СОЛАР

Solar Dozor 7.11

Предотвращение утечек информации, проведение расследований и профилактика внутренних инцидентов безопасности

White paper

МОСКВА, январь 2024

Содержание

Список иллюстраций

Список таблиц

1. Краткое описание

1.1. Назначение

Solar Dozor — система для предотвращения утечек конфиденциальной информации (Data Leak Prevention, DLP) корпоративного класса. Ее возможности обеспечивают контроль коммуникаций сотрудников, блокировку или изменение нежелательных сообщений, выявление и мониторинг групп риска, а также ретроспективный анализ архива коммуникаций для проведения расследований. Кроме этого, Solar Dozor анализирует поведение пользователей (User Behavior Analytics), что позволяет выявлять аномалии поведения, круг общения и приватные контакты сотрудников, а также профилировать их на основе 20 устойчивых паттернов поведения. Это дает возможность заниматься профилактикой инцидентов безопасности.

В Solar Dozor реализована современная концепция обеспечения внутренней безопасности организации — People-Centric Security[1]. Она предполагает концентрацию внимания службы безопасности на главном источнике угроз — человеке: фактической роли в коллективе, характере коммуникаций, особенностях работы с защищаемой информацией. Такой подход заметно эффективнее традиционного мониторинга разрозненных данных и низкоуровневых событий. В результате офицеры безопасности могут сосредоточиться на расследовании и профилактике критических инцидентов, не тратя большую часть своего времени на разбор ложных срабатываний и отвлекающих уведомлений.

Если организация состоит из нескольких дочерних зависимых обществ или территориально распределенных филиалов, инсталляции Solar Dozor могут работать как единое целое (функции модуля MultiDozor). Это дает возможность:

- В режиме реального времени получать и обрабатывать данные по всей организации или отдельным подразделениям;
- Контролировать деятельность всех пользователей DLP-системы;
- Выполнять централизованный мониторинг групп особого контроля;
- Проводить сквозные расследования в масштабе организации;
- Централизованно управлять системой и распространять политику безопасности в филиалы.

Пользователи Solar Dozor — представители служб информационной, экономической и внутренней безопасности крупных и средних коммерческих и государственных организаций, нуждающиеся в инструментах для контроля коммуникаций и предотвращения утечек, а также выявления корпоративного мошенничества, конфликтов интересов, взяточничества, сговоров, прямых или косвенных хищений денежных средств, шпионажа.

Solar Dozor необходим, если организации требуется:

- Защитить информацию ограниченного доступа, конфиденциальность которой критически важна для успешной деятельности (ноу-хау, коммерческая тайна, персональные данные, стратегии развития и инвестирования и т. д.);
- Выявлять коррупционные схемы при закупках, а также факты аффилированности, вымогательства и получения взяток;

[1] «Безопасность с фокусом на человеке». Термин введен международной консалтинговой компанией Gartner, специализирующейся на ИТ-рынке (ID: G00250121, Definition: People-Centric Security, 2013 г.).

- Контролировать сотрудников, имеющих доступ к важным финансовым и информационным активам;
- Отслеживать коммуникации по ключевым сделкам, управлять конфликтами интересов, обеспечивать непрерывность ключевых бизнес-процессов;
- Контролировать выполнение управленческих решений, отслеживать реакции на приказы и распоряжения, выявлять факты лоббирования;
- Отслеживать климат в коллективе, отзывы о руководителях, выявлять распространителей слухов и инсайдеров;
- Отслеживать связи с конфликтно уволенными, криминалом, конкурентами, СМИ;
- Контролировать сотрудников из групп риска для своевременного пресечения возможного ущерба (должники, наркоманы, игроманы, транжиры, ранее судимые, сектанты и т. д.);
- Отслеживать соответствие регламентам, кодексам, стандартам и законам;
- Выявлять признаки промышленного шпионажа и саботажа, террористических и экстремистских действий, вербовочных разработок, сокрытия нарушений режима охраны;
- Обеспечивать соответствие требованиям 152-ФЗ «О персональных данных», Постановления Правительства № 1119 «Об утверждении требований к защите персональных данных», Приказов ФСТЭК России № 17 и № 21, а также стандартов и рекомендаций Банка России.

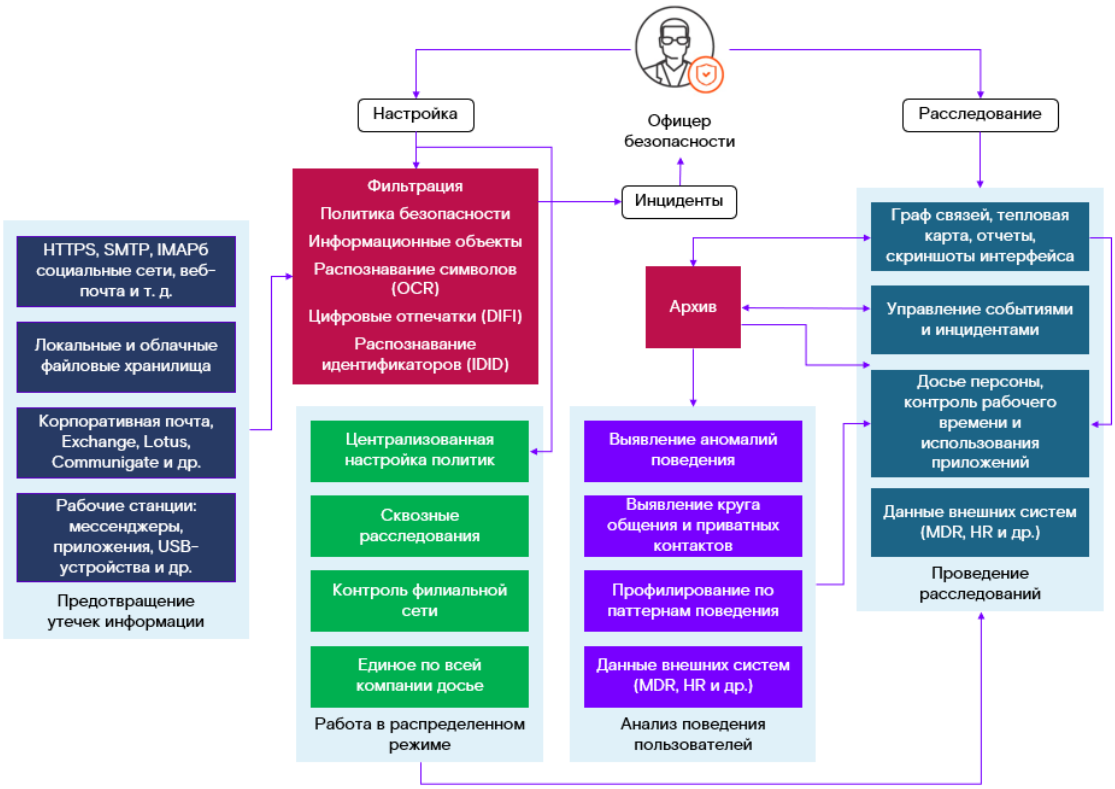


Рисунок 1. Концептуальная схема работы Solar Dozor

Предотвращение утечек информации

Для защиты конфиденциальной информации от утечек Solar Dozor использует специализированные модули — перехватчики. Они собирают и передают на анализ коммуникации сотрудников из различных каналов, контролируют действия пользователей на

персональных компьютерах, а также инвентаризируют и отслеживают локальные и облачные файловые ресурсы.

Защищаемая информация может быть представлена в текстовом, графическом или бинарном видах: сообщения в электронной почте, мессенджерах, веб-ресурсах и социальных сетях, технические чертежи САПР, документы Microsoft Office, отсканированные счета, страницы паспортов, голосовые сообщения, видеофайлы, архивы, изображения и т. д.

В зависимости от технических особенностей для каждого канала подбирается оптимальная точка перехвата информации — на почтовом сервере, сетевом шлюзе, прокси-сервере или рабочей станции. Это дает возможность равномерно распределить нагрузку на ИТ-инфраструктуру и обеспечить непрерывность бизнес-процессов организации.

Перехваченные данные анализируются в основном модуле Solar Dozor с помощью комплекса настраиваемых правил, отражающих актуальные задачи безопасности организации. По результатам анализа принимается решение о блокировке нежелательного действия или уведомлении офицеров безопасности о подозрительной активности.

Уникальная функция реконструкции сообщений электронной почты позволяет удалять из сообщений части, содержащих КИ, и/или отправлять сообщения с измененной текстовой частью (текст сообщения), в которую при реконструкции добавляется произвольный текст. При реконструкции Solar Dozor сам распознает формат сообщения и правильно изменит его текстовую часть. Такая отправка возможна как при автоматической обработке сообщений, при соответствующем правиле в политике, так и в ручном режиме, когда сообщение отправляется из архива.

Также система может с достаточной степенью точности распознавать в изображениях такие графические объекты как:

- Паспорт РФ: разворот 3-ей страницы, содержащей персональные данные;
- Печати организаций (круглую и треугольную);
- Лицевую и оборотную стороны платежной карты.

Solar Dozor может быть установлен в режиме блокировки (в разрыв трафика). Это позволяет надежно блокировать передачу конфиденциальной информации в реальном времени, а не просто констатировать факт утечки через несколько часов после ее совершения.

При интеграции с системой контроля и управления доступом (СКУД) Solar Dozor также может заблокировать пропуск сотрудника при попытке организовать утечку данных.

Анализ поведения пользователей

Анализ действий сотрудников и контрагентов может стать для офицера безопасности источником сведений о зарождающихся угрозах. Перед совершением преступления любой злоумышленник проводит подготовительные действия и неосознанно оставляет следы, которые являются отклонением от нормы — аномалиями. Solar Dozor предоставляет визуальные инструменты для быстрого выявления такого поведения. Специальные виджеты предоставляют быстрый доступ к информации по сотрудникам, входящим в группы особого контроля (на испытательном сроке, на увольнение и т. д.), или у которых было зафиксировано аномальное поведение.

С модулем UBA, ставшим доступным с выходом Solar Dozor 7, система может анализировать поведение пользователей автоматически, что открывает перед офицерами безопасности новые возможности. В их число входят сравнение аномалий в поведении нескольких сотрудников, выявление круга общения, в том числе рабочих сетей и неизвестных контактов, а также профилирование сотрудников в соответствии с 20 устойчивыми паттернами поведения.

Это позволяет работать с рисками превентивно, вовремя принимая соответствующие меры, а также выявлять злоумышленников, поведение которых большую часть времени стандартно. Например, менеджера по закупкам, иногда использующего аффилированные компании для участия в тендерах.

Реализованные в модуле UBA методы анализа и математическая модель поведения уникальны и являются собственной разработкой компании «Солар». Они базируются на теориях вероятности, случайных процессов и графов. Используемые алгоритмы относятся к классу unsupervised machine learning (обучение без учителя). Такие алгоритмы не требуют предварительных работ по настройке и адаптации под новые условия эксплуатации. Для подключения модуля UBA не требуется проводить какие-либо работы по интеграции — достаточно выделить вычислительные мощности и активировать лицензию.

Для предварительного анализа достаточно накопить массив данных о коммуникациях сотрудников за 1 месяц, для точной работы — за 2–3 месяца. Если организация уже использует Solar Dozor, то анализ поведения пользователей доступен сразу.

Проведение расследований

Вся собранная Solar Dozor информация может помещаться в архив и использоваться для дальнейшей работы службы информационной, внутренней и экономической безопасности. При необходимости возможна перефильтрация архива для ретроспективного анализа ранее накопленных данных по вновь открывшимся обстоятельствам и нахождения ранее пропущенных инцидентов.

Технология быстрого поиска, аналогичная поисковикам Яндекс или Google, позволяет мгновенно находить нужные сообщения и инциденты безопасности — поиск в архиве на 17 млн сообщений занимает 1 секунду. При этом не нужно составлять сложные поисковые запросы, требующие наличия профильного ИТ- или ИБ-образования — при начале ввода имени или части адреса Solar Dozor сразу отображает список сотрудников, данные которых содержат вводимые символы.

Простой и быстрый поиск дает возможность работать с системой специалистам служб экономической и внутренней безопасности организации, комплаенса, внутреннего контроля, HR-департамента и т. д. Также доступны поисковые шаблоны, отражающие многолетний опыт использования Solar Dozor в различных организациях России.

Нередко офицеры безопасности делегируют специалистам младшего звена поиск данных по заданным параметрам. Это повышает риск несанкционированного доступа к данным. В Solar Dozor офицер безопасности может предоставлять поисковые запросы только на запуск (чего-то), а также давать пользователю права доступа только к запросам такого типа. Вся информация о сотрудниках и внешних контактах концентрируется в специализированном разделе интерфейса — «Досье на персону». В нем сосредоточены все данные по активности персоны и инструменты для более глубокого анализа: граф связей, библиотека скриншотов, информация об активности на рабочем месте, используемых приложениях, веб-ресурсах и устройствах, а также данные об аномальном поведении. На основе информации в «Досье» можно мгновенно создать сводный отчет по персоне за требуемый период и отобразить его в веб-интерфейсе или выгрузить в PDF-файл и при необходимости распечатать.

Единый интерфейс Solar Dozor позволяет мгновенно переходить к интересующему событию или документу (концепция drill-down — «углубление в данные»). Это дает возможность оперативно анализировать обстановку, проводить сложные расследования и минимизировать ошибки, связанные с человеческим фактором.

Качество расследований в компаниях, имеющих сеть филиалов, может быть улучшено за счет использования возможностей работы в филиальной структуре (модуль MultiDozor). Благодаря

единому досье возможно осуществлять мониторинг групп особого контроля и проводить сквозные расследования по всей сети филиалов. Solar Dozor может интегрироваться с внешними ИТ-системами, такими как SIEM, SWG, HRM, MDM, IdM/IGA, для получения контекстной информации о сотрудниках и инцидентах. Начиная с версии Solar Dozor 7.11, реализован интеграционный модуль MultiConnector, который представляет собой набор коннекторов для удаленного управления политиками, событиями и инцидентами DLP-системы. Его возможности позволяют реализовать многие задачи администратора DLP-системы в консоли SIEM-, IRP-, SOAR-, XDR-систем.

Работа в территориально распределенном режиме

Офицеры безопасности, работающие в крупных территориально распределенных организациях с филиальной сетью, сталкиваются с трудноразрешимой проблемой — им очень сложно увидеть полную и актуальную картину происходящих процессов во всей организации. Часто имеющиеся данные по филиалам фрагментированы, отражают события ретроспективно или с задержкой по времени. Это может привести к запоздалой реакции на инцидент или ошибочным решениям по его отработке. Более того, инцидент может затрагивать сотрудников нескольких филиалов, но обнаружить их потенциально незаконную связь с помощью локальных инсталляций DLP-системы — сложная и трудоемкая задача.

Для решения этих проблем был реализован новый модуль — MultiDozor. Он объединяет разрозненные инсталляции Solar Dozor в единую логическую структуру, предоставляя офицерам безопасности принципиально новые инструменты и возможности для обеспечения информационной и экономической безопасности организации. Например, MultiDozor позволяет в режиме реального времени централизованно контролировать процессы, получать аналитику и мониторить группы особого контроля в разрезе всей организации. Не менее важная функция, которую не могут предоставить другие DLP-системы, — сквозные расследования по всей сети филиалов.

Данные событий и инцидентов хранятся в базах данных, развернутых в подкластерах организационных единиц. При этом сохраняется возможность их хранения в базе данных, развернутой на общих ресурсах головной организации. Такой подход позволяет гарантировать сохранность банковской тайны, выполнить требования регулятора и внутренней нормативной документации.

Сбор данных осуществляется локально в филиалах с помощью агентов на рабочих местах пользователей (Dozor Endpoint Agent). MultiDozor позволяет передавать собранные данные на общекорпоративные ресурсы для централизованного анализа и хранения. Снимки экранов, которые делает агент, могут храниться на локальных ресурсах филиалов и по запросам отображаться в интерфейсе пользователей, что позволяет значительно снизить нагрузку на корпоративную сеть. Снижение нагрузки при обработке данных в распределенных инсталляциях Solar Dozor происходит также за счет настройки информационных объектов, специфичных для филиалов.

Кроме этого, MultiDozor позволяет централизованно настраивать и распространять политики безопасности в филиалы организации. Это значительно облегчает управление системой и экономит ценное время, которое можно потратить на разбор инцидентов и проведение расследований.

Система позволяет вести централизованный контроль пользователей — офицеров безопасности, работающих в филиалах, — за счет использования журнала регистрации действий.

1.2. Решаемые задачи

Задачи, решаемые с помощью Solar Dozor, можно разделить на 5 основных групп:

Информационная безопасность

- Защита от утечек информации.
- Контроль передачи и хранения информации.
- Проведение расследований инцидентов и выявление причин нарушений.
- Профилактика инцидентов ИБ.

Экономическая безопасность

- Выявление признаков корпоративного мошенничества.
- Мониторинг коммуникаций по ключевым сделкам.
- Мониторинг непрерывности ключевых бизнес-процессов.
- Мониторинг коммуникаций с контрагентами.
- Выявление и мониторинг групп риска (должники, игроманы, транжиры и т. д.).
- Проведение расследований и сбор доказательной базы.

Борьба с коррупцией

- Управление конфликтом интересов.
- Выявление признаков аффилированности и проведение расследований.
- Выявление фактов вымогательства и получения взяток.
- Выявление и мониторинг групп риска (друзья, охотники, старослужащие и т. д.).

Внутренний контроль

- Выявление конфликтов интересов.
- Контроль исполнения управленческих решений.
- Контроль реакции на приказы и распоряжения.
- Выявление лоббирования управленческих решений.
- Выявление сокрытия нарушений.
- Контроль климата в коллективе.
- Контроль рабочего времени.
- Выявление фактов саботажа.
- Оценка соответствия регламентам (кодексам, стандартам, законам).

Внутренняя безопасность

- Выявление компрометирующих связей (с конфликтно уволенными, конкурентами, криминалом).
- Выявление признаков вербовочных разработок (разведка, шпионаж).
- Выявление распространителей слухов и инсайдеров.
- Выявление сокрытия нарушений режима охраны.
- Дезинформация получателя информации.
- Компрометация источника и ранее полученной информации.
- Профилактика экстремизма и терроризма.

1.3. Примеры применения по отраслям

Банки и финансы

- Предотвращение утечек баз данных клиентов, PAN, персональных данных и внутренних регламентов безопасности, стратегических и тактических планов, инсайдерской информации (слияния, поглощения, назначения, открытие новых точек и т. д.).
- Выявление признаков кредитного мошенничества, коррупции в сфере закупок, фактов вымогательства и дачи взяток.
- Выявление и мониторинг групп риска (сектанты, игроманы, должники, транжиры и т. д.).
- Проверка кадрового резерва.

Государственные органы

- Предотвращение утечек служебной информации (ДСП), персональных данных граждан, информации из государственных информационных систем.
- Выявление и мониторинг групп риска (сектанты, игроманы, должники, транжиры и т. д.).
- Выявление признаков коррупции при закупках и принятии решений.
- Предотвращение разглашения служебной информации на веб-ресурсах.
- Предотвращение нелегитимной передачи информации СМИ.
- Выявление фактов нарушения правил хранения информации ограниченного доступа на рабочих станциях сотрудников.
- Пресечение рабочей переписки через публичные сервисы электронной почты, мессенджеры, социальные сети.
- Выявление фактов саботажа и неисполнения служебных обязанностей.
- Проверка кадрового резерва.

Добывающая промышленность, нефтегазовая отрасль

- Предотвращение утечек информации ограниченного доступа, стратегических и тактических планов, инсайдерской информации (слияния, поглощения, назначения и т. д.).
- Предотвращение утечек информации в СМИ (об авариях, экологической обстановке, утилизации отходов).
- Выявление и мониторинг групп риска (сектанты, игроманы, должники, транжиры и т. д.).
- Выявление признаков коррупции в сфере закупок (закупки ГСМ, оборудования, инструмента), работы с аффилированными компаниями, фактов вымогательства и дачи взяток.
- Выявление фактов сокрытия аварий и чрезвычайных ситуаций.
- Выявление фактов саботажа и неисполнения служебных обязанностей.
- Проверка кадрового резерва.

Обрабатывающая промышленность

- Предотвращение утечек интеллектуальной собственности (чертежи, проектная документация, ноу-хау), стратегических и тактических планов, инсайдерской информации (слияния, поглощения, назначения, используемые АСУ ТП и т. д.).
- Предотвращение утечек информации в СМИ (о фактах аварий, экологической обстановке и т. д.).
- Выявление фактов саботажа и неисполнения служебных обязанностей.
- Выявление фактов сокрытия аварий и чрезвычайных ситуаций.
- Выявление и мониторинг групп риска (сектанты, игроманы, должники, транжиры и т. д.).
- Выявление признаков коррупции в сфере закупок, фактов вымогательства и дачи взяток, мошенничества с дебиторской задолженностью.
- Выявление фактов мошенничества на производстве (отбраковка продукции, подставные компании, использование ресурсов в личных целях).
- Проверка кадрового резерва.

Предприятия оборонно-промышленного комплекса

- Разглашение сведений о выполняемом государственном оборонном заказе.
- Выявление конфликта интересов при реализации государственного оборонного заказа.
- Выявление признаков коррупции в сфере закупок, фактов вымогательства и дачи взяток, мошенничества с дебиторской задолженностью.
- Предотвращение утечек служебной информации (ДСП), секретов производства, материалов конструкторской и эксплуатационной документации на изделия.
- Выявление фактов нарушения правил хранения информации ограниченного доступа на рабочих станциях сотрудников.
- Выявление рабочей переписки через публичные сервисы электронной почты, мессенджеры, социальные сети.
- Выявление и мониторинг групп риска (сектанты, игроманы, должники, транжиры и т. д.).
- Выявление признаков вербовочных разработок, фактов шпионажа и саботажа, интереса к секретоносителям.
- Выявление фактов нерегламентированного общения и передачи непубличных данных СМИ.
- Выявление фактов сокрытия аварий и чрезвычайных ситуаций.
- Проверка кадрового резерва.

Энергетика

- Предотвращение утечек информации служебной информации (ДСП), персональных данных граждан, стратегических и тактических планов, инсайдерской информации (слияния, поглощения, назначения, модернизация объектов, используемые АСУ ТП и т. д.).
- Выявление признаков коррупции в сфере закупок, продвижения аффилированных поставщиков, фактов вымогательства и дачи взяток.

- Выявление признаков мошенничества в сфере продаж, при выполнении ремонтных работ, фактов воровства оборудования.
- Предотвращение утечек информации в СМИ (о фактах аварий, экологической обстановке и т. д.).
- Выявление фактов сокрытия аварий и чрезвычайных ситуаций.
- Выявление и мониторинг групп риска (сектанты, игроманы, должники, транжиры и т. д.).
- Проверка кадрового резерва.

Ритейл

- Выявление признаков коррупции в сфере закупок (например, сговор закупщиков/мерчандайзеров с поставщиками или производителями), фактов вымогательства и дачи взяток (например, за место на полке), мошенничества с дебиторской задолженностью.
- Предотвращение утечек стратегических и тактических планов, инсайдерской информации (слияния, поглощения, назначения, открытие новых точек, условия работы с поставщиками и т. д.).
- Выявление и мониторинг групп риска (сектанты, игроманы, должники, транжиры и т. д.).
- Выявление фактов воровства со склада.
- Выявление фактов махинации с картами лояльности.
- Проверка кадрового резерва.

Фармацевтика и фармдистрибуция

- Предотвращение утечек документов на патентование интеллектуальной собственности, промежуточных результатов клинических исследований, протоколов о намерениях и договоров с фармдистрибьюторами, стратегических и тактических планов, инсайдерской информации (слияния, поглощения, назначения и т. д.).
- Выявление и мониторинг групп риска (сектанты, игроманы, должники, транжиры и т. д.).
- Выявление признаков коррупции в сфере закупок, работы с аффилированными компаниями и фактов вымогательства.
- Выявление фактов воровства и употребления медицинских препаратов.
- Проверка кадрового резерва.

Транспорт

- Предотвращение утечек персональных данных, служебной информации (ДСП), стратегических и тактических планов, инсайдерской информации (слияния, поглощения, назначения, используемые АСУ ТП и т. д.).
- Выявление и мониторинг групп риска — сектанты, игроманы, должники, транжиры и т. д.
- Выявление признаков мошенничества с дебиторской задолженностью, материалами (закупка ГСМ, оборудования, инструмента).
- Выявление фактов саботажа и неисполнения служебных обязанностей, сокрытия аварий, нарушения правил безопасности.

- Выявление коррупции в сфере закупок и фактов вымогательства, признаков мошенничества при выполнении ремонтных работ.
- Проверка кадрового резерва.

Телекоммуникации

- Предотвращение утечек персональных данных, служебной информации (ДСП), стратегических и тактических планов, инсайдерской информации (слияния, поглощения, назначения, открытие новых точек и т. д.).
- Выявление и мониторинг групп риска (сектанты, игроманы, должники, транжиры и т. д.).
- Выявление фактов воровства оборудования, сокрытия аварий.
- Выявление признаков коррупции в сфере закупок, мошенничества с дебиторской задолженностью и фактов вымогательства.
- Проверка кадрового резерва.

1.4. Интерфейс

Взаимодействие с Solar Dozor осуществляется через единую консоль управления, доступную из веб-браузера. Ее интерфейс организован по принципу ситуационного центра и позволяет службе безопасности оперативно оценить обстановку, выделить приоритетные направления работы и начать расследование инцидентов.

Для работы с Solar Dozor не требуются глубокие технические знания, поэтому с системой могут работать не только ИТ- и ИБ-специалисты, но и офицеры экономической и внутренней безопасности, а также представители других отделов. Возможности быстрого поиска без составления сложных поисковых запросов позволяют мгновенно проверять гипотезы и экономить ценное время.

Интерфейс адаптирован для работы как на персональных, так и на планшетных компьютерах. Поддерживается разрешение вплоть до 4К. Доступны русский или английский языки интерфейса, между которыми можно мгновенно переключиться в любой момент. Интеграция с Microsoft Active Directory (а также FreeIPA, ALD Pro) позволяет осуществлять вход в Solar Dozor без ввода логина и пароля — в этом случае используются данные входа в операционную систему.

Для удобства пользователей в интерфейсе Solar Dozor реализована интерактивная справка, которую можно открыть в любое время. В ней объяснены и с помощью соответствующих скриншотов наглядно показаны все функции системы.

Так как задачи офицера безопасности и их руководителя различаются, в Solar Dozor реализованы две версии рабочего стола: для аналитика и для руководителя.

Рабочий стол аналитика

Рабочий стол аналитика спроектирован с учетом потребностей офицеров безопасности, занимающихся настройкой политик безопасности, работой с инцидентами или проведением расследований.

Удобные виджеты на рабочем столе отражают самые нужные данные без необходимости строить сложные поисковые запросы, а принцип drill-down («углубление в данные») позволяет получить расширенную информацию по событиям, персонам, информационным объектам и инцидентам.

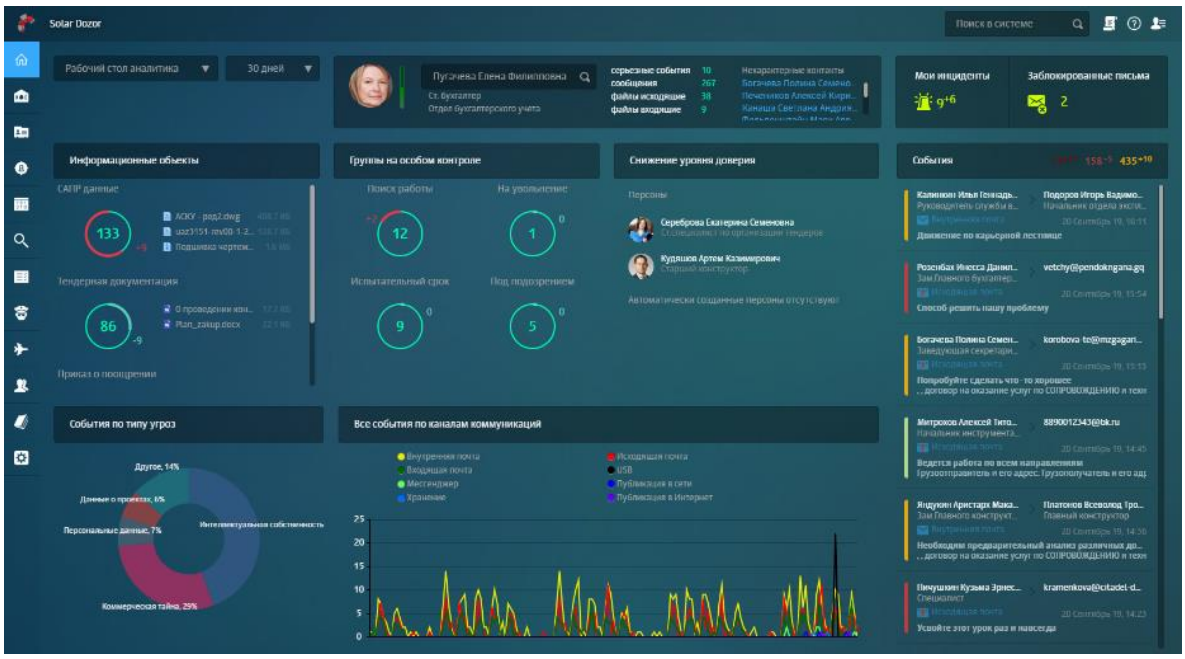


Рисунок 2. Рабочий стол аналитика

Для оперативной оценки обстановки Рабочий стол аналитика обращает внимание офицера ИБ на самые важные метрики:

- Критически важная для бизнеса информация;
- Персоны и группы персон на особом контроле;
- Нарушения (события и инциденты ИБ).

Благодаря такому подходу офицер безопасности может быстро оценить текущую обстановку и выбрать приоритетные задачи для подробного разбора. После этого он может углубиться в детали, сделав буквально пару кликов, — практически все элементы интерфейса являются интерактивными гиперссылками.

Например, нажав на строку с именем файла, можно перейти в карточку события, связанного с файлом; нажав на имя сотрудника, — перейти на карточку персоны.

Чтобы получить нужную информацию, не следует каждый раз писать поисковый запрос — в Solar Dozor уже предустановлены готовые срезы наиболее востребованных данных и отчетов. Функция «Хлебные крошки» позволяет просматривать последние посещенные страницы и быстро переходить по ним, не теряя нить расследования. Система отображает 10 последних активностей, к которым можно вернуться в один клик и не тратить время, пытаясь восстановить в памяти предыдущие события.

Система управления инцидентами Solar Dozor превращает расследование из головной боли службы безопасности в удобный и эффективный процесс ежедневной работы. Управляя жизненным циклом инцидента, система позволяет назначать ответственного за проведение расследования, контролировать его ход и получать результаты в кратчайшие сроки.

Система создания отчетов позволяет отправлять по электронной почте сводки руководителям и другим заинтересованным лицам. Отчеты генерируются как разово, так и по расписанию.

Рабочий стол руководителя

Рисунок 3. Рабочий стол руководителя

Рабочий стол руководителя предназначен для руководителей подразделения ИБ или бизнес-заказчиков DLP-системы. С его помощью можно отслеживать динамику изменений основных показателей угроз, эффективно управлять командой аналитиков и оперативно получать информацию для принятия решений.

Графические виджеты Рабочего стола руководителя отображают данные, необходимые для быстрой оценки ситуации и корректировки работы аналитиков, проводящих разбор инцидентов:

- «Группы на особом контроле» — топ-5 групп особого контроля;
- «Информационные объекты» — топ-5 информационных объектов, передаваемых в компании;
- «Нарушители» — топ-5 персон на особом контроле;
- «Общие показатели» — статистика по событиям ИБ за выбранный период;
- «Офицеры ИБ» — статистика обработки событий офицерами ИБ;
- «Подразделения» — топ-5 групп «Организационной структуры»;
- «Последние построенные отчеты» — 3 последних построенных отчета;
- «События по каналам коммуникации» — статистика по количеству событий за период с группировкой по каналам коммуникации;
- «События по критичности» — статистика событий по критичности угроз;
- «События по типу угроз» — самые критические события по типу угроз;
- «Файлы» — топ-5 файлов, передаваемых в компании;
- Фильтр по тенденциям — изменение показателей за заданный период времени.

1.5. Соответствие требованиям регуляторов

Solar Dozor разработан в России с применением собственных запатентованных технологий, внесен в Единый реестр отечественного ПО (№ 1480), сертифицирован ФСТЭК России как программное средство защиты от неправомерной передачи из информационной системы информации, не содержащей сведения, составляющие государственную тайну, и соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) по 4-му уровню контроля и технических условий (сертификат соответствия № 4459).

Для государственных организаций, ФОИВ, РОИВ и предприятий ВПК

Внедрение Solar Dozor обеспечит соответствие:

- отраслевым требованиям в качестве компенсирующей меры для обеспечения безопасности информации в части контроля потоков данных по требованиям к защите персональных данных (152-ФЗ «О персональных данных», Постановление Правительства № 1119 «Об утверждении требований к защите персональных данных»);
- Приказам ФСТЭК России № 21 и № 17 (меры РСБ.1, РСБ.2, РСБ.3, РСБ.5, РСБ.7, РСБ.8, ОЦЛ.5, ОЦЛ.8, ИНЦ.2, ИНЦ.3).

