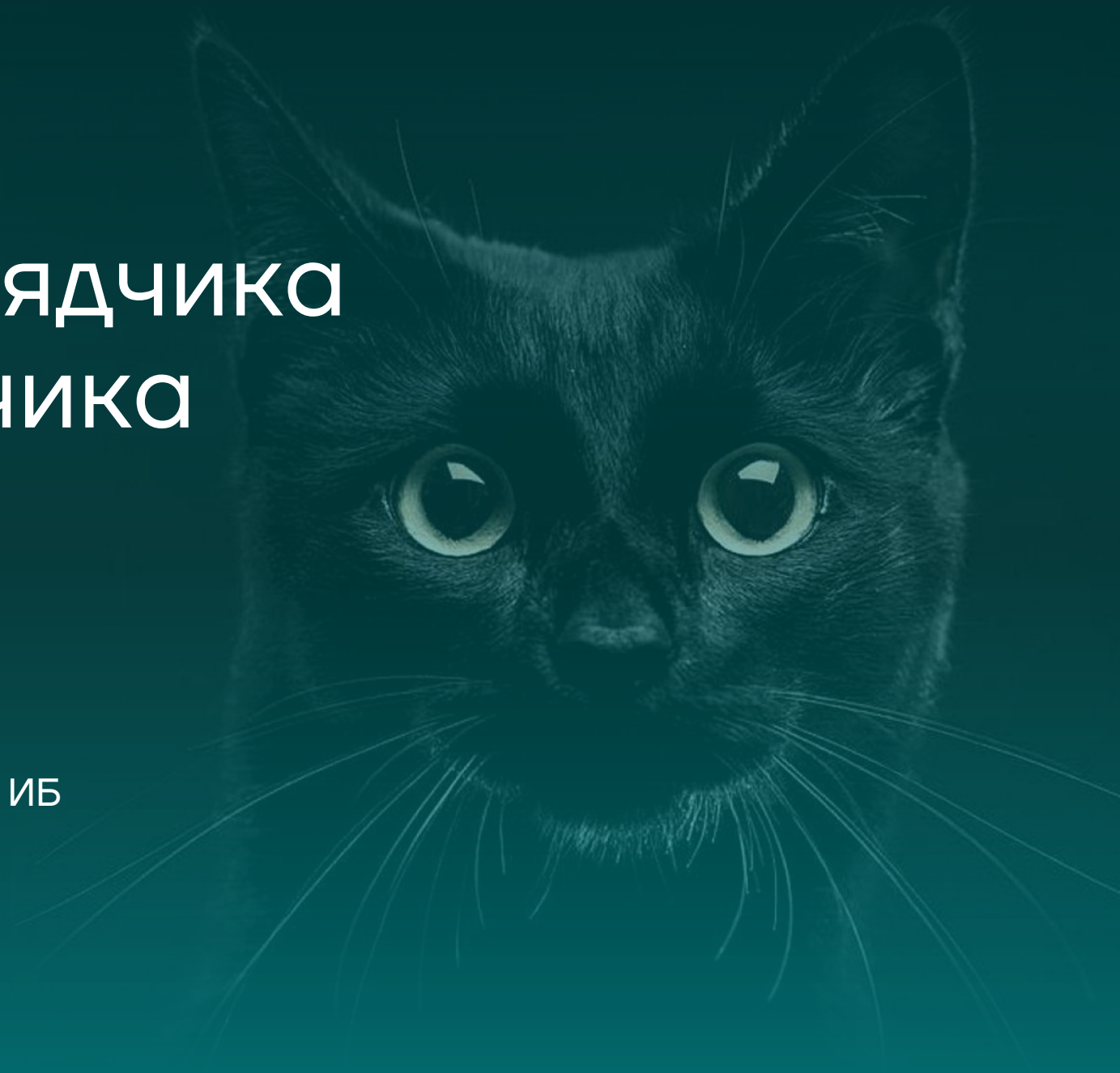




Оценка ИБ подрядчика глазами подрядчика



Игнатьева Алена
Руководитель отдела
консалтинга и аудита ИБ
STEP LOGIC
A_ignatyeva@step.ru
+7 963 061 27 48



