Инцидент до инцидента

Даниил Бориславский

Директор по продукту Staffcop, эксперт
по информационной безопасности Контур.Эгида

Контур staffcop

Who Am I:

Даниил Бориславский - директор по продукту Staffcop, амбассадор информационной безопасности.

Создал два подразделения в Staffcop; провёл более 500 пилотов; участвовал более чем в 50 конференциях как эксперт; как приглашенный специалист проводил учебные занятия в вузах.

8 лет работал в службе безопасности крупного холдинга; более 5 последних лет – в разработке средств ИБ; суммарно - более 20 лет в сфере ИТ и более 10 лет в информационной безопасности.

Фундаментальная база: ММФ НГУ, СФП НГУ, Проф.переподготовка по ИБ в АНО ДПО Эшелон.

О чём сегодня поговорим:

- Хронология сотрудника в компании
- Виды инцидентов
- Работа с сотрудником до трудоустройства
- Работа с инцидентом во время работы
- Работа с сотрудником как с человеком

Эта презентация сделана без использования ИИ

Человек

75%

инцидентов ИБ происходят
из-за человеческого фактора*

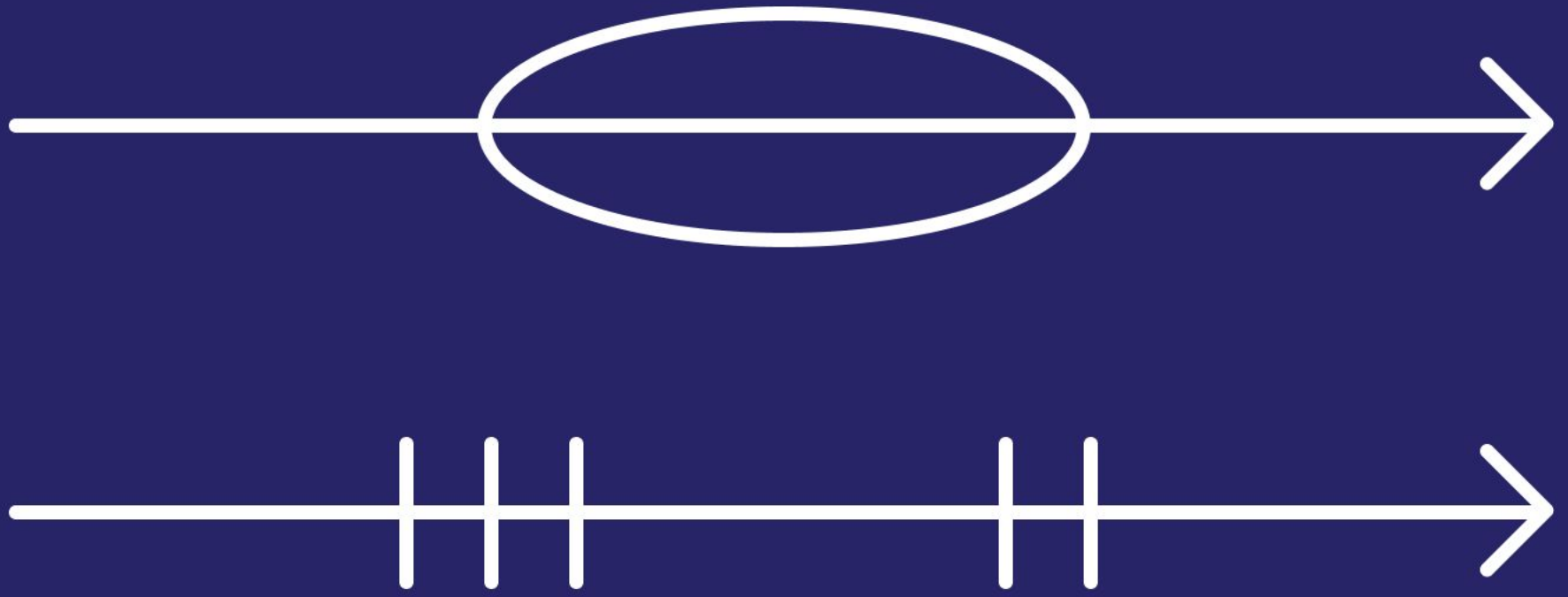
* исследование KnowBe4, 2025

67%

инцидентов ИБ происходят
с участием инсайдера*

* исследование Контур.Эгида и Piccard, 2025

~~Сотрудник~~
Корпоративный биоюнит



Инцидент с участием инсайдера

(в широком смысле) - это хищение коммерческой и НИОКР информации, кража ТМЦ, коррупция, фриланс, токсичное поведение, саботаж.