Для организаций кредитно-финансовой сферы

Применение Solar Dozor обеспечит соответствие отраслевым требованиям:

- Стандарта Банка России СТО БР ИББС;
- Положения Банка России от 09.06.2012 № 382-П;
- ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

1.6. Преимущества

Быстрый результат и развитая визуальная аналитика

- Единый удобный интерфейс значительно ускоряет работу.
- Инструменты визуализации и срезы данных облегчают оценку ситуации.
- Можно мгновенно переходить к нужным массивам данных.
- Аномалии поведения подкрепляются данными по рабочему времени и перемещаемым информационным объектам.
- Сводные отчеты позволяют быстро понять ситуацию с внутренними угрозами.
- Встроенные инструменты анализа данных избавляют от использования сторонних систем (Excel, BI и т. д.).
- Ретроспективное сканирование архива электронной почты выявляет нарушения до внедрения DLP.

Эффективные перехват и блокирование

- Перехват основного трафика на сетевом шлюзе снижает нагрузку на рабочие станции сотрудников.
- Возможность установки «в разрыв» трафика обеспечивает блокирование утечек даже при больших потоках трафика.

- Возможность уведомления сотрудника при срабатывании DLP формирует культуру кибербезопасности.
- Изменение и/или удаление содержимого сообщений электронной почты предотвращает утечки и позволяет проводить оперативные комбинации.

Удобные инструменты для расследований

- Для работы не требуются знания в области ИТ и опыт построения поисковых запросов.
- Инструменты кейс-менеджмента позволяют управлять жизненным циклом инцидента на всех этапах расследования.
- Ведение полного нереляционного архива коммуникаций сотрудников и продвинутые поисковые технологии.
- Быстрый поиск в любом окне интерфейса позволяет мгновенно находить информационные объекты и инциденты.
- Продуманное взаимодействие между несколькими аналитиками, отдельный рабочий стол руководителя.
- Инцидентная модель реализована в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

Снижение ложных срабатываний

- Мониторинг сотрудников и контроль данных обеспечивают превентивное обнаружение угроз.
- Внимание аналитика фокусируется на наиболее опасных сотрудниках и потенциальных угрозах.
- События и инциденты легко фильтруются и сортируются для максимального сужения выборки.
- Данные размечаются тегами по аналогии с поисковиками и социальными сетями.

Производительность

- Выдерживает нагрузки в 300 000+ пользователей (результаты получены практическим путем на крупных внедрениях системы).
- Встраивается в любую инфраструктуру без конфликтов с другим ПО или изменения архитектуры и организационных процессов.
- Позволяет реализовать любую программу хранения в соответствии с имеющимися мощностями и планами по масштабированию.
- Поддерживает модель здоровья Zabbix.

Гибкость и стабильность

- На лету перехватывает и архивирует данные для анализа.
- Подтвержденная нагрузка на укладку в архив — 3 ТБ в сутки.
- Рекордные сроки хранения архива коммуникаций — свыше 1000 ТБ сроком 10+ лет.
- Количество контролируемых пользователей — 300 000+.
- Быстрый поиск — меньше секунды в архиве на 17 млн сообщений.

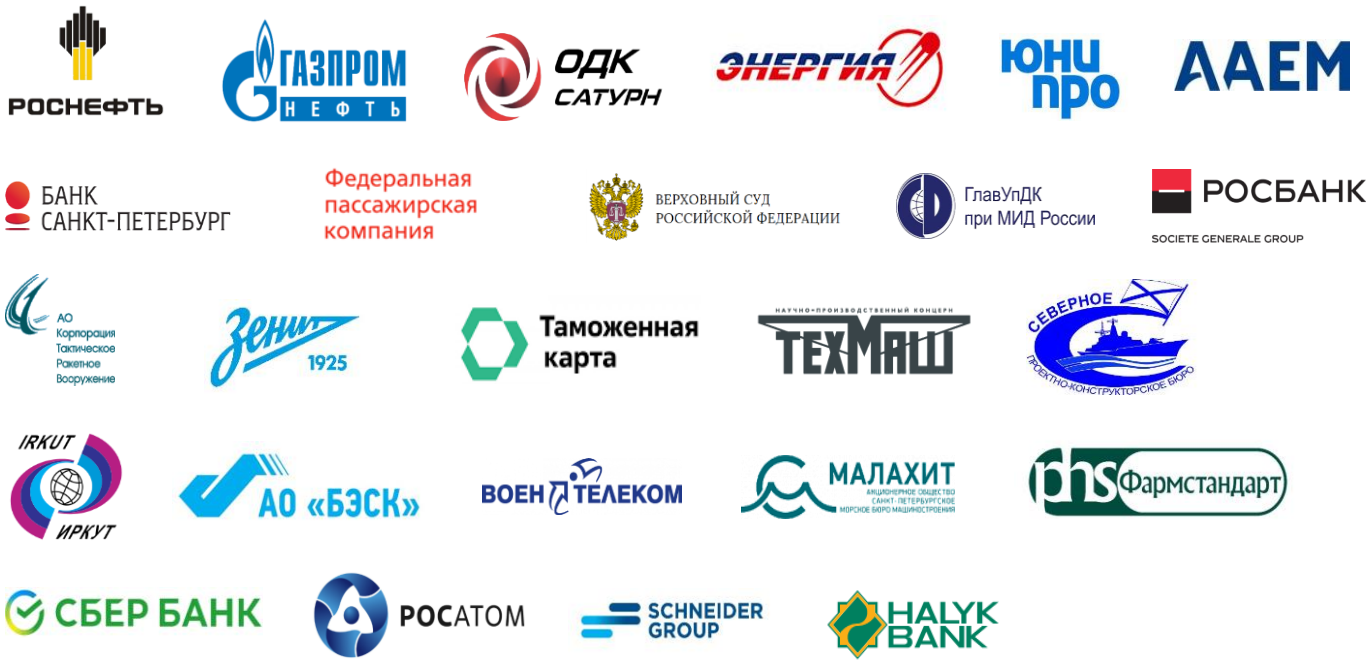
Высокая экспертиза команды

- 20+ лет развития продукта с учетом российской специфики.
- Крупнейшая команда по DLP в России — 120+ профильных специалистов.
- Отработанная методология внедрения и эксплуатации DLP-системы.
- 300+ внедрений в крупнейших коммерческих и государственных организациях.

Подходит для импортозамещения

- Все модули поддерживают работу на ОС GNU/Linux.
- Полнофункциональный агент для ПК с ОС Linux.
- Участник Единого реестра отечественного ПО (№ 1480).
- Сертификат соответствия ФСТЭК России № 4459 по 4-му уровню контроля отсутствия недекларированных возможностей и техническим условиям.

1.7. Ключевые заказчики



2. Предотвращение утечек информации

Ключевая функция Solar Dozor — автоматическое обнаружение нелегитимного перемещения или хранения конфиденциальной информации. Для этого применяются комплексные правила хранения, обработки и передачи информации, с помощью которых можно выполнять любые сценарии ее обнаружения и блокирования. Совокупность этих правил образует политику ИБ.

2.1. Политика информационной безопасности

Перехваченная информация пересылается в основной модуль Solar Dozor и подвергается контентному и контекстному анализу. При этом анализу подвергается не только текст сообщения и его вложенных частей, но и текст вложенных файлов (включая распознавание нескольких типов графических объектов в изображениях), а также печатей, платежных карт и паспортов РФ. Для всех вложенных частей сообщения проводится анализ форматов и по его результатам ведется дальнейшая обработка сообщения в соответствии с политикой фильтрации.

К каждому сообщению фильтр применяется столько раз, сколько указано адресатов, так как применяемые алгоритмы обработки зависят от получателя. Например, конфиденциальное внутрикорпоративное сообщение, отправленное директору и представителю сторонней организации, должно быть доставлено первому адресату, но заблокировано для второго.

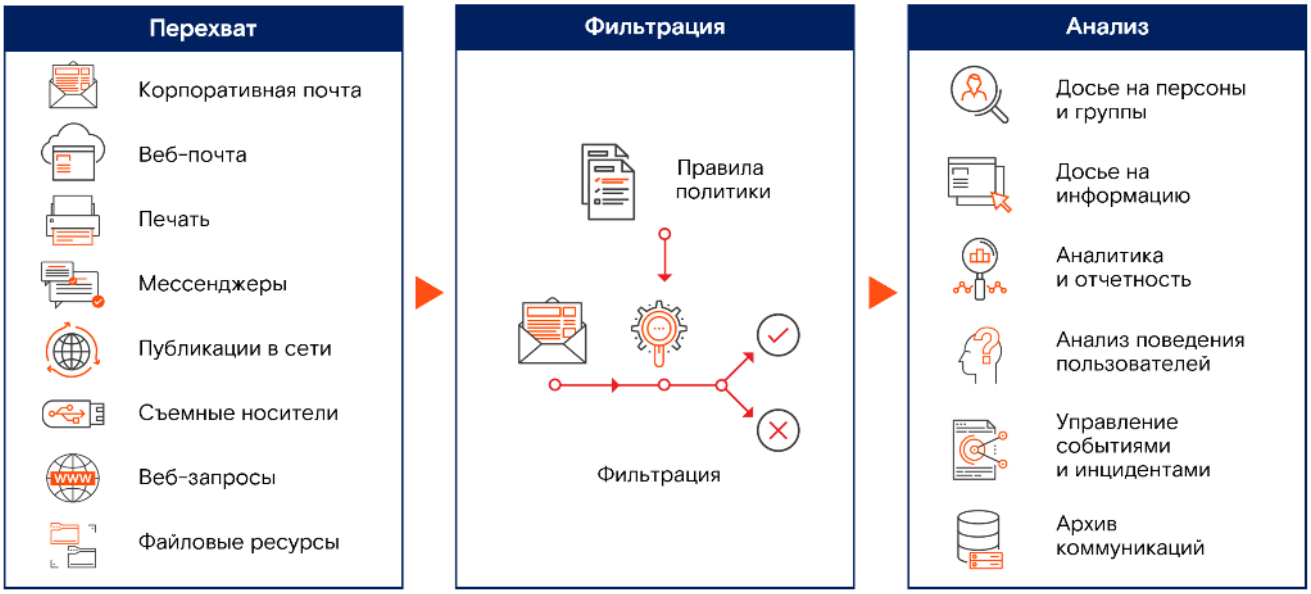


Рисунок 4. Принцип работы

Заданные правила политики ИБ позволяют генерировать и интерпретировать события ИБ, автоматически соотнося их с актуальным типом угроз для конкретной организации. Зная тип угрозы, офицер безопасности сможет оценить ее критичность и потенциальный ущерб. По умолчанию в Solar Dozor реализованы следующие типы угроз:

- Конфиденциальные данные (персональные данные, коммерческая тайна, финансовые сведения, интеллектуальная собственность, разглашение информации ДСП и т. д.);
- Организационные сведения;
- Подозрительная активность (поиск работы, аномальное поведение, использование криптографии и т. д.);
- Неправомерное использование ресурсов (посторонняя активность, нецелевое использование рабочего времени и т. д.);

- Проблемные бизнес-задачи (распоряжение руководства, авария, отказ, и т. д.);
- Намеренные нарушения (утечка конфиденциальной информации, неправомерный доступ к информации, мошенничество с помощью ИТ, саботаж или физический ущерб и т. д.);
- Случайные нарушения (неосторожные действия, отказ ПО или аномальное поведение бизнес-приложений и т. д.);
- Ошибки (операционные, в эксплуатации аппаратных средств и т. д.).

Solar Dozor позволяет увидеть взаимосвязи объектов и при необходимости быстро перейти к связанным объектам по имеющимся ссылкам. При этом можно перейти как к самому элементу набора правил (правилу, условию, шаблону документов, профилю отправки и т. п.), так и к тем элементам, при описании которых используется текущий набор правил.

Срабатывания внутри сообщений подсвечиваются, помогая быстро понять, где и почему сработало то или иное правило политики ИБ.

2.2. Возможности блокирования и изменения сообщений

В зависимости от задач заказчика, Solar Dozor может работать как в режиме мониторинга, так и в режиме блокировки передачи данных. Система не только фиксирует нарушения, но и предотвращает кражу и утечку конфиденциальных данных. В случае блокировки сообщения Solar Dozor также может выводить пользователю окно с предупреждением о нарушении политики безопасности.

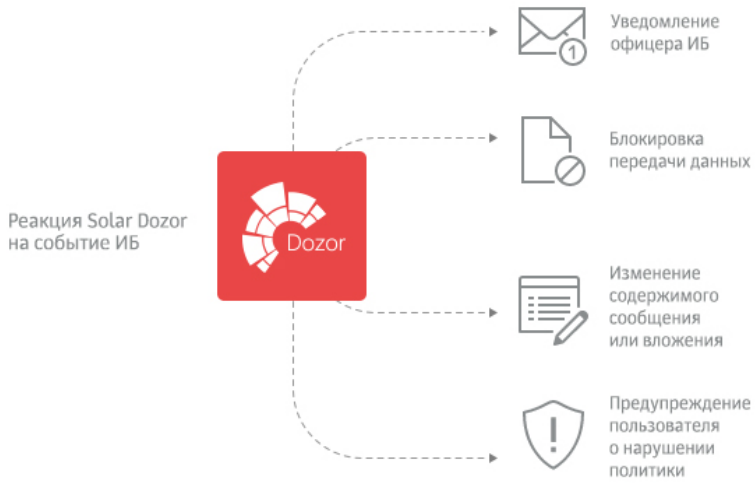


Рисунок 5. Возможная реакция Solar Dozor на потенциальную утечку

Кроме непосредственной блокировки сообщения электронной почты с конфиденциальной информацией Solar Dozor также может вносить изменения в почтовые заголовки и MIME-части сообщения (функция «реконструкция сообщений») — **исключать или заменять необходимую информацию**. Это позволяет проводить оперативные комбинации, когда злоумышленники не подозревают, что полученный документ содержит неверную информацию, а служба безопасности не только знает о попытке утечки, но и получает инструменты для дальнейших действий — выявления внешних и внутренних злоумышленников, определения заказчиков утечки, связи злоумышленников со СМИ и т. д.

2.3. Информационные объекты

Для контроля распространения конфиденциальной информации в Solar Dozor используется сущность «информационный объект». Она описывает класс информации, которая крайне важна для бизнеса и требует особого внимания со стороны службы безопасности. Например, к ней

относятся финансовые документы, персональные данные, стратегические планы, протоколы совещаний и т. п. Такая информация может передаваться в виде электронных документов или отсканированных изображений, в тексте сообщения или внутри архивов. По этой причине имеет смысл задать как можно больше разных представлений таких данных, сгруппировав их по общим критериям.

Например, для мониторинга и контроля движения финансовых документов можно объединить соответствующие информационные объекты в категорию «Финансовые документы». Информационные объекты, содержащие документы, с которыми работают специалисты кадрового отдела, объединяются в категории «Кадровый отдел». К объектам из разных категорий можно применить разные правила контроля.

Для идентификации информационных объектов в Solar Dozor реализованы технология цифровых отпечатков (DIFI, digital fingerprints), технология контроля идентификаторов (IDID, ID identification), графический шаблон, а также шаблоны документов, разбор конструкторской документации и инструменты контроля архивов.

DIFI

С помощью технологии DIFI осуществляется сравнение текстовых, графических и табличных данных с эталонными документами. Это позволяет находить как полностью, так и частично скопированные документы. Например, в случае графического изображения соответствие эталону можно установить после трансформации, поворота на любые углы и изменения четкости. Отпечатки с табличных документов помогают выявить комбинацию строк из таблицы-эталона и даже единственную строку.

DIFI позволяет обнаруживать:

- **Текстовые документы** (планы, уставы, приказы, типовые договоры, тендерные документы и т. д.);
- **Табличные данные** (базы клиентов, персональные данные и т. д.);
- **Графические документы** (сканы, фотографии, чертежи и т. д.);
- **Формы и анкеты**;
- **Стандартные элементы ГОСТ** и документов внутреннего стандарта;
- **Печать-гриф** («конфиденциально», «копия», «ДСП», и т. д.);
- **Элементы фирменного стиля** (шаблоны документов, логотипы и т. д.);
- **Подписи и факсимиле**.

IDID

Технология IDID распознает в тексте сообщений специальные идентификаторы. Ими являются последовательности цифр или букв, однозначно определяющие данные, интересные в контексте ИБ — контроля утечек информации и работы с персональными данными.

IDID позволяет обнаруживать:

- Банковские реквизиты (БИК, ОКАТО и т. д.);
- ИНН налогоплательщика;
- Имена;
- Номера пластиковых карт;
- Паспортные данные;
- СНИЛС;

- Email, URL, IP;
- Слова и фразы определенной тематики;
- Другие идентификаторы.

Графический шаблон

С помощью этого инструмента система с достаточной точностью распознает в изображениях:

- Паспорт РФ: разворот 3-ей страницы, содержащей персональные данные;
- Печати организаций (круглую и треугольную);
- Лицевую и оборотную стороны платежной карты.

Для распознавания объектов задействована специальная система глубокого обучения на основе нейронных сетей Faster RCNN (region-based convolutional neural networks). Объекты распознаются с учетом различных деформаций (растяжения, поворота, наложения на другие объекты), а также при полном отсутствии текстовой составляющей.

Офицер безопасности может настраивать графический шаблон под выполняемые задачи и задавать:

- Режим поиска объектов:
  - **точность** – обеспечивает минимальное количество ложных срабатываний, но объекты, которые распознаются нечетко, обнаружены не будут.
  - **полнота** – позволяет найти больше объектов, но вероятность ложных срабатываний будет выше.
- Необходимое для срабатывания условия политики количество объектов, которые нужно искать в проверяемых сообщениях и файлах.

После формирования графического шаблона офицер безопасности может легко задать правила, по которым сообщения, содержащие заданные в шаблоне объекты, будут перехватываться системой автоматически. По умолчанию на такие сообщения будет установлена пометка с именем соответствующего графического шаблона. Кроме того, в сами сообщения добавится информация о том, где (в каком файле) и сколько графических объектов обнаружено.

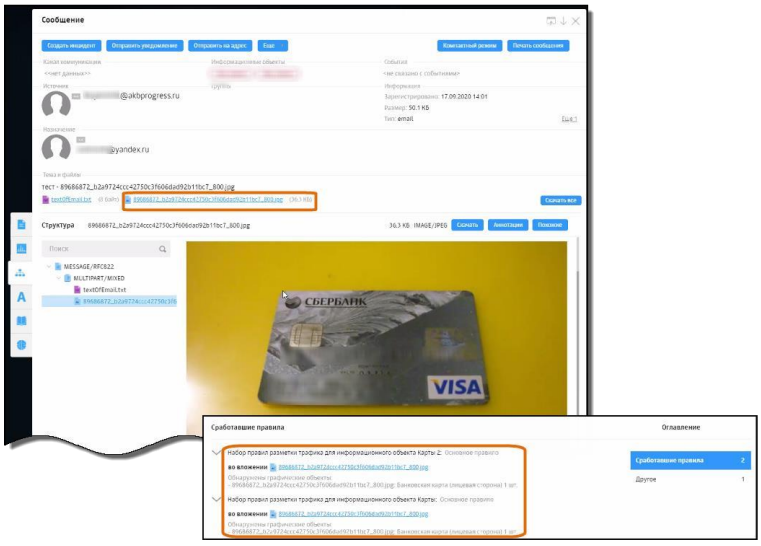


Рисунок 6. Перехваченное сообщение с изображением банковской карты

Шаблоны документов

Шаблоны документов — набор правил проверки текста на наличие или отсутствие определенных образцов. К ним относятся слова или фразы, введенные пользователем, текстовый файл с образцами, а также ключевые фразы или слова, извлеченные из файла с помощью IDID.

Применение шаблонов документов позволяет обнаруживать в большом потоке информации типовые документы с корпоративным стилем, документы бухгалтерского учета в строго определенном формате, как справка о доходах НДФЛ, и т. п.

Конструкторская документация

Solar Dozor может автоматически определять файлы инженерных пакетов CAD-систем и извлекать из них текстовую информацию (данные чертежей, схем, спецификаций, моделей и т. д.). Поддерживаются следующие форматы конструкторской документации: DWG, STL, STEP, ADEM CAD, M3D.

При настройке соответствующих правил при попытке передачи по сети файлов конструкторской документации Solar Dozor проверяет наличие в них конфиденциальных данных и при их обнаружении запрещает передачу.

Офицер безопасности может просматривать все текстовые данные инженерных файлов без использования соответствующих программ.

Архивы

Solar Dozor может определять архивы, в том числе защищенные паролем. Перехваченное сообщение с архивом относится к определенной категории и блокируется, после чего создается событие ИБ. Если сотрудники в соответствии с внутренними регламентами шифруют пересылаемую информацию выданным им корпоративным ключом, содержащиеся в архиве файлы будут расшифрованы и проанализированы.

Для реализации такого сценария в Solar Dozor создается справочник ключей, с помощью которых система пробует открыть запароленный архив и проанализировать его содержимое. Архивы, к которым не подошел ни один корпоративный ключ, могут блокироваться, и их дальнейшую судьбу будет решать офицер безопасности. Одновременно возможен поиск дубликатов этих архивов, которые могут обернуться инцидентами.

Практика показывает, что часто пароль к архиву высылается получателю вместе с архивом или же в ближайших сообщениях до или после.

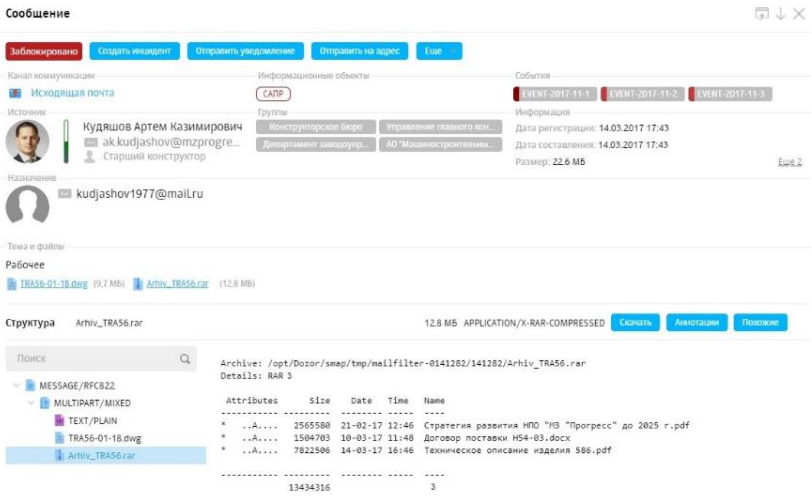


Рисунок 7. Отображение структуры архива в карточке сообщения

Как показывает практика, при шифровании архива подавляющее большинство сотрудников не пользуются опцией «Не показывать названия файлов». Это значит, что Solar Dozor может извлечь и проанализировать структуру архива и названия входящих в него файлов. Извлеченная структура архива сама по себе предоставляет ИБ-специалисту достаточно информации о его одержимом. Уже по структуре архива становится понятно, есть ли смысл заниматься глубоким расследованием данного сообщения или можно допустить его к отправке. Кроме того, извлеченная структура зашифрованного архива представляет собой текст, а значит, доступна для поиска и применения политики фильтрации. Это позволяет проводить расследования при наличии сотен защищенных паролем архивов.

В Solar Dozor можно на уровне рабочей станции заблокировать передачу защищенных паролем или поврежденных архивов – достаточно создать правило политики, в котором задать условие с атрибутами **Защищенный паролем архив** и/или **Поврежденный архив**.

Примечание: *поддерживаются наиболее распространенные форматы архивов: ZIP (.zip), RAR4, RAR5 (.rar), 7-zip (.7z), ARJ.*

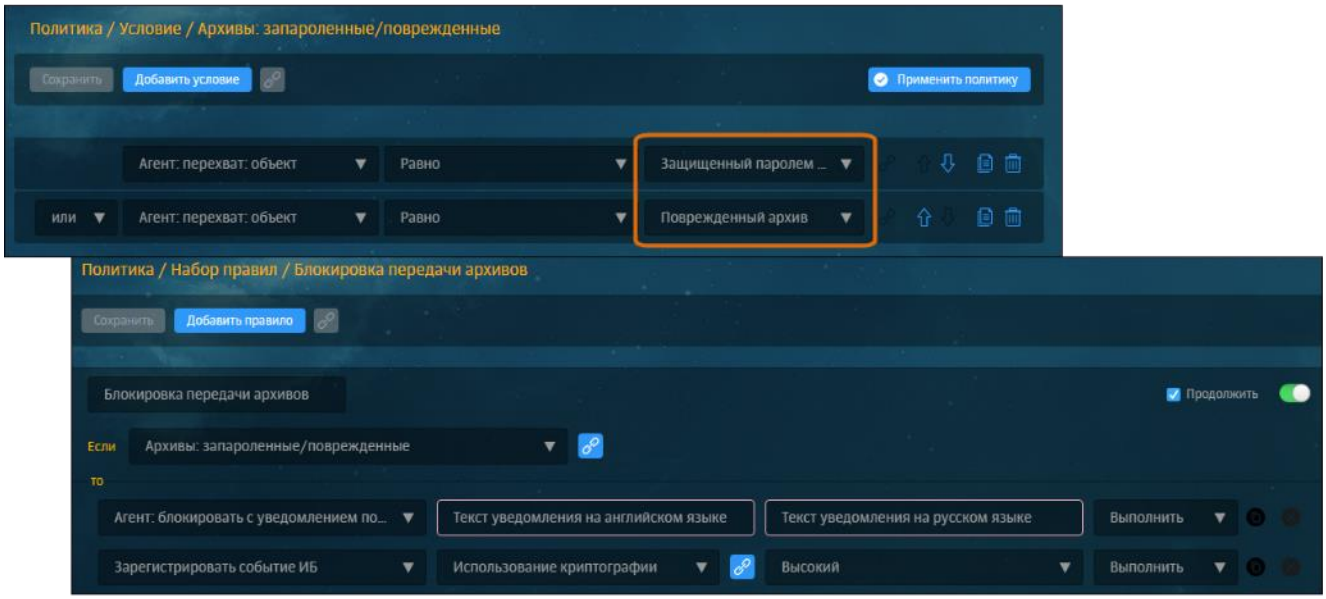


Рисунок 8. Раздел «Политика»: правило блокировки передачи защищенного паролем или поврежденного архива

2.4. Контролируемые каналы коммуникации

2.4.1. Электронная почта

Solar Dozor может контролировать переписку через корпоративные почтовые серверы (Microsoft Exchange, IBM Lotus Notes, CommuniGate и т. д.) и сервисы веб-почты (Яндекс.Почта, Gmail, Mail.ru и т. д.), а также выявлять в трафике сообщения, передаваемые по протоколам IMAP и POP3. Поддерживается 40+ сервисов, использующих протоколы HTTPS, SMTP и POP3. Возможен как пассивный режим работы (снятие трафика), так и активный (установка в «разрыв» трафика).

Возможности Solar Dozor позволяют не только контролировать текущий трафик электронной почты, но и анализировать архив электронной почты до своего внедрения. К системе можно подключить любой облачный и публичный почтовый сервер (Mail.ru, Gmail и т. д.) или сервис электронной почты с поддержкой протокола IMAP. В результате к архиву переписки будут применены политики и правила фильтрации, и офицер безопасности сможет проводить ретроспективный анализ переписки сотрудников.

Анализ архива электронной почты до внедрения Solar Dozor значительно сокращает время получения результатов на пилотных проектах. Обычно уже после первого сканирования служба ИБ получает ценную информацию по совершенным нарушениям и может оценить эффект от внедрения DLP-системы.

2.4.2. Мессенджеры

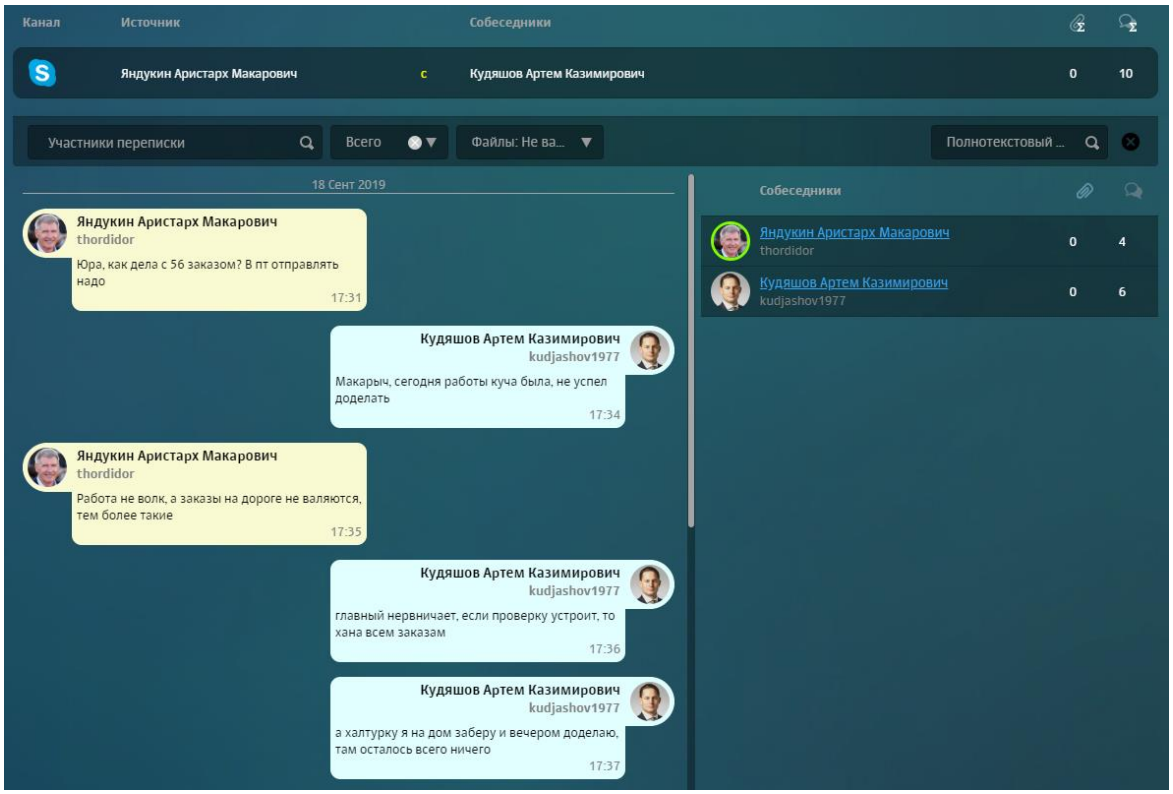


Рисунок 9. Пример восстановленного диалога в мессенджере

С помощью кейлоггера Solar Dozor может перехватывать исходящие сообщения и файлы, пересылаемые через популярные мессенджеры (как для десктопов, так и для веб-версии). При этом сообщения автоматически склеиваются, поэтому временное переключение на другие программы и вкладки браузера не влияет на сохраняемую переписку. Перехват файлов возможен с помощью специальной опции в настройках перехвата: «Приложения, которые считаются средствами передачи данных».

Solar Dozor поддерживает перехват следующих мессенджеров, и этот список постоянно пополняется:

- Telegram;
- WhatsApp;
- Viber;
- Mail.ru Agent;
- Skype 8;
- Skype for business (прежнее название — Microsoft Lync);
- eXpress;
- TrueConf;
- Microsoft Teams;
- RocketChat;

- Element (Matrix);
- Zoom;
- VK Teams.

Примечание: *даже небольшое изменение разработчиками мессенджера протокола обмена данными может привести к неработоспособности перехватчика на стороне агента.*

2.4.3. Веб-трафик и веб-сервисы

Специализированный модуль Dozor Traffic Analyzer совместно с другими решениями, стоящими на периметре сети, поставляющими ему расшифрованный HTTPS-трафик (например, шлюзом веб-безопасности Solar webProxy), позволяет контролировать веб-трафик, в том числе:

- Данные и документы, передаваемые на внешние серверы по протоколу HTTP/HTTPS с помощью браузеров Internet Explorer, Mozilla FireFox, Google Chrome, Opera, Яндекс.Браузер, Atom;
- Сообщения и переписку в социальных сетях Одноклассники, ВКонтакте, Facebook, LinkedIn, Mail.ru, Мой Круг и др.
- Загрузку файлов на видео- и фотохостинги, файлообменники и облачные хранилища (Microsoft One Drive, Яндекс.Диск, Google Drive, Облако Mail.ru);
- Публикации резюме на HH.ru, Job.ru, Zarplata.ru, SuperJob и др.;
- Сообщения на форумах phpBB, IP.board, Phorum, Drupal и др.;
- Публикации в блогах LiveJournal, WordPress, Mamba, Diary.ru, Juick, Imageboard и др.;
- Передачу файлов по HTTP, FTP, FTP over HTTP, WebDAV;
- SMS/MMS-сообщения, отправляемых через специальные сервисы — 500+ доменов;
- POST-запросы;
- Сообщения на веб-сервисах.

