



Информационная безопасность как сервис

Сервисная модель обеспечения ИБ

Москва, Варшавское ш., д.1 стр.6, БЦ «W-Plaza 2»

Преимущества ИБ-аутсорсинга

- ✓ Переведите затраты из CAPEX в OPEX и максимизируйте эффективность.
- ✓ Снизьте капитальные затраты, благодаря быстрому развертыванию сервисов ИБ.
- ✓ Оптимизируйте ресурсы ИБ-команды для более стратегических задач.
- ✓ Гибкое масштабирование.

ФИНАНСОВАЯ ЭФФЕКТИВНОСТЬ

Многолетний опыт

ВЫСОКИЙ УРОВЕНЬ КАЧЕСТВА УСЛУГ

- ✓ Наличие и соблюдение SLA.
- ✓ Доступность и компетентность команды аутсорсинга.
- ✓ Обеспечение НЕОБХОДИМОГО уровня информационной безопасности.
- ✓ Поддержка соответствия и соблюдение требований регуляторов



Основные аспекты перехода

Сложности владения:



Лицензии

Приобретение/обновление



Техника

Доставка/обслуживание



Люди

Найм/удержание



Сервисная модель предоставления услуг ИБ позволяет перевести CAPEX в OPEX.

Сервисные возможности:



Динамика

Любая производительность



Масштаб

Распределенные площадки



Экспертиза

Индустриальная специфика



Сервисы информационной безопасности



Virtual CISO

- Управление **внутренними** уязвимостями
- Управление **внешними** уязвимостями и контроль периметра
- Анализ защищенности WEB-приложений
- ASV-сканирование по требованиям PCI DSS
- Аудит паролей в среде AD



Опыт

Обучение и тестирование сотрудников

- Управление обновлениями
- SIEM as a Service
- Контроль целостности FIM
- Контейнер Security
- Product security



«Virtual CISO»



Поддержание процедуры повышения осведомленности сотрудников в вопросах ИБ



Анализ и актуализация нормативной документации по обеспечению ИБ



Контроль выполнения периодических проверок обеспечения ИБ



Контроль взаимодействия с регуляторами



Контроль внесения изменений в сетевую инфраструктуру



Консультирование по вопросам построения и поддержания защищенной среды



Обучение и тестирование сотрудников по вопросам ИБ

Фишинг – это совокупность методов, позволяющих обмануть пользователя и заставить его раскрыть свой пароль, номер кредитной карты и другую конфиденциальную информацию.

Назначение



Сервис «Обучения и тестирования навыков сотрудников по вопросам ИБ» позволяет обучить сотрудников и контролировать их навыки по информационной безопасности. Сервис – это платформа для обучения, тестирования и контроля готовности сотрудников компании противостоять фишингу. Имитируя фишинговые атаки, сервис выявляет сотрудников с недостаточным уровнем знаний и предоставляет необходимые электронные курсы и тесты для тренировки навыков по информационной безопасности.

Управление внутренними уязвимостями

Обнаружение уязвимостей во внутренней инфраструктуре сети

Назначение



Сервис обеспечивает высокий уровень контроля за уязвимостями внутри компании, оптимизируя ресурсы сотрудников служб ИТ и ИБ.



Своевременное выявление и устранение уязвимостей позволяет избежать многочисленных проблем, связанных с внутренними атаками.

Важно

14,8%

увеличение количества атак по сравнению с 2021 годом*



Запуск сервиса по “Управлению внутренними уязвимостями” поможет быстро оценить и устранить технические угрозы во внутренних сетях, без дополнительного приобретения и обслуживания оборудования, без увеличения бюджета на ресурсы службы информационной безопасности.



Rakasta

Управление внутренними уязвимостями



Отчет с
рекомендациями

Управление внешними уязвимостями и контроль периметра

Обнаружение уязвимостей на внешних ресурсах

Назначение



Сервис обеспечивает высокий уровень контроля за уязвимостями на периметре сети, оптимизируя ресурсы сотрудников служб ИТ и ИБ.

Особенность



Расширенные возможности сервиса обеспечит специальная методика по оценки уровня защищенности

- Rakasta Secure Border (RSB).

