Ростелеком
Солар

Программный комплекс «Solar Dozor»

Версия 7.3

Описание обновлений

МОСКВА, 2020

Содержание

1. Общие сведения о продукте

1.1. Назначение продукта

Программный комплекс (ПК) «Solar Dozor» (далее – Solar Dozor) – это система контроля корпоративных коммуникаций класса Data Leak Prevention (DLP), с помощью которой можно выявлять и блокировать несанкционированную передачу данных с компьютеров, а также определять признаки корпоративного мошенничества.

1.2. Краткое описание возможностей

К основным возможностям Solar Dozor относятся:

- контроль каналов утечки данных и использования сетевых ресурсов;
- отслеживание и ограничение движения потоков информации;
- сбор, анализ и хранение сообщений о фактах передачи информации (при этом обеспечивается анализ содержимого сообщений и документов; выявление документов определённой структуры и содержания; сравнение текстовых, графических и табличных документов с заранее заданными эталонными документами; распознавание в текстах сообщений определенных последовательностей – ИНН, номеров паспортов и т. д.);
- мониторинг и контроль сетевых коммуникаций персон (сотрудников, адресов);
- мониторинг и контроль местонахождения электронных материалов, содержащих конфиденциальную информацию;
- поддержка процессов работы офицеров службы безопасности (создание и настройка правил передачи и хранения информации; мониторинг событий и инцидентов; отслеживание действий персон; назначение сотрудников, ответственных за разбор инцидентов; получение статистических отчетов);
- поддержка проведения расследований инцидентов ИБ, КБ и ЭБ (поиск данных, выявление рабочих и личных контактов сотрудников; автоматический анализ сетевой активности каждого сотрудника);
- мониторинг и анализ особенностей поведения персон и ресурсов на основе данных об их информационных коммуникациях.

1.3. Версия продукта

В релизе поставляется Solar Dozor версии 7.3.

2. Описание релиза

2.1. Что нового в релизе

В Табл. 1 приведен обзор новых возможностей, реализованных в Solar Dozor версии 7.3.

Табл. 1. Краткий обзор новых возможностей

№	Новый функционал	Краткое описание	Полное описание
1	**Инструмент «Графический шаблон»**: возможность распознавания и перехвата изображений, содержащих критичные данные	В Solar Dozor 7.3 появился новый инструмент политики, позволяющий решить проблему контроля передачи критичных данных в графических форматах. С помощью этого инструмента система достаточно точно распознает в изображениях: • данные паспорта РФ; • печати организаций (круглую и треугольную); • данные лицевой и обратной сторон платежной карты. Офицер безопасности может легко задать правила, по которым сообщения с подобными данными будут перехватываться системой автоматически	Раздел 2.1.1
2	**Модуль анализа поведения Dozor UBA**: 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 UBA появилась возможность *на ранних стадиях* выявлять сотрудников, которые явно думают об увольнении. Также в версии 7.3 добавлены типы аномалий поведения, которые позволяют отслеживать в коммуникациях персон появление нового неизвестного контакта и нового информационного объекта	Раздел 2.1.2
3	**Контроль каналов передачи данных:** Telegram, Яндекс.Диск и Google Drive в списке контролируемых каналов	Расширен список контролируемых каналов передачи данных – теперь можно контролировать переписку в мессенджере Telegram и обмен файлами с помощью desktop-приложений сервисов Яндекс.Диск и Google Drive	Раздел 2.1.3
4	**Политика: фильтрация данных с учетом транслитерации и опечаток**	Добавлены механизмы, которые позволяют распознавать в сообщениях и именах файлов текст, написанный транслитом и/или с опечатками, и преобразовывать его к обычному/правильному виду. Таким образом, теперь можно контролировать передачу текста, который намеренно или случайно был искажен с помощью транслита или опечаток	Раздел 2.1.4
5	**Быстрый поиск: новый фильтр результатов поиска**	В версии 7.3 полностью переработан фильтр результатов быстрого поиска. Теперь он открывается в отдельном окне, где скомпонованы критерии фильтрации, которые офицер безопасности может задать для конкретной поисковой выборки. Такая реализация также обеспечила возможность добавления новых критериев – теперь фильтровать результаты поиска можно по пометкам, установленным на сообщения, а также по данным справочника приложений. С новым фильтром можно быстро находить нужные данные в уже сформированной поисковой выборке.	Раздел 2.1.5

2.1.1. Графический шаблон: решение проблемы передачи критичных данных в графических форматах

В Solar Dozor 7.3 появился новый инструмент политики **Графический шаблон**, позволяющий решить проблему контроля передачи критичных данных в графических форматах.

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

- 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). Скорость работы технологии практически не зависит от размера изображения.
Объекты распознаются с учетом различных деформаций (растяжения, поворота, наложения на другие объекты), а также при полном отсутствии текстовой составляющей.

Графический шаблон представляет собой заданную офицером безопасности комбинацию объектов (Рис. 1).