2.4.4. USB-устройства

Solar Dozor может контролировать USB-устройства, подключенные к персональным компьютерам сотрудников, пресекая утечки конфиденциальной информации через флешки и переносные диски, в том числе по протоколу MTP (Media Transfer Protocol). Возможна блокировка по черным и белым спискам, типу устройств, их идентификаторам.

Доступно ведение базы экземпляров USB-устройств, которая может пополняться как вручную, так и автоматически — с использованием перехваченных данных об устройствах, которые были подключены к какой-либо рабочей станции в корпоративной сети. При этом USB-устройства группируются по определенным категориям, которые используются для настройки запрета подключения конкретных устройств.

Офицер безопасности может задавать (в том числе, по модели или производителю), какие экземпляры и/или категории USB-устройств разрешено/запрещено подключать конкретному сотруднику/группе персон, либо к определенным рабочим станциям, входящим в конкретную группу. Подробная информация о том, какие USB-устройства пыталась подключить конкретная персона находится в полной карточке этой персоны (раздел Устройства).

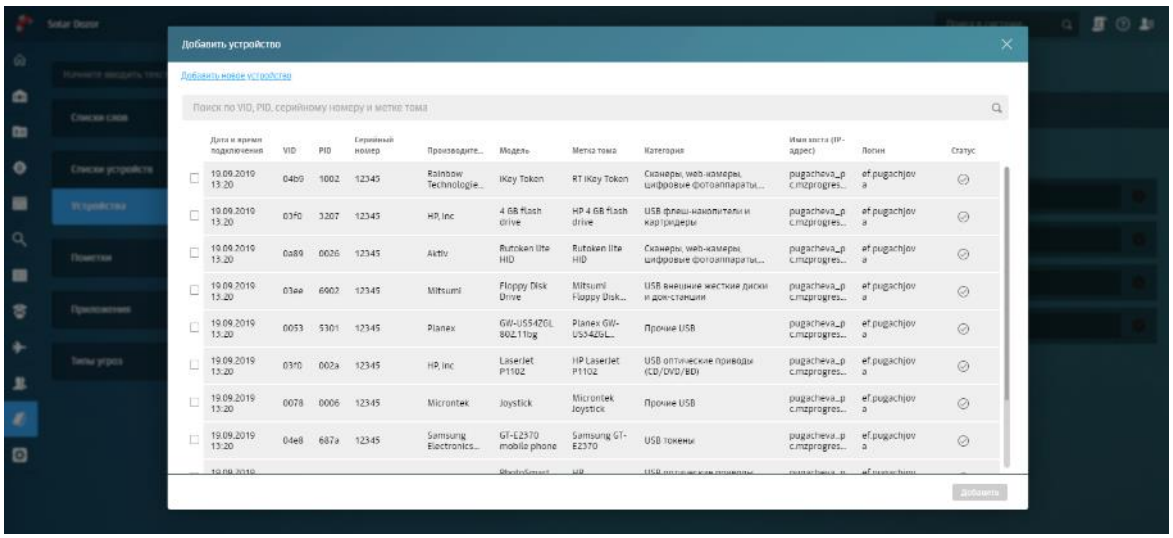


Рисунок 10. Добавление данных в базу экземпляров USB-устройств

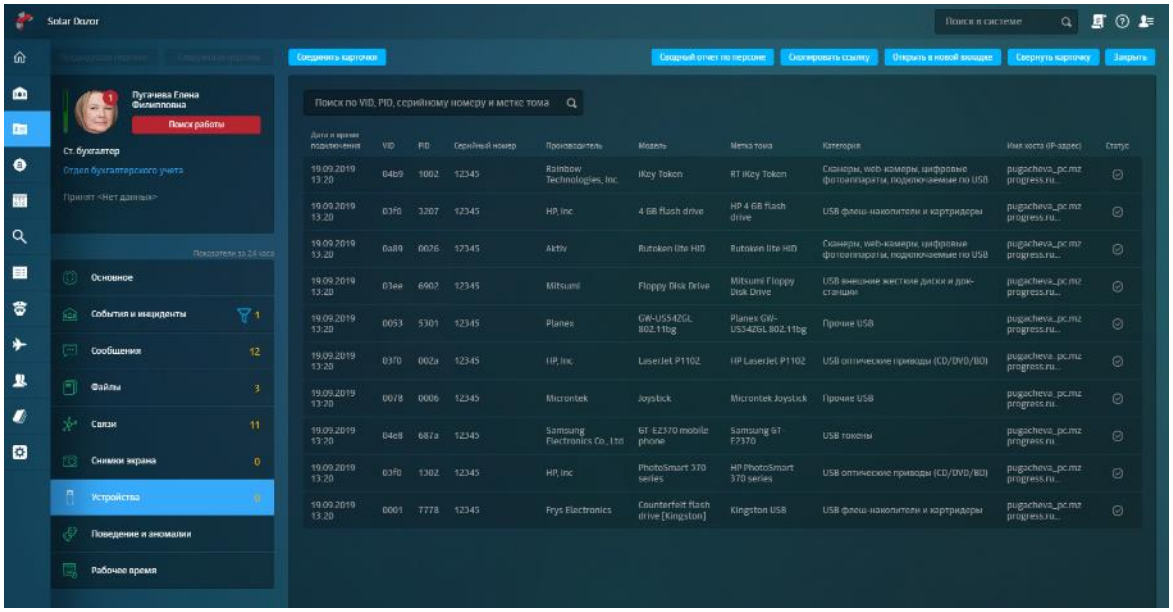


Рисунок 11. Полная карточка персоны, вкладка «Устройства»

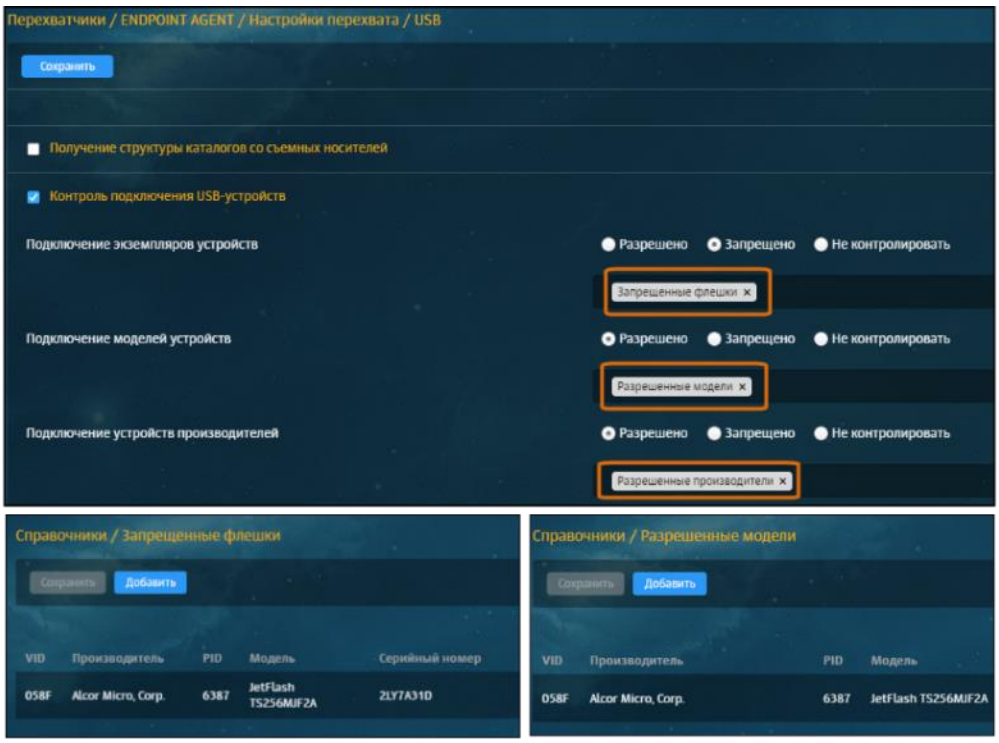


Рисунок 12. Контроль доступа к USB-устройствам по моделям и производителям

2.4.5. Файловые и облачные хранилища

Для предотвращения утечек конфиденциальных данных в корпоративных сетях необходимо контролировать не только каналы передачи информации, но и места ее хранения. Нередко информация ограниченного доступа содержится на ресурсах, не предназначенных для ее размещения: контролируемых и неконтролируемых специалистами по ИБ файловых хранилищах, жестких дисках рабочих станций сотрудников, съемных носителях.

Отследить процесс использования всей защищаемой информации зачастую невозможно — полный список всех узлов и ресурсов корпоративной сети неизвестен, а объемы накапливаемых данных и количество мест их хранения постоянно растут. Кроме того, в настоящее время для хранения информации стали активно использоваться облачные ресурсы, такие как Microsoft OneDrive, Яндекс.Диск, Google Drive, Облако Mail.ru. Это создает условия для случайных и намеренных утечек ценных данных и облегчает злоумышленникам их вывод за контролируемый периметр.

Solar Dozor может проверять все узлы корпоративной сети, включая файловые и облачные хранилища, электронную почту и другие ресурсы для обнаружения и пресечения нарушений правил хранения конфиденциальной информации. Эти функции реализуются с помощью отдельного модуля — Dozor File Crawler.

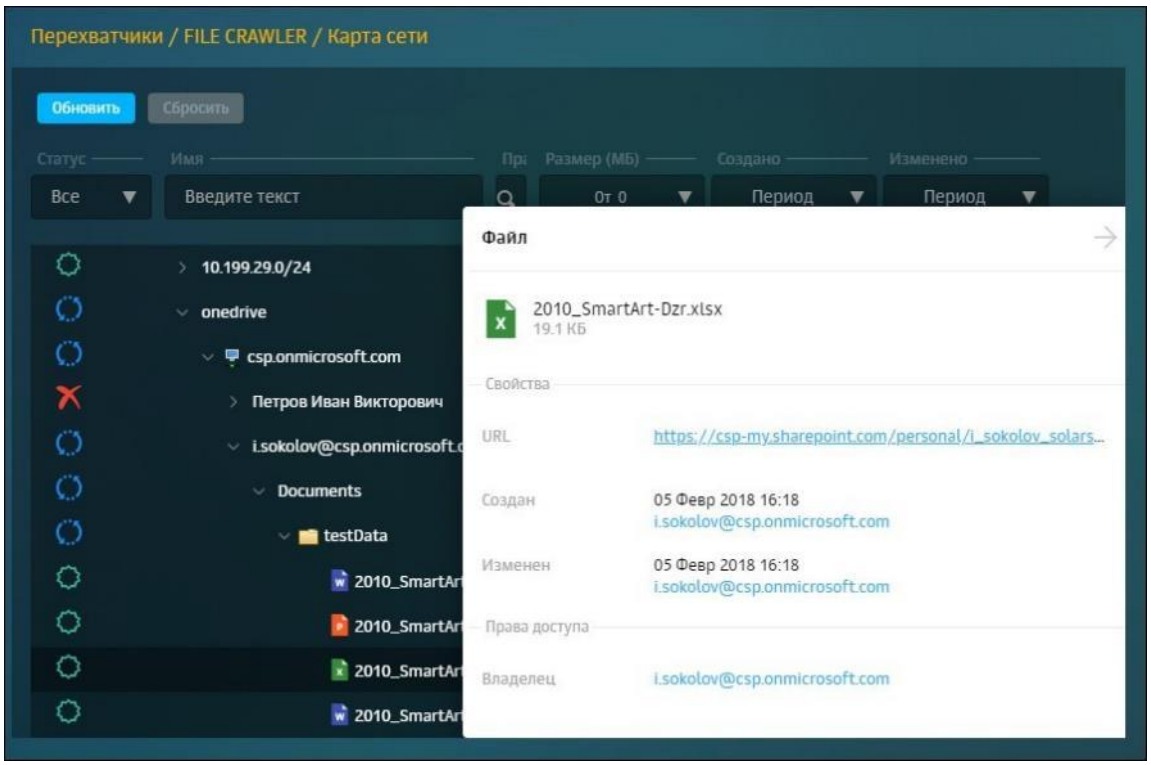


Рисунок 13. Основные сведения файлов, обнаруженных при сканированиях хранилищ

Основные возможности Dozor File Crawler:

- **Сканирование исторически накопленных почтовых сообщений** для ретроспективного исследования ранее накопленной в компании электронной почты. Задача — обнаружить нарушения политики безопасности и утечки ценной информации, а также выявить негативные тенденции в прошлом.

- **Построение карты корпоративной сети** для получения максимально полной информации обо всех узлах, ресурсах, каталогах и файлах, имеющихся в локальной сети предприятия. Позволяет получить представление в целом обо всей корпоративной сети и ее местах, уязвимых для утечек информации, а также о неконтролируемых ресурсах локальной сети.

- **Сканирование файловых хранилищ**. Применяется по аналогии со сканированием всей корпоративной сети, но выполняется только в отношении файловых ресурсов, т. к. размещаемые в сети файлы представляют первоочередной интерес с точки зрения ИБ. Важнейшим отличием от обычного сканирования является наличие режима активного противодействия: обнаруженные файлы проверяются на соответствие политике безопасности, и в случае нарушения к ним применяется ряд защитных мер. Результаты сканирования файловых хранилищ добавляются в общую карту сети компании, тем самым обогащая ее.

- **Сканирование исторического архива почтовых сообщений и файловых хранилищ** с использованием доступа администратора. Позволяет сканировать почтовые ящики и файловые ресурсы с ограниченным доступом с использованием учетной записи системного администратора. Это значительно расширяет состав доступной для обследования информации в корпоративной сети.

- **Сканирование облачных хранилищ** для проверки корпоративных облачных хранилищ на предмет наличия в них конфиденциальных данных. Результаты сканирования облачных хранилищ обогащают общую карту сети компании.

- **Сканирование массивов информации на съемных внешних носителях** позволяет при подключении к рабочим станциям пользователей проверять на наличие конфиденциальных данных информацию, которая передается с внешних носителей и на внешние носители. Результаты сканирования информации на съемных носителях обогащают общую карту сети компании.

- **Использование результатов предыдущих сканирований в качестве справочника для последующих**. Полученные ранее сведения об устройстве локальной сети можно использовать в качестве справочных данных при подготовке новых сканирований. Так, при проведении нового сканирования файловых ресурсов можно указывать в качестве целевых мест поиска найденные ранее каталоги и IP-узлы. При обновлении карты сети — найденные ранее узлы, при запуске нового сканирования облачного хранилища — найденные ранее каталоги облака.

- **Использование Dozor File Crawler для узкоцелевых расследований**. Все вышеперечисленные возможности помогут ИБ-специалисту не только в целом обследовать содержимого корпоративной сети и затем анализировать его, но и выполнять узконаправленные проверки. Целями подобных проверок могут являться:

  - поиск в корпоративной сети мест с повышенным риском;
  - поиск неконтролируемо хранимых в сети ценных сведений;
  - прицельное исследование узлов и ресурсов сети для поиска нарушений безопасности;
  - проверка рабочих станций сотрудников, находящихся под подозрением, на наличие конфиденциальной информации;
  - выявление путей движения защищаемых документов внутри компании.

- **Дополнительно Dozor File Crawler обеспечивает:**

  - гибкую настройку и управление сканированиями различных ресурсов и построением карты сети.
  - управление нагрузкой на ресурсы за счет указания хоста для выполнения задач, регулировки ограничений при выполнении задач и настройки выполнения задач по расписанию.
  - доступ к результатам как по окончании последнего полного сканирования, так и в режиме просмотра изменений.
  - просмотр общей карты сети, сформированной по результатам выполнения различных задач обследования сети.

2.5. Выявление продвинутых нарушителей

Расшифровывание HTTPS-трафика

Опытный нарушитель при работе с веб-сервисами может понадеяться на использование протокола HTTPS. Solar Dozor может интегрироваться с любыми периметровыми средствами защиты с поддержкой протокола ICAP, например, шлюзом веб-безопасности Solar webProxy, что позволяет бороться с таким способом обхода DLP-системы.

Такой подход позволяет клиенту использовать все преимущества прокси-серверов без дополнительных настроек интернет-соединения на персональных компьютерах — в браузере и прочих приложениях. Компьютеры сотрудников просто подключаются к сети, и вся их веб-активность, включая зашифрованный трафик, оказывается под контролем.

Система также может перехватывать трафик непосредственно на рабочей станции пользователя до шифрования, без подмены сертификатов в браузере.

Обход анонимайзеров

Для разбора трафика Solar Dozor использует сигнатурный анализ данных. Эта технология дает полное понимание структуры и содержимого данных, передаваемых через веб-почту, социальные сети и прочие веб-сервисы.

Даже если сотрудник воспользовался анонимайзером или TOR, Solar Dozor сохранит и проанализирует его активность и переписку.

Выявление транслита и опечаток

В Solar Dozor реализованы механизмы, которые позволяют распознавать в сообщениях и именах файлов текст, написанный транслитом или с опечатками, и преобразовывать его к правильному виду. Таким образом, теперь можно контролировать передачу текста, который намеренно или случайно был искажен.

3. Проведение расследований

Для того, чтобы заметить в массе коммуникационного трафика зарождающиеся признаки корпоративного мошенничества, DLP-система должна обладать мощным аналитическим потенциалом и удобными инструментами расследования инцидентов. Разглядеть в сотруднике нарушителя с первого взгляда удается не всегда, поэтому у офицера безопасности должна быть возможность определять косвенные признаки угроз и вовремя на них реагировать.

Перед тем как приступить к активным действиям, любой человек ведет подготовительную работу — для мошенничества всегда есть предпосылки и причины. Solar Dozor помогает службе безопасности обращать внимание на отклонения от нормальной активности сотрудников, выстраивать гипотезы и проводить их проверку.

Solar Dozor ведет расширенный архив переписки сотрудников, накапливает информацию по их активностям на рабочих станциях, профилирует полученные данные и выявляет нетипичные связи и аномалии в поведении. Такой подход позволяет на ранней стадии определить косвенные признаки зарождающихся угроз и вовремя начать расследование в отношении потенциального нарушителя.

Для организаций с территориально распределенной структурой дополнительную помощь в расследованиях может оказать модуль MultiDozor. При подключении модуля формируется единое Досье, включающее информацию о всех сотрудниках организации. Благодаря этому мониторинг персон и групп пользователей также может осуществляться в рамках всей организации, что делает возможным проведение сквозных расследований по всей территориально распределенной сети.

При этом, информация о всех сотрудниках организации доступна офицерам безопасности, наделенным соответствующими правами. Доступ офицеров безопасности, работающих с данными только своих филиалов, к данным персон из других филиалов организации ограничивается общими сведениями

3.1. Ведение архива цифровых коммуникаций

Во время расследования корпоративного мошенничества важнейшую роль играет сбор доказательств. Это сложная и кропотливая работа с архивом коммуникаций, предполагающая выявление скрытых закономерностей в их действиях и установление причинно-следственных связей. Чтобы распутать сложные схемы, службе безопасности приходится обрабатывать огромные массивы разнородной информации. Полный архив коммуникаций с функцией быстрого поиска Solar Dozor делает этот процесс максимально комфортным и эффективным.

При использовании дополнительного модуля долговременного хранения Solar Dozor автоматически переносит все перехваченные коммуникации и информацию по событиям и инцидентам в долгосрочный архив, который может расширяться практически безгранично (подтвержденный срок хранения данных — более 10 лет, объем — более 1000 ТБ). Это особенно полезно при проведении ретроспективного анализа, затрагивающего существенные периоды — месяцы и годы.

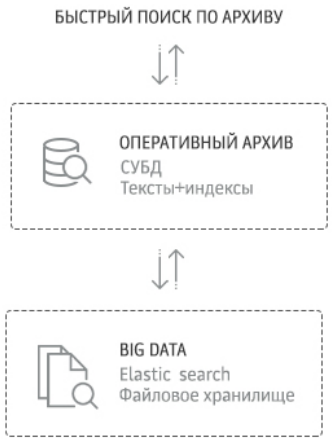


Рисунок 14. Применение концепции Big Data

Архитектура архива включает СУБД, в которой хранится проиндексированная информация для оперативного отображения, а также расширенное файловое хранилище с поддержкой технологии мгновенного поиска Elastic Search (меньше секунды в архиве на 17 млн сообщений). Такой подход эффективно решает задачу быстрого поиска по архиву, вместе с тем позволяя извлекать из долгосрочного хранения все необходимые данные.

3.2. Полнотекстовый гибкий поиск по архиву

Solar Dozor предоставляет простой и удобный поиск, аналогичный поисковикам Яндекс или Google. В нем можно найти необходимую информацию за считаные секунды. Опции «поиск от человека», «поиск от информации», «поиск вокруг события», «поиск похожих» и огромная библиотека готовых поисковых запросов с настраиваемыми параметрами значительно облегчают работу офицера безопасности.

Когда офицер безопасности начинает вводить имя или часть адреса, Solar Dozor сразу отображает список сотрудников, данные которых содержат вводимые символы. В условиях запроса расширенного поиска можно указать конкретный быстрый запрос поиска сообщений. Это позволит точнее и быстрее находить нужную информацию.

При использовании модуля MultiDozor поиск может осуществляться по всей сети филиалов. Принадлежность сообщений отображается как в их карточках, так и в результатах поисковых запросов. В зависимости от уровня доступа офицера безопасности изменяется статистика и отображение найденных сообщений.

3.3. Ведение досье по персонам

Досье позволяет накапливать всю нужную информацию по сотрудникам и внешним контактам. «Персона» — лежащая в основе досье сущность — обеспечивает работу в системе с конкретными людьми, а не с их идентификаторами и адресами, которые далеко не всегда очевидны.

Рисунок 15. Карточка персоны

В карточке персоны в компактном формате собрана вся информация о сотруднике и его активностях:

- Личные, сетевые и контактные данные, уровень доверия к человеку;
- Список событий и инцидентов, в которых фигурирует персона;
- Полученные и отправленные сообщения и файлы;
- Связи и контакты;
- Снимки рабочего стола;
- Используемые устройства;
- Поведенческие аномалии;
- Рабочее время.

Интеграция с внешними системами позволяет обогащать «Досье» информацией из сторонних баз данных и социальных сетей.

Непрерывный мониторинг персон из групп риска

В Solar Dozor есть инструменты постоянного контроля активности персон, поведение которых вызывает недоверие, — виджеты быстрого доступа к информации по сотрудникам:

- требующим наблюдения,
- входящим в группу особого контроля (на испытательном сроке, на увольнение и т. д.),
- у которых система зафиксировала аномальное поведение (снизился уровень доверия).

Идентификация пользователей

В системе применяются уникальные механизмы, которые связывают людей с их адресами, помогая соотносить непонятные адреса типа dfgff603@mail.com с реальными владельцами.

Беседы в коммуникациях

Отображение связных бесед при поиске коммуникаций в Solar Dozor позволяет аналитику постоянно оставаться в контексте диалога пользователей, просматривать предыдущие и

последующие сообщения. Создав поисковый запрос на переписку, офицер безопасности получает:

- Перечень бесед с указанием мессенджера;
- Список собеседников;
- Данные инициатора беседы;
- Общее количество сообщений и переданных файлов.

Выявление аномальной активности

Solar Dozor непрерывно анализирует действия сотрудников и внешних пользователей, выявляет нетипичные контакты и статистические аномалии в коммуникациях. Показатель «Уровень доверия», рассчитываемый по каждому сотруднику, помогает определять явных и скрытых нарушителей и проводить поведенческий анализ.

Поиск скрытых связей

Инструмент «Граф связей» позволяет выявлять и наглядно представлять неформальные связи между сотрудниками и внешними контактами, искать выходы на нужных персон и обнаруживать скрытые неочевидные связи.

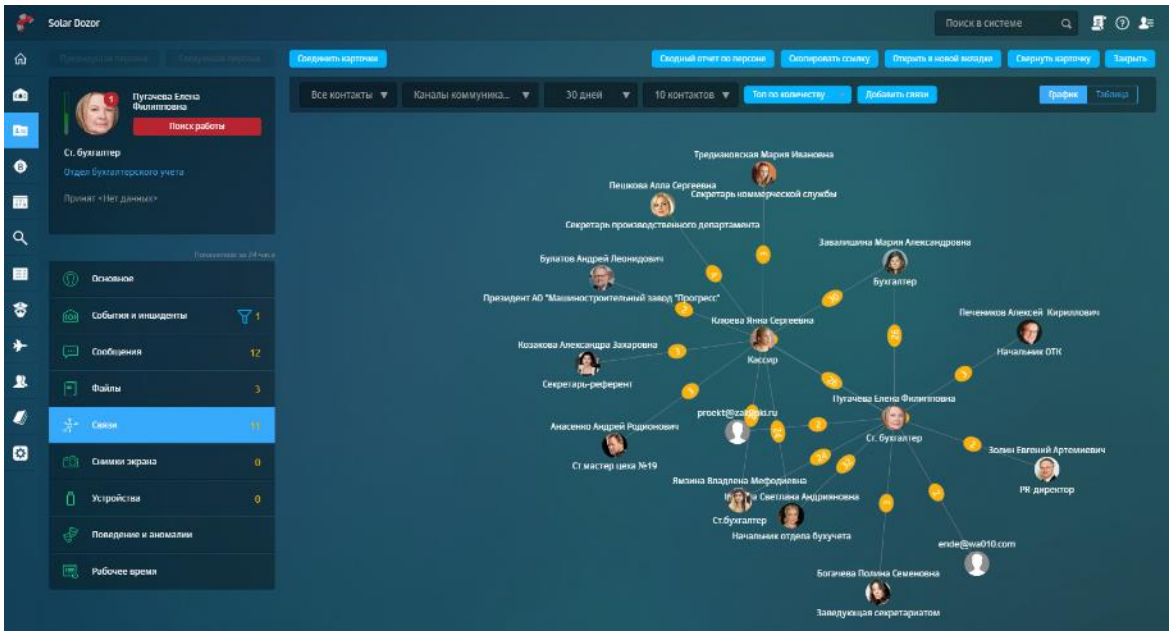


Рисунок 16. Граф связей

Снимки экрана

Solar Dozor позволяет с заданной периодичностью делать снимки экрана сотрудника, подкрепляя данные по инцидентам доказательствами. Создание скриншотов можно настроить по расписанию или привязать к действиям сотрудника на компьютере. Например, фотографировать рабочий стол после нажатия клавиши Enter или Print Screen, или при активации приложения.

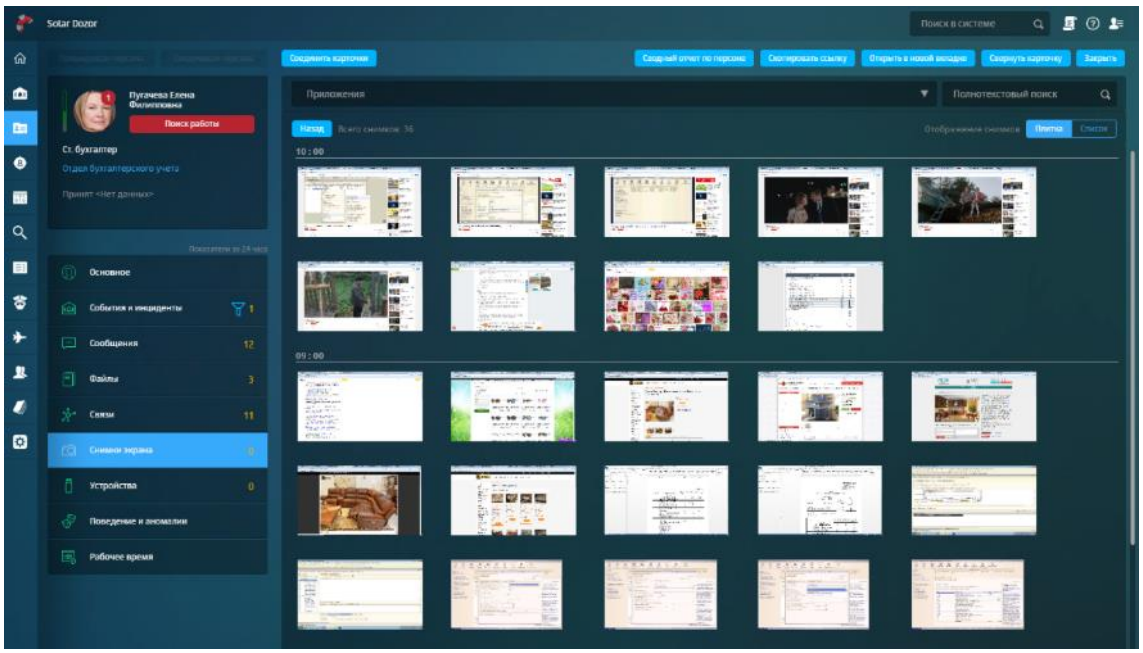


Рисунок 17. Галерея снимков рабочего стола

Архив изображений представлен в виде галереи с фильтрами для удобного отображения и визуализации.

Трансляция экрана рабочих станций

Для мониторинга активности персон, находящихся на контроле у офицера безопасности, можно просматривать трансляции экрана или экранов (если у сотрудника их несколько) в режиме реального времени.

Трансляция доступна из краткой и полной карточек персоны. Видео доступно только офицеру безопасности с соответствующими правами доступа. Можно настроить доступ к трансляции экрана как отдельных персон, так и групп сотрудников.

Офицеры безопасности получают возможность прицельного контроля за действиями сотрудников в реальном времени, что позволяет проверять гипотезы, отслеживать нарушения безопасности и проводить их профилактику.

Запись видео экрана рабочих станций

Для расширения доказательной базы и получения дополнительного контекста при проведении расследований в Solar Dozor реализована функция записи видео с экрана рабочих станций сотрудников. Действия пользователя с экранов мониторов записываются в видеофайл и передаются на сервер Solar Dozor. Кроме видеозаписи, передается информация о запущенных на рабочей станции процессах, заголовках открытых окон, а также URL, если пользователь на момент записи работал в браузере. На одной станции одновременно могут записываться до 4 подключенных мониторов.

Настройка параметров видеозаписи осуществляется в карточке персоны, во вкладке «Записи экрана»:

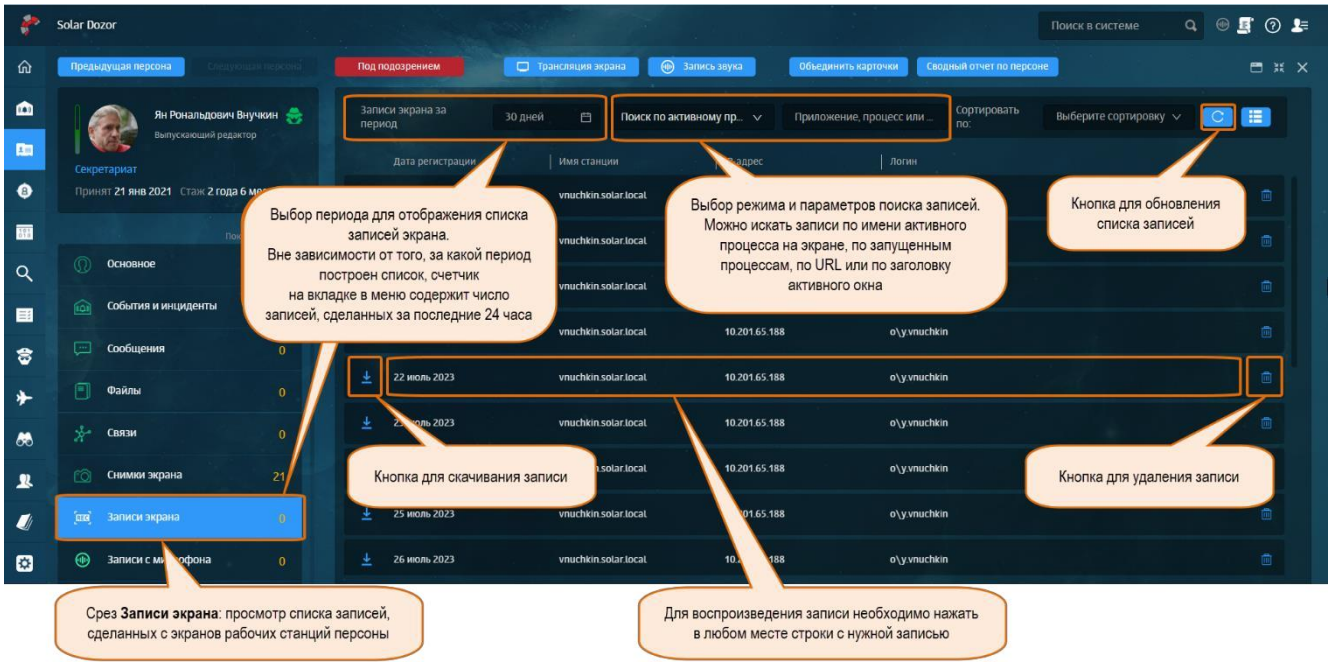


Рисунок 18. Вкладка Записи экрана в карточке персоны

Офицеры информационной безопасности получают возможность точечного контроля сотрудников и/или подразделений, находящихся в группе особого контроля (ГрОК), а также этот инструмент может использоваться для проведения реверсивных расследований.

