2024

www.it-bastion.com

2024

ПРАКТИЧЕСКИ БЕЗОПАСНО ИЛИ ПРАКТИЧЕСКАЯ БЕЗОПАСНОСТЬ?
ИСПОЛЬЗОВАНИЕ КОМПЛЕКСА СКДПУ НТ В СЕГМЕНТЕ АСУ ТП

АЛЕКСАНДРА ГОНЧАРОВА

АЙТИБАСТИОН

КАКОВА НЕОБХОДИМОСТЬ ИБ-ИНФРАСТРУКТУРЫ В АСУ ТП?

АЙТИБАСТИОН

УРОВНИ ЗАЩИТЫ В АСУ ТП

Нормативный

Регламенты, персонал, соответствие требованиям регуляторов

Внутренний технологический

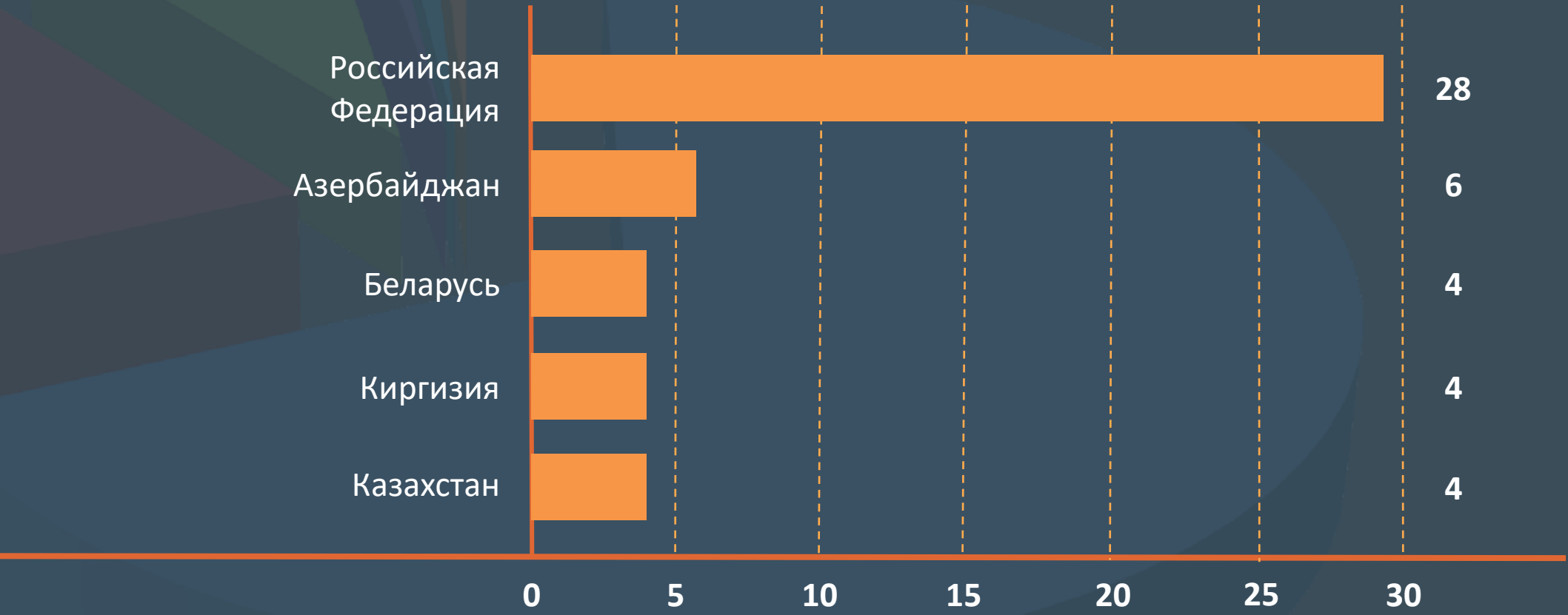
Система реагирования внутри контура АСУ ТП

Внешний технологический

Защита и контроль внешних подключений

АЙТИБАСТИОН

ТОП-5 АТАКУЕМЫХ ГОСУДАРСТВ В СНГ



По данным F.A.C.C.T., аналитический отчет «Киберпреступность в России и СНГ. Тренды, аналитика, прогнозы 2023-2024 гг.»

АЙТИБАСТИОН

ТОП-5 АТАКУЕМЫХ ОТРАСЛЕЙ В СНГ

По данным F.A.C.C.T., аналитический отчет «Киберпреступность в России и СНГ. Тренды, аналитика, прогнозы 2023-2024 гг.»

