

# ZECURION DLP **11**

Как DLP-системы перешли от разбора инцидентов к управлению рисками

# О ZECURION

## 20 ЛЕТ

Опыта в ИБ, из них 15 лет — на DLP-рынке

## ПАРТНЕРЫ

Широкая партнерская сеть в России и за рубежом

## МИРОВОЕ ПРИЗНАНИЕ

Gartner FORRESTER IDC

## КЛИЕНТЫ

В России и за рубежом, более 10 тыс. компаний

## ENTERPRISE РЕШЕНИЕ

Работа в сетях с 200 000 сотрудников и более

## ИМПОРТОЗАМЕЩЕНИЕ

Поддержка: Astra Linux, Red OS, Alt Linux, GosLinux Реестр, сертификаты



РОСГОССТРАХ



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ  
РОССИЙСКОЙ ФЕДЕРАЦИИ



МИНИСТЕРСТВО ОБОРОНЫ  
РОССИЙСКОЙ ФЕДЕРАЦИИ



МИНИСТЕРСТВО  
ФИНАНСОВ РФ

СИБУР



ФЕДЕРАЛЬНОЕ  
КАЗНАЧЕЙСТВО  
РОССИЙСКОЙ  
ФЕДЕРАЦИИ



# ПРЕМИИ



SC Magazine (США, 2020) – оценка  
**5.00/5, статус**  
**“Recommended”**



Cybersecurity Excellence Awards  
(США, 2021)  
**Gold Winner**



Softshell Vendor Award (Germany,  
2017)  
**Bronze**



Enterprise Security Magazine (США, 2020) –  
**Top 10 Fraud and Breach**  
**Prevention Solutions**

# ВНУТРЕННИЕ УГРОЗЫ

Результаты исследования Код ИБ и Zecurion Analytics

# ПРОБЛЕМНЫЕ ТОЧКИ

## Наиболее серьёзные угрозы корпоративной безопасности



## Самые сложные задачи внутренней безопасности



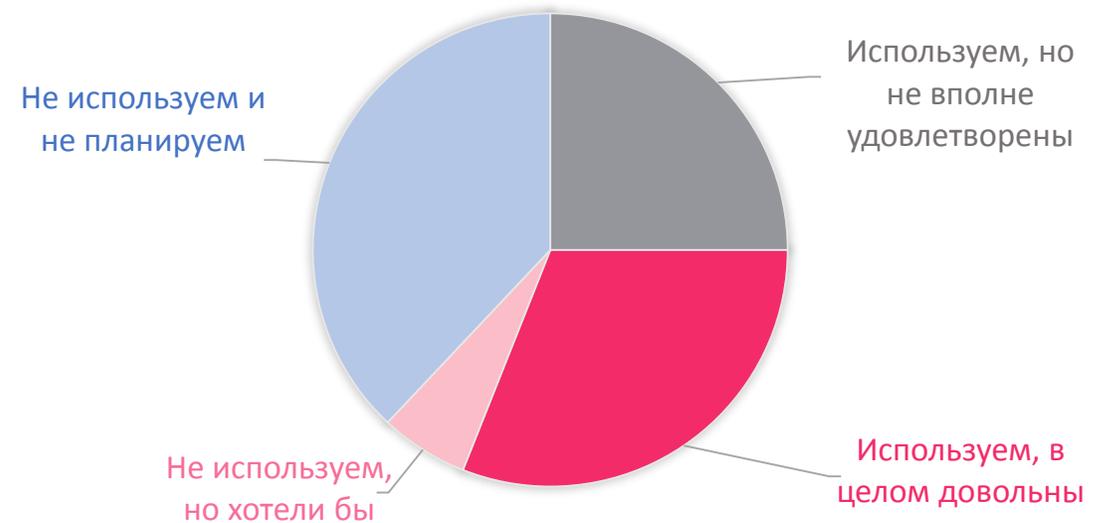
Источник: Код ИБ, Zecurion Analytics, 2021

# ИНСТРУМЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

Какие инструменты используете для решения проблем внутренней безопасности



## ИСПОЛЬЗОВАНИЕ DLP-СИСТЕМ



Источник: Код ИБ, Zecurion Analytics, 2021

# ПРЕИМУЩЕСТВА ZECURION DLP



Контроль всех возможных каналов утечки



Глубокая интеграция модулей



Оmnichannelные политики безопасности



Единая веб-консоль и iPad-приложение



Единый архив для расследований и сбора данных



10 технологий контентного анализа на базе машинного обучения и ИИ



13 вариантов внедрения и гибкая архитектура



Модуль отчетов с конструктором и готовыми шаблонами отчётов



Широкие возможности по интеграции (TITUS, SIEM, REST API)

# НОВОЕ В DLP 11



## Интерфейс

Существенное обновление карточки и списка сотрудников, возможность быстрого сравнения и более 10 точечных улучшений



## От инцидентов к рискам

Уникальная для DLP-рынка система оценки рисков с возможностью оперативно видеть актуальные угрозы



## Менеджер задач и IRP

Встроенный модуль расследований и управления регулярными задачами ИБ-отдела



## Screen Photo Detector

Модуль Screen Photo Detector с мгновенной реакцией на попытку сотрудника сфотографировать то, что находится на экране



## Staff Control Enterprise

Собственный модуль учёта и контроля рабочего времени сотрудников для крупных парков ПК



## Защита водяными знаками

Возможность выборочного показа водяного знака поверх окна приложения для доп. защиты от фотографирования и снятия скриншотов



## Диаграмма связей

Инструменты для быстрой работы с данными и оптимизация скорости работы с большим количеством связей, отображение до 1000 объектов



## Дополнительно

Связанные политики, блокировка учётной записи в AD, работа в бездоменных сетях, просмотр рабочего стола и ещё более 20 улучшений

# ОБНОВЛЁННЫЙ ИНТЕРФЕЙС

Карточка и список сотрудников, отчёты, инциденты

# ОБНОВЛЁННЫЙ СПИСОК СОТРУДНИКОВ

- Просмотр показателей уровня риска, продуктивности, сработавших политик и эмоционального состояния
- Настройка отображения с помощью фильтрации и быстрого поиска

The screenshot displays the ZECURION employee management interface. At the top, there is a navigation bar with the ZECURION logo and menu items: DLP, DLP PROCESSOR, LOG, OCR, REPORTS, STATUS. On the right, the user is identified as 'Админ Админ'. Below the navigation bar, there is a sidebar with 'Сводка' and 'Сотрудники' options. The main content area is titled 'Сотрудники' and includes a search bar and filters. The data is presented in a table with columns for employee name, risk level, productivity, activity index, policies, mood, and three numerical values. Each row includes a profile picture, name, position, and status icon.