Запись звука с микрофона

В Solar Dozor представлен еще один инструмент для выявления нарушений и сбора доказательной базы при проведении расследований: офицер безопасности может записать звук, который в данный момент поступает на микрофон рабочего компьютера сотрудника. Возможность реализована для полнофункциональных агентов и доступна из раздела «Досье».

Чтобы звук с микрофона рабочей станции нужной персоны начал записываться, достаточно перейти в карточку этой персоны (функционал доступен как в краткой, так и полной карточке), нажать кнопку записи и выбрать соответствующую рабочую станцию.

Доступ к записям звука (из большой и краткой карточки персоны) настраивается. Также настраиваются и параметры хранения, ротации, метаданных и длительности аудиозаписей (включая длительность тишины на записи). Прослушивание записанного возможно практически в режиме реального времени. Сведения о сеансе записи возможно удалить, а файл аудиозаписи — скачать.

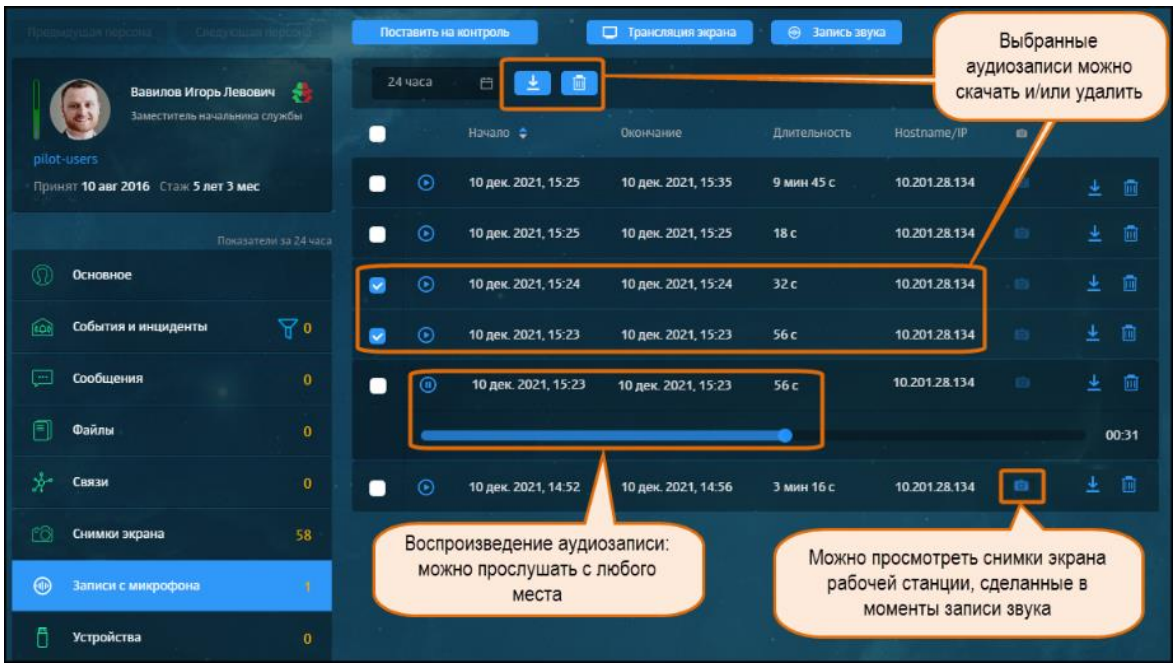


Рисунок 19. Запись звука с микрофона на рабочей станции

Контроль подключения к Wi-Fi-сетям

Офицер безопасности может контролировать подключение пользователей к беспроводным сетям, блокируя нежелательные каналы передачи данных. Ограничивать подключение к сетям Wi-Fi можно на уровне сетей (SSID) или отдельных точек доступа (BSSID), пользователей и групп. Разрешать или запрещать беспроводное подключение можно полностью или с использованием «черных» и «белых» списков. Настройка всех этих разрешений осуществляется в политике.

Данные о подключениях пользователя доступны на вкладке **Сети Wi-Fi** в карточке персоны. На странице отражены все попытки подключения к сетям Wi-Fi.

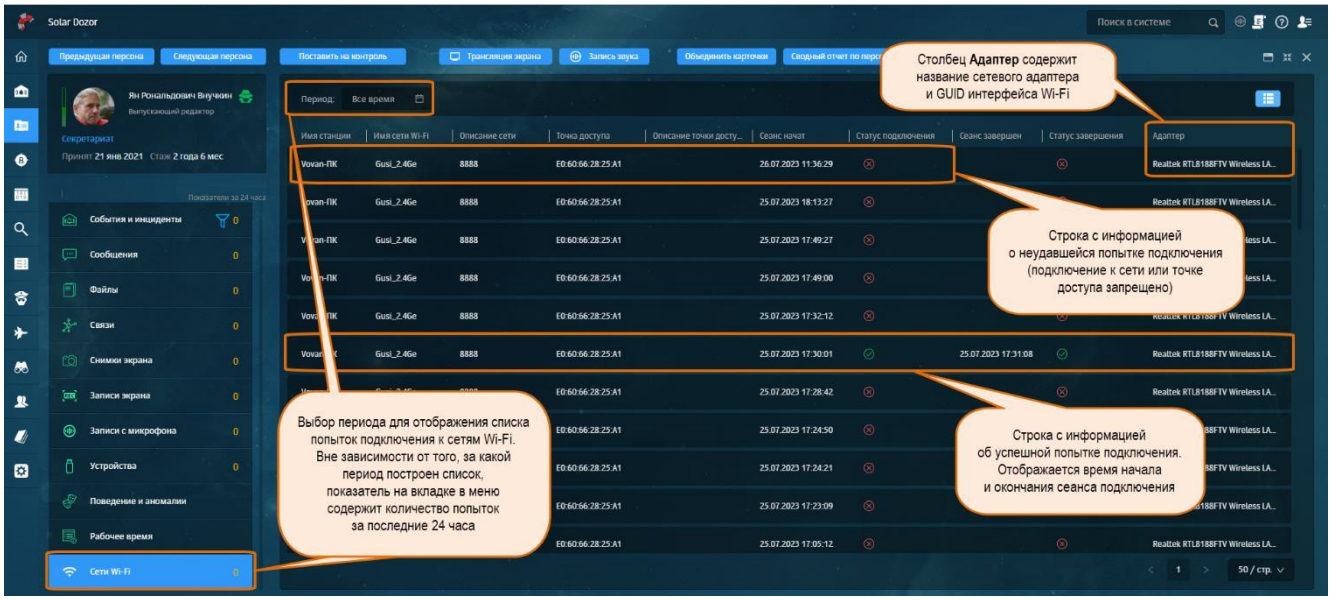


Рисунок 20. Раздел Досье Solar Dozor: карточка персоны. Вкладка Сети Wi-Fi

Контроль рабочего времени

Функция контроля рабочего времени сотрудников позволяет руководству и службе безопасности получать подробные сведения о том, чем занимается сотрудник на рабочем месте: сколько времени и на какую деятельность он тратит и какие веб-ресурсы и приложения использует.

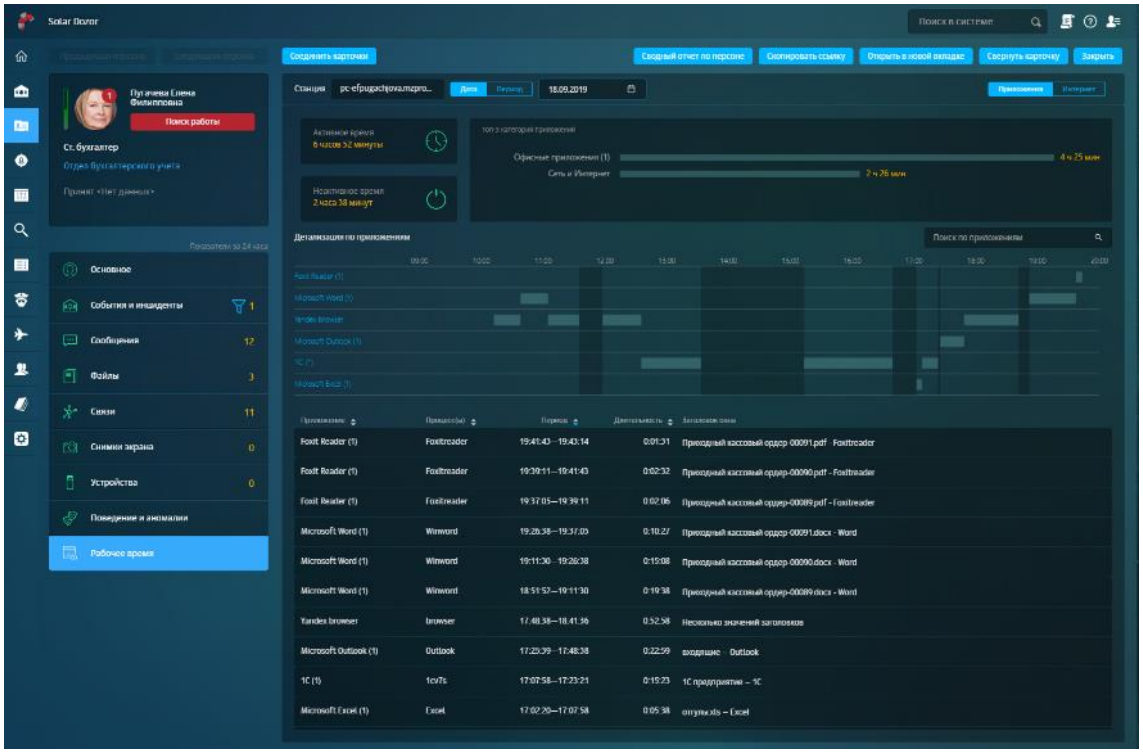


Рисунок 21. Контроль рабочего времени

Теперь офицер безопасности может просматривать:

- Суммарные за конкретный день или период сведения о том, сколько времени сотрудник тратит на работу;
- Топ-5 категорий приложений, которые использовались сотрудником больше всего (за день или период);
- Детальную статистику по использованию персоной рабочего времени: подробные данные о времени, проведенном сотрудником как в приложениях, так и в интернете (за день или за период).

Данные отображаются как в текстовом виде, так и в виде диаграмм, где периоды работы персоны в конкретном приложении представлены как временные отрезки, выделенные определенным цветом.

Функция ориентирована в первую очередь на решение задач безопасности. Например, с ее помощью можно выявлять использование сотрудником нежелательных приложений, оценивать риск утечки информации по активности сотрудника в интернете и т. п.

3.4. Эффективное управление событиями и инцидентами

Благодаря методологии управления разбором происшествий и полного контроля расследований Solar Dozor обеспечивает полный цикл работы с событиями и инцидентами.

Интеллектуальная система Solar Dozor автоматически регистрирует и классифицирует по уровню критичности события ИБ. Офицеры безопасности управляют жизненным циклом инцидентов при помощи специального интерфейса. В нем можно получить наглядную информацию о новых событиях, сгруппированных по уровню критичности, просмотреть список всех инцидентов в работе, а также загрузить подробные сведения о конкретном событии или инциденте.

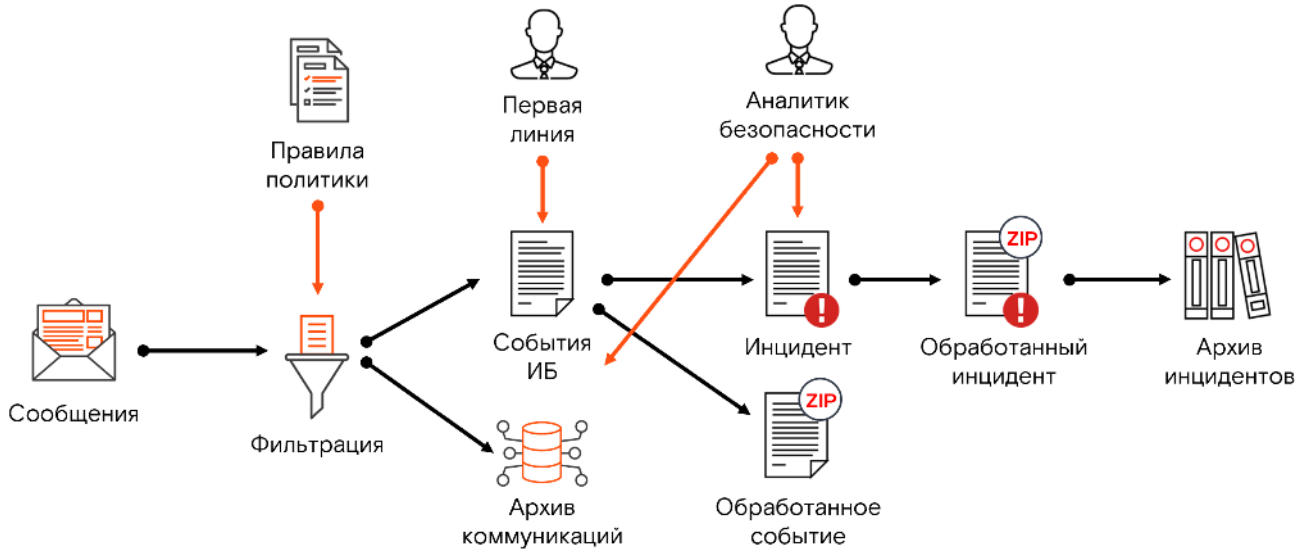


Рисунок 22. Управление событиями и инцидентами

С помощью системы кейс-менеджмента можно в несколько кликов назначить задачу определенному сотруднику, передать дело или инцидент коллеге, а также назначить ответственного за разбор инцидента и расследование. Таким образом удается реализовать единый и непрерывный процесс работы внутри службы безопасности, ускорить коммуникации и связать географически распределенные подразделения.

Лента комментариев в карточке инцидента расширяет возможности совместной работы над инцидентами. Любой специалист безопасности может оставлять комментарии, которые на практике превращаются в интерактивный чат сотрудников, ведущих расследование. Зная идентификатор события или инцидента, офицер безопасности может оперативно найти и посмотреть все интересующие его данные.

4. Построение отчетов по событиям и инцидентам

В Solar Dozor реализована мощная система построения отчетов для качественного представления результатов работы службы безопасности. В наглядных отчетах содержится исчерпывающая сводная информация о происшествиях, нарушителях, потоках данных и результатах проведенных расследований. С их помощью руководители службы безопасности могут видеть общую картину и текущее состояние защищаемой информации. Более подробные отчеты помогают выявить недочеты в политике безопасности компании.

4.1. Автоматическая генерация отчетов

Функция регулярной автоматической генерации отчетов по заранее разработанным шаблонам избавляет от необходимости срочной подготовки отчетов — они создаются по заданному расписанию и в удобном формате (интерфейс/XML/PDF/DOCX/CSV/HTML), после чего рассылаются всем заинтересованным лицам.

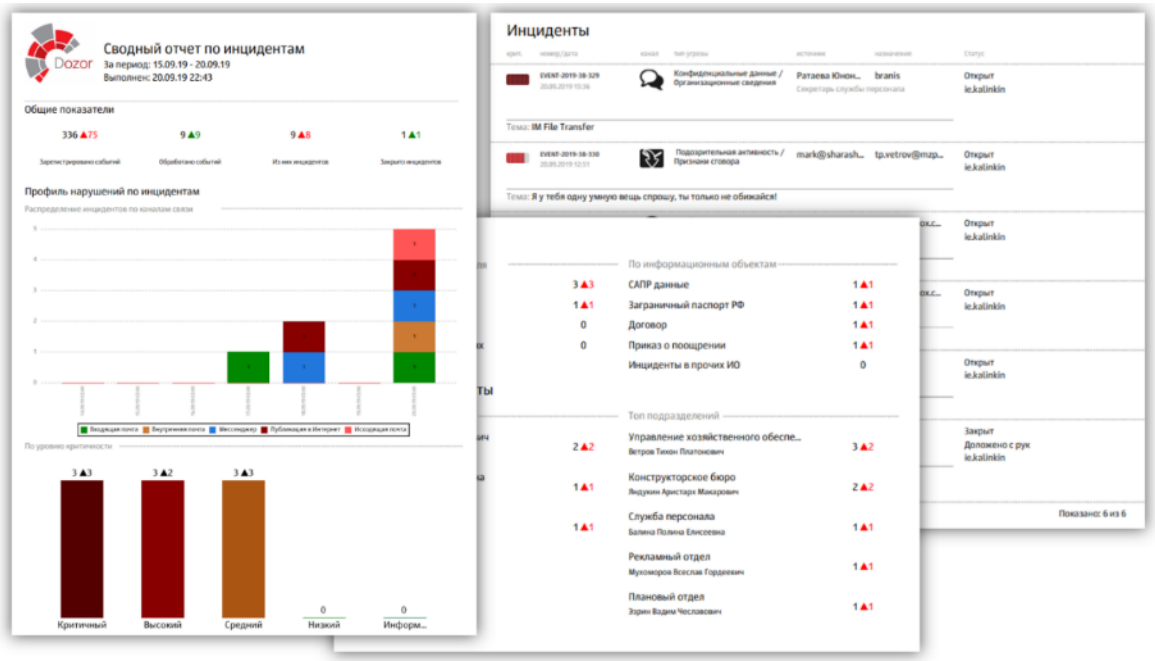


Рисунок 23. Примеры отчетов

4.2. Тепловая карта коммуникаций

В Solar Dozor реализована уникальная для DLP-систем функция — «Тепловая карта коммуникаций», на которой видна интенсивность коммуникаций сотрудников или движения информации. Карта дает офицеру безопасности возможность быстро оценить обстановку, увидеть потенциальные риски и горячие точки. Используя этот инструмент, офицер безопасности может построить графическую карту по интересующему его информационному объекту или персоне.

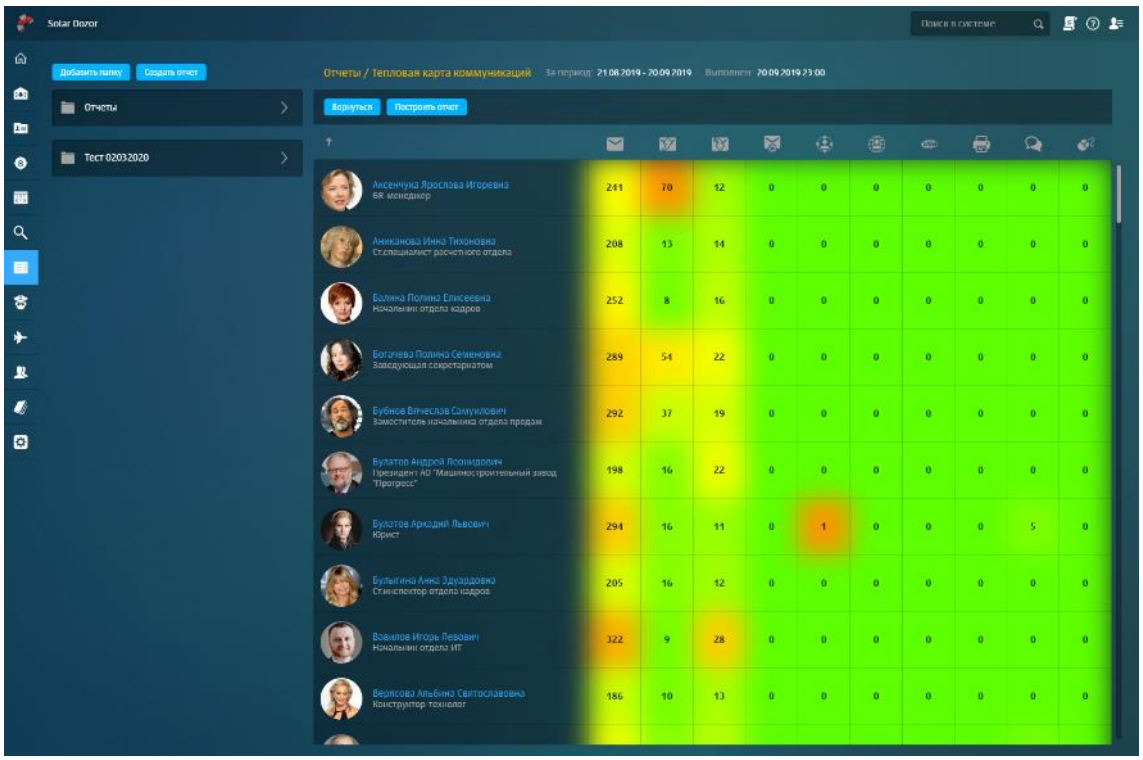


Рисунок 24. Тепловая карта коммуникаций

4.3. Сводный отчет по персоне

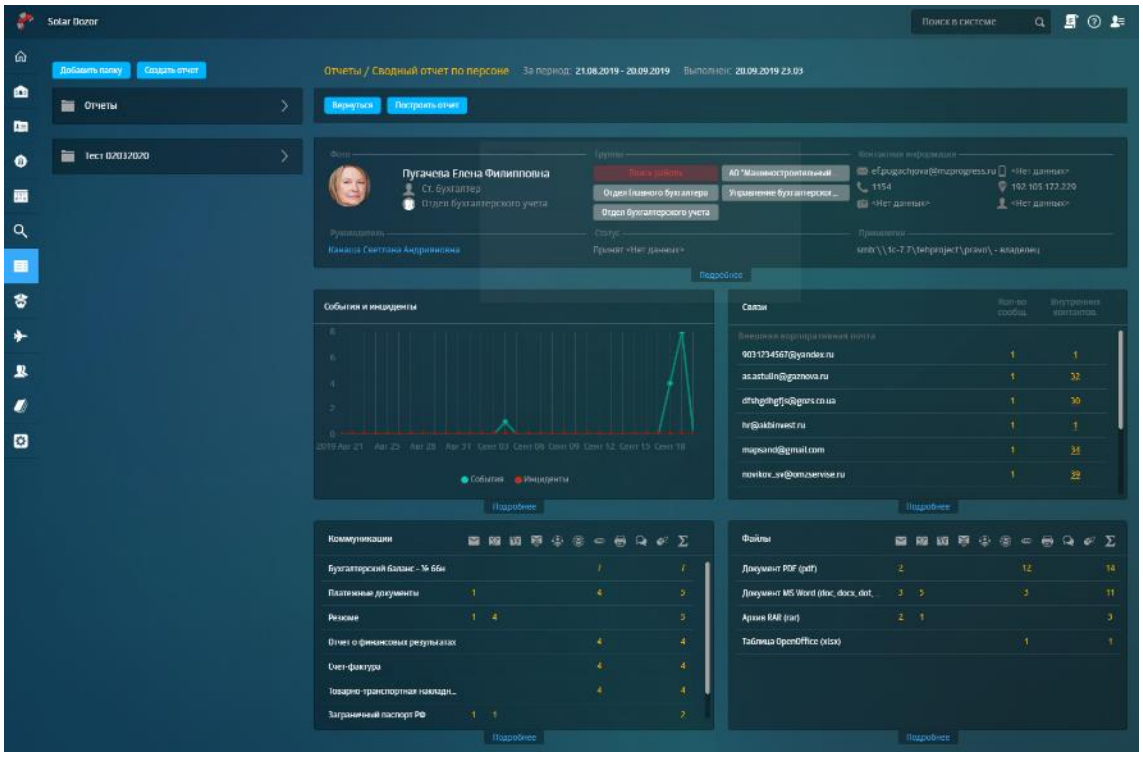


Рисунок 25. Сводный отчет по персоне

Зачастую служба ИБ получает от руководителей бизнес-подразделений задание собрать досье на кого-то из сотрудников, которая формулируется как «Что у нас есть на Васю?».

На основе информации в «Досье» можно мгновенно создать сводный отчет по персоне за требуемый период и отобразить его в веб-интерфейсе или выгрузить в PDF-файл для печати. Отчет по персоне содержит сводку активности сотрудника с краткой карточкой, событиями и

инцидентами, связями, коммуникациями и файлами, и при необходимости в него можно включить детальную информацию — конкретные сообщения, события и инциденты.

Для понимания сформированного отчета не нужно быть техническим специалистом — его можно показать руководителю, презентовать на совещании или прикрепить к личному делу в кадровой службе.

5. Анализ поведения пользователей

Главным нововведением Solar Dozor 7 стало появление модуля анализа поведения пользователей (UBA). Он в реальном времени анализирует историю коммуникаций каждого сотрудника и автоматически формирует личный профиль его нормального поведения. На основе собранной информации выявляются аномалии в поведении сотрудника. Также модуль UBA ищет работников, попадающих под значимые для безопасности паттерны поведения (группы поведенческих особенностей и аномалий).

Для работы функций поведенческого анализа используются данные в трех разрезах:

- Электронная почта (внутренняя, исходящая, входящая);
- Мессенджеры;
- Совокупно электронная почта + мессенджеры.

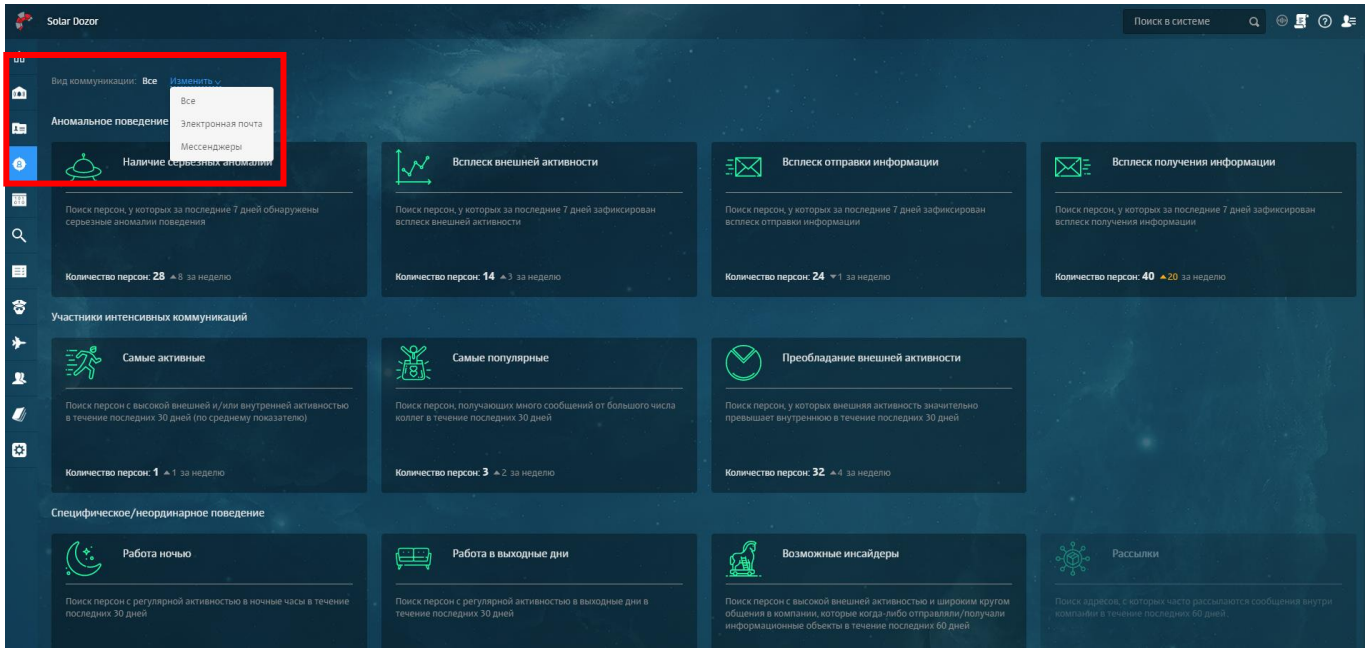


Рисунок 26. Выбор канала коммуникаций в списке паттернов

При этом для построения корректной аналитической картины достаточно данных, накопленных за 1 – 2 месяца. Если в организации уже используется Solar Dozor и накоплен соответствующий архив сообщений, результаты анализа поведения пользователей доступны сразу.

Информация, предоставляемая модулем UBA, позволяет офицеру безопасности анализировать:

- Общую поведенческую динамику и показатели поведения различных групп риска;
- Общую поведенческую динамику и показатели различных групп особого контроля и структурных подразделений компании;
- Динамику показателей поведения конкретной персоны.

В результате общего анализа можно оценить конкретные риски, связанные с деятельностью персоны, увидеть направление для дальнейшего анализа поведения персоны. Углубленный анализ динамики показателей поведения может выявить негативные тенденции в поведении персоны, что позволяет офицеру безопасности своевременно нейтрализовать риски, связанные с утечкой конфиденциальных данных.

В Solar Dozor поведение человека описывается с помощью специальных показателей, основными из которых являются:

- **Внешняя и внутренняя активность** — отражает интенсивность отправки персоной сообщений за пределы контура компании и внутри компании соответственно.
- **Объем отправленных/полученных информационных объектов (ИО)** — отражает интенсивность отправки/получения персоной различных видов ИО.
- **Круг общения** — отражает интенсивность взаимодействия персоны с другими персонами из различных групп (подразделений) компании.
- **Популярность** — отражает интенсивность получения персоной сообщений внутри компании.
- **Индекс уязвимости (ИУ)** – является показателем, обобщающим все вышеприведенные показатели, и отражает степень риска совершения случайных и/или намеренных нарушений ИБ со стороны персоны.

5.1. Паттерны поведения и групповые тенденции

На основе экспертного анализа и результатов пилотных проектов в модуль UBA включены 20 паттернов (шаблонов) поведения. С их помощью можно быстро найти сотрудников, в деятельности которых присутствуют признаки конкретного типа поведения. Кроме этого, паттерны поведения позволяют контролировать и отслеживать группы сотрудников по определенным комбинациям показателей поведения и найденным аномалиям, а также обнаруживать скрытые уязвимости и рисковые массовые тенденции в поведении. Проверка сотрудников по паттернам также помогает осуществлять профилактику случайных утечек, а также выявлять уязвимости в бизнес-процессах.

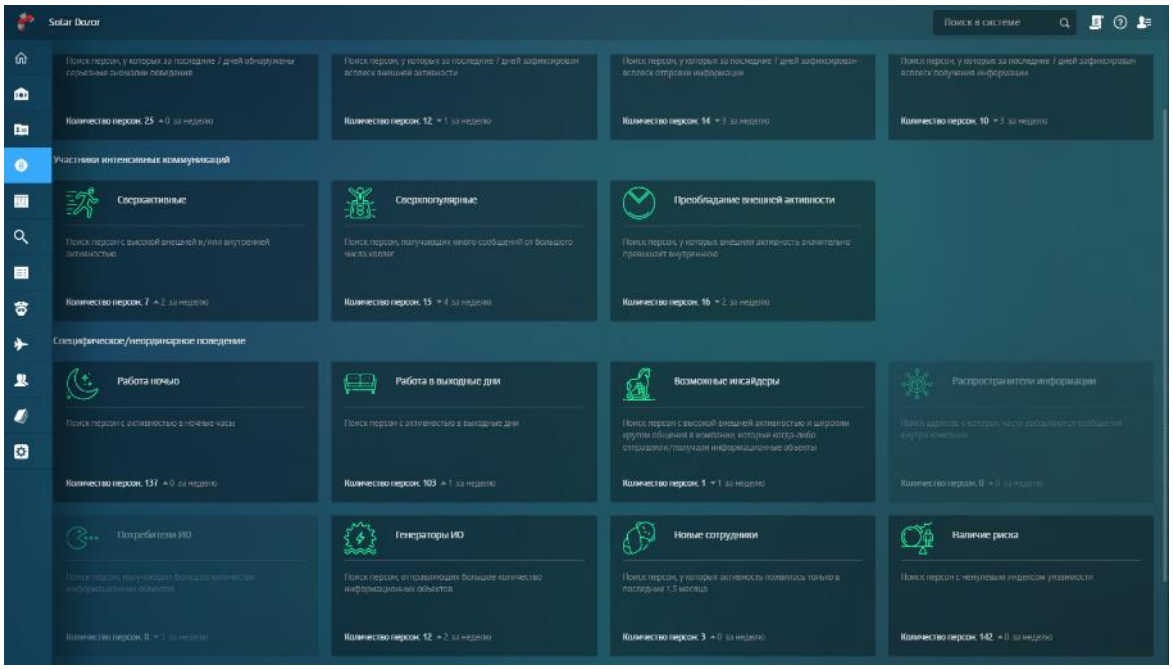


Рисунок 27. Паттерны поведения

Паттерны поведения объединены в группы, называемые группами риска:

- **Аномальное поведение:**
  - «Наличие серьезных аномалий» — поиск персон, у которых за последние 7 дней обнаружены серьезные аномалии поведения.

- «Всплеск внешней активности» — поиск персон, у которых за последние 7 дней зафиксирован всплеск внешней активности.
- «Всплеск отправки информации» — поиск персон, у которых за последние 7 дней зафиксирован всплеск отправки информации.
- «Всплеск получения информации» — поиск персон, у которых за последние 7 дней зафиксирован всплеск получения информации.