АТАКИ ПО ОТРАСЛЯМ АСУ ТП В РОССИИ

АЙТИБАСТИОН

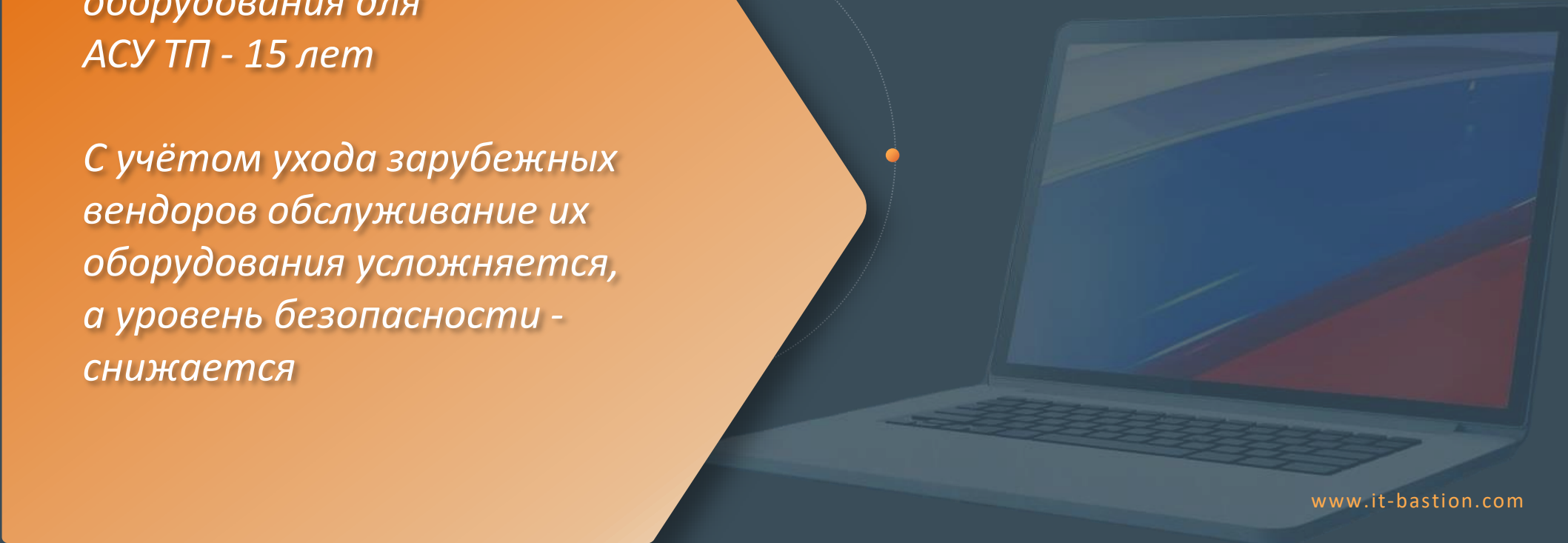
По данным Kaspersky ICS CERT

ИМПОРТОЗАМЕЩЕНИЕ
В АСУ ТП

АЙТИБАСТИОН

Средний срок жизни оборудования для АСУ ТП - 15 лет

С учётом ухода зарубежных вендоров обслуживание их оборудования усложняется, а уровень безопасности - снижается



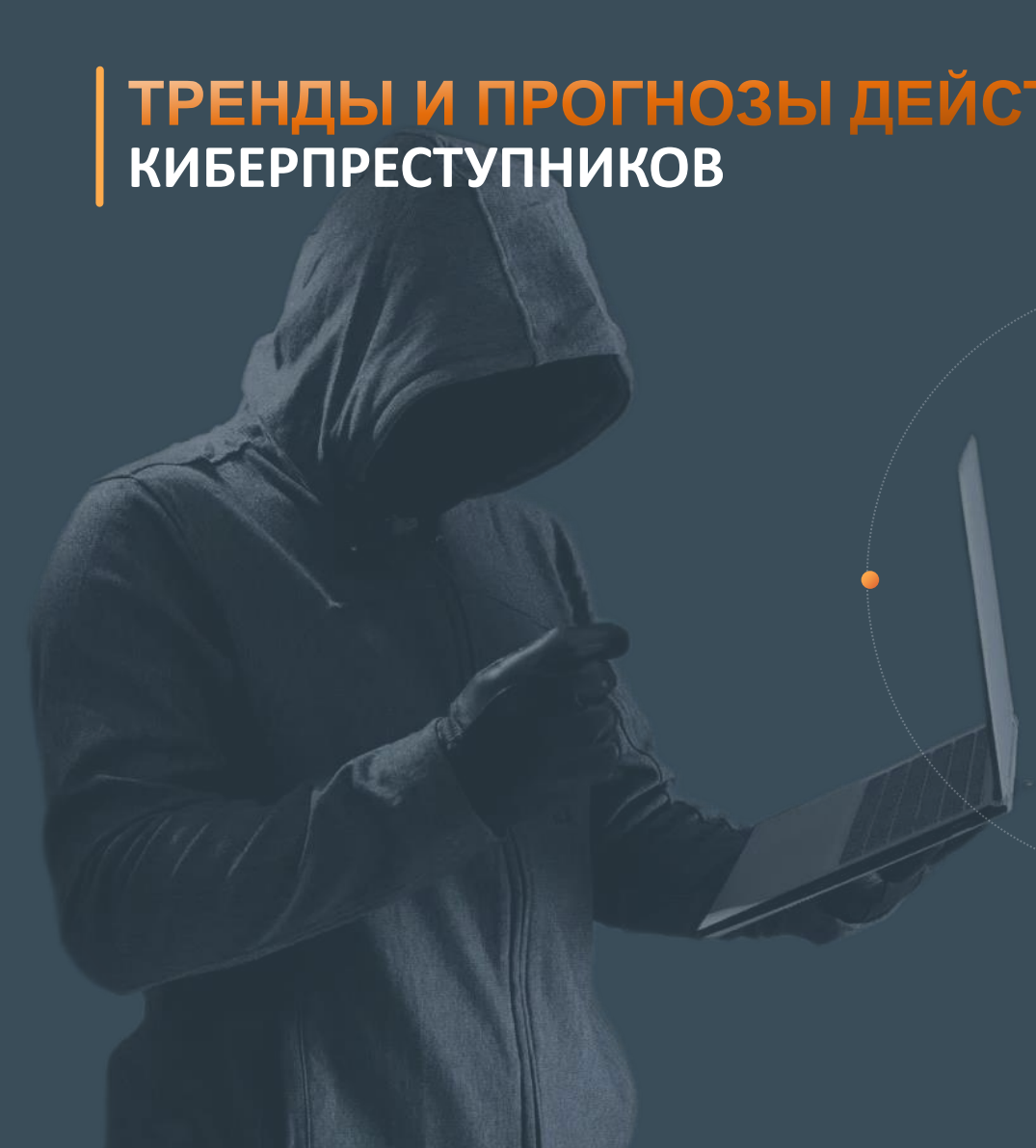
ИМПОРТОЗАМЕЩЕНИЕ
В АСУ ТП

АЙТИБАСТИОН

Используется эксклюзивное оборудование.

