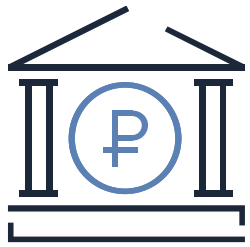
АБИСС

Ассоциация пользователей стандартов
по информационной безопасности АБИСС

конференция РусКрипто

ЗАКРЫТАЯ СЕКЦИЯ ДЛЯ ПРЕДСТАВИТЕЛЕЙ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ



Конференция РусКрипто
24.03.2021

АБИСС
Ассоциация пользователей стандартов
по информационной безопасности АБИСС

конференция
РусКрипто

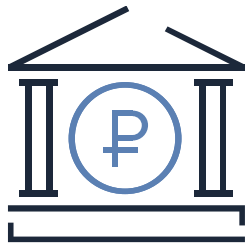
ЧАСТЬ I
РАЗГОВОР С РЕГУЛЯТОРОМ

АБИСС

Ассоциация пользователей стандартов
по информационной безопасности АБИСС

конференция РусКрипто

ЗАКРЫТАЯ СЕКЦИЯ ДЛЯ ПРЕДСТАВИТЕЛЕЙ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ



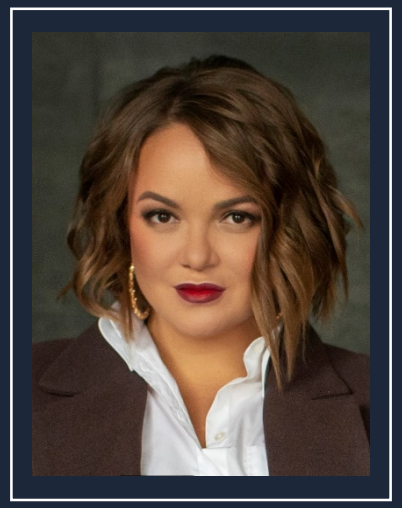
Конференция РусКрипто
24.03.2021

АБИСС
Ассоциация пользователей стандартов
по информационной безопасности АБИСС

конференция
РусКрипто

ЧАСТЬ I I
ПРАКТИЧЕСКИЕ АСПЕКТЫ

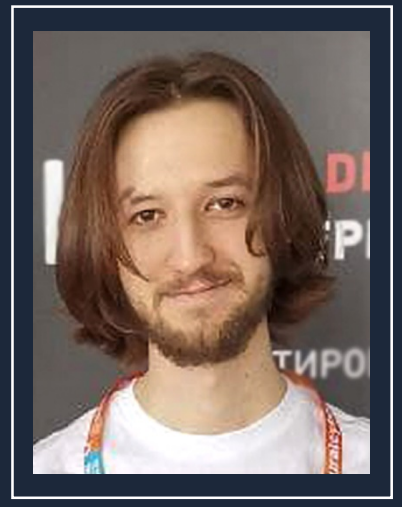
Эксперты Ассоциации АБИСС



Харыбина Анастасия,
председатель АБИСС,
директор по развитию
AKTIV.CONSULTING

Царев Евгений,
управляющий RTM Group

Свинцицкий Антон,
директор по консалтингу
ДиалогНаука



Иванцов Александр,
старший инженер
по защите информации
Deiteriy

Вопросы для обсуждения

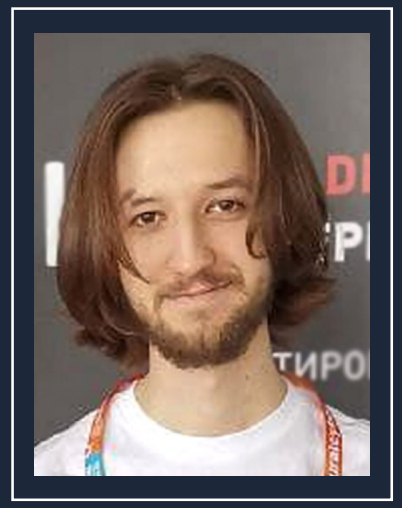
1. Новые требования Банка России по защите информации для кредитных и некредитных финансовых организаций
2. Выбор мер защиты информации путем составления модели нарушителя и модели угроз для финансовой организации
3. Проведение анализа уязвимостей программного обеспечения на ОУД4. Область оценки и пути ее прохождения
4. Тестирование на проникновение и (или) анализ защищенности
5. Повышение эффективности работы за счет объединения аудитов. Опыт проведения аудитов по PCI DSS, SWIFT и ГОСТ 57580
6. Особенности проведения оценки соответствия. Как подготовиться и пройти оценку соответствия в эпоху дистанционной работы