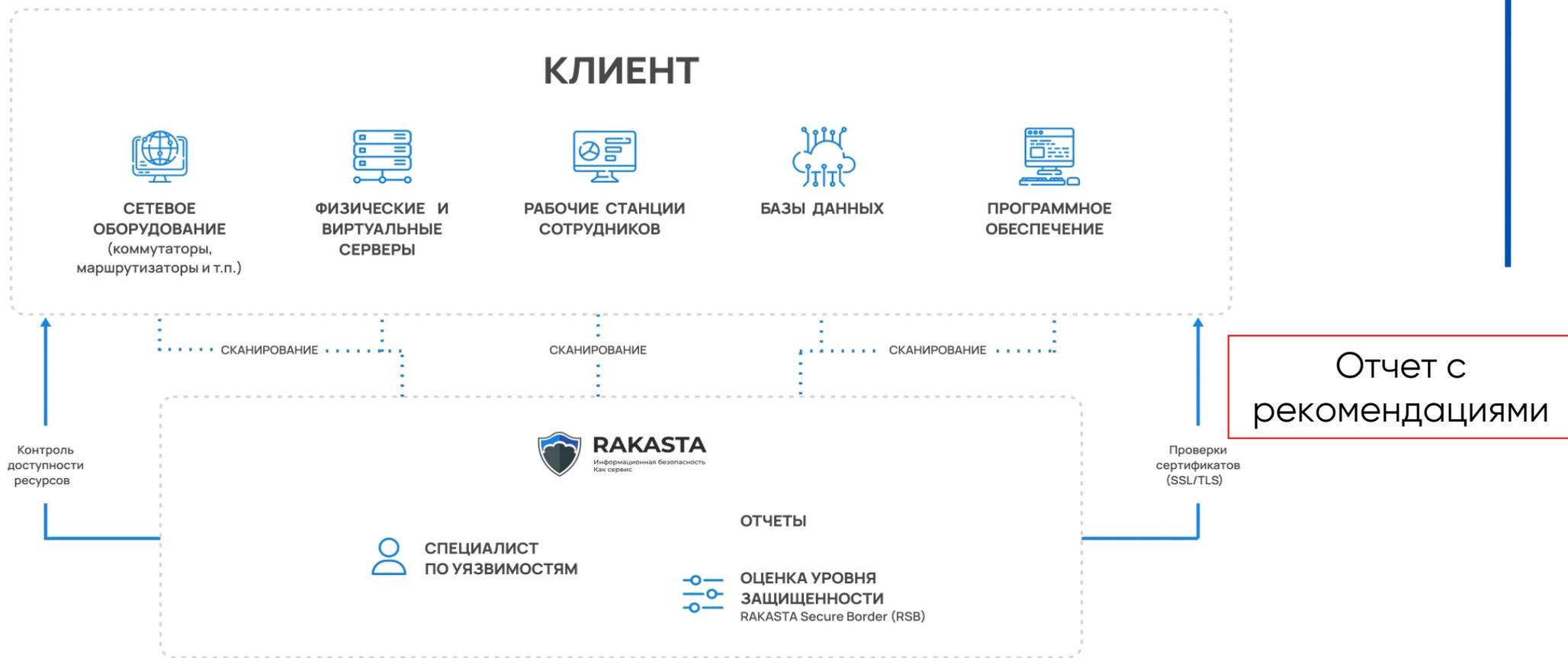


Важно

76%

компаний был преодолен внешний периметр*

Управление внешними уязвимостями и контроль периметра



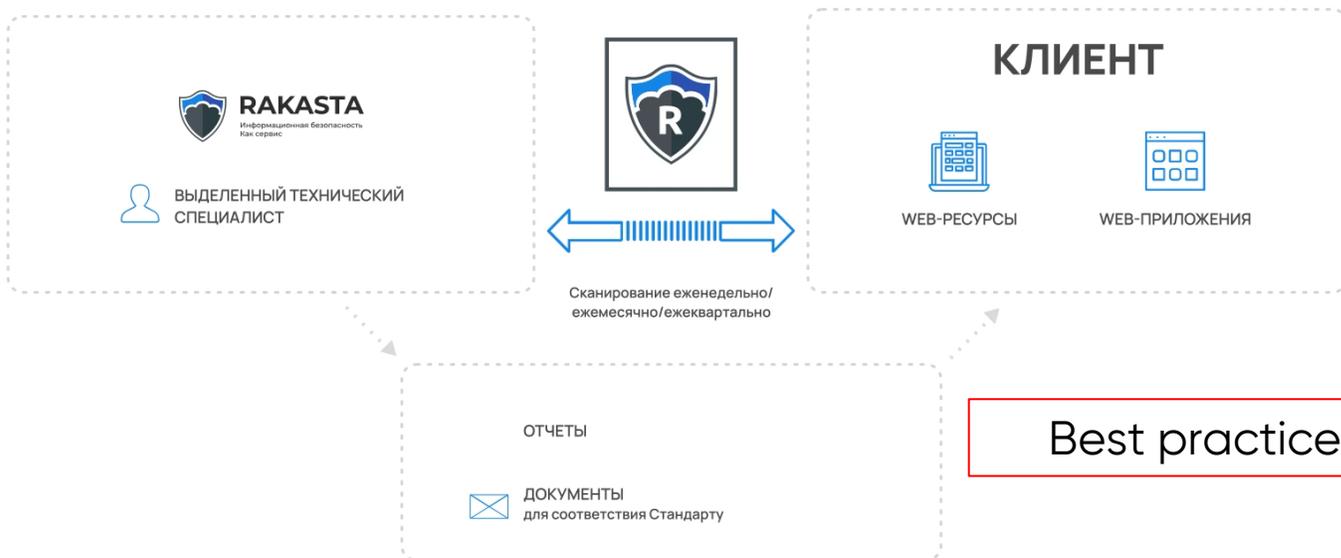
Регулярный тест Безопасность WEB

Обнаружение уязвимостей и определение уровня безопасности web-приложений

Назначение



Сервис обеспечивает контроль защищенности внешних и внутренних web-ресурсов..



Важно

53% имеют низкий уровень защищенности web-приложений*

- Это позволяет киберпреступникам получать доступ к конфиденциальным данным организаций и пользователей.
- Для оперативного выявления уязвимостей, характерных для web-приложений, необходимы специальные технические решения. Работу по настройке, мы рекомендуем, доверить команде профессионалов для дальнейшей интерпретации результатов сканирования, анализа выявленных угроз, с рекомендациями по их устранению.
- Завершающим этапом станет итоговая отчетность, которая обеспечит полную картину защищенности Ваших web-ресурсов.

ASV-сканирование по требованиям PCI DSS

Регулярное внешнее сканирование для поддержания соответствия требованиям стандарта PCI DSS