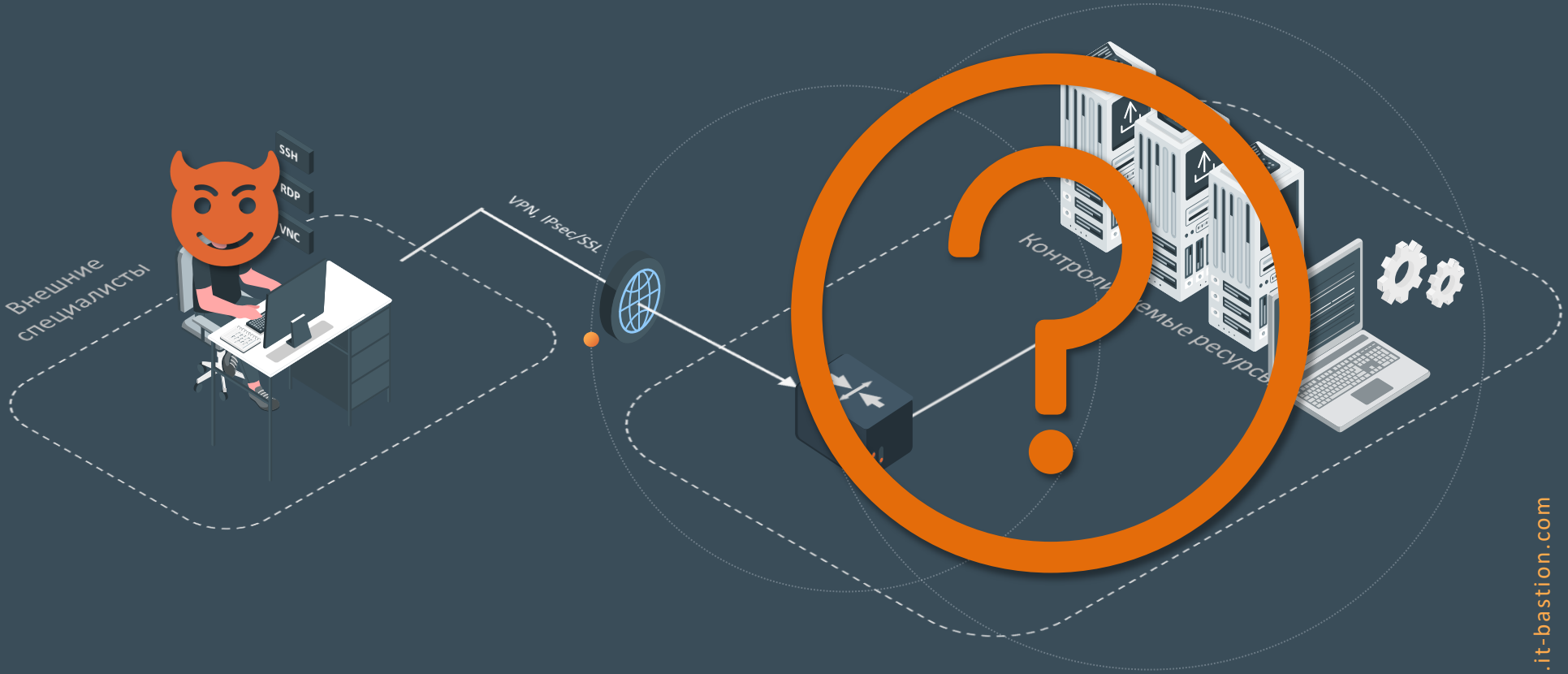
Для его обслуживания требуются специалисты с уникальной квалификацией, которых может быть всего несколько на всю страну