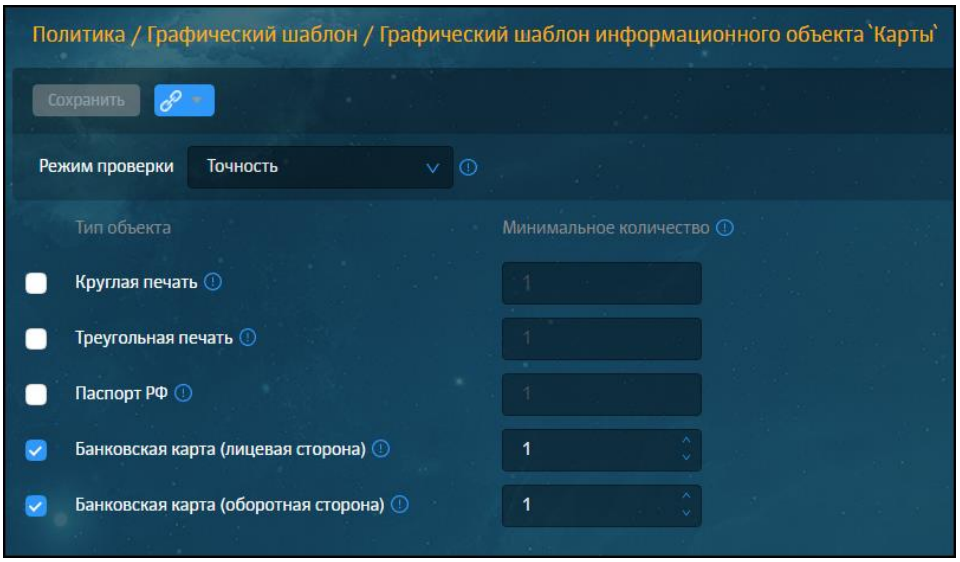


Рис. 1. Графический шаблон – комбинация графических объектов

Также можно задать:

- 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.

Можно сформировать графический шаблон для конкретного информационного объекта (Рис. 2).

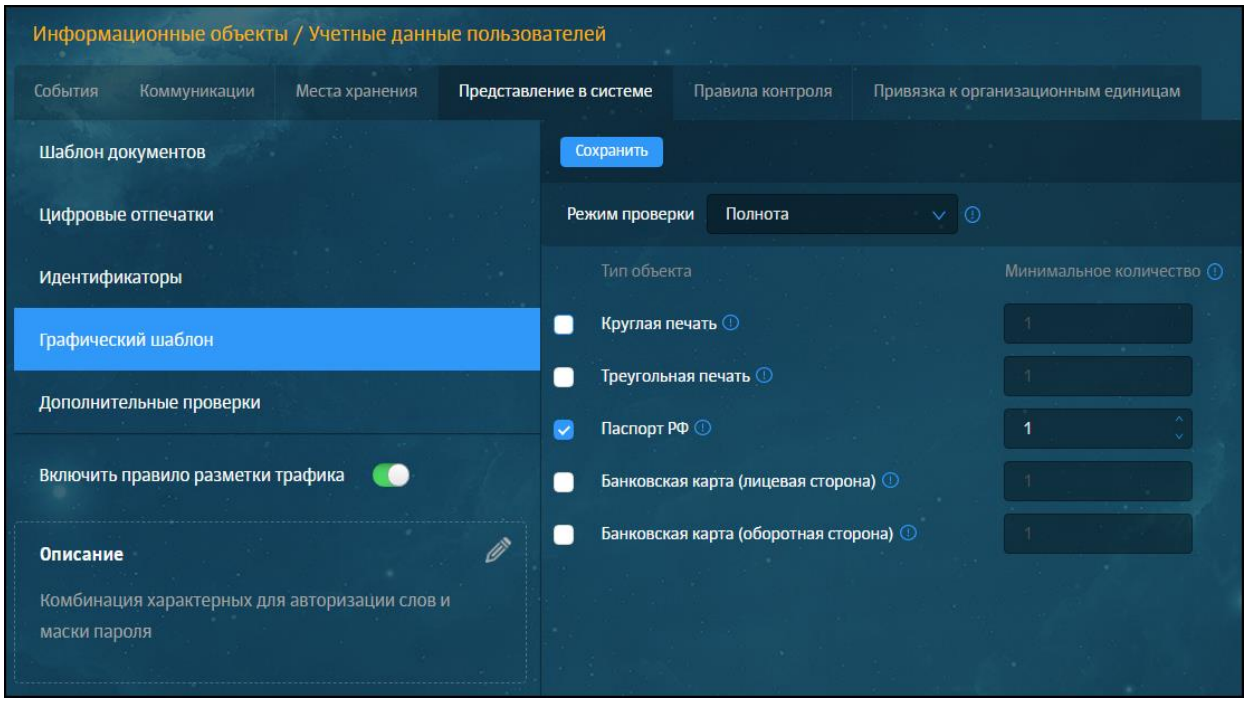


Рис. 2. Графический шаблон для информационного объекта

После формирования графического шаблона офицер безопасности может легко задать правила, по которым сообщения, содержащие заданные в шаблоне объекты, например, изображения банковской карты, будут перехватываться системой автоматически (Рис. 3). 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 (Рис. 4).