Назначение

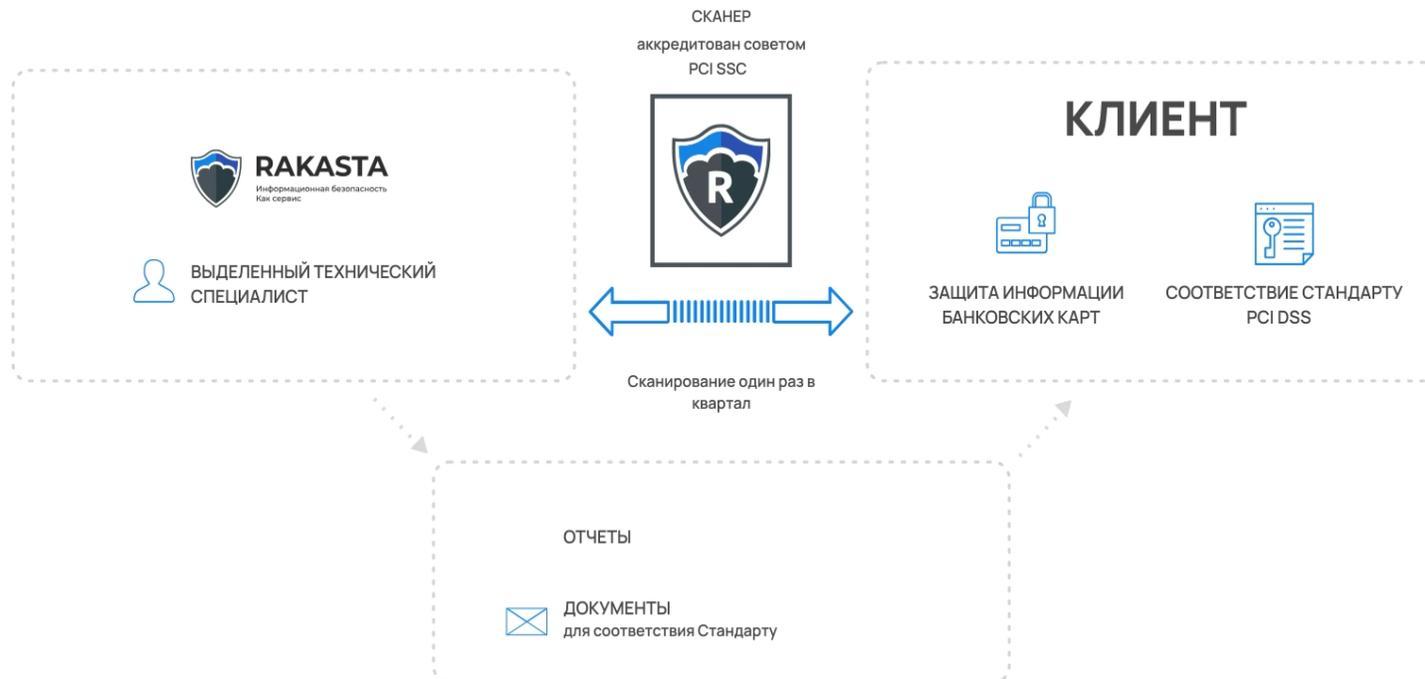
Сервис помогает не пропускать ежеквартальные сканирования.

Вы также будете получать подробную информацию по обнаруженным уязвимостям и методам их устранения.

Важно

- ✓ Соблюдать контроль за сроками сканирования
- ✓ Использовать только аккредитованные ASV-сканеры
- ✓ Согласовывать все «false positive»

>100 клиентов уже пользуются нашим сервисом.



Аудит паролей AD

Комплексный аудит паролей внутри компании

Назначение



Сервис обеспечивает выявление уязвимых паролей, а также потенциально опасные конфигурации в Active Directory с точки зрения аудита паролей.

Важно

Сервис позволяет **выявить пароли**, которые возможно подобрать с помощью атаки по словарю, так как проверка проходит по базе паролей, состоящей из более чем **613 миллионов паролей**, которые когда-либо утекали в глобальную сеть Интернет. База постоянно обновляется.



Непрерывный сетевой аудит

Назначение



Сервис предоставляет комплексный аудит межсетевых экранов, обеспечивающий полную проверку на валидность и безопасность сети.

Рекомендации в
отчете

Важно

Неправильно настроенный NGFW может стать причиной проблем с:

- Несанкционированным доступом в сеть организации;
- Скачиванием вредоносных файлов;
- Доступом к вредоносным сайтам и нежелательным приложениям;
- Отсутствием защиты от вторжений и атак на активы организации.

