

# НОВЫЕ ТЕХНОЛОГИИ КОНТРОЛЯ: БЫТЬ ИЛИ НЕ БЫТЬ?



Игорь Лебедев

Руководитель департамента экономической  
безопасности и управления рисками

[ilebedev@fa.ru](mailto:ilebedev@fa.ru)

# Предпосылки цифровой трансформации СБ



## Трансформация угроз из-за цифровизации бизнеса

Новые цифровые технологии радикально трансформируют традиционные и создают новые угрозы для бизнеса

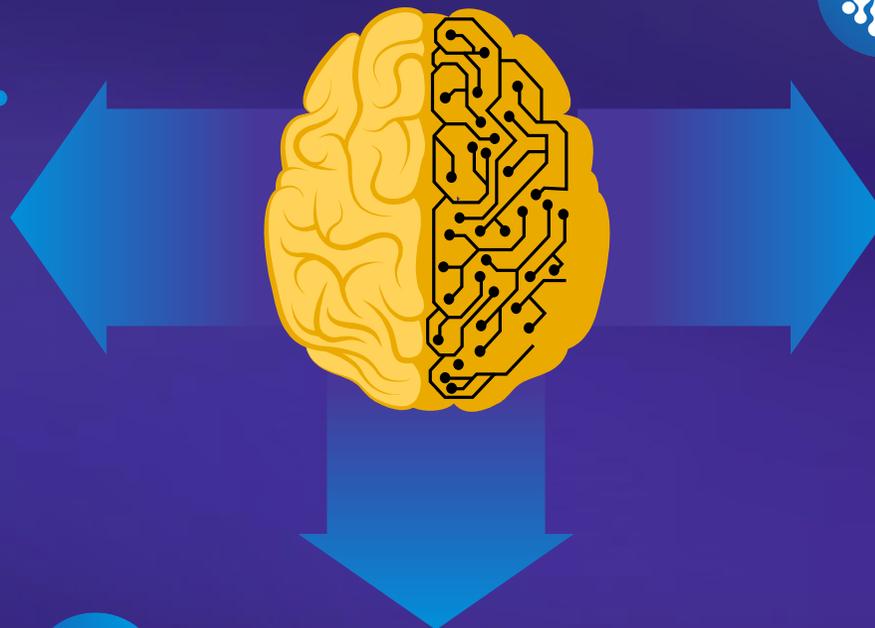
Четвертая промышленная революция, «интернет вещей», искусственный интеллект, машинное обучение, «большие данные», роботизация, облачные технологии и многократно усилило угрозы и риски бизнеса



## Трансформация бизнес-моделей и функции СБ

Давление на традиционные формы поддержки бизнеса со стороны СБ

Необходимость постоянного изменения, адаптации к меняющимся условиям и технологиям ведения бизнеса. Меняется картина бизнес-рисков, появляются новые возможности – СБ должна своевременно реагировать.