Целенаправленное действие

Действие на эмоциях

Случайность, ошибка

67%

Целенаправленное действие

10%

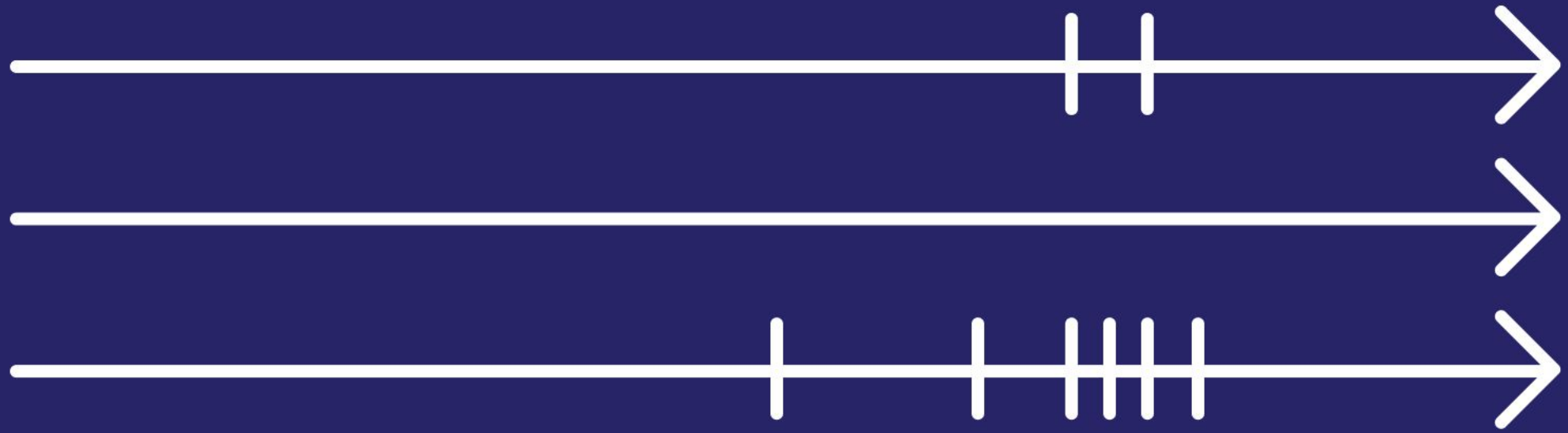
украдут в любой ситуации*

10%

не украдут*

80%

украдут в зависимости
от ситуации
и при благоприятных условиях*



* Институт психологии РАН, в отношении краж ТМЦ.

Действие на эмоциях

На самом деле это не совсем так. Это не эмоции, а результат микса:

1. Психотип
2. Ценности
3. Прошлый опыт
4. Ситуативный стрессор

Случайность, ошибка

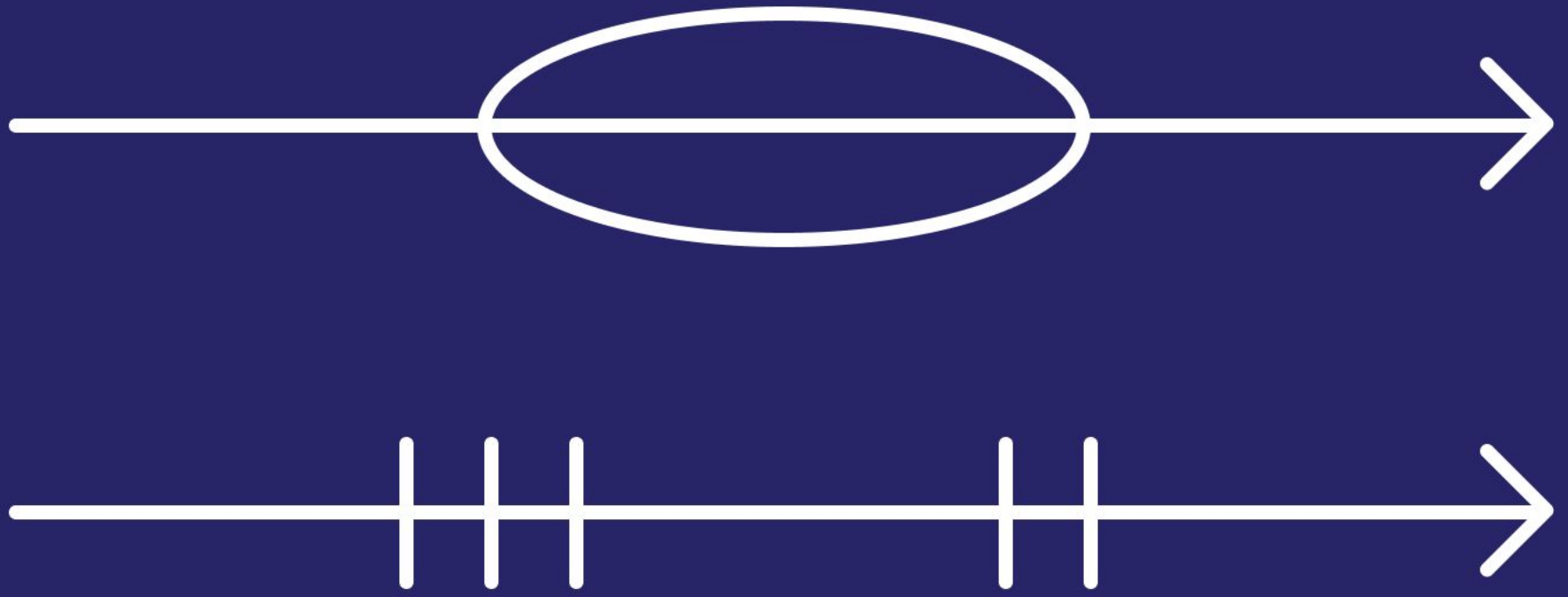
«Всякая случайность есть непознанная закономерность» (с)

Случайности – не случайны

- прогулки на природе являются интуитивным желанием снизить напряжение
- внимание новостям указывает на невротизацию и повышение потребности в контроле
- наличие законченных коллекций свидетельствует о педантичности
- экстраверты публикуют больше селфи
- любовь к ассиметричным рисункам указывает на высокий уровень дивергентности
- бренды первой линии предпочитают персоны с высоким уровнем невротизации

*Результаты исследований от наших технологических партнёров с 20-и летним опытом.
А теперь поймите, что таких связей a^n

~~Сотрудник~~
Корпоративный биоюнит



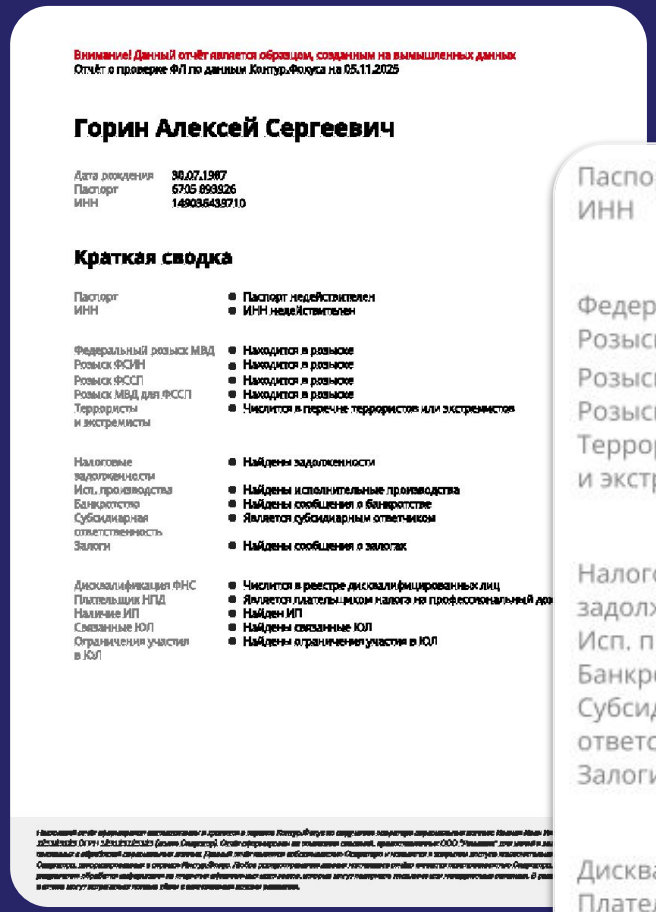
«Думайте как вы будете увольнять сотрудника на этапе собеседования с ним» (с)

До трудоустройства

До трудоустройства

Контур.Фокус:

– проверка ЮЛ и ИП
– проверка ФЛ



Внимание! Данный отчёт является образцом, созданным на вымышленных данных
Отчёт о проверке ФЛ по данным Контур.Фокуса на 05.11.2025

Горин Алексей Сергеевич

Дата рождения 30.07.1987
Паспорт 6705 893926
ИНН 149036439710

Краткая сводка

Паспорт
ИНН
- Паспорт недействителен
- ИНН недействителен

Федеральный розыск МВД
Розыск ФСИН
Розыск ФССП
Розыск МВД для ФССП
Террористы и экстремисты
- Находится в розыске
- Находится в розыске
- Находится в розыске
- Находится в розыске
- Числится в перечне террористов или экстремистов

Налоговые задолженности
Исп. производства
Банкротство
Субсидиарная ответственность
Залоги
- Найдены задолженности
- Найдены исполнительные производства
- Найдены сообщения о банкротстве
- Является субсидиарным ответчиком
- Найдены сообщения о залогах

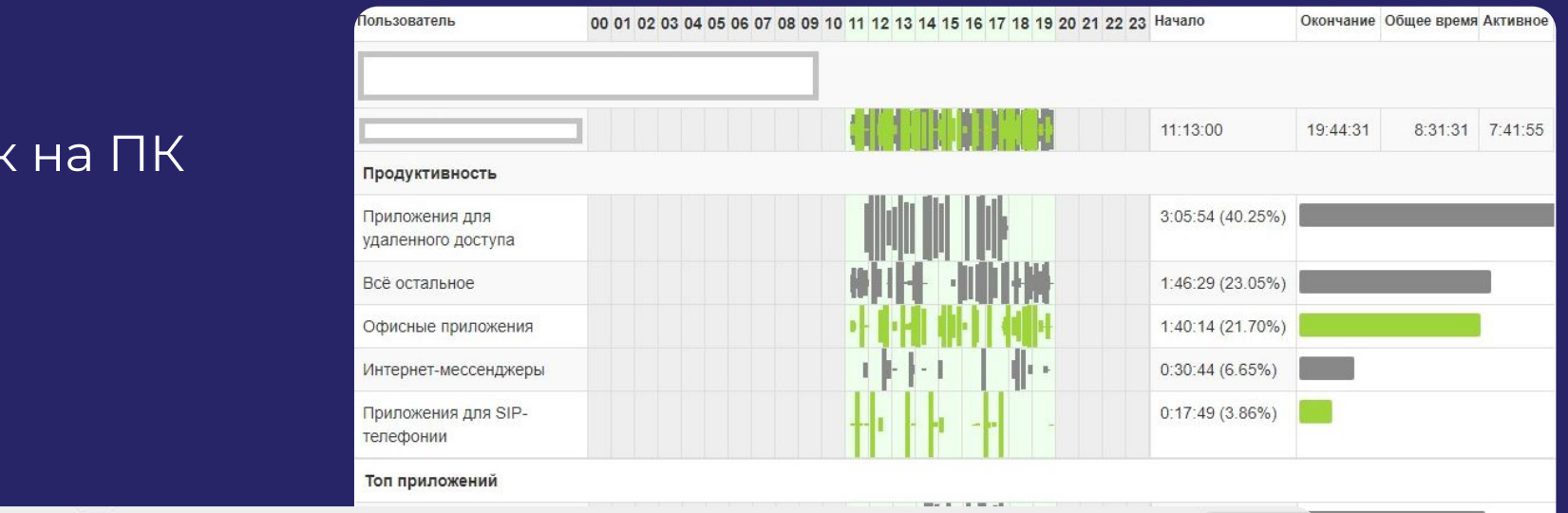
Дисквалификация ФНС
Плательщик НПД
Наличие ИП
Связанные ЮЛ
Ограничения участия в ЮЛ
- Числится в реестре дисквалифицированных лиц
- Является плательщиком налога на профессиональный доход
- Найден ИП
- Найдены связанные ЮЛ
- Найдены ограничения участия в ЮЛ