- **Участники интенсивных коммуникаций:**
  - «Сверхактивные» — поиск персон с высокой внешней и/или внутренней активностью.
  - «Сверхпопулярные» — поиск персон, получающих много сообщений от большого числа коллег.
  - «Преобладание внешней активности» — поиск персон, у которых внешняя активность значительно превышает внутреннюю.
- **Специфическое/неординарное поведение:**
  - «Работа ночью» — поиск персон с активностью в ночные часы.
  - «Работа в выходные дни» — поиск персон с активностью в выходные дни.
  - «Возможные инсайдеры» — поиск персон с высокой внешней активность и широким кругом общения в компании, которые когда-либо отправляли/получали информационные объекты.
  - «Распространители информации» — поиск адресов, с которых часто рассылаются сообщения внутри компании.
  - «Потребители ИО» — поиск персон, получающих большое количество информационных объектов.
  - «Генераторы ИО» — поиск персон, отправляющих большое количество информационных объектов.
  - «Новые сотрудники» — поиск персон, у которых активность появилась только в последние 1,5 месяца.
  - «Наличие риска» — поиск персон с ненулевым индексом уязвимости.
  - «Признаки увольнения» — поиск персон, поведение которых достаточно четко (уже на ранних стадиях) указывает на то, что они собираются увольняться.
- **Контакты и общение с неизвестными:**
  - «Наличие приватных эго-сетей» — поиск персон, регулярно переписывающихся один на один по адресам, которые никто в компании не использует.
  - «Контакты с неизвестными» — поиск персон, переписывающихся по адресам, которые никто в компании не использует.
- **Отсутствие активности:**
  - «Мертвые души» — поиск персон, у которых нулевая активность.
  - «Отсутствие» — поиск персон, у которых за последние 2 месяца зафиксировано исчезновение активности на срок от 7 до 21 дня.

Список сотрудников, в деятельности которых присутствуют признаки конкретного типа поведения, можно:

- Отфильтровать, отобразив данные только сотрудников, соответствующих определенным критериям;

- Отсортировать по возрастанию/убыванию критерия сортировки. Критерии подразделяются на общие данные персоны (ФИО, Должность, Подразделение, Группа контроля) и показатели ее поведения (внешняя/внутренняя активность, индекс уязвимости, популярность и др.).

5.2. Анализ поведения по выборке персон

При необходимости сравнить показатели поведения определенных сотрудников офицер безопасности может отобразить только их данные (рис 12). Это позволяет обнаруживать нехарактерное для сотрудника и его должности поведение. С помощью гибкого фильтра можно осуществлять поиск по множеству критериев поведения.

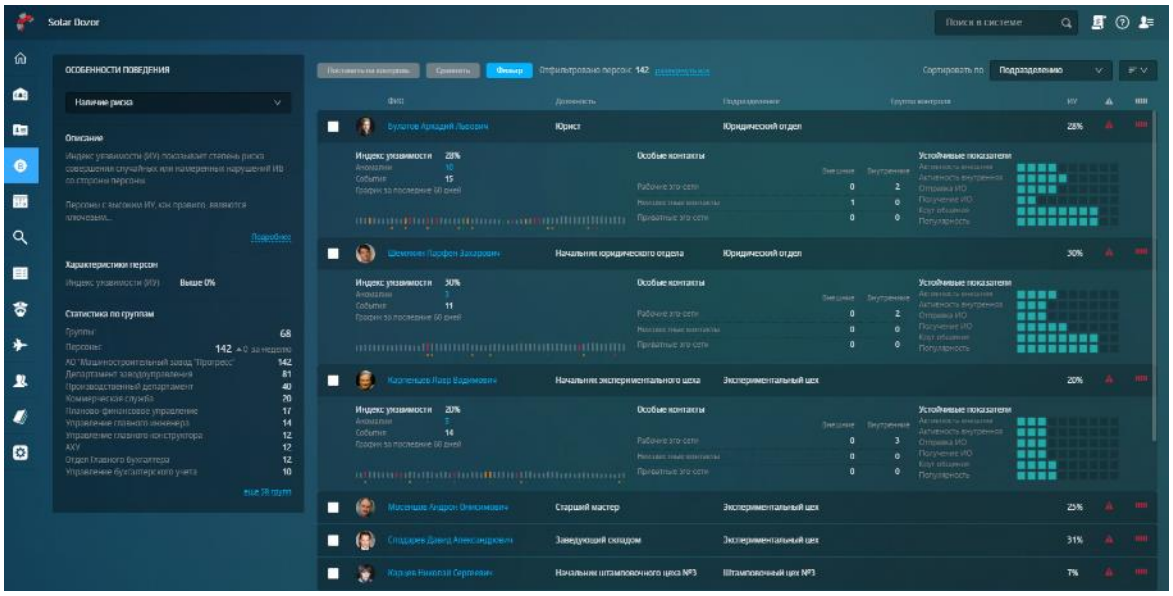


Рисунок 28. Сравнение показателей поведения сотрудников

5.3. Подробная карточка поведения

Рисунок 29. Вкладка «Поведение и аномалии»: раздел «Круг общения»

Получить детальные сведения о поведении персоны можно в ее полной карточке на вкладке «Поведение и аномалии». С ее помощью можно подробно рассматривать значительные отклонения от стандартного поведения сотрудника и исследовать его взаимодействие с другими отделами, своим кругом общения, а также выявлять приватные контакты и общение с неизвестными контактами.

Все данные сгруппированы по соответствующим разделам:

- **Профиль персоны** — значения важнейших показателей ее поведения, рассчитанные за последние 30 дней.
- **Аномалии** — динамика индекса уязвимости и все аномалии поведения персоны (уровень критичности каждой аномалии отмечен значком соответствующего цвета: высокий — красный, средний — желтый, низкий — зеленый).
- **Активность, Информационные объекты, Круг общения, Популярность** — динамика и аномалии соответствующих показателей поведения персоны.
- **Особые контакты** — статистика по адресам электронной почты, используемым персоной для переписки с коллегами и внешними лицами:
- **Рабочая эго-сеть** — известные в компании адреса, по которым персона регулярно ведет переписку один на один;
- **Приватная эго-сеть** — никому не известные в компании адреса, по которым персона регулярно ведет переписку один на один;
- **Неизвестные контакты** — никому не известные в компании адреса, по которым ведет переписку только персона (в данном случае персона может не только быть отправителем/получателем, но и стоять в копии сообщения).

При необходимости можно получить сведения о поведении персон в виде отчета для печати или сохранения в файл.

Доступные данные:

- О поведении выбранных персон по определенному паттерну поведения. В отчет попадает сводная информация о паттерне, список соответствующих персон и показатели поведения каждой персоны: особые контакты, количество событий, количество аномалий, индекс уязвимости.
- О поведении конкретной персоны за 45 дней. В отчете указываются общие сведения и контакты персоны, информация о стаже и руководителе и история поведенческих особенностей:
  - динамика индекса уязвимости и все аномалии;
  - динамика внутренней/внешней активности;
  - динамика отправки и получения информационных объектов;
  - динамика популярности;
  - список особых контактов: рабочая и приватная эго-сети, неизвестные контакты.

5.4. Минимизация риска утечки данных при увольнении сотрудников

Увольняющиеся сотрудники могут вынести за пределы компании огромное количество важной для бизнеса информации. Чтобы офицер безопасности мог вовремя принять меры по предотвращению утечки данных, в модуле Dozor UBA появилась возможность на ранних

стадиях выявлять сотрудников, поведение которых достаточно четко указывает на то, что они собираются увольняться.

Для получения списка таких сотрудников достаточно в интерфейсе системы в разделе «Анализ поведения (UBA)» нажать на виджет «Признаки увольнения».

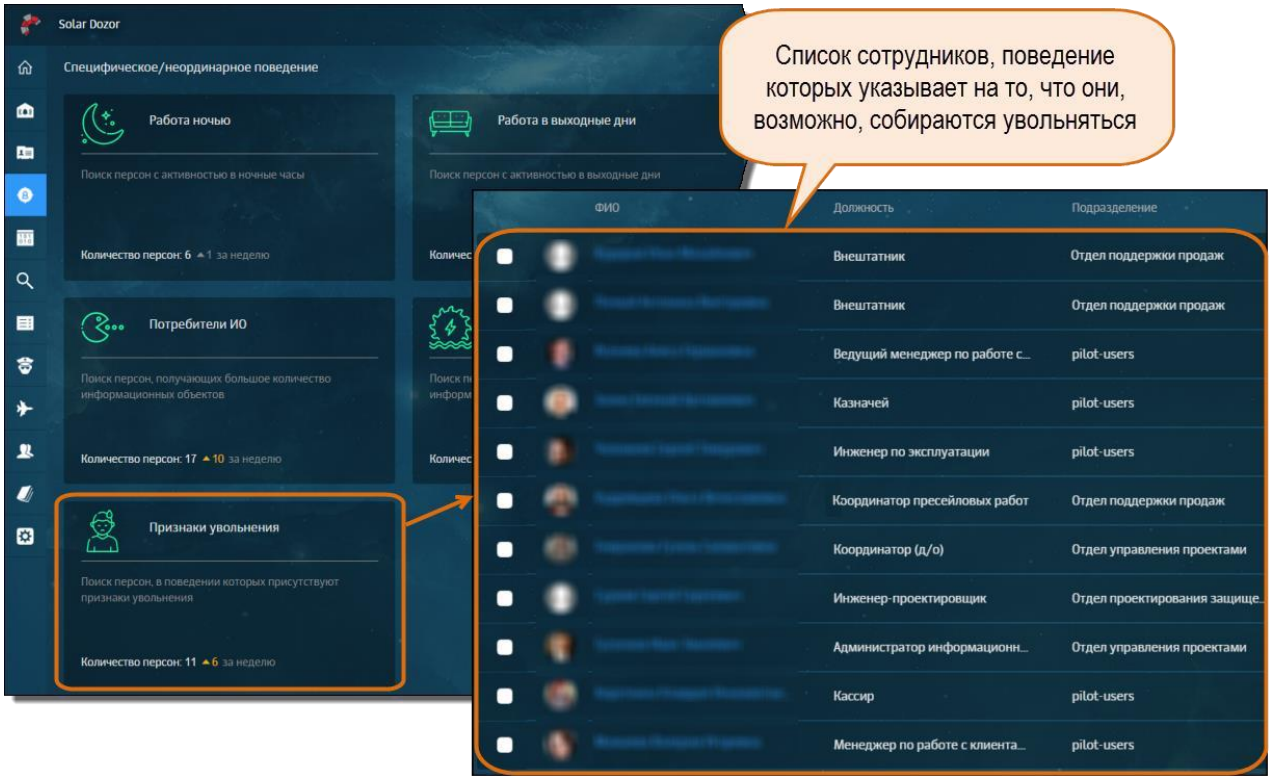


Рисунок 30. Список сотрудников с характерным для увольняющихся персон поведением

Критерии, на основании которых система относит сотрудников к увольняющимся, были сформированы в результате практических исследований и наблюдения за поведением увольняющихся сотрудников. К таким критериям относятся:

- Постепенное падение активности (внешней или внутренней);
- Оптимизация или сокращение сотрудником собственного рабочего графика;
- Появление новых уникальных контактов в коммуникациях;
- Передача нехарактерных для сотрудника информационных активов;
- Наличие событий безопасности с типом угрозы «Поиск работы».

Также для выявления увольняющихся персон используются такие признаки аномального поведения как появление новых неизвестных уникальных контактов и новых нехарактерных для конкретного сотрудника информационных объектов. Например, эти аномалии будут зафиксированы в поведении сотрудника, который вдруг начал собирать не имеющие отношения к его работе документы компании и пересылать их на неизвестную системе электронную почту.

Другой пример: сотрудник финансового отдела случайно отправил дизайнеру отчет о состоянии счетов компании – у дизайнера будет зафиксировано появление нового информационного объекта.

Таким образом, служба безопасности сможет на ранних стадиях выявлять как различные нарушения в бизнес-процессах, так и случайную или умышленную утечку данных.

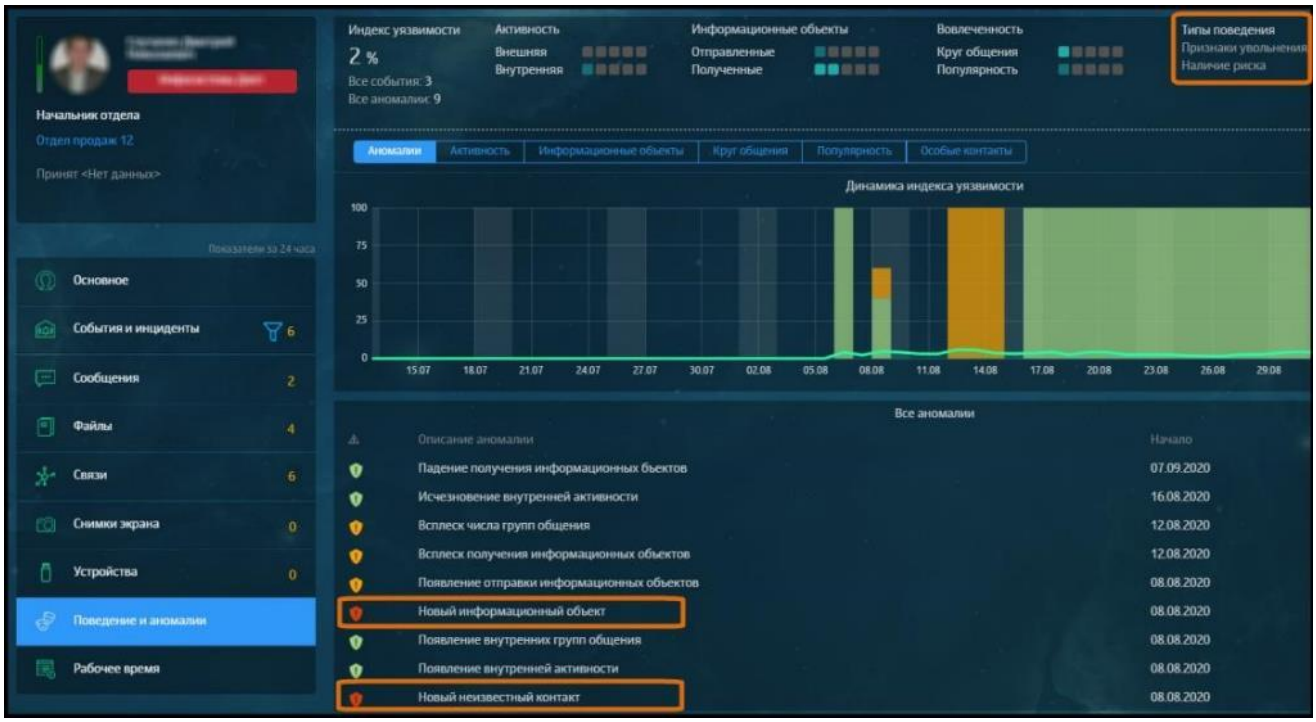


Рисунок 31. Карточка сотрудника с признаками увольнения

6. Контроль рабочего времени

Массовый перевод сотрудников на удаленный или дистанционный режимы работы выявил отсутствие в организациях инструментов отображения рабочей активности сотрудников в режиме реального времени.

Отсутствие непосредственного контроля ведет к росту рисков информационной безопасности, так как сотрудники, оказавшись в новых для себя условиях, могут совершать действия, напрямую угрожающие безопасности данных организации.

В результате организации стали активно инвестировать средства в специализированные ПО для получения дополнительных инструментов по управлению рабочими процессами.

В Solar Dozor доступен функционал контроля рабочего времени (КРВ), позволяющий оперативно оценить использование рабочего время сотрудниками и эффективность работы компании в целом. Например, теперь можно отследить использование рабочего времени или оборудования в личных целях.

Контроль рабочего времени разработан для менеджеров высшего и среднего звена, линейных руководителей, специалистов служб безопасности и HR-специалистов.

Решаемые задачи:

- Учет и контроль времени работы сотрудников;
- Оценка эффективности работы отдельных подразделений/компании в целом;
- Получение сведений о приложениях, используемых сотрудниками на рабочих местах;
- Контроль посещения сайтов.

При использовании возможностей КРВ руководство организации и офицеры безопасности могут:

- Оперативно оценить тенденции в работе сотрудников компании в целом: изменения в продолжительности рабочего дня, соблюдении трудового распорядка;
- Проанализировать деловую активность отдельно взятых подразделений и сотрудников компании;
- Выявить злоупотребления: использование игр, неделовых программ и программ, несущих риски для безопасности (например, приложений для подключения к удаленным рабочим столам).

Для этого в Solar Dozor созданы:

- Рабочий стол «Контроль рабочего времени» (РСКрв);
- Вкладка «Рабочее время» группы сотрудников.

6.1. Рабочий стол «Контроль рабочего времени»: процесс работы и решаемые задачи

Рабочий стол «Контроль рабочего времени» (РСКрв) разработан для руководителей высшего и среднего звена. На РСКрв представлены обобщенные показатели работы департаментов (подразделений, отделов и т.п.) в разрезе рабочей недели. При этом можно посмотреть не только показатели выбранной недели, но и их изменение по отношению к предыдущей неделе.

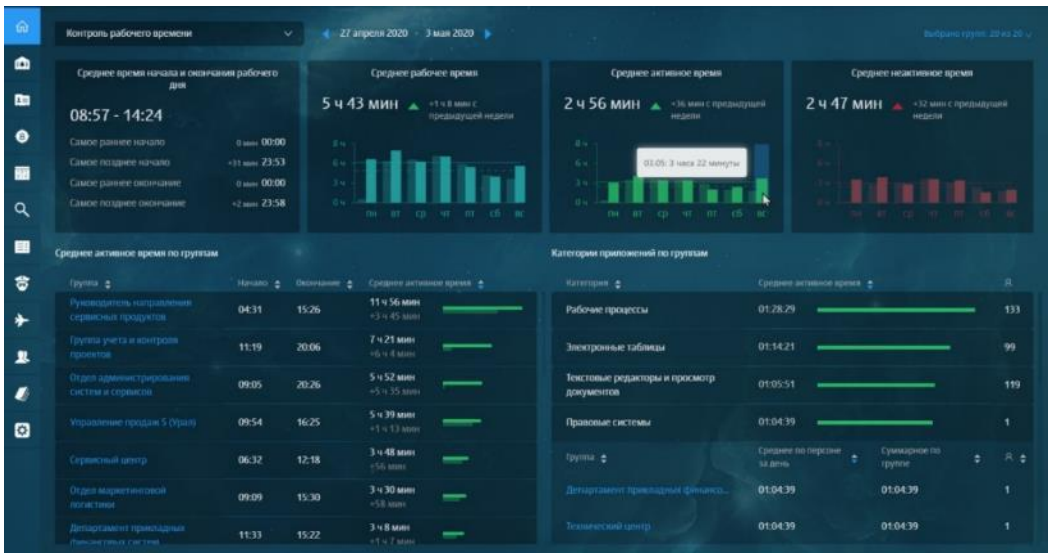


Рисунок 32. Рабочий стол «Контроль рабочего времени»

Детальные данные о рабочем времени группы сотрудников менеджер может посмотреть в карточке группы, нажав на ее название на рабочем столе.

6.2. Вкладка «Рабочее время»: процесс работы и решаемые задачи

Вкладка «Рабочее время» разработана для линейных руководителей. В ней представлены данные по показателям работы группы сотрудников за неделю и изменение этих показателей по отношению к предыдущей неделе. Эта информация позволит руководителю понять:

- Занимаются ли его подчиненные поставленными задачами;
- Есть ли тенденции к недоработкам, переработкам, прогулам;
- Соблюдают ли рабочий распорядок дня.

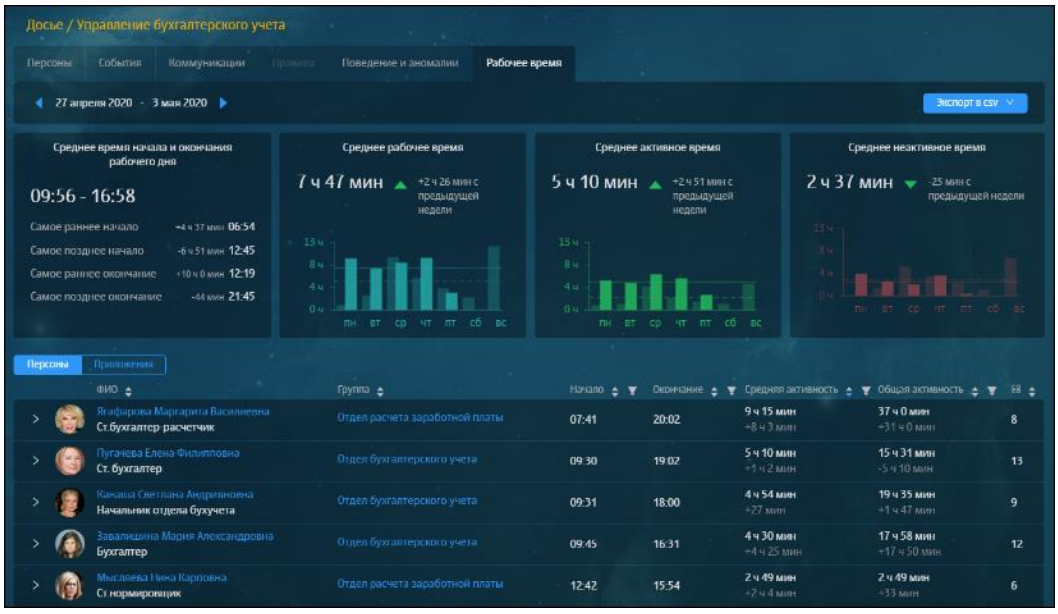


Рисунок 33. Вкладка «Рабочее время»

Отсортировав список сотрудников, можно легко найти отстающих, например, по активности. Также можно задать один или несколько фильтров и быстро найти тех, кто, например, недорабатывает.

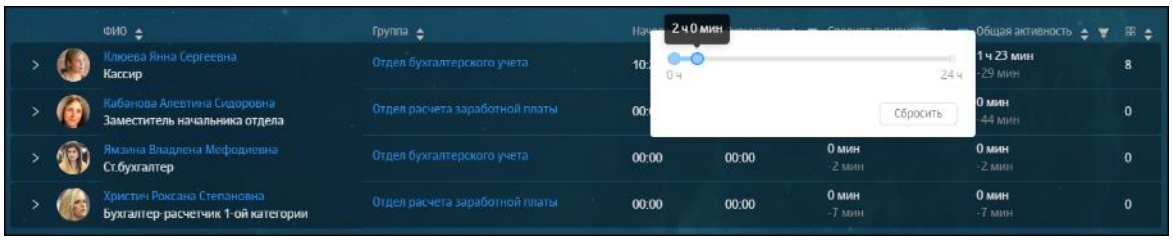


Рисунок 34. Вкладка «Рабочее время»: сортировка по активности

Использование комбинаций фильтров открывает неограниченные возможности поиска нарушителей трудового распорядка. Например, можно сделать выборку по сотрудникам, которые поздно начинают и, при этом, рано заканчивают рабочий день.

6.3. Рабочий стол «Контроль рабочего времени»: суммарные показатели деятельности сотрудников компании

Рабочий стол «Контроль рабочего времени» (РСКрв) предназначен для мониторинга ключевых показателей деятельности сотрудников с возможностью сравнения данных за текущую и прошедшую недели. При этом можно проводить анализ по конкретным группам (подразделениям, группам особого контроля).

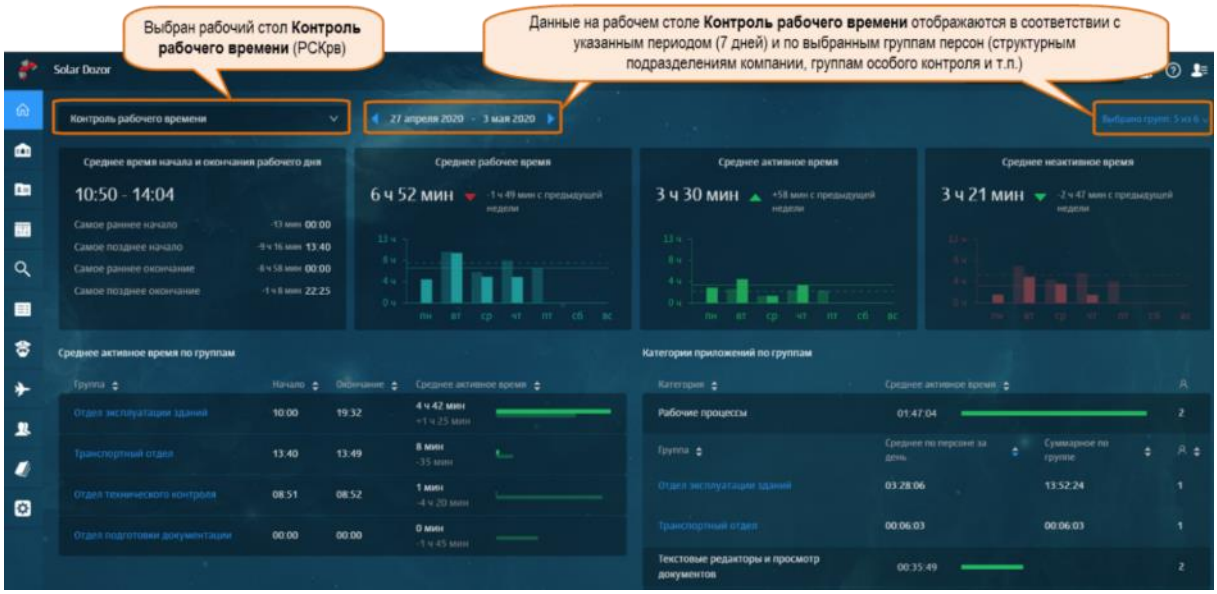


Рисунок 35. Рабочий стол «Контроль рабочего времени»: общий вид

Рабочий стол «Контроль рабочего времени» отображает:

- Усредненные данные о том, когда сотрудники начинали и заканчивали работу;
- Сведения о средней по компании продолжительности рабочего дня на неделе;
- Средние показатели по активному и неактивному времени работы всех сотрудников на неделе.

Начало/окончание рабочего дня – момент первого/последнего в сутках перехвата модулем Endpoint Agent активности на рабочей станции (например, запуска какого-либо приложения).

Активное/неактивное время – промежуток времени, в течение которого в Solar Dozor поступала/не поступала информация об активных процессах на рабочей станции. Сотрудник считается неактивным после неактивности клавиатуры и мыши в течение

некоторого периода времени (значение по умолчанию — 15 минут, его можно настраивать от 1 мин до 24 часов)

При учете за сутки промежутки активного/неактивного времени суммируются.

Рисунок 36. РС «Контроль рабочего времени»: общие показатели деятельности сотрудников

Кроме того, на РСКрв отображается недельная статистика в разрезе выбранных групп:

- По среднему времени активности сотрудников, входящих в группы, можно быстро сравнить данные по активному времени работы сотрудников конкретной группы за текущую и предыдущую недели.
- По приложениям, которые использовали сотрудники, входящие в группы: можно получить общее представление о том, с какими приложениями работают сотрудники той или иной группы.

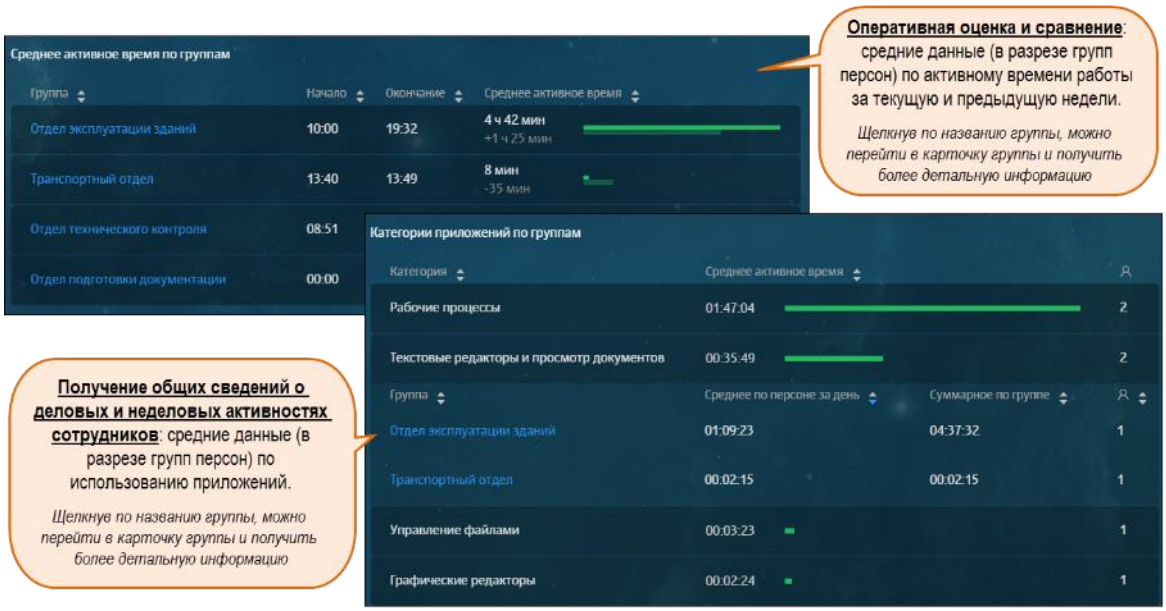


Рисунок 37. РС «Контроль рабочего времени»: недельная статистика в разрезе групп

6.4. Карточка группы: сведения о деятельности группы сотрудников на рабочих местах

Во вкладке «Рабочее время» можно просмотреть данные (за неделю) о том, как работают сотрудники группы: сколько времени тратят; какие приложения используют; когда начинают и заканчивают работу.

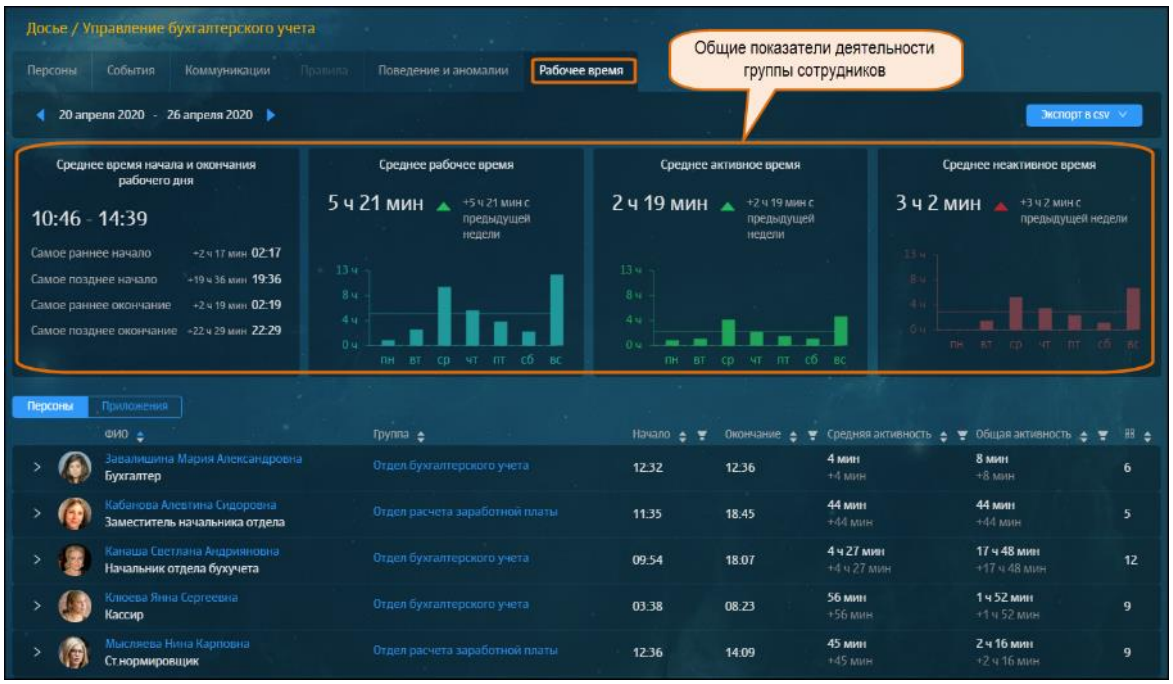


Рисунок 38. Карточка группы, вкладка «Рабочее время»: контроль рабочего времени группы сотрудников

Кроме блока с общими временными показателями группы («Среднее время начала и окончания рабочего дня», «Среднее рабочее/активное/неактивное время»), на вкладке имеется блок «Персоны/Приложения» со статистикой по сотрудникам/приложениям. Просмотрев эти данные, можно узнать статистику по:

- Количеству рабочих часов по каждому сотруднику;

- Использованию приложений и количество приложений, не относящихся к деловой активности, по каждому сотруднику;
- Началу и окончанию рабочего дня по каждому сотруднику.