ТРЕНДЫ И ПРОГНОЗЫ ДЕЙСТВИЙ
КИБЕРПРЕСТУПНИКОВ

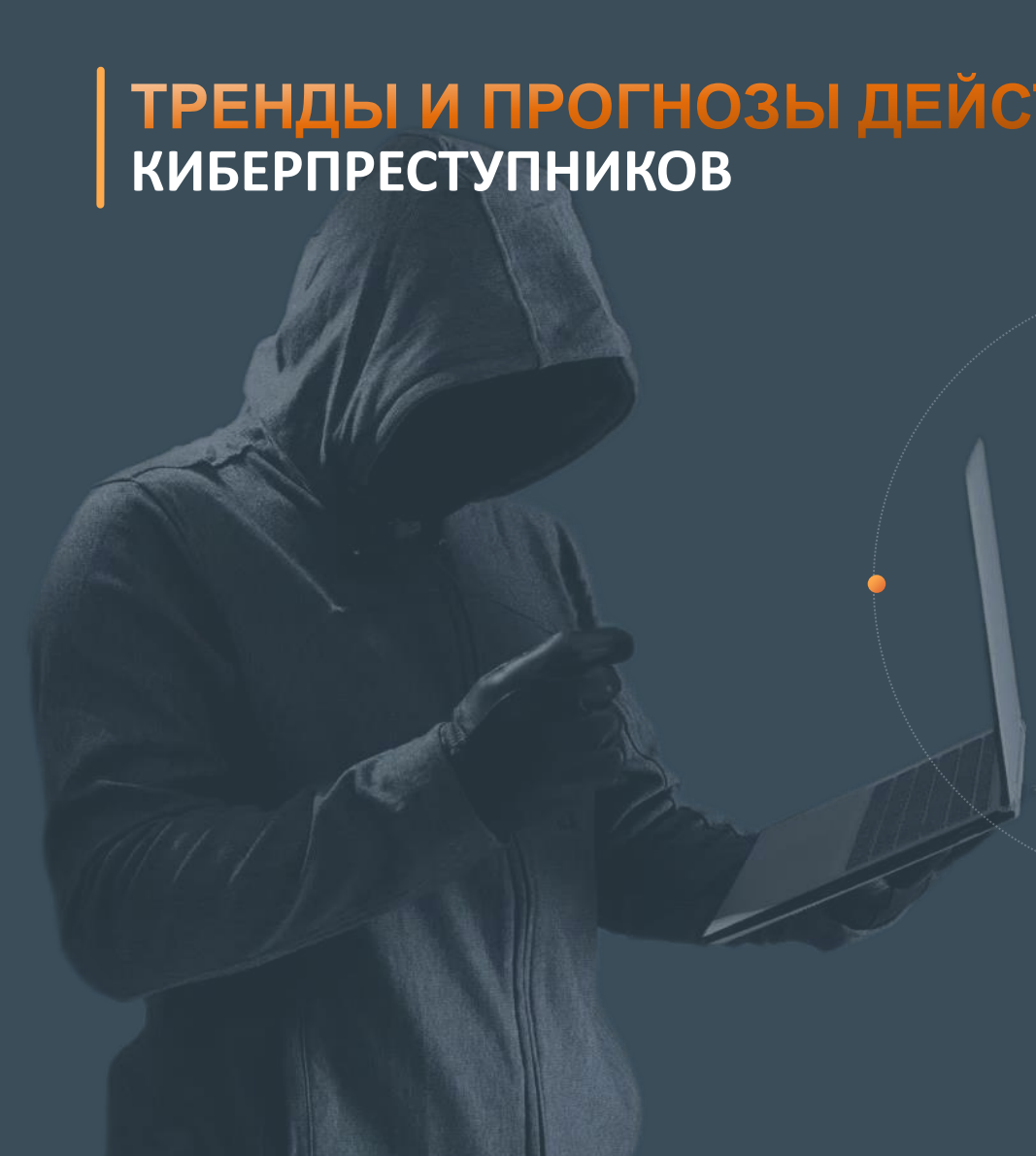


Мотивом киберпреступников зачастую становится не финансовая выгода, а политические взгляды.