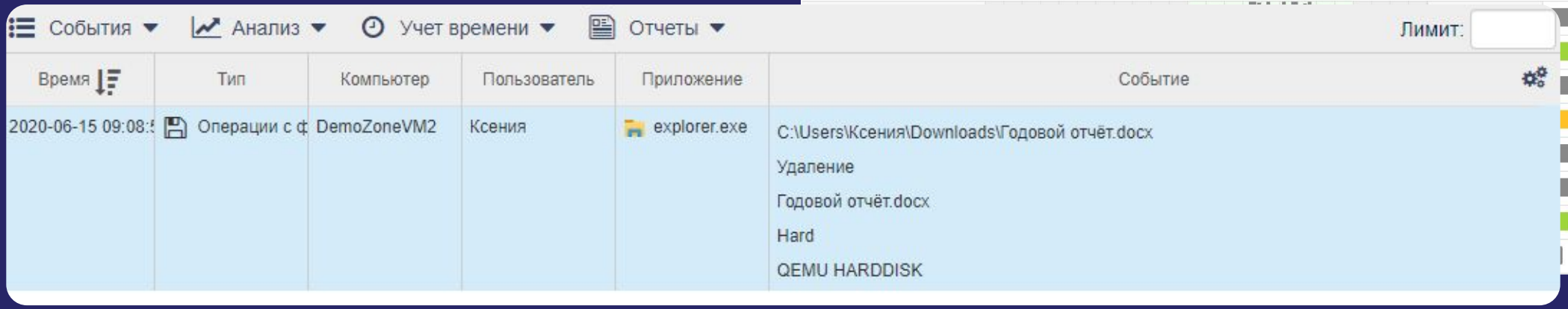
Паспорт	● Паспорт недействителен
ИНН	● ИНН недействителен
Федеральный розыск МВД	● Находится в розыске
Розыск ФСИН	● Находится в розыске
Розыск ФССП	● Находится в розыске
Розыск МВД для ФССП	● Находится в розыске
Террористы и экстремисты	● Числится в перечне террористов или экстремистов
Налоговые задолженности	● Найдены задолженности
Исп. производства	● Найдены исполнительные производства
Банкротство	● Найдены сообщения о банкротстве
Субсидиарная ответственность	● Является субсидиарным ответчиком
Залоги	● Найдены сообщения о залогах
Дисквалификация ФНС	● Числится в реестре дисквалифицированных лиц
Плательщик НПД	● Является плательщиком налога на профессиональный доход
Наличие ИП	● Найден ИП
Связанные ЮЛ	● Найдены связанные ЮЛ
Ограничения участия в ЮЛ	● Найдены ограничения участия в ЮЛ

Во время работы

Во время работы

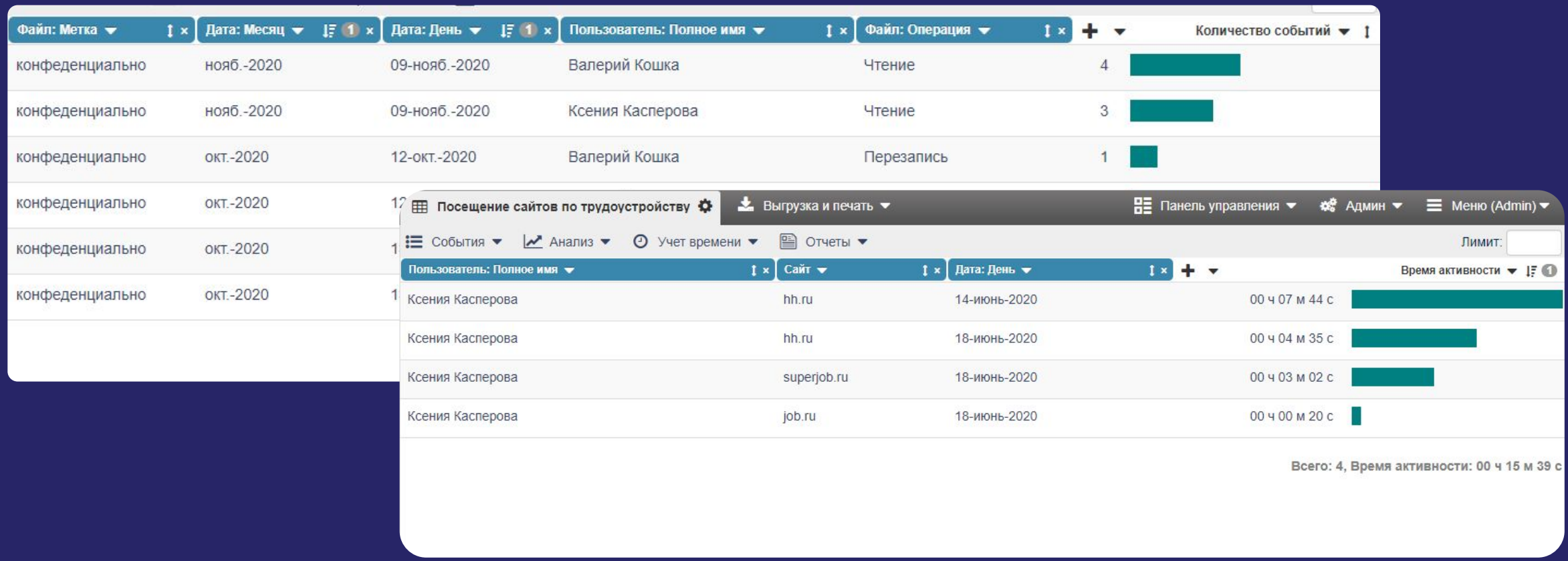
Что именно делал
(или не делал) сотрудник на ПК