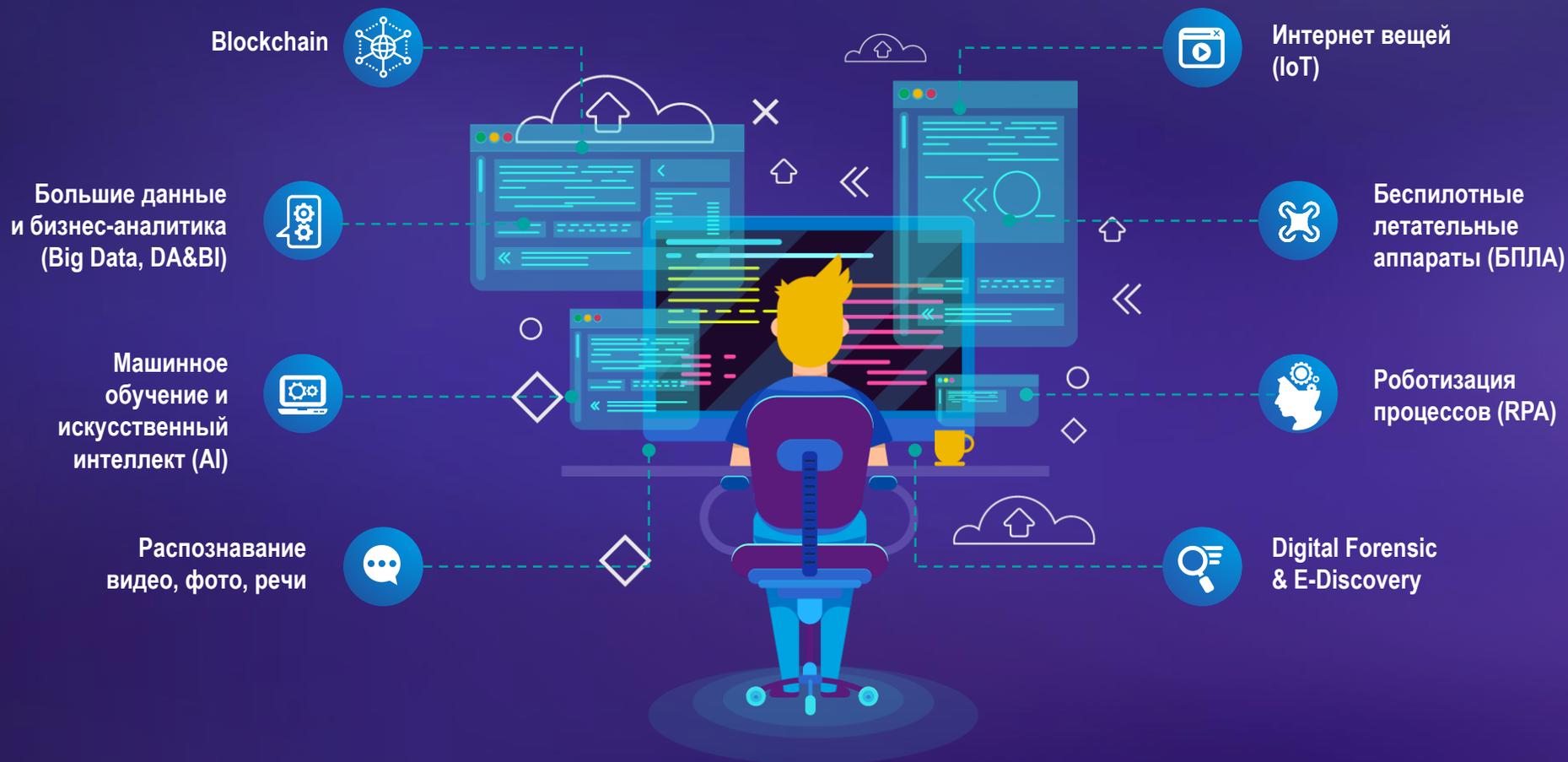


## Изменение и развитие человеческого потенциала

Меняются профили работников - новые требования к компетенциям и новые возможности для развития экспертизы СБ

Перед СБ стоят задачи цифровой трансформации своих компетенций, расширения экспертизы в направлении «цифровых профессий».

# Ключевые цифровые и технологические инновации. Возможности их применения в контуре СБ



# Blockchain

## Решаемая проблематика:

Blockchain позволяет хранить в защищенном распределенном реестре как результаты транзакций, так и «цифровые отпечатки» электронных документов. При этом хранение в распределенном реестре обеспечивает **достоверность всех результатов транзакций, неизменность, актуальность, регистрацию изменений/записей в реестр – кем и когда произведена.** Результат транзакций и выгрузка текущего состояния любого процесса/системы осуществляется любыми сторонними приложениями через смарт-контракты, сущность которых также не может быть изменена.

## Пример использования

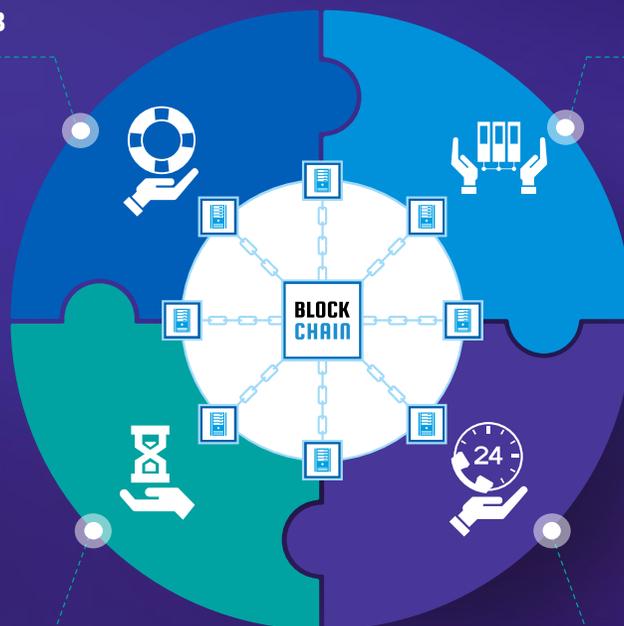
**Алроса** – отслеживание торгового пути алмазов для повышения прозрачности в цепи поставок

## Поддержка квалификации контрагентов

В распределенном реестре хранится актуальная информация о квалификации контрагентов и «цифровые отпечатки», ссылки на документы. Данные по результатам квалификации вносятся через смарт-контракты и поддерживается общая база контрагентов. Данные могут обновляться самими контрагентами.

