	Block roskomsvoboda.org	* Любой	roskomsvoboda.org	* Любой	* Любое	Отбросить	* Не задан	Выкл	* Всегда	Лог	SGWC	
7	Users HTTP	Пользователи	* Любой	HTTP	* Любое	Фильтра...	Users HTTP	Выкл	* Всегда	Лог	SGWC	
8	Users HTTPS	Пользователи	* Любой	TLS	* Любое	Фильтра...	Users HTTPS	Выкл	* Всегда	Лог	SGWC	
9	Block Apps	* Любой	* Любой	* Любой	AnyDesk VNC	Отбросить	* Не задан	Выкл	* Всегда	Лог	SGWC	
10	Admins&Services	192.168.1.0/24 192.168.2.0/24	* Любой	* Любое	* Любое	Пропустить	* Не задан	Вкл	* Всегда	Нет	SGWC	
11	iPerf	192.168.1.0/24 192.168.3.0/24	192.168.1.0/24 192.168.3.0/24	IPERF	* Любое	Пропустить	* Не задан	Выкл	* Всегда	Нет	SGWC	
12	DNS	* Любой	* Любой	DNS	* Любое	Пропустить	* Не задан	Выкл	* Всегда	Нет	Безде	
13	NTP	* Любой	* Любой	NTP	* Любое	Пропустить	* Не задан	Выкл	* Всегда	Нет	Безде	
14	TRex	10.0.0.32 192.168.3.32 192.168.4.32	10.0.0.32 192.168.3.32 192.168.4.32	* Любой	* Любое	Пропустить	* Не задан	Вкл	* Всегда	Нет	Безде	



Центр сертификации (DC:SD.LOCAL)\sd-DC-CA\Шаблоны сертификатов

File Edit Operations Tools Bookmarks Help

Address: 192.168.1.254 Advanced... OID: 1.3.6.1.2.1.1.5.0 Operations

SNMP MIBs

Name/OID	Value
sysName.0	SGW1.domain-128

Виртуальные частные сети (1)

Поиск...

Топология	Состав	Защищаемые ресурсы
Corporation		
Полносвязная сеть	<ul style="list-style-type: none"> SGW3 192.168.4.0/24 SGWC 192.168.1.0/24 192.168.2.0/24 192.168.3.0/24 	

№	Название	Отправитель	Получатель	Сервис	Протокол/приложение	Действие	Профиль	COB	Временной интервал	Лог	Установить	Описание
1	CCM	CCM	NCC	* Любая	* Любая	Пропустить	* Не задан	- Выкл	* Всегда	- Нет	<input type="checkbox"/> SGWC	
2	Ping	* Любая	* Любая	ICMP Echo	ICMP Echo Request							
3	DNAT bWAPP	* Любая	10.0.0.254	8080/TCP								
4	bWAPP	* Любая	bWAPP	* Любая								
5	Block US	* Любая	Соединенные Штаты	* Любая								
6	Block roscomsvoboda.org	* Любая	roscomsvoboda.org	* Любая								
7	Users HTTP	<input checked="" type="checkbox"/> Пользователи	* Любая	HTTP								
8	Users HTTPS	<input checked="" type="checkbox"/> Пользователи	* Любая	TLS								
9	Block Apps	* Любая	* Любая	* Любая								
10	Admins&Services	<input checked="" type="checkbox"/> 192.168.1.0/24 <input checked="" type="checkbox"/> 192.168.2.0/24	* Любая	* Любая								
11	iPerf	<input checked="" type="checkbox"/> 192.168.1.0/24 <input checked="" type="checkbox"/> 192.168.3.0/24	<input checked="" type="checkbox"/> 192.168.1.0/24 <input checked="" type="checkbox"/> 192.168.3.0/24	IPERF								
12	DNS	* Любая	* Любая	DNS	* Любая	Пропустить	* Не задан	- Выкл	* Всегда	- Нет	* Безде	
13	NTP	* Любая	* Любая	NTP	* Любая	Пропустить	* Не задан	- Выкл	* Всегда	- Нет	* Безде	
14	TPex	<input checked="" type="checkbox"/> 10.0.0.32 <input checked="" type="checkbox"/> 192.168.3.32 <input checked="" type="checkbox"/> 192.168.4.32	<input checked="" type="checkbox"/> 10.0.0.32 <input checked="" type="checkbox"/> 192.168.3.32 <input checked="" type="checkbox"/> 192.168.4.32	* Любая	* Любая	Пропустить	* Не задан	<input checked="" type="checkbox"/> Вкл	* Всегда	- Нет	* Безде	