Новые требования Банка России по защите информации

Свинцицкий Антон,
дректор по консалтингу
ДиалогНаука

Положения Банка России по защите информации

Выбор мер защиты информации путем составления модели нарушителя и модели угроз для финансовой организации



Иванцов Александр,
старший инженер
по защите информации
Deiteriy

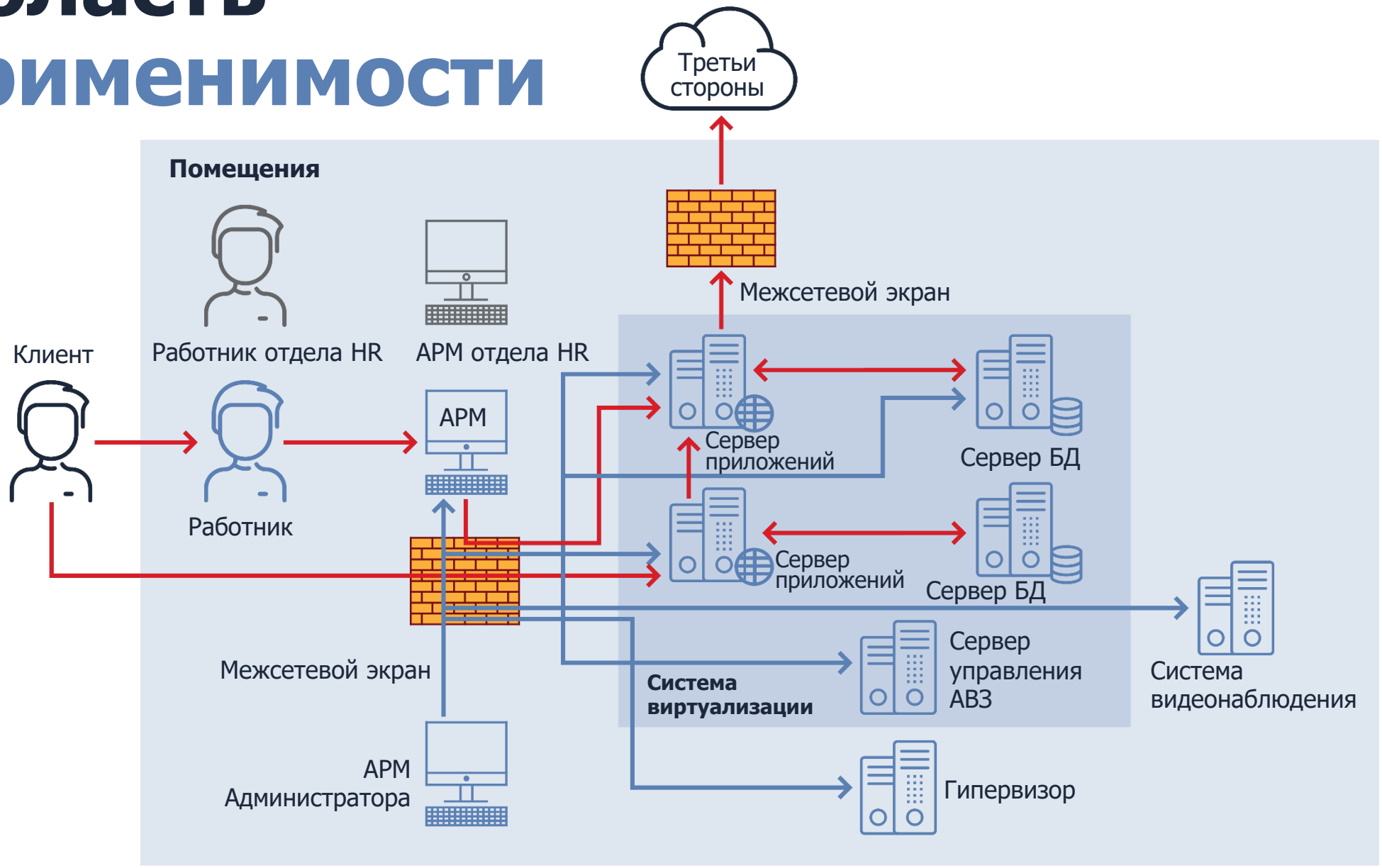
Область применимости

С чего начать подготовку к выбору мер защиты?
С определения области применимости

Область применимости определяется защищаемой информацией:

1. Информация о банковских (финансовых) операциях и состоянии счета
2. Информация, необходимая для авторизации клиентов
3. Ключевая информация СКЗИ
4. Конфигурация компонентов информационной инфраструктуры, в том числе средств защиты

Область применимости



Модель угроз и нарушителей

Что можно сделать с помощью модели угроз и нарушителей:

1

Исключить требования, связанные с неактуальными угрозами

2

Применить компенсирующие меры защиты вместо определенных в требованиях ГОСТ 57580.1-2017

3

Изменить требования для конкретных автоматизированных систем — через частные модели угроз

Примеры компенсационных мер

- Замена технических мер защиты на организационные
- Использование устаревшей ОС на банкоматах
- Использование средств антивирусной защиты для Linux

Проведение анализа уязвимостей программного обеспечения на ОУД4

Царев Евгений,
управляющий RTM Group

ОУД4 – что смотреть

- ДБО — да
- АБС — ?
- АРМ КБР — нет (да)

ОУД4 – как глубоко смотреть

- Анализ уязвимостей
- Оценка соответствия
- Профиль защиты

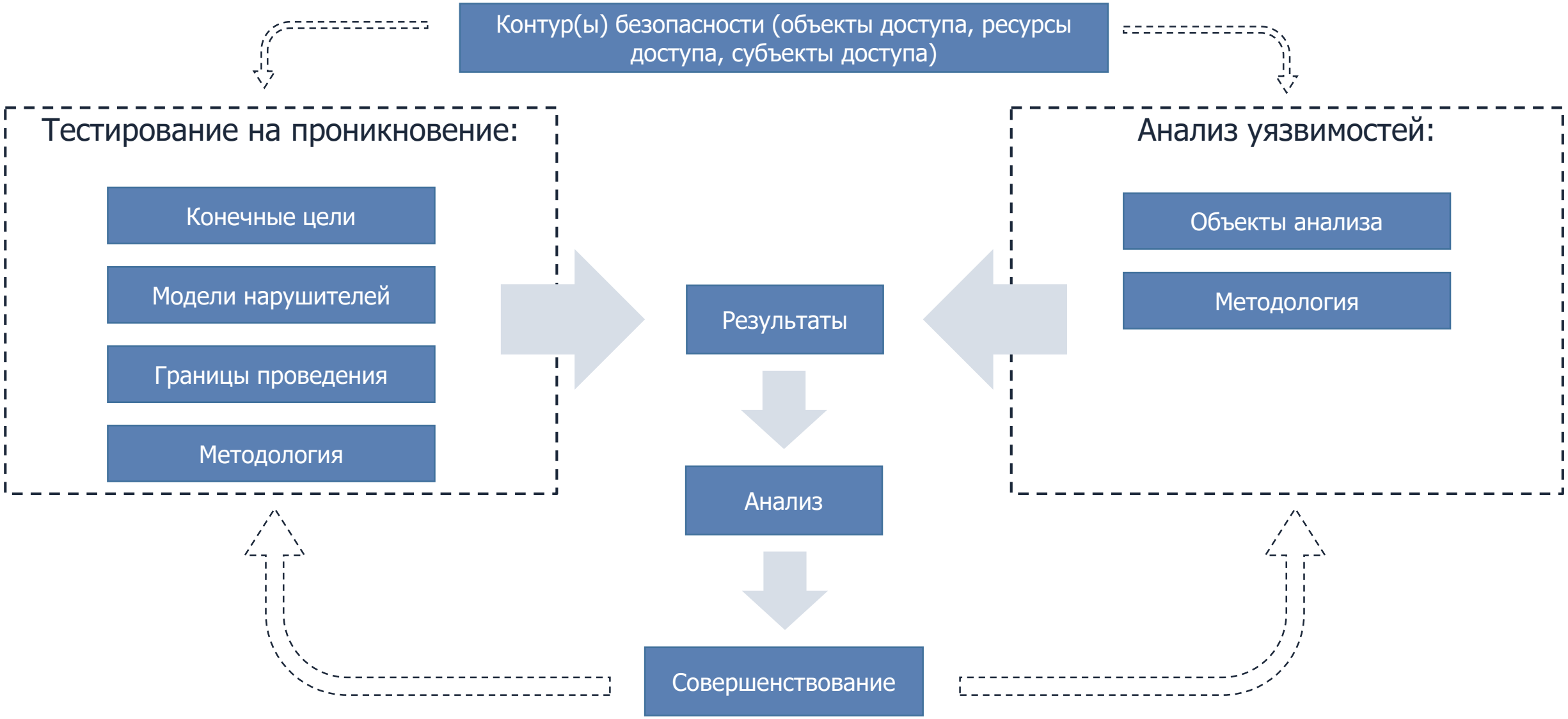
ОУД4 – единственный вариант?

