



**CROSSTECH**  
SOLUTIONS GROUP

Презентация решений  
компании

# Crosstech Solutions Group

Российский разработчик решений для мониторинга, контроля и комплексной защиты от внутренних угроз с учетом специфики каждой отдельной организации.

Продукты входят в реестр российского ПО и рекомендованы для импортозамещения на предприятиях России.

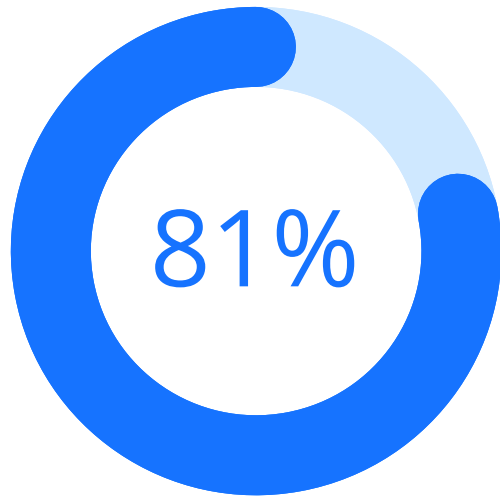


**6**  
решений

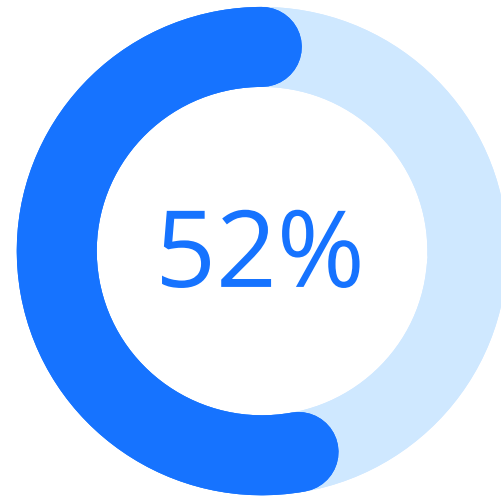
**>50**  
актуальных  
партнеров

**5**  
лет на  
IT-рынке

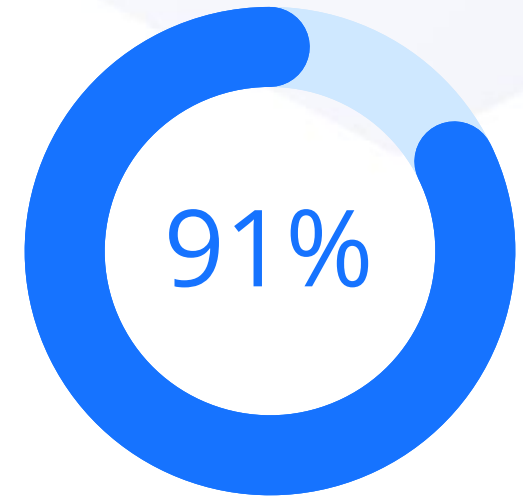
# Внутренние угрозы



Утечек в российских компаниях, совершаемых во внутреннем контуре, являются умышленными



Инцидентов происходили по причине «злоупотребления привилегиями» и нарушения прав доступа



Составляет доля утечек персональных данных

# Важность защиты

---

Для ИТ/ИБ директоров

Обеспечение стабильной работы ИТ-инфраструктуры с минимизацией рисков возможной компрометации информации при работе с документами и конфиденциальной информацией

---

Для офицеров ИБ

Сбалансированная защита конфиденциальности, целостности и доступности данных. Ускорение процесса обнаружения утечки, установления злоумышленника и реагирования на инцидент

---

Для сотрудников

Повышение ответственности при работе с конфиденциальной информацией, понимание политик информационной безопасности компании

## Docs Security Suite (DSS)

платформа маркирования, уникализации и шифрования электронных документов, позволяющая разграничить доступ пользователей к конфиденциальной информации и настроить политики действий с документами

## Jay Data

платформа, осуществляющая поиск, классификацию, статическое и динамическое маскирование конфиденциальной информации в БД

## DataNova Object Recognition (OR)

решение, реализованное на основе глубоких нейронных сетей в алгоритмах компьютерного зрения, позволяющее с помощью перехвата видеопотока с веб-камеры осуществлять мониторинг за деятельностью сотрудников, выявлять нелегитимную активность согласно настроенным политикам безопасности

## DataGrain RUMA

решение, предназначенное для мониторинга поведения пользователей, нацеленное на обнаружение и реагирование аномальной и нелегитимной деятельности сотрудников компании

## DataGrain ESO

решение, предназначенное для сбора, профилирования, сжатия и хранения событий ИБ, с возможностью разграничения прав доступа и осуществления статистического анализа собираемых данных

## CrossTech Smart Assets (CTSA)

комплексный продукт, ориентированный на физический учёт, финансовый контроль и управление контрактными обязательствами ИТ-активов организации в течение всего жизненного цикла

# Docs Security Suite (DSS)

российская платформа маркирования, уникализации и шифрования электронных документов, позволяющая разграничить доступ пользователей к конфиденциальной информации и настроить политики разрешенных действий с документами

Снижение ложных срабатываний DLP-системы более чем на 80%

DSS включен в единый реестр российского ПО МИНКОМ связи №4427 от 16.04.2018

Соответствие требованиям Регуляторов: 152-ФЗ, 161-ФЗ, ФСТЭК №17, ГОСТ Р 57580.4-2022

# Модули Docs Security Suite

## Маркирование

Добавление как скрытых, так и видимых меток конфиденциальности в документе

## Логирование

Фиксация всех действий пользователя при работе с документами, даты, времени, атрибутов пользователя и рабочей станции

## Разграничение доступа

Получение информации о правах пользователя. Ограничение доступа к документу, если у пользователя нет прав на основе меток конфиденциальности

## Шифрование

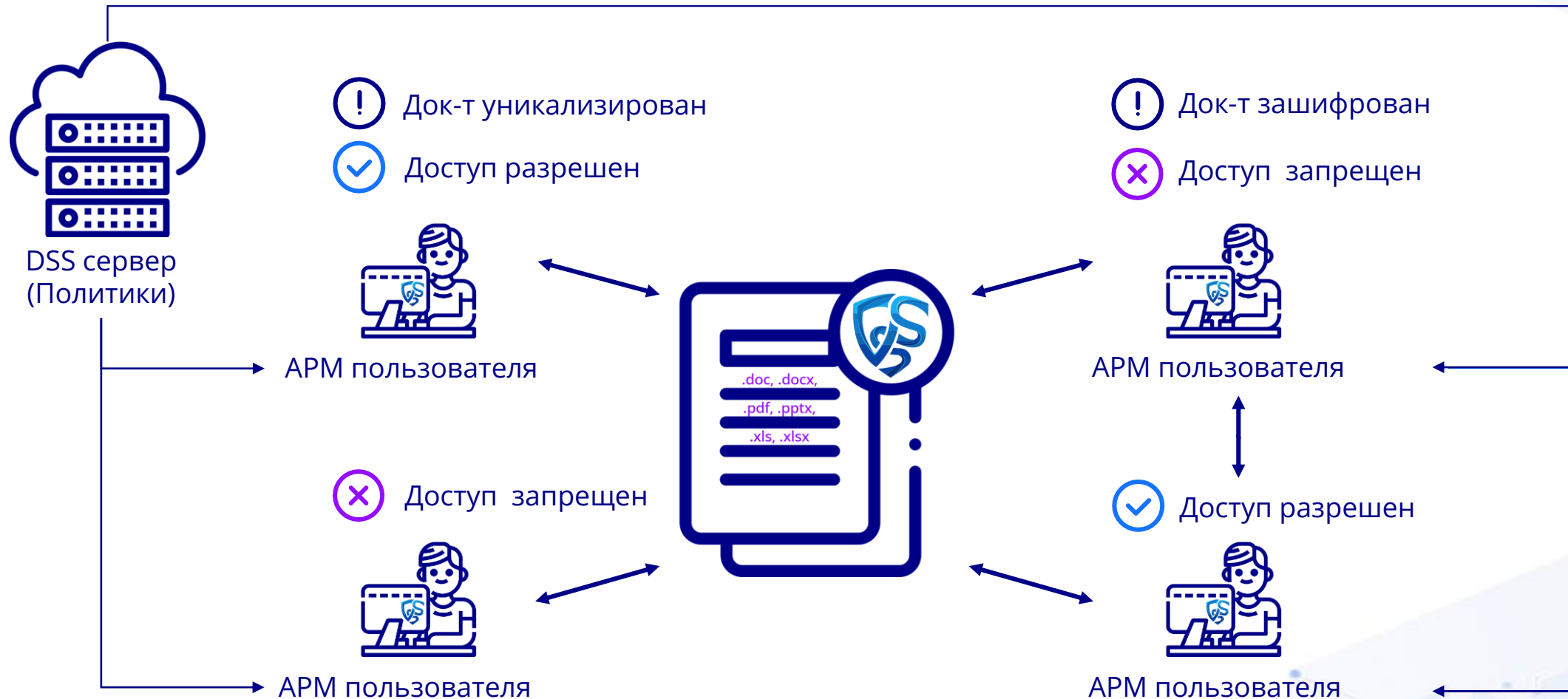
Использование алгоритмов AES или ГОСТ (КриптоПро CSP) для защиты от несанкционированного доступа и открытия случайным получателем вне контура безопасности