Кластер безопасности - SGWC

- Кластер безопасности
 - Состав
 - Диагностика
 - Идентификация пользователей
 - Сервер доступа**
 - Интерфейсы
 - Multi-WAN
 - Межсетевой экран
- Журналирование и оповещения
 - Локальное хранилище
 - Внешнее хранилище
 - DNS

Серверы DNS

Предпочитаемый:

Альтернативный 1:

Альтернативный 2:

Домен:

Пул адресов API

Адреса:



Центр сертификации (DC.SD.LOCAL)\sd-DC-CA\Шаблоны сертификатов

Address: 192.168.1.254 | Advanced... | OID: 1.3.6.1.2.1.1.5.0 | Operations

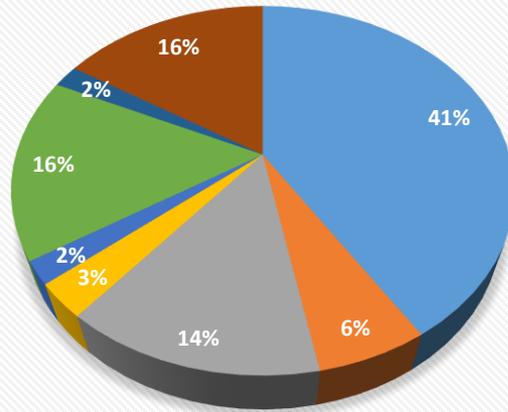
SNMP MIBs	Result Table	Trap Receiver
MIB Tree	Name/OID	Value
iso.org.dod.internet.mgmt.mib	sysName.0	SGW1.domain-128

Виртуальные частные сети (1)

Поиск...

Топология	Состав	Защищаемые ресурсы
Corporation	<ul style="list-style-type: none"> SGW3 SGWC 	<ul style="list-style-type: none"> 192.168.4.0/24 192.168.1.0/24 192.168.2.0/24 192.168.3.0/24

Доли основных протоколов в трафике



■ HTTPS
 ■ HTTP
 ■ SMB
 ■ SSH
 ■ RDP
 ■ VoIP
 ■ SMTP
 ■ Citrix



Предварительные
испытания

Приемочные
испытания



Цель – продемонстрировать и подтвердить работоспособность функционала комплекса
Континент 4:

- Сетевые возможности
- Межсетевое экранирование
- Обнаружение и предотвращение вторжений
- Защищенная передача данных
- Регистрация событий
- Управление системой
- Производительность
- Нефункциональные требования

Сетевые возможности	
1	Поддержка протокола LACP (IEEE 802.3ad)
2	Поддержка технологии VLAN (IEEE 802.1Q)
3	Поддержка статической маршрутизации
4	Поддержка протоколов динамической маршрутизации (OSPF, BGP)
5	Поддержка технологии NAT (SNAT, DNAT)
6	Поддержка функций DHCP-сервера
7	Поддержка протокола NTP
8	Поддержка протокола LLDP
9	Поддержка протокола SNMP
10	Поддержка протокола NetFlow
11	Наличие механизмов горячего резервирования
12	Возможность аутентификации через LDAP

Цель – продемонстрировать и подтвердить работоспособность функционала комплекса
Континент 4:

- Сетевые возможности
- Межсетевое экранирование
- Обнаружение и предотвращение вторжений
- Защищенная передача данных
- Регистрация событий
- Управление системой
- Производительность
- Нефункциональные требования