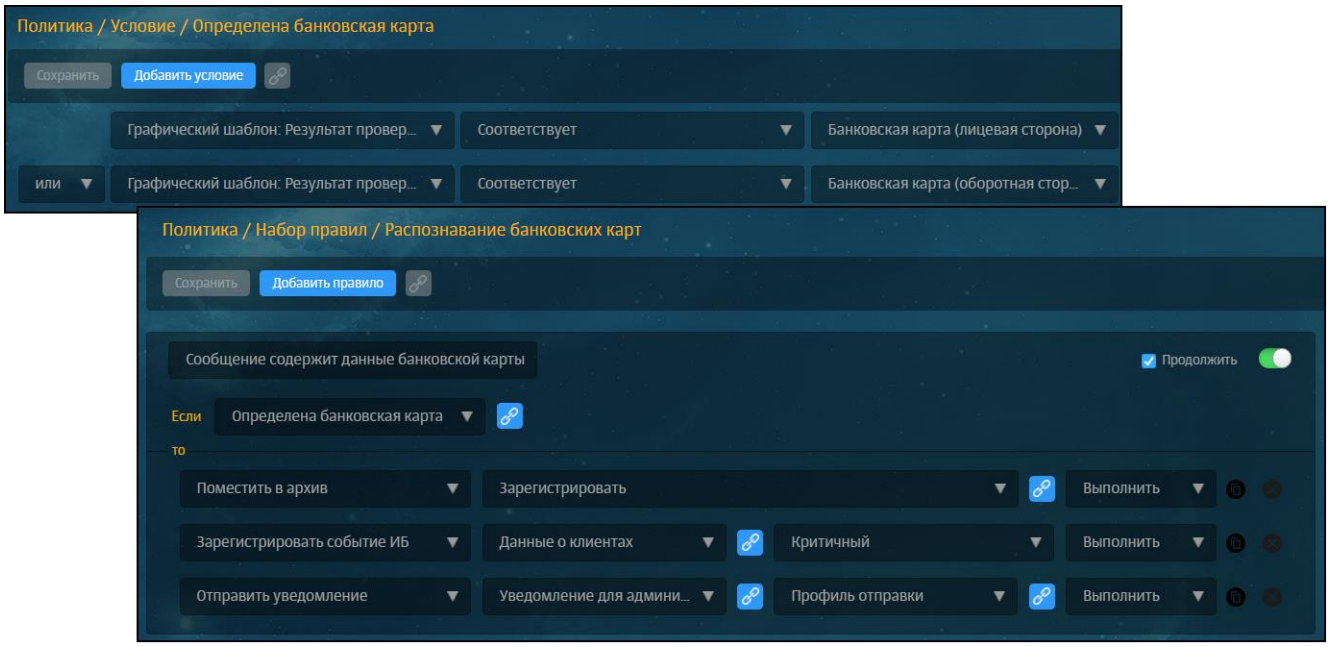


Рис. 3. Политика: пример правила, по которому перехватываются сообщения, содержащие изображение банковской карты

