Ассоциация Российских Банков

Противодействие современным угрозам безопасности. Необходимый минимум

Федорец А.О. – «iDSystems» и «SDK Systems»
Умницын М.Ю. - «ИЦ РЕГИОНАЛЬНЫЕ СИСТЕМЫ»
Коростелев П.В. – «Код Безопасности»

Положение 683-п и его место в экосистеме нормативных актов по ИБ

Регуляторы

ЦБ РФ

ФСТЭК

683-п. Основные требования

- Оценка соответствия по ГОСТ 57580.х
- Модернизация системы защиты информации (2 этапа)
- Тестирование на проникновение и анализ уязвимостей
- Сертификация или анализ уязвимостей по ОУД 4
- Применение мер по защите персональных данных
- Рекомендации для клиентов по ИБ
- Регистрация инцидентов защиты информации
- Требование ИБ к бизнес-процессам (подписание сообщений ЭЦП, использование СКЗИ; регламентация, реализация, мониторинг технологии и …. обработки информации)

Анализ уязвимостей по требованиям к ОУД 4 (п. 4)

Вступил в силу, но ЦБ не штрафует до июля 2020.

Что делать

Сертифицировать или
провести анализ по требованиям ОУД 4:

- прикладного программного обеспечения АС и приложений, распространяемых клиентам для совершения финансовых операций;

- программного обеспечения, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в АС с использованием Интернет

Состав работ

Подготовка стенда, развертывание ПО

Оценка уязвимостей программного обеспечения

Функциональное, статическое, динамическое тестирование, тестирование на проникновение

Оценка документации (на ПО, организации процесса разработки, тестирования и т.д.)

! Для анализа нужно подготовить очень большой объем документации

Какие документы необходимы для успешного прохождения ОУД

Что передается Оценщику в электронном виде:

- Инсталляционная версия программного обеспечения;
- Исходный код программного обеспечения ;
- Программные утилиты, используемые для компиляции программного обеспечения из исходных текстов программных модулей.

Что передается Оценщику в электронном или печатном виде:

- Сведения о программном обеспечении;
- Проектная документация;
- Эксплуатационная документация;
- Дополнительная документация, содержащая сведения о ПО;
- Документация по безопасной разработке.

Документы должны быть оформлены официально, с указанием версии, регистрационного номера и датой утверждения каждого из документов.

Что дополнительно надо учесть при разработке:

- Методический документ «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций».

! Данный документ до сих пор находится в стадии проекта в ТК 122 и может претерпеть изменения!

Какие сложности при прохождении ОУД:

- Отсутствует документация на программное обеспечение;
- Отсутствует документация по безопасной разработке;
- Сложность получения исходного кода (заявитель на анализ уязвимостей не является разработчиком ПО).

! Общий вердикт по анализу уязвимостей «положительный тогда и только тогда, когда все составляющие вердикта положительные»! (ГОСТ Р ИСО/МЭК 18045-2013, п.7.2.5.)

Какие документы необходимы для успешного прохождения ОУД

Документация на программное обеспечение:

- Описания объекта оценки;
- Функциональная спецификация;
- Задание по безопасности;
- Руководство пользователя;
- Руководство администратора;
- Формуляр;
- Технические условия;
- Регламент передачи ПО пользователю;
- Регламент отслеживания и исправления обнаруженных ошибок ПО и уязвимостей программы;
- Регламент приема и обработки сообщений от пользователей об ошибках ПО и уязвимостях программы;
- Регламента доведения до пользователей информации об уязвимости программы и рекомендаций по их устранению;
- Регламент управления конфигурацией;
- Регламента регистрации событий изменений конфигурации ПО;
- Регламент экстренного выпуска обновлений ПО;
- Регламент маркировки версий ПО;
- Журнала регистрации изменений конфигурации ПО;
- Журнал ошибок и уязвимостей программы;
- Регламента поддержки жизненного цикла; Описание архитектуры безопасности;
- Регламент и протоколы тестирования программы;
- Регламент и протоколы экспертизы исходного кода программы;
- Регламент и протоколы тестирования на проникновение;
- Регламент, протоколы, журналы поиска уязвимостей программы;
- Отчет по анализу уязвимостей и тестированию на проникновение.

