ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

ГАРДА АНАЛИТИКА

ПЛАТФОРМА ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

ГАРДА АНАЛИТИКА
ГАРДА ТЕХНОЛОГИИ

ПРИНЦИП РАБОТЫ

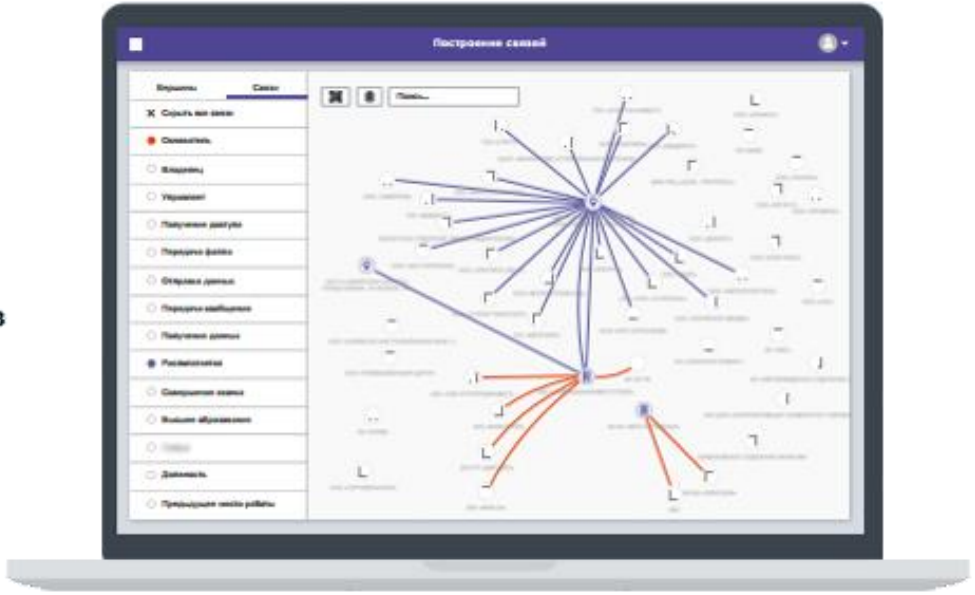
ОТ ИНЦИДЕНТОВ К ПОДРОБНОЙ ИНФОРМАЦИИ

Выявление рисков

Проведение расследований

Автоматизация процессов выявления инцидентов

Формирование библиотеки инцидентов



Динамическое обогащение данных
из десятков источников

Выявление отклонений
в поведении людей или устройств

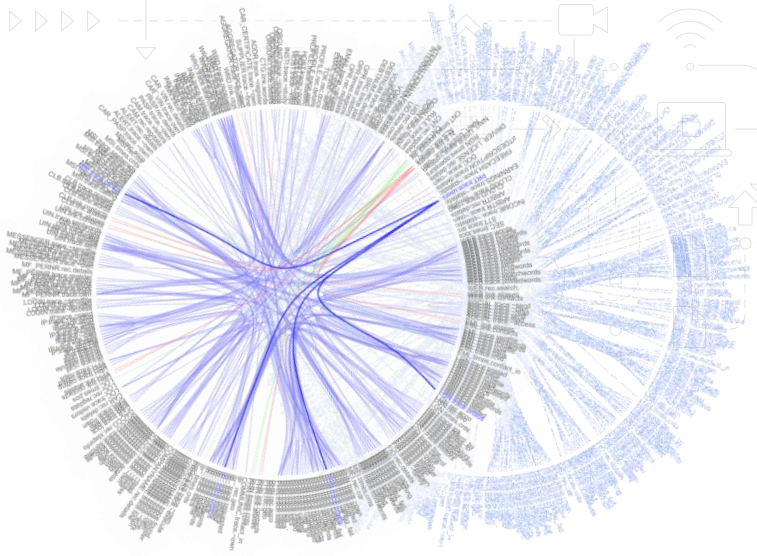
Объединение различных технологий анализа
данных в одном инструменте

Построение явных и скрытых связей
между объектами реального мира

ГАРДА АНАЛИТИКА ГАРДА ТЕХНОЛОГИИ

ГАРДА АНАЛИТИКА

ИНФОРМАЦИОННОЕ ЯДРО БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ



- Поиск последовательности событий среди огромного количества данных, поступающих из различных внутренних и внешних источников
  - Выявление фактов нарушения бизнес-процессов
  - Контроль целостности и защиты критичных данных в информационных системах
  - Выявление мошенничества при производстве и сбыте
- Выявление и построение связей между объектами реального мира
  - Оперативная оценка клиента, сотрудника, контрагента, создание постоянно обновляемой информационной базы/досье
  - Контроль закупочной деятельности (Выявление фактов аффилированности и сговоров)
  - Выявление попыток несанкционированного доступа к данным, в том числе с использованием техник обхода стандартных систем защиты
- Обнаружение угроз безопасности на основе поведенческого анализа с помощью методов машинного обучения
  - Обнаружение атак, заражений и теневых информационных технологий в сети
  - Выявление аномального поведения сотрудника перед увольнением
  - Выявление недобросовестного соблюдения всех процедур при заключении договоров

ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

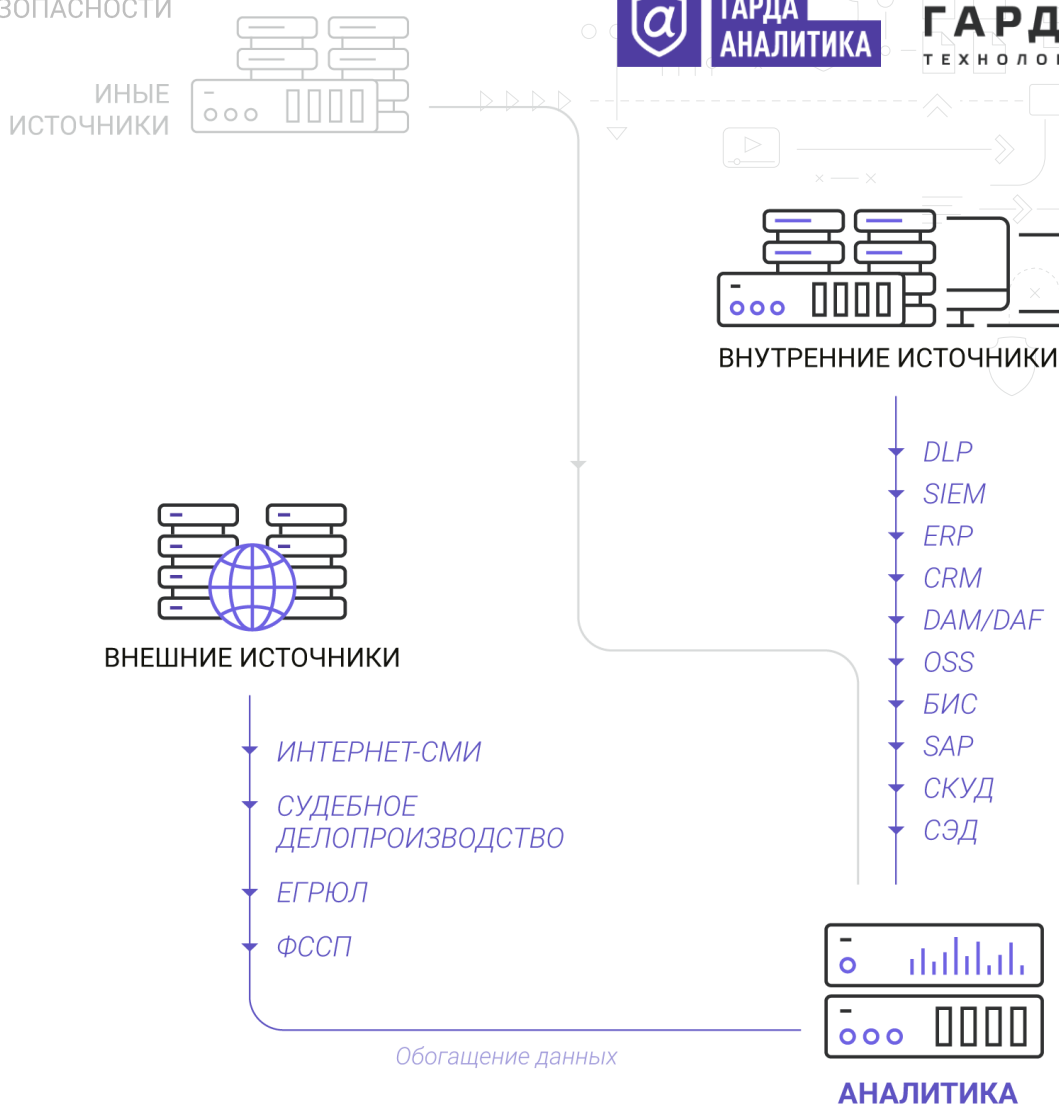
ИСТОЧНИКИ ДАННЫХ

ВНУТРЕННИЕ И ВНЕШНИЕ

«Гарда Аналитика»:

- Интегрируется с бизнес-процессами предприятия, приложениями и информационными системами
- Связывает события, полученные из различных систем и бизнес-приложений
- Использует внешние информационные системы для обогащения данных
- Использует пассивное местоположение сотрудников

Система открыта для подключения дополнительных информационных систем и бизнес-приложений



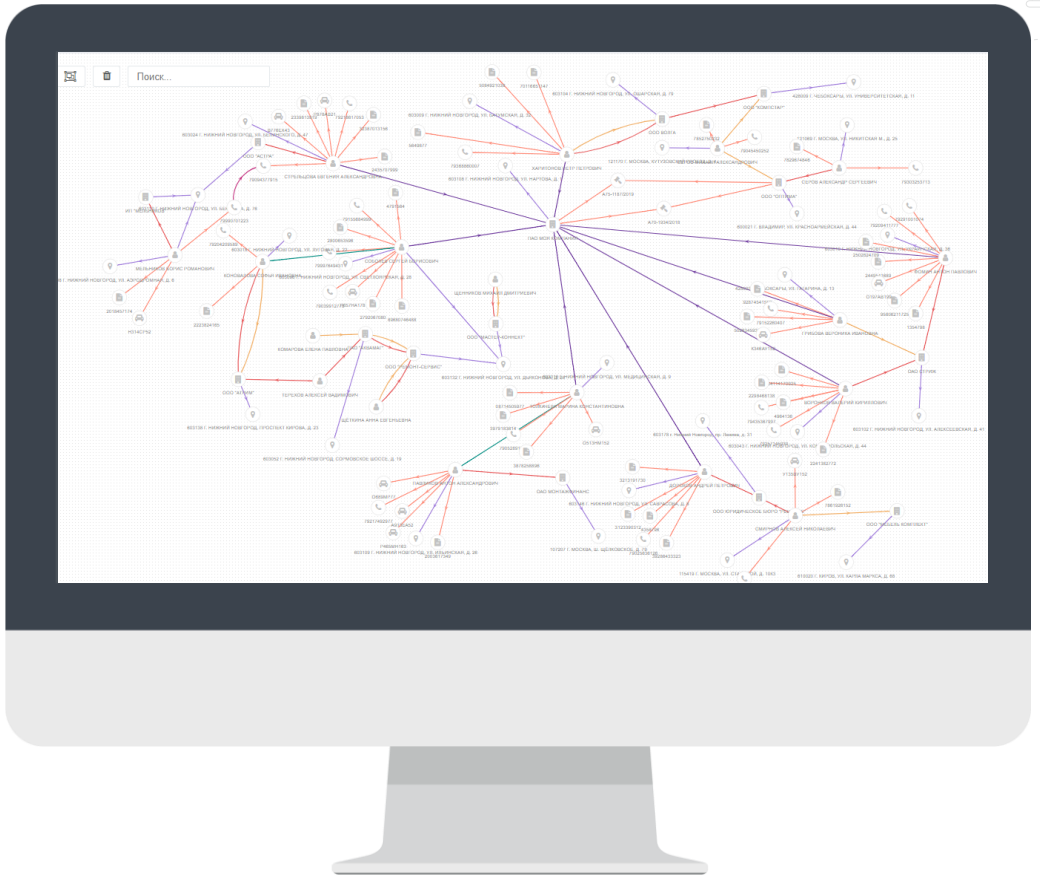
ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

ГАРДА АНАЛИТИКА

НАХОДИТ СВЯЗИ ЧЕРЕЗ 7 ОБЪЕКТОВ

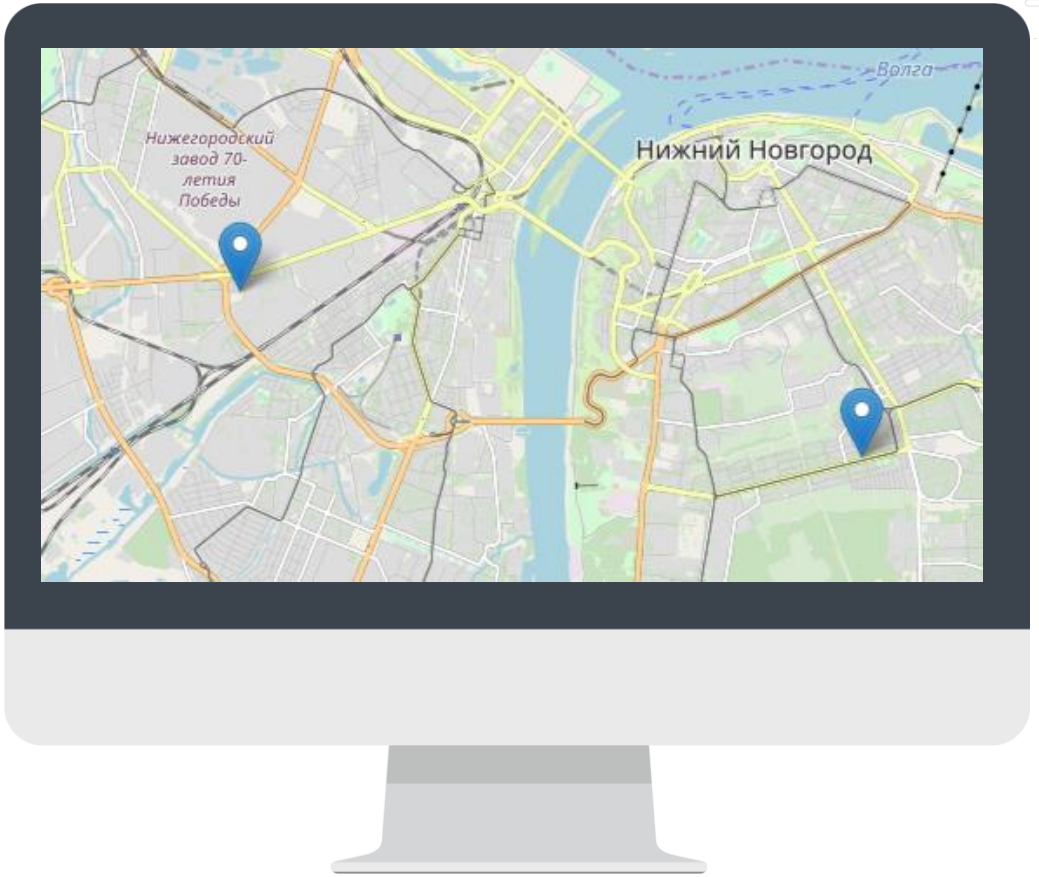
- ☑ Арбитражные, исполнительные дела
- ☑ Факты любых коммуникаций
- ☑ Адреса присутствия и координаты