В распределенном реестре хранится информация по статусу исполнения договорных обязательств компании или контрагентов, выявленных нарушений, при этом данные в реестр вносятся и заверяются как службами компании, так и самими контрагентами.

## Контроль статуса исполнения договоров



## Мониторинг корпоративной карты рисков Защита критичных данных

Блокчейн позволяет отражать текущий статус корпоративных рисков – данные по рискам и их текущим оценкам через смарт-контракты заносятся в реестр, также при возникновении инцидентов любого рода смарт-контрактами инициируется пересмотр текущего уровня рисков, формируются требования по их актуализации, статус в блокчейне обновляется по результатам выполнения мер реагирования.

В распределенном реестре может отражаться текущий статус проведения служебных расследований и расследований, «цифровые отпечатки» документов, результаты заключений. При этом в блокчейн информация может поступать из различных систем.

## Мониторинг статуса служебных расследований

# Большие данные и бизнес-аналитика (Big Data, DA&BI)

## Решаемая проблематика:

Развитие инструментов и методов Big Data&Data Analytics в части накопления и обработки структурированных и неструктурированных данных больших объемов позволяет в требуемые сроки получать новые аналитические результаты и выводы, выявлять корреляции и зависимости, отклонения и аномалии в условиях непрерывного прироста и трансформации данных. Развитие инструментов Business Intelligence позволяет быстро и **гибко управлять аналитикой данных, строить аналитические модели, управлять рисками компаний** в условиях постоянных изменений, что особенно актуально для **функции безопасности – необходимости постоянного реагирования на меняющиеся угрозы.**

## Пример использования

**НЛМК** – кластер централизованного накопления данных с датчиков и систем управления производством, интеллектуальный анализ

**Алроса** – прогнозная аналитика и контроль обогатительных процессов на базе Big Data

## Проверка юридических и физических лиц

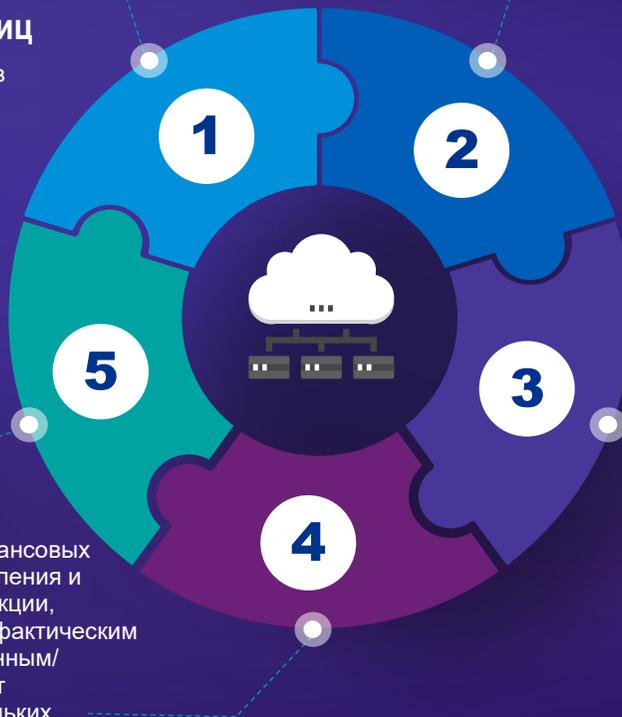
Автоматизация, ускорение и больший охват субъектов процедур проверки юридических и физических лиц по всем доступным источникам, включая негосударственные БД, СМИ, социальные сети, автоматизация поиска аффилированности и связей между юрлицами и/или физлицами, анализ расходов физлиц на соответствие официальным доходам.

## Аналитический монитор СБ

Решения BI позволяют создать легко настраиваемый и адаптируемый инструмент постоянного мониторинга основных KPI и KRI на основе данных из различных источников в виде набора аналитических динамических табло и отчетов, возможен доступ в режиме онлайн.