Непрерывный сетевой аудит



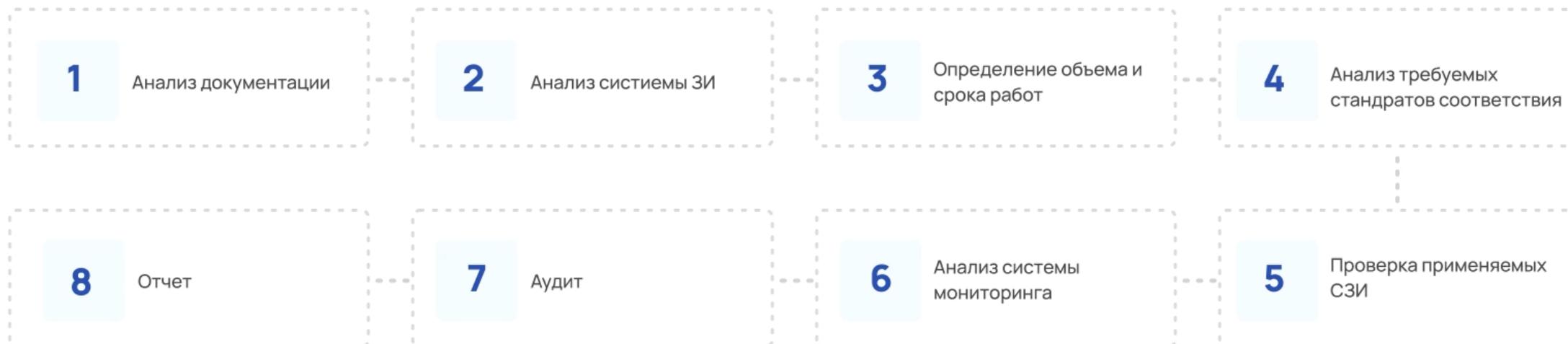
Непрерывный аудит настроек СЗИ

Назначение

Рекомендации в отчете

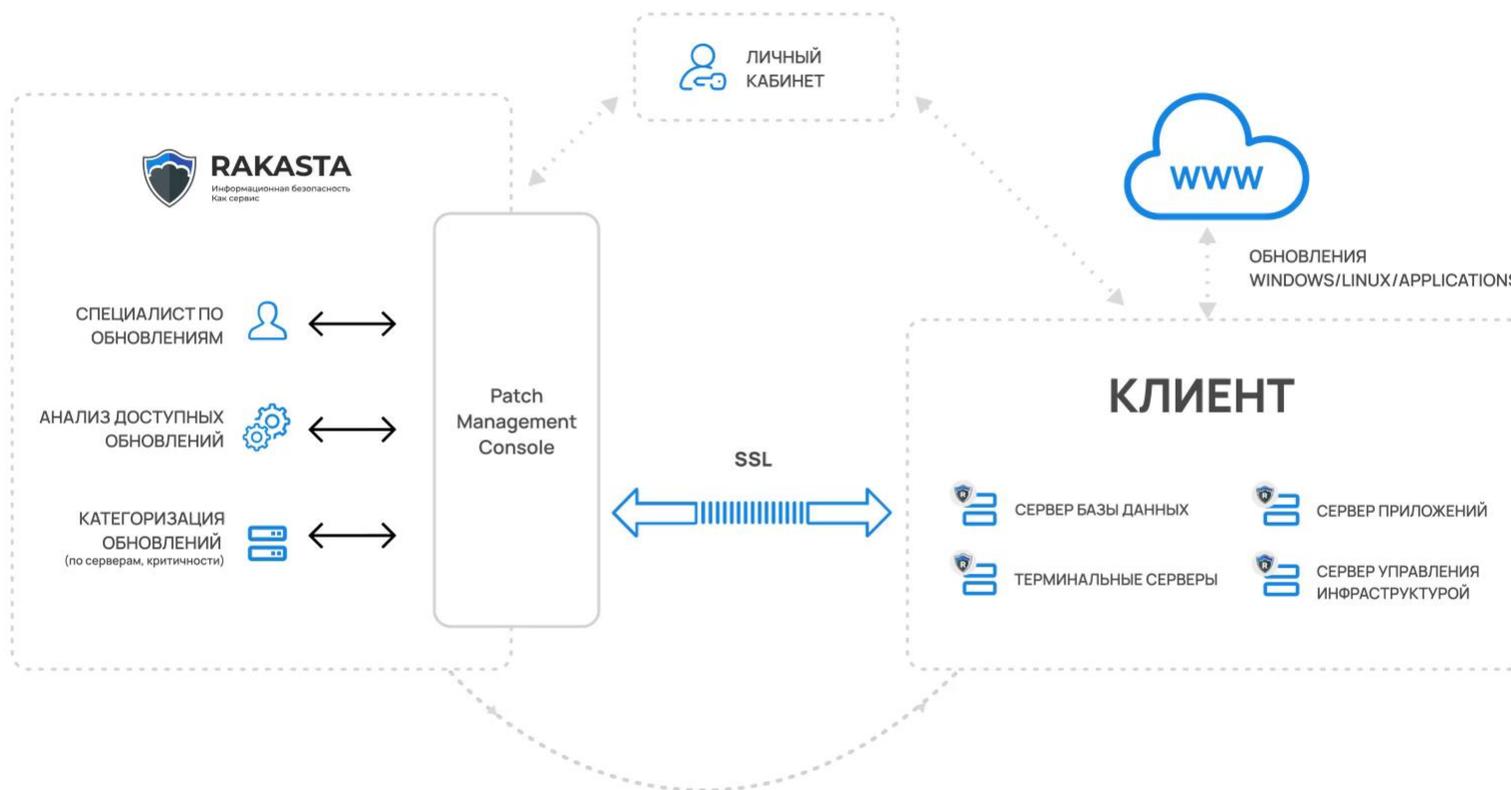


Сервис предоставляет комплекс услуг в одном пакете по проверке степени защищенности вашего бизнеса. Вся инфраструктура кроме сетевого оборудования пройдет проверку по определенным критериям и показателям безопасности в целях максимально обезопасить вашу внутреннюю систему.



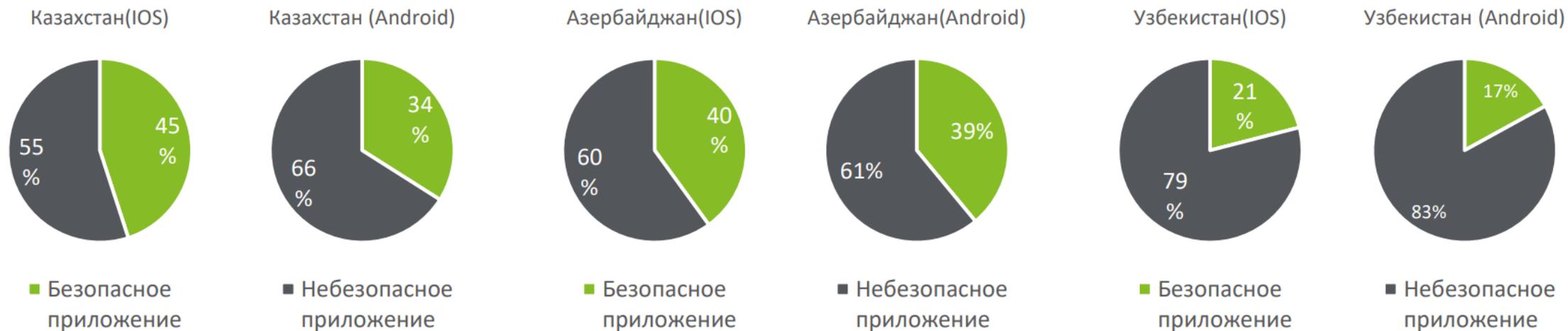
Сервис управления обновлениями

Сервис управления обновлениями позволяет снизить риски потери работоспособности информационных систем за счет непрерывного управления актуальными версиями программного обеспечения.



Актуальная статистика

Обобщенный результат безопасности мобильного банкинга по странам:



Непрерывный Анализ кода

Автоматизированный и ручной анализ кода приложений

Назначение



Сервис поможет существенно снизить количество ошибок в коде, которые могут привести к уязвимостям вашего ПО.