- Сертификация по НДВ
- Сертификация по 131 приказу ФСТЭК

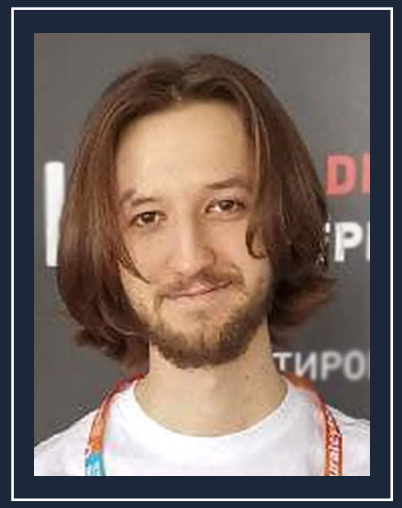
Тестирование на проникновение и (или?) анализ уязвимостей

Свинцицкий Антон,
дректор по консалтингу
ДиалогНаука

Тестирование на проникновение и (или?) анализ уязвимостей



Проведение оценок соответствия



Иванцов Александр,
старший инженер
по защите информации
Deiteriy

Периодичность проведения оценок соответствия

Стандарт	ГОСТ 57580	ГОСТ 57580 (контур Единой Биометрической Системы)	PCI DSS	SWIFT
Период	2 года	1 год	1 год	1 год
Требования к организации	Лицензия ФСТЭК на проведение работ и услуг: Положение о лицензировании деятельности по технической защите конфиденциальной информации, пункт 4, подпункты «б», «д», «е»		Организация должна быть включена в список Qualified Security Assessors на сайте совета PCI SSC	Опыт проведения оценок соответствия PCI DSS, ISO 27001, NIST SP 800-53, SWIFT CSP/CSCF
Требования к аудитору	—		Статус PCI Qualified Security Assessor	▪ Статус PCI QSA ▪ CISSP ▪ CISA ▪ CISM ▪ Ведущий аудитор ISO 27001 ▪ SANS GIAC

Оценка ГОСТ 57580.1 – нарушения

Выявленные при оценке нарушения, из-за которых могут возникнуть инциденты защиты информации, наносящие ущерб финансовой организации или ее клиентам, дополнительно фиксируются в отчете и снижают итоговую оценку

Примеры нарушений:

Осуществление доступа под разделяемыми неперсонифицированными учетными записями

Хранение паролей в открытом виде

Отсутствие применения средств защиты от воздействия вредоносного кода

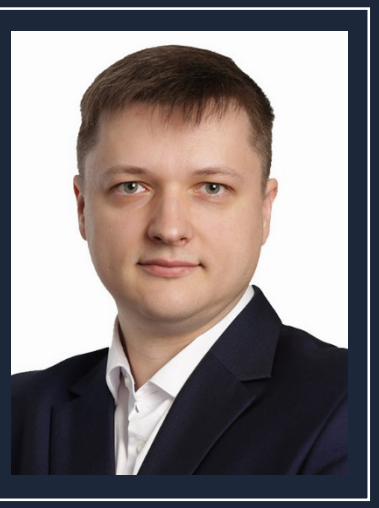
Как обработать нарушения?

Подготовить планы устранения!

Примеры нарушений:

1. Средства защиты от воздействия вредоносного кода не используются
2. Пароли хранятся в открытом виде
3. Не реализованы меры по предотвращению утечек информации
4. Для используемого прикладного ПО не проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже чем ОУД 4

Как подготовиться и пройти оценку соответствия в эпоху дистанционной работы



Царев Евгений,
управляющий RTM Group

Дистанционная работа и оценка соответствия

Организационные способы реализации аудита:

Интервью: Zoom, Skype и т.п.

Документы: Спецсвязь, СДЭК

Файлы данных: отчуждаемый носитель и Спецсвязь, запароленный архив, облако

Дистанционная работа
и оценка соответствия

Проблемы-решения:

1 **Доверие к подлинности файлов логов и скриншотов**

↓

Подписи на перечне свидетельств (приложение А)

2 **Временные задержки на спецсвязь**

↓

Не составляют глобальную проблему – необходимо сделать запас в сроках договора

Дистанционная работа и оценка соответствия

Проблемы-решения:

1 **Невозможность выделить время сотрудников проверяемой организации**

↓

Необходимо согласование на этапе подписания договора

2 **Трудности при анализе физической защищенности**

↓

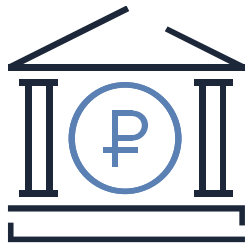
На помощь приходит видеосвязь!

АБИСС

Ассоциация пользователей стандартов
по информационной безопасности АБИСС

конференция РусКрипто

ЗАКРЫТАЯ СЕКЦИЯ ДЛЯ ПРЕДСТАВИТЕЛЕЙ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ



Конференция РусКрипто
24.03.2021