Вид **Персоны** – список сотрудников группы с показателями их активности за выбранную неделю. Запись о сотруднике можно развернуть и посмотреть список приложений, в которых этот сотрудник работал. С помощью фильтров можно легко сужать выборку и находить сотрудников, которые недорабатывают/перерабатывают, не придерживаются рабочего графика и т.п.

Вид **Приложения** – список приложений с показателями активности работы в них за выбранную неделю. Запись о приложении можно развернуть и посмотреть список сотрудников, которые работали с этим приложением.

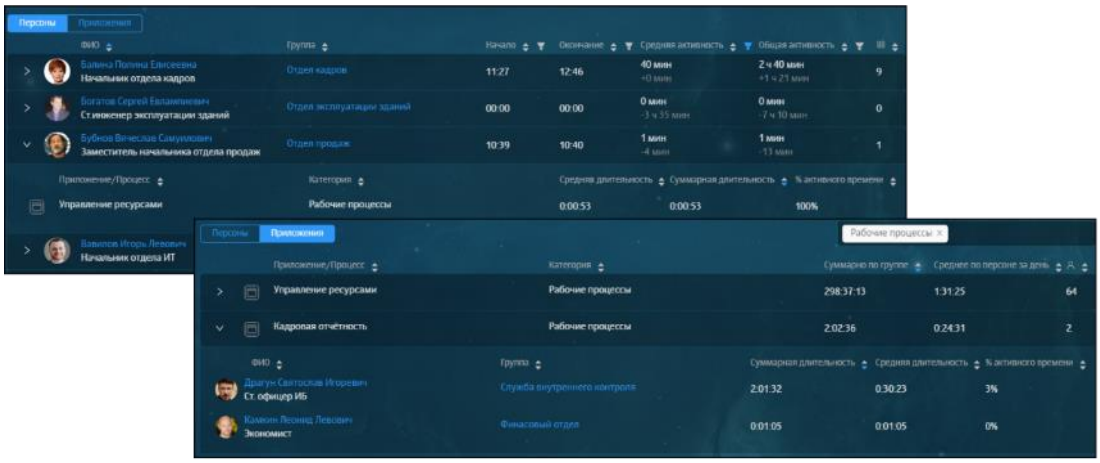


Рисунок 39. Контроль рабочего времени группы: данные в разрезе персон/приложений

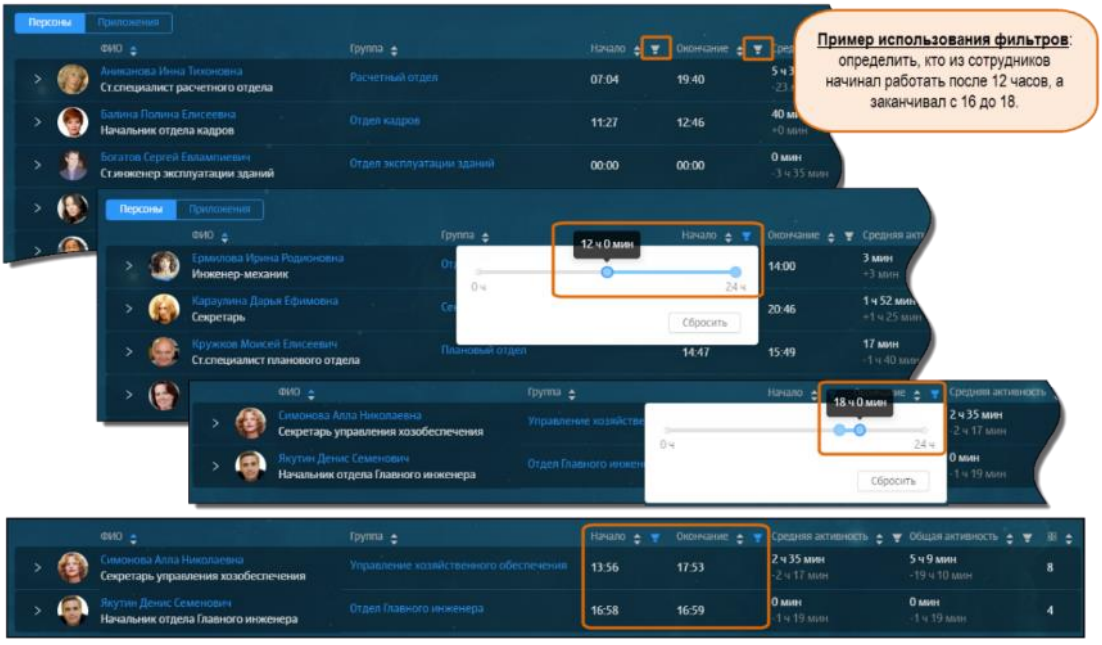


Рисунок 40. Контроль рабочего времени группы: пример использования фильтров

Сведения о рабочем времени группы сотрудников можно экспортировать в файл формата CSV. С помощью этих выгрузок можно строить отчеты по:

- Приложениям по дням/суммарно за период;
- Рабочим дням за период: аналог табеля.

6.5. Карточка сотрудника: сведения о деятельности сотрудника на рабочем месте

В карточке сотрудника можно просмотреть:

- Суммарные за конкретный день или период сведения о том, сколько времени сотрудник тратит на работу;
- Топ-5 категорий приложений, которые использовались сотрудником больше всего (за день или период);
- детальную статистику по использованию сотрудником рабочего времени: подробные данные о времени, проведенном как в приложениях, так и в интернете (за день или за период).

Данные отображаются как в текстовом виде, так и в виде диаграмм, где периоды работы персоны в конкретном приложении представлены как временные отрезки, выделенные определенным цветом.

Рисунок 41. Статистика за день: время, проведенное сотрудником в приложениях (вверху) и в интернете (внизу)

6.6. Контроль рабочего времени: особенности организации доступа к данным

Настройки КРВ позволяют задать доступ пользователей к данным о рабочем времени сотрудников. Можно задать:

- Отсутствие доступа к данным о рабочем времени;
- Полный доступ к данным о рабочем времени сотрудников всех групп (подразделений, групп особого контроля и т.п.);
- Доступ к данным о рабочем времени сотрудников только определенных групп.

При этом может быть задан полный или ограниченный доступ к данным Досье. Ограниченный доступ к Досье предполагает, что пользователю будут видны только краткие сведения о

сотрудниках из групп организационно-штатной структуры (ОШС). Доступа к переписке, группам особого контроля, коммуникациям и событиям, правилам политики для групп, сведениям о поведении и другим объектам Досье не будет.

Так можно организовать ограниченный доступ к данным, например, для специалистов HR-службы компании: только краткие сведения о сотрудниках определенных подразделений ОШС, включая данные о рабочем времени этих сотрудников.

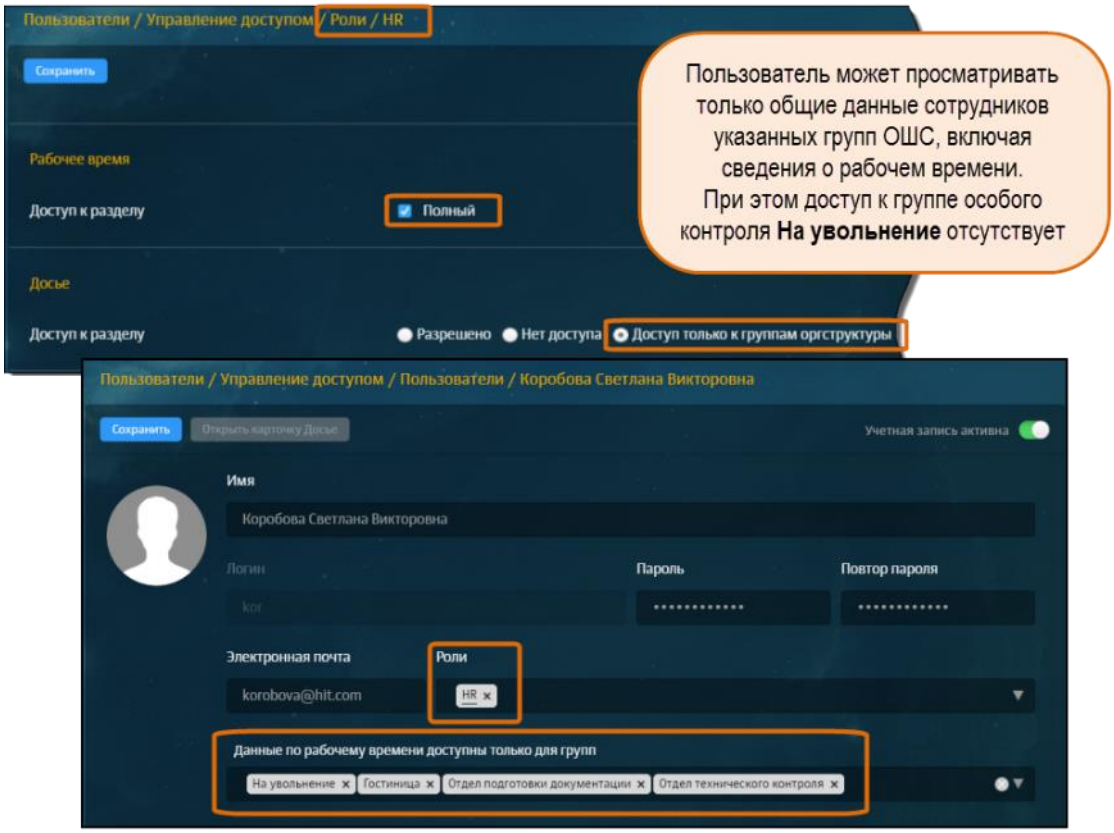


Рисунок 42. Пример настройки прав доступа для HR-специалиста

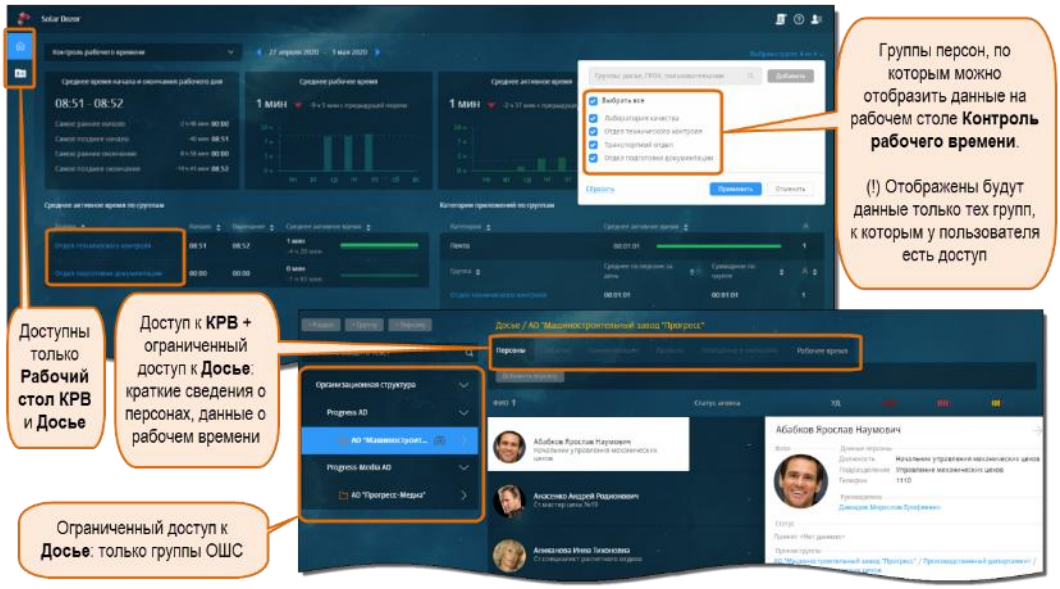


Рисунок 43. Ограниченный доступ к данным системы для HR-специалиста

7. Работа в территориально распределенном режиме

Офицеры безопасности, работающие в крупных территориально распределенных организациях с большой филиальной сетью, сталкиваются с трудноразрешимой проблемой — им очень сложно увидеть полную и актуальную картину происходящих процессов во всей организации. Часто имеющиеся данные по филиалам фрагментированы, отражают события ретроспективно или с задержкой по времени. Это может привести к запоздалой реакции на инцидент или ошибочным решениям по его отработке. Более того, инцидент может затрагивать сотрудников нескольких филиалов, но обнаружить их потенциально незаконную связь с помощью локальных инсталляций DLP-системы — сложная и трудоемкая задача.

Для решения этих проблем был создан новый модуль — MultiDozor. Он объединяет разрозненные инсталляции Solar Dozor в единую логическую структуру, предоставляя офицерам безопасности принципиально новые инструменты и возможности для обеспечения информационной и экономической безопасности организации. Например, MultiDozor позволяет в режиме реального времени централизованно контролировать процессы, получать аналитику и мониторить группы особого контроля в разрезе всей организации. Не менее важная функция, которую не могут предоставить другие DLP-системы — сквозные расследования по всей сети филиалов.

7.1. Архитектурные схемы работы MultiDozor

Функции MultiDozor могут быть активированы в различных ИТ-инфраструктурах с разными требованиями к обработке, хранению и передаче данных.

Поддерживаются следующие архитектурные схемы:

- Сообщения могут обрабатываться и храниться локально в филиалах. При этом работа с данными осуществляется как с единым целым;
- Сообщения могут храниться и обрабатываться централизованно. Например, при использовании общей корпоративной почты;
- Часть сообщений может быть общими для организации, другая же их часть может обрабатываться в филиалах и затем передаваться в общий центр обработки данных.

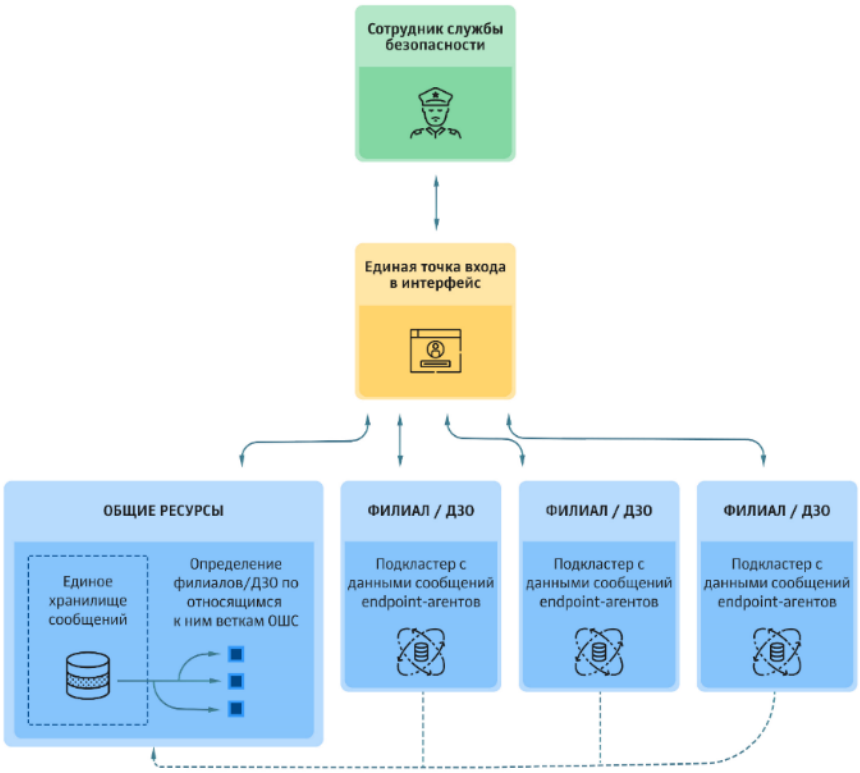


Рисунок 44. Один из вариантов конфигурации MultiDozor

7.2. Рабочие столы руководителя и аналитика

На рабочих столах руководителя и аналитика при подключении модуля MultiDozor возможно просматривать статистику филиалов, интересующих офицера безопасности. При выборе различных филиалов информация на рабочих столах перестраивается в соответствующих разрезах.

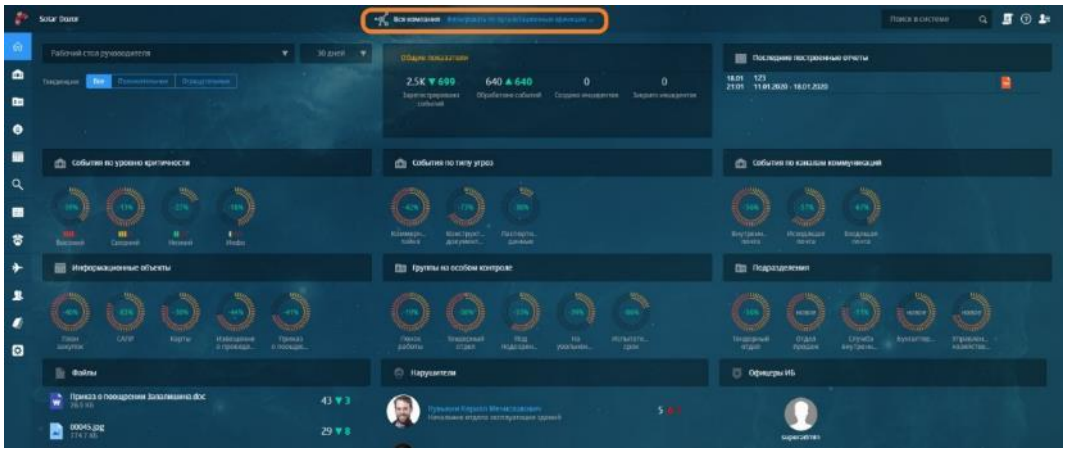


Рисунок 45. Влияние выбора филиалов на отображение данных на рабочем столе руководителя

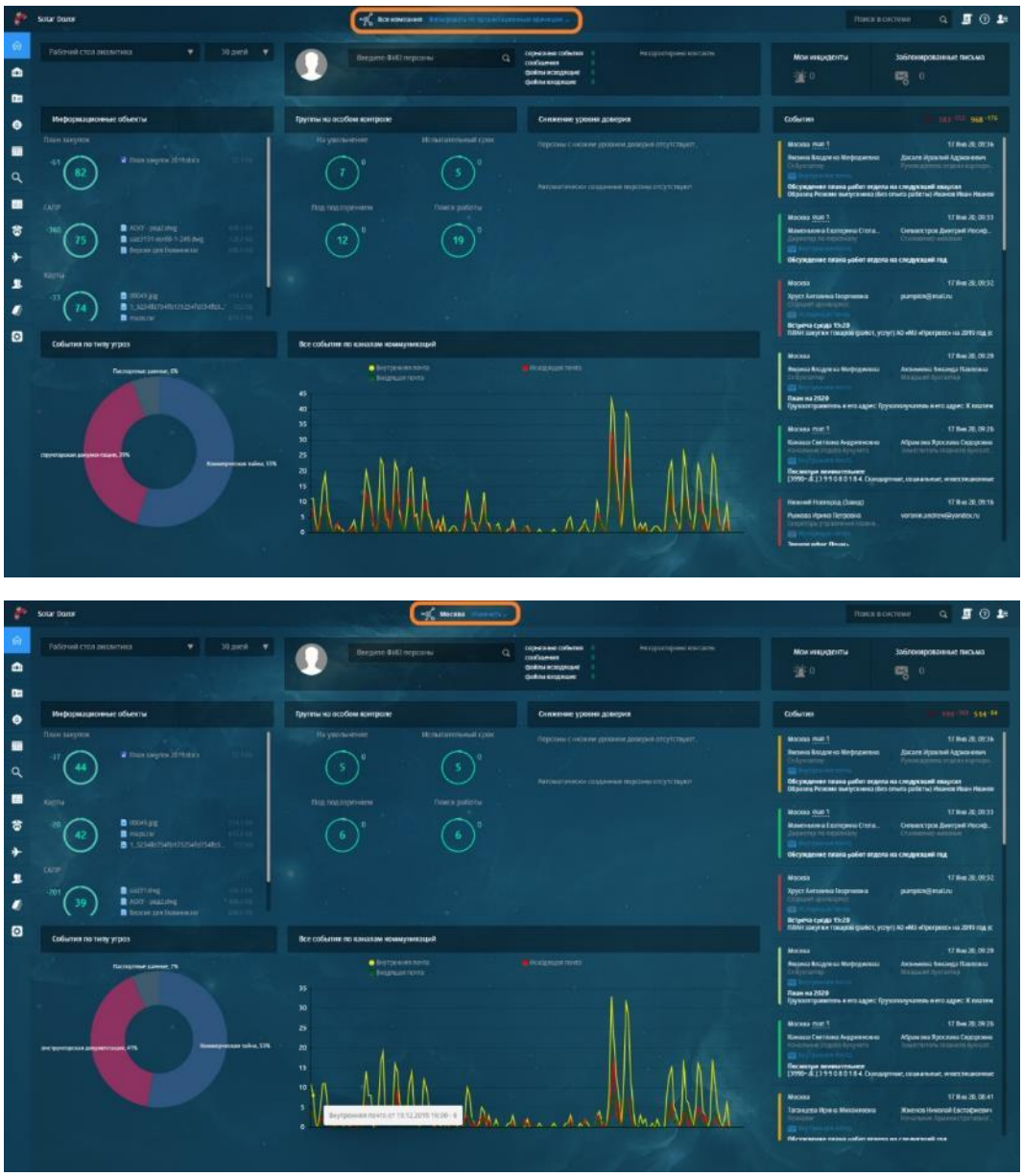


Рисунок 46. Влияние выбора филиалов на отображение данных на рабочем столе аналитика

7.3. Разграничение прав доступа офицеров безопасности к системе

Права доступа к данным распределяются как на общесетевом уровне организации, так и на уровне локальной сети филиала. Офицер безопасности, в зависимости от уровня доступа, может работать в системе:

- С данными всей организации;
- С данными нескольких филиалов;
- С данными конкретного филиала.

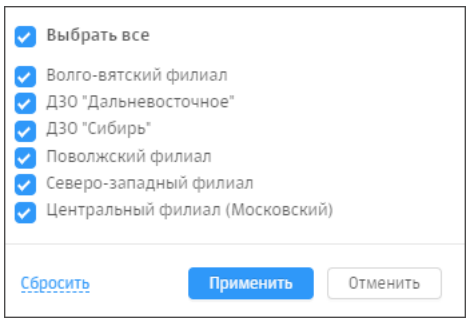


Рисунок 47. Элемент выбора филиалов

7.4. Работа с сообщениями, событиями и инцидентами в сети филиалов

- Поиск и работа с сообщениями, событиями и инцидентами осуществляется по филиалам в зависимости от прав доступа офицера безопасности;

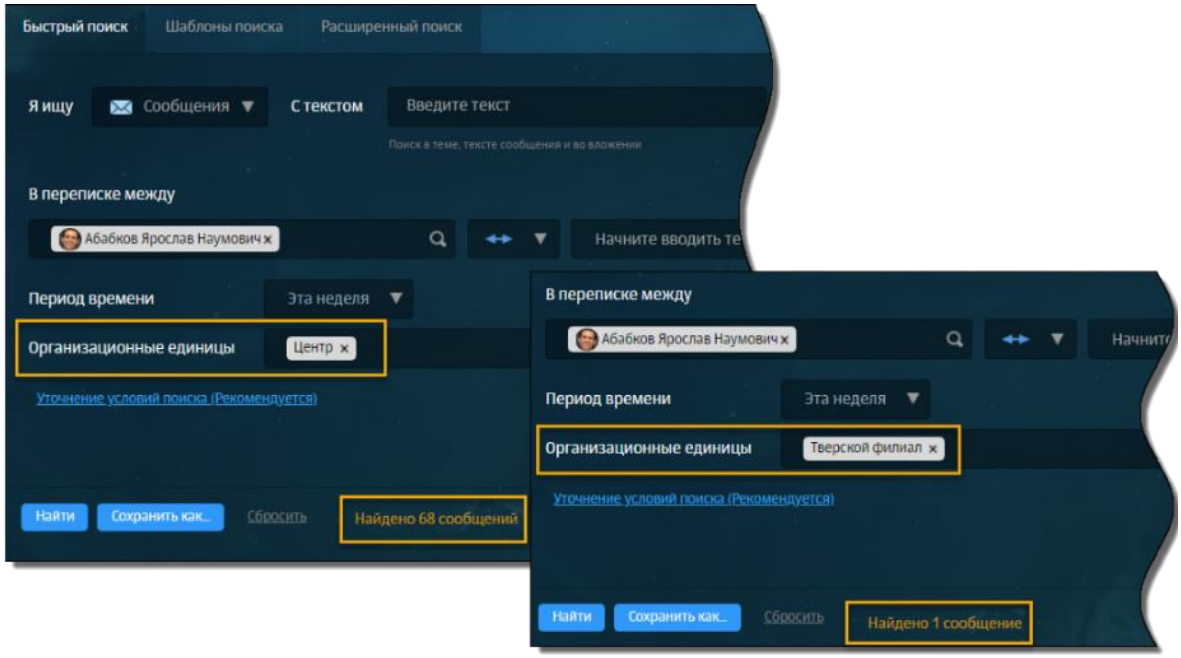


Рисунок 48. Выбор филиалов при выполнении быстрого поиска

- Принадлежность сообщений, событий и инцидентов к филиалам отображается как в их карточках, так и в результатах поисковых запросов.

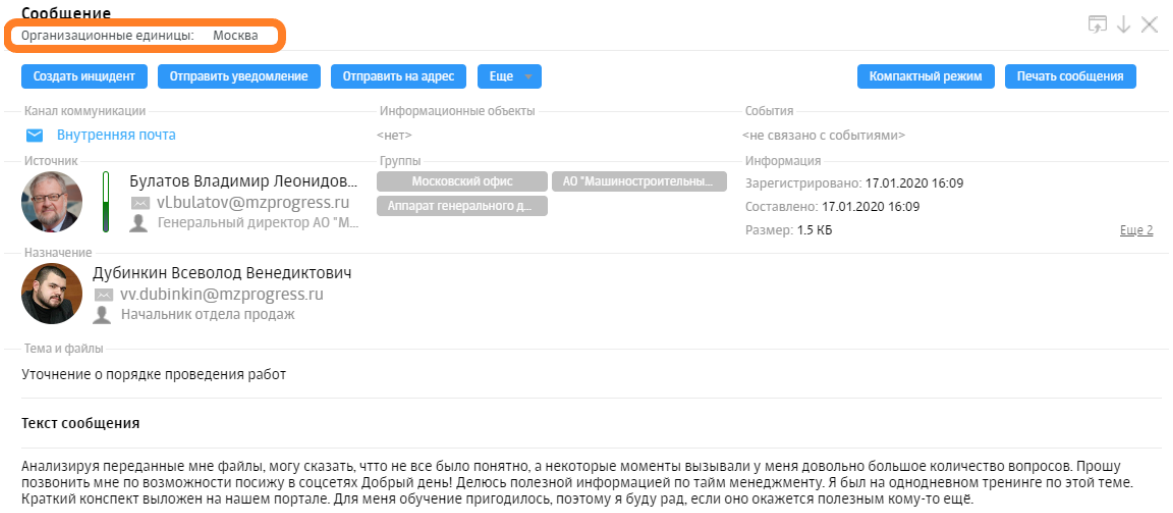


Рисунок 49. Отображение сведений о принадлежности сообщений к филиалам в карточке сообщения

7.5. Формирование отчетности

- При создании таких отчетов, как статистика по адресам, отчет в виде списка, сводный отчет по инцидентам, тепловая карта коммуникаций, офицеры безопасности могут выбрать те филиалы, по данным которых следует сформировать требующийся отчет;
- Информация о принадлежности сообщений, событий и инцидентов к филиалам отображается в интерфейсе печатных форм отчетов.

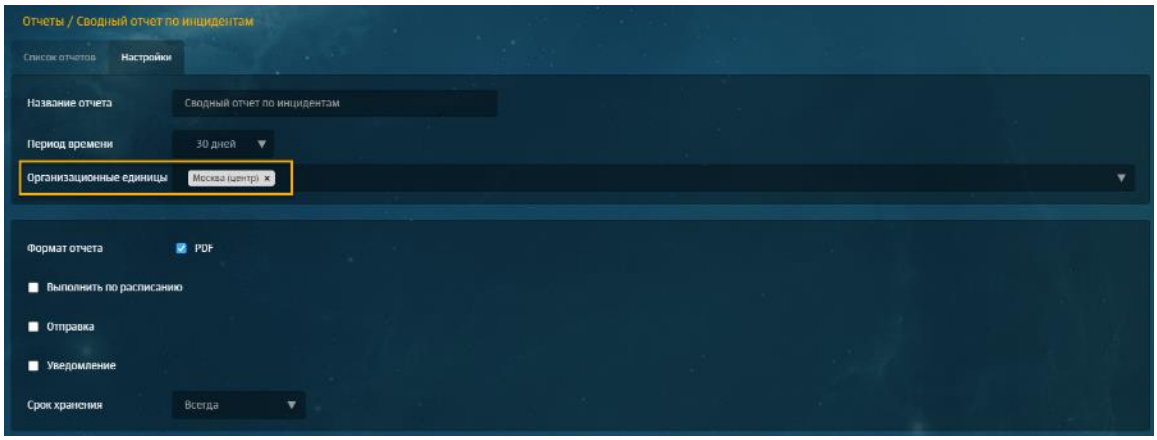


Рисунок 50. Выбор филиала при построении сводного отчета по инцидентам

7.6. Работа с группами особого контроля

- Мониторинг групп особого контроля осуществляется в каждом филиале отдельно;
- Видимость групп особого контроля и правил политики безопасности для этих групп ограничивается в соответствии с правами доступа офицеров безопасности.

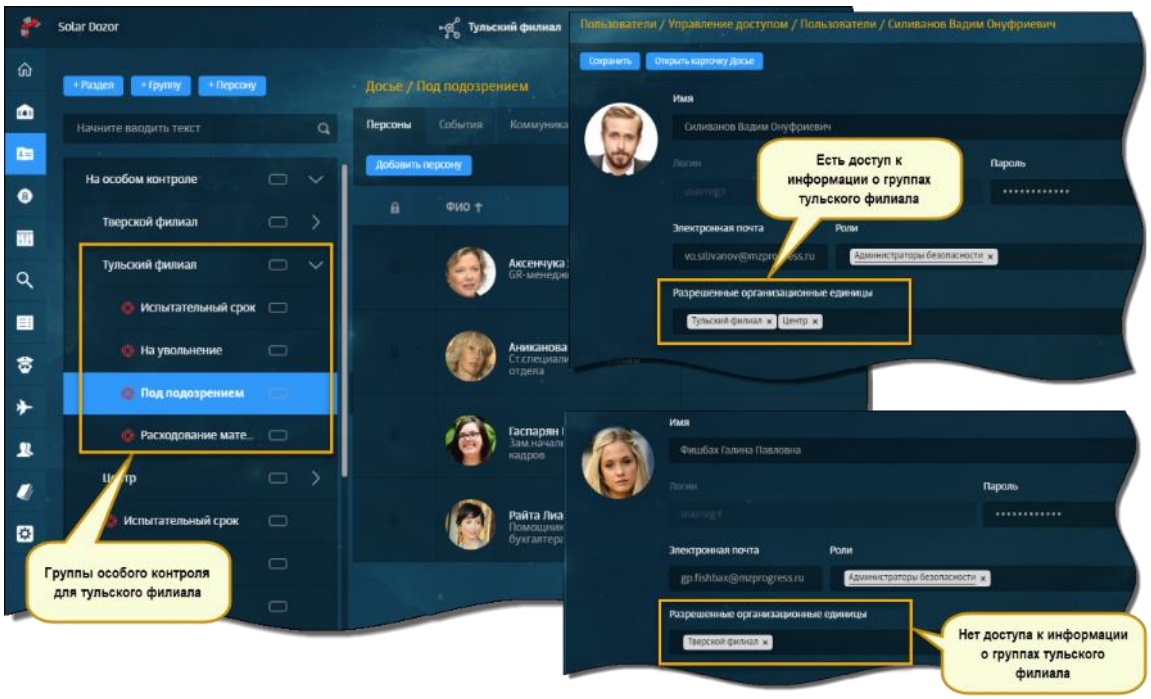


Рисунок 51. Работа с группами особого контроля в разрезах филиалов

7.7. Работа с досье и персонами в сети филиалов

- В карточках персон отображается информация о принадлежности к соответствующим филиалам;

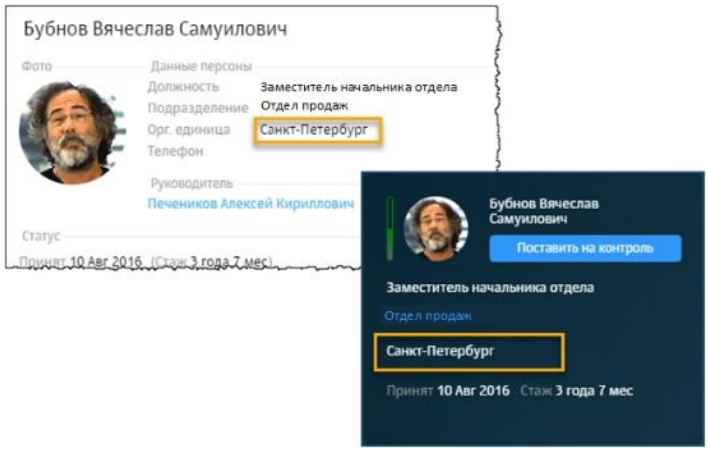


Рисунок 52. Отображение на карточках персон сведений о филиалах, в которых они числятся

- Доступ офицеров безопасности, работающих с данными только своих филиалов, к данным персон из других филиалов организации ограничивается общими сведениями.