ГАРДА АНАЛИТИКА ГАРДА ТЕХНОЛОГИИ

ДАННЫЕ О МЕСТОПОЛОЖЕНИИ

- ☑ Выявление аффилированности контрагента
- ☑ Определение благонадежности контрагента
- ☑ Выявление аффилированности сотрудника
- ☑ Определение благонадежности кандидата
- ☑ Выявление фактов дискредитации вне компании
- ☑ Пассивное местоположение
  - Маршруты передвижения
  - Места присутствия в заданные дату и время
  - Определение совместного местонахождения
  - Определение совместного передвижения
- ☑ Автоматизация проверки:
  - Появление новых связей
  - Появление новых дискредитирующих фактов
  - Изменение внешних статусов



ГАРДА АНАЛИТИКА ГАРДА ТЕХНОЛОГИИ

СФЕРЫ ПРИМЕНЕНИЯ ПЛАТФОРМЫ

- Финансовая организация
  - Внутренний Фрод (Сотрудники)
  - ПОД/ФТ, AML, теневые операции
  - Мошенничества в ДБО, мобильном банке
- Страховая компания
  - Оформление страховых полисов по недостоверным данным
  - Урегулирование убытков по сфальсифицированным страховым случаям
  - Недобросовестные внешние эксперты (Оценщики, судебные и т.п.)
- Промышленность
  - Распространение конструкторской документации, производственных секретов
  - Нарушения производственных и бизнес-процессов
  - Мошенничество при сбыте
- ТЭК
  - Мошенничества с присоединением потребителей и оплатой
  - Мониторинг безопасности процессов генерации (добычи), транспортировки, передачи
- Ритейл
  - Махинации с поставками
  - Мошенничества в интернет-магазине
  - Нарушения в процессах функционирования складов, торгового зала, кассовых узлов
- Транспорт и логистика
  - Безопасность перевозок
  - Мошенничества с оплатой проезда, провоза
  - Мониторинг состояния, местоположения, доступности объектов
- Государственные системы
  - Злоупотребления при оказании государственных услуг
  - Поддержка безопасности процессов государственного управления
  - Поддержка процессов обеспечения правопорядка

ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

ВНЕДРЕНИЕ И СЕРВИС

ПРЕДПРОЕКТНОЕ ОБСЛЕДОВАНИЕ

- Анализ бизнес-процессов и угроз безопасности
- Определение источников данных

ВНЕДРЕНИЕ

- Инсталляция
- Подключение источников данных
- Настройка платформы в соответствии с библиотекой сценариев

ФОРМИРОВАНИЕ БИБЛИОТЕКИ СЦЕНАРИЕВ

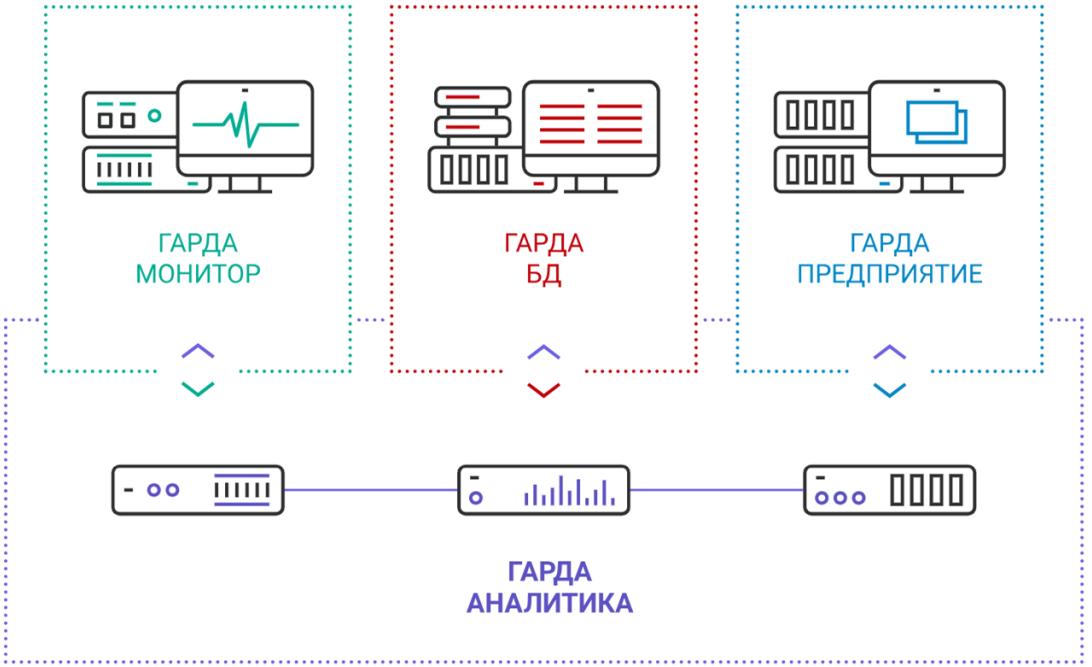
- Описание сценариев безопасности
- Создание базы сценариев

ЭКСПЕРТНОЕ СОПРОВОЖДЕНИЕ

- Аудит бизнес-процессов на предмет появления новых рисков
- Обновление базы инцидентов
- Обмен "Best Practices"