## Уникализация

- Уникализация документа на основе технологии стеганографии и аффинных преобразований
- Идентификация принадлежности уникализированного документа по сотруднику

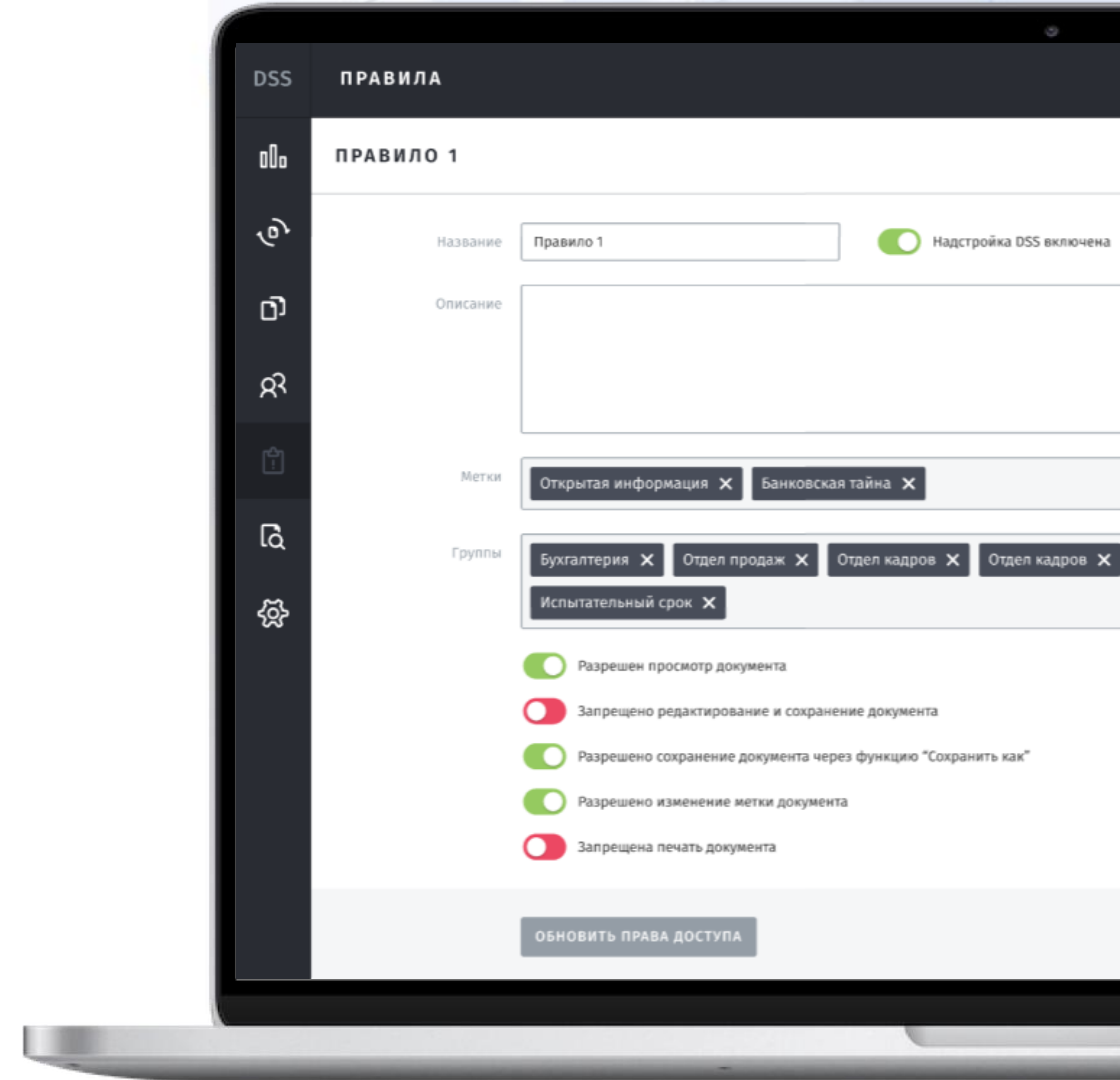


# Схема работы Docs Security Suite

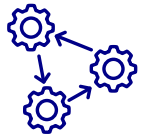


# Задачи, решаемые DSS

- **Разграничение доступа**  
сотрудников к документам по меткам конфиденциальности
- **Уникализация**  
документов с возможностью дальнейшего расследования утечек
- **Шифрование**  
критически важных документов компании
- **Фиксация**  
фактов нарушения политик безопасности и оповещение ответственных
- **Логирование**  
действий сотрудников при работе с документами
- **Осознанный подход**  
к обеспечению безопасности информации со стороны сотрудников при работе с документами



# Результат внедрения DSS



Выявление нарушителя, сфотографировавшего экран/распечатавшего документ, копия которого утекла, за счет скрытых стегано меток



Централизованная и непрерывная регистрация всех доступов и попыток доступа к документам организации



Гарантированное уничтожение документа, всех его копий и черновиков



Доступ к документу и всем его копиям может быть централизованно изъят вне зависимости от того где они и у кого

# Кейс. Случайная утечка информации



## Описание ситуации

При отправке конфиденциального документа по электронной почте в адресной строке пользователь случайно указывает однофамильца получателя или иного адресата, находящегося вне контура ИБ

## При отсутствии DSS

При отсутствии в организации систем класса DLP, письмо будет доставлено и содержимое документа будет скомпрометировано сторонним лицом. В случае их наличия, отправка письма зависит от контентного анализа и принятия решения со стороны администратора DLP, что тормозит бизнес-процессы

## При использовании DSS

DSS позволяет разграничивать права на работу с документами и электронными письмами. В настройках работы с определенными метками конфиденциальности можно запретить отправку писем с определенными метками за контур организации.

# Кейс.

## Утечка фото с содержимым документа



### Описание ситуации

У сотрудника организации имеется доступ к конфиденциальному документу. Пользователь фотографирует содержимое документа и выносит его за контур ИБ

### При отсутствии DSS

В случае, когда у пользователя стоит система решения класса DAG/DCAP, – отследить утечку конфиденциальной информации невозможно.

Заявленная функциональность систем класса DLP зачастую не позволяет выявить нарушителя

### При использовании DSS

С помощью уникализации экрана по технологии стеганографии сотрудник службы безопасности за короткий срок может провести расследование и точно определить пользователя, допустившего утечку и его последнюю активность с документом

# Кейс. Перемещение документа за контур ИБ



## Описание ситуации

Злоумышленник обманом вынудил сотрудника организации вынести и передать документ за пределы защищаемого контура

## При отсутствии DSS

В случае использования систем класса DLP или DAG/DCAP можно зафиксировать место утечки документа. При этом содержимое документа все равно будет доступно злоумышленнику

## При использовании DSS

DSS позволяет зашифровать документ при помощи AES-шифрования или алгоритма ГОСТ (КриптоПро CSP), таким образом злоумышленник не сможет получить доступ к конфиденциальной информации

# Кейс. Похищение содержимого документа



## Описание ситуации

Преследуя цель незаконного обогащения сотрудник пытается скопировать и пересохранить содержимое конфиденциального документа в другой файл на ПК для последующей продажи данных

## При отсутствии DSS

В случае отсутствия мер по обеспечению безопасности сотрудник скомпрометирует данные компании, что может привести к финансовым и репутационным рискам. Функциональность решений класса DLP не позволяет устанавливать ограничения на копирование содержимого документа и вставку его через буфер обмена в любое другое приложение вне защищаемого контура

## При использовании DSS

DSS позволяет контролировать и настраивать роли и права доступа пользователей на основе меток конфиденциальности.

Следовательно, пользователю при разрешенной возможности открывать и просматривать документ можно запретить выполнять следующие действия при работе с документом:

- «сохранить как»;
- «копировать»

# Jay Data

российская платформа, осуществляющая поиск, классификацию, маскирование конфиденциальной информации в базе данных, что позволяет компаниям обеспечить надежную защиту чувствительных данных от нелегитимного использования сотрудниками и сторонними лицами



# Jay Data – поиск и маскирование чувствительной информации в базах данных

## Задачи, которые решает Jay Data:

- Безопасный обмен чувствительной информацией в базах данных отделам разработки и тестирования
- Соответствие требованиям PCI DSS, GDPR, 152-ФЗ, ISO/IEC 27001:2022
- Нахождение чувствительной информации в базах данных

## Результат внедрения Jay Data:

- Управление конфиденциальными данными для надежных и безопасных политик обмена
- Уменьшение риска неправомерного использования или потери данных
- Безопасное использование чувствительных данных в тестовых и облачных средах
- Соответствие принятым в компании политикам безопасности

# Jay Data – это



## **Масштабируемая платформа для поиска и маскирования данных**

Запускайте процессы поиска и маскирования чувствительных данных и управляйте ими из единой высокопроизводительной платформы.



## **Гибкий и надежный инструмент маскирования данных**

Создавайте структурные правила для обезличивания данных путем применения различных методов и алгоритмов с возможностью сохранения консистентности, уникальности, контрольных сумм и пр.



## **Широкий выбор функциональных возможностей**

Воспользуйтесь возможностями микросервисной архитектуры для масштабирования решения и гибкой встраиваемости в тестовые среды. Профилируйте и маскируйте различные типы СУБД: Oracle, PostgreSQL, Vertica, Apache Hive, MySQL, MS SQL, ClickHouse и пр.

