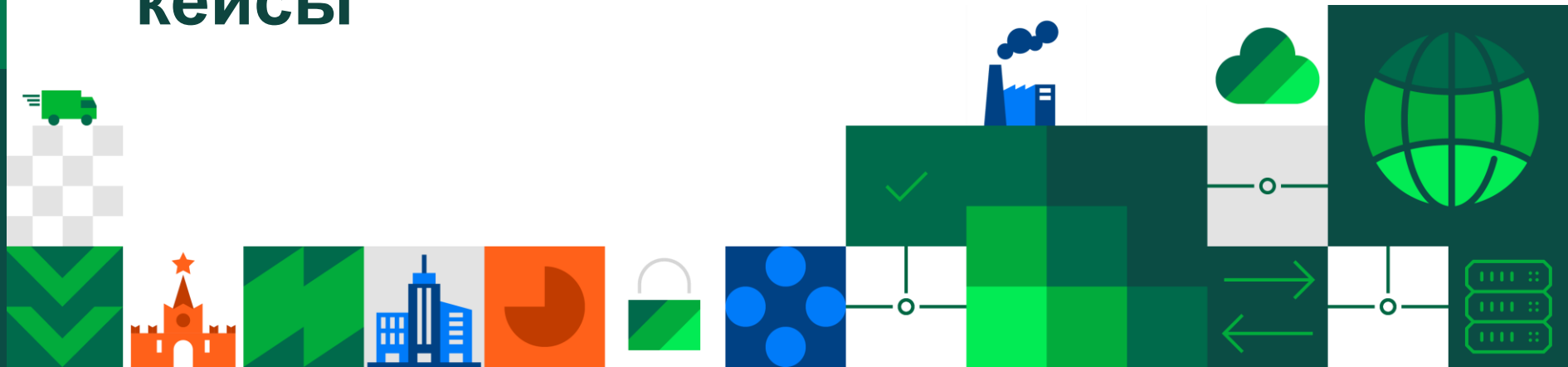
КОД безопасности

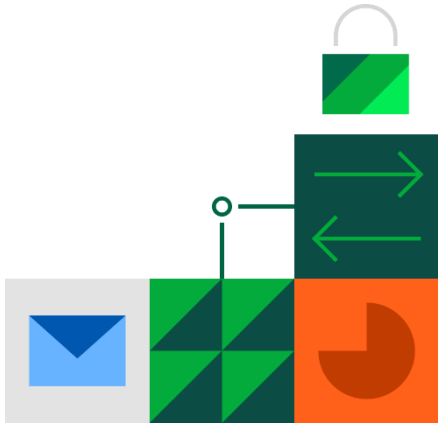
Практика миграции с иностранных NGFW: Документация, сценарии, кейсы



КОД безопасности

План

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



КОД безопасности

Замена иностранных решений по защите сети

Требования по импортозамещению остались прежними или ужесточились → Прямых аналогов ушедшим вендорам нет → Для выбора решения нужно определить сценарии использования СЗИ

Важна не сама технология, а закрываемые потребности

КОД безопасности

Как правильно подобрать решение?

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 георапределенной сети
- Для малого и среднего бизнеса

КОД безопасности

Континент 4

КШ Криптошлюз (КШ)

КК Криптокоммутатор (КК)

Детектор атак (ДА)

Центр управления сетью (ЦУС)

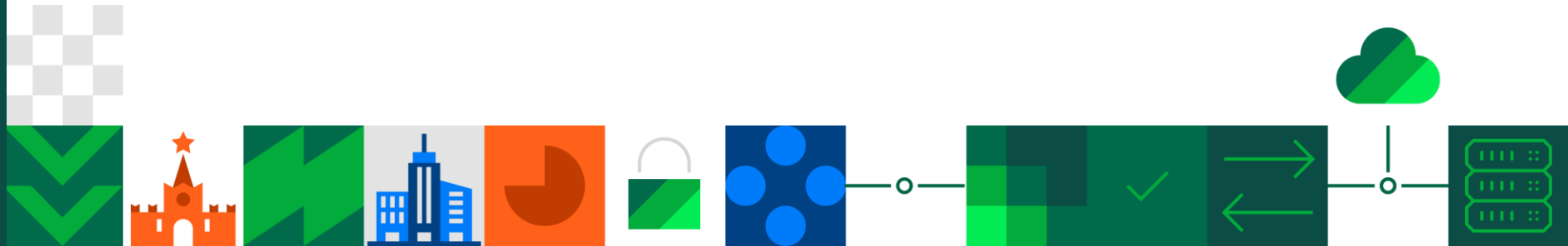
Узел безопасности (УБ)

FW | IPS | App control | L2 VPN | L3 VPN | MGMT | Threat Intelligence | Log | URL Filtering | User Identity