С учетом
индустриальной
специфики

Важно

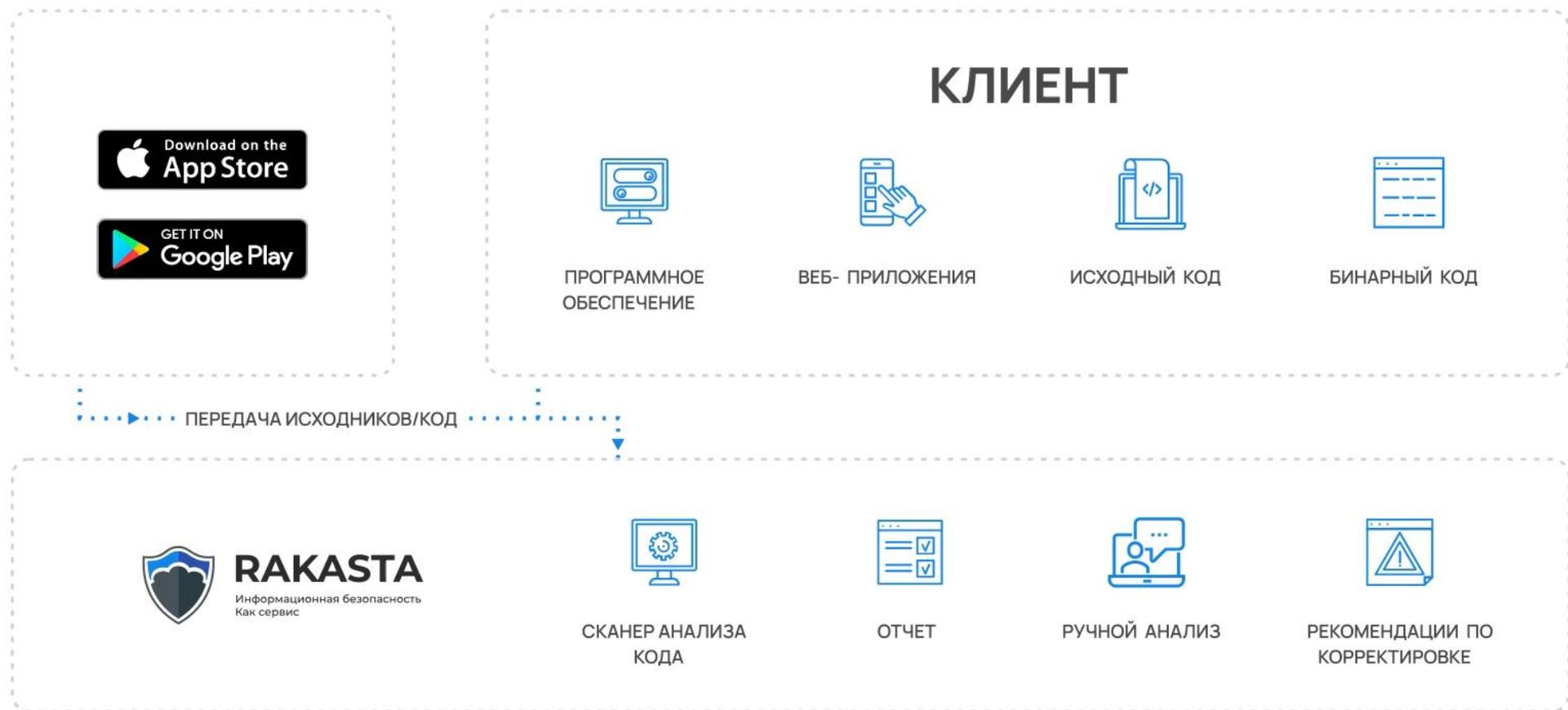
ЗАЩИТИТЕ СВОЙ БИЗНЕС И КОНТРОЛИРУЙТЕ КАЧЕСТВО РАЗРАБОТКИ.

Анализ исходного кода позволяет злоумышленникам выявить слабые места в приложениях и спланировать дальнейшее развитие атак.

Будьте на шаг впереди!

Кроме того, в исходном коде приложения может содержаться чувствительная информация для доступа к критически важным ресурсам.