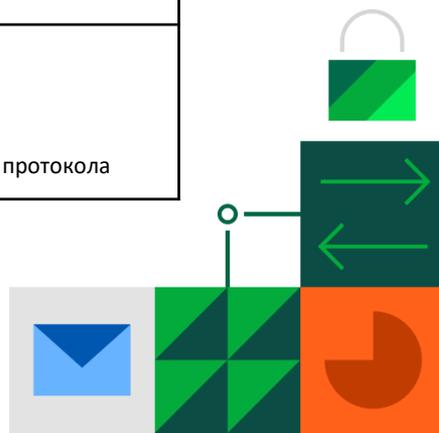
Межсетевое экранирование	
1	Управление доступом к ресурсам на основе правил фильтрации
2	Возможность введения временного ограничения на действие правила фильтрации
3	Использование в правилах именованных объектов и групп именованных объектов
4	Возможность добавления нестандартных протоколов в правила
5	Возможность указания географической привязки адресов в качестве критерия фильтрации
6	Возможность использования доменных имен в качестве критерия фильтрации
7	Возможность использования протоколов и приложений в качестве критерия фильтрации
8	Возможность использования URL-категорий в качестве критерия фильтрации
9	Возможность дешифрации HTTPS-трафика
10	Наличие потокового антивируса

Цель – продемонстрировать и подтвердить работоспособность функционала комплекса
Континент 4:

- Сетевые возможности
- Межсетевое экранирование
- Обнаружение и предотвращение вторжений
- Защищенная передача данных
- Регистрация событий
- Управление системой
- Производительность
- Нефункциональные требования

Обнаружение и предотвращение вторжений	
1	Обнаружение и предотвращение вторжений средствами сигнатурного анализа
2	Возможность выбора метода реагирования сигнатуры
3	Возможность создания собственных сигнатур
4	Защита от DoS
Защищенная передача данных	
1	Организация L3VPN по схеме Site-to-Site
2	Возможность реализации L3VPN-топологий «Централизованная» и «Полносвязная»
3	Организация L3VPN по схеме Remote Access
4	Возможность мониторинга состояния туннелей

Тест №	19	Возможность использования протоколов и приложений в качестве критерия фильтрации
Процедура испытания:		<ol style="list-style-type: none">1. Убедиться, что в конфигурации ЦУС создано правило фильтрации (Контроль доступа > Межсетевой экран) с логированием без указания отправителя и получателя с блокировкой приложения AnyDesk и протокола VNC, а также создано разрешающее правило фильтрации по всем сервисам из сети «192.168.1.0/24».2. Зайти на МК и запустить ping до bWAPP и anydesk.com. Убедиться, что приходят ICMP-ответы.3. На МК запустить приложение AnyDesk.4. На bWAPP запустить VNC-сервер командой vncserver. Попытаться подключиться к нему с помощью VNC-клиента MobaXterm на МК.5. Зайти в интерфейс подсистемы ведения журналов (Структура > Мониторинг > Журналы > Сетевая безопасность) и убедиться в наличии событий о том, что в трафике обнаружена попытка использования указанных протоколов и к их пакетам применено действие «Запретить»
Ожидаемый результат:		<ol style="list-style-type: none">1. Необходимые правила присутствуют в конфигурации ЦУС.2. От хостов поступают ICMP-ответы.3. Подключение к сети AnyDesk не устанавливается.4. Подключение к VNC-серверу не устанавливается.5. В журнале событий фиксируются события блокировки пакетов обнаруженного приложения и протокола



№	Требование	Ожидаемый результат	Пункты методики	Результат проверки
Межсетевое экранирование				
1	Фильтрация трафика согласно заданным правилам межсетевого взаимодействия	Фильтрация осуществляется по критериям: - L3-L4 (IP-адреса и/или порты TCP/UDP, FQDN); - L7 (приложения и URL); - учетные записи пользователей	12	Выполнено
			13	Выполнено
			16	Выполнено
			19	Выполнено
2	Возможность инспекции HTTPS-трафика	Выполняется блокировка при попытке скачивания вредоносного файла с ресурса https://www.eicar.org/	20	Выполнено
			21	Выполнено
3	Наличие встроенного функционала обнаружения и предотвращения атак	Обнаруживаются и блокируются атаки типа: - SQL Injection; - XSS; - DoS	22	Выполнено
			23	Выполнено
			26	Выполнено



№	Требование	Ожидаемый результат	Пункты методики	Результат проверки
Межсетевое экранирование				
1	Фильтрация трафика согласно заданным правилам межсетевого взаимодействия	Фильтрация осуществляется по критериям: - L3-L4 (IP-адреса и/или порты TCP/UDP, FQDN); - L7 (приложения и URL); - учетные записи пользователей	12	Выполнено
			13	Выполнено
			16	Выполнено
			19	Выполнено
2	Возможность инспекции HTTPS-трафика	Выполняется блокировка при попытке скачивания вредоносного файла с ресурса https://www.eicar.org/	20	Выполнено
			21	Выполнено
3	Наличие встроенного функционала обнаружения и предотвращения атак	Обнаруживаются и блокируются атаки типа: - SQL Injection; - XSS; - DoS	22	Выполнено
			23	Выполнено
			26	Выполнено

Общий результат и выводы

В ходе проведения пилотного проекта с использованием комплекса безопасности «Континент» были достигнуты следующие цели:

1.

