Выполнение требований ГОСТ Р 57580.1-2017. Практическое применение продуктов Кода Безопасности.

Коростелев Павел
Руководитель отдела продвижения продуктов

КОД БЕЗОПАСНОСТИ

КОРОТКО О НАС

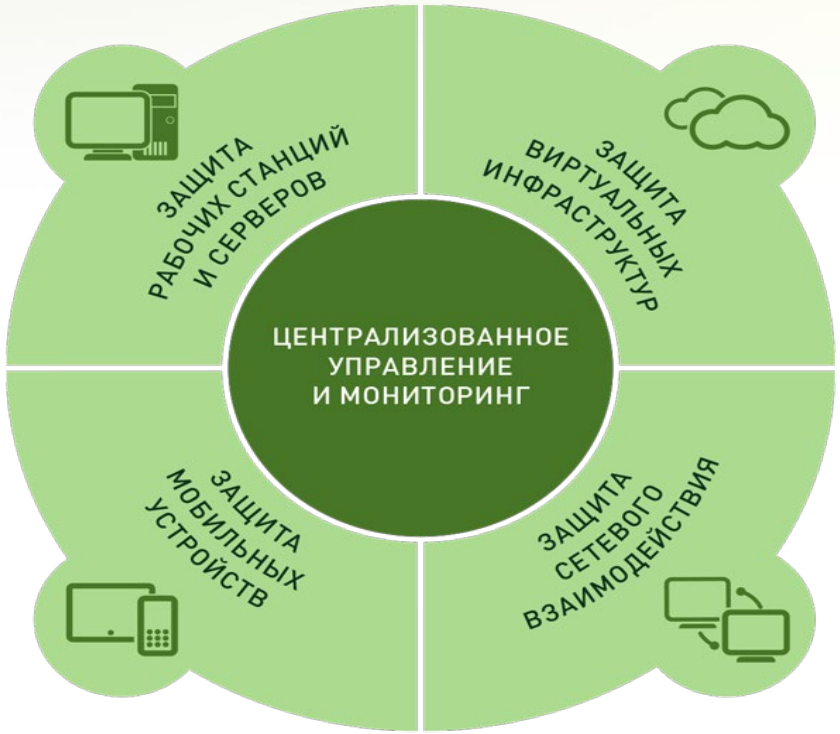
Ведущий российский разработчик
средств защиты информации.

Самый широкий портфель решений по ИБ.

3 центра разработки – Москва, Санкт-Петербург, Пенза. Более
300 разработчиков.

Полный цикл работ.
Проектирование, внедрение, сопровождение.

Более 70-ти сертификатов ФСТЭК, ФСБ, МО
на всю продуктовую линейку.



КОД БЕЗОПАСНОСТИ

ЧТО ЕСТЬ НА РЫНКЕ СЕГОДНЯ

Средства криптографической защиты	Средства аутентификации	Межсетевые экраны	Data Loss Prevention	Identity Management System
Анализ исходного кода и сканеры уязвимости	Антивирусы	Средства резервного копирования	АПМДЗ МДЗ	Средства защиты от DOS/DDOS-атак
Средства защиты среды виртуализации	Средства защиты от несанкционированного доступа	Системы обнаружения вторжения	Операционные системы	Антифрод

КОД БЕЗОПАСНОСТИ

ПО НАПРАВЛЕНИЯМ

ENDPOINT SECURITY	NETWORK SECURITY	VIRTUALIZATION SECURITY
СЗИ от НСД КСН HOST FW ЛОКАЛЬНОЕ ШИФРОВАНИЕ СОВ (HIPS) АНТИВИРУС АПМДЗ ТЕРМИНАЛЬНЫЙ ДОСТУП	FW IDS/IPS WAF GOST VPN URL-FILTERING APPLICATION CONTROL TLS/SSL DPI	СЗИ ВИ FW

КОД БЕЗОПАСНОСТИ

SECRET NET STUDIO

Защита системы

- Межсетевое экранирование с авторизацией соединений
- Система обнаружения и предотвращения вторжений
- Контроль устройств
- Замкнутая программная среда
- Антивирусная защита