Непрерывный Анализ кода



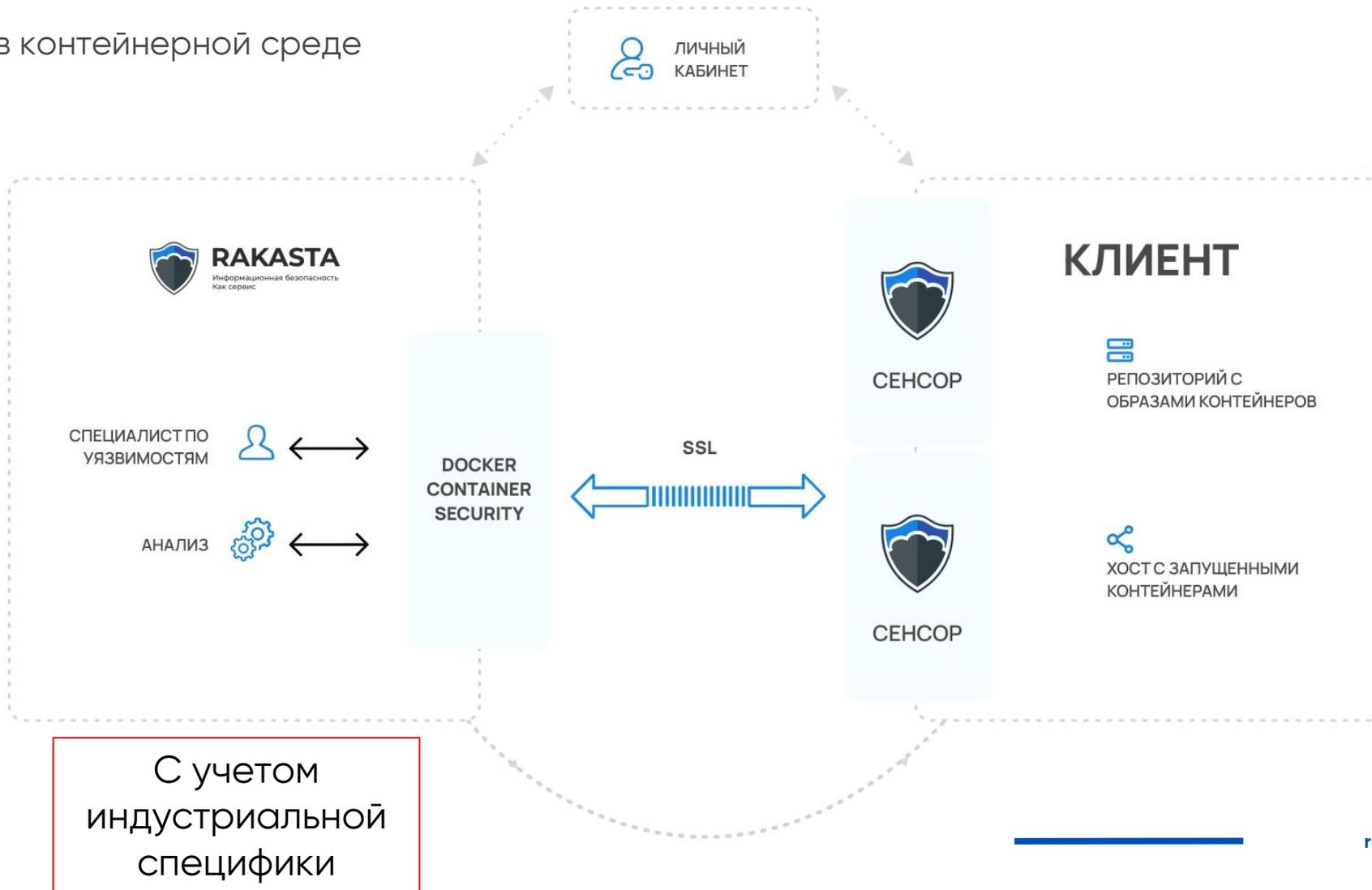
Процесс «Контейнер Security»

Контроль за уязвимостями в контейнерной среде

Назначение



Сервис позволит отслеживать, обнаруживать и блокировать поведение контейнера на основе политик во время выполнения.



Непрерывное Управление обновлениями

Назначение



Автоматизация процесса доставки обновлений на инфраструктуру компании, позволяет снизить риски остановки бизнес-процесса. В рамках данного сервиса производится управляемая доставка контента обновлений до выбранного набора сервисов.

Важно

57% жертв кибератак сообщают, что это можно было предотвратить, установив доступный патч,

а также **34%** этих жертв знали об уязвимости, но не предприняли никаких действий