ГАРДА АНАЛИТИКА
ГАРДА ТЕХНОЛОГИИ

ЭКОСИСТЕМА БЕЗОПАСНОСТИ



ГАРДА АНАЛИТИКА СОВМЕСТИМА
С РЕШЕНИЯМИ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ ЛИНЕЙКИ ГАРДА

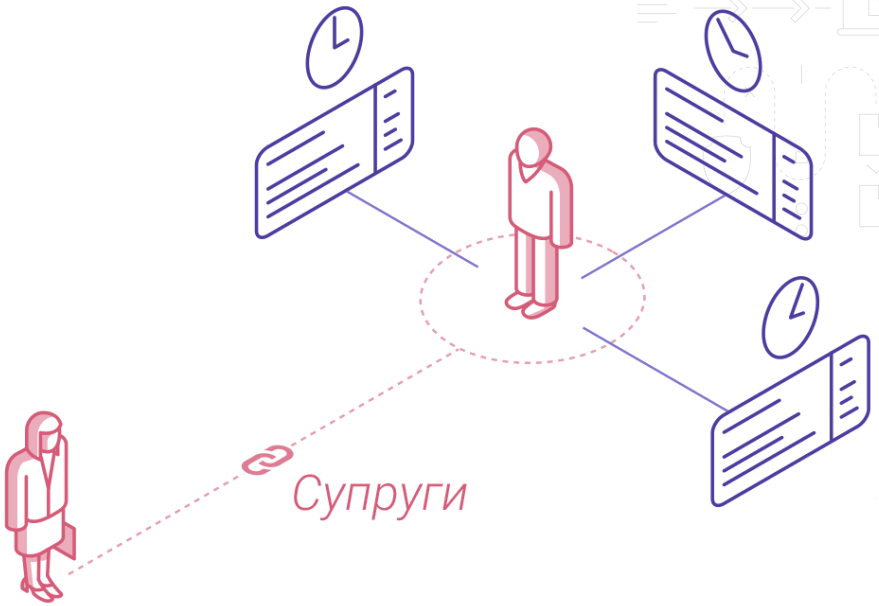
- ☑ Позволяет оперативно создавать всесторонний комплекс защиты организации от угроз информационной и экономической безопасности
- ☑ Минимизирует затраты на внедрение систем безопасности

ГАРДА АНАЛИТИКА ГАРДА ТЕХНОЛОГИИ

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

- **Проверка благонадежности ФЛ**
  - Сотрудников или кандидатов при трудоустройстве,
  - Составление досье, поиск связей
- **Проверка благонадежности ЮЛ**
  Контрагентов, составление досье, поиск связей
- Мониторинг закупочных процедур
- **Выявление накруток KPI менеджерами**
  - Теневые или многоразовые продажи, фиктивные документы
  - Изменений условий договоров, навязанные услуги
- Финансовые мошенничества со стороны сотрудников
  (Нелегитимные калькуляции, проводки, занижение стоимости)
- Выявление мошеннических действий и операций со стороны клиентов

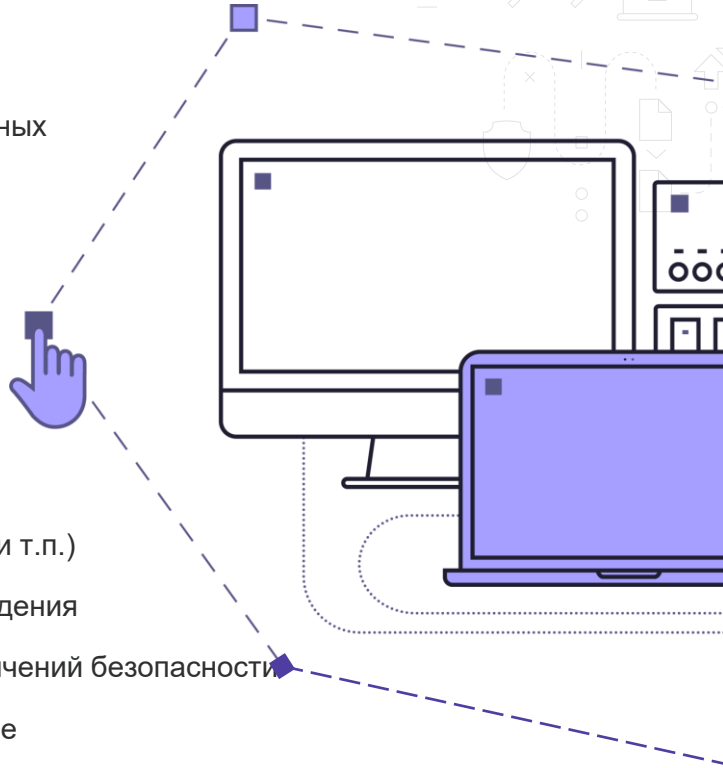


ГАРДА АНАЛИТИКА ГАРДА ТЕХНОЛОГИИ

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

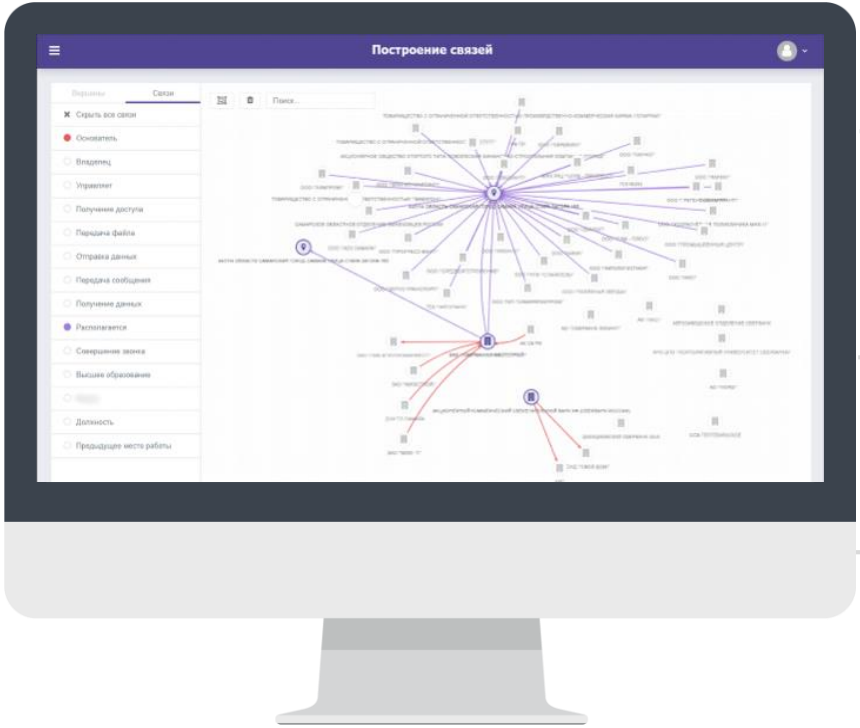
- Выявление хищений и несанкционированного распространения персональных данных
- Выявление распространения коммерческой тайны
  (Критичные данные для бизнес-процессов, базы данных клиентов,
  ноу-хау и т.п.)
- **Внешние атаки ||** Прямое хищение денежных средств компании
- **Внешние атаки ||** Прямое хищение денежных средств клиентов компании
- **Внешние атаки ||** Мошенничества через личные кабинеты клиентов
- Контроль работы сотрудников с критически важной информацией
  (Например, с данными VIP-персон, с ключевой интеллектуальной собственностью и т.п.)
- Мониторинг активности и связей пользователей, выявление подозрительного поведения
- Выявление нецелевого использования ИТ-ресурсов, обхода установленных ограничений безопасности
- Выявление сетевых атак, вредоносной активности в корпоративной инфраструктуре