Документация по реализации процесса безопасной разработки:

- Руководство по разработке безопасного ПО;
- Перечень инструментальных средств разработки ПО;
- Порядок оформления исходного кода программы;
- Регламент защиты инфраструктуры среды разработки ПО;
- Программа обучения сотрудников в области разработки безопасного ПО;
- Журнал обучения сотрудников в области разработки безопасного ПО.

Требования к документам

- ГОСТ ИСО/МЭК 15408: Общие критерии.
- ГОСТ ИСО/МЭК 15408-1: Введение и общая модель.
- ГОСТ ИСО/МЭК 15408-2: Функциональные компоненты безопасности.
- ГОСТ ИСО/МЭК 15408-3: Компоненты доверия к безопасности.
- ГОСТ ИСО/МЭК 18045: Методология оценки.
- ГОСТ Р 58142: Использование источников для идентификации уязвимостей.
- ГОСТ Р 56545: Правила описания уязвимостей.
- ГОСТ Р 56546: Классификация уязвимостей.
- ГОСТ Р 58143: Тестирование проникновения.
- ГОСТ ИСО/МЭК ТО 20004: Уточнённый анализ уязвимости программного обеспечения.
- ГОСТ Р 57628-2017: Руководство по разработке профилей защиты и заданий по безопасности.
- ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования.
- ГОСТ Р 58412-2019 Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения.
- ГОСТ 19.501-78 Единая система программной документации (ЕСПД). Формуляр. Требования к содержанию и оформлению.
- ГОСТ 2.114-2016 «Единая система конструкторской документации (ЕСКД). Технические условия».
- ГОСТ Р 56920-2016/ISO/IEC/IEEE 29119-1:2013 Системная и программная инженерия. Тестирование программного обеспечения. Часть 1. Понятия и определения.
- ГОСТ Р 56921-2016/ISO/IEC/IEEE 29119-2:2013 Системная и программная инженерия. Тестирование программного обеспечения. Часть 2. Процессы тестирования.
- ГОСТ Р 56922-2016/ISO/IEC/IEEE 29119-3:2013 Системная и программная инженерия. Тестирование программного обеспечения. Часть 3. Документация тестирования.
- ГОСТ Р ИСО 10007 Менеджмент организации. Руководящие указания по управлению конфигурацией.
- ГОСТ Р ИСО/МЭК 12207 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств.

! Перечень документов, который необходимо изучить при самостоятельной разработки документации.

Реальный кейс. ОУД-4

Исходные данные:	Анализ уязвимостей по требованиям к ОУД	Разработка проектов документов и консультации по заполнению	Общая длительность работ
1 ПО **1 язык ПО** **~ 700 000 строк кода**	Стоимость услуг: **2,2 млн. руб.** Длительность работ: **120 дней**	Стоимость услуг: **1,6 млн. руб.** Длительность работ: **100 дней**	**~ 130-145 дней**

Оценка соответствия уровню защиты информации (п. 9)

Что делать

Не реже одного раза в 2 года проводить оценку соответствия уровню защиты информации **для объектов информационной инфраструктуры** с привлечением лицензированной организации.