ТРЕНДЫ И ПРОГНОЗЫ ДЕЙСТВИЙ
КИБЕРПРЕСТУПНИКОВ

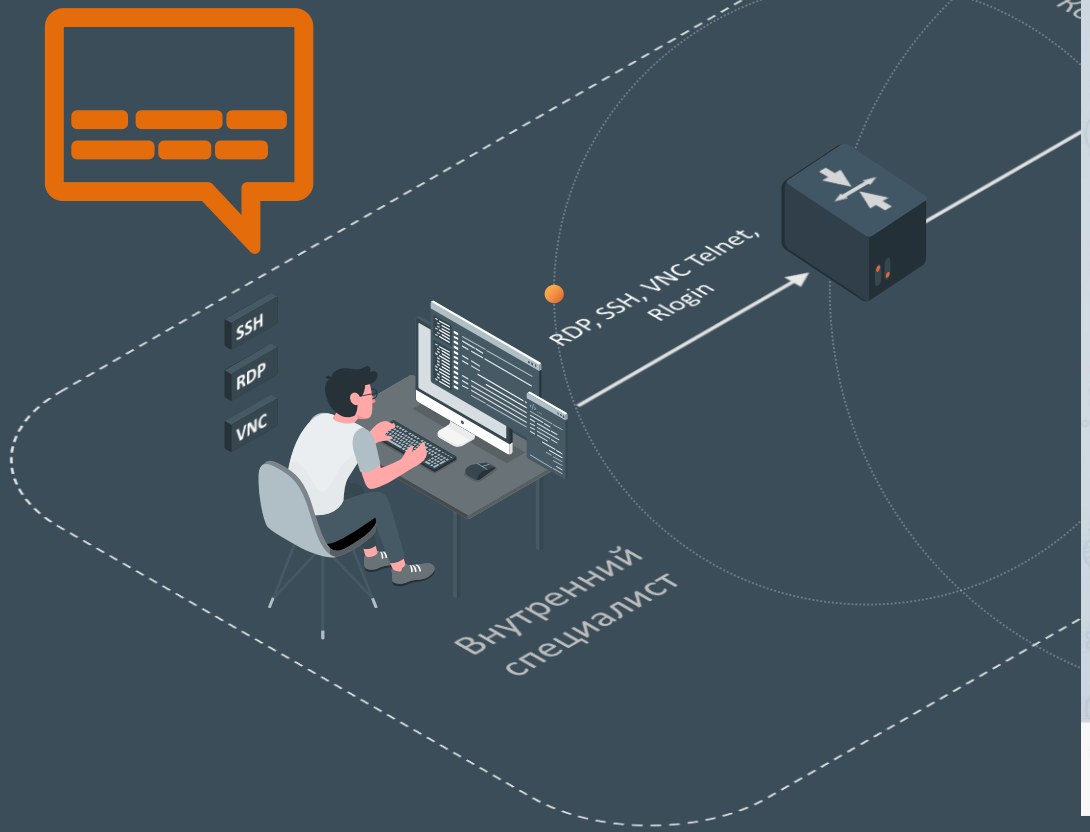


ТРЕНДЫ И ПРОГНОЗЫ ДЕЙСТВИЙ
КИБЕРПРЕСТУПНИКОВ



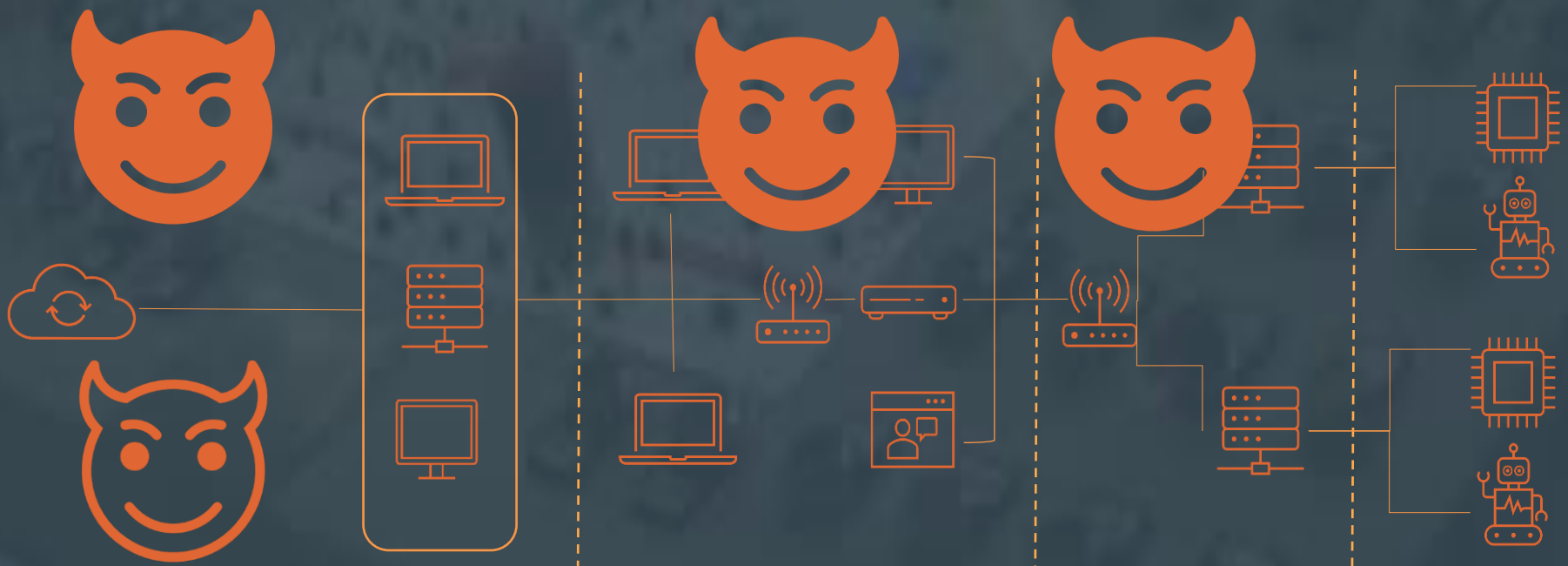
Злоумышленник может находиться в инфраструктуре долгое время, изучая уязвимые точки и планируя атаку с наибольшим ущербом

ТРЕНДЫ И ПРОГНОЗЫ ДЕЙСТВИЙ КИБЕРПРЕСТУПНИКОВ



АЙТИБАСТИОН

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ ЗОНЫ АТАКИ В АСУ ТП



Корпоративная сеть *Верхний уровень* *Средний уровень* *Нижний уровень*

АЙТИБАСТИОН

КАК ОСУЩЕСТВЛЯТЬ КОНТРОЛЬ?

Использовать персонифицированную УЗ для пользователя и обозначать его роль

Разграничивать доступы к устройствам и скрывать УЗ от них

Вести видеозапись сессий, иметь возможность их прерывать и задавать правила разрыва

Анализировать поведение пользователей и реагировать в случае отклонений от типичного

Privileged Access Management (PAM)

Класс решений для ограничения, отслеживания, обнаружения, предотвращения и расследования несанкционированного привилегированного доступа к критически важным ресурсам, что способствует защите инфраструктуры от киберугроз.