# Алгоритм работы Jay Data

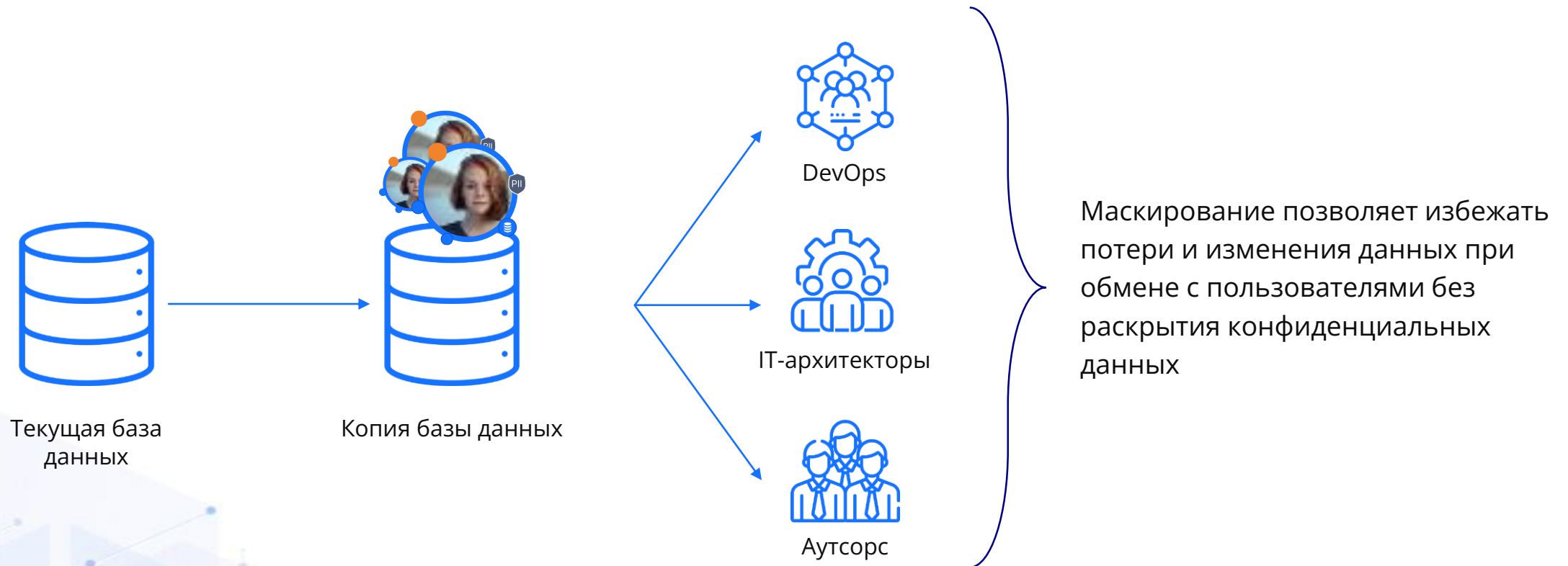


# Методы маскирования данных

| Методы маскирования   | В продуктивной базе     | В маскированной копии базы  |
|---|-------------------------|-----------------------------|
| Маскирование числа  | 45.798.776              | 78.849.012                  |
| Замена на NULL  | Директор по продажам    | Null                        |
| Замена на константу   | Галина                  | Полина                      |
| Замена N последних символов на другие служебные символы               | 1234 5678 9578 1122     | 1234 5678 9578 ****         |
| Маскирование времени и даты   | 12.03.2023 14:45:00     | 23.04.2022 21:55:01         |
| Замена на значения из справочника                                     | г.Москва, ул. Дубровина | г.Казань, ул. 40 лет победы |
| Замена ИНН, СНИЛС, номера карты/счета с сохранением контрольной суммы | 9687 4657 0845 3412     | 5674 6850 0044 5634         |

# Статическое маскирование

В режиме статического маскирования создается копия продуктивной базы данных, в которой обезличивается вся чувствительная информация путем применения заранее настроенных правил и выбранных методов маскирования. Таким образом специалисты отделов тестирования, разработки или сторонних компаний получают альтернативную версию продуктивной базы данных



# Особенности Jay Data

- Запускайте одновременно несколько параллельных процессов маскирования
- Проводите профилирование и маскирование как определенного количества строк, так и всей базы
- Создавайте копию базы с замаскированными данными путем применения статического маскирования
- Контролируйте отключение и включение служебных объектов
- Используйте два режима маскирования (INSERT и UPDATE) для более гибкого решения задач компании



# Кейс. Маскирование данных в БД



## Описание ситуации

В компании стоит задача по передаче базы данных в отдел разработки для создания нового приложения. При этом структура данных должна быть сохранена в неизменном виде

## Решение

С целью предотвращения возможной утечки конфиденциальных данных было решено приобрести и внедрить систему маскирования информации в передаваемых базах данных

## Результат

Компания замаскировала базу с сохранением консистентности данных и передала ее в работу отделу разработки, минимизировав тем самым риски потери чувствительных данных

# Кейс. Маскирование данных в БД



## Описание ситуации

Банкам необходимо соответствовать стандартам PCI DSS с целью выполнения требований платежной системы Мир и сотрудничества с Union Pay

## Решение

Банк внедрил решение Jay Data для хранения номеров карт PAN в базах данных в замаскированном виде. Теперь только персонал банка при бизнес-необходимости может видеть все платежные данные клиентов

## Результат

Банк успешно прошел процесс сертификационного аудита на соответствие требованиям международного стандарта безопасности данных PCI DSS



# DataNova Object Recognition (OR)

комплексное решение, реализованное на основе глубоких нейронных сетей в алгоритмах компьютерного зрения, необходимое для анализа и реагирования на инциденты, связанные с нарушением прав доступа и компрометацией конфиденциальной информации со стороны сотрудников компании

# DataNova OR позволяет фиксировать



Наличие  
нелегитимных /  
незарегистрированных  
лиц за APM



Факт отсутствия  
сотрудника за рабочим  
местом



Приложения, которыми  
пользуется сотрудник



Наличие телефона при  
попытках фотографирования  
экрана APM



Наличие сторонних  
объектов  
в объективе  
веб-камеры

# Особенности DataNova OR

- Формируйте аналитические отчеты для специалистов информационной или кадровой безопасности
- Используйте около 100 объектов обнаружения «из коробки» помимо мобильного телефона
- Перехватывайте события во время видеоконференцсвязи за счет подключения виртуальной камеры
- Воспользуйтесь гибкой настройкой формирования индивидуальных правил мониторинга



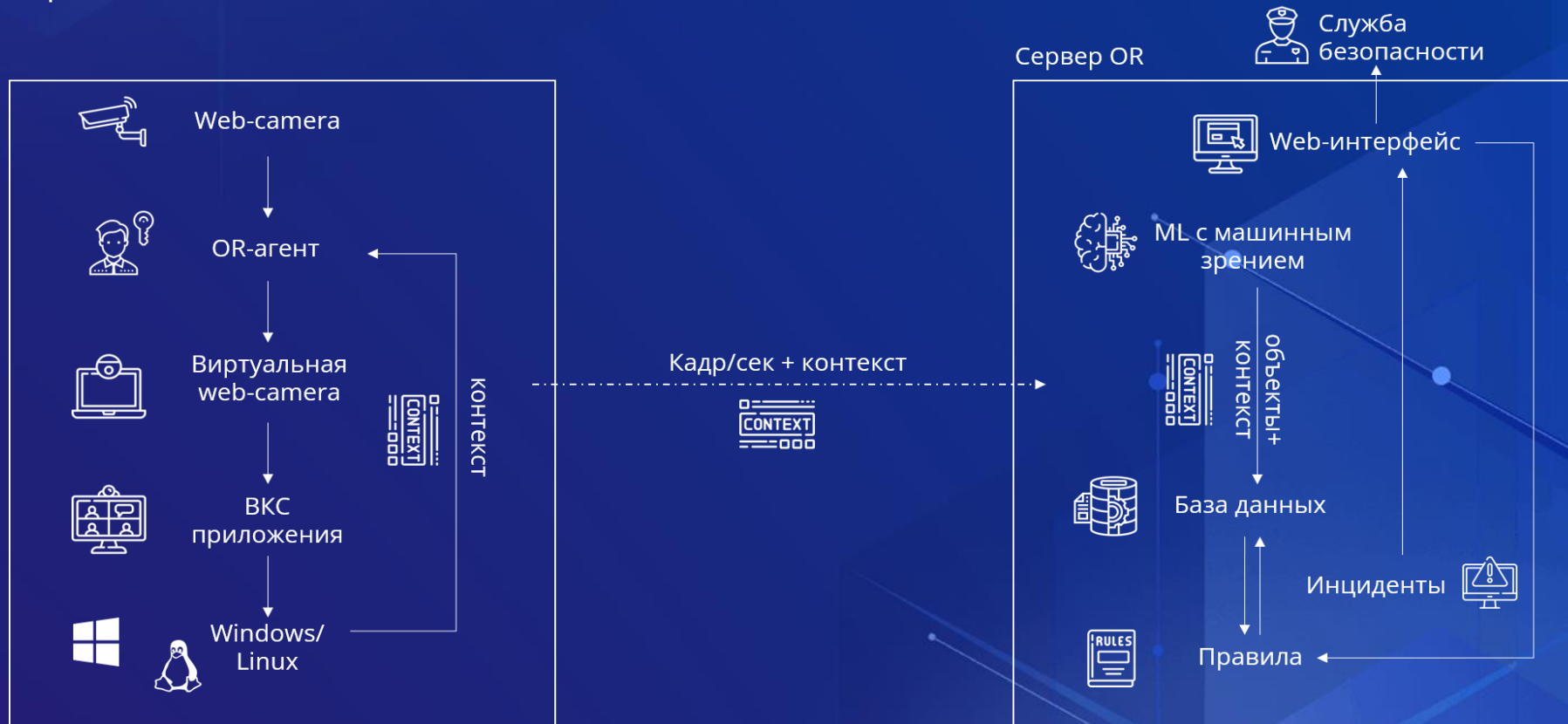
# Особенности DataNova OR

- Отслеживайте работающие и фоновые приложения, включая собственные сервисы компании
- Воспользуйтесь возможностью распознавания живого/ неживого (фото, телефон) человека, т.е. реализованным функционалом так называемого Live Detect
- Сохраняйте «историю» событий, полученных из видео-потока, что позволит идентифицировать факт нарушения политик безопасности компании