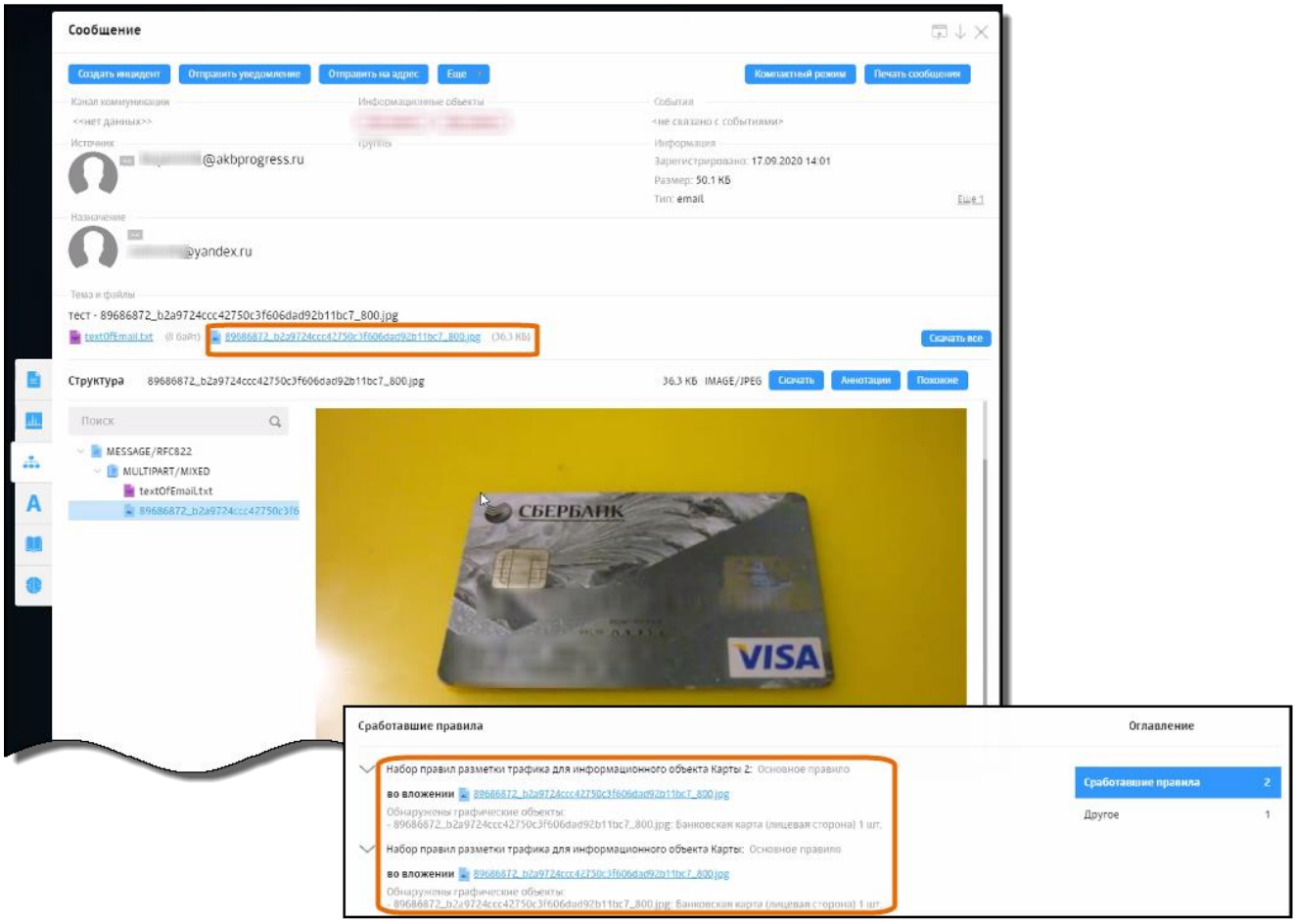


Рис. 4. Перехваченное сообщение: в сообщении содержится изображение банковской карты

2.1.2. Модуль анализа поведения Dozor UBA: минимизация риска утечки данных при увольнении сотрудников

Модуль анализа поведения **Dozor UBA** в версии 7.3 содержит изменения, призванные минимизировать риск 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** (Рис. 5).

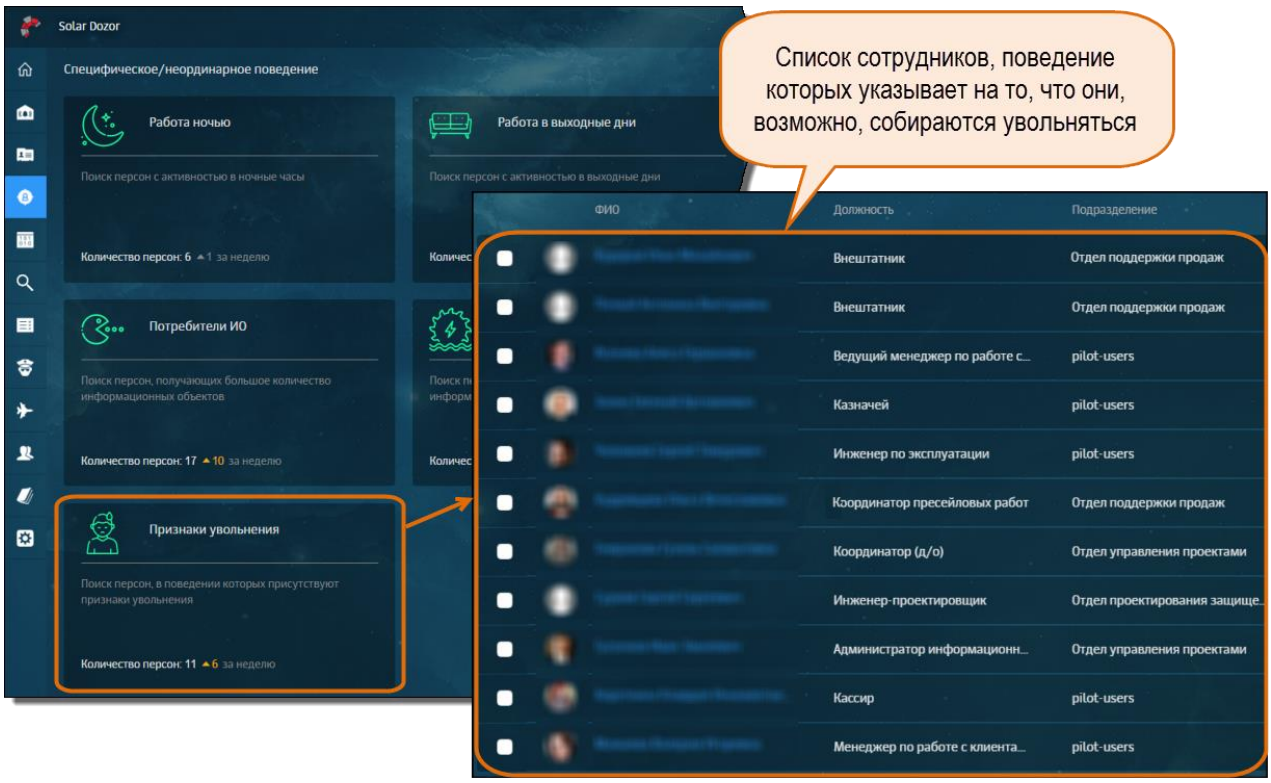


Рис. 5. Получение списка сотрудников, в поведении которых присутствуют признаки, характерные для персон, собирающихся увольняться

Критерии, по которым система выявляет тех, кто собирается уволиться, 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 в версии 7.3 добавлены использующиеся в том числе и при выявлении увольняющихся персон аномалии поведения **Новый неизвестный контакт** и **Новый информационный объект** (Рис. 6). Они позволяют отслеживать в электронных коммуникациях сотрудников 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.