Защита данных

- Мандатный контроль доступа к информации
- Авторизация сетевых соединений
- Шифрование контейнеров
- Контроль целостности данных

Удобство и надежность

- Доверенная среда
- Централизованное управление распределенной системой
- Сертификаты на все защитные механизмы за исключением локального шифрования
- Сертификат под ГТ на СЗИ от НСД и МЭ

ПАК СОБОЛЬ

КОД БЕЗОПАСНОСТИ

ЭЛЕКТРОННЫЙ ЗАМОК
«СОБОЛЬ» 4
Аппаратно-программный модуль доверенной загрузки, функционирующий в среде UEFI

ПРЕИМУЩЕСТВА

- КОНТРОЛЬ ЦЕЛОСТНОСТИ СИСТЕМНОГО РЕЕСТРА WINDOWS, АППАРАТНОЙ КОНФИГУРАЦИИ КОМПЬЮТЕРА И ФАЙЛОВ ДО ЗАГРУЗКИ ОПЕРАЦИОННОЙ СИСТЕМЫ
- ФУНКЦИОНИРОВАНИЕ В СРЕДЕ UEFI И ПОДДЕРЖКА РАЗМЕТКИ ДИСКА В ФОРМАТЕ GPT
- УСИЛЕННАЯ ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ С ПОМОЩЬЮ СОВРЕМЕННЫХ ПЕРСОНАЛЬНЫХ ЭЛЕКТРОННЫХ ИДЕНТИФИКАТОРОВ
- ПРОСТОТА УСТАНОВКИ, НАСТРОЙКИ И АДМИНИСТРИРОВАНИЯ
- ВОЗМОЖНОСТЬ ПРОГРАММНОЙ ИНИЦИАЛИЗАЦИИ БЕЗ ВСКРЫТИЯ СИСТЕМНОГО БЛОКА
- АППАРАТНЫЙ ДАТЧИК СЛУЧАЙНЫХ ЧИСЕЛ

Принцип работы

- КОНТРОЛЬ ПЕРЕХОДА УПРАВЛЕНИЯ «СОБОЛЮ»
- ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ
- БЛОКИРОВКА ЗАГРУЗКИ ОС СО СЪЕМНЫХ НОСИТЕЛЕЙ
- КОНТРОЛЬ ЦЕЛОСТНОСТИ ФАЙЛОВ И СЕКТОРОВ ЖЕСТКОГО ДИСКА
- КОНТРОЛЬ ЦЕЛОСТНОСТИ РЕЕСТРА WINDOWS
- КОНТРОЛЬ ЦЕЛОСТНОСТИ АППАРАТНОЙ СРЕДЫ

→ РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

VGATE

- Фильтрация трафика виртуальных машин на уровне гипервизора
- Назначение политик безопасности напрямую на объекты виртуальной инфраструктуры
- Группировка объектов доступа и автодобавление виртуальных машин в группы
- Отправка инцидентов безопасности во внешние системы
- Разграничение доступа к управлению виртуальной инфраструктурой
- Защита от несанкционированного копирования, клонирования, переноса и уничтожения виртуальных машин
- Доверенная загрузка и контроль целостности виртуальных машин
- Сегментация виртуальной инфраструктуры по категориям и уровням безопасности
- Регистрация и аудит событий безопасности
- Защита от специфических угроз, характерных для виртуальных сред
- Централизованное управление и контроль
- Поддержка распределенных инфраструктур
- Встроенные шаблоны политик безопасности
- Наличие сертификатов ФСТЭК как под конфиденциальную информацию, так и под ГТ

КОД БЕЗОПАСНОСТИ

КОНТИНЕНТ TLS

- Криптографическая защита трафика по алгоритмам ГОСТ
- Два режима аутентификации TLS:
  - Анонимный TLS: Аутентификация сервера без необходимости аутентификации пользователя
  - Взаимная аутентификация сервера и пользователя
- Разграничение прав доступа удаленных пользователей с помощью портала приложений
- Туннелирование TCP-трафика через протокол TLS
- Интеграция с Active Directory
- Использование удобного для пользователей программного клиента:
  - «Континент TLS VPN Клиент»
  - «КриптоПро CSP» 3.9/4.0
- Работа пользователя через любой веб-браузер