Сотрудник	уровень риска	продуктивность	индекс активности	политики	настроение			
<b>Aleksandr Galiev</b> ☺ Служба управления рисками, Начальник службы Статус	86 <span>↑</span> +95.5%	6.42%	7.6 <span>↑</span> +733.3%	14	😊	143	118	3590
<b>Aleksandr Zhuravlyov</b> ☺ Управление информационных технологий, Системн Статус	36 <span>↑</span> +80%	24.3%	10 <span>↑</span> +1000.0%	9	😬	61	20	3541
<b>Aram Oganyan</b> ☺ Отдел сопровождения банковского программного об Статус	93 <span>↑</span> +19.2%	22%	9.9 <span>↑</span> +988.9%	10	😞	296	46	2618
<b>Artyom Vagner</b> ☺ Отдел сопровождения биржевых систем, Главный пр Статус	68 <span>↓</span> -4.23%	6.52%	3.6 <span>↑</span> +288.9%	9	😞	192	81	4973
<b>Ekaterina Nikiforova</b> ☺ Управление расчетно-кассовых операций, Начальн Статус	16 <span>↓</span> -15.8%	7.96%	10 <span>↑</span> +1000.0%	9	😞	51	6	3539
<b>Gennadij Osipov</b> ☺ Управление информационных технологий, Начальн Статус	73 <span>↑</span> +37.7%	22.9%	9.1 <span>↑</span> +900.0%	10	😬	191	119	11855
<b>Kerol Nyuman</b> ☺ Отдел сопровождения биржевых систем, Главный сп Статус	14 <span>↓</span> -17.6%	6.06%	8.6 <span>↑</span> +844.4%	7	😞	57	7	429
<b>Lyudmila Larionova</b> ☺ Служба внутреннего аудита, Ведущий специалист Статус	67 <span>↑</span> +42.6%	4.98%	9.9 <span>↑</span> +988.9%	10	😬	97	626	14306



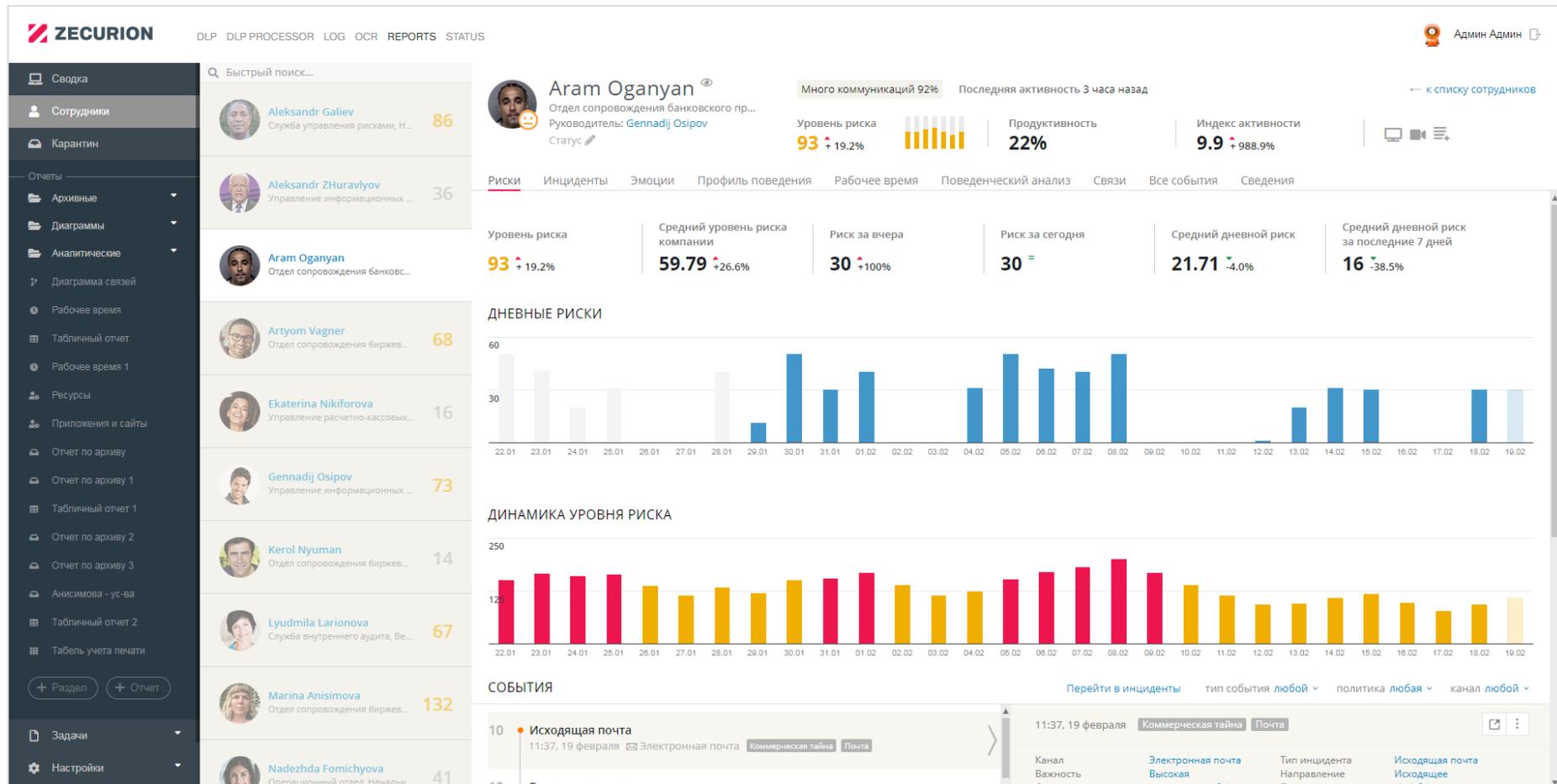
# ОБОГАЩЕНИЕ

Риски, профили, UBA



# РИСКИ, ПРОФИЛИ ПОВЕДЕНИЯ, ЭМОЦИИ

Для получения большего объема информации при расследованиях, прогнозирования развития ситуаций и принятия верных решений.



# РИСКОВАЯ МОДЕЛЬ



## 6 риск-показателей

Все ключевые риск-показатели в карточке сотрудников для понимания текущей ситуации и её динамики

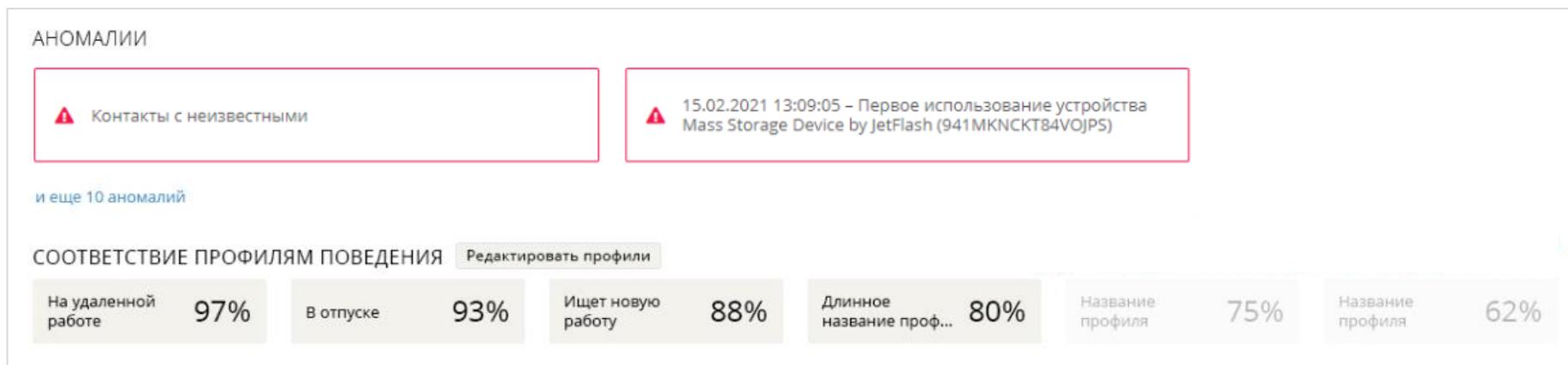
## Использование в сравнении

Простая и быстрая сортировка, фильтрация и сравнение сотрудников и отделов

## Таймлайн рисков

Уровни риска отображаются в виде таймлайна – временной шкалы с затуханием через 3 недели