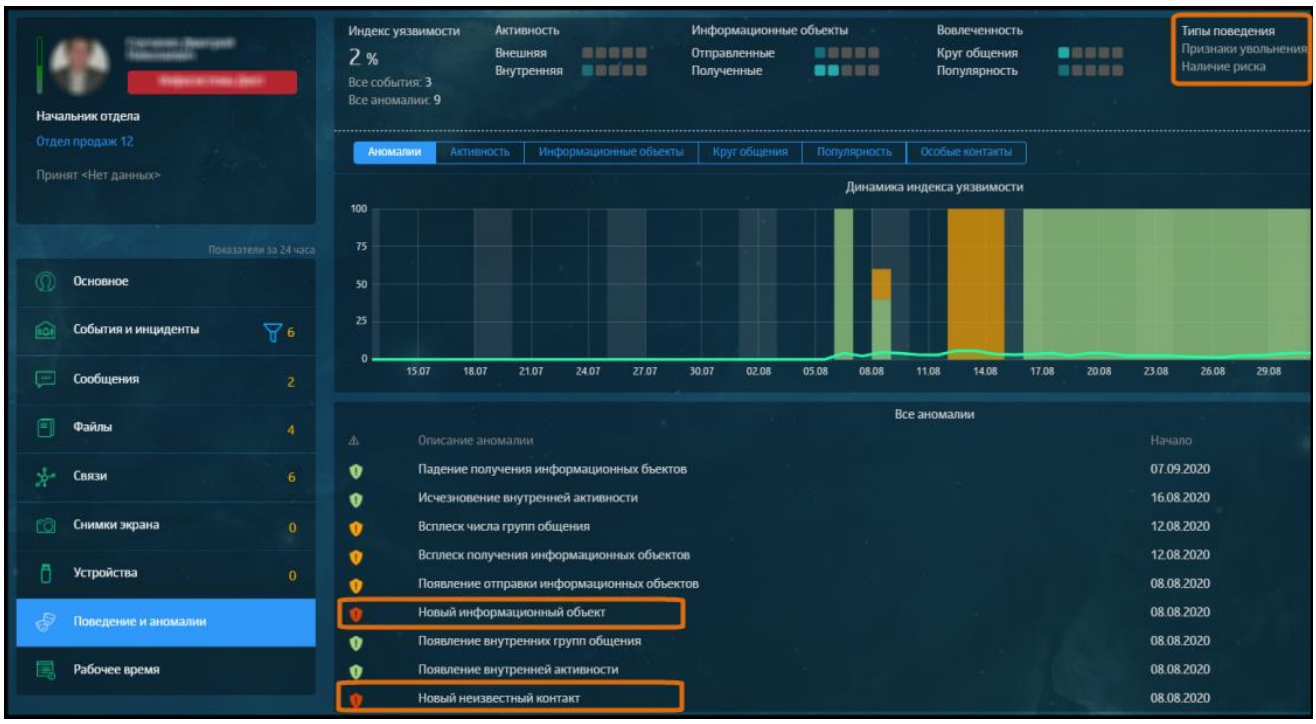


Рис. 6. Карточка сотрудника, вкладка «Поведение и аномалии»: в поведении сотрудника система обнаружила признаки увольнения – в их числе наличие аномалий «Новый информационный объект» и «Новый неизвестный контакт»

2.1.3. Расширение списка контролируемых каналов передачи данных – Telegram, Яндекс.Диск и Google Drive

В Solar Dozor 7.3 расширен список контролируемых каналов передачи данных – теперь с помощью модуля **Dozor Endpoint Agent** (Агент) версии 3.7 и выше, установленного на рабочих станциях корпоративной сети, можно контролировать переписку в мессенджере Telegram и обмен файлами с использованием desktop-приложений сервисов Яндекс.Диск и Google Drive (наряду с их веб-версией).

Агент перехватывает и передает Solar Dozor как сообщения, которыми обмениваются сотрудники в Telegram, так и файлы, отправленные в облачные хранилища Яндекс.Диск и Google Drive. Офицер безопасности может просматривать переданные Агентом данные в интерфейсе Solar Dozor и формировать политику фильтрации сообщений с учетом новых возможностей перехвата.