ГАРДА АНАЛИТИКА ГАРДА ТЕХНОЛОГИИ

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ



Проверка благонадежности физических и юридических лиц

ОБЪЕКТЫ ЗАЩИТЫ

- Сотрудники Компании
- Материальные ценности

ИСТОЧНИКИ

- Внешние источники
- ERP
- Собственные Скоринг-базы

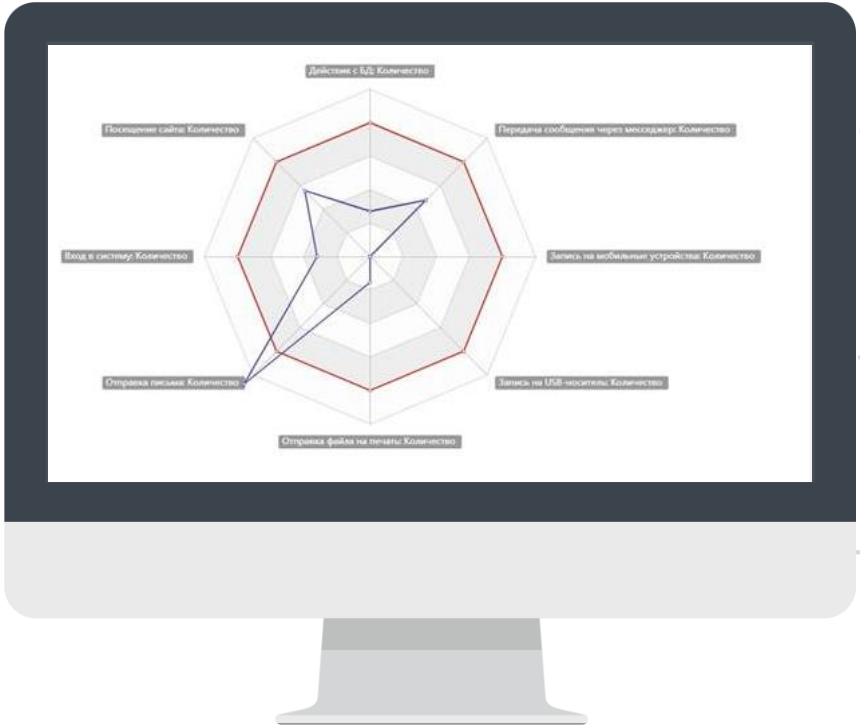
ИНДИКАТОРЫ

- Исполнительных делопроизводства
- Арбитражные процессы
- Банкротство
- Кредитные риски
- Присутствия в недобросовестных реестрах
- Смена руководителей или собственников
- Мониторинг финансовых показателей

ГАРДА АНАЛИТИКА ГАРДА ТЕХНОЛОГИИ

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ



Контроль и выявление нарушений при оформлении банковских договоров и продаже финансовых услуг

ОБЪЕКТЫ ЗАЩИТЫ

- Финансовые средства
- Сведения и банковские операции со счетами
- Информация по кредитным картам

ИСТОЧНИКИ

- CRM
- ERP, АБС
- Service Desk
- Личный кабинет/ДБО

ИНДИКАТОРЫ

- Фиктивные продажи «своим», двойные продажи, оформление на «левых» людей
- Нарушение процедуры при оформлении договоров
- Фиктивные регистрации обращений клиентов, расторжений договоров и т.п.

ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

СИТУАЦИЯ

В одном из крупных российских промышленных предприятий при анализе карты связей сотрудников служба безопасности заметила нетипичную коммуникацию между менеджером отдела по продажам и руководителем ОТК.
Его внимание привлекла длительная переписка по внутренней почте.

РЕШЕНИЕ

Просмотр нескольких писем подтвердил подозрения об мошеннических действиях. Оказалось, что руководитель ОТК умышленно завышал процент брака продукции, а менеджер по продажам в свою очередь предлагал купить данный товар клиентам по заниженной цене с некоторой выгодой для себя. Обсуждение данных вопросов велось прямо на работе, но чтобы не вызывать подозрений сотрудники использовали рабочую тему письма «Закупки для производства».

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

Выявление сговоров сотрудников, с целью осуществления каких-либо противоправных действий или других аффилированностей

ОБЪЕКТЫ ЗАЩИТЫ

- Материальные ценности
- Конфиденциальная и критичная информация, к которой сотрудники имеют доступ

ИСТОЧНИКИ

- DLP
- DAM
- ERP

ИНДИКАТОРЫ

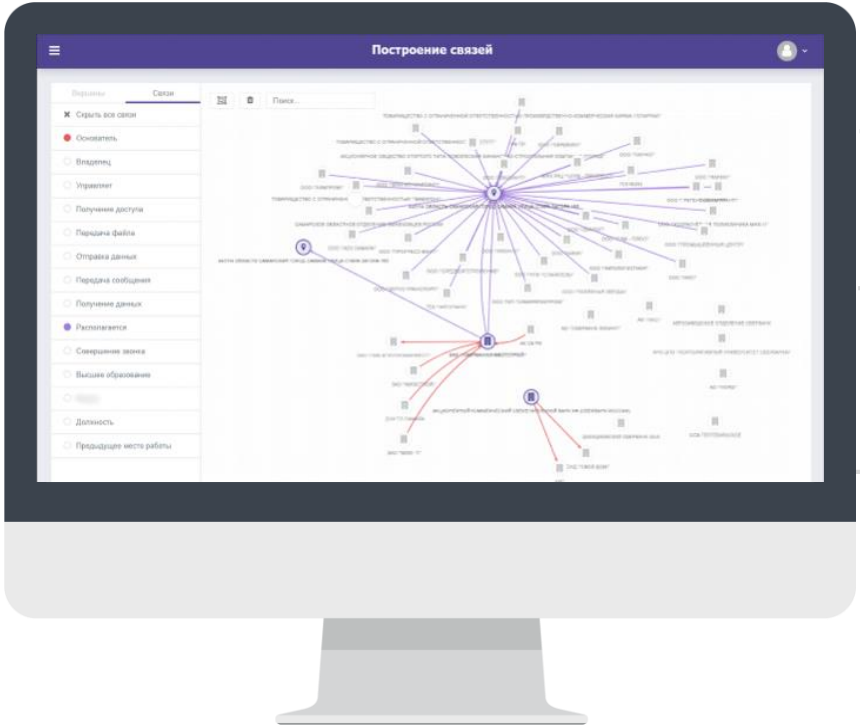
- Факты коммуникаций сотрудников внутри компании или третьими лицами за пределами компании, в том числе с конкурентами

ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ



Выявление мошенничеств при пользовании банковскими картами

ОБЪЕКТЫ ЗАЩИТЫ

- Финансовые средства
- Сведения и банковские операции со счетами
- Информация по кредитным картам

ИСТОЧНИКИ

- Личный Кабинет/ДБО
- AML (ПОД/ФТ)
- FMS

ИНДИКАТОРЫ

- Аномальная транзакционная и сессионная активность ДБО
- Связи участников платежа из «реального мира»
- Платёж на новые реквизиты, «из черного списка» или с нетипичного устройства
- Нехарактерные для клиента операции
- Быстрое выполнения операций из географических мест, имеющих удаление

ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

СИТУАЦИЯ

«Гарда Аналитика» определила, что сотрудник регулярно посещает сайты ставок и букмекерских контор, в следствии чего он был отнесён к группе риска «Сотрудники, склонные к азартным играм», о чём была поставлена в известность служба безопасности

РЕШЕНИЕ

Сотрудники службы экономической безопасности получили оповещение о данном факте и создали дополнительные правила контроля действий данного сотрудника, в том числе в имеющейся ERP системе.