# ПРОФИЛИРОВАНИЕ ПОВЕДЕНИЯ



## 7 типов аномалий

Все ключевые риск-показатели в карточке сотрудников для понимания текущей ситуации и её динамики

## Индекс активности

Простая и быстрая сортировка, фильтрация и сравнение сотрудников и отделов

## Ручное профилирование

Инструмент раннего реагирования и предупреждения до появления инцидентов

# БЫСТРОЕ СРАВНЕНИЕ СОТРУДНИКОВ

Удобный инструмент для быстрого сопоставления данных, выявления различий по всем ключевым показателям работы сотрудника или отдела

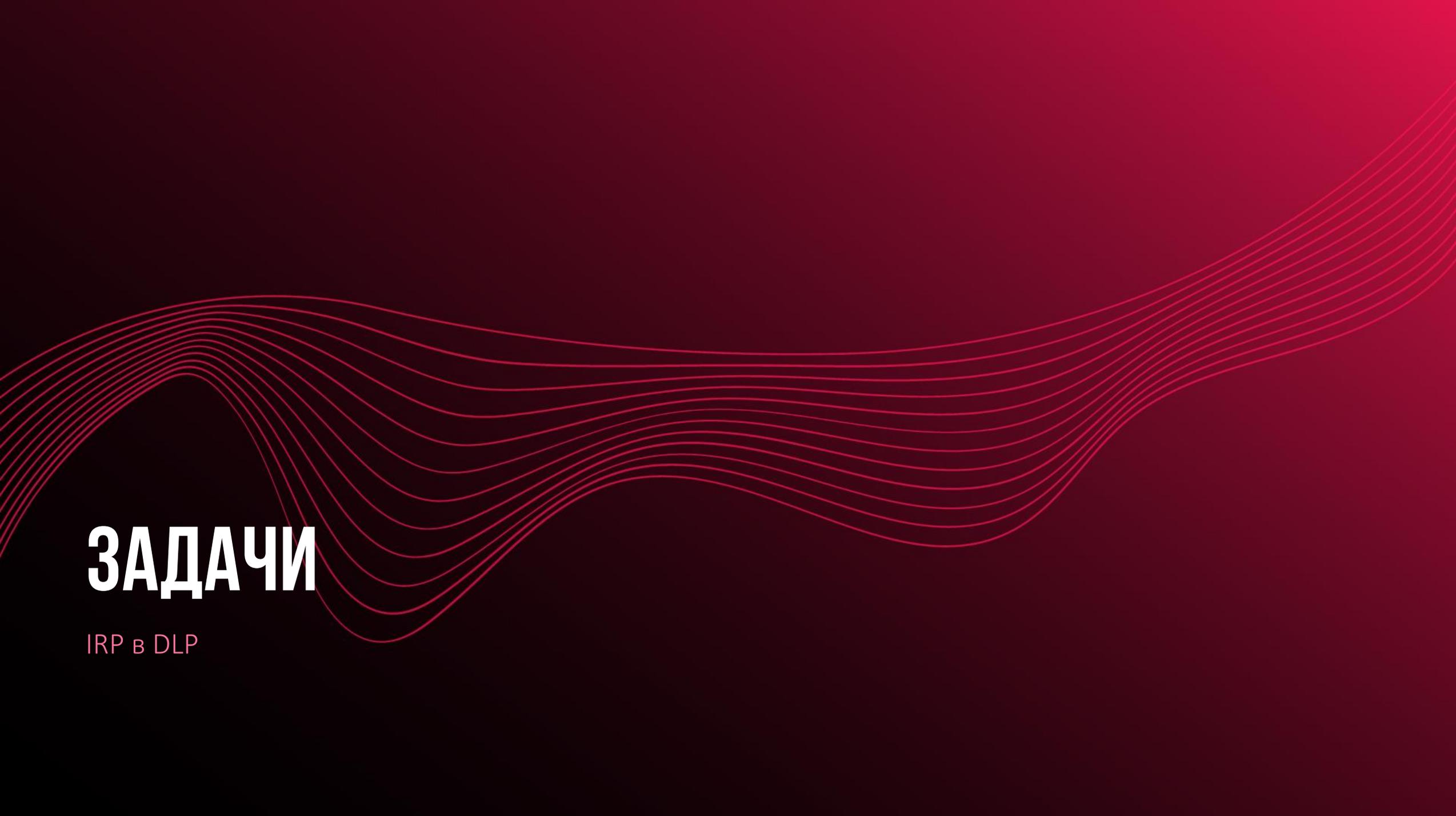
**Сравнение**

	<b>Aleksandr Galiev</b> Служба управления рисками, Начальник службы	<b>Artyom Vagner</b> Отдел сопровождения биржевых систем, Главный программист	<b>Aram Oganyan</b> Отдел сопровождения банковского программного обеспечения, Главный специалист	<b>Lyudmila Larionova</b> Служба внутреннего аудита, Ведущий специалист
▲ Уровень риска	94 +9.3%	66 -2.94%	106 +14%	59 -11.9%
Риск за вчера	21 -58%	10 +0%	30 +0%	4 -85.7%
Средний дневной риск	11.3 -9.2%	12.5 -23.2%	22.6 +6.5%	10.3 +30.9%
Средний дневной риск за последние 7 дней	17.4 +134%	13.4 -2.08%	20.1 +6.02%	11.7 +36.7%
▲ Продуктивность <b>Последние 14 дней</b>	8.07% +2.1%	6.05% -4.40%	24.46% +0.6%	5.66% +1%
Последняя активность	16 часов назад	17 часов назад	15 часов назад	15 часов назад
Нецелевое использование	25.7% +30%	16% -22%	8.7% -59.9%	23.8% +10.7%
Невыход	4	4	4	4
Опоздания	5 +0%	6 +0%	6 +0%	3 -40%
Ранние уходы	0 -100%	6 +20%	2 -60%	0 -100%
▲ Инциденты <b>Все время</b>	3851	5246	2960	15029
Высокой важности	143	192	296	97
Средней важности	118	81	46	626
Низкой важности	3590	4973	2618	14306
Связи	32	55	46	36

Средние значения для отделов

Очистить список сравнения | Свернуть

удалить из списка сравнения



# ЗАДАЧИ

IRP в DLP

# ПРИМЕНЕНИЕ

## РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ — IRP

- Готовый шаблон типа задачи для расследования инцидентов:
- Система делегирования
- Оперативные уведомления об изменениях на почту и в SIEM/Syslog