## Выявление рискованных транзакций

Автоматизация процедур проверки транзакций – финансовых расчетов и начислений за продукцию и услуги, поступления и списания в производство материалов, поставки продукции, оказания услуг - на соответствие условий договоров, фактическим производственным показателям, соответствие медианным/допустимым отклонениям и пр. Инструменты позволяют автоматизировать выборку и анализ данных из нескольких источников, показать расхождения с «паттернами».



## Таргетирование рискованных контрагентов и сотрудников

Анализ взаимодействия с контрагентами в процессах закупки товаров и услуг и реализации продукции на основе «паттернов», профилей контрагентов/сотрудников – анализ процедур и условий договоров, стоимости и сроков закупок/реализации продукции – сквозной анализ всех данных по процессу, в т.ч выявление отклонений от нормализованных «паттернов» – идентификация контрагентов и сотрудников с высоким уровнем риска.

## Анализ Life Style

Методы Big Data позволяют анализировать Life Style – поездки, покупки, наличие машин и недвижимости, социальные связи, помогая тем самым выявлять признаки потенциальных нарушений корпоративных политик и признаки коррупции и мошенничества.

# Машинное обучение и искусственный интеллект (AI)

## Решаемая проблематика:

Технологии машинного обучения позволяют проводить анализ потока данных на предмет построения типовых моделей и определения корреляций и зависимостей, выявления аномалий и отклонений и принятия решений на их основе. Для задач СБ большой интерес представляет возможность систем машинного обучения **анализировать транзакции на предмет нарушения финансовой дисциплины, анализировать журналы регистрации и события информационных систем.**

## Пример использования

**Северсталь** – оптимизация производственного процесса на ЧерМК, контроль за производительностью

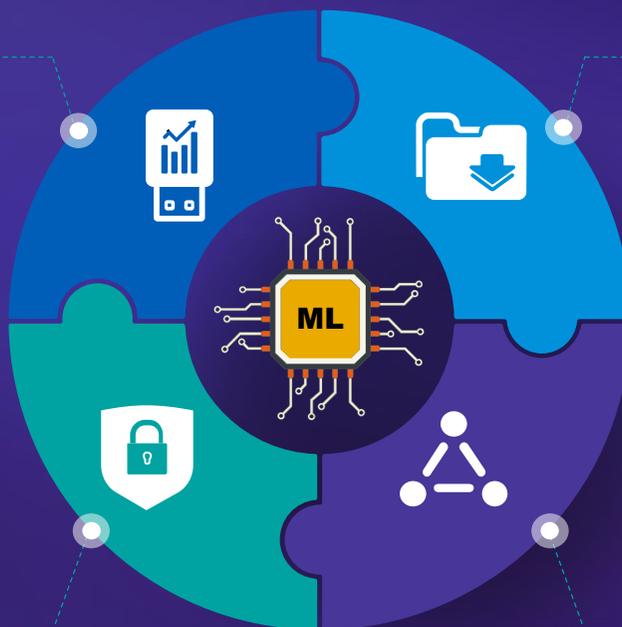
**НЛМК** – контроль за расходом ферросплавов при выплавке стали на основе AI

## Развитие систем антифрода

Алгоритмизация поиска признаков мошенничества и нарушений в процессах закупок товаров и услуг, капитального строительства и ремонтов объектов, реализации продукции, расчетов с персоналом на основе рассчитываемых статистических метрик, экспертных критериев и правил, выявление новых аномалий и схем фрода.

Формирование стандартной модели работы пользователей, приложений, коммуникации с сайтами и ресурсами – поведенческой аналитики, выявление отклонений от нормального поведения пользователей или приложений - в т.ч. Разбор сообщений и логов систем ИБ и SIEM.

## Противодействие кибератакам



## Анализ сообщений Горячей линии (ГЛ)

Автоматизации работы собственно ГЛ (внедрение чат-ботов), автоматизация оператора ГЛ - анализ и разбор сообщений ГЛ – классификация, предварительная оценка и маршрутизация сообщений ГЛ в соответствующие подразделения компании.

Формирование типовых моделей информационного обмена пользователей – поведенческой аналитики, анализ и разбор логов и сообщений систем обнаружения утечки данных – сопоставление с поведенческой моделью и экспертными критериями – верификация признаков утечки данных.