БАЗОВЫЕ ФУНКЦИИ
СКДПУ НТ

АЙТИБАСТИОН

ЕДИНАЯ ТОЧКА ДОСТУПА

ЗАПИСЬ СОБЫТИЙ ДОСТУПА

БЕЗ УСТАНОВКИ АГЕНТОВ

ПРОСМОТР И ПРЕРЫВАНИЕ СЕССИЙ

УПРАВЛЕНИЕ ПАРОЛЯМИ

РАБОТА С ПОДТВЕРЖДЕНИЕМ ДОСТУПА

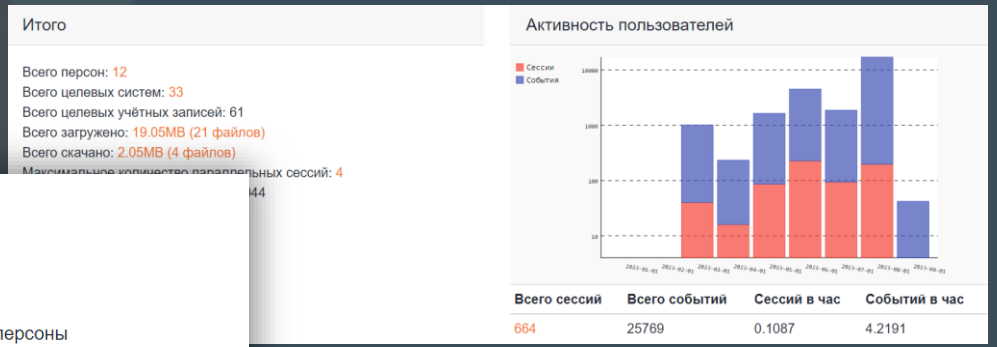
АЙТИБАСТИОН

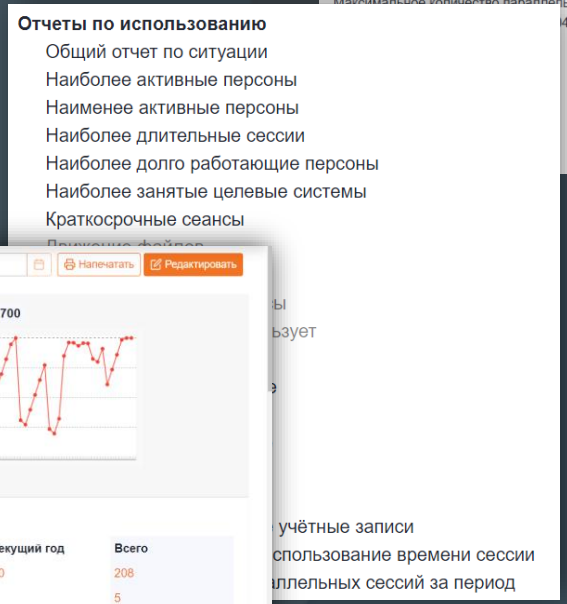
www.it-bastion.com

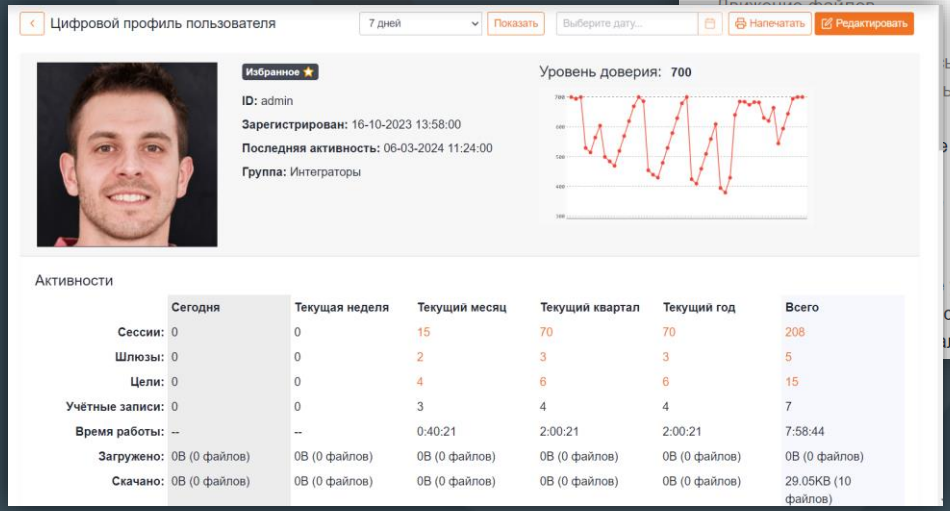
БАЗОВЫЕ ФУНКЦИИ
МОНИТОРИНГА И АНАЛИТИКИ

АЙТИБАСТИОН

www.it-bastion.com



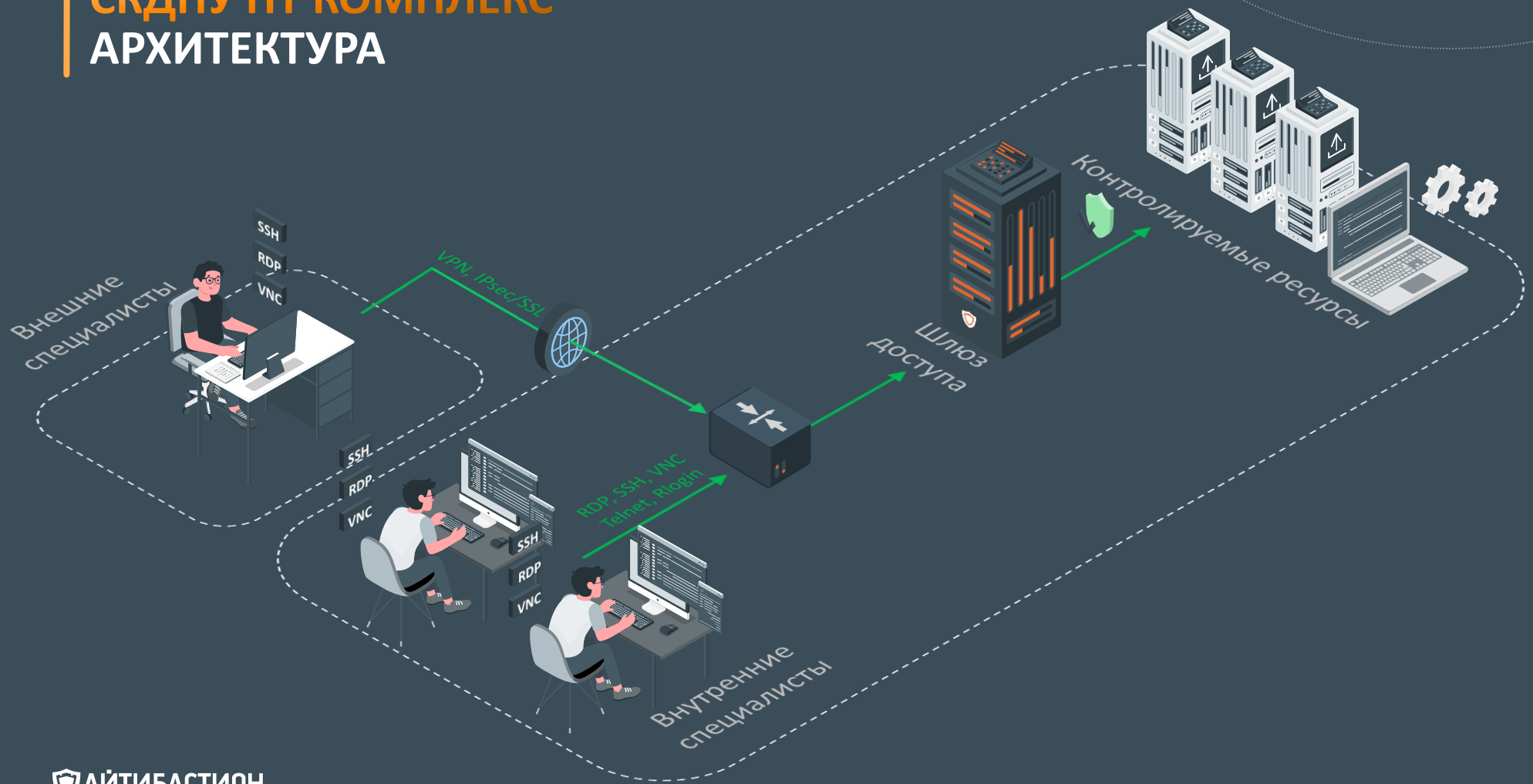




АЙТИБАСТИОН

ВЕРНЁМСЯ К ПРАКТИКЕ

СКДПУ НТ КОМПЛЕКС
АРХИТЕКТУРА



АЙТИБАСТИОН

www.it-bastion.com

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ
ПРИ ПОМОЩИ КОМПЛЕКСА СКДПУ НТ

АЙТИБАСТИОН

ДАНО:

Замедление работы оборудования после диагностических работ, проведенных подрядчиком

ПРЕДПОЛАГАЕМЫЕ ПОСЛЕДСТВИЯ:

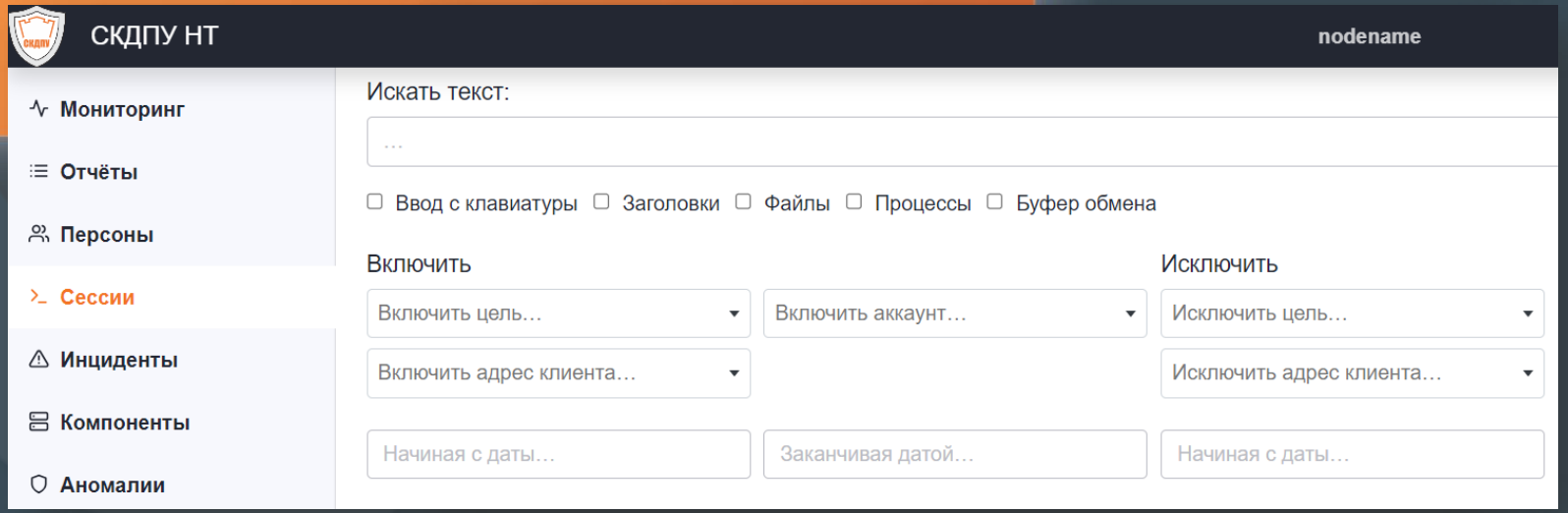
Снижение объёмов производства, а следовательно - дальнейшее уменьшение объёмов сбыта, упущенная выгода, выплаты неустоек

АЙТИБАСТИОН

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ПРИ ПОМОЩИ КОМПЛЕКСА СКДПУ НТ

РЕШЕНИЕ:

1. Идентификация времени изменения скорости оборудования и соотнесение с сессиями в этот период

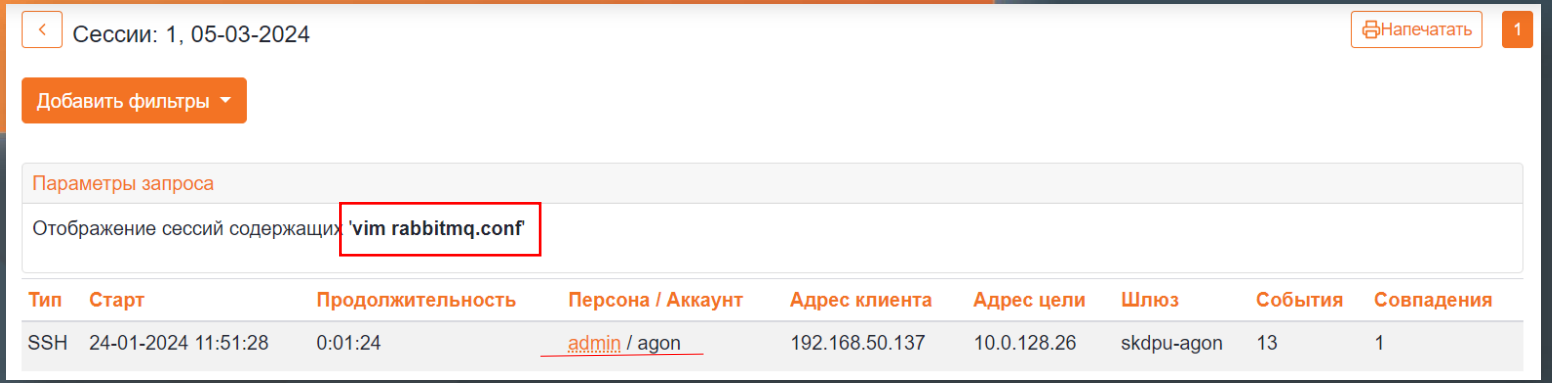


РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ПРИ ПОМОЩИ КОМПЛЕКСА СКДПУ НТ

АЙТИБАСТИОН

РЕШЕНИЕ:

2. Обнаружение интересующего действия поиском и просмотром полной записи и установление причастных



АЙТИБАСТИОН

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ПРИ ПОМОЩИ КОМПЛЕКСА СКДПУ НТ

РЕШЕНИЕ:

3. Устранение инцидента, возврат конфигурационного файла в прежние значения

РЕЗУЛЬТАТ:

Финансовые и репутационные потери предотвращены

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ
ПРИ ПОМОЩИ КОМПЛЕКСА СКДПУ НТ

АЙТИБАСТИОН

ДАНО:

СКДПУ Модуль Мониторинга и аналитики активно сигнализирует нам о нетипичном поведении пользователя

ПРЕДПОЛОЖЕНИЯ:

Пользователь совершает что-то нелигитимное, или его доступы скомпрометированы

АЙТИБАСТИОН

ОПЕРАТИВНОЕ РЕАГИРОВАНИЕ
ПРИ ПОМОЩИ КОМПЛЕКСА СКДПУ НТ

РЕШЕНИЕ:

1. Анализ уровня доверия пользователя

АЙТИБАСТИОН

ОПЕРАТИВНОЕ РЕАГИРОВАНИЕ
ПРИ ПОМОЩИ КОМПЛЕКСА СКДПУ НТ

РЕШЕНИЕ:

2. Анализ инцидентов

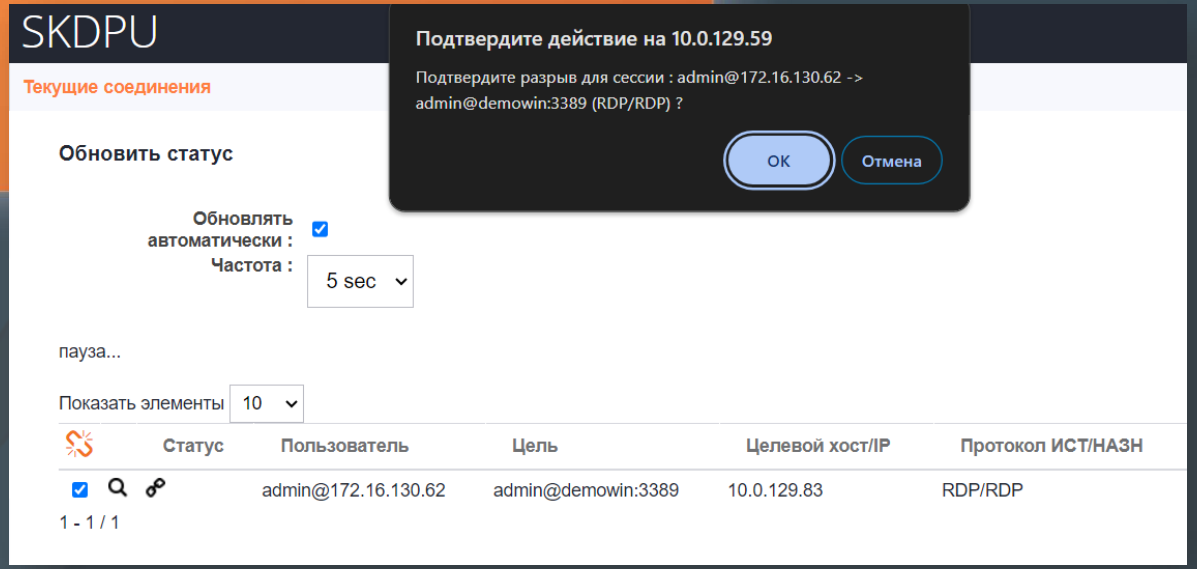
AF-1000232	05-03-2024 07:13:01	admin		Ошибка аутентификации	Низкий	10
TF-1000231	05-03-2024 07:03:20	admin	172.16.137.42	Необычное время работы	Низкий	10
SA-1000230	05-03-2024 07:03:20	admin	172.16.137.42	Сетевое расположение	Низкий	10
TF-1000229	05-03-2024 06:29:55	admin	172.16.130.62	Необычное время работы	Низкий	10

АЙТИБАСТИОН

ОПЕРАТИВНОЕ РЕАГИРОВАНИЕ ПРИ ПОМОЩИ КОМПЛЕКСА СКДПУ НТ

РЕШЕНИЕ:

3. Переход к сессии и разрыв



АЙТИБАСТИОН

ОПЕРАТИВНОЕ РЕАГИРОВАНИЕ
ПРИ ПОМОЩИ КОМПЛЕКСА СКДПУ НТ

РЕЗУЛЬТАТ:

Предотвращен инцидент безопасности, который мог повлечь за собой потери

АЙТИБАСТИОН

КОМПАНИЯ
АЙТИ БАСТИОН

2014

ОСНОВАНИЕ КОМПАНИИ
Более 9 лет на российском рынке информационной безопасности

100+

ПАРТНЕРОВ-ИНТЕГРАТОРОВ
Интеграции с компаниями, позволяющие выполнить квалифицированную помощь в реализации защиты инфраструктуры

180+

ЗАКАЗЧИКОВ И ПРОЕКТОВ
Присутствие во всех отраслях от нефтяных компаний до футбольных клубов, от небольших офисов до георасределенных площадок

>70%

РАМ-РЫНКА РФ
Комплекс СКДПУ НТ
решение, проверенное «в боях» и доказавшее свою эффективность, надежность и качество

АЙТИБАСТИОН

ВНЕДРЕНИЕ В ИНФРАСТРУКТУРУ
МУЛЬТИВЕНДОРНОСТЬ

Обширные возможности технологических интеграций с различными классами решений рынка ИБ

ТЕХНОЛОГИЧЕСКИЕ ПАРТНЁРСТВА

ASTRA LINUX®
POSITIVE TECHNOLOGIES
kaspersky
INFOWATCH®
Пассворк
DATALINE
GIS ГАЗИНФОРМ СЕРВИС
ROSA
CyberLympha®
РУТОКЕН
Аладдин
zVIRT
alt linux
с•терра®
MULTIFACTOR
UserGate
Rusiem
КОД безопасности
РЕДОС

и другие партнеры

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

АЙТИБАСТИОН

Соответствие требованиям

Сертификаты и реестр

Целевые и клиентские ОС

Варианты поставки

Техническая поддержка

Базовая ОС

АЙТИБАСТИОН

И ЧТО В СУММЕ?

Контроль за исполнением условий SLA подрядчиками

Контроль доступа к информационной инфраструктуре в реальном времени

Ведение отчётности: быстрый доступ к аналитике, отчётам и потенциальным инцидентам

Создание доказательной базы для ретроспективного аудита и анализа сбоев или инцидентов ИБ

Контроль соблюдения **корпоративной политики ИБ**

Соблюдение **требований регуляторов**

Контроль действий подрядчиков, потенциально влекущих за собой утечку информации и различные атаки

Защита собственных специалистов от неправомерных претензий в случае инцидентов ИБ или аварий

Спасибо за внимание!

АЙТИБАСТИОН

Гончарова Александра
инженер поддержки продаж

a.goncharova@it-bastion.com

+7 499 495 45 40

it-bastion.com