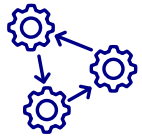


# Схема работы DataNova OR

Решение позволяет с помощью перехвата видеопотока с веб-камеры осуществлять мониторинг за деятельностью сотрудников и выявлять нелегитимную активность согласно настроенным политикам безопасности и блокировать рабочую станцию



# Результат внедрения DataNova OR



Выявление лиц, пытающихся сфотографировать\подглядывающие в экран с конфиденциальными данными



Выявление наличия посторонних лиц, нахождения в публичном месте при удалённой работе с конфиденциальными данными



Проверка по FaceID, подтверждающая, что доступ к данным получает авторизованный сотрудник



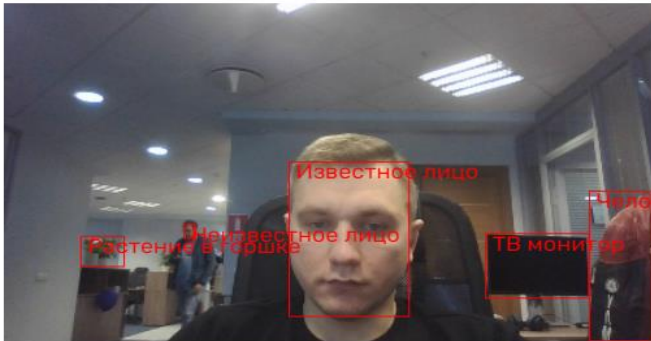
Выявление фактов отсутствия на рабочем месте, а так же занятия посторонними занятиями

# Примеры инцидентов, зафиксированных ОР

Событие GUID: 861554f5-7a5b-49a2-bd29-119a1d9e96d4

|                       |  |
|-----------------------|--|
| Уникальный GUID       | 861554f5-7a5b-49a2-bd29-119a1d9e96d4   |
| Время на АРМ          | 20.12.22 15:13:31                      |
| Время индексации      | 30.01.23 15:13:17                      |
| Имя АРМ               | DESKTOP-M3FCBTU                        |
| Пользователь          | lovtsov.d                              |
| Серийный номер АРМ    | MP25JEZ8                               |
| Активное приложение   | WINWORD.EXE                            |
| Запущенные приложения | Taskmgr.exe, WINWORD.EXE, explorer.exe |
| Критичность события   | low                                    |
| Статус АРМ            | разблокировано                         |

Выделить распознанные объекты на изображении



| Название распознанного объекта | Количество | Уверенность модели | Названия правил |
|--------------------------------|------------|--------------------|-----------------|
| Человек                        | 1          | 0.76               |                 |
| Растение в горшке              | 1          | 0.65               |                 |
| ТВ монитор                     | 1          | 0.61               |                 |



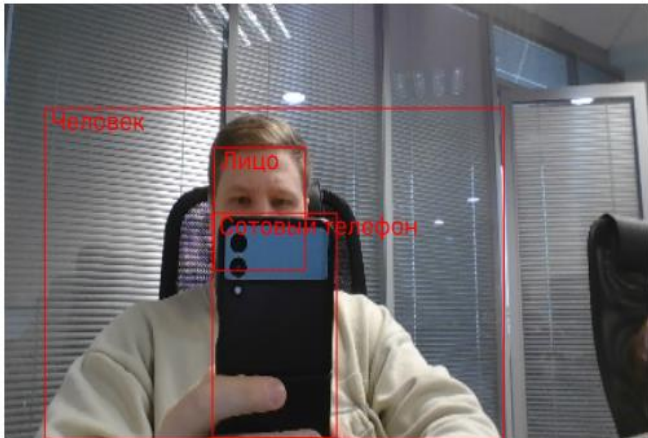
Фиксация неизвестного лица в кадре

# Примеры инцидентов, зафиксированных OR

Событие GUID: 2b97eab7-ca91-4854-85d1-66f762cea866

|                       |   |
|-----------------------|---|
| Уникальный GUID       | 2b97eab7-ca91-4854-85d1-66f762cea866                |
| Время на АРМ          | 30.01.23 14:37:04                                   |
| Время индексации      | 30.01.23 14:36:56                                   |
| Имя АРМ               | DESKTOP-RH2PG11                                     |
| Пользователь          | bodnar.i  |
| Серийный номер АРМ    | PF3B3CBF  |
| Активное приложение   | WINWORD.EXE   |
| Запущенные приложения | Taskmgr.exe, WINWORD.EXE, browser.exe, explorer.exe |
| Критичность события   | low   |
| Статус АРМ            | разблокировано                                      |

Выделить распознанные объекты на изображении



| Название распознанного | Количество | Уверенность | Названия правил |
|------------------------|------------|-------------|-----------------|
|------------------------|------------|-------------|-----------------|



Фиксация сотового телефона в кадре



# Кейс. Попытка кражи информации



## Описание ситуации

Пользователь осуществляет попытку кражи конфиденциальной информации путем фотографирования экрана рабочей станции

## Решение

С целью предотвращения возможной утечки конфиденциальных данных было решено приобрести и внедрить решение для выявления попыток фотографирования экрана

## Результат

При определении в кадре веб-камеры рабочей станции мобильного телефона при работе с приложениями, потенциально содержащими конфиденциальную информацию, происходит создание события инцидента с возможной блокировкой рабочей станции

# Кейс. Попытка передачи информации третьему лицу



## Описание ситуации

Пользователь, имеющий доступ к конфиденциальной информации, показывает ее коллегам, доступа к ней не имеющим, на экране своего рабочего компьютера

## Решение

С целью предотвращения возможной утечки конфиденциальных данных было решено приобрести и внедрить решение отслеживания события появления в кадре незарегистрированного лица

## Результат

При определении в кадре веб-камеры рабочей станции неизвестных лиц при работе с приложениями, потенциально содержащими конфиденциальную информацию, происходит создание события инцидента с возможной блокировкой рабочей станции

# DataGrain Remote User Monitoring Analytics (DataGrain RUMA)

решение, предназначенное для мониторинга поведения пользователей, нацелено на обнаружение и реагирование на аномальную и нелегитимную деятельность сотрудников компании

Соответствие требованиям законодательства:  
152-ФЗ, ФСТЭК №21, 17

Решение RUMA включено в единый реестр  
российского ПО МИНКОМ связи от 30.12.2022 №16236

# Задача DataGrain RUMA

Решение осуществляет сбор и анализ данных из множества источников:

- Логи серверов, рабочих станций, маршрутизаторов и других устройств
- Реестры систем контроля доступа и аутентификации
- Данные других ИБ-решений – брандмауэров, антивирусов, SIEM-продуктов и DLP-систем
- Кадровые регистры компании и другая информация
- Данные по поведению пользователей в системе
- Переписку пользователей в социальных сетях, мессенджерах, по электронной почте

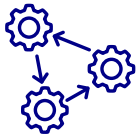


# Особенности DataGrain RUMA

- Актуальная взвешенная оценка уровня риска по каждому сотруднику
- Возможность сбора логов из неограниченного количества источников, включая архивные события
- Создание шаблонов нормального поведения пользователей для сравнения показателей по сотрудникам
- Кастомная настройка правил выявления аномального поведения
- Наличие статистических аналитических моделей, марковских цепей



# Результат внедрения DataGrain RUMA



Выявление ранее не известных схем нарушений внутренним злоумышленником



Сигнализация о проблемах на раннем этапе при отклонении от стандартного профиля поведения

