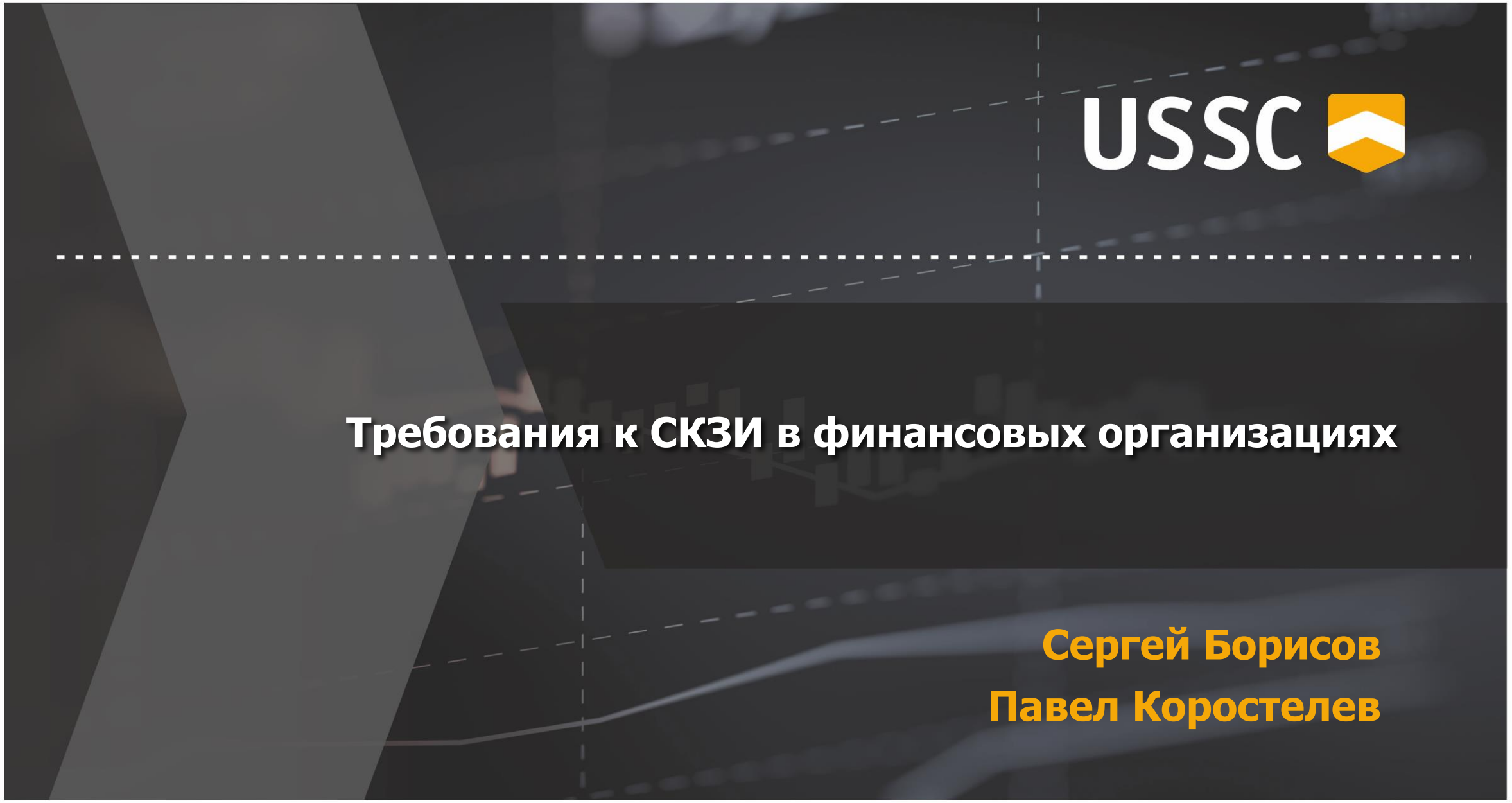


Требования к СКЗИ в финансовых организациях

Сергей Борисов
Павел Коростелев

График проведения вебинаров

№	Дата	Название
1	15.04	Требования Банка России по информационной безопасности некредитных финансовых организаций
2	22.04	Требования Банка России по информационной безопасности кредитных финансовых организаций
3	29.04	Анализ уязвимостей по требованиям к ОУД4
4	20.05	Обзор требований ГОСТ Р 57580.1-2017
5	17.06	Как проводится аудит по ГОСТ Р 57580?
6	08.07	Онлайн-сервис оценки соответствия ГОСТ Р 57580.2-2018
7	26.08	Требования к средствам криптографической защиты информации в финансовых организациях
8	16.09	Пентесты для финансовых организаций
9		Изменения в НПА по информационной безопасности финансовых организаций

Ведущие седьмого выпуска

Сергей Борисов

Заместитель руководителя по ИБ обособленного подразделения УЦСБ в г. Краснодар.

Работа в ИБ – 15 лет

sborisov@ussc.ru

https://sborisov.blogspot.com

Павел Коростелев

Руководитель отдела продвижения продуктов «Кода Безопасности»

Работа в ИБ – 11 лет

p.korostelev@securitycode.ru

План

- [ ] Обзор свежих НПА с требованиями к СКЗИ
- [ ] Типовые требования документации на СКЗИ и нарушения с СКЗИ, выявляемые Банком России
- [ ] Организационные мероприятия по реализации требований
- [ ] Технические решения, необходимые для реализации требований

КОД БЕЗОПАСНОСТИ

Требования к СКЗИ в финансовых организациях

Павел Коростелев, 26.08.2020

Старая гвардия

Федеральные законы	Приказы ФСБ
• №152-ФЗ «О персональных данных» • №63-ФЗ «Об электронной подписи» • №161-ФЗ «О национальной платежной системе»	• №378 «Об утверждении состава мер…» - защита ПДн с использованием СКЗИ • №66 «Об утверждении положения о разработке, производстве и эксплуатации СКЗИ» (Положение ПКЗ-2005) • Приказ ФАПСИ №152 «Об утверждении инструкции об организации и обеспечении безопасности…» – требования по эксплуатации СКЗИ

КОД БЕЗОПАСНОСТИ

СКЗИ в финансовом секторе

Отраслевые модели угроз

- Указание Банка России №3889-У - Про специальные ПДн
- Указание Банка России №4859-У - Про биометрические ПДн (ЕБС)

ГОСТ 57580

- РЗИ.14 – Использование СКЗИ КС2 для 1-го уровня ЗИ*
- КЗИ.3 - Контроль эксплуатации и использования технических мер ЗИ
- ЗСВ.27 - Запрет на копирование образов ВМ с загруженными ключами

382-П (НПС)

- 2.20 Требования к СКЗИ в информационной инфраструктуре
- 2.9.2 Встраивание СКЗИ в техпроцесс перевода денежных средств
- 2.9.3 Определяет порядок применения СКЗИ

672-П (ПС БР)

- 14.2 Защита взаимодействия между ОПКЦ и участниками СБП
- 14.3 Защита взаимодействия между ССНП и БР
- 14.4 Защита взаимодействия между ОПКЦ и БР

Предоставление информации

- ФНС России (440-П)
- ФТС России (390-П)
- РосФинМониторинг **(655-П)**
- Фонд социального страхования (562-П)

* В случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определенных в модели угроз и нарушителей безопасности информации финансовой организации.