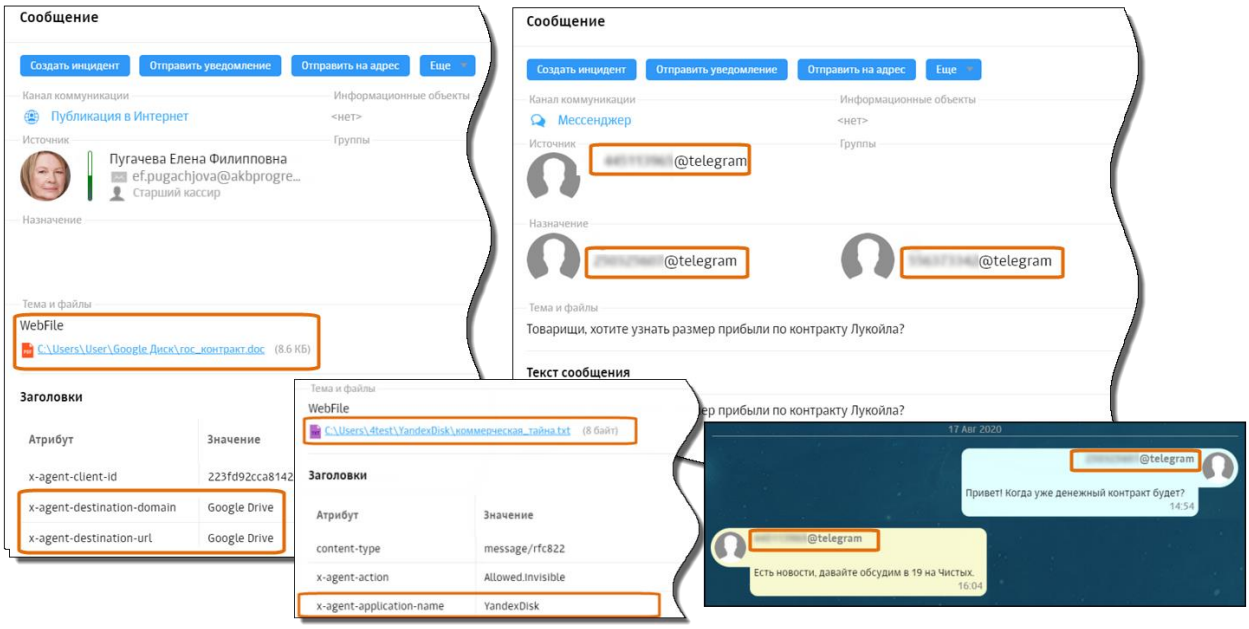


Рис. 7. Интерфейс Solar Dozor, карточки сообщений и беседы: перехваченные Агентом данные

2.1.4. Контроль передачи текста с учетом транслитерации и опечаток

В Solar Dozor 7.3 добавлены механизмы, которые позволяют распознавать в сообщениях и именах файлов текст, написанный транслитом и/или с опечатками, и преобразовывать его к обычному/правильному виду.

Теперь офицер безопасности может формировать политику фильтрации сообщений с учетом новых возможностей – в условиях политики доступны соответствующие операции сравнения (Рис. 8).

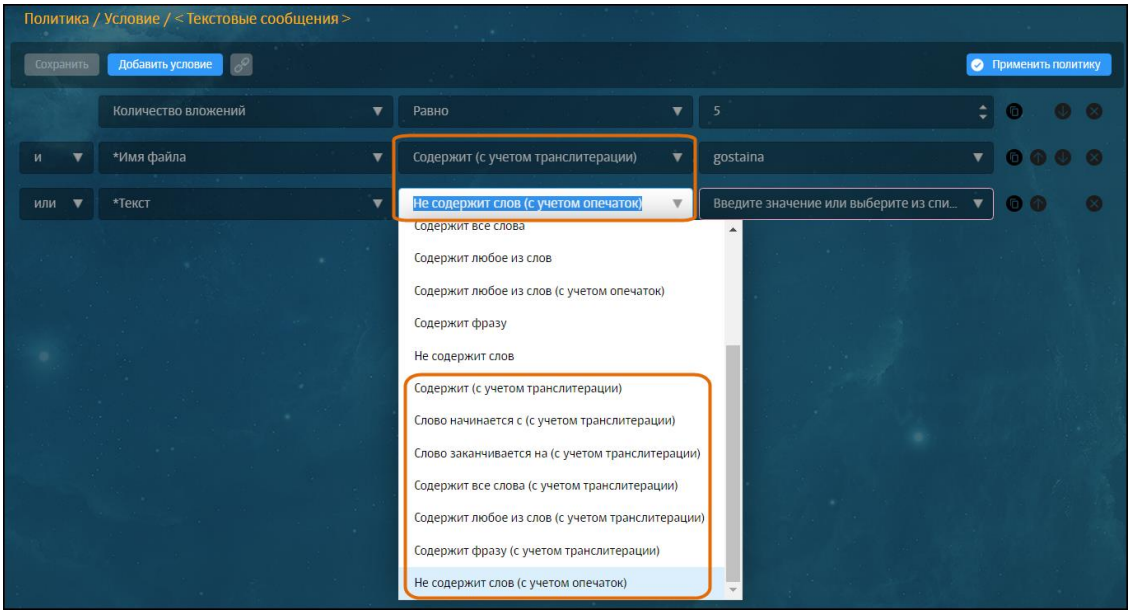


Рис. 8. Политика: задание условий для фильтрации текста с учетом транслитерации и опечаток

Таким образом, теперь можно контролировать передачу текста, который намеренно или случайно был искажен с помощью транслита и/или опечаток.

2.1.5. Быстрый поиск: новый фильтр результатов поиска

В Solar Dozor 7.3 полностью переработан фильтр результатов быстрого поиска. Теперь он доступен по нажатию кнопки в отдельном окне, где скомпонованы критерии фильтрации, которые офицер безопасности может задать для конкретной поисковой выборки (Рис. 9).