## TASK-MЕНЕДЖЕР

- Любое кол-во типов задач, в т. ч. кастомизируемые для разных задач
- Возможность использования задач как внутреннего таск-менеджера ИБ и ИТ за счёт гибкого конструктора форм

# РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

The screenshot displays the Zecurion Reports interface. On the left is a dark sidebar with navigation options like 'БД sveta\_incident', 'Сводка', 'Сотрудники', 'Карантин', 'Отчеты', 'archive', 'chart', 'table', 'Отчет по архиву', 'Video', 'Файлы с вложениями', 'All', 'диаграмма', 'Табличный отчет', 'Настройки', and 'Раздел'. The main area is titled 'Задачи' (Tasks) and features a search bar and filters for 'Исполнитель', 'Нарушитель', 'Тип', 'Статус', and 'Сортировка'. A list of tasks is shown, including 'Проверить интернет трафик пользователя Svetlana Volodina' (marked 'в работе') and 'Изменить политику «Для бухгалтерии»' (marked 'новая'). Below the tasks, a detailed view of an incident is visible, showing a 'Неизвестный' user and a file named 'http\_packet.zip' with a 'Сообщение' (Message) field containing a long alphanumeric string.

**Задачи**

Быстрый поиск...

Исполнитель любой | Нарушитель любой | Тип любой | Статус любой | Сортировка: дата создания | сначала новые

- Расследование** | Evgeny Andrukhov | **в работе** | Svetlana volodina | 05.05.2019  
**Проверить интернет трафик пользователя Svetlana Volodina**  
Увеличился интернет трафик пользователя Svetlana Volodina. Необходимо проверить является это нормой или нарушением. [Отчет](#)
- Изменение настроек** | Evgeny Andrukhov | **новая** | 05.05.2019  
**Изменить политику «Для бухгалтерии»**  
Сделать так чтобы все финансовые документы отправлялись только после подтверждения главным бухгалтером. Если бухгалтер не подтвердил отправку данного файла в течении следующего рабочего дня - отправитель...
- Мониторинг** | Igor Shornikov | **на проверке** | Svetlana volodina, Anastasiya Shulga | 05.05.2019  
**Проверить действия пользователей на предмет слива информации**  
Указанные сотрудники подозреваются в сливе информации конкурентам. Необходимо усилить наблюдение и выявить нарушения.
- Расследование** | Evgeny Andrukhov | **в работе** | Svetlana volodina | 20.05.2019  
**Проверить интернет трафик пользователя Svetlana Volodina**  
Увеличился интернет трафик пользователя Svetlana Volodina. Необходимо проверить является это нормой или нарушением. [Отчет](#)
- Изменение настроек** | Evgeny Andrukhov | **новая** | 20.05.2019  
**Изменить политику «Для бухгалтерии»**  
Сделать так чтобы все финансовые документы отправлялись только после подтверждения главным бухгалтером. Если бухгалтер не подтвердил отправку данного файла в течении следующего рабочего дня - отправитель...
- Мониторинг** | Igor Shornikov | **на проверке** | Svetlana volodina, Anastasiya Shulga | 05.05.2019  
**Проверить действия пользователей на предмет слива информации**  
Указанные сотрудники подозреваются в сливе информации конкурентам. Необходимо усилить наблюдение и выявить нарушения.
- Расследование** | Evgeny Andrukhov | **в работе** | Svetlana volodina | 05.05.2019  
**Проверить интернет трафик пользователя Svetlana Volodina**  
Увеличился интернет трафик пользователя Svetlana Volodina. Необходимо проверить является это нормой или нарушением. [Отчет](#)

**Неизвестный** | диск | зигбит | длинное имя политики! раз раз скоп...  
**http\_packet.zip** | Сообщение | sip2key: 9:470131809 sip2href: d00a85891ac18ac41ca82dd74e11519729efe49b155f9237ce86d9ee19e5ae...

**Админ Админ** | диск | зигбит | длинное имя политики! раз раз скоп...  
**NameMised\_0.xml** | Сообщение | sip2key: 8:124591867 sip2href: 3c05579d5e2c1ea074cf878c3a9abf072f966d49e549550a8320a06a8054т...

**Админ Админ** | диск | зигбит | длинное имя политики! раз раз скоп...

Zecurion Reports. Версия 3.0.0.317 | 14 мая

- Совместная работа над задачей
- Лёгкая постановка и контроль задач
- Сбор доказательств и обсуждение ИБ-стратегии
- Использование чек-листов и лучших практик
- Удобное обучение ИБ-аналитиков

# TASK-MЕНЕДЖЕР

- Любое количество типов задач
- Гибкий конструктор форм
- Комментарии исполнителей
- Отображение действий исполнителей в ленте
- Прикрепление инцидентов и файлов для доказательств
- Чек-листы
- Отчёты за периоды

- БД Основная
- Сводка
- Сотрудники
- Карантин
- Отчеты
  - archive
  - Отчет по архиву
  - chart
  - table
  - video

Сводка > Задачи > Проверить интернет трафик пользователя Svetlana Volodina

## Проверить интернет трафик пользователя Svetlana Volodina

Тип задачи	Расследование	Важность	Средняя	Статус	в работе
Инициатор	Maxim Nikulin	Исполнитель	Evgeny Andrukhov	Нарушитель	Svetlana Volodina
Создано	30.04.2019	Контрольная дата	06.05.2019		

Описание  
Увеличился интернет трафик пользователя Svetlana Volodina. Необходимо проверить является это нормой или нарушением.

Дополнительное поле 1

Дополнительное поле 2

Чек-лист

- Собрать все инциденты пользователя за текущую неделю
- Выявить инциденты являющиеся нарушениями

Кто виноват? Никто

Все события   Комментарии   Инциденты   Файлы   Доказательства

Evgeny Andrukhov — 14.03 в 09:15   новый комментарий  
Давайте у Светы спросим.

Evgeny Andrukhov — 13.03 в 09:17   изменен ответственный  
Evgeny Andrukhov → Svetlana Volodina

Svetlana Volodina — 12.03 в 12:22   новый комментарий  
Какая-то непонятная ерунда происходит. МЕНЯ на этих сайтах не было. Это все шпиены.