Во время работы

Подготовка и сбор данных «для выноса»



Файл: Метка	Дата: Месяц	Дата: День	Пользователь: Полное имя	Файл: Операция	Количество событий
конфеденциально	нояб.-2020	09-нояб.-2020	Валерий Кошка	Чтение	4
конфеденциально	нояб.-2020	09-нояб.-2020	Ксения Касперова	Чтение	3
конфеденциально	окт.-2020	12-окт.-2020	Валерий Кошка	Перезапись	1
конфеденциально	окт.-2020	12			
конфеденциально	окт.-2020	1			
конфеденциально	окт.-2020	1			

Посещение сайтов по трудоустройству | Выгрузка и печать | Панель управления | Админ | Меню (Admin)

События | Анализ | Учет времени | Отчеты | Лимит:

Пользователь: Полное имя	Сайт	Дата: День	Время активности
Ксения Касперова	hh.ru	14-июнь-2020	00 ч 07 м 44 с
Ксения Касперова	hh.ru	18-июнь-2020	00 ч 04 м 35 с
Ксения Касперова	superjob.ru	18-июнь-2020	00 ч 03 м 02 с
Ксения Касперова	job.ru	18-июнь-2020	00 ч 00 м 20 с

Всего: 4, Время активности: 00 ч 15 м 39 с

Во время работы

Подготовка плана «зачистки»

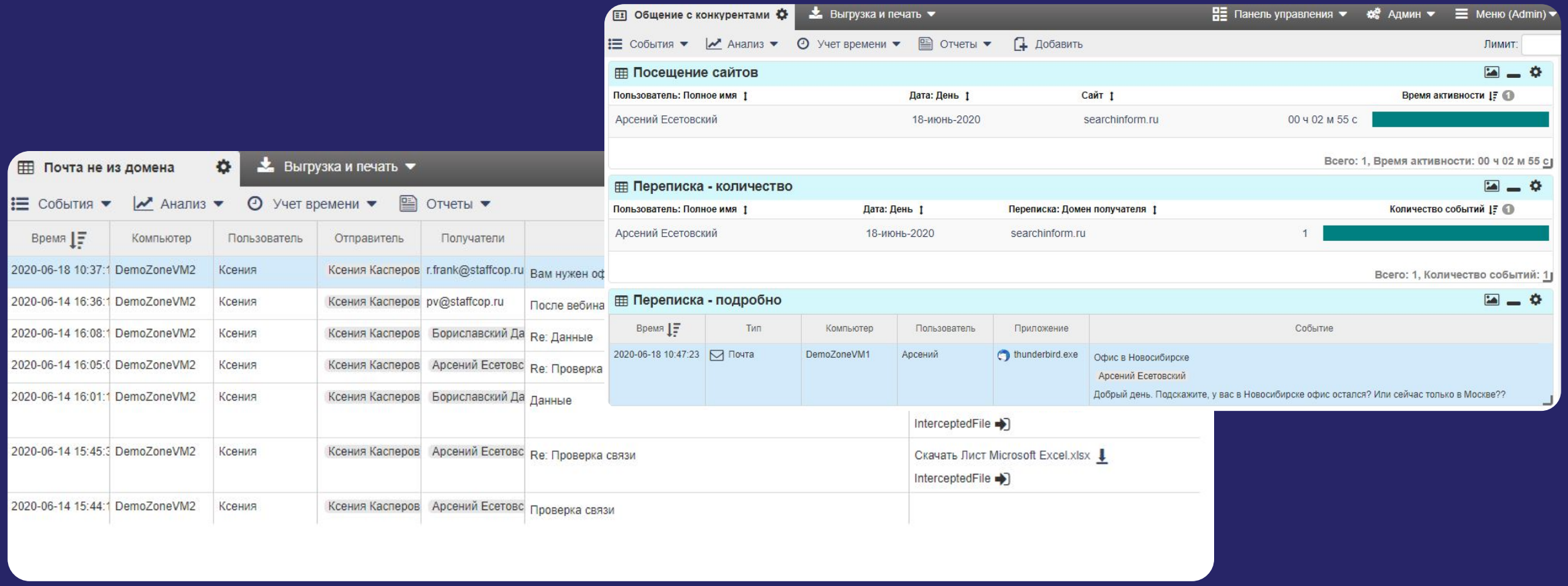
2020-04-23 15:09:14	Перехваченный ф	DemoZoneVM2 (1.27)	Ксения	chrome.exe	Выгруженные через браузер файлы Re: По делам Годовой отчёт.rtf Скачать Годовой отчёт.rtf Ксения Здесь данные за год. От генерального директора А также много картинок и цифр Mail
2020-04-23 15:05:56	Почта	DemoZoneVM1 (1.41)	Арсений	thunderbird.exe	Ищем директора Re: Письмецо Ксения ХЗ. Директор может поступить к что после самоизоляции нас та подробности?