...

n.

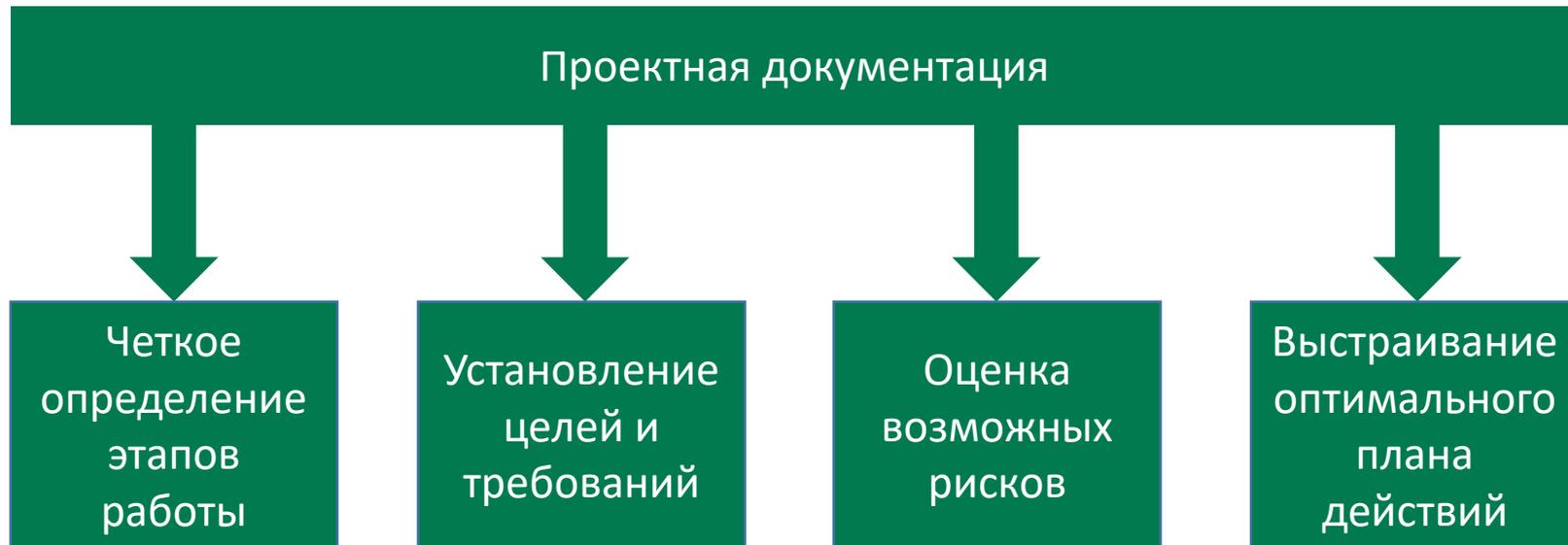
По результатам пилотного проекта можно утверждать, что ...



Предлагается оценить степень удовлетворенности исходя из следующих критериев:

- 5 баллов (полная удовлетворенность)
- 4 балла (хорошая степень удовлетворенности)
- 3 балла (средняя степень удовлетворенности)
- 2 балла (низкая степень удовлетворенности)
- 1 балл (полная неудовлетворенность)

№	Вопрос	Ответ
Основные параметры		
1	Общее соответствие продукта предъявленным требованиям	
2	Соответствие конструктивного исполнения	
Функциональные возможности		
1	Соответствие функций межсетевого экранирования, обнаружения и предотвращения вторжений	
2	Соответствие функций криптографической защиты	
3	Соответствие сетевой функциональности	
4	Удобство интерфейса	
Производительность		
1	Соответствие полосы пропускания в режиме межсетевого экрана	
2	Соответствие полосы пропускания в режиме VPN-шлюза	
Дополнительная информация		





КОД безопасности

info@securitycode.ru
www.securitycode.ru