## Анализ угроз утечки данных

# Распознавание видео, фото, речи

## Решаемая проблематика:

Технологии машинного обучения дополнительно позволяют расширить сферы применения технологий распознавания и выделения значимой информации из текста, речи, фото и видеоизображений. Данные технологии позволяют упростить, **ускорить и расширить процедуры обеспечения физической защиты объектов, расширить возможности систем антифрода, систем обнаружения утечки конфиденциальной информации** за счет вовлечения дополнительных данных для анализа.

## Пример использования

**НЛМК** – внедрение машинного зрения на Стойленском ГОКе (безопасность перевозки сырья и объем загрузки автосамосвалов)

**Северсталь** – биометрическая СКУД для московского представительства компании

## Распознавание лиц

Технологии распознавания лиц позволяют автоматизировать процессы физического контроля доступа – распознавание лиц при проходе через КПП, контроль нахождения лиц на территории объектов – в специальных зонах. В части проверки контрагентов или физлиц технология распознавания лиц позволит дополнительно расширить данные для анализа аффилированности или анализа расходов за счет распознавания лиц в Интернет.

Распознавание и интеллектуальный анализ изображений позволяют автоматизировать целый ряд проверок – состояния защищенности объектов, наличие и состояние активов/оборудования/ресурсов, выявление хищений, распознавание текстов договоров. Это позволяет дополнять аналитику антифрода и систем обнаружения утечек конфиденциальной информации.

## Распознавание изображений



## Распознавание голоса

Технологии распознавания голоса и перевода голосовой информации в текст позволяют автоматизировать анализ голосовых сообщений на ГЛ с последующим их разбором и анализом, автоматизировать общение через чат-боты (голосовые роботы), автоматизировать процедуры записи и распознавания речи – записей телефонных переговоров с целью дальнейшего анализа и выявления признаков мошенничества (например, трейдеров, закупщиков), разглашения конфиденциальной информации и прочих нарушений.

Распознавание видео позволяет существенно расширить область и возможности мониторинга – контроль прохода/нахождения и анализ действий сотрудников – факт и корректность выполнения операций, выявление опасных операций и нарушений, контроль состояния сотрудников, соблюдения ими правил безопасности на объектах.

## Распознавание видео

# Интернет вещей (IoT)

## Решаемая проблематика:

**Сбор данных с оборудования и контроль его состояния, мониторинг параметров производственных операций** и контроль качества продукции в реальном времени, интеллектуальное потребление ресурсов – энергии, воды, контроль перемещения и состояния работников, транспортных средств, движения МТР - как ресурсов, так и товарной продукции - решение этих задач обеспечивается технологиями Интернета вещей.

## Пример использования

**Северсталь** – исключение несанкционированных подключений к энергосетям и кражи электричества

**ММК** – контроль транспортировки, погрузки и складирования железорудного сырья

## Мониторинг перемещения и состояния сотрудников и транспорта

Рабочая одежда сотрудников (комбинезон, каска) и транспортные средства снабжаются датчиками (GPS-датчиками, RFID-метками), позволяющими отслеживать перемещение (в т.ч. и отсутствие движения) людей и ТС по территории объектов, выявлять несанкционированные проникновения и проезды, остановки, несчастные случаи и ДТП.

Вся технологическая цепочка – от приемки сырья до отгрузки товарной продукции снабжается датчиками, позволяющими осуществлять мониторинг приемки партии сырья с определенными характеристиками, передачи в производство, маркировки новыми датчиками товарной продукции, контроль ее перемещения, погрузки и вывоза с территории объектов.

## Мониторинг движения МТР и продукции



## Интеллектуальный контроль оборудования

Оснащение оборудования датчиками и системами диагностики, позволяющими определить его рабочие параметры и провести диагностику состояния для повышения контроля за ремонтами оборудования.

Сигналы о нарушениях в режиме реального времени направляются на мобильный смартфон инспектора охраны, который обеспечивает своевременное реагирование на возникшие угрозы. Мобильное приложение информирует об угрозе, контексте угрозы и необходимых действиях. Инспектор отчитывается по выполненным действиям с приложением фото и видеоматериалов, снятых на мобильный.

## Мобильный инспектор охраны

# Беспилотные летательные аппараты (БПЛА)

## Решаемая проблематика:

**Обеспечение контроля за физическими объектами** – территорией, производственными объектами, оборудованием, ведущимися работами, особенно, удаленными, территориально распределенными, имеющими значительную протяженность, габариты или физические объемы требует привлечения значительных ресурсов. Использование БПЛА позволяет как обеспечить постоянный мониторинг таких объектов, так и анализ состояния объектов, объемов выполненных работ, контроль строительства объектов.