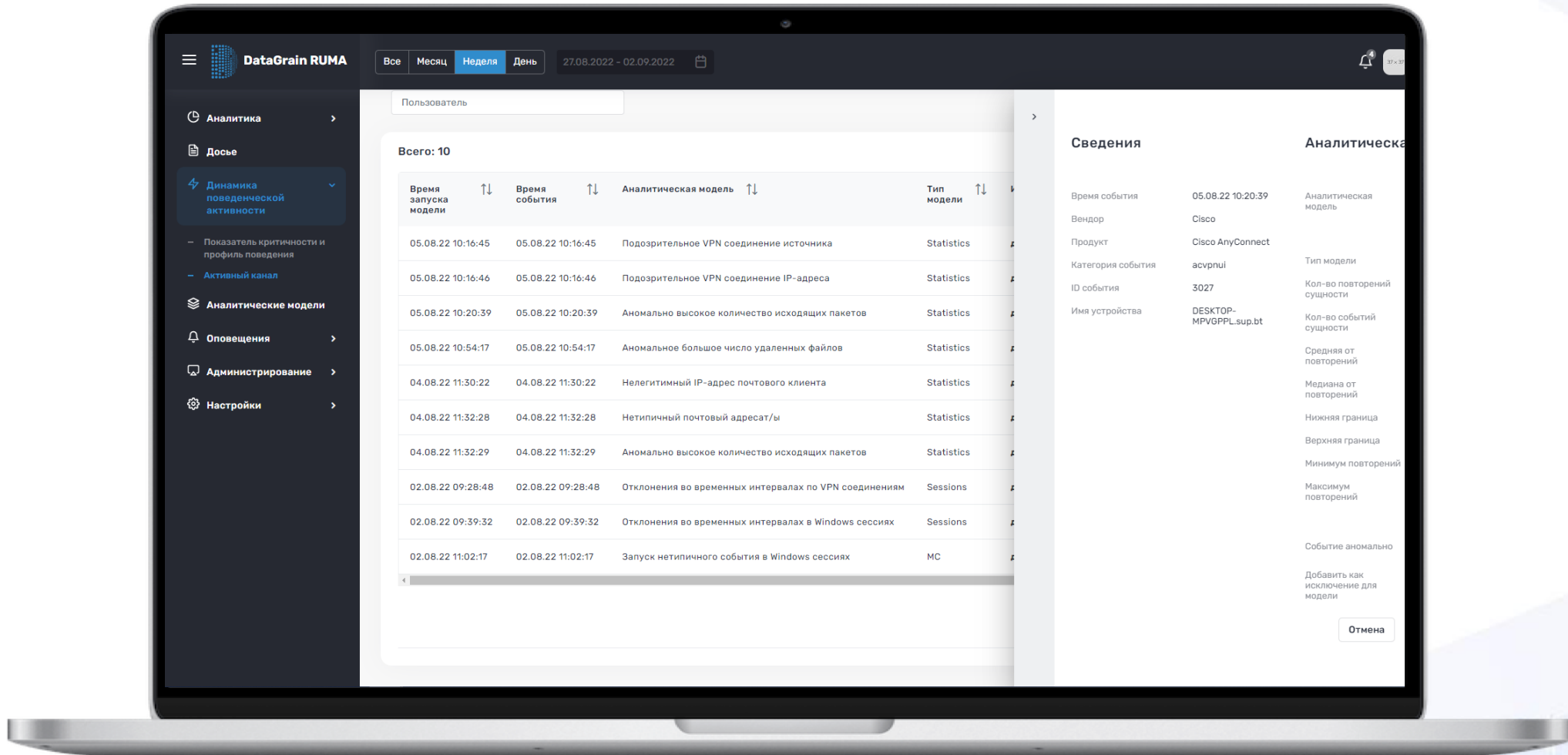


Выявление случаев компрометации, шпионажа, мошенничества, кражи интеллектуальной собственности

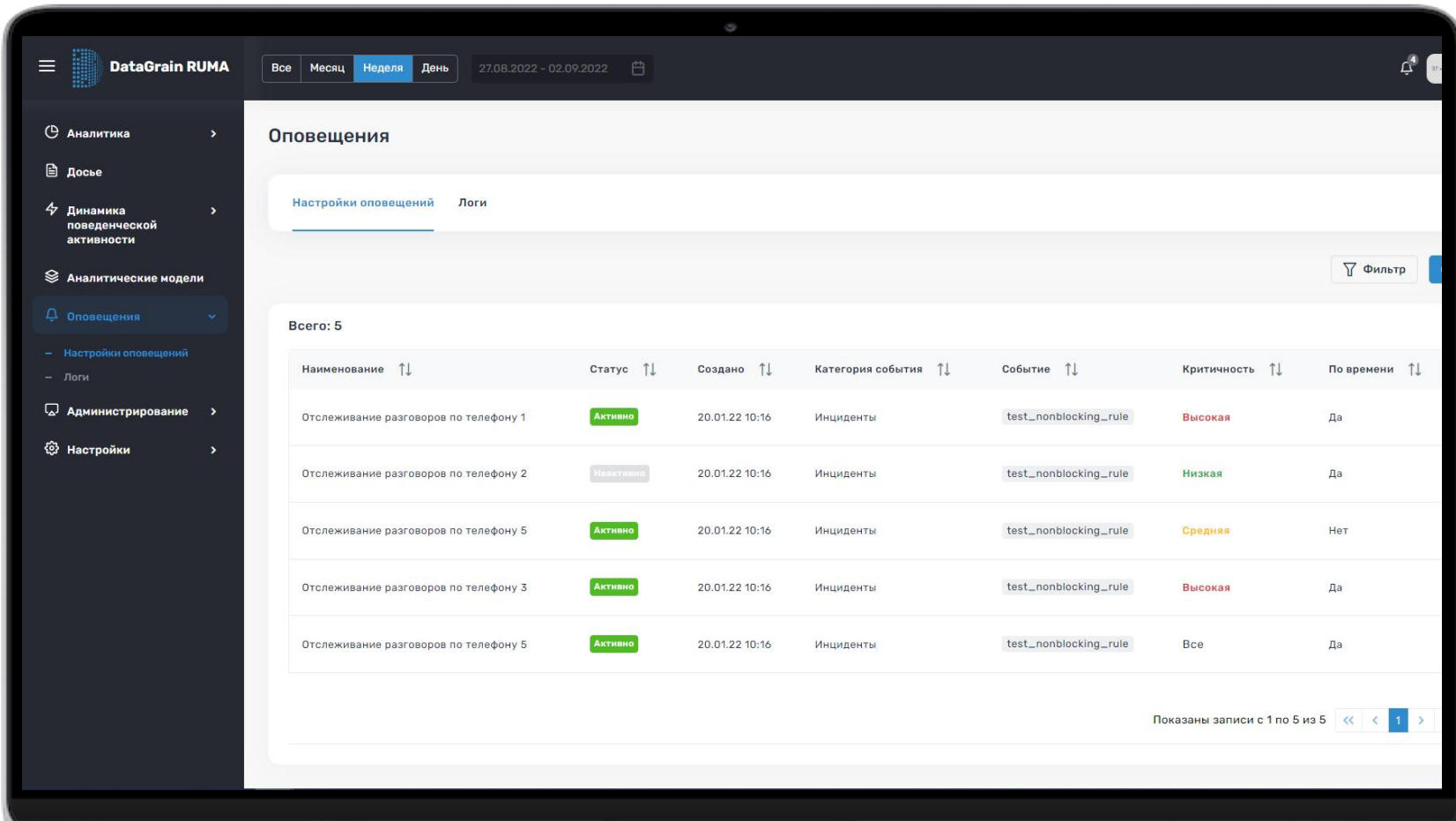


Выявление случаев небрежности и халатности

# Примеры интерфейса DataGrain RUMA



# Примеры интерфейса DataGrain RUMA



The screenshot displays the DataGrain RUMA interface. The top navigation bar includes a menu icon, the product name "DataGrain RUMA", and filters for "Все", "Месяц", "Неделя", and "День". The date range "27.08.2022 - 02.09.2022" is also visible. The left sidebar contains a navigation menu with items: "Аналитика", "Досье", "Динамика поведенческой активности", "Аналитические модели", "Оповещения" (selected), "Настройки оповещений", "Логи", "Администрирование", and "Настройки".

The main content area is titled "Оповещения" and has two tabs: "Настройки оповещений" (active) and "Логи". A "Фильтр" button is located in the top right of the main area. Below the tabs, it indicates "Всего: 5" items.

| Наименование ↑↓                       | Статус ↑↓ | Создано ↑↓     | Категория события ↑↓ | Событие ↑↓            | Критичность ↑↓ | По времени ↑↓ |
|---------------------------------------|-----------|----------------|----------------------|-----------------------|----------------|---------------|
| Отслеживание разговоров по телефону 1 | Активно   | 20.01.22 10:16 | Инциденты            | test_nonblocking_rule | Высокая        | Да            |
| Отслеживание разговоров по телефону 2 | Неактивно | 20.01.22 10:16 | Инциденты            | test_nonblocking_rule | Низкая         | Да            |
| Отслеживание разговоров по телефону 5 | Активно   | 20.01.22 10:16 | Инциденты            | test_nonblocking_rule | Средняя        | Нет           |
| Отслеживание разговоров по телефону 3 | Активно   | 20.01.22 10:16 | Инциденты            | test_nonblocking_rule | Высокая        | Да            |
| Отслеживание разговоров по телефону 5 | Активно   | 20.01.22 10:16 | Инциденты            | test_nonblocking_rule | Все            | Да            |

At the bottom right of the table area, it says "Показаны записи с 1 по 5 из 5" and includes pagination controls with a "1" button.