Делает обязательным ГОСТ 57580

Закрепляет правильность работы с СКЗИ

Требует подписывать сообщения в соответствии с 63-ФЗ

Требует обеспечить долговременное хранение подписанных данных

КОД БЕЗОПАСНОСТИ

Новинка! Требования к СКЗИ в информационной инфраструктуре ПС (ФТ-56-3/32)

Документ определяет требования к техническим средствам и ПО, которые реализуют защиту в следующих объектах:

- Платежных устройствах с терминальным ядром (терминалы и банкоматы)
- Аппаратных модулях безопасности информационной инфраструктуры платежных систем (HSM модулях)
- Платежных картах
- Иных технических средствах информационной инфраструктуры платежной системы

Документ описывает:

- Модель нарушителя для СКЗИ
- Принципы построения СКЗИ в технических средствах информационной инфраструктуры ПС
- Принципы применения криптографических механизмов
- Принципы применения инженерно-криптографических механизмов защиты

Требования к технологиям обработки защищаемой информации в 683-П и 684-П

КОД БЕЗОПАСНОСТИ

При формировании, передаче и приеме сообщений

Должны быть обеспечены:

- Проверка правильности формирования сообщений
- Проверка правильности заполнения полей сообщения и права владельца электронной подписи
- Контроль дублирования сообщения
- Структурный контроль сообщений
- **Защита информации при передаче по каналам связи**

КОД БЕЗОПАСНОСТИ

При удостоверении прав клиентов на распоряжение средствами

Должны быть обеспечены:

- Подписание клиентом электронных сообщений электронной подписью, равнозначной подписью на бумажном носителе
- Получение от клиента подтверждения совершенной банковской операции

КОД БЕЗОПАСНОСТИ

При осуществлении банковских операции и учете результатов

Должны быть обеспечены:

- **Сверку выходных сообщений с соответствующими входными сообщениями**
- **Сверку результатов банковских операций с информацией в электронных сообщениях**
- Направление клиентам уведомлений об осуществлении банковских операций (если предусмотрено законодательством

Долговременное хранение

Необходимо хранить пять лет:

- Электронные документы созданные при осуществлении банковских операций
- Информация о банковских операциях
- Данные о действиях работников
  - Дата и время осуществления банковской операции
  - Идентификатор работника
  - Код технологического участка
  - Результат банковской операции
  - Сетевой адрес АРМа
- Данные о действиях клиентов
  - Дата и время осуществления операции
  - Идентификатор клиента
  - Код технологического участка
  - Результат действия клиента
  - Идентификационная информация клиента
- Информация об инцидентах ИБ

План

- [x] Обзор свежих НПА с требованиями к СКЗИ
- [ ] Типовые требования документации на СКЗИ и нарушения с СКЗИ, выявляемые Банком России
- [ ] Организационные мероприятия по реализации требований
- [ ] Технические решения, необходимые для реализации требований

Примеры требований из документации на СКЗИ СКАД Сигнатура 6

Формуляр

1.2 Эксплуатирующая организация распечатывает и ведёт настоящий **формуляр** на бумаге. Формуляр должен находиться в подразделении, ответственном за эксплуатацию АПК «Средство КЗИ».

1.4 Сведения об установке/удалении АПК «Средство КЗИ» на каждой ЭВМ эксплуатирующая организация заносит в раздел «Сведения об установке» настоящего формуляра.

2.5 К установке, эксплуатации и сопровождению АПК «Средство КЗИ» **допускаются специалисты**, изучившие соответствующие эксплуатационные документы.

3.5 Варианты исполнения и выполняемые нормативные требования 3.5.1 АПК «Средство КЗИ» имеет два варианта исполнения: – исполнение 1, для которого использование средств защиты информации от несанкционированного доступа (СЗИ от НСД), сертифицированных ФСБ России, является рекомендательным; – исполнение 2, для которого **использование СЗИ от НСД, сертифицированных ФСБ России, является обязательным**.

3.8.3 Использование АПК «Средство КЗИ» совместно с указанными выше СЗИ от НСД допускается только при **наличии у них действующих сертификатов соответствия** требованиям к АПМДЗ по классу не ниже 3Б, выданных ФСБ России.

Примеры требований из документации на СКЗИ СКАД Сигнатура 5

Формуляр

2.14 Информационная безопасность АПК «Средство КЗИ СКАД «Сигнатура» версия 5» обеспечивается при условии отсутствия подключения вычислительных средств с установленным АПК «Средство КЗИ СКАД «Сигнатура» версия 5» к техническим средствам сетей общего пользования. Для передачи информации, поступающей от криптосредства и на криптосредство, допускается использование выходящих за пределы контролируемой зоны каналов связи, относящихся к корпоративной сети и оснащённых СЗИ от НСД (**межсетевыми экранами, сертифицированными по требованиям ФСБ России не ниже 4 класса защиты**). При этом должна быть обеспечена конфиденциальность передаваемой информации вне контролируемой зоны.

2.17 При эксплуатации СКЗИ должны использоваться **средства антивирусной защиты, сертифицированные ФСБ России по классу Б** (для применения на серверах) и классу В (для применения на рабочих станциях). В случае использования значительного количества рабочих мест с установленными СКЗИ целесообразно применять средства антивирусной защиты, сертифицированные ФСБ России по классу А.

2.18 АПК «Средство КЗИ СКАД «Сигнатура» версия 5» подлежит поэкземплярному учёту.

Примеры требований из документации на СКЗИ АПКШ «Континент»

Формуляр

4.1. Функционирование АПКШ "Континент" допустимо при **наличии действующих сертификатов** ФСБ России на ПАК "Соболь", СКЗИ "КриптоПро CSP" и СКЗИ М-506А-ХР (только для вариантов исполнения, в которых требуются сертифицированные СКЗИ "КриптоПро CSP" и СКЗИ М-506А-ХР).

Правила пользования

2.15 На компьютер с программой управления устанавливаются ПАК «Соболь»

2.22 В настройках BIOS Setup компонентов комплекса в качестве первого загрузочного устройства должен быть установлен НЖМД со штатной ОС и, если позволяет BIOS Setup, необходимо **исключить все остальные устройства из списка порядка загрузки**.

3.6 Помещение, в котором устанавливается комплекс, должно быть **аттестовано в соответствии с руководящими документами специально созданной комиссией**. Результатом работы комиссии является акт проверки выделенного помещения для работы с комплексом, утвержденный начальником организации-пользователя

3.9. Для хранения ключевых документов (ключевой носитель с наклейкой или нанесенной маркировкой, обеспечивающей поэкземплярный учет), нормативной и эксплуатационной документации помещение **оснащается металлическим шкафом** (хранилищем, сейфом), оборудованным внутренними замками с двумя экземплярами ключей и приспособлением для опечатывания. Дубликаты ключей от металлического шкафа и входных дверей помещения должны храниться в сейфе руководителя организации.

Примеры требований из документации на СКЗИ АПКШ «Континент»

USSC

Правила пользования

4.9. Администраторы безопасности организации (их обязанности могут выполнять администраторы безопасности АПКШ "Континент") **ведут Журнал абонента сети**, где записывают данные о полученных ключевых документах, результатах **ежесуточных проверок**, нештатных ситуациях, произошедших в сети.

7.6. К **системному блоку** АПКШ "Континент" должны применяться правила обращения с ключевыми носителями вследствие хранения ключевой информации в энергонезависимой памяти ПАК "Соболь".

7.23 При установке программного обеспечения СКЗИ следует:

- На технических средствах, предназначенных для работы с СКЗИ, использовать только **лицензионное программное обеспечение** фирм-изготовителей.
- При установке ПО СКЗИ на компьютер должен быть обеспечен **контроль целостности** и достоверность дистрибутива СКЗИ, совместно поставляемых с СКЗИ компонентов среды функционирования криптосредства, а также компонентов операционной системы, используемых при работе СКЗИ.
- Для обеспечения **антивирусной защиты** может использоваться сертифицированное антивирусное ПО без оценки влияния:
  - Kaspersky Endpoint Security 10 для Windows;
  - Dr.Web Desktop Security Suite (для Windows).

Примеры требований из документации на СКЗИ «Континент TLS-сервер»

USSC

Формуляр

9.1. Функционирование СКЗИ "Континент TLS-сервер" допустимо только при наличии **действующего сертификата ФСБ** России на ПАК "Соболь".

9.5. TLS-сервер обеспечивает выполнение заявленных функций при реализации на предприятии (в организации) следующих ограничений по применению

• реализация мероприятий по антивирусной защите и обеспечение свободной от вирусов программной среды компьютеров внешнего периметра сети администрирования и сети администрирования инфраструктуры

Правила пользования

3.3.1. Для безопасности эксплуатации компьютеров и программного обеспечения должны выполняться организационно-технические и административные требования.