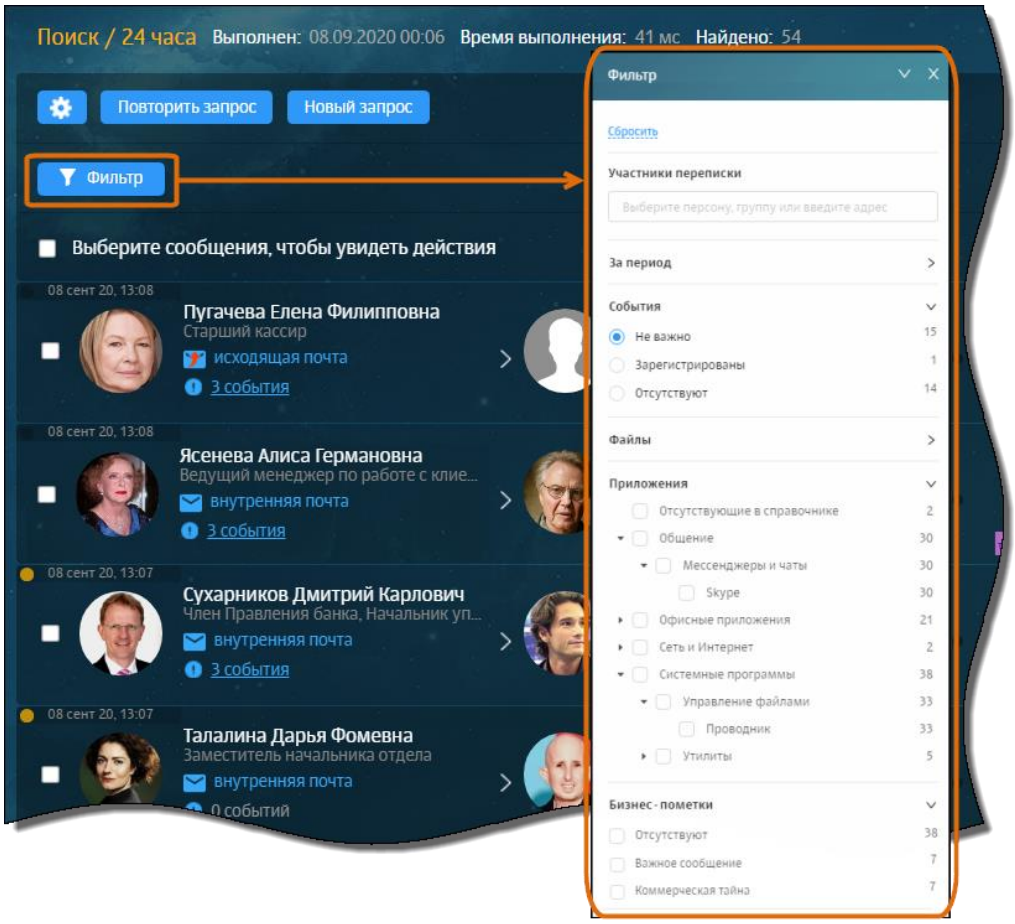


Рис. 9. Быстрый поиск: фильтр результатов поиска

Такая реализация также обеспечила возможность добавления новых критериев – теперь фильтровать результаты поиска можно по пометкам, установленным на сообщения, а также по данным справочника приложений (если в поисковой выборке есть соответствующие сообщения и данные).

С новым фильтром можно быстро находить нужные данные в уже сформированной поисковой выборке (Рис. 10). Это сэкономит время на поиск утечек и расследование инцидентов.