Antivirus | GeoIP

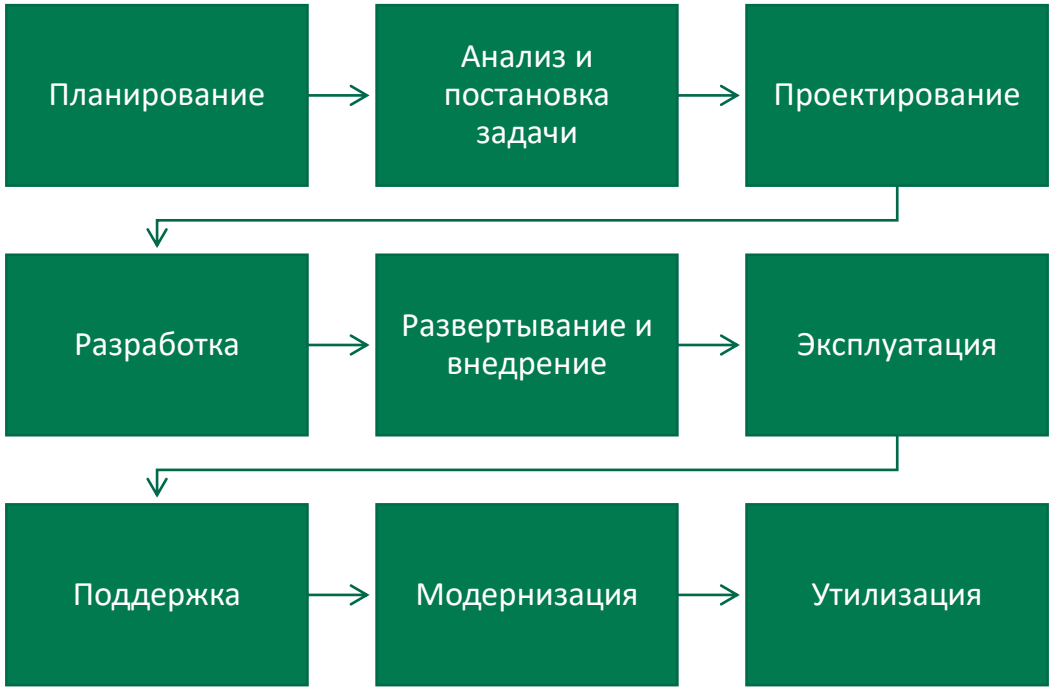
КОД безопасности

Процессы внедрения и тестирования



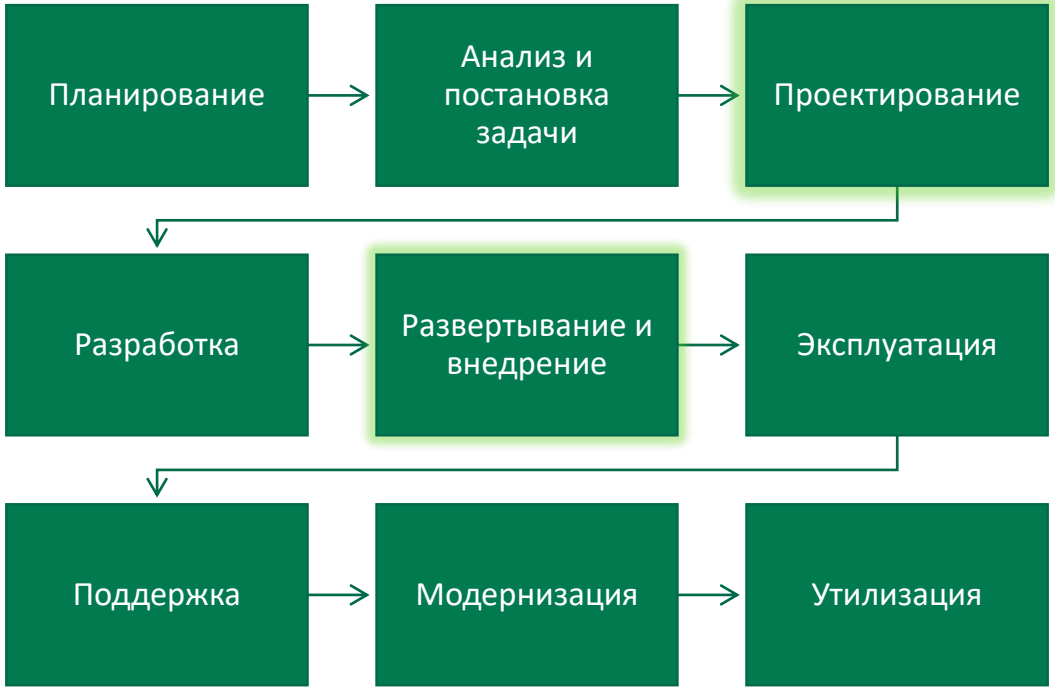
КОД безопасности

Проектный подход



КОД безопасности

Проектный подход



КОД безопасности

Вероятность ошибки

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

КОД безопасности

Вероятность ошибки

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

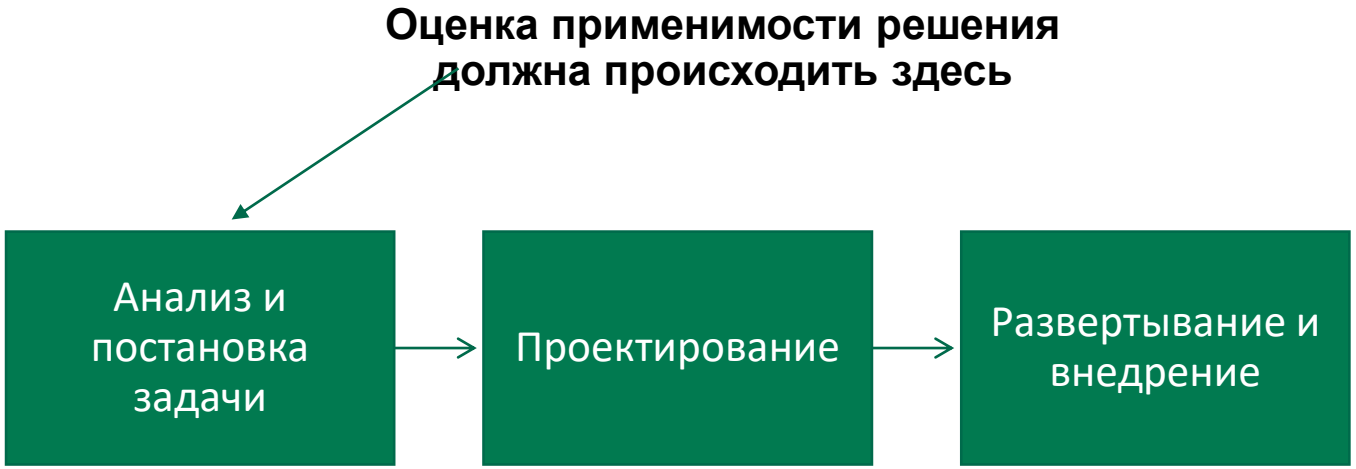
Развертывание и внедрение:

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?

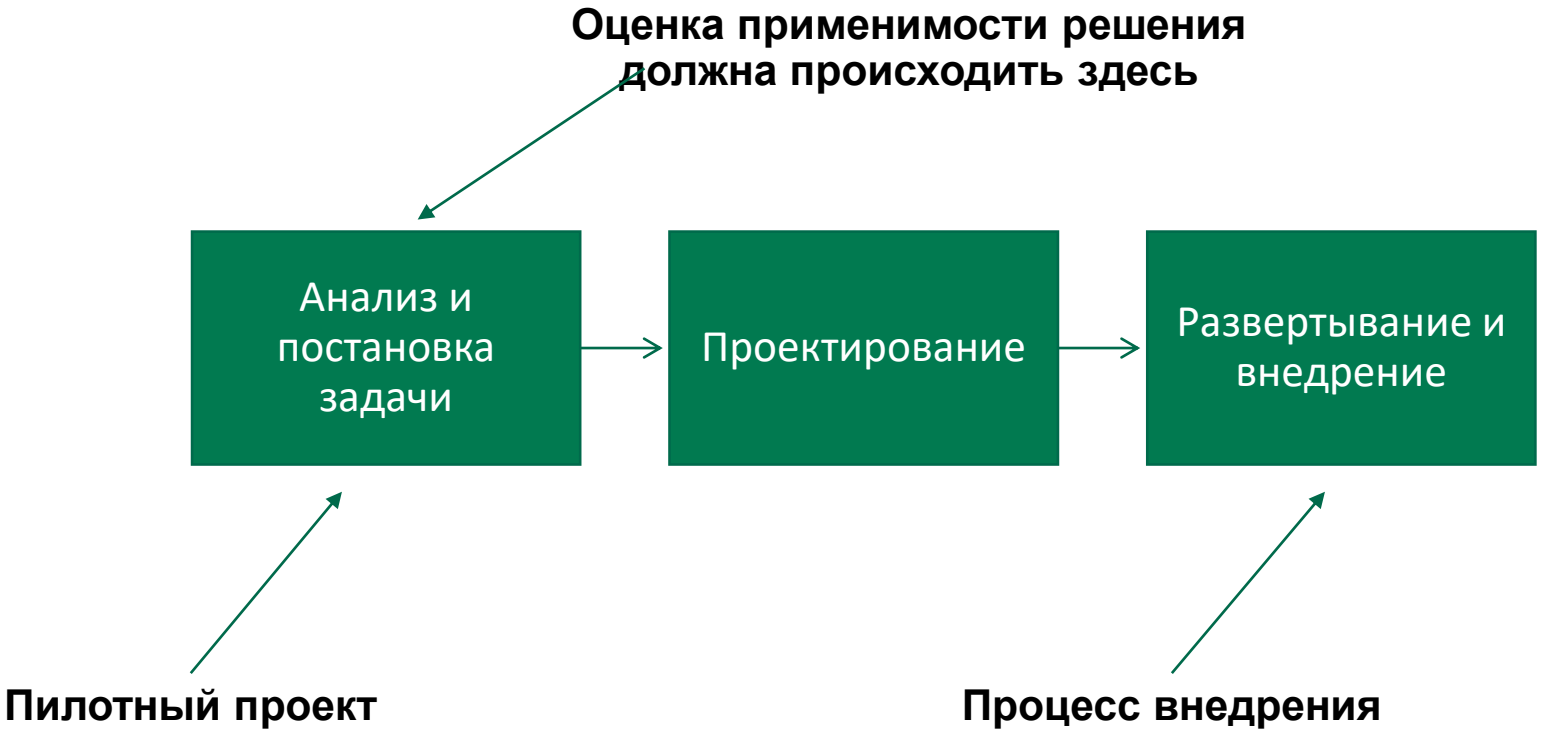
КОД безопасности

Проектный подход



КОД безопасности

Проектный подход

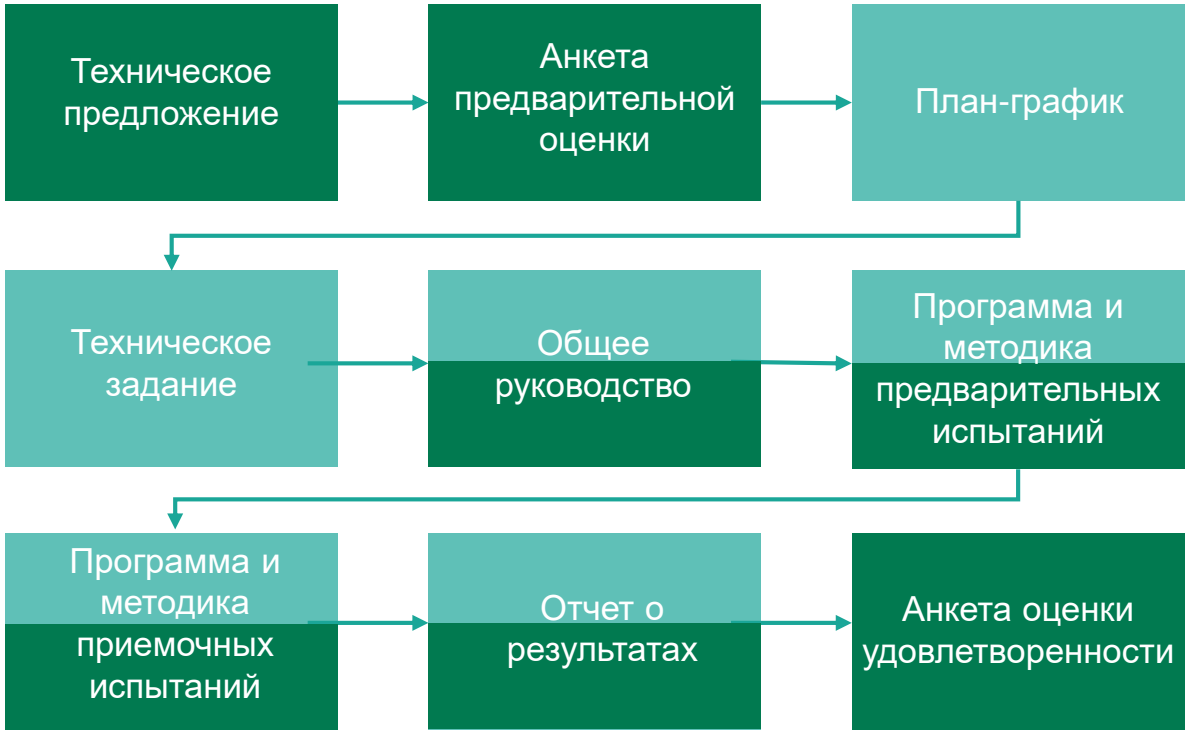


КОД безопасности

Перечень документов

Внедрение

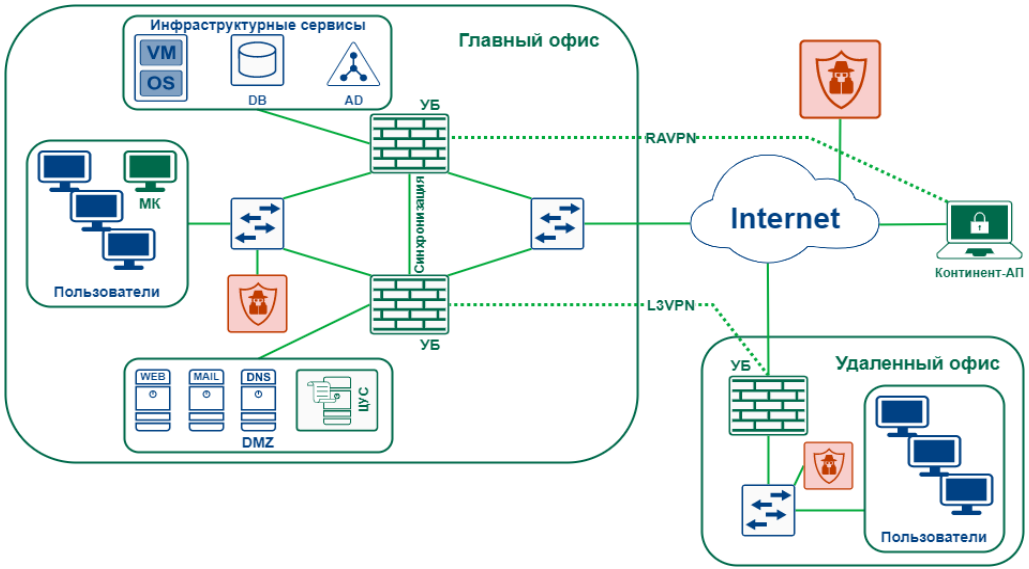
Пилотный проект



Техническое предложение

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



КОД безопасности

Анкета предварительной оценки

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	☐ Требуется
2	Интеграция продукта в пилотной зоне с реальной инфраструктурой	☐ Требуется
3	Имитация в пилотной зоне угроз безопасности и их предотвращение с помощью продукта	☐ Требуется
4	Подтверждение количественных характеристик продукта	☐ Требуется
5	Иное	