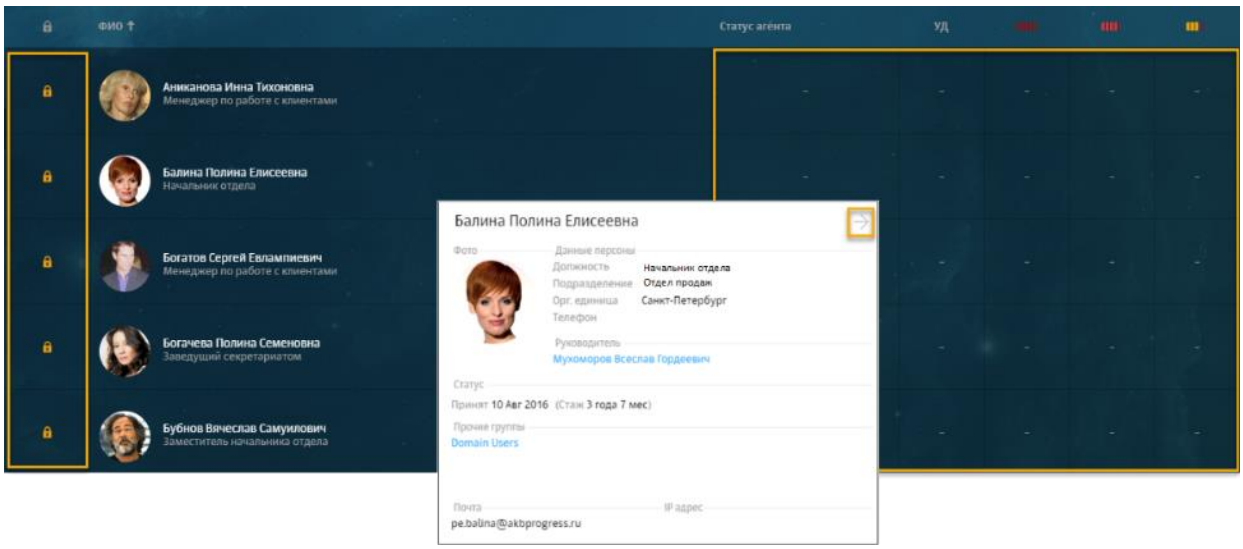


Рисунок 53. Доступ к данным персон, числящихся в филиалах, отличных от доступных сотруднику службы безопасности

7.8. Настройка политики безопасности и работа с информационными объектами:

Политика безопасности настраивается централизованно и распространяется по филиалам после ее применения.

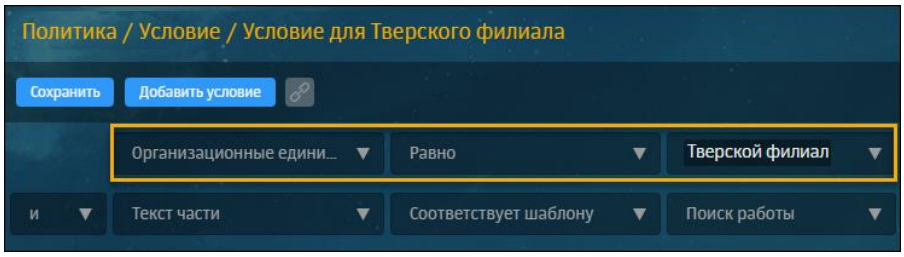


Рисунок 54. Настройка условия политики безопасности для применения к филиалу

При этом можно настроить специфические правила политики для определенных филиалов. Настраиваются как общие по организации детектируемые информационные объекты, так и информационные объекты, специфичные для определенных филиалов.

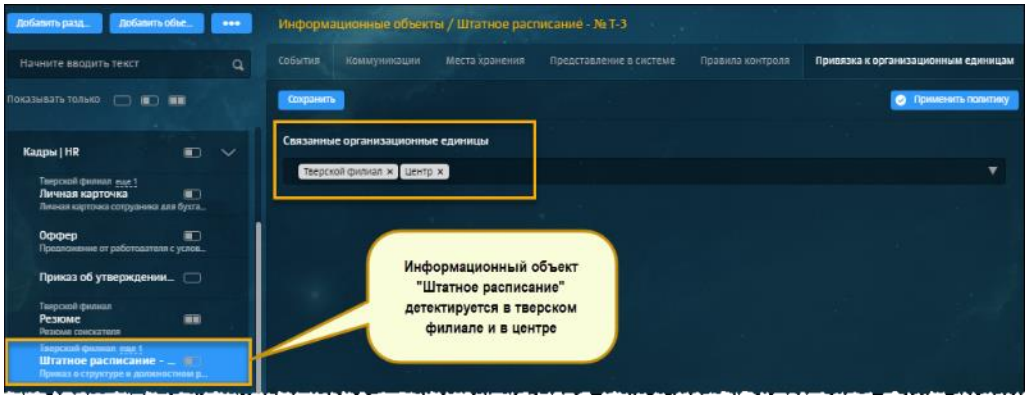


Рисунок 55. Настройка информационного объекта для использования в филиалах

7.9. Управление Dozor Endpoint Agent

Видимость групп Dozor Endpoint Agent и данных агентских приложений ограничивается в соответствии с правами доступа офицера безопасности к данным филиалов.

Управление Dozor Endpoint Agent может выполняться как централизованно, так и локально – уполномоченными специалистами службы безопасности или ИТ-подразделения в каждом из филиалов организации.

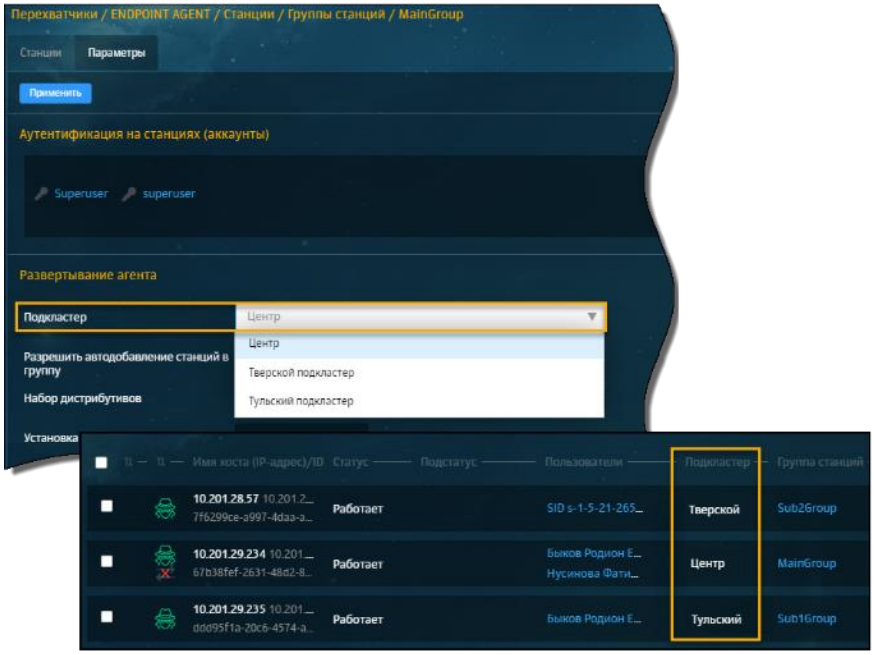


Рисунок 56. Настройка агентов, разворачиваемых на территориально распределенных технических ресурсах организации

7.10. Мониторинг технического состояния системы

Для проведения технического обслуживания и выявления проблем в работоспособности технических ресурсов территориально распределенной системы Solar Dozor добавлена возможность выбора для мониторинга только тех технических ресурсов филиалов, которые интересуют ответственного специалиста.

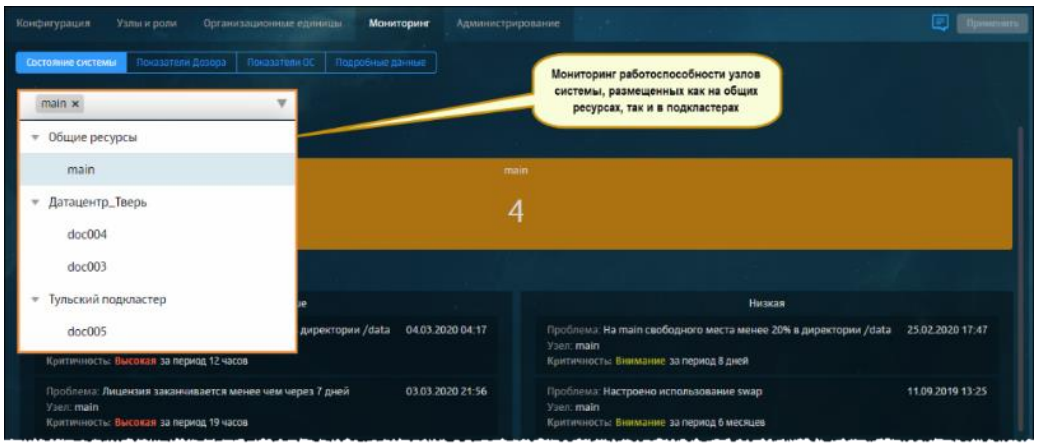


Рисунок 57. Мониторинг технического состояния системы Solar Dozor, работающей в территориально распределенном режиме

8. Администрирование и безопасность

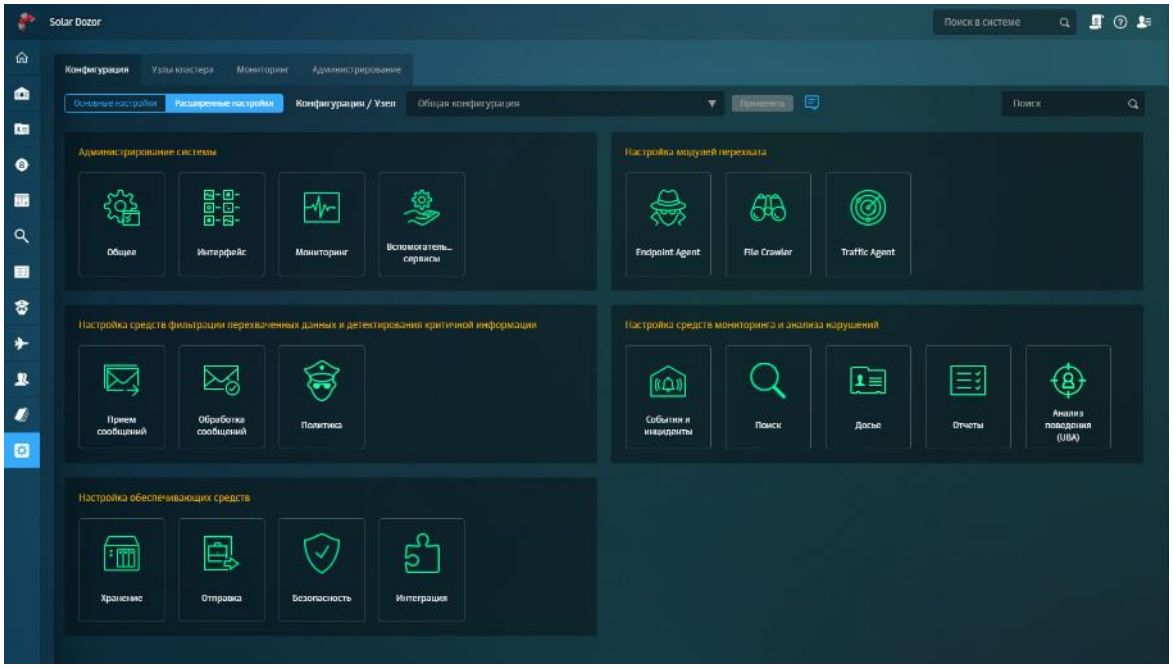


Рисунок 58. Расширенные настройки Solar Dozor

Повышение безопасности DLP-системы

Так как у ИБ-аналитиков и администраторов DLP-систем есть доступ к критическим данным переписки сотрудников организации, потенциально они могут использовать их в личных целях, вносить изменения и влиять на ход расследования. Для снижения этих рисков в Solar Dozor реализованы инструменты по мониторингу действий пользователей и гибкая система управления пользователями, позволяющая легко создавать и удалять учетные записи.

Поддерживается гранулированное управление доступом, разграничивающее права на отдельные разделы интерфейса, объекты и функции системы.

В Solar Dozor также можно определить, от какой сторонней системы по протоколу ICAP поступает трафик на сервер фильтрации, а также — ошибки, связанные с этим трафиком. Для каждого ICAP-источника можно настроить триггеры, которые срабатывают в случаях отсутствия полученных сообщений, отсутствия обработанных сообщений и наличия ошибок при обработке сообщений. Сервис фильтрации обладает возможностью балансировки трафика с учетом нагрузки.

Благодаря этому можно оперативно определить и устранить проблемы с поступлением/обработкой трафика, что важно для контроля и предотвращения утечки информации из внешней системы.

Аудит действий пользователей системы

Журнал действий пользователей Solar Dozor содержит максимально детализированные записи о том, кто, когда и что делал в системе. Это позволяет решить проблему «наблюдения за наблюдателями», когда нужно контролировать действия как конкретных ИБ-специалистов, так и всех пользователей Solar Dozor.

Система поддерживает отправку уведомлений, срабатывающую при заданных условиях, что позволяет оперативно реагировать на недопустимые действия пользователей и минимизировать негативные последствия.

Интерфейс управления конфигурацией

Solar Dozor обладает широкими возможностями диагностики и администрирования, настройки и проектирования. Большая часть операций по обслуживанию системы и мониторинг состояния осуществляется с помощью веб-интерфейса. Нужный параметр настройки можно легко найти с помощью интуитивной группировки и быстрого сквозного поиска.

Модульная структура Solar Dozor позволяет настраивать производительность, надежность и скорость работы в зависимости от имеющихся задач, оборудования и трафика, а также избегать единой точки отказа. Доступна тонкая настройка — можно изменять такие технические параметры как нагрузка на сеть, на CPU, распределение нагрузки на узлы и т. д.

Объединение серверов в группы и отображение информации о работе групп серверов

В системе можно создавать и выбирать группы серверов, по которым нужно отобразить информацию. Так, например, можно отобразить показатели группы серверов, которые являются фильтрами для обработки почтового трафика, или показатели группы агентских серверов.

Таким образом, можно отслеживать показатели работы групп серверов, которые решают одинаковые задачи, и оценивать нагрузку именно по этим укрупненным показателям

Настройка действий системы

Для администраторов доступна настройка действий по условиям и показателям, что позволяет автоматизировать действия системы, такие как отправка уведомлений на электронную почту в зависимости от параметров или по событиям.

Статус активности и целостности Dozor Endpoint Agent

У каждой рабочей станции с установленным агентом в Solar Dozor есть своя карточка, где отражаются сведения о статусе агента, актуальности настроек и политик, целостности агента, а также технические данные о рабочей станции.

Функция контроля статуса активности агентского модуля обеспечивает непрерывность мониторинга действий сотрудников на рабочих станциях. Офицер безопасности может практически в любой ситуации проверить стабильность связи агентов с центральным сервером — например, когда просматривает группы пользователей или отдельные карточки сотрудников. Индикатор статуса показывает, был ли установлен на рабочую станцию агент, его активность на данный момент, а также время отключения при потере связи.

При угрозе несанкционированного доступа к агенту, например, для его отключения или удаления, в системе создается событие с высоким уровнем критичности. Статус агента изменяется на «Поврежден». Также можно настроить запись логов о нарушении целостности агента в журнал syslog.

Управление Dozor Endpoint Agent

Все операции по развертыванию агентов и управлению ими выполняются в едином удобном интерфейсе. Офицер безопасности может централизованно устанавливать агентов на рабочие станции, настраивать политики и отслеживать их состояние, а также перезагружать рабочие станции при необходимости настройки каналов перехвата. Начиная с версии Solar Dozor 7.9 доступно автоматическое развертывание агента на новых станциях, добавленных в группы AD и ALD Pro для агентов под ОС Linux и FreeIPA для агентов под ОС Linux и Windows.

При возникновении проблем во время установки Dozor Endpoint Agent система может выявить и подсветить следующие проблемы:

- наличие версии ОС, которая не поддерживается для установки Dozor Endpoint Agent;
- отсутствие необходимых для развертывания агента обновлений ОС;

- обнаружение ПО, которое может вызывать проблемы в работе Dozor Endpoint Agent или ОС;
- отсутствие доступа к рабочей станции во время установки Dozor Endpoint Agent;
- ошибка подключения к рабочей станции из-за неверного имени пользователя или пароля.

В случае выявления проблемы пользователь получает соответствующее уведомление.

Можно сформировать и скачать отчет об актуальном состоянии списка агентов, предварительно отфильтровав его по требуемым параметрам.

Также, например, при проведении профилактических работ есть возможность из интерфейса деактивировать и активировать агенты. При этом все настройки сохраняются, и переналадка агента при повторной активации не требуется.

Поддержка сред виртуализации

В Solar Dozor поддерживается работа с временными виртуальными машинами на основе популярных сред виртуализации (Citrix VDI, KVM, Hyper-V и т. д.). Dozor Endpoint Agent можно включить в «золотой образ» (Master Image) — готовое состояние виртуальной станции. Это позволяет в короткие сроки разворачивать и изменять инфраструктуру, включающую перехватчик Solar Dozor для рабочих станций.

Справочник приложений

В Solar Dozor доступен справочник приложений, содержащий записи о приложениях, процессах и веб-ресурсах. Большое количество записей позволяет точно настраивать политику безопасности. Все приложения/категории делятся на системные («из коробки») и пользовательские (создаваемые пользователем). Такое деление позволяет исключить конфликты импорта и обновления справочника, возникающие при изменении его структуры. Справочник приложений постоянно обновляется.

Поддержка модели здоровья Zabbix

В Solar Dozor реализован новый интерфейс на базе универсальной системы мониторинга Zabbix. Информация в разделе сгруппирована — можно просмотреть сведения по каждому узлу кластера Solar Dozor, конкретному сервису или определенному показателю/группе показателей.

В результате системный администратор может оперативно получить:

- сводную информацию о состоянии и проблемах в работе Solar Dozor;
- сведения о значениях и динамике показателей работы Solar Dozor;
- информацию о значениях показателей операционной системы.

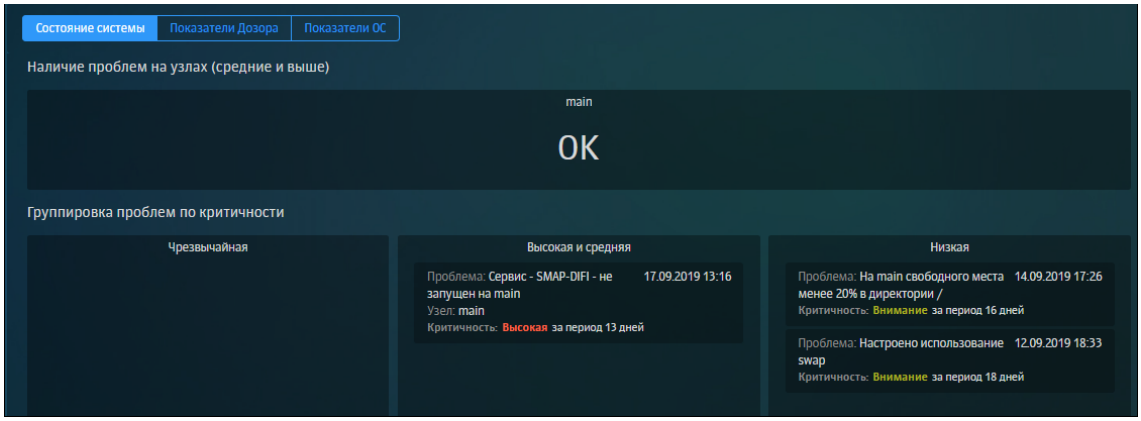


Рисунок 59. Диагностика проблем Solar Dozor

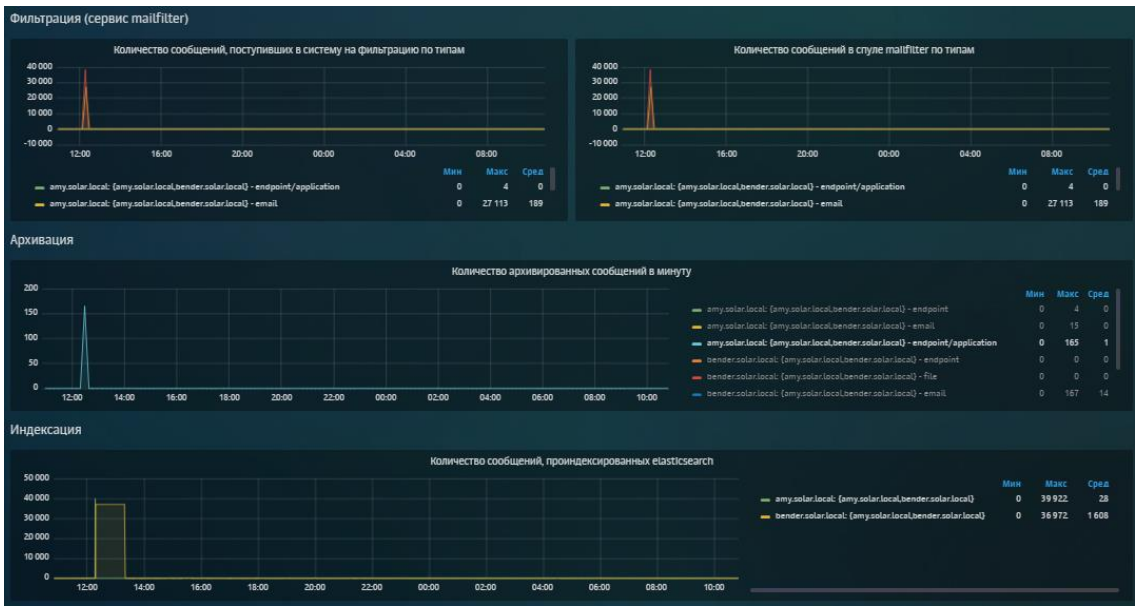


Рисунок 60. Сведения о показателях работы Solar Dozor

Рисунок 61. Сведения о показателях работы ОС

9. Концептуальная архитектура

Solar Dozor состоит из трех функциональных блоков:

- **Базовый модуль системы** (Dozor Core), отвечает за реализацию основных функций системы. Состоит из редактора политик безопасности, подсистем оперативного хранения данных, поиска и управления событиями и инцидентами ИБ, отчетности, а также включает единый интерфейс управления.

- **Модули расширения** (Dozor Dossier, Dozor UBA, Dozor Long-term Archive, Dozor OCR, MultiDozor, MultiConnector) предоставляют дополнительные инструменты для выявления аномалий, аналитики, построения отчетов, управления долговременными архивами и распознавания графических документов, а также для управления филиалами.

- **Модули-перехватчики** (Dozor Mail Connector, Dozor Traffic Analyzer, Dozor Endpoint Agent, Dozor File Crawler) обеспечивают контроль коммуникаций сотрудников по всем ключевым каналам: корпоративная почта, доступ в интернет, сетевой трафик, действия на рабочих станциях и файлы в корпоративной сети.

Благодаря такому подходу обеспечивается гибкость как в установке, настройке и эксплуатации, так и в лицензионной политике при продаже. Блоки и модули могут комбинироваться и масштабироваться в соответствии с размером организации (от компаний среднего бизнеса до крупных холдингов и органов государственной власти с обширной сетью филиалов).

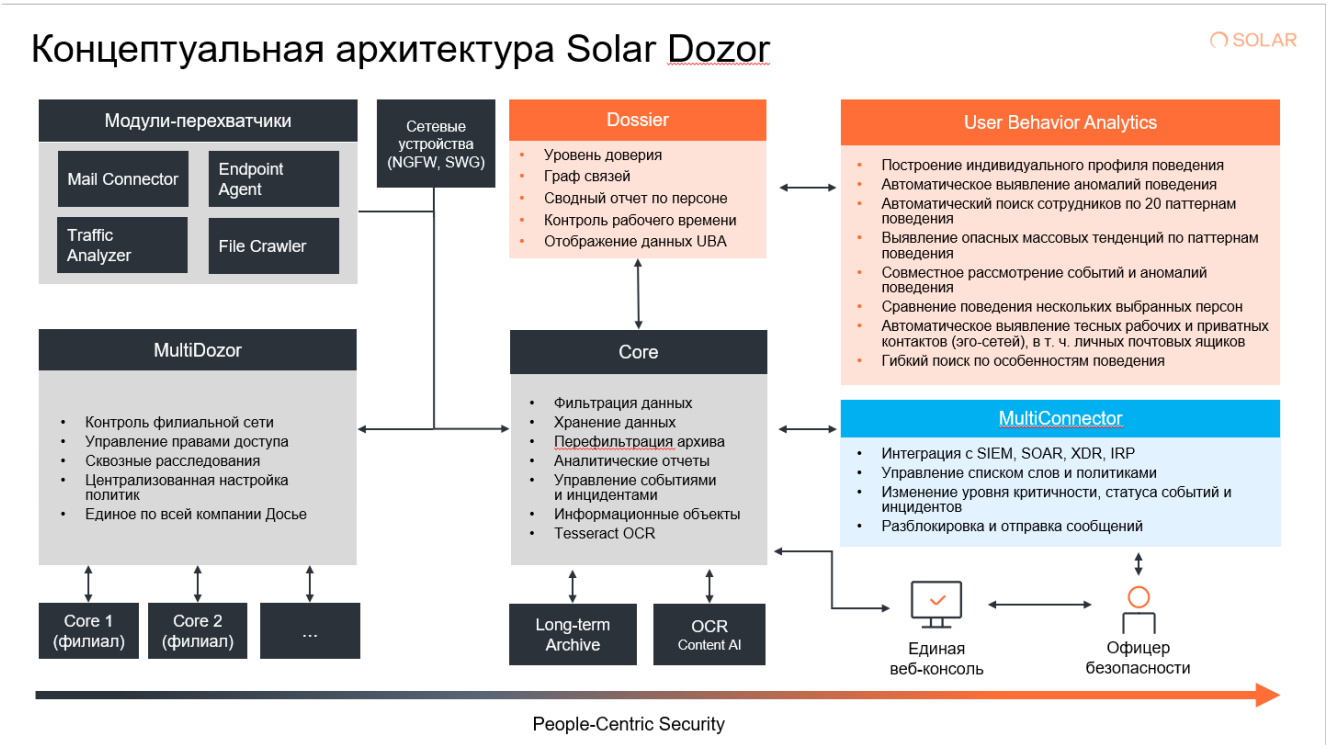


Рисунок 62. Концептуальная архитектура Solar Dozor

9.1. Dozor Core

Базовый модуль системы. Состоит из подсистем хранения, поиска и управления инцидентами, отвечающих за реализацию центрального компонента решения. Может быть расширен опцией долговременного хранения для увеличения плеча и глубины расследований инцидентов. В состав уже входит система оптического распознавания текста (OCR) Tesseract, что позволяет распознавать конфиденциальную информацию в графических файлах, которые

присылают для анализа перехватчики. При необходимости можно подключить лицензируемый модуль Dozor OCR, использующий технологии распознавания компании Content AI.

Состав Dozor Core:

- Подсистема фильтрации вместе с редактором политик безопасности;
- Подсистема оперативного хранения;
- Подсистема поиска;
- Подсистема управления событиями и инцидентами;
- Подсистема отчетности (включает, помимо прочего, сводный отчет по инцидентам и тепловую карту коммуникаций);
- Единый интерфейс управления.

9.2. Dozor Long-term Archive

Модуль долговременного (от 6 месяцев до более 10 лет) хранения архива коммуникаций. Позволяет управлять несколькими хранилищами, переносить данные на долгосрочное хранение, отключать и подключать обратно части базы данных сообщений, в т. ч. можно записать их на ленту, а позже — подключить обратно для расследования. Dozor Long-term Archive будет полезен организациям, которым требуются инсталляции с большим объемом или сроком хранения данных, или же нужно снизить деградацию производительности на больших объемах данных.

9.3. Dozor OCR

Модуль распознавания текста Dozor OCR позволяет защитить конфиденциальные данные от утечки, даже если они конвертированы в графический формат — отсканированы, сфотографированы, сохранены в PDF, распечатаны, сняты с экрана в виде скриншотов и т. д.

К перехваченным и распознанным сообщениям с графическими файлами применяются политики безопасности и правила обработки документов: полнотекстовый поиск, контентный и контекстный анализ.

В основе модуля Dozor OCR лежат технологии ведущего разработчика OCR-решений — компании Content AI, что обеспечивает следующие показатели работы:

- Производительность и скорость распознавания до 1 ТБ в сутки — до 380% быстрее аналогов;
- Точность до 98% — на 12% точнее для типовых и на 35% для сложных изображений;
- Расширенные возможности анализа — удаление шумов, мусора, определение и корректировка ориентации изображения и т. п.

Основные функции

Поточное распознавание, извлечение и преобразование изображений в текст из графических файлов следующих форматов:

- BMP (Bitmap Picture);
- JPEG (в том числе JPEG2000);
- PNG (в том числе ISO 15948 и RFC 2083);
- TIFF (в том числе ISO 12639, ISO 12234-2);
- PDF (в том числе IDO 32000, PDF/A, PDF/E, PDF/UA, PDF/VT, PDF/X)

- QR-коды.

Этапы работы

1. Ядро системы Dozor Core обнаруживает данные в формате изображений (скан документа, фотографию и т. п.).
2. Обнаруженные изображения передаются на распознавание в Dozor OCR.
3. Dozor OCR распознает изображения и передает извлеченную текстовую информацию (TEXT/PLAIN) обратно в Dozor Core.
4. Dozor Core проверяет полученную текстовую информацию на нарушение политики безопасности организации.
5. В случае обнаружения Dozor Core фиксирует нарушения корпоративной политики.

9.4. Dozor Dossier

Модуль расширенного досье для продвинутой аналитики персон и расследования инцидентов ИБ. Аналитические инструменты этого модуля позволяют выявлять скрытые связи сотрудников, строить отчеты по персоне, исследовать интенсивность коммуникаций и используемые при этом каналы. Кроме этого, в модуле Dozor Dossier аккумулируется информация из модуля автоматического анализа поведения пользователей Dozor UBA.

Основные функции

- Построение уровня доверия сотрудника, отображение графика изменения уровня доверия персоны, отображение текущего уровня доверия персоны на виджетах рабочего стола и в карточках персоны, сообщений и событий;
- Построение графа связей персоны;
- Отображение данных UBA в виде виджетов (сведения о нехарактерных контактах и аномальном поведении сотрудников);
- Обнаружение изменений в профиле нарушений сотрудника или его внешнего адреса.
- Сводный отчет по персоне – консолидация в виде статистики коммуникаций, контактов, действий, нарушений персоны за указанный период времени;
- Контроль рабочего времени сотрудника для отслеживания его рабочей и нерабочей активности в течение рабочего дня.

9.5. Dozor UBA

Dozor UBA — модуль продвинутой аналитики, предназначенный для мониторинга динамики поведения персон, выявления аномальных поведенческих отклонений от нормы, поиска особенностей поведения, интересных с точки зрения безопасности, сравнения и анализа особенностей поведения персон, формирования аналитического наполнения Досье и расследования инцидентов информационной и экономической безопасности и случаев внутреннего мошенничества. Например, обнаружение действий менеджера по закупкам, иногда использующего аффилированные компании для участия в тендерах. Или инсайдера, незаметно время от времени устраивающего утечки.

Аналитическая модель модуля UBA базируется на теории вероятности, теории случайных процессов и теории графов. При этом не требуется предварительная настройка и адаптация модуля под условия эксплуатации — он полностью интегрирован в Solar Dozor и готов к работе.

Для предварительного анализа достаточно накопить массив данных о коммуникациях сотрудников за 1 месяц, для точной работы — за 2–3 месяца. Если организация уже использует Solar Dozor, то анализ поведения пользователей доступен сразу. Показатели рассчитываются ежесуточно.

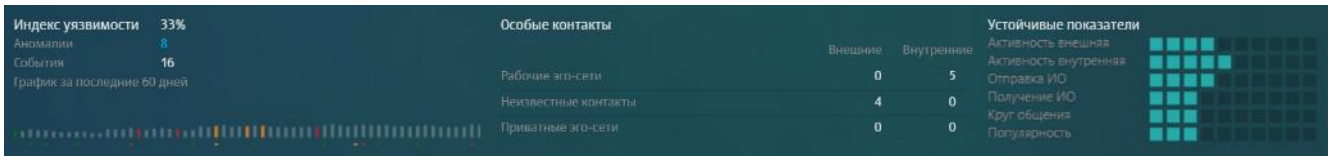
Решаемые задачи

- Построение индивидуального профиля поведения.
- Автоматическое выявление аномалий поведения.
- Автоматический поиск сотрудников по 20-ти паттернам поведения.
- Выявление опасных массовых тенденций по паттернам поведения.
- Совместное рассмотрение событий ИБ и аномалий поведения.
- Сравнение поведения нескольких выбранных персон.
- Выявление тесных рабочих и приватных контактов (эго-сетей).
- Автоматическое определение неизвестных контактов, в т. ч. личных почтовых ящиков.
- Гибкий поиск по особенностям поведения.