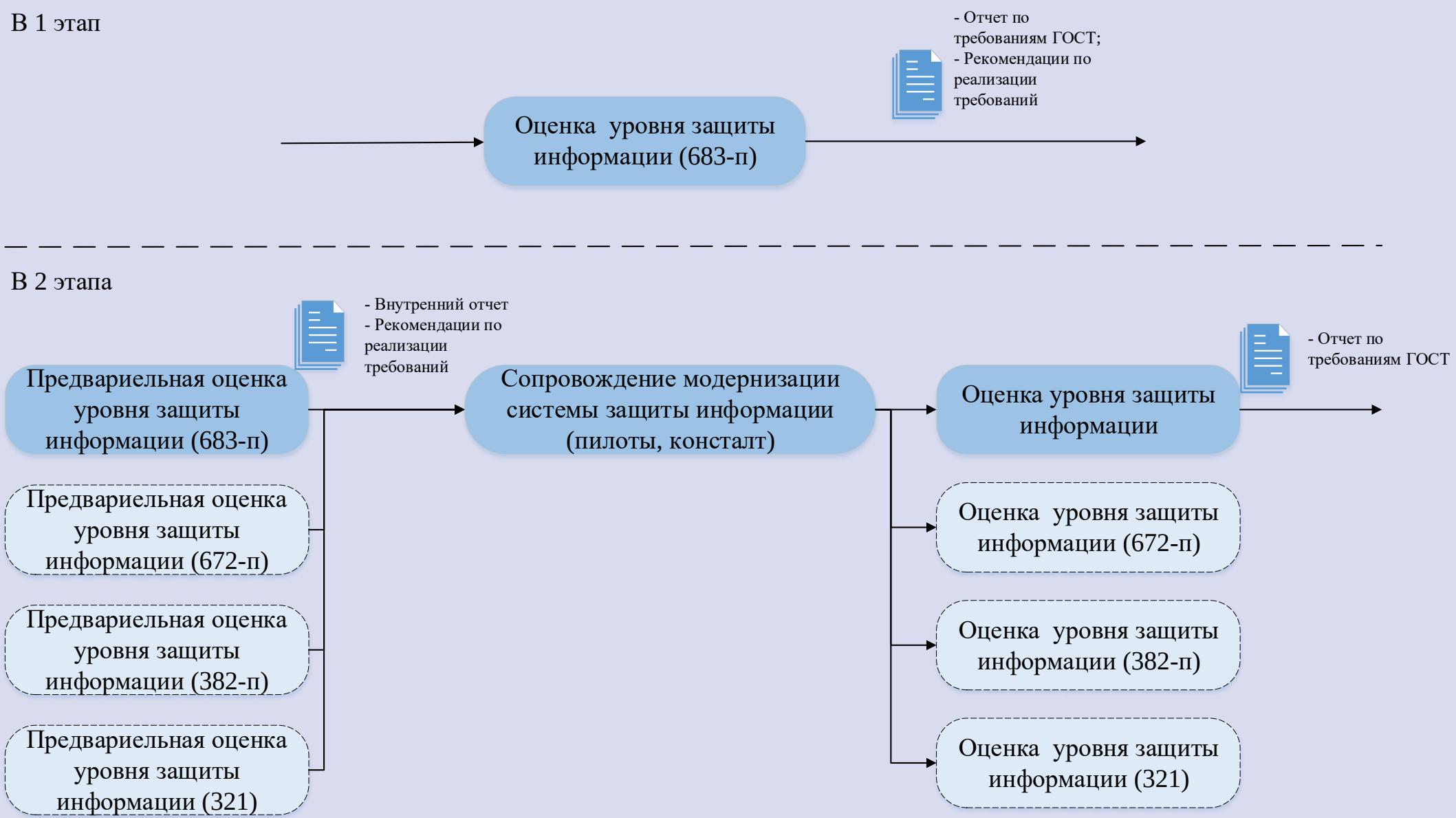
Почему оценку соответствия нужно проводить сейчас, а не в следующем году

Система защиты информации банка должна обеспечивать 3 уровень соответствия уже с **01.01.2021 г.** Поэтому, необходимо уже сейчас понимать текущую оценку и планировать мероприятия по модернизации системы защиты.

Что мы предлагаем

Оценка уровня защиты информации в соответствии с ГОСТ Р 57580.2-2018

Этапы оценки соответствия уровню защиты информации (п. 9)



Результаты оценки соответствия уровня защищенности (п.9)

Требования ГОСТ:

- Текущая оценка соответствия
- Отчет об оценке, уровня защиты информации по требованиям ГОСТ

Внутренний отчет (дополнительно) включает в себя:

- Предложения по корректировке ОРД Заказчика
- Различные варианты модернизации системы защиты информации по требованиям Положения 683-п по этапам (с указанием стоимости):
  - с учётом числового значения оценки соответствия каждого типа СрЗИ.
  - с учетом различных производителей СрЗИ.

Реальные кейсы. Оценка соответствия

1

1 контур

15 филиалов

Оценка соответствия:

Стоимость услуг – **900 тыс. руб**.