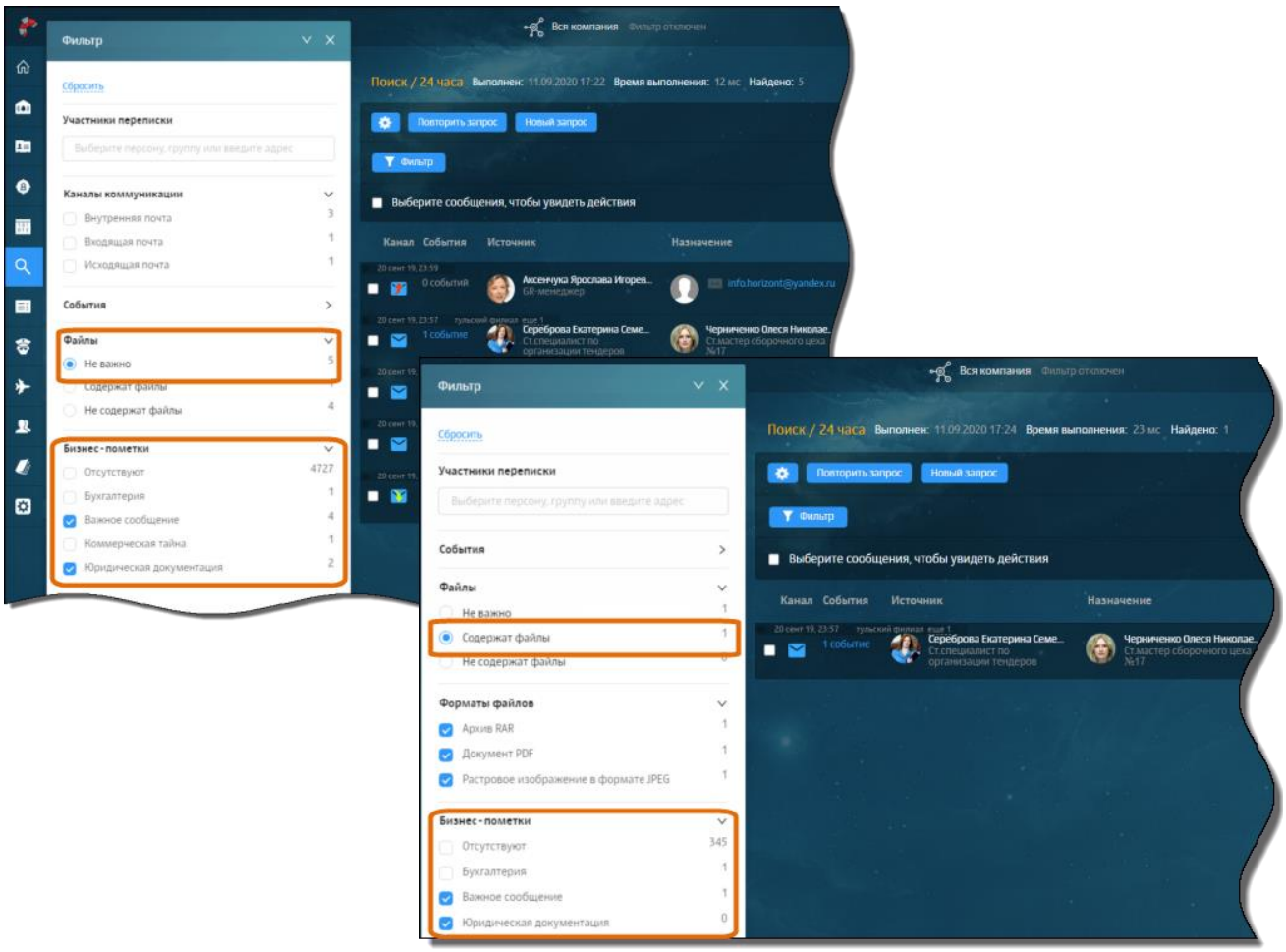
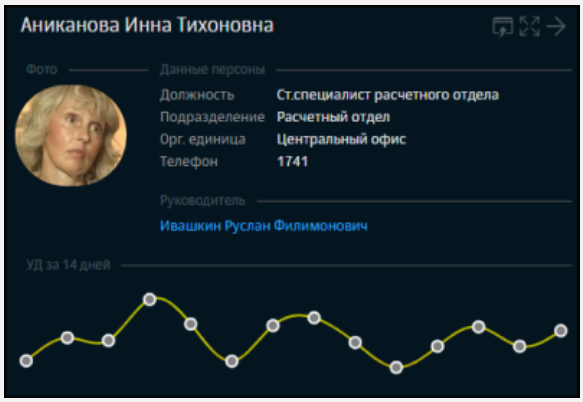


Рис. 10. Быстрый поиск: демонстрация работы фильтра

2.2. Улучшение функционала

В Табл. 2 приведен обзор доработок системы, реализованных в Solar Dozor версии 7.3.

Табл. 2. Обзор доработок системы

№	Доработка	Краткое описание
1	Возможность создания новой папки для хранения поисковых запросов и отчетов сразу в процессе их добавления	В предыдущих версиях системы ее новому пользователю для сохранения первого поискового запроса или отчета необходимо было сначала добавить папку для запросов/отчетов в специальном месте интерфейса и только потом приступать к формированию запроса/отчета. Теперь создать папку для хранения поисковых запросов или отчетов можно прямо из окна добавления запроса/отчета
2	Источники данных Досье: возможность запуска синхронизации данных с AD из интерфейса	В предыдущих версиях системы запустить синхронизацию с AD вручную можно было только с помощью утилиты командной строки. Это затрудняло и замедляло развертывание и эксплуатацию системы. Теперь синхронизировать Досье со всеми AD-источниками данных можно одним нажатием кнопки в интерфейсе Solar Dozor
3	Endpoint Agent: сбор и получение диагностической информации с рабочих станций	Теперь можно легко получить диагностическую информацию, касающуюся рабочих станций корпоративной сети, включая: • список программ, установленных на рабочей станции; • список запущенных на момент сбора информации процессов; • данные системных журналов; • настройки конфигурации и политики Агента. Для этого достаточно в интерфейсе системы выбрать нужные рабочие станции и нажать соответствующую кнопку (**Собрать диагностику**). Эта кнопка также доступна в карточке агента
4	Масштабирование интерфейса системы для больших экранов	Информация на рабочих столах пользователей и отчеты о работе системы (раздел **Система – Мониторинг**) теперь одинаково отображаются на всех экранах, в том числе на экранах с разрешением FullHD. Также можно разместить дополнительные виджеты. При расположении всех необходимых элементов на одном экране пользователь может одновременно получать больше информации и, соответственно, оперативнее реагировать на нарушения, оценивать текущее состояние системы и т.п.
5	Интерфейс, скин Dark: изменение дизайна кратких карточек событий/инцидентов и персон	Дизайн кратких карточек событий/инцидентов и персон изменен со светлых тонов на темные:  В итоге интерфейс выглядит более целостным и гармоничным, а из-за снижения контрастности информация воспринимается легче

№	Доработка	Краткое описание
6	Изменение формата названий экспортируемых из системы файлов, включая отчеты	Разработана единая система наименования для всех файлов, экспортируемых из системы – теперь генерируются читаемые названия с указанием даты/времени отправки запроса на формирование файла. Например, *PersonSummaryReport_2019-09-20_00-27.pdf*