КОД безопасности

Анкета предварительной оценки

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	

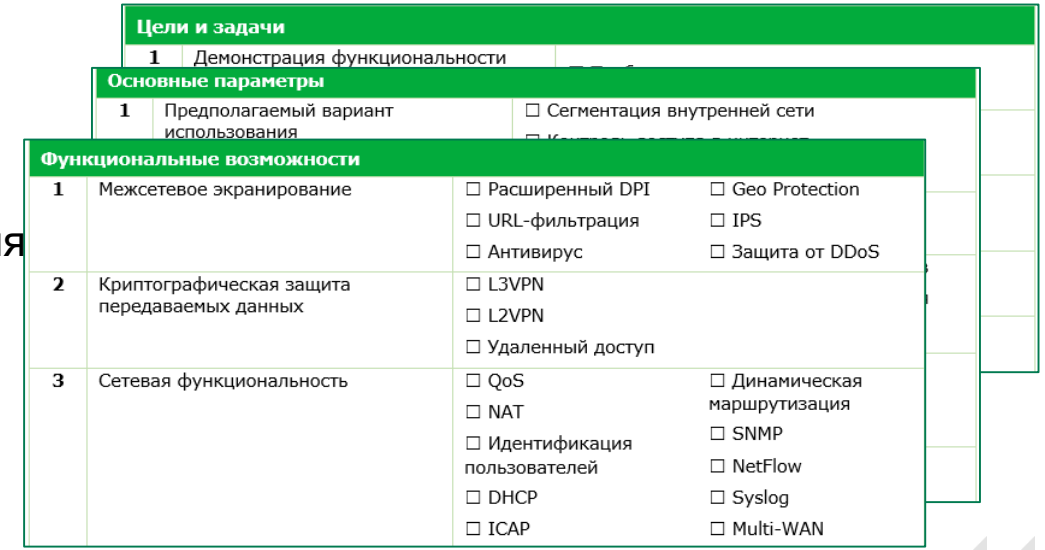
Основные параметры		
1	Предполагаемый вариант использования	☐ Сегментация внутренней сети ☐ Контроль доступа в интернет ☐ Построение VPN
2	Исполнение	☐ Аппаратное ☐ Виртуальное
3	Отказоустойчивость	☐ Узлов безопасности ☐ Сетевых портов ☐ Серверов управления ☐ Блоков питания ☐ Внешних каналов связи
4	Сетевые порты	1000Base-T – ____ шт. ☐ Трансиверы 1000Base-SX – ____ шт. ☐ Трансиверы 10GBase-SR – ____ шт. ☐ Трансиверы
5	Кабели питания	☐ Евровилка ☐ IEC-320-C14

КОД безопасности

Анкета предварительной оценки

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	☐ Сегментация внутренней сети

Функциональные возможности

1	Межсетевое экранирование	☐ Расширенный DPI ☐ URL-фильтрация ☐ Антивирус	☐ Geo Protection ☐ IPS ☐ Защита от DDoS
2	Криптографическая защита передаваемых данных	☐ L3VPN ☐ L2VPN ☐ Удаленный доступ	
3	Сетевая функциональность	☐ QoS ☐ NAT ☐ Идентификация пользователей ☐ DHCP ☐ ICAP	☐ Динамическая маршрутизация ☐ SNMP ☐ NetFlow ☐ Syslog ☐ Multi-WAN

КОД безопасности

План-график

№	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	
…	…	…	…	…

КОД безопасности

Техническое задание

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

Составляется на основе технического предложения.

Содержание

КОД безопасности

Общее руководство

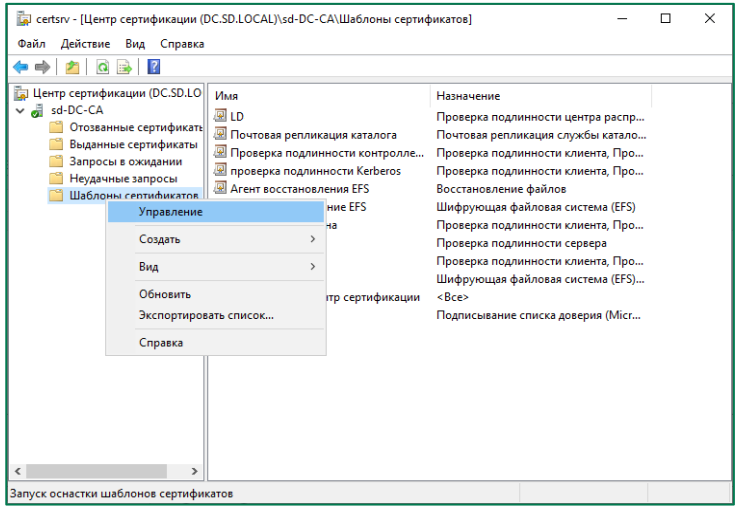
Цель – предоставить описание процесса подготовки и проведения пилотного проекта/ внедрения.