К ним относятся требования к физическому размещению компьютеров, установке на них программного обеспечения, средствам защиты от несанкционированного доступа (НСД) к ОС и управлению СКЗИ, обеспечению бесперебойного режима работы компьютеров.

Безопасность эксплуатации СКЗИ обеспечивается при его установке на технические средства, для которых выполнены действующие в РФ требования по защите информации от утечки по техническим каналам, в том числе по каналам связи, при этом если технические средства аттестованы на соответствие установленным требованиям по защите информации без учета канала связи, то для обеспечения защиты ключевой и цифровой открытой информации СКЗИ по уровню КС от утечки по каналу линейной передачи достаточно, чтобы канал связи был реализован в виде:

• радиоканалов GSM, GPRS, 3G/4G, Wi-Fi, а также других каналов мобильной или беспроводной связи, работающих в диапазоне частот несущей выше 800 МГц в цифровой модуляции штатного информационного сигнала;

• волоконно-оптической линии связи, уходящей за пределы контролируемой зоны;

• проводного канала связи с установленной в нем волоконно-оптической развязки и при условии расположения входного медиаконвертера (медь – ВОЛС) рядом с СКЗИ, а выходного медиаконвертера (ВОЛС – медь) на расстоянии не менее 1 метра от СКЗИ.

Примеры требований из документации на СКЗИ «Континент TLS-сервер»

Правила пользования

4.2.1. Администраторы безопасности организации (их обязанности могут выполнять администраторы безопасности сервера) **ведут журнал абонента сети**, где записывают данные о полученных ключевых документах, результатах ежесуточных проверок, нештатных ситуациях, произошедших в сети.

5.1.1. Аутентификация администратора при удаленном управлении осуществляется на основе сертификатов открытых ключей (сертификата управления) в пределах одной контролируемой зоны. Срок действия ключей – 1 год.

7.1.2. Право доступа к рабочему месту сервера **предоставляется** только администратору безопасности, **ознакомленному** с правилами пользования и изучившему эксплуатационную документацию, входящую в комплект поставки.

7.1.3. **Первое подключение** администратора (до загрузки сертификата) необходимо выполнять из изолированного или защищенного сегмента сети.

7.2.1. Период непрерывной работы всех компонентов СКЗИ без выключения питания не должен превышать 1 сутки. По окончании этого срока **необходимо проводить перезагрузку** компьютера с установленными компонентами СКЗИ.

Типовые нарушения выявляемые Банком России

Выявленные недостатки	Приводит к нарушению НПА
невыполнение уничтожения путем переформатирования ключевых носителей с ключами электронной подписи, срок действия которых истек	• п. 3 Положения Банка России № 684-П в части необеспечения защиты информации с помощью СКЗИ в соответствии с технической документацией; • п. 1 ст. 8 Федерального закона № 75-ФЗ в части осуществления деятельности не на основании нормативных актов Банка России
незаполнение формуляров на средства СКЗИ, в том числе отсутствие записей о закреплении изделия за ответственным лицом и записи о проведении технического обслуживания	п. 3 Положения Банка России № 684-П в части эксплуатации СКЗИ без учета требований технической документации
эксплуатация СКЗИ не в полном соответствии с требованиями технической документации	п. 3 Положения Банка России № 684-П
использование СКЗИ российского производства с истекшим сроком действия сертификата соответствия ФСБ России	абз. 2 п. 4 Положения Банка России № 684-П
необеспечение безопасности процессов изготовления криптографических ключей СКЗИ организационными мерами защиты информации в соответствии с технической документацией СКЗИ	абз. 3 п. 4 Положения Банка России № 684-П

Типовые нарушения выявляемые Банком России

Примеры нарушений технической документации на СКЗИ

Необеспечение защиты BIOS серверов СКЗИ	• необеспечение применения политики назначения паролей для входа в BIOS; • необеспечение защиты настроек BIOS паролем
Необеспечение отключения альтернативных вариантов загрузки ОС в BIOS серверов СКЗИ	• необеспечение отключения в BIOS альтернативных вариантов загрузки, в том числе сетевой; • неисключение возможностей загрузки и использования ОС, отличной от предусмотренной штатной работой
Необеспечение ввода в эксплуатацию рабочего места, оснащенного СКЗИ	• необеспечение ввода в эксплуатацию рабочего места, оснащенного СКЗИ, и отсутствие акта о вводе в эксплуатацию по типовой форме
Необеспечение установки обновлений ОС СКЗИ	• необеспечение установки последнего известного на момент установки пакета обновления ОС и всех известных критических обновлений, опубликованных производителем ОС; • необеспечение установки последних обновлений безопасности пакетов, установленных ОС, а также настройки скачивания выходящих обновлений безопасности в автоматическом режиме

Типовые нарушения выявляемые Банком России

Примеры нарушений технической документации на СКЗИ

Отсутствие регламентации деятельности администраторов СКЗИ	Отсутствие регламентации деятельности администраторов согласно требованиям инструкций, определяющих порядок и правила выполнения администраторами своих функциональных обязанностей
Необеспечение применения мер по защите аппаратной части технических средств СКЗИ	Необеспечение мер, исключающих возможность несанкционированного, не обнаруживаемого изменения аппаратной части технических средств, на которых установлены СКЗИ
Необеспечение аттестации помещения, в котором находится СКЗИ	Неаттестация помещения, в котором установлено СКЗИ, в соответствии с руководящими документами специально созданной комиссией

План

- [x] Обзор свежих НПА с требованиями к СКЗИ
- [x] Типовые требования документации на СКЗИ и нарушения с СКЗИ, выявляемые Банком России
- [ ] Организационные мероприятия по реализации требований
- [ ] Технические решения, необходимые для реализации требований

Этапы внедрения систем защиты





Планирование → Приобретение → Разработка документации → Пуско-наладочные работы → Обучение

Эксплуатация

1. Планирование

- Необходимость сертифицированных СКЗИ
- Требуемые классы СКЗИ
- Выбрать исполнение СКЗИ
- Выбрать тип СЗИ от НСД (если есть вариативность)
- Выбрать носители ключей
- Сроки действия сертификатов
- Планы по продлению и выпуску новых версий СКЗИ от производителя
- Определить все места (АРМ, серверы, шлюзы) установки
- Определить ОС и технические характеристики
- Используемые среды виртуализации
- Планируемые помещения, в которых будет работа с СКЗИ
- Нужны ли централизованные системы мониторинга и управления, их иерархия
- С чем необходимо будет интегрироваться
- Кто будет администрировать, с каких АРМ
- У кого будут хранится дистрибутивы и документация

1. Планирование

- Количество дистрибутивов и документации
- Лицензии
- Техподдержка
- Подменные аппаратные средства

- Кто будет устанавливать - лицензиат или своими силами
- Обучены ли эти лица
- Производить настройку можно на отдельном стенде, потом уже отвезти на места установки
- Централизованная настройка или локальная
- Как (на каком УЦ) будут генерироваться ключи для пользователей и безопасно передаваться пользователям

2. Приобретение

Проверяем комплектность и ведем первоначальный учет

- аппаратные средства
- дистрибутивы
- документация
- сертификаты
- лицензии на право использования
- лицензии на техническую поддержку
- установочные ключи, закрытые ключи и справочники открытых ключей

Акты приема-передачи

Распределяем в подразделения

3. Подготовка документации

- Приказ об ответственности за эксплуатацию СКЗИ
  - функциональные обязанности администратора безопасности
  - правила доступа в помещения, где ведется эксплуатация СКЗИ
  - схема организации криптографической защиты
  - план проверок за соблюдением условий эксплуатации СКЗИ
  - перечень лиц, ответственных за эксплуатацию СКЗИ
  - перечень лиц, допущенных к работе с СКЗИ
  - перечень лиц, имеющих право доступа в помещения, где ведется эксплуатация СКЗИ
  - журнал поэкземплярного учета СКЗИ
  - журнал опломбирования аппаратных средств с СКЗИ
- Заключение о возможности допуска пользователей к работе с СКЗИ
- Заключение о возможности эксплуатации СКЗИ