Может использоваться в сервисной модели

Есть virtual appliance для тестирования

КОД БЕЗОПАСНОСТИ

КОНТИНЕНТ WAF

- Защита веб-приложений от специфических угроз (OWASP TOP 10)
- Автоматическое построение модели работы приложения с использованием механизмов машинного обучения
- Анализ отклонений поведения пользователя от стандартного сценария
- Анализ данных в SSL-туннеле
- Обнаружение аномалий внутри вложенных данных, передаваемых по протоколу HTTP

Может использоваться в сервисной модели

Есть virtual appliance для тестирования

JINN SERVER

- Усиление электронной подписи меткой времени
- Подтверждение действительности и квалифицированности сертификатов
- Разбор конфликтных ситуаций
- Проверка и формирование электронной подписи

Не может использоваться в сервисной модели

Есть virtual appliance для тестирования

КОД БЕЗОПАСНОСТИ

АПКШ КОНТИНЕНТ

АПКШ «Континент»
многофункциональный программно-аппаратный комплекс сетевой безопасности.

- **Маршрутизация.**
- **Межсетевое экранирование.**
- **Криптографическая защита информации (L3 Site-to-Site VPN, L2 VPN).**
- **Безопасный доступ мобильных сотрудников к ресурсам корпоративных сетей (Remote Access VPN).**
- **Система обнаружения вторжения (СОВ).**
- **Web Application Firewall**

КОД БЕЗОПАСНОСТИ

КРИПТОГРАФИЯ И МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ

Центр Управления Сетью
КОНТИНЕНТ

КРИПТОШЛЮЗ
L3

КРИПТОКОММУТАТОР
L2

ДЕТЕКТОР АТАК
IDS

КОД БЕЗОПАСНОСТИ

ПРОАКТИВНАЯ ЗАЩИТА

- Двухуровневая система анализа трафика (сигнатурный анализ и анализ сетевых приложений)
- Два режима работы: пассивный (режим обнаружения атак, IDS) и активный (режим предотвращения атак, IPS)
- Распределение сетевого трафика между фермой Детекторов атак для достижения производительности анализа свыше 10 Гбит/с
- Обеспечение отказоустойчивости благодаря поддержке функции software-bypass
- Централизованное иерархическое управление системой защиты в территориально распределенных организациях с большим количеством филиалов
- Новая система мониторинга состояния сети и отдельных узлов в режиме реального времени с возможностью создания отчетов о событиях безопасности
- Собственная лаборатория сетевой безопасности для разработки сигнатур

Может использоваться в сервисной модели

Есть virtual appliance для тестирования

КОД БЕЗОПАСНОСТИ

КОНСОЛИДАЦИЯ ВСЕХ ЗАЩИТНЫХ МЕХАНИЗМОВ В ОДНОМ УСТРОЙСТВЕ

Криптошлюз

Криптокоммутатор

Детектор Атак

Центр Управления Сетью

FW	IPS	DPI
L2 VPN	L3 VPN	MGMT
Anti bot	Log	URL reputation

https://www.continent4.ru/

КОНТИНЕНТ 4 NF2

Высокопроизводительный движок NF2 (~80Гбит/с)

АПКШ КОНТИНЕНТ 4 NF2

Высокопроизводительный МЭ на платформе Intel DPDK и префиксных деревьев

Отдельная аппаратная платформа, предназначенная для реализации задач сегментации внутри сети.

Производительность одной ноды – до 80 Гбит/сек.

Производительность не падает при увеличении числа правил фильтрации.