В скором времени были выявлены (В дополнение к нецелевому использованию служебного ПК) нарушения в складском учёте с его стороны, а это уже прямые убытки.

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выявление групп рисков сотрудников

ОБЪЕКТЫ ЗАЩИТЫ

- Материальные ценности
- Конфиденциальная и критичная информация, к которой сотрудники имеют доступ

ИСТОЧНИКИ

- DLP
- ERP
- DAM
- IDS
- NTA/Network Forensics

ИНДИКАТОРЫ

Регулярное посещение сотрудниками определённых групп сайтов:

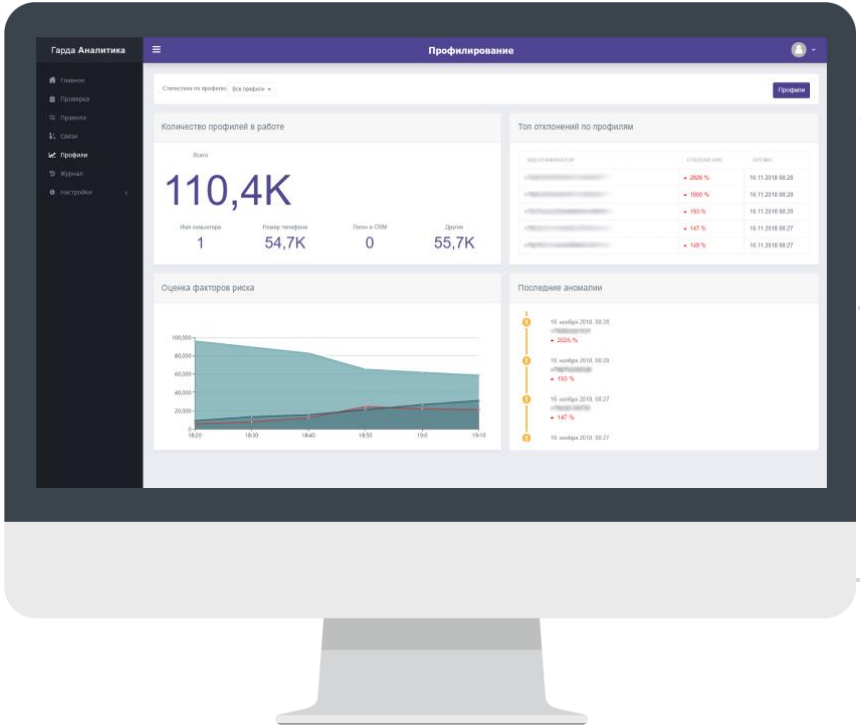
- Поиск работы
- Азартные игры и букмекерские конторы
- Сайты хакерской направленности

ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



Выявление мошенничеств при проведении платёжный операций

ОБЪЕКТЫ ЗАЩИТЫ

- Финансовые средства
- Сведения и банковские операции со счетами
- Информация по кредитным картам

ИСТОЧНИКИ

- Личный Кабинет/ДБО
- АБС, EPR
- AML (ПОД/ФТ)
- FMS
- Собственные скоринг-базы банка

ИНДИКАТОРЫ

- Подозрительного поведение пользователей на сайте банка, в ДБО
- «Лоббирование» менеджерами отдельных клиентов, ускорение операций
- Нетипичные способы онлайн-оплаты

ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

СИТУАЦИЯ

Сотрудник отдела разработок и проектирования решил сменить место работы, часто «зависая» на сайтах о работе, при этом на его ПК была замечена повышенная активность при работе с внешними устройствами.

РЕШЕНИЕ

Сотрудник регулярно посещает сайты по поиску работы - он был отнесён к группе риска «сотрудники, склонные к увольнению», с алертом в адрес СБ. Безопасники поставили сотрудника «на карандаш» с применением более строгих правил контроля в «Гарда Аналитика». В скором времени были выявлены выявили попытки несанкционированного копирования и распечатки документов, являющихся коммерческой тайной компании. Параллельно с этим был проведён ретроспективный анализ, в ходе которого были обнаружены факты копирования аналогичной информации.

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выявление несанкционированного распространения коммерческой тайны и иной конфиденциальной информации

ОБЪЕКТЫ ЗАЩИТЫ	• Документация по тендерной и закупочной деятельности • Ноу-хау и секреты производства • Патенты и сертификация • Отчётность и планы по развитию производства • Конструкторская документация и чертежи • Методики расчётов, технические условия, инструкции • Стандарты организации и нормы расходов
ИСТОЧНИКИ	• DLP • DAM • SIEM и другие СрЗИ
ИНДИКАТОРЫ	• Ключевые слова • Словари • Регулярные выражения • Сканы документов • Содержимое файлов • Неоднократные нарушения формальных процедур

ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

СИТУАЦИЯ

Новый сотрудник планово-экономического отдела проявлял аномальную активность в виде чрезмерного доступа к базам данных производственного учёта. Через две недели выяснилось, что данный сотрудник со своего IP адреса выполнял аутентификацию в базе данных под разными учетными записями своих коллег и выполнял работу практически за весь отдел.

РЕШЕНИЕ

Предварительно сотрудник службы безопасности создал политику контроля системных учетных записей, по которым удалось отследить IP и отслеживать время обращения к базам данных и производимые сотрудником действия, а также установить, что с IP других пользователей длительное время доступ к базам не совершался.

Благодаря отчетам по Гарде БД выяснилось, что столь частые обращения к базам данных совершались не в личных целях, а в виде работы за коллег, которые в это время занимались личными делами.