Длительность работ **– 50 дней.**

2

1 контур

9 филиалов

Оценка в 2 этапа

Оценка соответствия:

Стоимость услуг – **1,4 млн. руб.**

Длительность работ **– 207 дней.**

Модернизация системы защиты информации

! План и оценку мы делаем в рамках оценки соответствия

Что делать

Кредитная организация должна обеспечить уровень соответствия уровню защиты информации:

- **не ниже 3-го с 1 января 2021 г.**
- **не ниже 4-го с 1 января 2023 г.**

Состав работ

- План модернизации системы защиты информации
- Оценка стоимости системы защиты информации
- Запуск процессов бюджетирования в Банке
- Пилотирование отдельных решений по ИБ (при необходимости)
- Модернизация системы защиты информации до 3го уровня соответствия
- Модернизация системы защиты информации до 4го уровня соответствия

Реальный кейс

120 сотрудников

9 филиалов

2 ЦОДа

1 AD-домен

МЭ без IDS/IPS, AV, AppControl

AV-Endpoint решения (АРМ, сервера), AV-Mail.

Гипервизор с централизованным управлением

VPN (ГОСТ VPN)

Средства инвентаризации и мониторинга

Исходный бал: 0,672

1 ЭТАП (3й уровень соответствия)

- Настройка существующих СрЗИ;
- SIEM.

Выходной бал по результатам этапа: + 0,079 (Итого: 0,751)

Стоимость реализации мер ~ 8 млн. руб.

2 ЭТАП (4й уровень соответствия)

- Модернизация подсистемы МЭ;
- Система обнаружения вторжения;
- Корректировка ОРД.

Выходной бал по результатам этапа: + 0,137 (Итого: 0,888)

Стоимость реализации мер ~ 18 млн. руб.

Тестирование на проникновение и анализ уязвимостей (п.3.2)

Вступил в силу!

Что делать

Проводить **ежегодное** тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

Что мы предлагаем

Тестирование на проникновение ИТ инфраструктуры банка согласно рекомендациям ЦБ РФ

Внимание

Цели тестирования на проникновение в рамках 382-п и 683-п различаются!

Реализация мер по защите персональных данных (п. 1)

Вступил в силу!

Что делать

Кредитные организации должны применять меры по обеспечению безопасности персональных данных

Что мы предлагаем

- Аудит на соответствие требованиям
- Разработка модели угроз и нарушителя
- Разработка организационно-распорядительной документации
- Разработка технического проекта на ИСПДн
- Аттестационные испытания
- Внедрение системы защиты персональных данных

683-п. План на 2020 год

№ п/п	Мероприятие	Рекомендуемый срок	Требование ЦБ	Примечание
1	Анализ уязвимостей ПО по требованиям ОУД4	Заключение договора не позднее 01.07	Январь 2020	Санкции за несоблюдение с июля 2020
2	(Предварительная) оценка соответствия	Май 2020	-	Понять текущий уровень защиты
3	Модернизация технических средств защиты	Май – Декабрь 2020	-	Цель - выйти на 3 уровень соответствия к 01.01.2021 г.
4	Корректировка ОРД			
5	Тестирование на проникновение	Декабрь 2020	Вступило в силу!	Цели пентеста по 382 и 683 разные!
6	Применение мер по защите ПДн	Аудит ПДн с мая 2020	Апрель 2019	
7	Оценка соответствия	Ноябрь – Декабрь 2020	Январь 2021	Полноценная оценка по требованиям ГОСТ

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

Коростелев Павел
Руководитель отдела продвижения продуктов

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

По направлениям

ENDPOINT SECURITY	NETWORK SECURITY	VIRTUALIZATION SECURITY
СЗИ от НСД КСН HOST FW ПРОГРАММНАЯ СЕГМЕНТАЦИЯ ЛОКАЛЬНОЕ ШИФРОВАНИЕ СОВ (HIPS) АНТИВИРУС ДОВЕРЕННАЯ ЗАГРУЗКА	NGFW FW IDS/IPS WAF GOST VPN TLS/SSL	СЗИ ВИ МИКРОСЕГМЕНТАЦИЯ