Подрядчики

Поддержка
и обслуживание
инфраструктуры

Техподдержка

Администри-
рование

Колл-центр

Поддержка
сетей

Облачные и
инфраструктур-
ные сервисы

Iaas, Paas,
SaaS

Резервное
копирование
и восста-
новление

Процессинг

ИБ

Аудиты
и оценки
соответствия

Тестирование
на проник-
новение

Управление
инцидентами

Внедрение
и сопровож-
дение СЗИ

Бизнес-
приложения и
автоматизация

1С

ERP

CRM

Сайты

Разработка
и проектные
услуги

Разработка и
доработка ПО

Тестирование
и контроль
качества

ОУД

Миграция ИС

Обработчики
по поручению

Бухгалтерия

Кадры

Агенты по
привлечению

Коллекторы

Что включить в скоуп?

Скоуп определяется на всех уровнях: от физического оборудования до прикладного ПО, web- и почтовых ресурсов

Объекты и ресурсы доступа рассматриваются в совокупности с персоналом, который имеет доступ к данным и/или носителям

Если объект или ресурс не участвует в обработке защищаемых данных по заказкам из данного сектора, то его в скоуп не включаем



Примеры объектов оценки

ЭДО

Файловые серверы для хранения, «комнаты данных» и файлообменники

Серверы и АРМ для доступа подрядчиков к вашей инфраструктуре

Web-ресурсы, серверы для доступа ваших работников к инфраструктуре подрядчика

Электронная почта

Принтсерверы

Системы ВКС

Электронный архив документации

Сети передачи данных

СЗИ (особенно PAM, DLP)

Ресурсы SOC

Система резервного копирования

Заявочные системы

Среда разработки и тестирования

ML

Защищаемые данные для целей аудита



Сведения об ИТ-инфраструктуре, методах и средствах ЗИ и обеспечения операционной надежности заказчика, аттестационная документация, акты категорирования, акты определения уровня защищенности, протоколы сканирования уязвимостей...

Данные, используемые для аутентификации в инфраструктуре заказчиков (как для работников подрядчика, так и УЗ работников/клиентов заказчика и сервисные УЗ)

Ключевая информация (в т.ч. загруженные в виртуальные машины ключи)

Журналы событий из бизнес-систем заказчика

Применимость мер

ГОСТ 57580.1-2017. СМЭ.4, СМЭ.5,
ВСА.1, ВСА.2, ВСА.13, ЦЗИ.1, ЦЗИ.2,
ЗВК.15, ЗВК.16 «... и иными сетями
финансовой организации»

Мера неприменима? Оцениваем
реализацию только если взаимодействуем
с сетями финансовой организации? Или?

МД ФСТЭК России от 12.04.2026.
Беспроводной доступ

Если в документах установлен запрет на
использование беспроводных сетей и нет
санкционированных точек беспроводного
доступа, но сигнал не глушим, то меры
неприменимы?

Кто будет проверять проверяющих?

Объективность оценки /
Риски для бизнеса

Инфраструктура
оценщика может быть
скомпрометирована
как во время работ, так
и после их завершения

Оценщик должен
подтвердить свой
уровень зрелости

Доверие к результатам

- Непредвзятость
- «Следы» проверки

Оценщик —
прямой конкурент



На что обратить внимание в отчете об оценке подрядчика

Описание скоупа проверки и инфраструктуры, которую подрядчик использует для работы с вами

Свидетельства. Возможно ли контролировать фактическое выполнение в ходе ваших работ?

Какие меры не были оценены и почему?

Готовность подрядчика совместно с вами отвечать на запросы надзорных органов

Участники группы оценки. Штатные действующие работники подрядчика? Это те же исполнители, что выполняют работы?



Спасибо за внимание!



Игнатьева Алена
Руководитель отдела
консалтинга и аудита ИБ
STEP LOGIC
A_ignatyeva@step.ru
+7 963 061 27 48