КОД БЕЗОПАСНОСТИ

ПРОПУСКНАЯ СПОСОБНОСТЬ МЭ БЕЗ ШУТОК

Результаты измерения показателя Пропускная способность по UDP

Объект испытания	Схема сети	Количество потоков	Пропускная способность по UDP, Mbps						
			Размер кадра, Байт						
			70	128	512	1024	1518	8900	IMIX
Ver4 АПКШ IPC-3000F, S021	МСЭ	1	204	349	1399	2822	4199	9977	980
	МСЭ	16	1267	2249	9798	19403	25137	25827	5801
	МСЭ	512	1608	2794	11410	22401	25647	25978	7598
Ver4 АПКШ IPC-3000NF2, LN021E*	МСЭ	1	7822	8648	9624	9808	9869	-*	9880
	МСЭ	16	16119	27915	76992	78467	78959	-*	75300
	МСЭ	512	15125	26239	76992	78467	78959	-*	72880

Результаты измерения показателя Пропускная способность по TCP

Объект испытания	Схема сети	Количество потоков	Пропускная способность по TCP, Mbps
Ver4 АПКШ IPC-3000F, S021	МСЭ	1	3278
	МСЭ	16	13202
Ver4 АПКШ IPC-3000NF2, LN021E	МСЭ	1	9869
	МСЭ	16	78912

Результаты измерения показателя Пропускная способность по HTTP

Объект испытания	Схема сети	Пропускная способность по HTTP, Mbps
Ver4 АПКШ IPC-3000F, S021	МСЭ	11975
Ver4 АПКШ IPC-3000NF2, LN021E	МСЭ	37469

КОД БЕЗОПАСНОСТИ

КОНТИНЕНТ 4 UTM

APPLICATION CONTROL	NETFILTER	DEEP PACKET INSPECTION	L2 & L3 VPN на одном устройстве (ГОСТ)
IDS/IPS	БЛОКИРОВКА ДОСТУПА К ВРЕДОНОСНЫМ САЙТАМ (КАСПЕРСКИЙ)	ПОДДЕРЖКА JUMBO-FRAME	ИНТЕГРАЦИЯ С LDAP

КОД БЕЗОПАСНОСТИ

КОНТИНЕНТ 4 UTM

Централизованное управление:

- Узлами сети
- Настройками маршрутизации
- Правилами фильтрации трафика
- VPN-сообществами
- Криптографическими ключами

Пользователь «в центре» политики

- Интеграция с LDAP
- Captive-портал

Единая база сетевых объектов для политики безопасности

Отдельный web-интерфейс мониторинга

Application control (2600 приложений)

- VoIP/messaging: Skype, Oscar (ICQ & AIM), SIP, Skinny, H323, WhatsApp
- Social networking: Facebook, Twitter, MySpace, LinkedIn, Instagram, Tumblr
- P2P/filesharing: BitTorrent, eDonkey, Rapidshare, Uploaded.to, Xunlei
- Streaming: YouTube, Netflix, Hulu, Deezer, MyVideo, Vimeo, QQLive, Youku
- Enterprise: Citrix, Blackberry, SAP, MS Lync, MS Exchange, Lotus Notes, WebEx, etc.