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

Оглавление

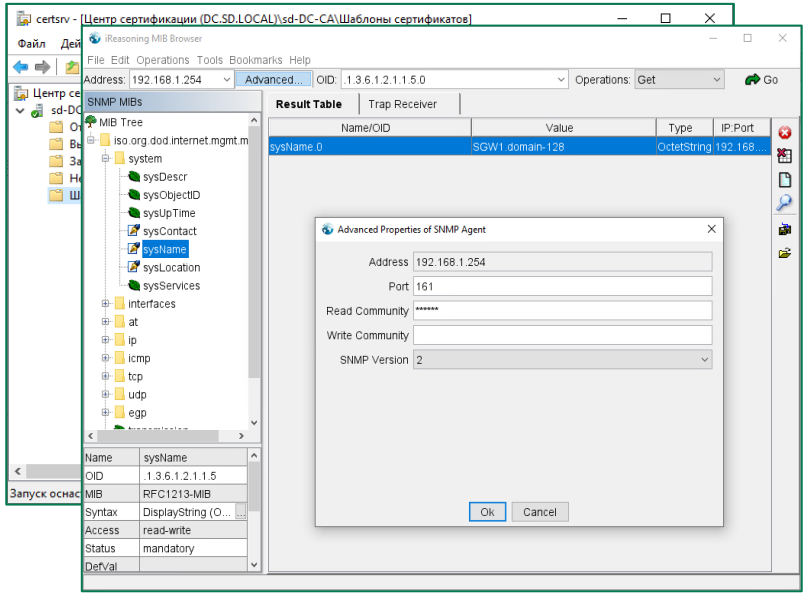
КОД безопасности

Общее руководство



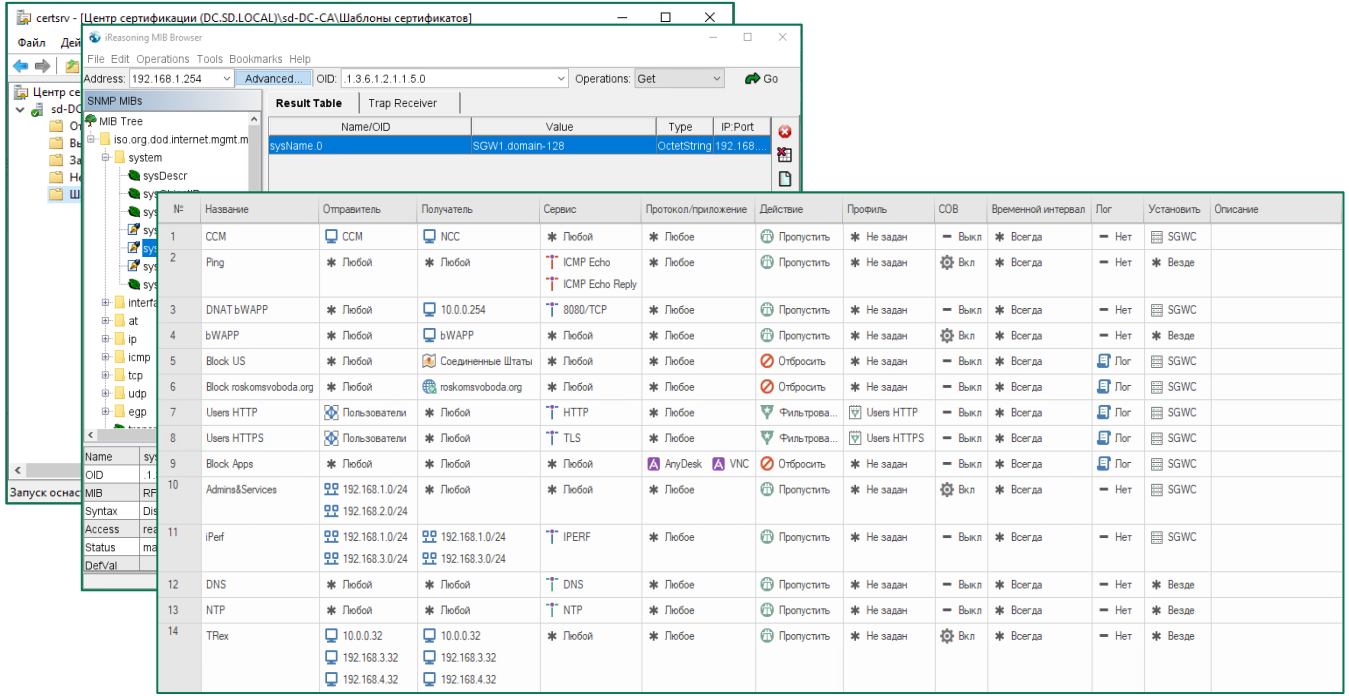
КОД безопасности

Общее руководство



КОД безопасности

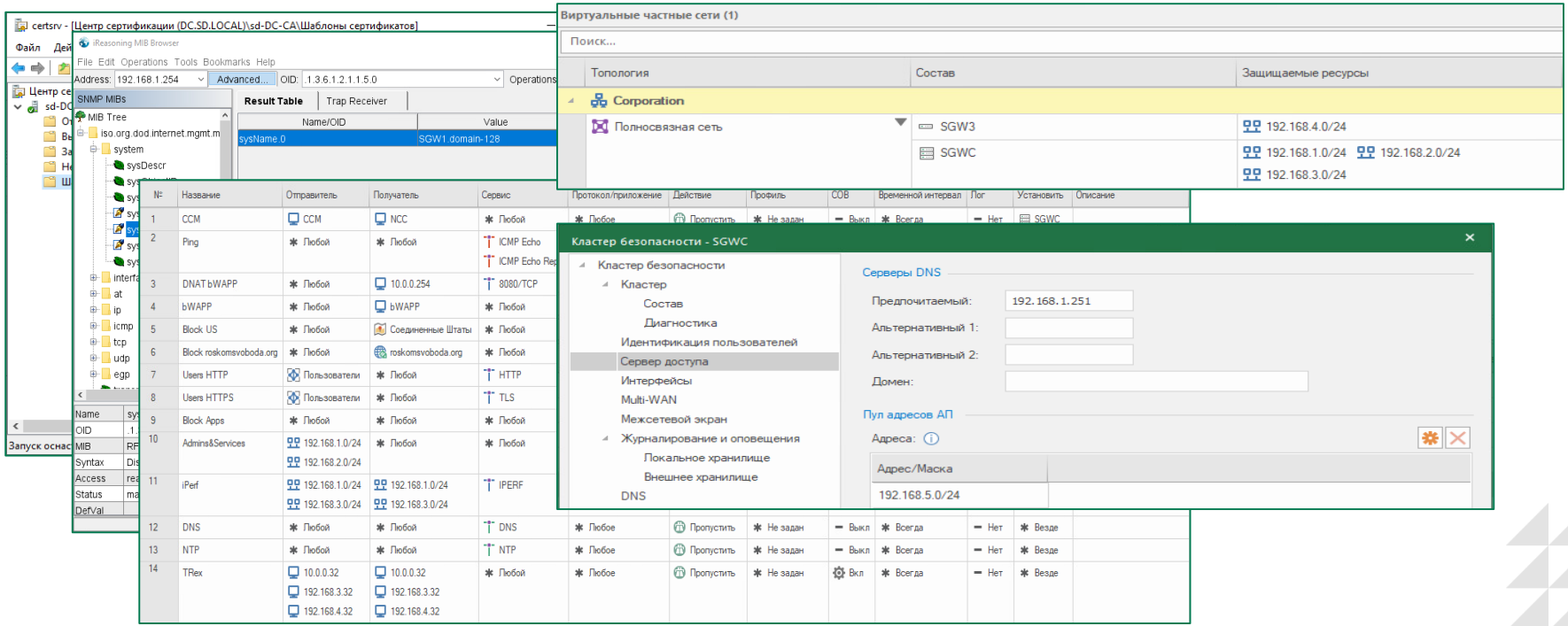
Общее руководство



№	Название	Отправитель	Получатель	Сервис	Протокол/приложение	Действие	Профиль	СОВ	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	Везде	
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	Везде	
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	Фильтрова...	Users HTTP	Выкл	Всегда	Лог	SGWC	
8	Users HTTPS	Пользователи	Любой	TLS	Любое	Фильтрова...	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	Любой	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	Везде	