## Пример использования

**Полюс** – отслеживание неподвижности стенок бортов карьера, 3D картирование местности

**Норильский Никель** – БПЛА для охраны объектов инфраструктуры, исследование горных выработок

## Мониторинг строительных работ, разработки карьеров с БЛА

Решения на базе БЛА позволяют осуществлять оперативную систематическую съемку строящихся объектов, либо ведущейся разработки карьеров или насыпных объектов. Оцифровка и обсчет результатов съемки позволяет осуществлять контроль объемов работ и их соответствия представленным актам, контроль хода строительства – соблюдение сроков строительства, привлечение техники подрядчиков согласно договорам и сметам и пр.

Решения на базе БЛА позволяют осуществлять регулярную съемку территорий с автоматическим обнаружением и выделением типов оборудования, например, локомотивов, самосвалов и иной техники и контроля ее состояния и/или фактического наличия либо оперативного оповещения об ее отсутствии.

## Мониторинг состояния и сохранности техники и оборудования



## Мониторинг состояния технологических объектов и территорий

Кроме техники, решения на базе БЛА позволяют осуществлять мониторинг и контроль состояния территорий, технологических объектов – зданий и конструкций, ЛЭП, трубопроводов, ограждений.

При возникновении происшествий, требующих вовлечения СБ, с использованием дронов может быть организовано оперативное наблюдение за объектами, в т.ч. отслеживание перемещений людей и транспорта.

## Организация оперативного наблюдения за ситуациями

# Роботизация процессов (RPA)

## Решаемая проблематика:

Для роботизации выбираются трудоемкие, повторяющиеся и систематичные бизнес-процессы, где принятие решения либо отсутствует, либо основано на формализуемых критериях, создается «робот» для автоматизации управления этими процессами. Одним из ключевых преимуществ программных роботов является исключение «человеческого фактора» при принятии решений.

## Пример использования

**Норильский Никель** – робот проверяет заявки и документы для аккредитации поставщиков (в SAP SLC)

**НЛМК** – формирование статистических отчетов, обработка банковских выписок

## Роботизация транзакционных проверок

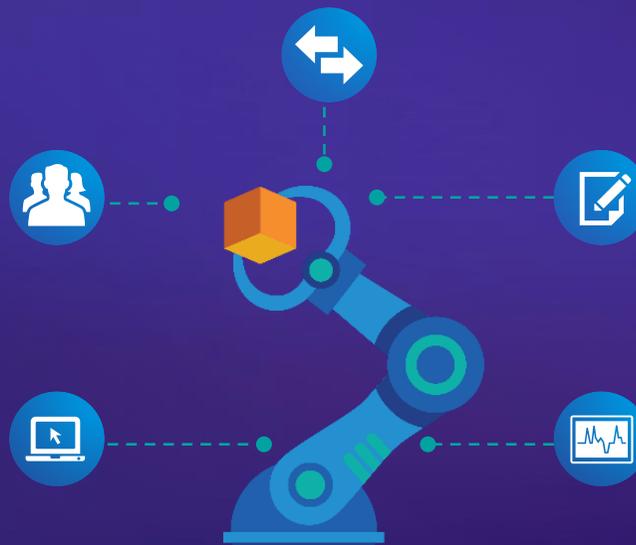
Поиск и консолидация данных, рутинные проверки и сверки данных из различных источников, выполняемые в рамках контроля СБ могут быть выполнены автоматически.

## Роботизация проверки ФЛ и ЮЛ

Роботизация позволяет в автоматическом режиме проводить проверки по формальным критериям соответствия тем или иным требованиям, комплектности документов, с заполнением соответствующих шаблонов и документированием результатов проверки в системах.

## Роботизация назначения прав доступа пользователей

Роботизировать можно присвоение прав доступа пользователей: робот обеспечит автоматизацию получения всех авторизаций, анализ требований прав доступа на соответствие критериям и присвоит соответствующие права доступа.



## Распознавание документов

В ходе проведения проверок контрагентов, проведения расследований роботы могут автоматизировать распознавание сканов документов, предварительные проверки корректности данных и формирование электронных документов из сканов или ввод данных в системы.

## Подготовка отчетности

Автоматизация сбора, консолидации, анализа и обработки отчетности от подразделений и региональных служб, формирование сводной отчетности по блоку.