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выявление несанкционированного доступа к имеющимся базам данных как со стороны сотрудников, так и со стороны злоумышленников

ОБЪЕКТЫ ЗАЩИТЫ	• Экономическая деятельность предприятия • Патенты и сертификация • Бухгалтерская документация • Аналитические данные • Отчётность и планы по развитию производства • Проектная документация и чертежи • Стандарты организации и нормы расходов
ИСТОЧНИКИ	• IP Адрес:Порт • Логин БД/ОС • Таблицы, объекты, поля • Имена программ, функций, процедур • SQL операции • Объёмы запросов или ответов • Ключевые слова или регулярные выражения
ИНДИКАТОРЫ	• Использование чужих УЗ • Нелегитимное и нерегламентированное использование системных и привилегированных УЗ • Большое количество неуспешных авторизаций • Отклонение от текущего профиля и нестандартное поведение под имеющимися УЗ

ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

КАК ПРОВЕРЯЕТСЯ НОВЫЙ СОТРУДНИК

ОФИЦЕР ИБ

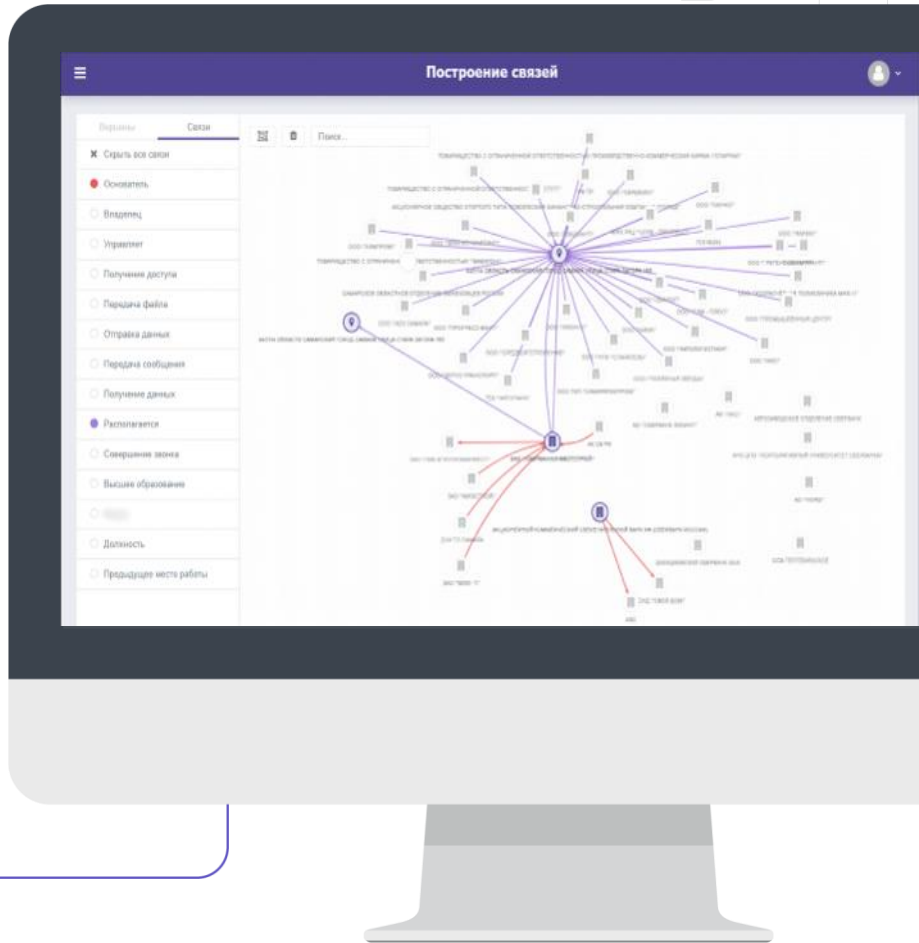
Время — минимум 1 день

Проверка по 15 источникам:
- Выявляет события
- Выявляет связи
- Анализирует информацию
- Принимает решение

ГАРДА АНАЛИТИКА

Время — менее 1 минуты

Все процессы поиска связей, построения схем, анализа — автоматизированы

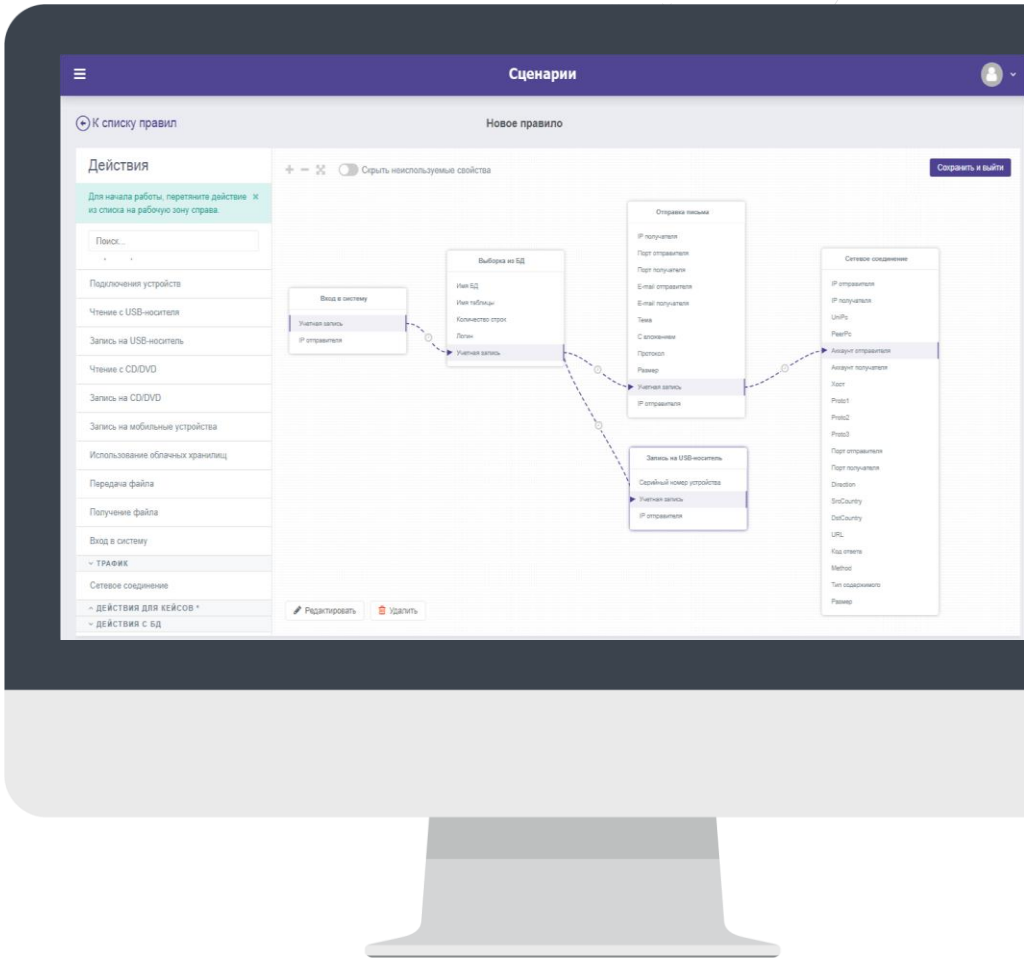


ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

СТАТИСТИЧЕСКИЕ МЕТОДЫ ДЛЯ ВЫЯВЛЕНИЯ НАРУШЕНИЙ ПРИ ПРОВЕДЕНИИ ЗАКУПОК?