3. Подготовка документации

- Формуляр
- Инструкция по эксплуатации сертифицированных средств СКЗИ
- Журнал учета эталонных дистрибутивов
- Журнал пользователя/абонента сети
- План действий в чрезвычайных ситуациях

4. Пусконаладочные работы

Кроме установки и настройки СКЗИ

- Учет получения СКЗИ, установки СКЗИ, генерации ключей, выдачи СКЗИ
- Проверка контрольных сумм установочного ПО
- Настройка контроля целостности установленного ПО
- Проверка наличия обновлений ОС и ПО
- Проверка отсутствия запрещенного ПО
- Настройка журналирования ОС и сбора логов
- Настройка BIOS или электронного замка
- Опечатывание и учет системных блоков с СКЗИ

5. Обучение

- Ознакомление лиц, ответственных за эксплуатацию с документацией на СКЗИ
- Памятка пользователя СКЗИ
- Инструктаж для пользователей СКЗИ
- Тестирование пользователей СКЗИ

6. Эксплуатация

Управление изменениями	Учет любых изменений СКЗИ
Контроль эффективности ИБ	Контроль соблюдения условий эксплуатации СКЗИ
Обеспечение непрерывности и восстановление	Действия с СКЗИ при ЧП
Реагирование на инциденты ИБ	Мероприятия при компрометации ключей
Обучение и повышение осведомленности в ИБ	Обучение по работе с СКЗИ
Управление обновлениями ПО	Обновление СКЗИ

План

- [x] Обзор свежих НПА с требованиями к СКЗИ
- [x] Типовые требования документации на СКЗИ и нарушения с СКЗИ, выявляемые Банком России
- [x] Организационные мероприятия по реализации требований
- [ ] Технические решения, необходимые для реализации требований

Технические решения

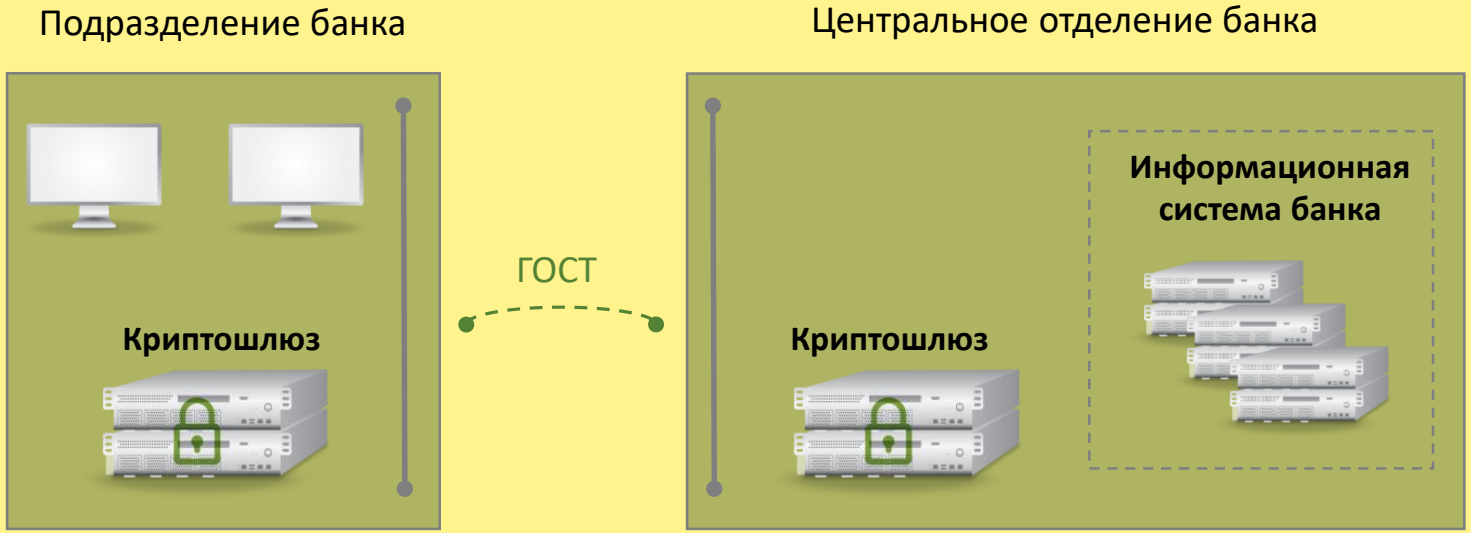
КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

Использование криптошлюза

Типовые кейсы:

- Защита канала связи между офисами

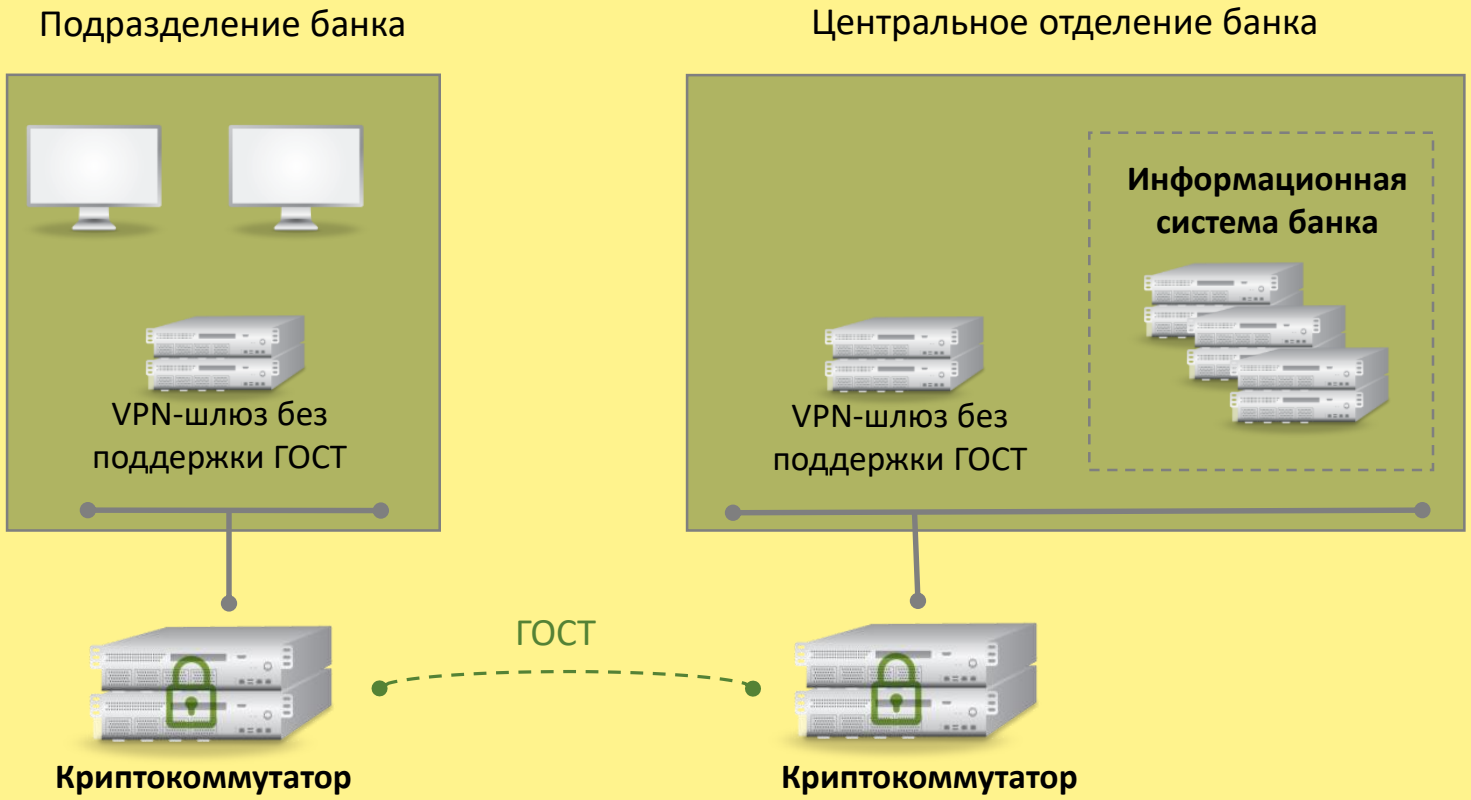


КОД БЕЗОПАСНОСТИ

Использование криптокоммутатора

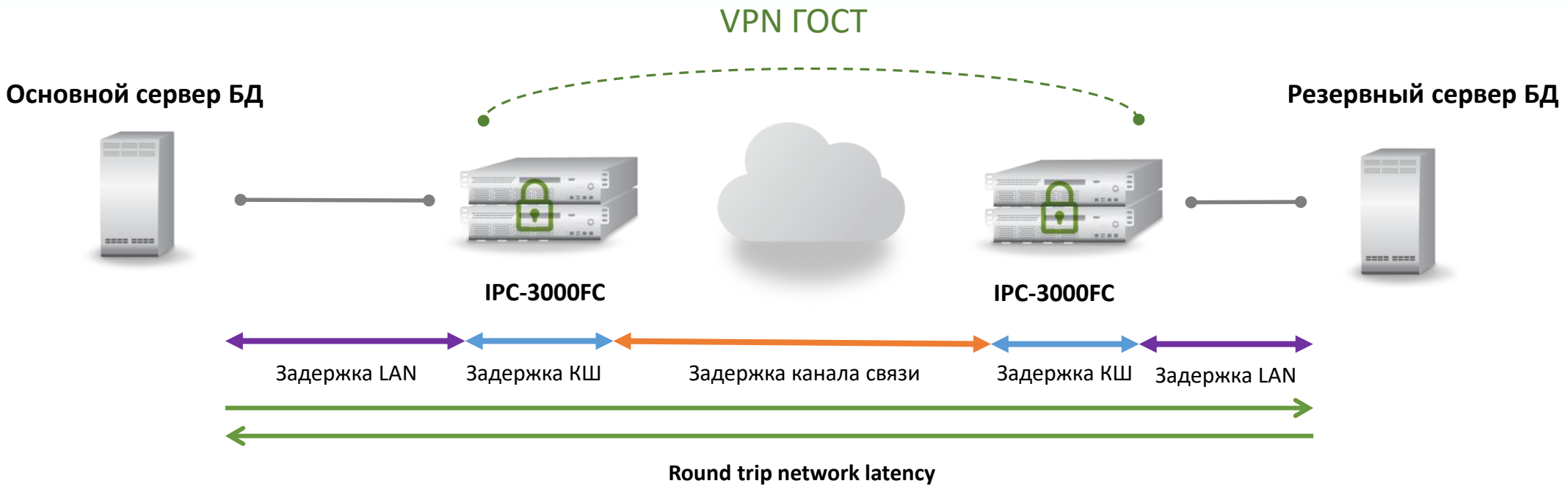
Типовые кейсы:

- Защита канала связи между ЦОД
- Внедрение ГОСТ без изменения топологии



КОД БЕЗОПАСНОСТИ

Важность задержки при резервировании СУБД



Для архитектора высоконагруженной БД очень важен параметр **Round trip network latency.** Это время затраченное на передачу пакета плюс время до получения пакета-подтверждения.

Он состоит из:

- задержка криптошлюза
- задержка локальной сети
- задержка канала связи

Задержка криптошлюза должна минимально влиять на общую задержку передачи данных

КОД БЕЗОПАСНОСТИ

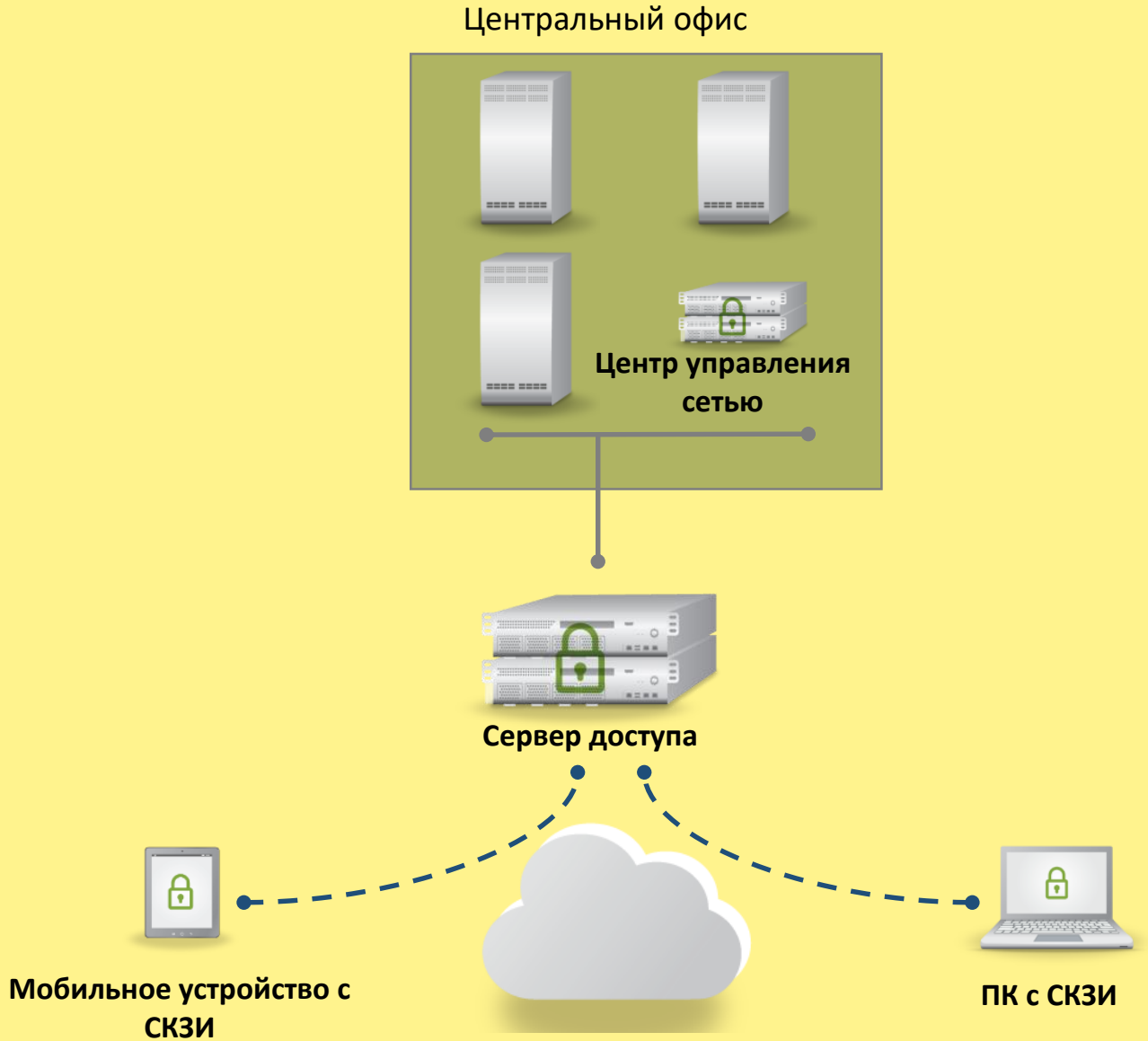
Использование VPN-клиента

Типовые кейсы:

- Защищенный удаленный доступ

Нюансы:

- Для КС2 и КС3 требуется наличие сертифицированного АПМДЗ
- Для КС3 требуется формирование замкнутой программной среды
- Сертификацией СЗИ от НСД в зависимости от СКЗИ могут быть:
  - СЗИ от НСД (Secret Net Studio, SecurePack Rus) сертифицированные по классу АК2-АК3
  - АПМДЗ