Svetlana Volodina — 11.03 в 12:24   прикреплен файл



Svetlana Volodina — 10.03 в 12:25   прикреплен файл



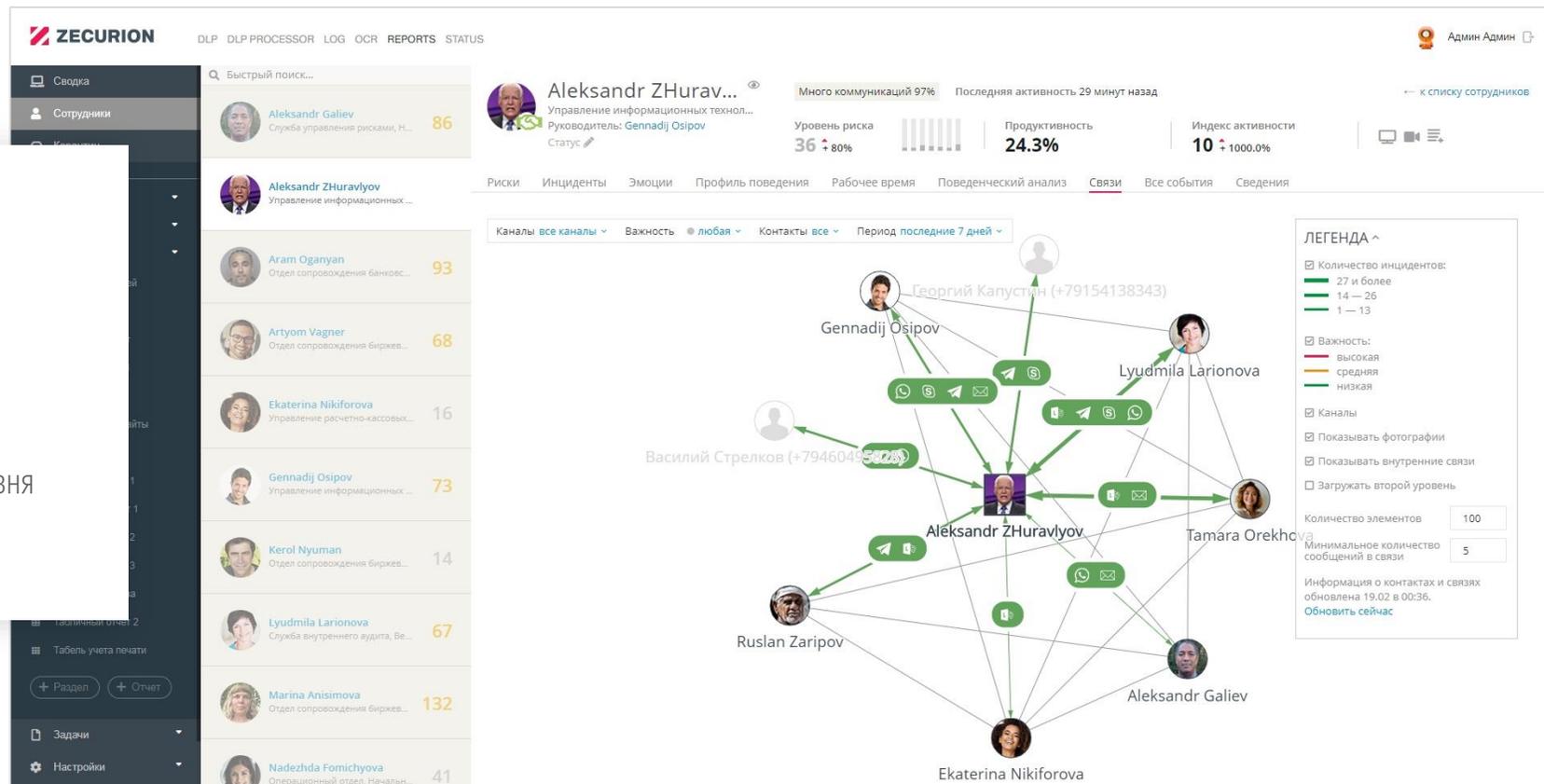
# ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Диаграмма связей, режим беседа, screen watermarks



# ДИАГРАММА СВЯЗЕЙ

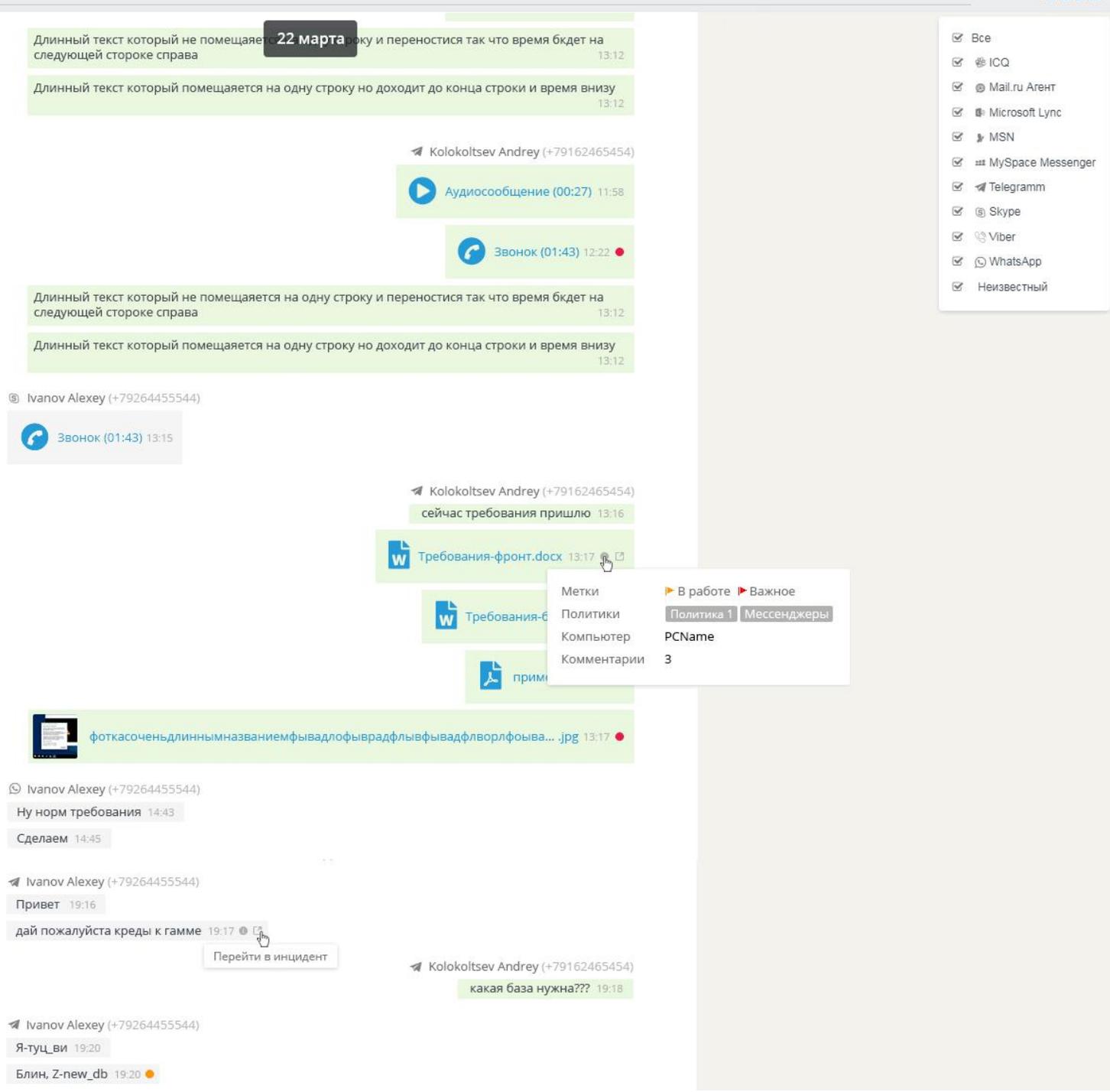
- Быстрые фильтры
- Возможность показа до 1000 объектов и масштабирования
- Настройка внешнего вида с помощью легенды
- Быстрое разворачивание связей 2-го уровня