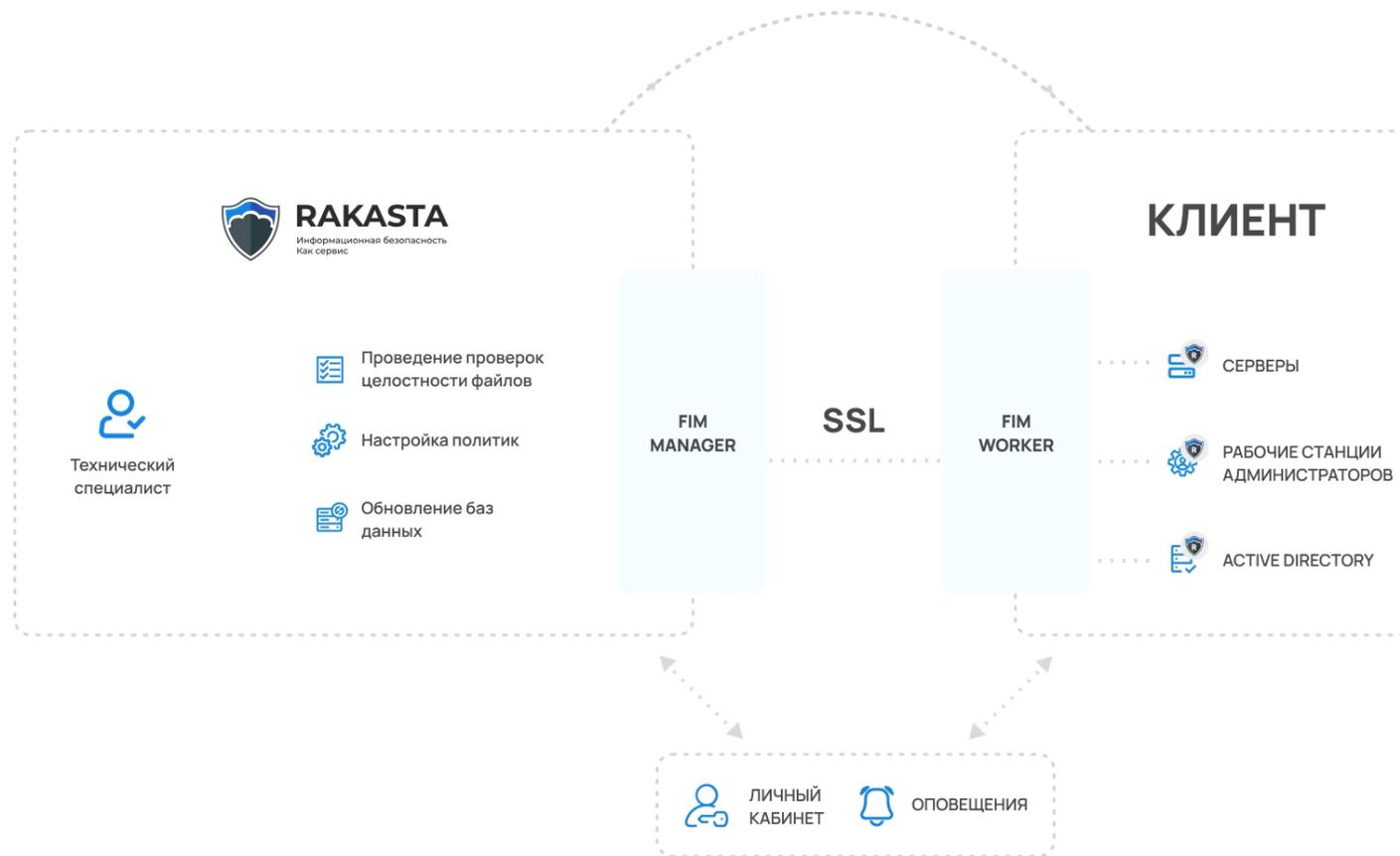
Сервис Контроль целостности FIM

FIM (File Integrity Monitoring) – это средства по контролю целостности программных сред предназначены для обнаружения и защиты от несанкционированного изменения критически важных компонентов.

Назначение



Сервис в режиме реального времени осуществляет непрерывный мониторинг состояния конфигурации, включая проверку целостности файлов и защиту системы от изменений.



SIEM as a Service

Централизованный сбор и управление событиями безопасности

Назначение



Сервис обеспечивает автоматизированный процесс сбора, анализа, корреляции данных для управления событиями ИБ, с целью выявления и предупреждения инцидентов в режиме 8x5.



Возможность использовать полноценную SIEM-систему без сложного внедрения и развертывания внутри компании.

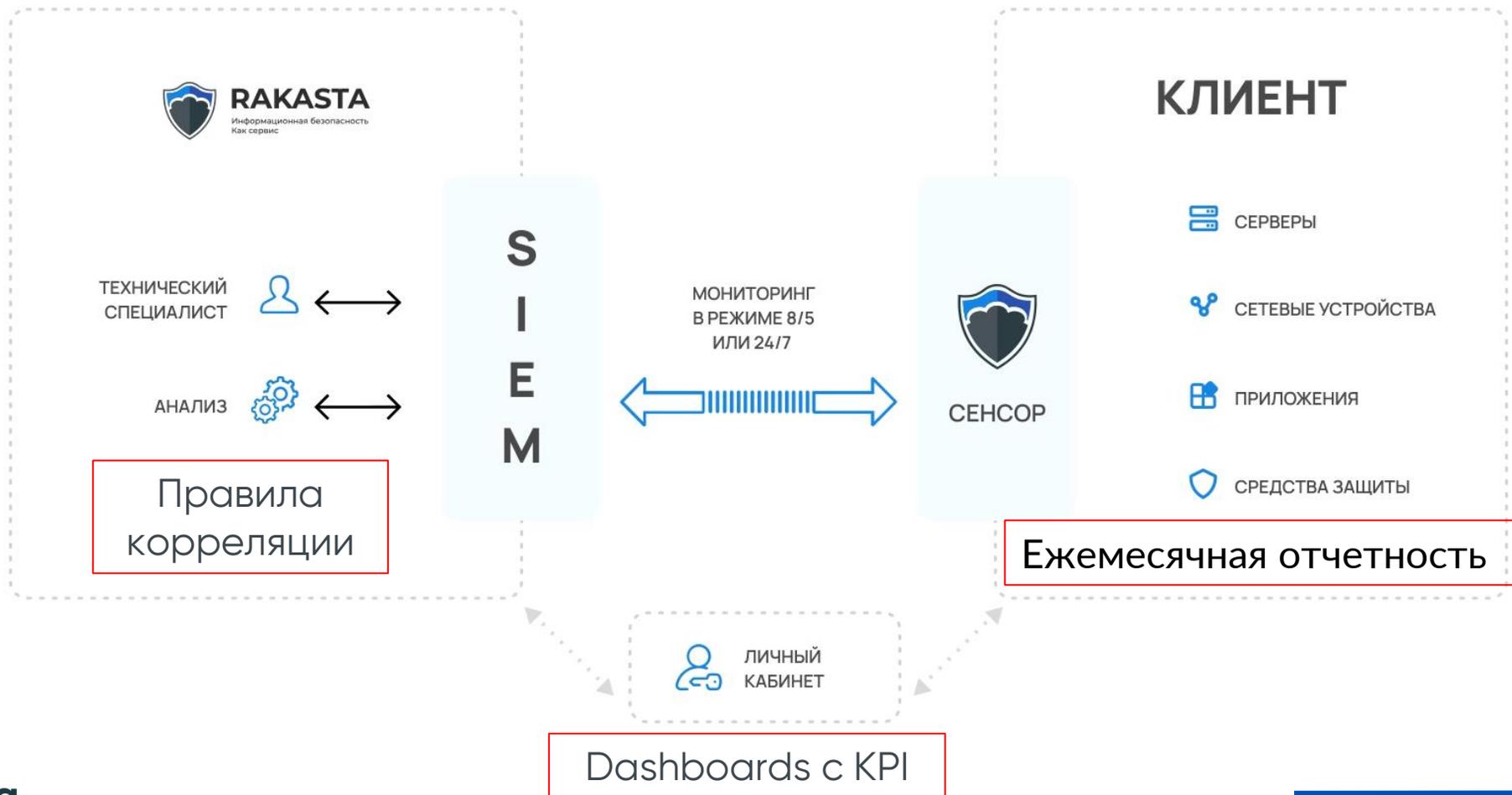
Важно

- Идеальное решение для оптимизации затрат и ресурсов.
- Построение собственной системы сбора и анализа событий требует больших затрат, включая поиск квалифицированных сотрудников.
- Использование сервиса позволит избежать данных трудностей.



SIEM as a Service

Для работы системы необходимо устанавливать специальный сенсор внутри инфраструктуры Заказчика.



Преимущества сервисов

- ✓ **Не требуется увеличения** капитальных затрат (только OPEX)
- ✓ **Эффективное использование** уже имеющихся возможностей по обеспечению информационной безопасности
- ✓ **Профессиональное взаимодействие** с партнерами и подрядчиками по вопросам обеспечения информационной безопасности
- ✓ Применение **многолетнего опыта** здесь и сейчас.