КОД БЕЗОПАСНОСТИ

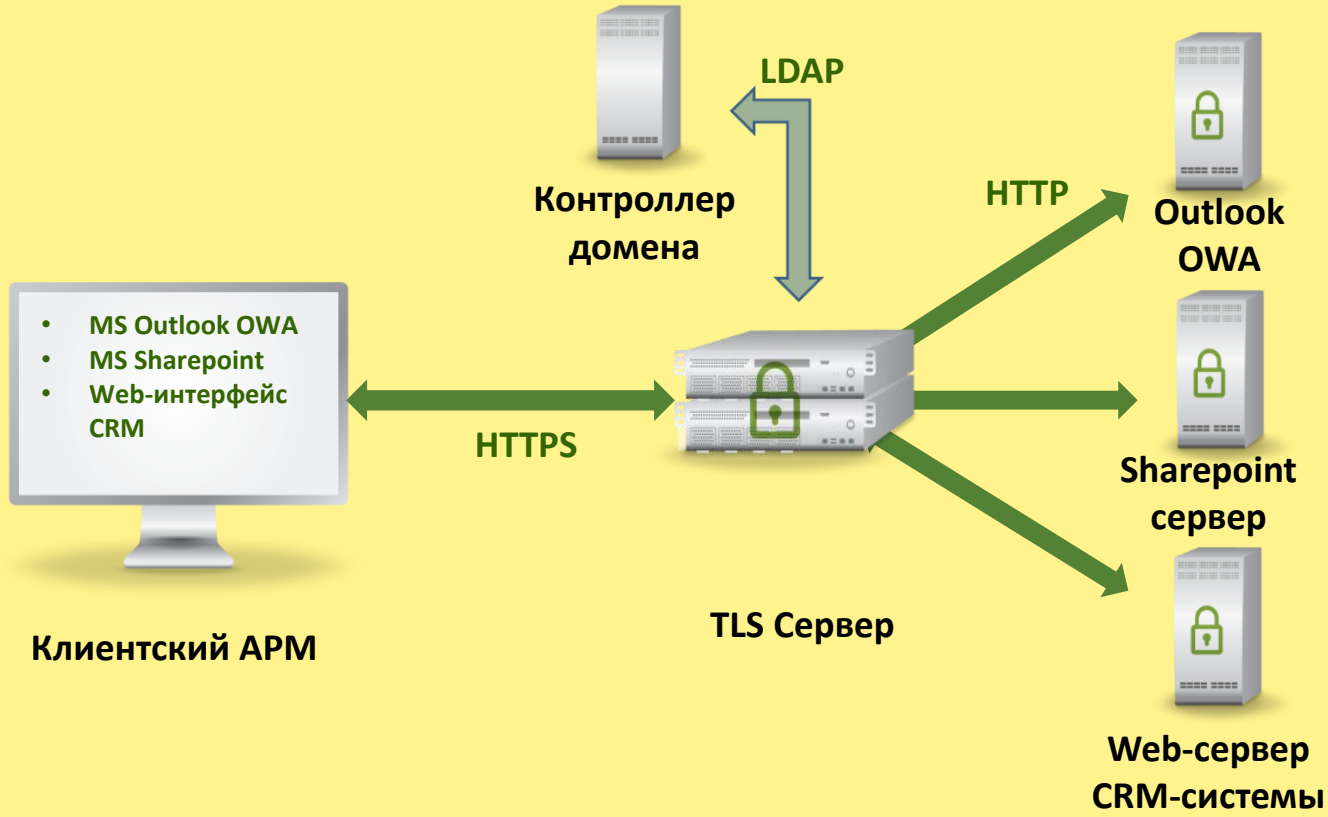
Использование TLS-сервера для защищенного удаленного доступа

Типовые кейсы:

- Защищенный удаленный доступ

Нюансы:

- Лучше изоляция сети от удаленного пользователя
- Лицензирование по числу одновременных подключений, а не целиком

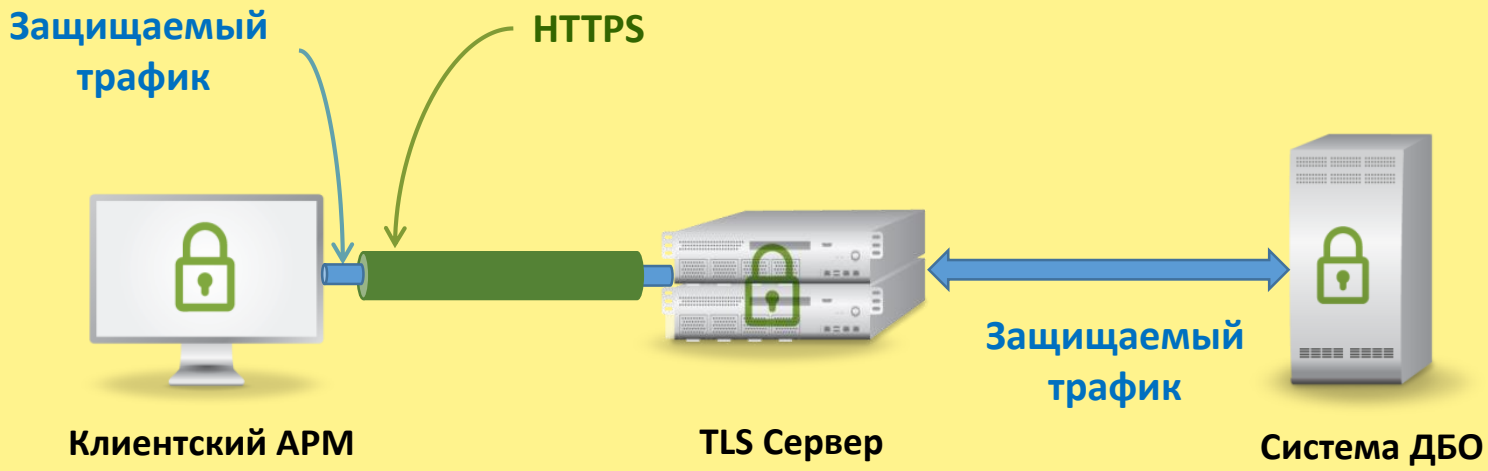


КОД БЕЗОПАСНОСТИ

Использование TLS-сервера для защиты ДБО

Типовые кейсы:

- Удаленный доступ к ДБО для юрлиц

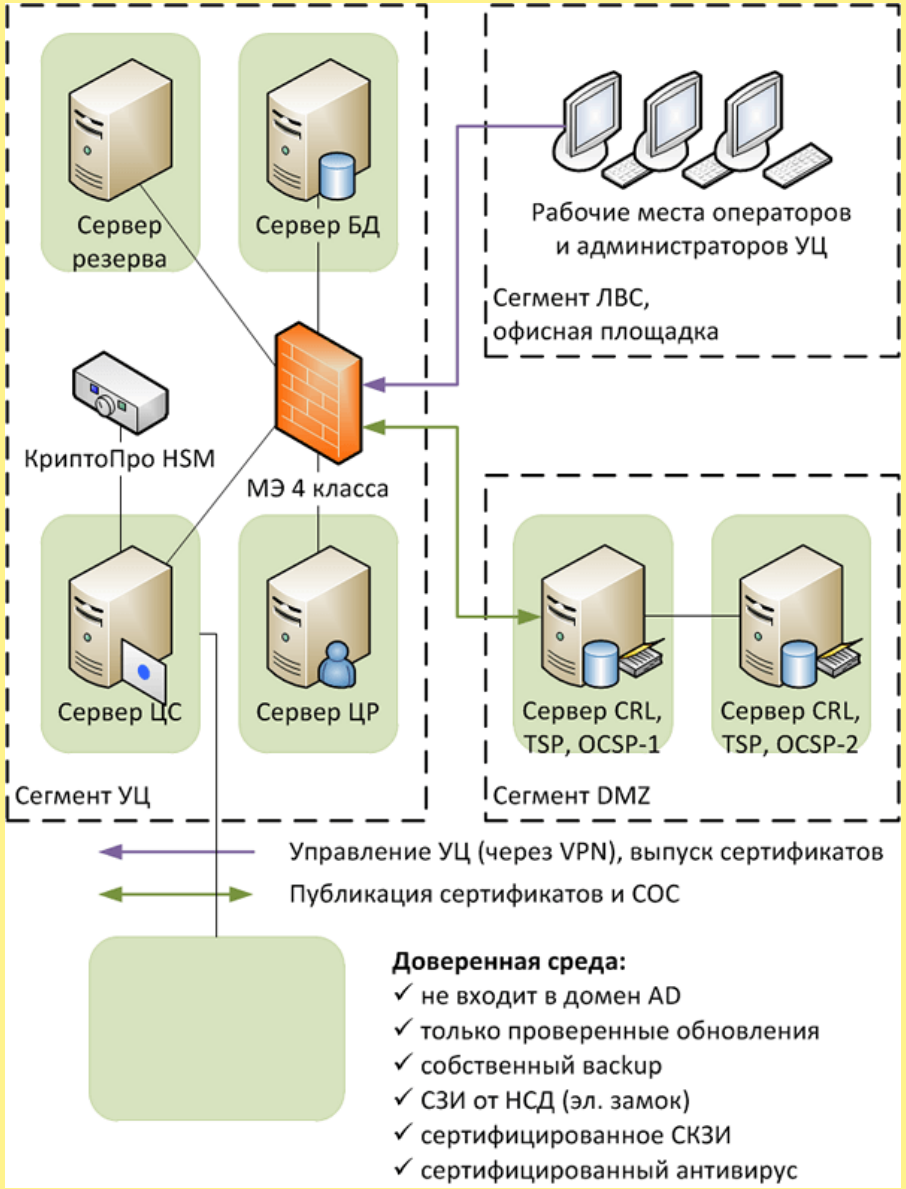


КОД БЕЗОПАСНОСТИ

Удостоверяющий центр

Типовые кейсы:

- Корпоративный УЦ

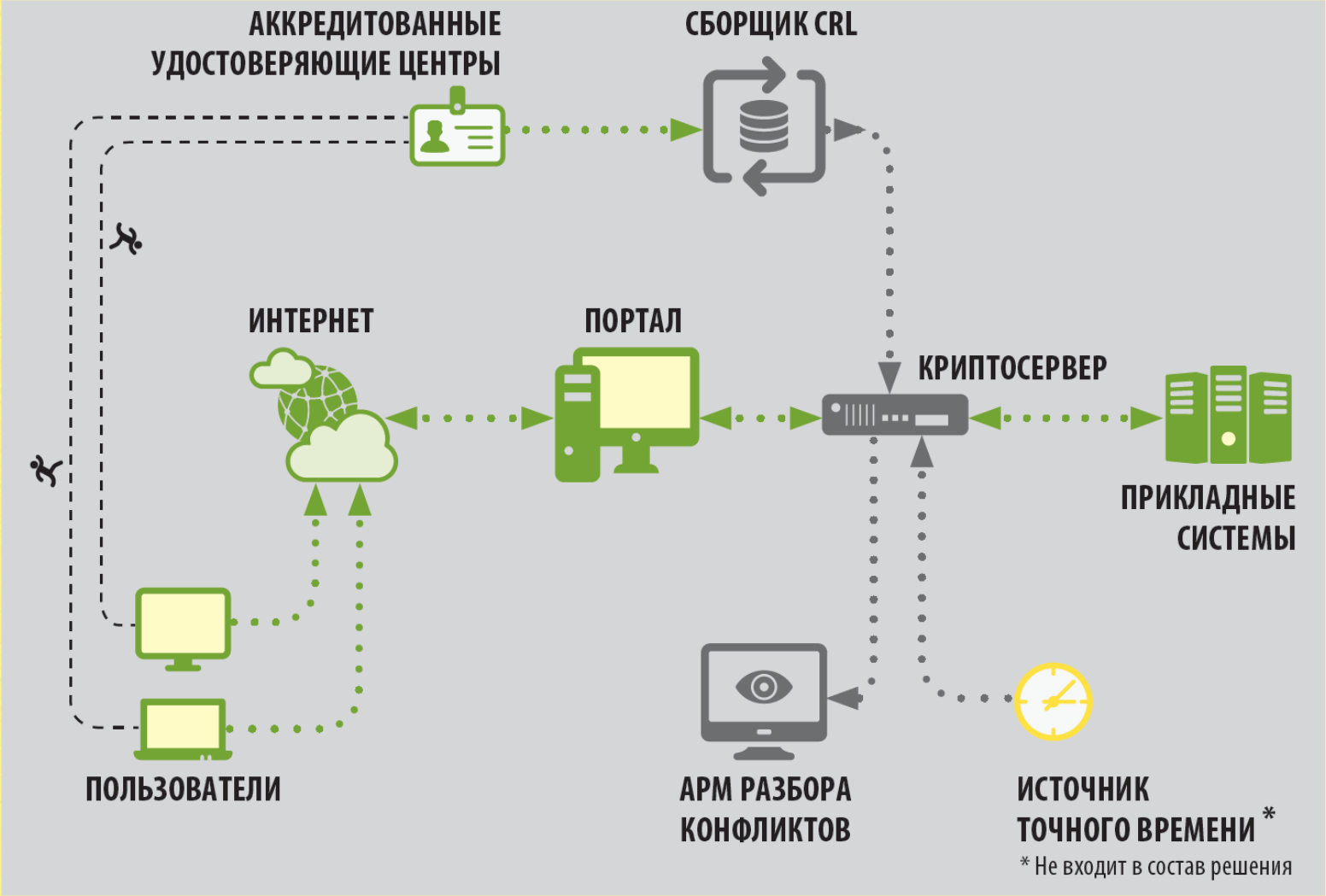


КОД БЕЗОПАСНОСТИ

Криптосервер

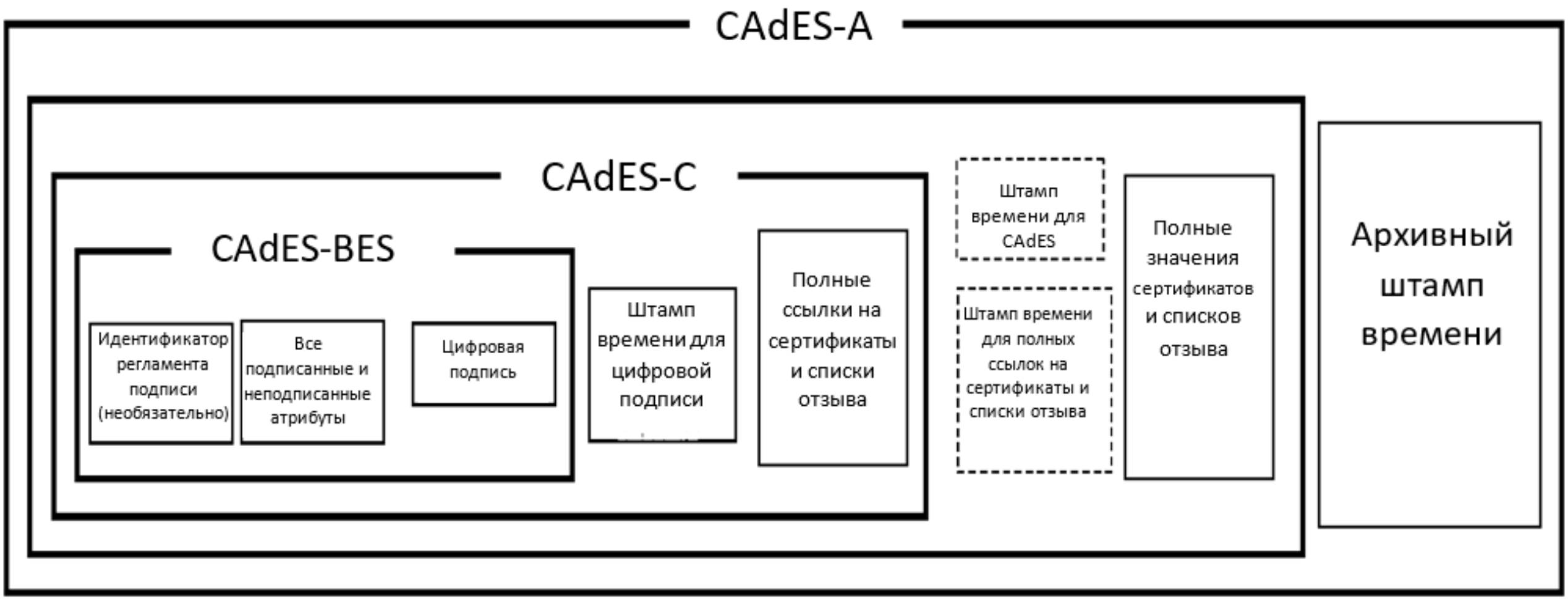
Типовые кейсы:
- Проверка ЭП
- Архивная ЭП для долговременного хранения