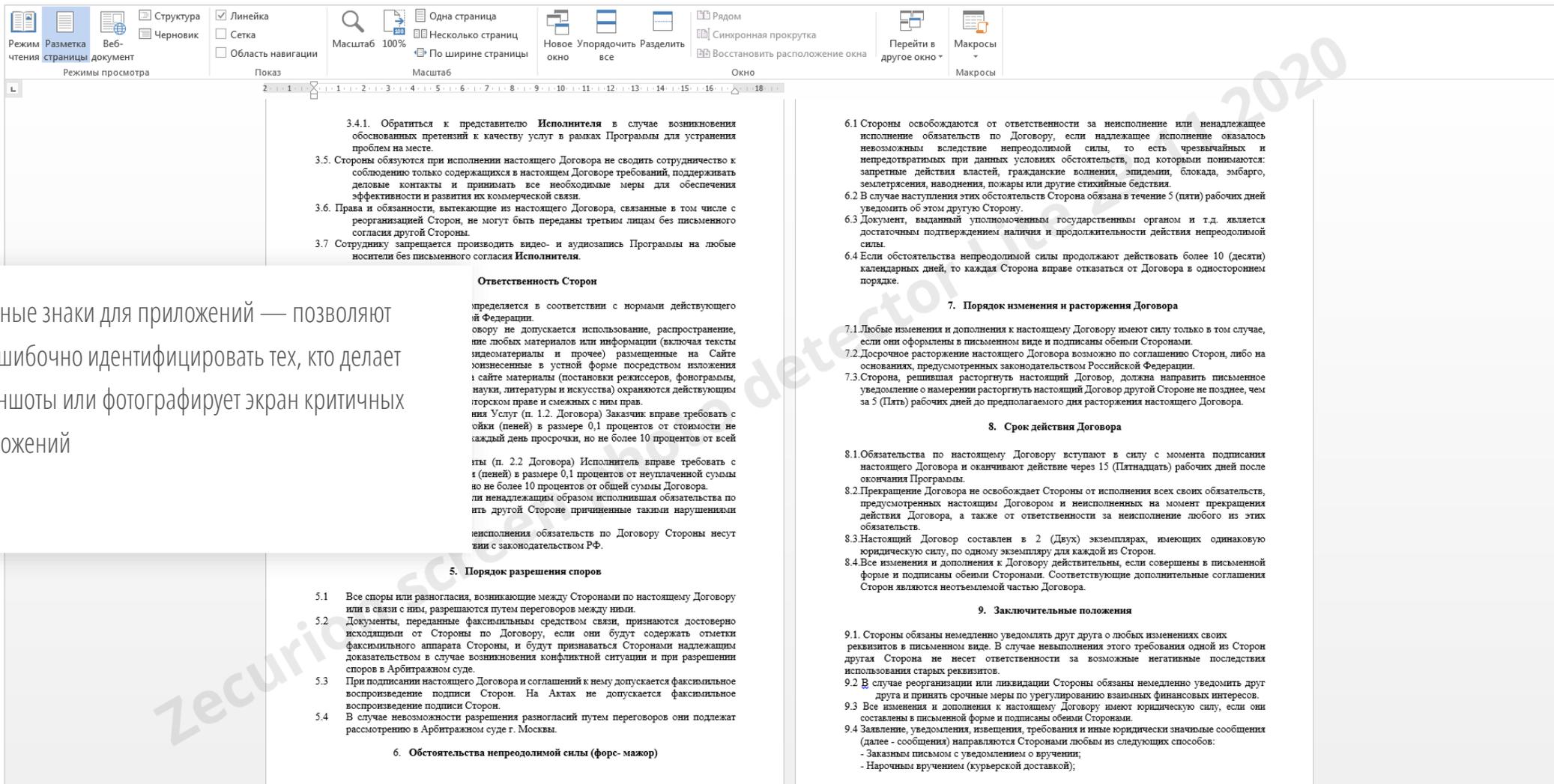
# ОТЧЁТ «БЕСЕДА»

По аналогии с Telegram отображает сообщения (инциденты) в виде диалога из всех мессенджеров.

- Возможность просмотра прикрепленных файлов
- Звонки и аудиосообщения
- Быстрый переход из чата в инцидент
- Дополнительная информация по событию в чате



# SCREEN WATERMARKS SCREEN PHOTO DETECTOR LITE



Водяные знаки для приложений — позволяют безошибочно идентифицировать тех, кто делает скриншоты или фотографирует экран критических приложений

**МОДУЛЬ**

**STAFF CONTROL 2.0** ENTERPRISE

Контроль рабочего времени сотрудников в Zecurion DLP 11

# STAFF CONTROL

Собственное решение Zecurion для учёта рабочего времени и построения отчётов по эффективности работы сотрудников.

- Полный учёт рабочего времени
- Присутствие и активность на рабочем месте
- «Фотографии рабочего дня» сотрудника/отдела
- Сводные отчёты за период по 15+ показателям
- ТОПы опаздывающих, отсутствующих, уходящих раньше, работающих удалённо
- Отчёты по приложениям и веб-сайтам
- Подсчёт продуктивности работы
- Удалённое подключение
- Табели учёта использования ресурсов



# ОТЧЁТЫ В STAFF CONTROL

## Карточка сотрудника

Все нужные показатели и общая сводка эффективности использования рабочего времени сотрудника в одном месте

## Конструктор отчётов

Новые виды отчётов, включая специальный табличный с быстрыми фильтрами и поддержкой работы с десятком тысяч ПК

## Посещение ресурсов

Списки приложений и сайтов. Могут быть показаны как конкретные ресурсы, так и категории

## Табели

Удобные отчёты по использованию сотрудниками принтеров и соблюдению дисциплины — приходо-уходов с рабочего места и др.

## Лента событий

Подробная лента событий в карточке сотрудника с удобным форматом отображения инцидентов

# РАБОЧЕЕ ВРЕМЯ

**ZECURION** DLP DLP PROCESSOR LOG OCR REPORTS STATUS Админ Админ

Сводка > Рабочее время Статистика обновлена 19.02 в 16:40 [Обновить статистику сейчас](#) [Обновить](#) [Сохранить](#) [Отменить](#)

### Рабочее время

Показаны первые 11 сотрудников за 100 дней Группировка по дате Период все время Статус любой Отдел любой Сортировка по параметру Поля (20)