Время 2020-04-23 15:05:56
Приложение thunderbird.exe
Фильтр Ищем директора
Тип события Почта
Агент DemoZoneVM1 (1.41)
Пользователь Арсений
Отправитель Ксения
Получатели Ксения
Участники Ксения ➤ Ксения
Формат Plain
Заголовок окна Re: Письмецо
Содержимое
```
ХЗ. Директор может поступить как мудак
23.04.2020 14:54, Ксения Касперова пишет:
> Сеня, говорят, что после самоизоляции нас так и оставят из дома
> работать, чтоб аренду не платить. Знаешь подробности?
```
PID 1904

Пользователь	Приложение	Домен	Текст
Арсений	firefox.exe	youtube.com	мир дикого запада 3 сезон 5 серия
Арсений	firefox.exe	youtube.com	мир дикого запада 3 сезон
Арсений	firefox.exe	yandex.ru	youtube
Арсений	firefox.exe	yandex.ru	youtube
Арсений	firefox.exe	yandex.ru	soliter.exe
Арсений	firefox.exe	yandex.ru	soliter.exe
Арсений	firefox.exe	yandex.ru	солитер виндовс 7 скачать бесплатно
Арсений	firefox.exe	yandex.ru	солитер
Арсений	firefox.exe	yandex.ru	солитер
Ксения	chrome.exe	google.com	купить тест на беременность с 2 полосками
Арсений	firefox.exe	yandex.ru	как удалить staffcop с компьютера
Арсений	firefox.exe	yandex.ru	как удалить staffcop с компьютера