# Кейс. Компрометация учетной записи сотрудника



## Описание ситуации

Сотрудник, не соблюдающий политики информационной безопасности, скомпрометировал свою учетную запись

## Решение

С целью предотвращения возможной утечки конфиденциальных данных было решено приобрести и внедрить решение для выявления аномальных действий сотрудников

## Результат

RUMA выявила нетипичное количество запущенных процессов, тем самым, обнаружив аномалию. Risk score сотрудника был повышен, в связи с чем, RUMA направила оповещение сотруднику безопасности. После проведения расследования инцидента, с помощью решения RUMA, была выявлена компрометация учетной записи

# Кейс.

## Сложности с процессом регулирования предоставления прав



### Описание ситуации

Компания с крупной инфраструктурой и большим количеством сотрудников имеет сложности с процессом регулирования предоставления прав на использование ресурсов информационной среды

### Решение

С целью предотвращения возможной утечки конфиденциальных данных было решено приобрести и внедрить решение для выявления превышения уровня прав сотрудников

### Результат

RUMA позволяет выявлять превышение предоставленных прав доступа или чрезмерное количество неактивных учетных записей пользователей. С помощью решения RUMA, было задетектировано несоответствующее предоставление прав доступа некоторым пользователям, и выявлены пути получения этого доступа

# DataGrain Event Stream Optimization (DataGrain ESO)

решение, предназначенное для сбора, профилирования, сжатия и хранения событий ИБ, с возможностью разграничения прав доступа и осуществления статистического анализа собираемых данных

Соответствие требованиям законодательства:  
152-ФЗ, ФСТЭК №21, 17

Решение ESO включено в единый реестр российского  
ПО МИНКОМ связи от 03.02.2023 №16469

# Задача DataGrain ESO

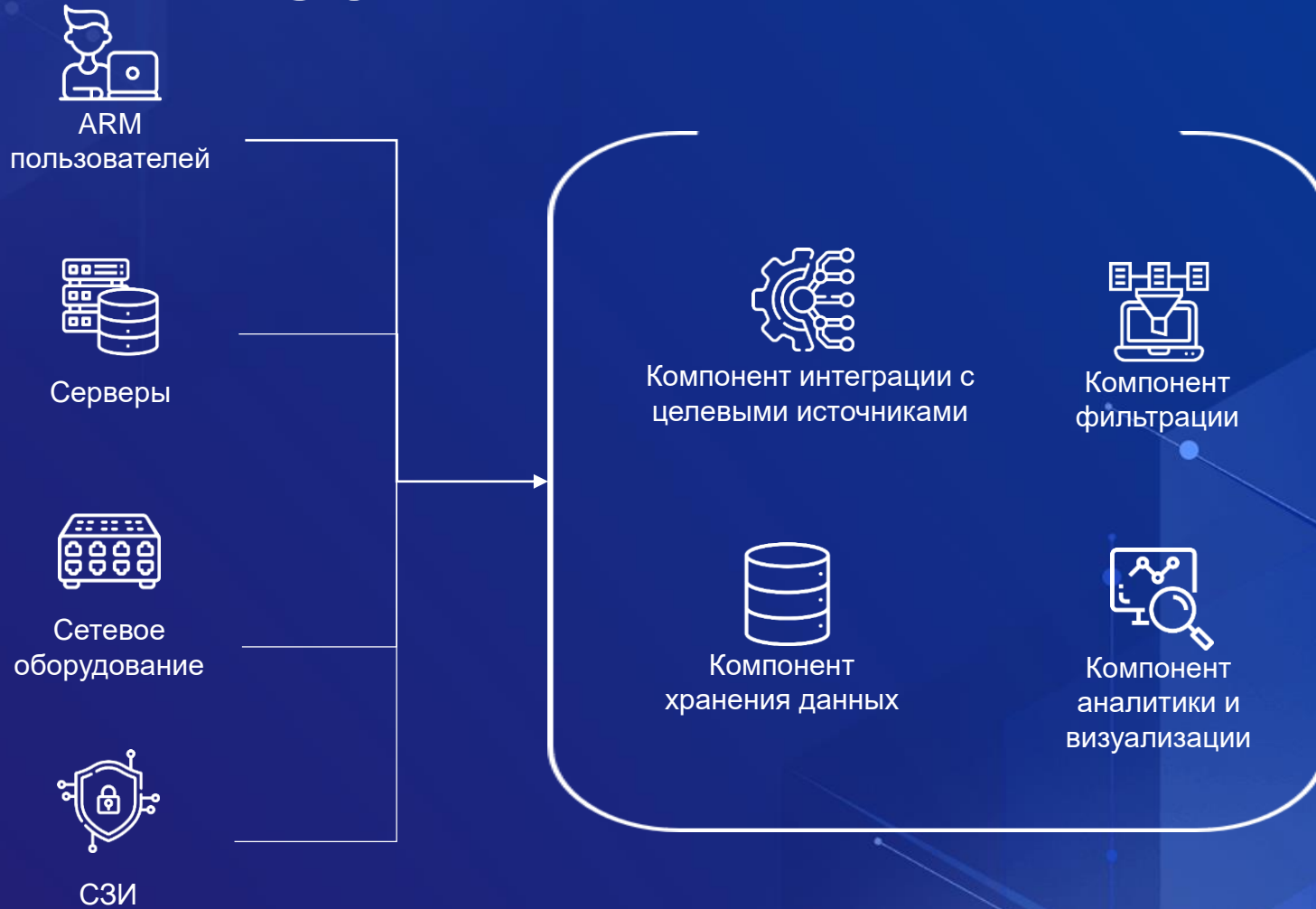
Решение объединяет данные журналов и передает их в один централизованный, доступный и простой в использовании интерфейс с возможностью:

- Эффективной интерпретации данных за счет хранения журналов из нескольких источников в одном месте
- Применение политик хранения к данным, чтобы они были доступны в течение определенного периода времени
- Поиска необходимой информации в собираемых данных
- Низкие затраты и увеличенное пространство для хранения и резервного копирования исторических данных
- Предоставление доступа пользователям к определенным данным

# Особенности DataGrain ESO

- Интеграция с целевыми источниками данных по различным протоколам и интерфейсам
- Расширенный мониторинг системы и ее компонентов
- Реализация наиболее эффективной структуры по долгосрочному хранению данных
- Гибкие возможности по разграничению доступа к данным
- Гибкие возможности по поиску информации в собираемых данных

# Архитектурная схема ESO



# Ключевые показатели



Высокоэффективная  
компрессия данных

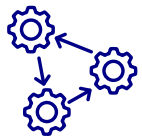


Быстрые поисковые  
запросы и визуализация



Архитектурные  
привилегии

# Результат внедрения DataGrain ESO



Выявление схожих инцидентов (эпизодов) и нарушений в прошлом



Проведение всеобъемлющих расследований в случае инцидента, подготовка доказательной базы



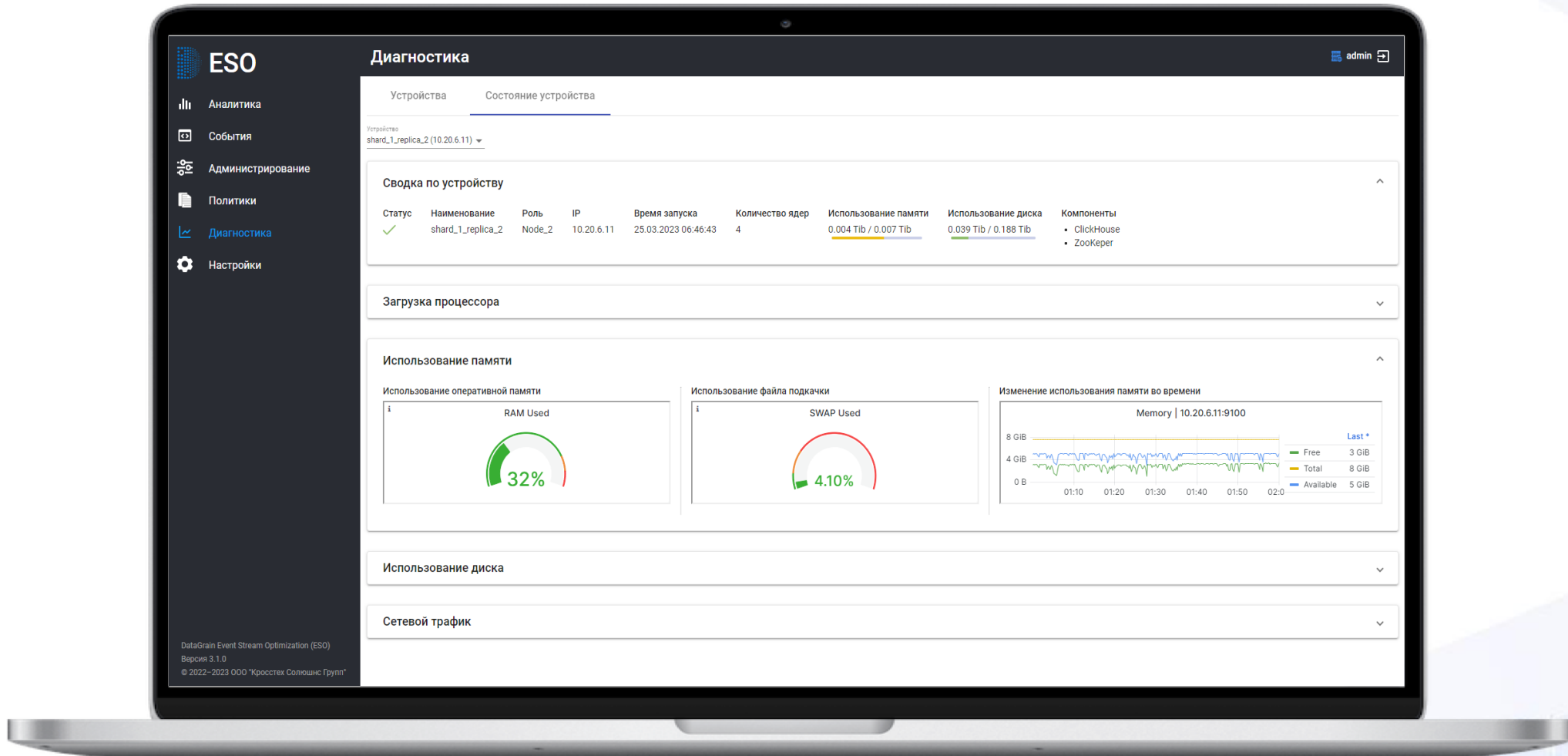
Сбор и долгосрочное хранение всего, что происходило в инфраструктуре организации