13	NTP	Любой	Любой	NTP	Любое	Пропустить	Не задан	Выкл	Всегда	Нет	Везде	
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	Везде	

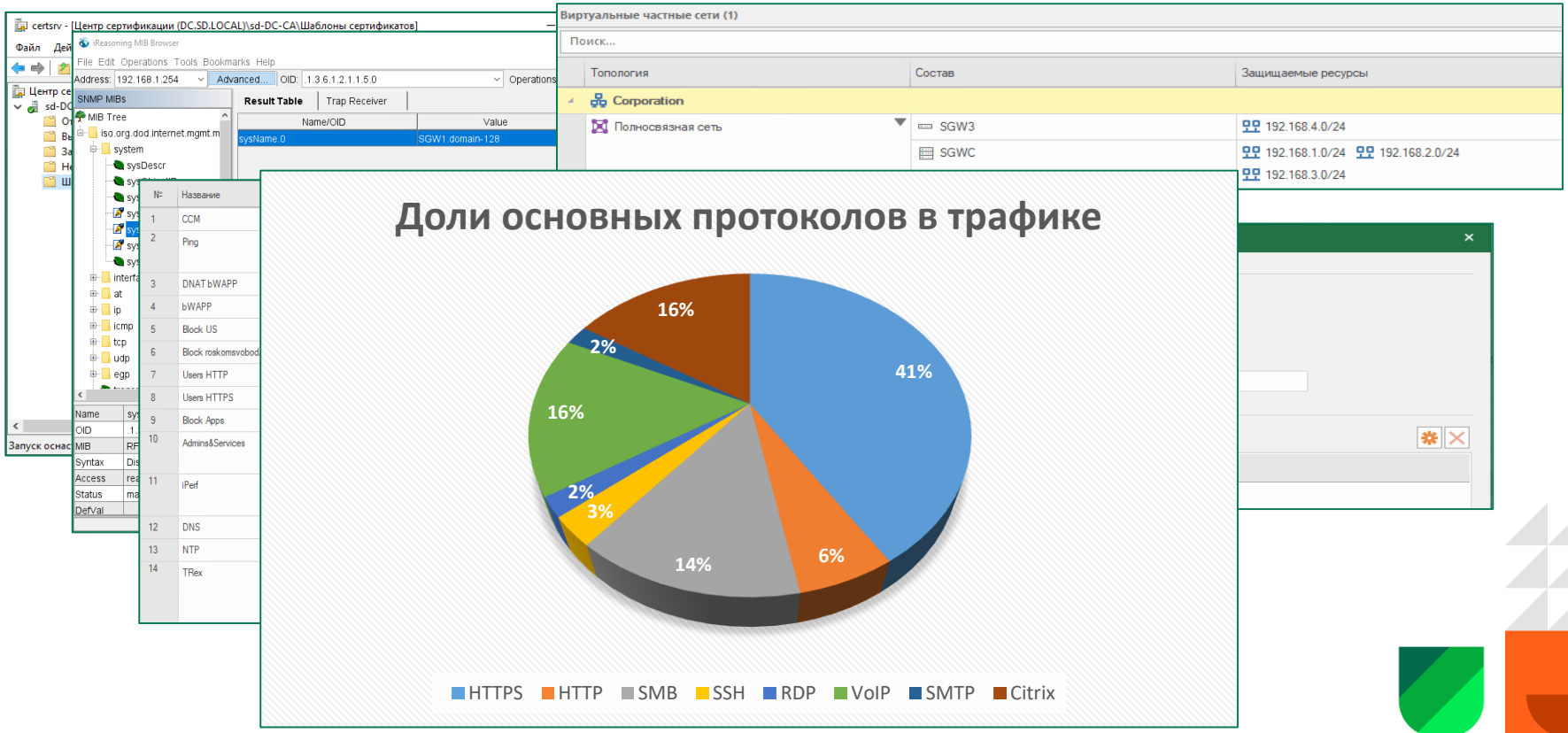
КОД безопасности

Общее руководство



КОД безопасности

Общее руководство



КОД безопасности

Программа и методика испытаний

Предварительные испытания

Приемочные испытания

КОД безопасности

Программа и методика испытаний

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

КОД безопасности

Программа и методика испытаний

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

КОД безопасности

Программа и методика испытаний

Цель – продемонстрировать и подтвердить работоспособность функционала комплекса Континент 4:

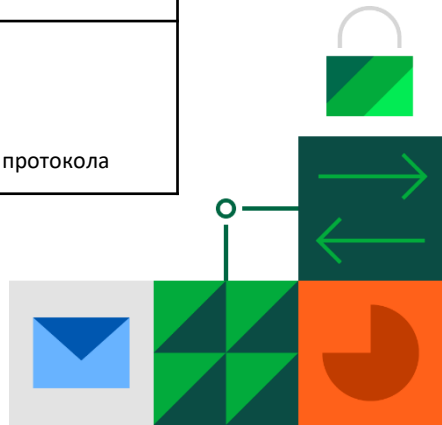
- Сетевые возможности
- Межсетевое экранирование
- Обнаружение и предотвращение вторжений
- Защищенная передача данных
- Регистрация событий
- Управление системой
- Производительность
- Нефункциональные требования

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

КОД безопасности

Процедуры испытаний

Тест №	19	Возможность использования протоколов и приложений в качестве критерия фильтрации
Процедура испытания:		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:		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



КОД безопасности

Отчет о результатах пилотного проекта

№	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
			20	Выполнено
2	Возможность инспекции HTTPS-трафика	Выполняется блокировка при попытке скачивания вредоносного файла с ресурса https://www.eicar.org/	21	Выполнено
			22	Выполнено
3	Наличие встроенного функционала обнаружения и предотвращения атак	Обнаруживаются и блокируются атаки типа: - SQL Injection; - XSS; - DoS	23	Выполнено
			26	Выполнено

КОД безопасности

Отчет о результатах пилотного проекта

№	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
			20	Выполнено
2	Возможность инспекции HTTPS-трафика	Выполняется блокировка при попытке скачивания вредоносного файла с ресурса https://www.eicar.org/	21	Выполнено
			22	Выполнено
3	Наличие встроенного функционала обнаружения и предотвращения атак	Обнаруживаются и блокируются атаки типа: - SQL Injection; - XSS; - DoS	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 …

КОД безопасности

Анкета оценки удовлетворенности

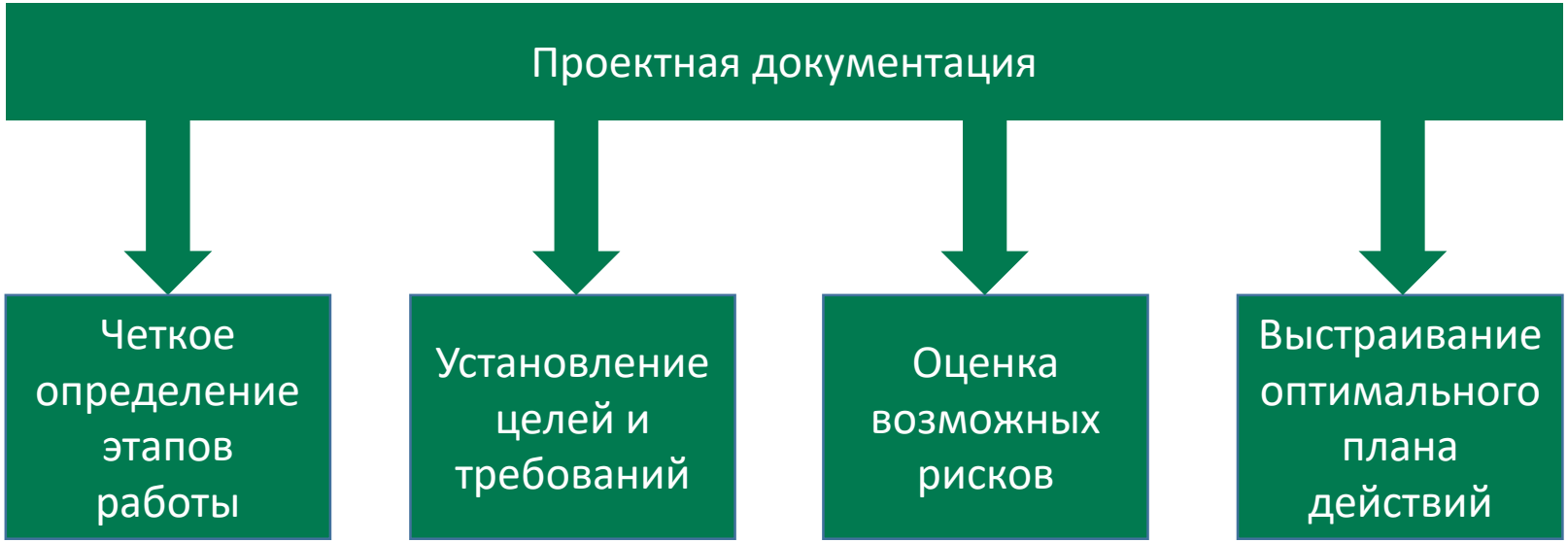
Предлагается оценить степень удовлетворенности исходя из следующих критериев:

- 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

Выводы



КОД безопасности

info@securitycode.ru
www.securitycode.ru