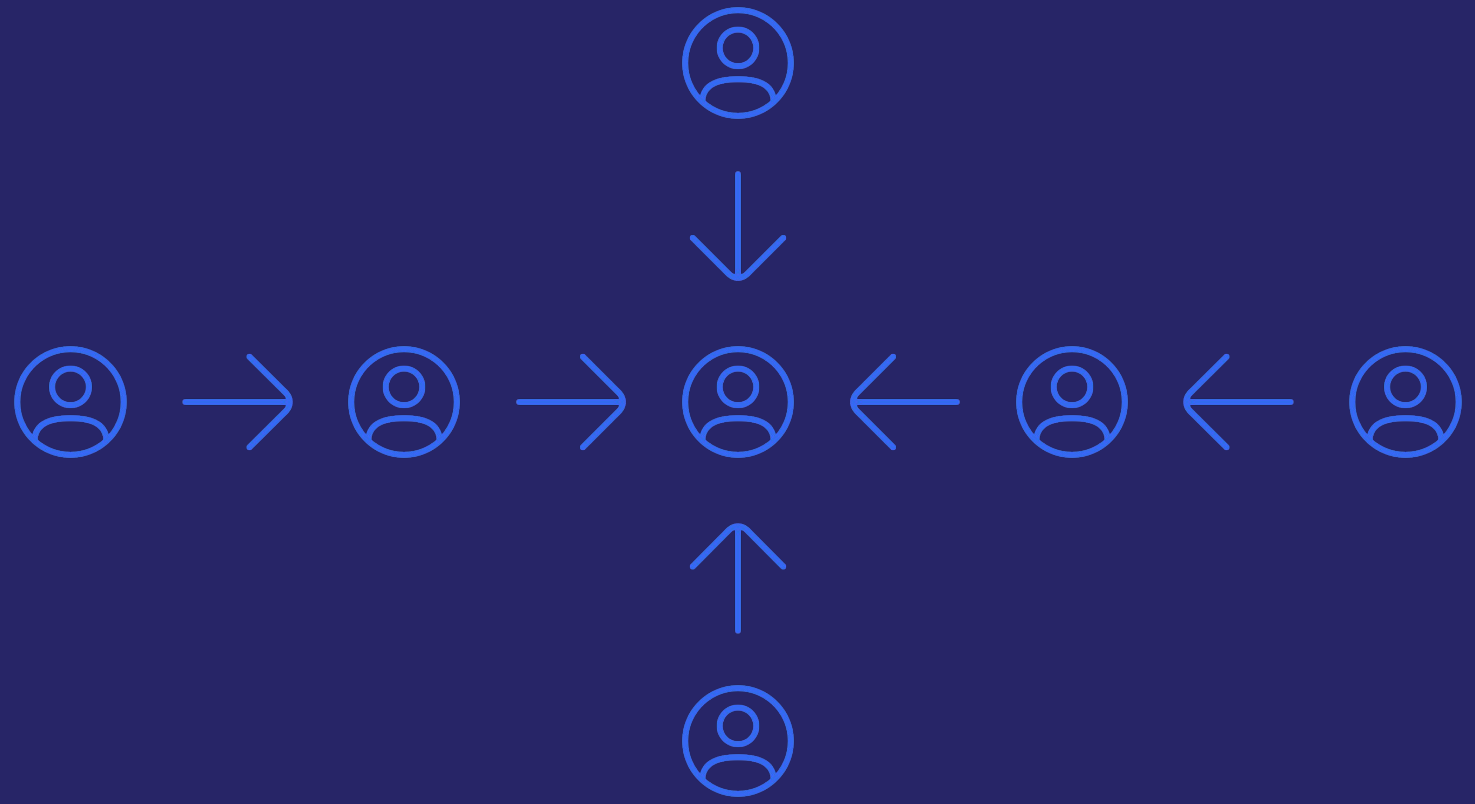
Во время работы

Общение с конкурентами и личная почта



Во время работы

Карта коммуникаций



Случайность, ошибка

– Интересы

– Самовыражение

– Цифровой след

– Референтная группа

–Семантика

Для тех, кто не знает науку –
мир полон магии

Наш профайлинг

Это не цифровой охотник на ведьм

это помощник, который подсветит риски до их появления;

это инструмент раннего информирования и автоматического целеуказания.

Наши пилоты (срезовые)

~500

деперсонифицированных наборов данных
в пилотах профайлинга клиенты передали нам

Мы провели «слепое» тестирование и вернули
результаты клиентам.

Наши пилоты (срезовые)

Клиенты проверили информацию по своей «верифицированной» выборке и получили информацию по контрольной группе.

Затем клиенты дали ОС по достоверности и контрольной группе.

~70-90%

достоверность, если в системе достаточное количество данных

Наши кейсы

Строительная компания: Фокус+Staffcop = увольнение сотрудника с прокладками и жизнью не по средствам.

Маркетинговое агентство: пилот профайлинга, который подтвердил гипотезы, и затем увольнение биоюнита.

Страховая компания: пилот профайлинга, подтверждение гипотез и обнаружение новых биоюнитов в группах риска.

Альтернативы нашего профайлинга

Почему не «360» или просто опросники?

– Сотрудники дают социально ожидаемые ответы
– Есть методология успешного прохождения теста
– Ничего не говорит о рисках

Почему не полиграф?

– Сложно
– Дорого
– Нельзя часто

Альтернативы нашего профайлинга

Почему не SOC?

- Очень много ручной работы
- Эпическая борьба с FP и TN
- SOC требует процессов и наличие инструментов

Почему не «старые» методы?

- Печень не выдержит
- Паяльники уже стали не те
- Удалёнка всё сломала

Пилот профайлинга – сейчас только для действующих клиентов по запросу. Или дождитесь релиза.

Пилот Staffcop

- без ограничения функционала
- на любое количество сотрудников
- на 14 дней

Узнать подробнее о **Контур.Фокус**

Благодарю за внимание! Вопросы?

Наш канал в MAX

Наш канал в Telegram

Даниил Бориславский

Директор по продукту Staffcop, эксперт по информационной безопасности Контур.Эгида

Контур staffcop