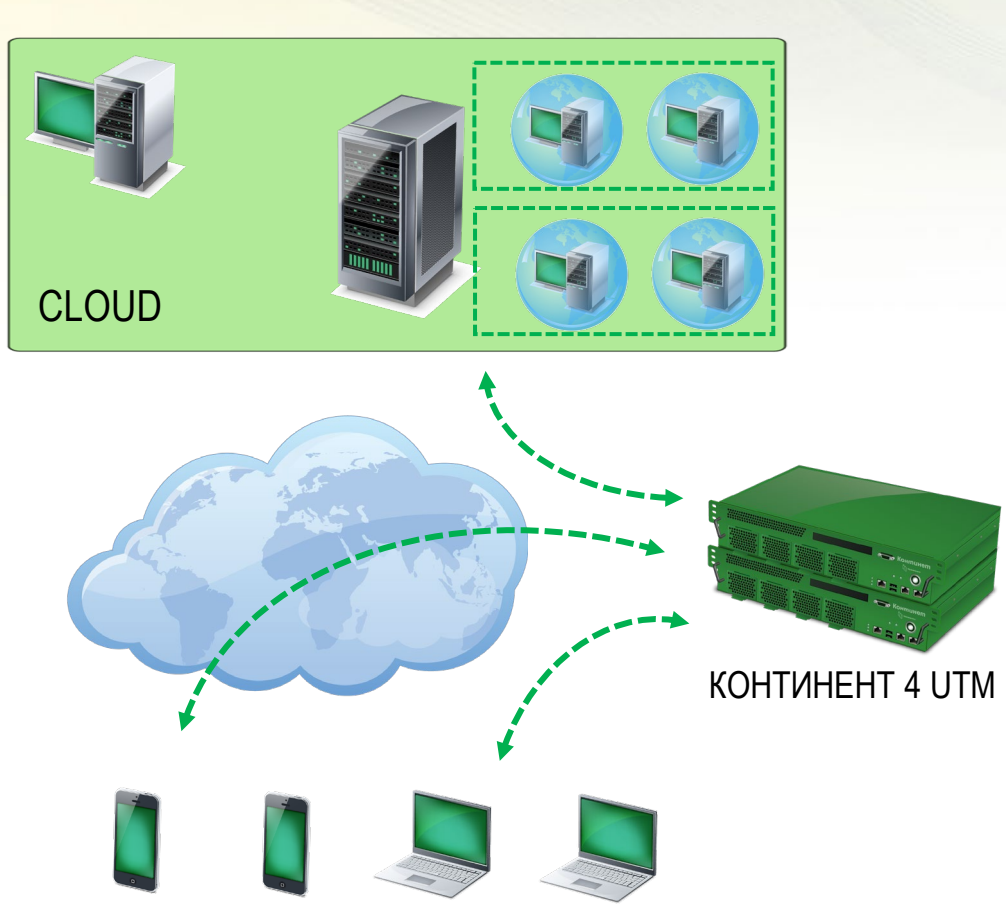
Предотвращение сетевых вторжений

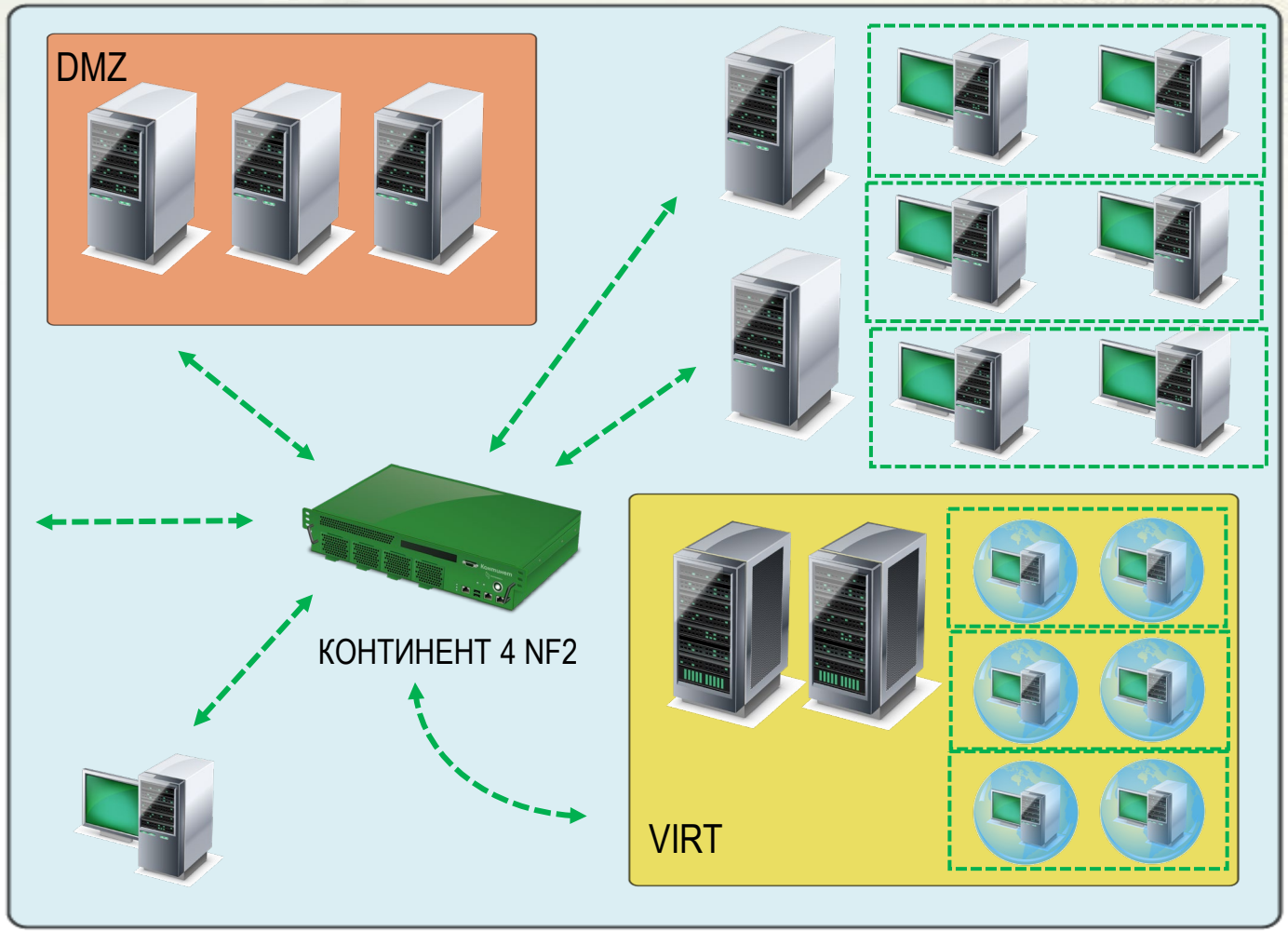
- Сигнатуры собственной разработки
- Возможность работы как на Сетевом, так и на канальном уровнях

SSL-decryption

Анализ сетевого трафика на наличие аномалий

СЦЕНАРИИ ПРИМЕНЕНИЯ





А ТЕПЕРЬ ВЕРНЕМСЯ УРОВНЯМ СООТВЕТСВИЯ ГОСТ ДЛЯ БАНКОВ…

Уровень соответствия	Диапазон значений	
Нулевой	0	Все очень плохо…
Первый	До 0,5	Меры системы защиты реализуются бессистемно
Второй	От 0,5 до 0,7 (включительно)	Меры осуществляются в значительном объеме
Третий	От 0,7 до 0,85 (включительно)	Меры осуществляются в значительном объеме. Контроль и совершенствование реализации мер ЗИ происходит эпизодически
Четвертый	От 0,85 до 0,9 (включительно)	Меры осуществляются в полном объеме. Контроль и совершенствование реализации мер ЗИ в основном обеспечены
Пятый	От 0,9 до 1	Меры осуществляются в полном объеме. Контроль и совершенствование реализации меры ЗИ обеспечены в полном объеме

КОД БЕЗОПАСНОСТИ

СОКРАЩЕНИЯ ГРУПП МЕР ИЗ ГОСТ 57580.1

УЗП - Управление учетными записями и правами субъектов логического доступа
РД - Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа
ФД - Защита информации при осуществлении физического доступа
ИУ - Идентификация и учет ресурсов и объектов доступа
СМЭ - Сегментация и межсетевое экранирование вычислительных сетей
ВСА - Выявление вторжений и сетевых атак
ЗВС - Защита информации, передаваемой по вычислительным сетям
ЗБС - Защита беспроводных сетей
ЦЗИ - Контроль целостности и защищенности информационной инфраструктуры
ЗВК - Защита от вредоносного кода
ПУИ - Предотвращение утечек информации
МАС - Мониторинг и анализ событий защиты информации
РИ - Обнаружение инцидентов защиты информации и реагирование на них
ЗСВ - Защита среды виртуализации
ЗУД - Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств
ПЗИ - Планирование процесса системы защиты информации
РЗИ - Реализация процесса системы защиты информации
КЗИ - Контроль процесса системы защиты информации
СЗИ - Совершенствование процесса системы защиты информации
ЖЦ - Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений