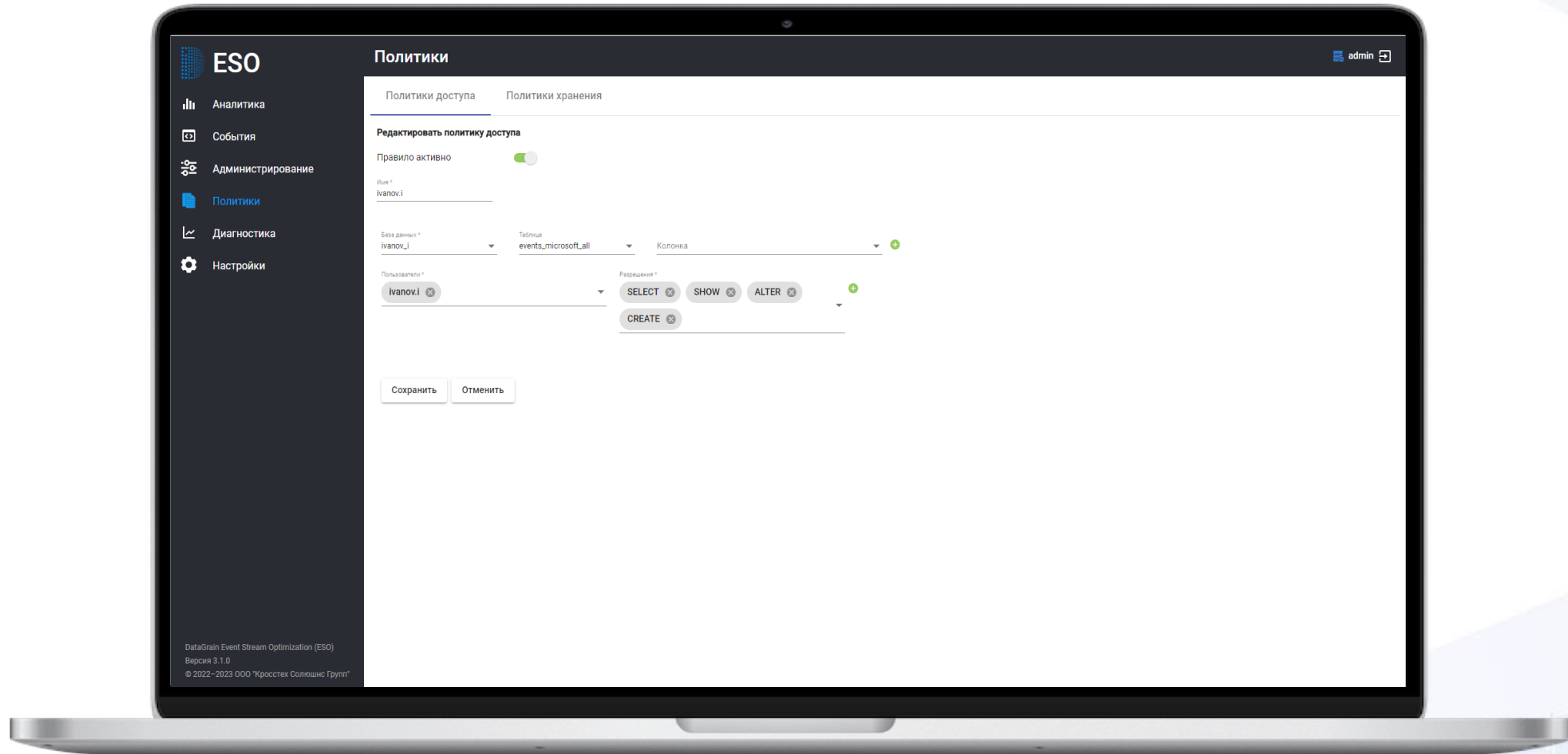
Снижение затрат на хранения исторических данных



# Примеры интерфейса DataGrain ESO



# Примеры интерфейса DataGrain ESO



# Кейс. Соблюдение требований регулятора

## Описание ситуации

Субъектам КИИ необходимо соответствовать мере ИНЦ.6 «Хранение и защита информации о компьютерных инцидентах» по Приказу ФСТЭК России № 239

## Решение

Решение ESO обеспечивает долгосрочное высокоэффективное хранение событий безопасности с высоким коэффициентом сжатия

## Результат

Благодаря ESO компания выполнила требования регулятора и сократила затраты на средства хранения событий безопасности

# Кейс.

## Расследование распределенных по времени инцидентов

### Описание ситуации

Компания с крупной инфраструктурой испытывает сложности с процессом расследования инцидентов из-за наличия множества различных СЗИ и решений для хранения логов безопасности

### Решение

С помощью решения ESO было реализовано единое централизованное хранилище событий безопасности

### Результат

Была повышена эффективность проведения расследований за счет централизации всех журналов безопасности в ESO, обеспечение возможности анализа хранимых данных с использованием пользовательских фильтров, датасетов, витрин (дашбордов)

# CrossTech Smart Assets (CTSA)

комплексный продукт, ориентированный на физический учёт, финансовый контроль и управление контрактными обязательствами IT-активов организации в течение всего их жизненного цикла

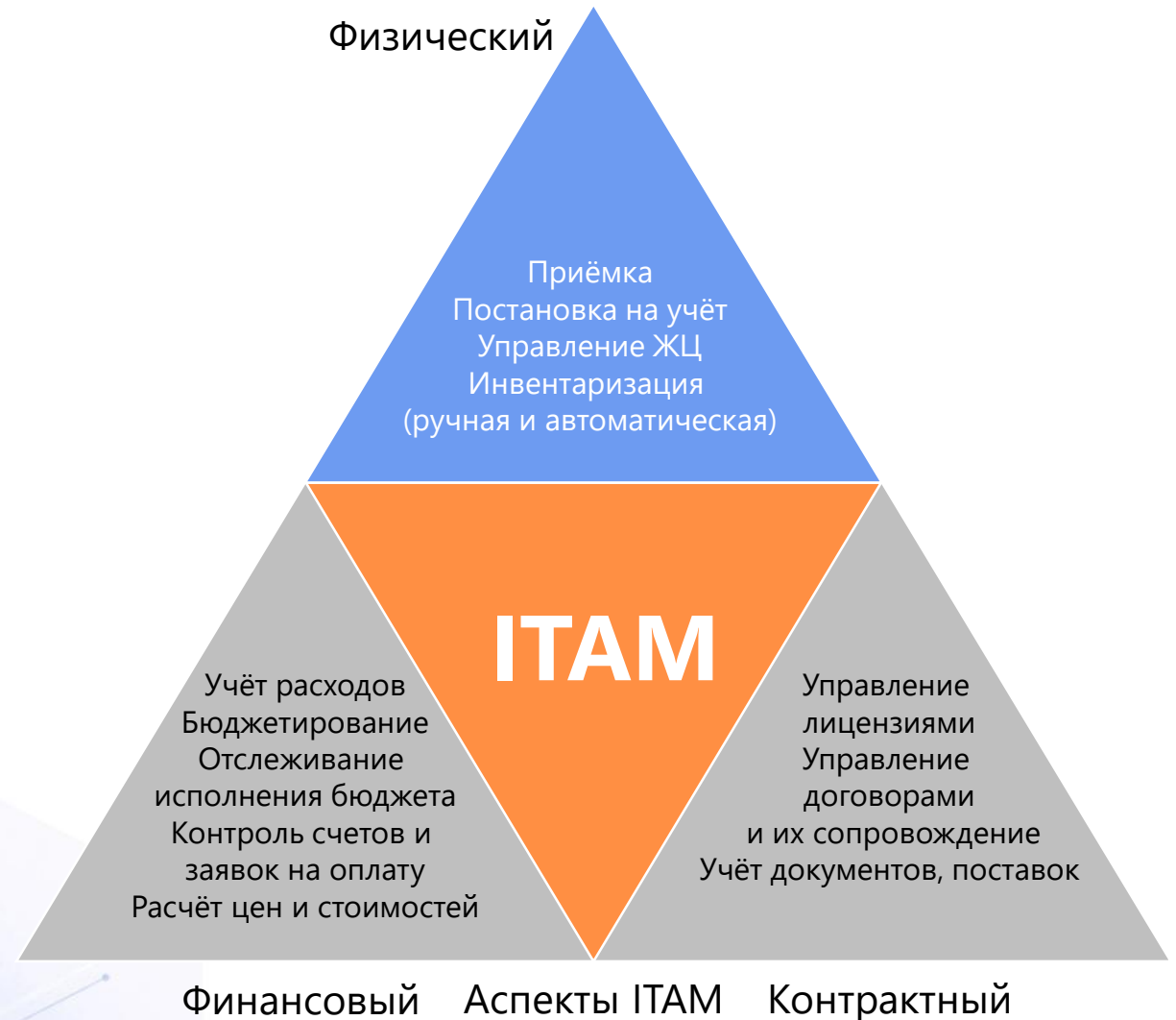
Соответствие требованиям законодательства:  
152-ФЗ, ФСТЭК №21, 17