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

По направлениям

ENDPOINT SECURITY	NETWORK SECURITY	VIRTUALIZATION SECURITY
Secret Net Studio Secret Net LSP Соболь	Континент 3.X Континент 4 UTM Континент TLS Континент WAF	vGate

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

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

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

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

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

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

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

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

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

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

Продуктовый вес

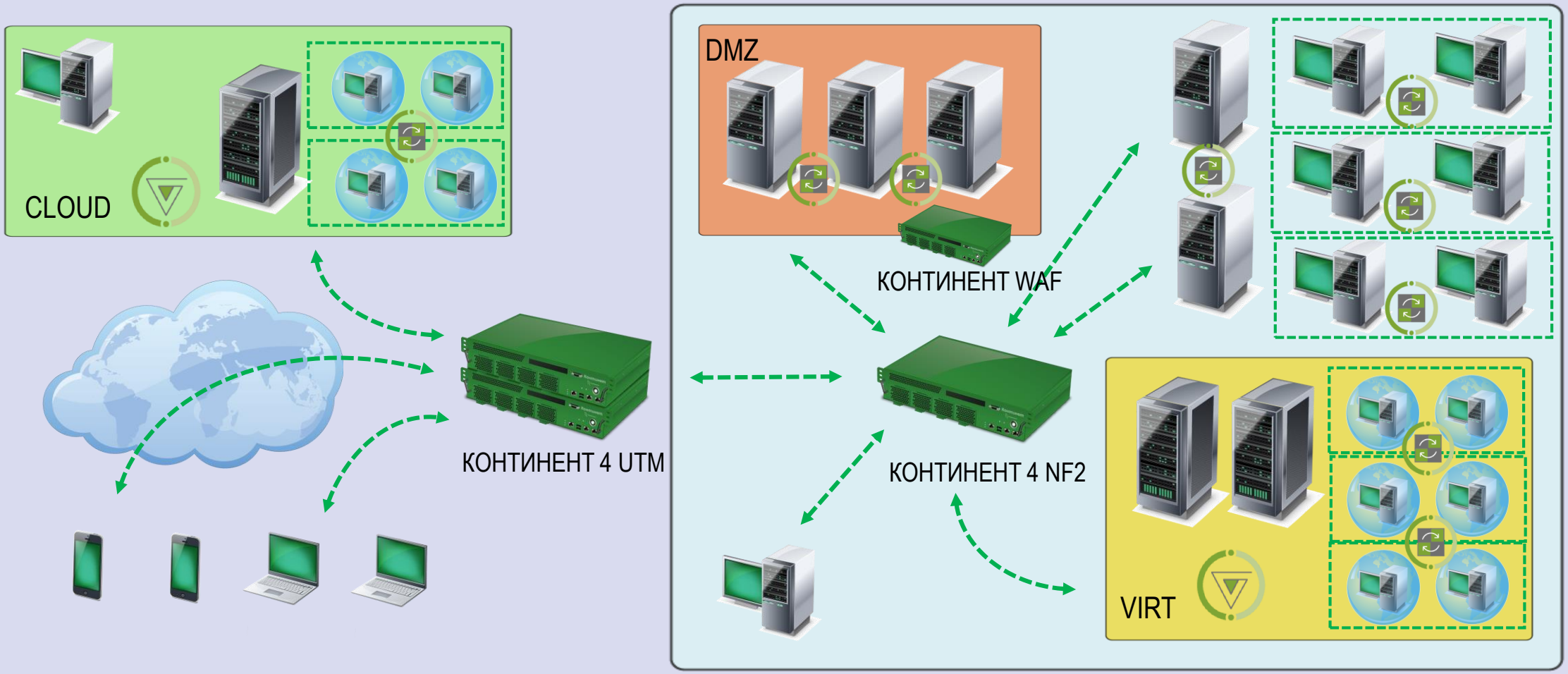
При условии что мы выполняем все необходимые организационные меры:

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



Спасибо за Внимание!

Ассоциация Российских Банков

SDK Systems
ИННОВАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ

Systems

+ 7 (499) 707 19 40

post@id-sys.ru

www.id-sys.ru

Региональные системы
Инжиниринговый центр

КОД БЕЗОПАСНОСТИ