КАТЕГОРИИ МЕР

Secret Net Studio

Механизм/категория	Категории мер ГОСТ 57580.1
Межсетевой экран	СМЭ, ЗВС, ЗБС, ЦЗИ, ПУИ, РД
СОВ	ВСА
Антивирус	ЗВК, ЗУД, КЗИ
Механизмы защиты от НСД	УЗП, РД, ИУ, ЦЗИ, ЗВК, ПУИ, РИ, ЖЦ
Централизованное управление и аудит	УЗП, РД, ФД, ЗБС, ЦЗИ, ЗВК, ПУИ, МАС, РИ, РЗИ, КЗИ, ЖЦ
Контроль устройств	РД, ИУ, ЗВК, ПУИ
Шифрование данных	ПУИ

КАТЕГОРИИ МЕР

Secret Net LSP

Механизм/категория	Категории мер ГОСТ 57580.1
Аутентификация и разграничение доступа	УЗП, РД, РИ, ЖЦ
Контроль приложений	ИУ, ЦЗИ, ЗВК, ЖЦ
Контроль устройств	РД, ИУ, ЗВК, ПУИ
Централизованное управление и аудит	УЗП, РД, ФД, ЦЗИ, ПУИ, МАС, РИ, РЗИ, КЗИ, ЖЦ
Контроль целостности и затирание данных	ЦЗИ, ПУИ

КАТЕГОРИИ МЕР

ПАК СОБОЛЬ

Механизм/категория	Категории мер ГОСТ 57580.1
Аутентификация и разграничение доступа	УЗП, РД
Регистрация событий	УЗП, РД, ФД, МАС, РИ, КЗИ
Доверенная загрузка	РД, ФД, ЦЗИ
Аппаратный контроль целостности	ЦЗИ, МАС, РИ

КАТЕГОРИИ МЕР

vGate

Механизм/категория	Категории мер ГОСТ 57580.1
Межсетевой экран	СМЭ,
Контроль доступа администраторов и контроль безопасности настроек виртуальной среды	ЗСВ, УЗП, ИУ, РЗИ, РД
Сервер мониторинга vGate	МАС, РИ

КАТЕГОРИИ МЕР

АПКШ КОНТИНЕНТ

Механизм/категория	Категории мер ГОСТ 57580.1
Межсетевой экран и Сервер доступа	СМЭ, ЗВС, ЗБС, ЗУД
Детектор атак	ВСА
Центр управления сетью	МАС, РИ

ВВОДНЫЕ…

Входные данные для оценки

- В организации есть **только один** контур безопасности
- Все меры **организационного характера** по-умолчанию считаются **выполненными** в системе
- Из мер **технического** характера выполненными считаются **только** те меры, которые выполняют продукты Кода Безопасности
- **Не выявлено** грубых нарушений при аудите

В ИТОГЕ

технические меры за счет продуктов КБ + организационные меры + отсутствие нарушений

КОД БЕЗОПАСНОСТИ

ИТОГОВАЯ ОЦЕНКА

Уровень ЗИ	Итоговая оценка с продуктами КБ	Уровень соответствия с продуктами КБ
1 - Усиленный	>0.86	**четвертый**
2 – Стандартный	>0.9	**пятый**
3 – Минимальный	>0.95	**пятый**

С продуктами Кода Безопасности:

- **5й (максимальный) уровень** соответствия ГОСТ при реализации стандартного либо минимального уровня защиты
- **4й уровень** соответствия ГОСТ при реализации усиленного уровня защиты
- **4й уровень** соответствия оптимален с точки зрения ЦБ*