Нюансы:
- На больших объемах лучше масштабируется
- Архивные ЭП могут занимать больше места, чем сами документы



КОД БЕЗОПАСНОСТИ

Архивное хранение



Спасибо за внимание!

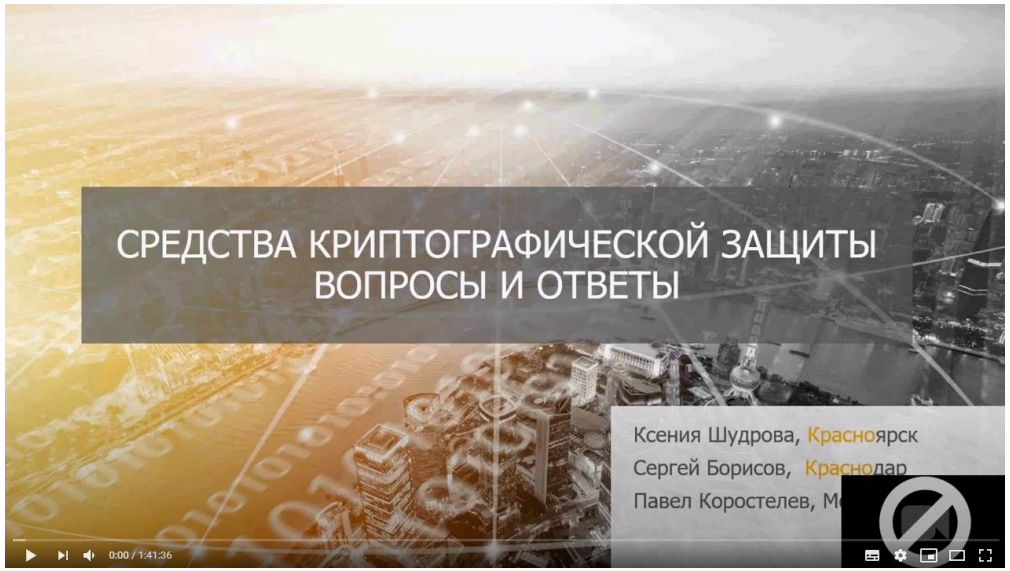
Павел Коростелев
p.korostelev@securitycode.ru

КОД БЕЗОПАСНОСТИ

info@securitycode.ru
http://securitycode.ru

Другие полезные вебинары по теме СКЗИ

[Совместный вебинар Кода Безопасности и УЦСБ по организации работы с СКЗИ]



[Межблогерский вебинар про СКЗИ. Вопросы и ответы]

Наши предложения для финансовых организаций

USSC

Оценка соответствия требованиям ГОСТ Р 57580

Тестирование на проникновение

Анализ уязвимостей по ОУД

Онлайн-сервис дистанционной оценки соответствия ГОСТ Р 57580

Комплексные аудиты

Предварительный аудит и приведение в соответствие с требованиями регуляторов

О компании

Опыт

Специалисты компании УЦСБ выполняют проекты в области информационной безопасности более 10 лет

Сертификации

Проектная команда - сотрудники с высшим профессиональным образованием по направлению подготовки 090100 «Информационная безопасность», имеющие сертификаты:

- Certified Information Systems Auditor (CISA);
- Certified Information Systems Security Professional (CISSP);
- Certified Information Security Manager (CISM);
- Cisco Certified Internetwork Expert (CCIE);
- Ethical Hacking and Penetration Testing (CEH);
- Computer Hacking Forensic Investigator (CHFI);
- Offensive Security Certified Professional (OSCP);
- Offensive Security Certified Expert (OSCE);

О компании

Уральский центр систем безопасности (УЦСБ) – компания-эксперт в области безопасного использования информационных технологий. С 2007 года компания непрерывно развивается, наращивает компетенции и выполняет все более сложные проекты.

Компетенции

- **Информационные технологии**
- **Комплексы инженерно-технических средств охраны**
- **Анализ защищенности**
- **Сервисное обслуживание**
- **Информационная безопасность**
- **Информационные инфраструктуры**
- **Безопасность промышленных систем автоматизации и управления**

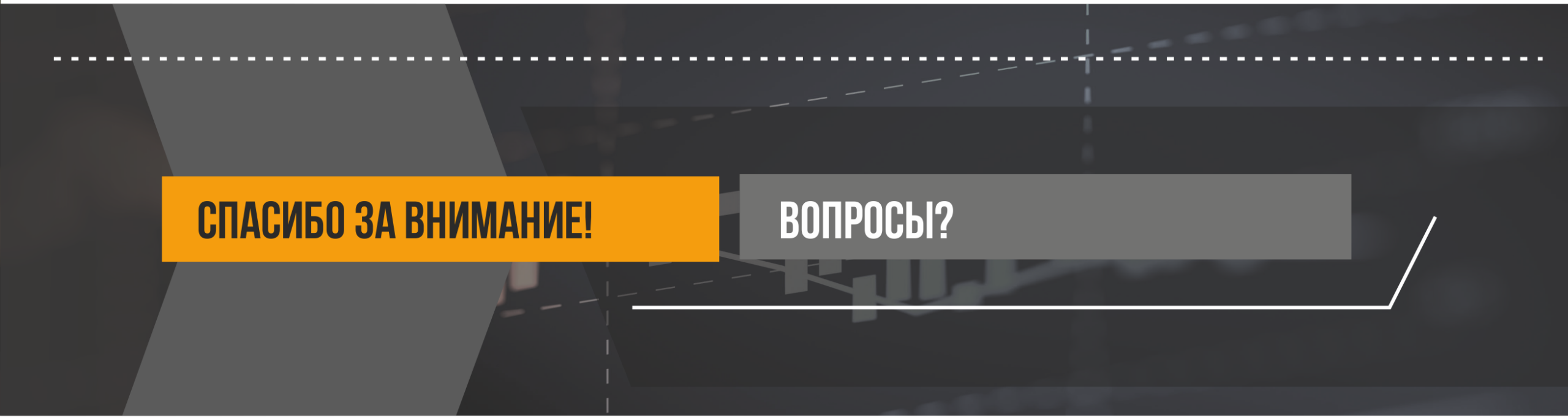
USSC.RU

620100, г. Екатеринбург, ул. Ткачей, д. 6
620100, г. Екатеринбург, ул. Ткачей, д. 23

Тел.: +7 (343) 379-98-34,
e-mail: info@ussc.ru

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ

USSC



СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

НОВЫЙ СЕЗОН ВЕБИНАРОВ:

БЕЗОПАСНОСТЬ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Борисов Сергей

УЦСБ

sborisov@ussc.ru

Павел Коростелев

Код безопасности

p.korostelev@securitycode.ru

Telegram и Facebook группы: ИБ в Финсекторе