Дата/сотрудник	Продуктивность	Полезное время за ПК		Нецелевое использование ПК			Время за ПК		Отсутст	
		Время	% от рабочего дня	Время	% от рабочего дня	% от времени за ПК	Время	% от рабочего дня	Время	% от работ
▲ 19.02.2021	13.6% -2.89%	3:13 -16.7%	2.88% -16.7%	5:04 -35%	4.54% -35%	17% -26.5%	29:49 -11.5%	26.6% -11.5%	54:34 -6.02%	48.7% -6
Vadim Subbotin	19.7% -32.6%	0:35 -37.6%	7.43% -37.6%	0:22 -0.15%	4.77% +0.15%	12.6% +7.79%	3:01 -7.09%	37.8% -7.09%	3:36 +3.96%	45.1% +2
Tamara Orekhova	0.63% -88.7%	0:00 -88.2%	0.09% -88.2%	0:14 -4.72%	2.94% -4.72%	21.2% +31.4%	1:06 -27.5%	13.9% -27.5%	5:32 -45.6%	69.2% -4
Stepan Komissarov	17.2% -30.7%	0:30 -41.5%	6.43% -41.5%	0:20 -60.1%	4.35% -60.1%	11.7% -52.7%	2:59 -15.6%	37.3% -15.6%	4:48 +43.4%	60.2% +2
Ruslan Zaripov	36.7% +2.5%	0:17 +18.1%	3.74% +18.1%	0:06 -20.3%	1.28% -20.3%	12.6% -30.9%	0:48 +15.2%	10.2% +15.2%	5:58 -25.3%	74.7% -2
Nadezhda Fomichyova	0% -100%	0:00 -100%	0% -100%	0:14 +6.41%	3% +6.41%	23% -32.8%	1:02 +58.4%	13.1% +58.4%	0:45 -90.9%	9.38% -9
Marina Anisimova	6.51% +14.9%	0:22 +9.3%	4.69% +9.3%	1:36 -15.7%	20.1% -15.7%	27.9% -11.4%	5:45 -4.87%	72% -4.87%	5:43 +124%	71.6% +1
Lyudmila Larionova	5.71% +3.06%	0:20 -9%	4.36% -9%	0:55 -39%	11.6% -39%	15.2% -33.9%	6:06 -7.82%	76.3% -7.82%	2:48 +5.3%	35.2% +1
Kerol Nyuman	2.52% -73.2%	0:00 -14.8%	0.08% -14.8%	0:05 +266%	1.13% +266%	35.7% +15.1%	0:15 +218%	3.17% +218%	0:38 +572%	8.08% +5
Gennadij Osipov	22.9% +57.8%	0:43 +94%	8.98% +94%	0:15 -56.7%	3.14% -56.7%	8% -64.8%	3:08 +22.9%	39.2% +22.9%	3:32 -30.3%	44.2% -3
Ekaterina Nikiforova	23.1% +537%	0:02 +163%	0.43% +163%	0:00 -87.8%	0.02% -87.8%	0.93% -70.5%	0:08 -58.6%	1.86% -58.6%	3:03 -48.4%	38.3% -4
Прочие	13.7% +0.13%	0:19 -43.3%	0.29% -43.3%	0:53 -53.2%	0.8% -53.2%	16.4% -28.4%	5:26 -34.6%	4.85% -34.6%	18:06 +113%	16.2% +1
▲ 18.02.2021	14% +100%	3:52 +100%	3.46% +100%	7:48 +100%	6.97% +100%	23.2% +100%	33:40 +100%	30.1% +100%	58:03 +100%	51.8% +1
Vadim Subbotin	29.3% +100%	0:57 +100%	11.9% +100%	0:22 +100%	4.76% +100%	11.7% +100%	3:15 +100%	40.7% +100%	3:28 +100%	43.4% +1
Tamara Orekhova	3.85% +100%	0:03 +100%	0.74% +100%	0:14 +100%	3.09% +100%	16.1% +100%	1:31 +100%	19.1% +100%	10:10 +100%	127% +1
Stepan Komissarov	24.8% +100%	0:52 +100%	11% +100%	0:52 +100%	10.9% +100%	24.7% +100%	3:32 +100%	44.2% +100%	3:21 +100%	42% +10
Ruslan Zaripov	35.8% +100%	0:15 +100%	3.16% +100%	0:07 +100%	1.6% +100%	18.2% +100%	0:42 +100%	8.83% +100%	8:00 +100%	100% +1
Nadezhda Fomichyova	8.21% +100%	0:03 +100%	0.68% +100%	0:13 +100%	2.82% +100%	34.2% +100%	0:39 +100%	8.24% +100%	8:15 +100%	103% +1
Marina Anisimova	5.67% +100%	0:20 +100%	4.29% +100%	1:54 +100%	23.8% +100%	31.5% +100%	6:03 +100%	75.7% +100%	2:33 +100%	31.9% +1
Lyudmila Larionova	5.54% +100%	0:22 +100%	4.59% +100%	1:31 +100%	19.1% +100%	23% +100%	6:37 +100%	82.8% +100%	2:40 +100%	33.4% +1
Kerol Nyuman	9.41% +100%	0:00 +100%	0.09% +100%	0:01 +100%	0.31% +100%	31% +100%	0:04 +100%	1% +100%	0:05 +100%	1.2% +1
Gennadij Osipov	14.5% +100%	0:22 +100%	4.63% +100%	0:34 +100%	7.24% +100%	22.7% +100%	2:33 +100%	31.9% +100%	5:04 +100%	63.4% +1
Ekaterina Nikiforova	3.63% +100%	0:00 +100%	0.16% +100%	0:00 +100%	0.14% +100%	3.17% +100%	0:21 +100%	4.5% +100%	5:55 +100%	74.1% +1
Прочие	13.7% +100%	0:34 +100%	0.51% +100%	1:54 +100%	1.7% +100%	22.9% +100%	8:18 +100%	7.42% +100%	8:28 +100%	7.57% +1
▲ 15.02.2021	12.9% -29.1%	4:09 +9.59%	3.72% +9.59%	6:08 +3.21%	5.48% +3.21%	18.3% -5.42%	33:28 +9.13%	29.9% +9.13%	38:16 -19%	34.2% -1

- Группировка по дате или отделу
- Быстрые фильтры и группировка
- Более 15 полей с динамикой показателей
- Динамика использования рабочего времени по дням

# ИСПОЛЬЗОВАНИЕ РЕСУРСОВ

- Списки приложений и сайтов.
- Могут быть показаны как конкретные ресурсы, так и категории
- Данные по приходам, уходам, недоработкам и переработкам
- Лента событий

The screenshot shows the ZECURION dashboard for an employee named Aleksandr Zhuravlyov. The interface includes a sidebar with navigation options like 'Сводка', 'Сотрудники', 'Карантин', 'Отчеты', and 'Архивные'. The main content area displays the employee's profile, including their name, position, and contact information. Key performance indicators are shown, such as 'Много коммуникаций 97%', 'Уровень риска 36 + 80%', 'Продуктивность 24.3%', and 'Индекс активности 10 + 1000.0%'. Below this, there are three data tables: 'ПРИЛОЖЕНИЯ И КАТЕГОРИИ', 'САЙТЫ И КАТЕГОРИИ', and 'ДИСЦИПЛИНА'. The 'СОБЫТИЯ' section at the bottom shows a log of system events, such as 'Выход пользователя из системы' and 'Вход пользователя в систему'.