- ☑ Выявление намеренного обхода бизнес-процессов при закупках
- ☑ Выявление закупочных цен
- ☑ Уведомление об изменении данных о контрагентах — смена руководителей, состав учредителей
- ☑ Мониторинг существующих и новых связей

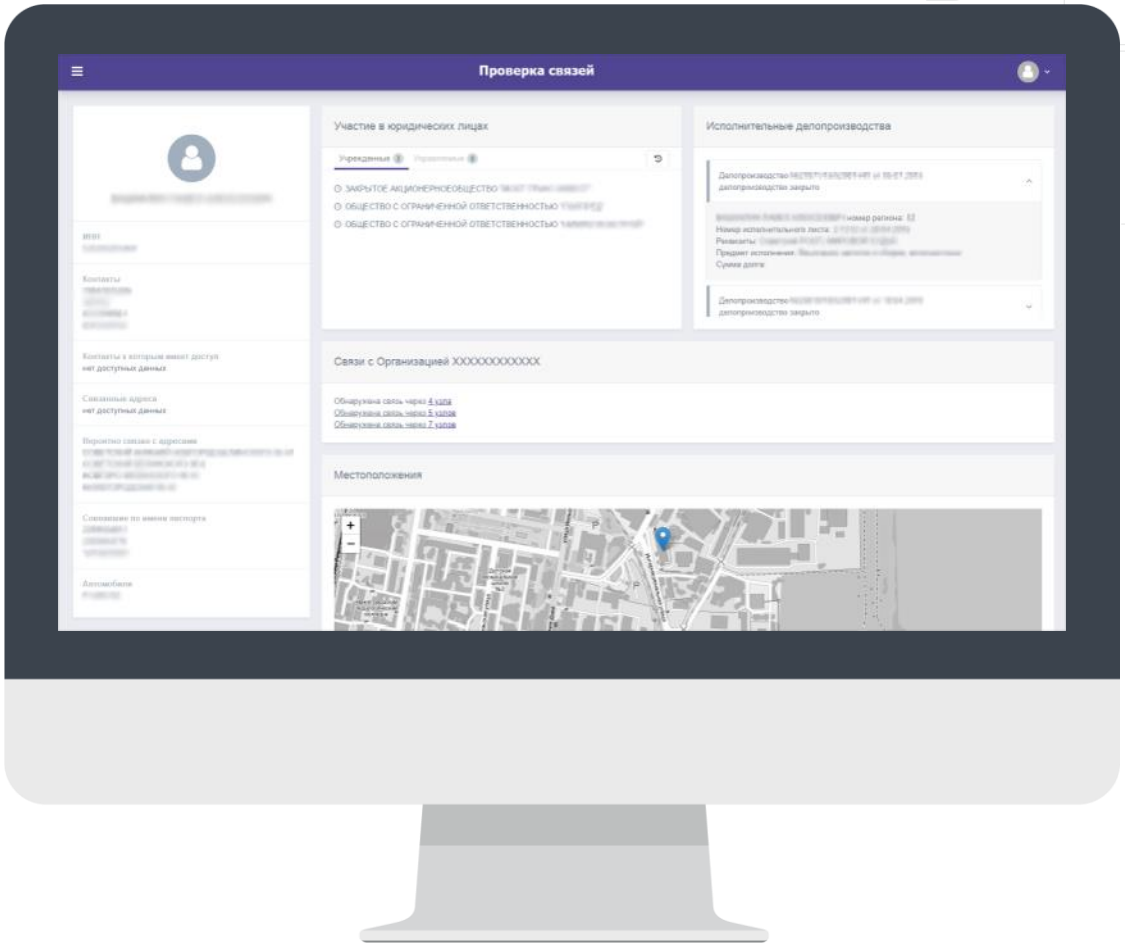


ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

ФОРМИРОВАНИЕ

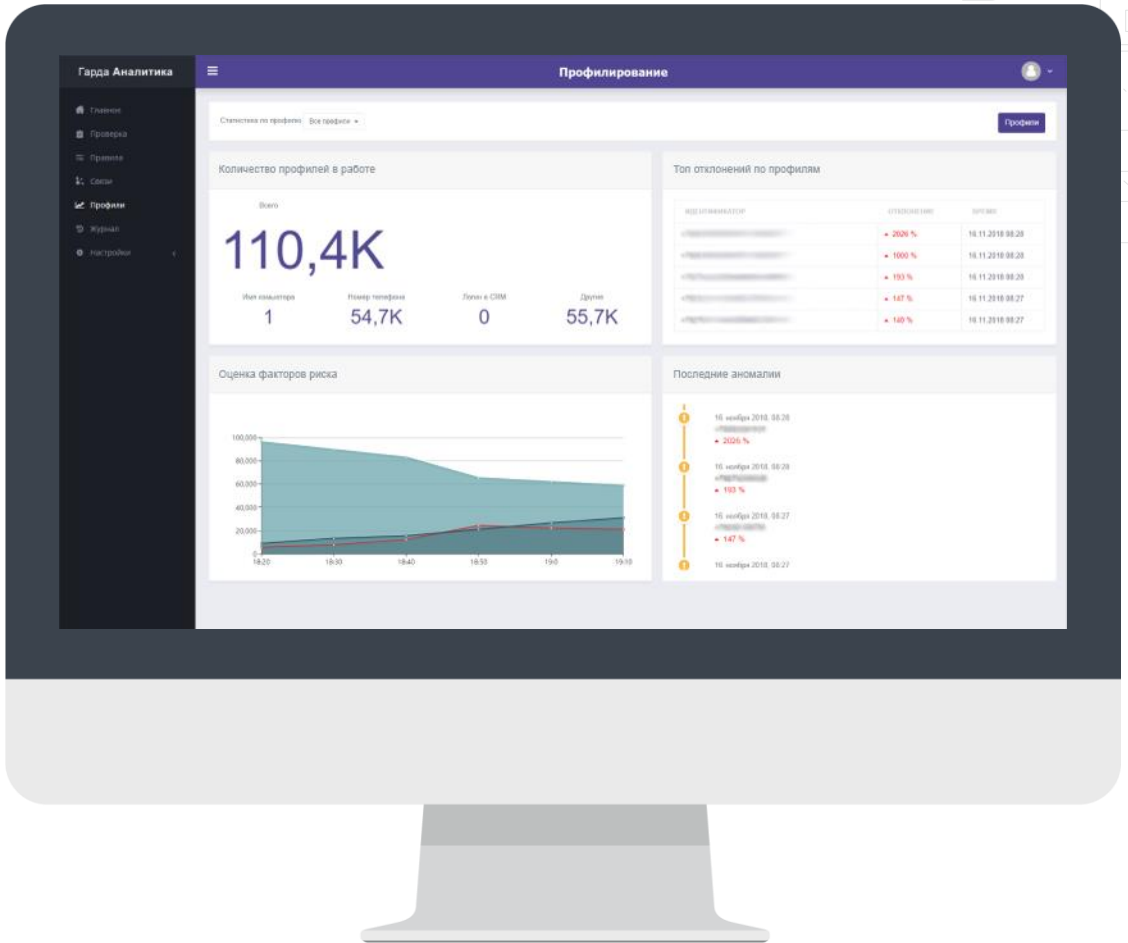
ДОСЬЕ СОТРУДНИКА



ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

ПОСТРОЕНИЕ
ПРОФИЛЕЙ
ВЫЯВЛЕНИЕ
АНОМАЛИЙ



СПАСИБО
ЗА ВНИМАНИЕ!

ГАРДА АНАЛИТИКА

ГАРДА ТЕХНОЛОГИИ

info@gardatech.ru
8 (831) 422 12 21
gardatech.ru