Решение CTSA включено в единый реестр российского  
ПО МИНКОМ связи от 30.12.2021 №12408

# Управление ИТ-активами (ИТАМ)

**IT Asset Management, ИТАМ** - Это набор взаимосвязанных процедур, нацеленных на решение вопросов физического учёта, финансового контроля и контрактных обязательств, связанных с ИТ-активами, на протяжении всего их жизненного цикла

**ИТ-актив** - это любой материальный или нематериальный элемент ИТ-инфраструктуры, имеющий финансовое значение для организации



# Ценность внедрения ITAM

- Получение достоверной информации о состоянии ИТ-активов для принятия эффективных управленческих решений, бизнес-планирования, обеспечения информацией ответственных лиц и подразделений
- Снижение операционных затрат вследствие неэффективного использования и учета ИТ-активов
- Снижение трудозатрат для сбора ИТ-потребностей, отслеживания статуса закупок и планирования ИТ-бюджетов
- Снижение репутационных и финансовых рисков ввиду отсутствия учета использования лицензионного ПО

# Особенности CTSA

- Масштабирование и отказоустойчивая конфигурация
- Одновременное управление по нескольким юридическим лицам
- Возможность «динамически» добавлять атрибуты объектов
- Отслеживание изменений любых атрибутов
- Предоставление доступа пользователям к определенным данным
- Конфигуратор отчетов/виджетов и полнотекстовый поиск (в том числе по вложениям)
- Модуль администрирования для управления приложением без перезапуска
- Возможность разработки Web-портала и личного кабинета для «внешних» пользователей



# Автоматизированные в СТСА процедуры



Управление  
потребностями и  
заказами



Управление делами  
(заявками, запросами и  
нарядами)



Управление договорами



Управление поставками  
и оплатами



Управление портфелем  
ИТ-активов



Управление финансами

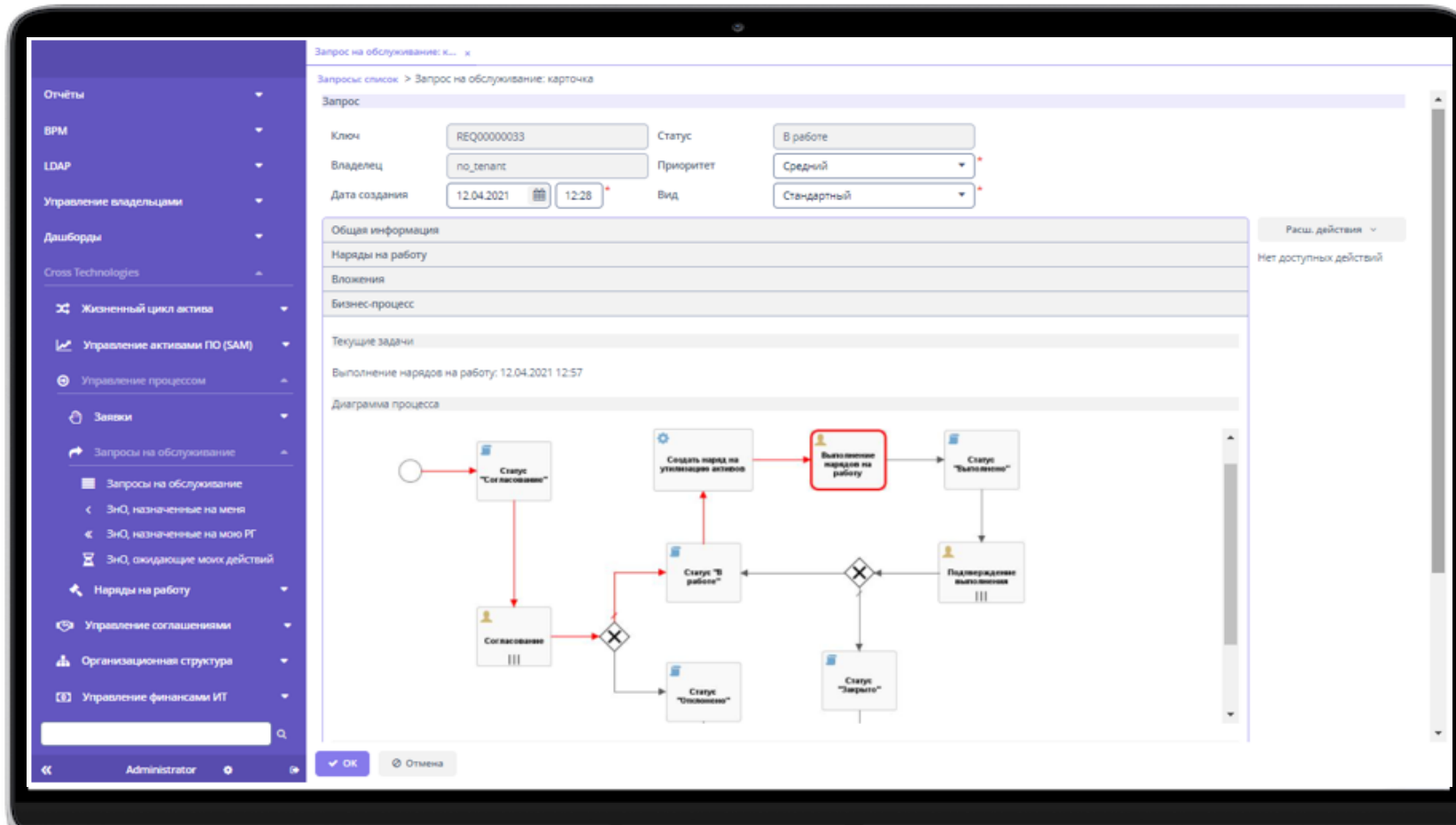


Проведение  
инвентаризации



Управление активами  
ПО (SAM)

# Примеры интерфейса CTSA



The screenshot displays the CTSA interface for a service request. On the left is a navigation menu with categories like 'Отчёты', 'BPM', 'LDAP', and 'Управление владельцами'. The main area shows a 'Запрос на обслуживание' card with the following details:

- Ключ: REQ00000033
- Статус: В работе
- Владелец: no\_tepalr
- Приоритет: Средний
- Дата создания: 12.04.2021 12:28
- Вид: Стандартный

Below the card, there are sections for 'Общая информация', 'Наряды на работу', 'Вложения', and 'Бизнес-процесс'. The 'Бизнес-процесс' section shows a flowchart with the following steps:

- Статус "Согласованно"
- Создать наряд на утилизацию активов
- Выполнение нарядов на работу (highlighted in red)
- Статус "Выполнено"
- Подтверждение выполнения
- Статус "Закрыто"
- Статус "Отклонено"
- Статус "В работе"
- Согласование

The interface also includes a 'Расш. действия' dropdown menu and 'Нет доступных действий' text. At the bottom, there are 'OK' and 'Отмена' buttons.

# Примеры интерфейса CTSA

Связи клиент-ресурс x Информационная система: к... x  
 Запись активна

Основная информация  
 Сервисно-ресурсная модель

Тип связи: ИСПОЛЬЗУЕТ  
100 %

Открыть Создать... Ж Удалить

| Класс клиента   | Название      | Тип      | Вес |
|-----------------|---------------|----------|-----|
| am_informationS | Crosstech Srv | Располож | 0.5 |

Открыть Создать... Ж Удалить

| Класс рес | Название               | Тип       | Вес |
|-----------|------------------------|-----------|-----|
| am_Asset  | 1 Windows Server 2016  | Используй | 1   |
| am_Asset  | 1 ProLiant Server D500 | Используй | 1   |

Administrator

# Кейс. Снижение операционных затрат

## Описание ситуации

Необходимость снижения операционных затрат вследствие неэффективного использования и учета ИТ-активов

## Решение

Внедрение продукта, ориентированного на физический учёт, финансовый контроль и управление ИТ-активами организации в течение всего их жизненного цикла

## Результат

Внедрение CТСА позволяет реализовать:  
Отслеживание расходов на ИТ-активы, позволяющее рассчитывать их совокупную стоимость владения (ТСО)  
Отслеживание расходов в разрезе МВЗ, статей затрат  
Распределение и планирование ИТ-бюджетов в разрезе статей бюджетов  
Возможность автоматического расчёта цен с учётом ставок НДС и курса валют  
Формирование оперативных и периодических отчетов

# Кейс. Снижение репутационных и финансовых рисков

## Описание ситуации

Необходимость снижения репутационных и финансовых рисков ввиду отсутствия учета использования лицензионного ПО

## Решение

Внедрение продукта, ориентированного на физический учёт, финансовый контроль и управление IT-активами организации в течение всего их жизненного цикла

## Результат

Внедрение CTSA позволяет реализовать:  
Автоматический сбор информации об устройствах в сети и установленном на них ПО  
Учёт и управление жизненным циклом лицензий  
Сведение количества закупленных лицензий с установленным ПО (лицензионный баланс)  
Автоматическая нормализация данных из системы дискаверинга  
Формирование оперативных и периодических отчетов



# CROSSTECH

## SOLUTIONS GROUP



Москва, Ленинградский пр.31А,  
стр.1,  
БЦ Монарх

+7 (495) 741-88-64

[info@ct-sg.ru](mailto:info@ct-sg.ru)