**Сводка > Сотрудники > Aleksandr Zhuravlyov**

Статистика обновлена 19.02 в 16:40 [Обновить статистику сейчас](#) [Обновить](#)

**Aleksandr Zhuravlyov**  
Управление информационных технол...  
Руководитель: [Gennadij Osipov](#)  
Статус

Много коммуникаций 97%    Последняя активность 34 минуты назад    [← к списку сотрудников](#)

Уровень риска **36** + 80%    Продуктивность **24.3%**    Индекс активности **10** + 1000.0%

Риски    Инциденты    Эмоции    Профиль поведения    **Рабочее время**    Поведенческий анализ    Связи    Все события    Сведения    [последние 14 дней](#)

**ПРИЛОЖЕНИЯ И КАТЕГОРИИ**

Категории приложений	время	%	рост
Удаленный доступ	00:38:12	28	-15%
Почтовые клиенты	00:11:14	8	-21%
Мессенджеры	00:08:38	6	-40%
Файловые менеджеры	00:02:10	2	-16%
Офисные	00:00:60	1	-41%
Неопределенные	01:13:35	55	-2%

**САЙТЫ И КАТЕГОРИИ**

Категории сайтов	время	%	рост
Разработка	00:09:49	20	+35%
Поиск	00:05:13	11	-56%
Соцсети	00:04:01	8	+108%
Развлечения	00:01:42	4	+137%
Новости	00:00:21	1	-79%
Веб-почта	00:00:20	1	-63%
Неопределенные	00:27:02	56	-50%

**ДИСЦИПЛИНА**

дата	Приход на работу	Уход с работы	Время на работе
19.02	11:30 +2 ч 30 мин	16:47 -12 мин	5:17 -2 ч 43 мин
18.02	09:11 -11 мин	09:34 -7 ч 25 мин	00:23 -7 ч 37 мин
15.02	15:40 +6 ч 40 мин	15:59 -1 ч	00:20 -7 ч 40 мин
14.02	13:02	13:47	00:45
13.02	11:29	11:50	00:21
12.02	14:17 +5 ч 17 мин	15:58 -1 ч 1 мин	1:41 -6 ч 19 мин
11.02	11:16 +2 ч 16 мин	17:48 +48 мин	6:32 -1 ч 28 мин
08.02	17:22 +8 ч 22 мин	17:58 +58 мин	00:37 -7 ч 23 мин
07.02	07:08	14:51	7:43
06.02	10:35	16:58	6:23

**СОБЫТИЯ**    [Перейти в инциденты](#)    тип события любой

- 16:47, 19 февраля    Staff Control
- 16:47, 19 февраля    Staff Control
- 11:30, 19 февраля    Staff Control
- 09:34, 18 февраля    Staff Control
- 09:11, 18 февраля    Staff Control

16:47, 19 февраля

Канал	Важность	Пользователь	Тип инцидента	Направление	Компьютер	Выход пользователя из с...
Staff Control	Низкая	aleksandr.zhuravlyov@...	Компьютер	Внутреннее	AZHURAVLYOV	Выход пользователя из с...

Нет комментариев +

# ZECURION SCREEN PHOTO DETECTOR

2 нейросети распознают смартфон, фиксируют инцидент  
и предотвращают утечку со скоростью от 0,06 сек

- Уникальная технология
- Мгновенная реакция
- Экономия на оборудовании
- Предотвращение утечек



# ZECURION DLP 12 + DCAP

**ZECURION** REPORTS Имя Фамилия

Сводка Сотрудники Данные Отчеты Карантин Задачи Настройки

### Данные

Силосы	Владелец	Размер	Классы
Users	Ivan Ivanov	147.3 МБ	ФЗ-146 Бухгалтерские документы Персональные данные
Downloads	Ivan Ivanov	88.7 МБ	Бухгалтерские документы
Defaultfile.txt	Ivan Ivanov	976 КБ	Персональные данные
Defaultfile1.txt	Ivan Petrov	875 КБ	

#### Users

Основное Сетевой доступ Локальный доступ События

Тип: Папка с файлами

Классы: ФЗ-146 Бухгалтерские документы Персональные данные

Владелец: Ivan Ivanov (ivanov@domainname)

Расположение: C:\Users\Ivanov.DOMAIN

Размер: 13,4 МБ (14 060 198 байт)

Содержание: Файлов: 304; папок: 146

Создание: 6 августа 2018 г., 9:24:31

Последнее изменение: Последнее изменение

[Найти похожие](#)

# ЧТО ПРОИСХОДИТ ВНУТРИ ПЕРИМЕТРА?

Какие данных хранятся в организации? Где хранятся критичные данные? Кто имеет к ним доступ? Есть ли неактуальные аккаунты и права? Какие данные есть у конкретного отдела или сотрудника? Кто «втихую» меняет файлы? Кто читает чужую почту? Чьи аккаунты используются не владельцами? Кто решил скачать себе все данные перед утечкой?

Какие DATA-риски у вас есть сейчас?



01

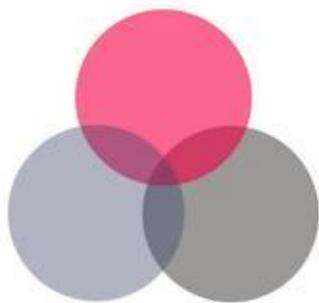
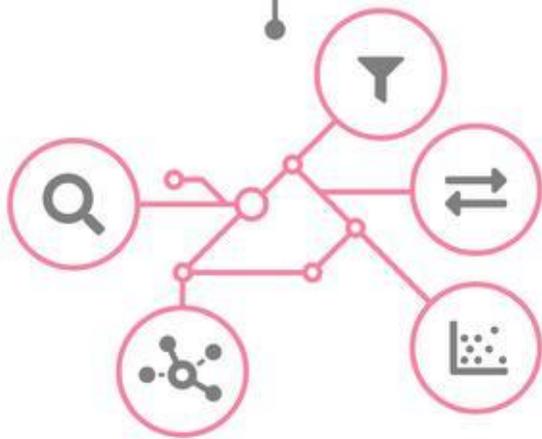
## ИСТОЧНИКИ

- Файл-серверы
- Локальные ПК
- Папки общего доступа
- Microsoft Exchange и почтовые папки
- Microsoft Active Directory и LDAP
- Места хранения
- Структуры
- Атрибуты
- События
- Права

## ОБРАБОТКА

- Сбор
- Фильтрация
- Нормализация
- Агрегация
- Корреляция

02



03

## АНАЛИЗ

- Классификация
- Определение угроз
- Детектирование аномалий

## РЕАГИРОВАНИЕ

- Запись событий
- Теневое копирование
- Создание инцидентов
- Блокировка доступа
- Изменение прав
- Запуск расследований
- Действия с данными
- Запуск сторонних приложений

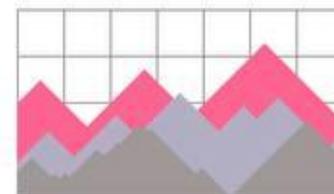
04



05

## ОТЧЕТЫ

- Структура
- Data Dashboard индикаторы
- 10+ готовых отчетов
- Конструктор отчетов
- Единая DLP-консоль



# FORENSIC ALLIANCE

Корпоративные расследования и защита бизнеса



<https://t.me/forensictoday>



# СПАСИБО ЗА ВНИМАНИЕ!

Узнайте больше о DLP11, DLP12, DCAP и SWG/NGFW у нас на стенде  
или оформите приоритетное право на пилот [welcome@zecurion.com](mailto:welcome@zecurion.com)