Принцип работы

Модуль использует и обрабатывает данные, перехваченные по следующим каналам коммуникации: электронная почта (внутренняя, исходящая, входящая), мессенджеры, комбинация обоих видов каналов. На основе этих данных формируются поведенческие профили персон и выявляются аномалии поведения. При этом для построения корректной аналитической картины достаточно данных, накопленных за 1–2 месяца.

Поведение человека описывается в системе с помощью специальных показателей. Значение конкретного показателя в профиле персоны всегда относительно — показатели ранжируются по уровням от 0 до 5 с шагом 0,5 относительно всех персон в компании:



Набор показателей, характеризующий конкретное поведение, называется типом поведения. Например, для сотрудников, работающих с 23:00 до 06:00, можно выделить тип поведения «Работа ночью». Один и тот же тип поведения может быть как у одного, так и у нескольких сотрудников. С другой стороны, у сотрудника могут наблюдаться признаки разных типов поведения.

Особенности работы в территориально распределенном режиме

Офицер безопасности может выбирать интересующую его организационную единицу, просматривать паттерны с попавшими в них персонами из выбранной орг. единицы и тенденциями за неделю, а также делать выборку по заданному паттерну поведения.

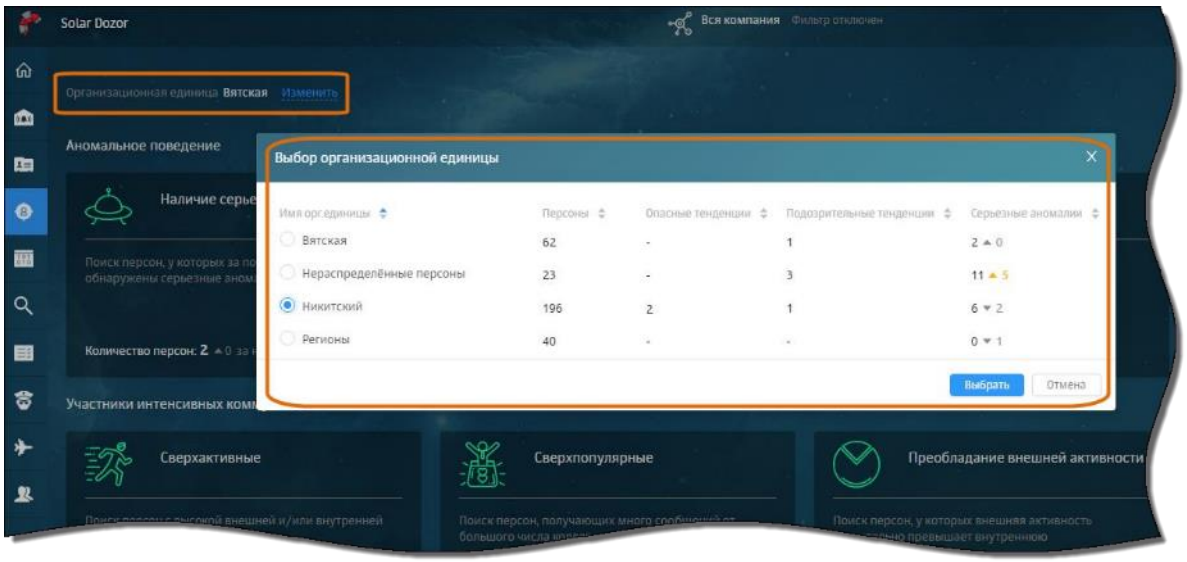


Рисунок 63. Выбор организационной единицы

Благодаря всплывающему окну с темами сообщений и участниками переписки при переходе в исходящие или входящие сообщения с особыми контактами персоны не теряется контекст. Информация о персонах из особых контактов дополнена сведениями о должности.

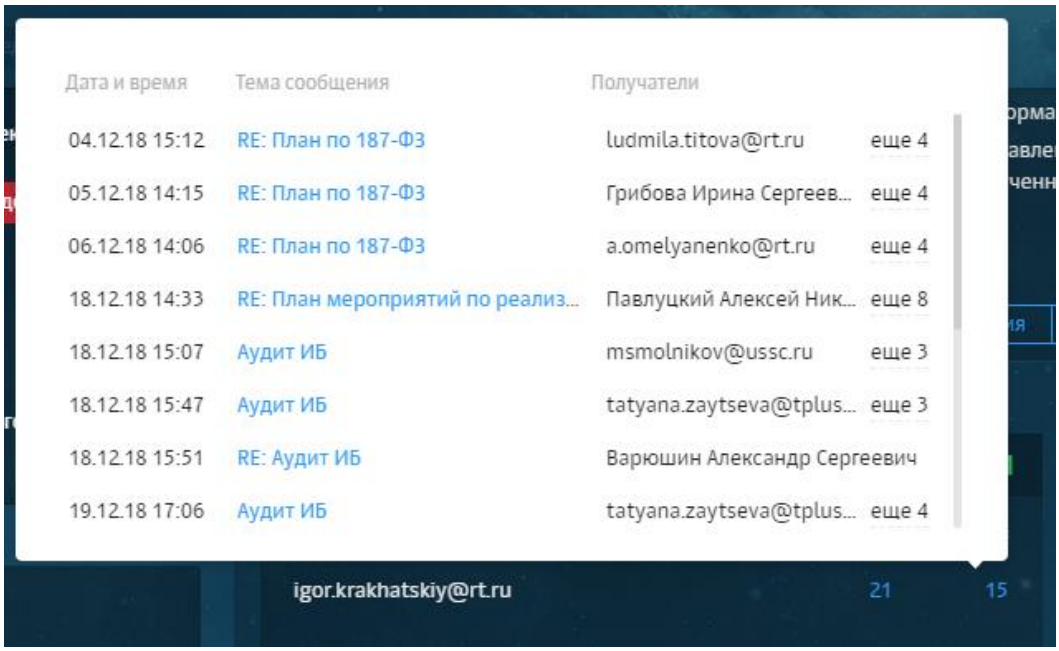


Рисунок 64. Особые контакты. Всплывающее окно с сообщениями

При построении профиля поведения сотрудника учитывается часовой пояс региона, где работает конкретный сотрудник. К примеру, часовые пояса учитываются при определении типов поведения «Работа ночью», «Работа в выходные дни» и «Признаки увольнения», а также в статистике суточной активности сотрудников.

9.6. Dozor Mail Connector

Модуль контроля коммуникаций, проходящих через корпоративные почтовые системы.

Основные функции

- Мониторинг сообщений почтовых серверов: Microsoft Exchange Server, CommuniGate Pro, Zimbra и других популярных SMTP-серверных платформ;

- Мониторинг и блокирование отправки почтового сообщения, нарушающего политики безопасности, безусловно или до получения подтверждения отправки от администратора безопасности или пользователя (карантин);

- Возможность удаления нарушающих политику частей сообщения и реконструкции почтовых сообщений, в том числе части содержимого вложенных архивов, или добавление текста в тело сообщения.

Этапы работы

1. Прием копии сообщений корпоративной почты от почтового сервера с применением правил журналирования или при помощи fetchmail.
2. Блокировка (помещение в карантин) сообщений, нарушающих настроенные политики безопасности.
3. Маршрутизация исходящей почтовой переписки через сервер Solar Dozor при установке системы в разрыв сети.
4. Проведение сквозных расследований на распределенном по всей организации архиве данных;

На корпоративную почту приходится более 50% всех утечек данных и мошеннических схем, поэтому ее рекомендуется контролировать в полном объеме. Режим контроля (мониторинг или блокировка) зависит от задач безопасности и критичности утечки информации в организации.

9.7. Dozor Traffic Analyzer

Модуль перехвата и распознавания сетевого трафика (сниффер) разбирает, анализирует и восстанавливает сообщения, передаваемые по протоколам прикладного уровня, извлекает из сообщений контент и отправляет их в Dozor Core для анализа и хранения.

Основные функции

Перехват данных:

- Веб-почты;
- Социальных сетей, форумов, блогов;
- Сервисов передачи файлов;
- Сервисов мгновенных сообщений;
- Почтовых протоколов;
- Нажатия клавиш (кейлогер);
- Снимки экрана;
- Сервисов поиска работы.

Этапы работы

1. Захват входящего и исходящего трафика (зеркалирование со SPAN-порта или ICAP с прокси-сервера), пересборка пакетов.
2. Обработанный трафик анализируется средствами Dozor Traffic Analyzer.
3. В результате анализа сформированное сообщение отправляется в Dozor Core на фильтрацию согласно настроенным правилам политики.

Модуль Dozor Traffic Analyzer, необходимый для анализа SPAN-трафика, — обязательное связующее звено при интеграции прокси-сервера и Solar Dozor.

9.8. Dozor Endpoint Agent

Модуль контроля рабочих станций под управлением трех наиболее популярных операционных систем: Windows, Linux и macOS[1]. Перехватывает и анализирует данные, блокирует определенные действия и доступ к отдельным приложениям и устройствам, контролируя поведение пользователей на рабочем месте.

Dozor Endpoint Agent отслеживает печать на принтере, буфер обмена, съемные носители, мессенджеры (WhatsApp, Skype, Telegram, eXpress и др.), нажатие клавиш, а также активность пользователей и отдельных приложений на рабочей станции. Его можно настроить на работу в режиме активного противодействия, т. е. при необходимости в зависимости от контента запрещать копирование файлов, блокировать буфер обмена, отправку через браузеры — безусловно или до подтверждения пользователя. Кроме того, модуль может делать снимки рабочего стола пользователя по нажатию определенных клавиш, например Enter или Print Screen, или через определенные периоды времени. Также офицер безопасности может записать звук, который в данный момент поступает на микрофон рабочего компьютера сотрудника (возможность реализована для полнофункциональных агентов и доступна из раздела «Досье»).

Таблица 1. Сравнение возможностей Dozor Endpoint Agent

DOZOR ENDPOINT AGENT

SOLAR

Функция (канал перехвата)	Windows	GNU/Linux	macOS
Разрешение и блокировка подключения USB-устройств по заданным категориям и экземплярам	✔	✔	✔
Перехват сетевого трафика по протоколу HTTP(S), включая веб-почту и облачные хранилища	✔	✔	✔
Контроль почтовой переписки по протоколам SMTP, POP3, IMAP, в том числе с шифрованием SSL/TLS	✔	✔	✔
Контроль и блокировка печати	✔	✔	✔
Снятие снимков с экрана рабочей станции	✔	✔	✔
Перехват нажатия клавиш (кейлогер)	✔	✔	✔
Контроль передачи данных через буфер обмена (текст, изображение, файлы)	✔	✔	✔
Контроль копирования файлов на USB-устройства и сетевые диски	✔	✔	✔
Контроль рабочего времени пользователей: название сайтов и приложений, время работы с ними, аналитика по сотруднику и отделу	✔	✔	✔
Запись звука с микрофона рабочей станции	✔	✔	✔
Трансляция видео экрана рабочей станции	✔	✔	В разработке
Запись видео экрана рабочей станции	✔	В разработке	В разработке
Контроль подключения к Wi-Fi	✔	В разработке	В разработке
Контроль демонстрации экрана (ВКС и мессенджеры)	Яндекс.Телемост, TrueConf, МТС Линк (Webinar), SberJazz, Express	В разработке	В разработке
Перехват сообщений и файлов в мессенджерах	Telegram, WhatsApp Viber, Skype, Zoom, MS Teams	Telegram WhatsApp	Telegram WhatsApp Skype

С помощью Dozor Endpoint Agent можно контролировать содержимое внешних устройств (флеш-накопителей, карт памяти и внешних жестких дисков), подключенных через USB-порт к рабочим станциям сотрудников компании. Это позволяет своевременно выявлять нарушения, связанные с операциями, выполняемыми с данными, хранящимися на съемных носителях. Dozor Endpoint Agent также можно использовать для контроля работы пользователей на терминальных серверах.

Основные функции

Dozor Endpoint Agent контролирует следующие каналы передачи информации:

- Печать документов через локальный или сетевой принтер;

[1] Ведется работа по добавлению функций для паритета с агентами для Linux и Windows

- Копирование файлов на внешние устройства (в том числе по протоколу MTP);
- Передача файлов конкретными приложениями, в том числе iTunes, Dropbox и Яндекс.Диск, а также через браузеры;
- Запуск приложений;
- Передача данных по протоколу HTTPS;
- Передача сообщений, звонков и файлов через мессенджеры;
- Буфер обмена;
- Контроль подключения к Wi-Fi;
- Контроль демонстрации экрана;
- Подключенные внешние устройства.

Принцип работы

Установка и работа модуля Dozor Endpoint Agent происходят на уровне ядра операционной системы и незаметны для сотрудника. Это позволяет использовать Dozor Endpoint Agent для активного противодействия утечкам, в том числе с применением анализа содержимого, а также собирать трафик с протоколов, которые технически нельзя перехватить на шлюзе.

Для обеспечения высокого уровня ИБ рекомендуем установить Dozor Endpoint Agent на рабочие станции всех пользователей.

9.9. Dozor File Crawler

Модуль позволяет проводить инвентаризацию содержимого файловых хранилищ (общедоступных файловых обменников и локальных жестких дисков рабочих станций), выявляя нарушения правил хранения конфиденциальной информации.

Важным отличием Dozor File Crawler является использование принципа централизованной обработки. В отличие от discovery-решений, реализованных на клиентских агентах, Dozor File Crawler сразу аккумулирует результаты своей работы в одном месте и предоставляет пользователю целостную картину всех сегментов корпоративной сети.

Рисунок 65. Основные возможности Dozor File Crawler

Основные функции

- Контроль содержимого сетевых ресурсов и компьютеров пользователей.
- Выявление нарушений корпоративных политик хранения конфиденциальной информации.
- Поиск и классификация корпоративных данных с помощью автоматического сканирования общедоступных файловых ресурсов.
- Контроль распространения информации в рамках компании, между отделами и группами пользователей.
- Сканирование сети для построения дерева сети и обнаружения неавторизованных запущенных сервисов.

Этапы работы

1. Для выявления рисков хранения конфиденциальных данных Dozor File Crawler составляет наглядную карту сети и хранения информации в организации.
2. Карта отображает все доступные ресурсы (файловые хранилища, серверы приложений, сетевые устройства вывода, почтовые серверы, закрытые директории и рабочие станции сотрудников) и хранимые документы — как общедоступные, так и скрытые, и системные.
3. Гибкие средства планирования задач и расписания проверок Dozor File Crawler позволяют непрерывно контролировать безопасность компании в полностью автоматическом режиме.
4. При обнаружении конфиденциальных документов и нарушении политик безопасности это событие отображается в едином ситуационном центре — на «рабочем столе руководителя» офицера безопасности.
5. Все данные, события и инциденты безопасности привязываются к конкретному сотруднику и категориям защищаемой информации. В досье на сотрудника появляется копия документа и вся информация о нем: какие правила политики безопасности нарушены, кто владелец файла, где он размещен.

Таблица 2. Функциональные характеристики Dozor File Crawler

Параметр	Характеристики
Средняя скорость идентификации хостов сети	1 000 хостов/сек.
Средняя скорость анализа информации	188 КБ/сек, 37,54 файлов/сек
Веб-сервисы	IIS, Apache HTTP Server, NGINX
Анализ и контроль файловых серверов	Сервисы DFS, FTP, NFS, SMB EMC, NetApp, Microsoft Windows Server 2008-2016
СУБД	Microsoft SQL Server 2012-2017, Oracle SQL, PostgreSQL, MySQL, DB2, Informix, Interbase, Sybase, ЛИНТЕР
Анализ и контроль рабочих станций	Хранилища рабочих станций и ноутбуков на любой из ОС: Microsoft Windows, macOS, Linux
Виртуальные и терминальные сервисы	Citrix XenApp, Citrix XenDesktop, Microsoft Windows Terminal Server, VMware vSphere ESXi, X Window System и др.
Серверы приложений	GlassFish, JBoss, Tomcat, IBM Lotus Notes, WebSphere, WebLogic и др.
Почтовые серверы	Microsoft Exchange Server 2007-2016, IBM Lotus Notes, CommuniGate, UserGate, Zimbra, Kerio Connect и др.
Сетевое оборудование	Принтеры, МФУ, сканеры, модемы, роутеры

Контроль Cisco Webex Teams

С помощью возможностей Dozor File Crawler можно настроить систему так, что все сообщения и файлы, отправленные сотрудниками в личных или общих чатах Cisco Webex Teams, будут поступать в Solar Dozor и проходить проверку по условиям политики безопасности организации.

Можно получить историю сообщений, отправленных сотрудниками организации даже до того, как в ней был установлен Solar Dozor. При этом учитываются ограничения мессенджера: по умолчанию Cisco Webex хранит историю сообщений за 90 дней, но при наличии пакета Webex Control Hub сохраняется вся история с момента установки мессенджера. Соответственно, можно получить либо историю за конкретный период (максимум 90 дней), либо всю историю сообщений.

Особенности работы в территориально распределенном режиме

Для повышения удобства использования Dozor File Crawler в территориально распределенном режиме, можно разграничивать доступ офицеров безопасности к задачам сканирования и построенной карте сети в соответствии с доступными пользователю организационным единицами.

При создании каждая задача сканирования связывается с организационной единицей. Далее все настройки задачи выполняются с использованием ресурсов этой единицы – сканирующий хост выбирается из списка относящихся к организационной единице, элементы карты сети также доступны для выбора из относящихся только к этой единице.

9.10. MultiDozor

Модуль MultiDozor предназначен для организаций, имеющих сеть филиалов. Он объединяет разрозненные инсталляции Solar Dozor в цельную систему, что позволяет комплексно повысить безопасность организации.

Решаемые задачи:

- Получение в режиме реальном времени информации о внутренних процессах как по всей организации в целом, так и в отдельных филиалах;

- Мониторинг персон и групп пользователей как по всей организации в целом, так и в отдельных филиалах;
- Контроль деятельность сотрудников безопасности в сети филиалов;
- Проведение сквозных расследований на распределенном архиве по всей организации;
- Централизованное управление системой и распространение политики безопасности в филиалы.

Принцип работы

Переход в территориально распределенный режим осуществляется через единый веб-интерфейс Solar Dozor. MultiDozor обеспечивает связь инсталляций Solar Dozor в филиалах с одинаковым набором модулей. Это необходимо для получения полного среза данных о процессах в организации и, при необходимости, подключения к расследованию инцидента специалистов из разных филиалов сети. При этом, локальную инсталляцию Solar Dozor с установленным модулем MultiDozor по-прежнему можно использовать для решения задач конкретного филиала.

9.11. MultiConnector

Интеграционный модуль — это отдельный сервис Solar Dozor, который включает в себя несколько "коннекторов", каждый для интеграции с определенным классом систем (SIEM, SOAR, XDR, IRP). Каждый коннектор содержит набор HTTP/HTTPS API, обеспечивающий необходимую функциональность и сценарии. На текущий момент реализовано 2 коннектора:

Коннектор №1 — для удаленного управления политиками безопасности Solar Dozor - с помощью создания, редактирования, удаления списков слов, а также применения обновленной политики фильтрации, просмотра состояния лицензии и сервиса интеграции.
Коннектор №2 — для удаленного изменения атрибутов событий и инцидентов безопасности (уровень критичности, статус, состояние); разблокировка и отправка заблокированных писем; передача крупных атрибутов событий и инцидентов (все адреса получателей, все тело сообщения со всеми срабатываниями и т. п.).

Для удобства создания удаленных запросов к Solar Dozor реализован графический справочный интерфейс. В нем приведены описания, параметры и возвращаемые значения API.

10. Системные требования

Минимальная установка

Для минимальной установки достаточно одного узла со следующей конфигурацией:

- Количество ядер — 8;
- Тактовая частота — от 2,2 ГГц;
- Объем оперативной памяти — от 32ГБ;
- Объем жесткого диска — от 600 ГБ.

В дополнение к указанному размеру системы хранения рекомендуется использовать дисковые полки или СХД для хранения баз данных и долговременного файлового хранилища.

Требования к инфраструктуре

Для поддержания нормальной работоспособности Solar Dozor, инфраструктура корпоративной сети должна соответствовать следующим требованиям:

- Наличие DNS-сервера и сервера точного времени;
- Сеть должна пропускать трафик между компонентами Solar Dozor в соответствии с матрицей доступа;
- Пропускная способность сетевых интерфейсов серверов системы не менее 100 Мбит/с.

Необходимое ПО для установки

Для установки Solar Dozor необходимо наличие следующего ПО:

- ОС:
  - CentOS 7.9;
  - Red Hat Enterprise Linux (RHEL) 7.9;
  - RED OS 7.3;
  - ОС Astra Linux 1.7 Special Edition ("Смоленск");
  - ОС Astra Linux 1.7 Special Edition ("Воронеж").
- ОС Astra Linux 1.7 Common Edition ("Орел");
- СУБД на выбор: PostgreSQL 11, 12; Oracle Database Enterprise Edition 11, 12, 19; Jatoba;
- SSH-клиент;
- Дистрибутив Solar Dozor;
- Лицензия на Solar Dozor.

Требования к конфигурации контролируемых рабочих станций

Для установки и эффективной работы Dozor Endpoint Agent рекомендуется следующая конфигурация рабочей станции:

- Количество ядер — от 2;
- Оперативная память — 2 ГБ (Windows, Linux), 4 ГБ (macOS);
- Запоминающее устройство — 50 ГБ (Microsoft Windows, Linux, macOS);

- ОС:

Характеристика	Рекомендуемое значение		
	EAW	EAL	EAM
Версии ОС (с установленными критичными обновлениями, рекомендованными вендором ОС)	• Windows 7 SP1 32/64 bit • Windows 8.1 32/64 bit • Windows 10 32/64 bit • Windows 11 32/64 bit • Windows Server 2008 R2 64 bit • Windows Server 2012 R2 32/64 bit • Windows Server 2016 • Windows Server 2019 • Windows Server 2022	• AlterOS 7.5; • Astra Linux Special Edition 1.6, уровень защищенности «Смоленск»; • Astra Linux Special Edition 1.7.4, уровень защищенности «Воронеж»/«Орёл»/«Смоленск»; • Astra Linux Common Edition 2.12, уровень защищенности «Орёл»; • CentOS Linux 7 Desktop; • CentOS Stream 8; • Debian 11 Desktop; • Ubuntu 20.04 LTS Desktop; • Альт 8.1/8.3 СП Рабочая Станция; • Альт 8.4 СП Рабочая станция (релиз 9); • Альт 8 СП с установленными СЗИ Secret Net LSP и Kaspersky Endpoint Security • Альт Рабочая станция 9.1/9.2; • Альт Рабочая станция 10.1; • РЕД ОС 7.3.x «Муром».	• macOS версий 11.x (Big Sur) • macOS версий 12.x (Monterey) • macOS версий 13.x (Ventura)

Интеграция с другими продуктами

Solar Dozor поддерживает интеграцию со следующими видами систем:

- Security Information and Event Management (SIEM);
- Secure Web Gateway (SWG);
- Next Generation Firewall (NGFW)
- Business Intelligence (BI);
- Mobile Device Management (MDM);
- System and Network Management;
- IRP (Incident Response Platform), SOAR (Security Orchestration, Automation and Response);
- XDR (Extended Detection and Response).

11. Solar webProxy

Solar Dozor может тесно взаимодействовать с другой разработкой компании «Солар» — Solar webProxy.

11.1. Назначение

Solar webProxy — шлюз веб-безопасности (Secure Web Gateway, SWG) для контроля доступа сотрудников и приложений к веб-ресурсам, защиты от веб-угроз, таких как запрещенные, зараженные или фишинговые сайты, а также блокирования утечек конфиденциальной информации через веб-канал.

Для защиты организации в Solar webProxy применяются следующие механизмы:

- **Аутентификация и авторизация** — для контроля доступа сотрудников и приложений к конкретным веб-ресурсам;
- **Расшифровка HTTPS-трафика** — для проверки зашифрованного трафика и его передачи другим средствам защиты по протоколу ICAP;
- **Категоризатор веб-ресурсов** – для управления доступом к конкретным категориям веб-ресурсов (интернет-магазины, порносайты, образовательные ресурсы и т. д.);
- **Потоковый антивирус Dr. Web** — для защиты от вредоносного ПО и веб-фишинга;
- **Блокировщик рекламы** — для защиты от вредоносных скриптов в рекламных баннерах и программ для сбора данных сотрудников (кук);
- **Реверс-прокси** — для контроля доступа удаленных сотрудников к Outlook Web Access и другим корпоративным веб-ресурсам;
- **Досье на персону** — для применения персонализированных политик безопасности и индивидуального контроля трафика;
- **Контентный анализ** — для предотвращения утечек конфиденциальной информации.

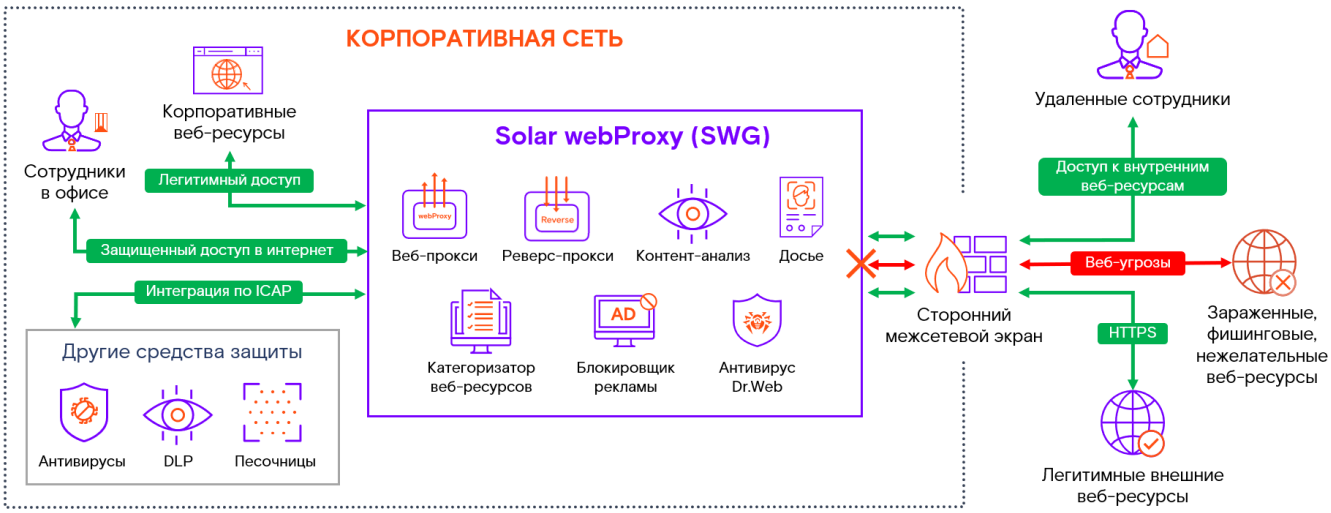


Рисунок 66. Solar webProxy в сетевой инфраструктуре

Отличительные особенности Solar webProxy — высокая производительность и отказоустойчивость, встроенные настраиваемые отчеты с возможностью детализации до

«сырых» данных, досье на сотрудника, удобный веб-интерфейс, а также тесная интеграция с DLP-системой Solar Dozor для предотвращения утечек конфиденциальной информации в автоматическом режиме.

Помимо основной функции — обеспечения веб-безопасности — Solar webProxy позволяет снизить потребление интернет-трафика, одновременно увеличив скорость доступа к веб-ресурсам. Это достигается за счет возможностей кэширования часто запрашиваемых страниц, блокирования развлекательных ресурсов, навязчивой рекламы, а также лимитирования трафика для пользователей.

Solar webProxy внесен в Единый реестр отечественного ПО (№ 7765), и успешно заменяет лидирующие зарубежные SWG, такие как McAfee SWG, Symantec ProxySG, Forcepoint SWG, в крупнейших российских корпорациях.

11.2. Области применения

Solar webProxy может:

- Отслеживать использование веб-ресурсов пользователями и приложениями;
- Разграничивать доступ сотрудников и приложений к внешним веб-ресурсам;
- Контролировать доступ удаленных сотрудников к внутренним ресурсам организации;
- Предотвращать утечки конфиденциальной информации;
- Контролировать скачиваемые и отправляемые в интернет данные;
- Контролировать доступ сотрудников к конкретным веб-сайтам или категориям веб-ресурсов;
- Ограничивать объем веб-трафика для снижения нагрузки на канал связи;
- Поддерживать высокую скорость и надежный доступ к веб-ресурсам;
- Блокировать вредоносное ПО и доступ к зараженным ресурсам;
- Блокировать рекламные баннеры;
- Регулярно формировать статистические отчеты о работе сотрудников компании в интернете;
- Выполнять требования и рекомендации регуляторов в части ограничения доступа к веб-ресурсам.

11.3. Принцип работы

Solar webProxy устанавливает «в разрыв» трафика» и контролирует все данные, передаваемые между сотрудниками и интернет-ресурсами.

1. При обращении к ресурсу (внутреннему или внешнему) приложение проходит аутентификацию в Solar webProxy. Возможна настройка доступа без запроса аутентификации для отдельных ресурсов и приложений.
2. Solar webProxy в соответствии с настройками отправляет данные на проверку во встроенный антивирусный модуль и/или стороннюю систему по протоколу ICAP. При положительном ответе от принимающей системы соединение прерывается, а пользователь получает заранее настроенную страницу с указанием причины блокировки.
3. Solar webProxy применяет соответствующую политику безопасности исходя из полученных на этапе аутентификации данных о пользователе, сервере назначения, а также технических параметров запроса.

4. Если передача данных разрешена по политике, запрос от приложения передается на сервер назначения.

5. Полученный ответ от сервера назначения также проверяется антивирусным модулем, а затем — на соответствие настроенной политике безопасности. При положительном результате передается приложению — источнику запроса.

6. Если запрос или ответ не соответствуют политике безопасности, то вместо них пользователь получает подготовленную страницу с описанием запрета, а приложению отказывается в доступе. При обнаружении нарушения происходит уведомление офицера безопасности.

Рисунок 67. Принцип работы Solar webProxy

12. О группе компаний «Солар»

Группа компаний «Солар» — ведущий поставщик решений кибербезопасности в России, архитектор комплексной кибербезопасности. Ключевые направления деятельности — аутсорсинг ИБ, разработка собственных продуктов, обучение ИБ-специалистов, аналитика и исследование киберинцидентов.

С 2015 года предоставляет ИБ-решения организациям от малого бизнеса до крупнейших предприятий ключевых отраслей. Под защитой «Солара» – более 850 крупнейших компаний России. Продукты и сервисы «Солара» объединены в домены экспертизы: Безопасная разработка программного обеспечения, Управление доступом, Защита корпоративных данных, Детектирование угроз и хакерских атак. Домены экспертизы закрывают все потребности заказчиков и включают собственные разработки, решения партнеров, услуги по созданию стратегии и архитектуры ИБ, консалтинг, обучение персонала.

Компания предлагает сервисы первого и крупнейшего в России коммерческого SOC — Solar JSOC, экосистему управляемых сервисов ИБ — Solar MSS. Линейка собственных продуктов включает DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, межсетевой экран нового поколения Solar NGFW, IdM-систему Solar inRights, PAM-систему Solar SafeInspect, анализатор кода Solar appScreener и другие.

ГК «Солар» развивает платформу для практической отработки навыков защиты от киберугроз «Солар Кибермир». Работа центра исследования киберугроз Solar 4RAYS нацелена на изучение тактик киберпреступников. Полученные аналитические данные обогащают разработки Центра технологий кибербезопасности.

Группа компаний «Солар» инвестирует в развитие отрасли кибербезопасности и помогает решать проблему кадрового дефицита. Совместно с Минцифры реализует всероссийскую программу кибергигиены, направленную на повышение цифровой грамотности населения.

Штат компании — более 1 800 специалистов. Подразделения «Солара» расположены в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Ростове-на-Дону, Томске, Хабаровске и Ижевске. Технологии компании и наличие распределенных по всей стране центров компетенций позволяют ей работать в режиме 24/7.

13. Контактная информация

Телефоны:

+7 (499) 755-07-70 — продажи и общие вопросы

+7 (499) 755-02-20 — техническая поддержка

E-mail:

solar@rt-solar.ru — продажи и вопросы по сервису

support@rt-solar.ru — техническая поддержка

Адреса:

- Москва, Никитский пер., 7, стр. 1
- Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд
- Нижний Новгород, Казанское шоссе, 25, корпус 2
- Самара, Молодогвардейская ул., 204
- Ростов-на-Дону, Доломановский пер., 70Д
- Хабаровск, ул. Серышева, 56