Преимущества клиента

- ✓ **Качественные сервисы ИБ**, которые будут запущены всего за несколько недель
- ✓ Дополнительные **бесплатные мини-сервисы и внутренние мероприятия**, направленные на повышение уровня обеспечения ИБ
- ✓ **Полные отчеты** о работе всех систем защиты, которые будут предоставляться еженедельно и ежемесячно
- ✓ Существенная **экономия бюджета** на технические средства ИБ и команду в штат.

Как перейти на сервисную модель ИБ



- Общее состояние СОИБ
- Процессы ИБ
- Классификация процессов по степени критичности
- Финансовая выгода
- Перечень списка задач на передачу аутсорсинга



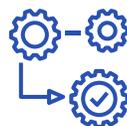
- План работ
- Регламент взаимодействия
- Настройка и запуск
- Корректировка

АНАЛИЗ

ВЫБОР ИСПОЛНИТЕЛЯ

СТАРТ РАБОТ

КОНТРОЛЬ



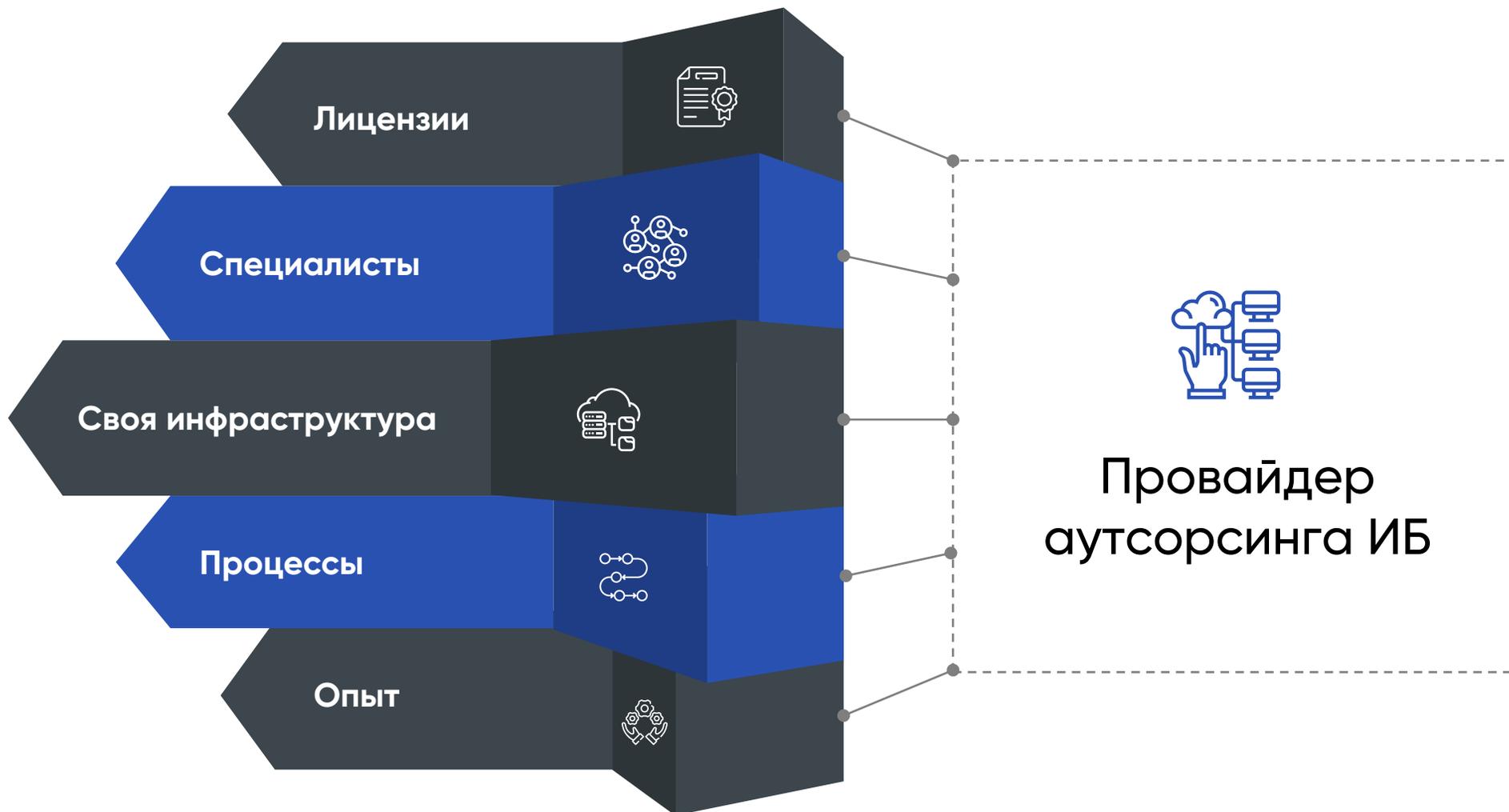
- Подготовка ТЗ
- Формирование SLA
- Запрос предложений
- Анализ предложений
- Изучение референсов!
- Пилотное тестирование
- Подписание договора



- Соблюдение регламента
- Оценка качества сервиса
- Оценка рисков
- Возможная корректировка



Требование к сервис-провайдеру услуг ИБ



Сервисная модель обеспечения ИБ

0 КОМПАНИИ



3 КОМАНДЫ

10+ лет опыта

40+ экспертов



Rakasta

10+
стран

100+
клиентов уже
используют наши
сервисы



Доверьте нам решение
вопросов
информационной
безопасности вашего
бизнеса



И сконцентрируйтесь на его
развитии!



Спасибо!

Прокудин Аркадий
Коммерческий директор
a.prokudin@rakasta.ru
+7(903) 224-59-50

**Информационная
безопасность как сервис**

 **+7 (495) 968 57 66**

 www.rakasta.ru