*необходимо реализовать до 1 января 2022 года

КОД БЕЗОПАСНОСТИ

ПРОДУКТОВЫЙ ВЕС

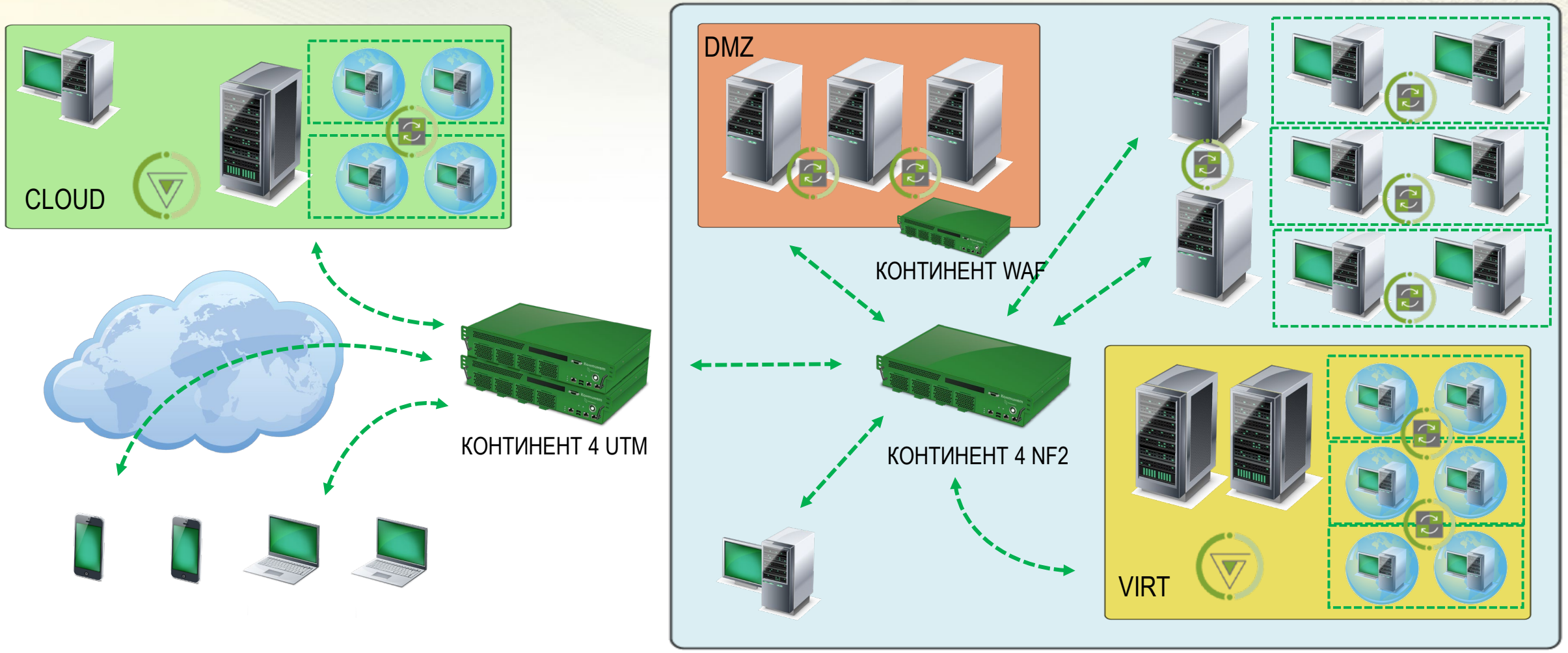
При условии что мы выполняем все необходимые организационные меры:

SNS - 0,8
SN LSP - 0,67
Континент 3 - 0,7
СД АП - 0,66
vGate - 0,73
Соболь - 0,62

При условии что мы не выполняем все организационные меры:

SNS - 0,31
SN LSP - 0,20
Континент 3 - 0,23
СД АП - 0,16
vGate - 0,25
Соболь - 0,15

СЦЕНАРИИ ПРИМЕНЕНИЯ



БЛАГОДАРЮ ЗА ВНИМАНИЕ!

Павел Коростелев
p.korostelev@securitycode.ru