Ростелеком
Солар

Программный комплекс «Solar Dozor»

Версия 7.4

Описание обновлений

МОСКВА, 2021

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 7.4.

2. Описание релиза

2.1. Что нового в релизе

В Табл. 1 приведен обзор новых возможностей, реализованных в Solar Dozor версии 7.4.

Табл. 1. Краткий обзор новых возможностей

№	Новый функционал	Краткое описание	Полное описание
1	**Модуль анализа поведения Dozor UBA**: поддержка работы в территориально-распределенных организациях (**Multi UBA**)	Функциональные возможности модуля Dozor UBA, задействованные в Solar Dozor 7.4, позволяют полноценно использовать его в территориально-распределенных организациях. При этом учитываются особенности работы каждой структурной единицы (филиала, дочернего предприятия, департамента и т.п.). Теперь все доступные сведения о поведении сотрудников можно получить именно в разрезе отдельной организационной единицы (ОЕ). Для этого офицеру безопасности достаточно в соответствующем разделе интерфейса выбрать ОЕ из списка доступных. Также можно получить сводную статистику по всем доступным ОЕ, где отражены наиболее значимые с точки зрения безопасности показатели. Кроме того, теперь в расчетах, на основе которых строятся UBA-профили сотрудников, учитывается часовой пояс региона, где работает конкретный сотрудник	Раздел 2.1.1
2	**Модуль File Crawler:** поддержка работы в территориально-распределенных организациях (**Multi Crawler**)	Реализована поддержка работы Краулера в территориально-распределенных организациях. Теперь можно: • сканировать файловые/облачные хранилища, локальную сеть и почтовые серверы ресурсами определенных структурно-организационных единиц (филиалов, дочерних организаций и т.п.); • разграничивать доступ к задачам сканирования и отображаемым на карте сети ресурсам – в соответствии с разрешенными для офицера безопасности ОЕ	Раздел 2.1.2
3	**Трансляция экрана компьютеров/ноутбуков сотрудников**: просмотр видео с экранов в режиме реального времени	В версии 7.4 офицер безопасности может просмотреть видеотрансляцию того, что прямо сейчас происходит на рабочем компьютере/ноутбуке интересующего сотрудника. Функционал доступен из краткой и полной карточек персоны (сотрудника). По умолчанию видео открывается в окне-миниатюре, при этом интерфейс Solar Dozor остается доступным для работы. При необходимости видео можно раскрыть на весь экран. Таким образом офицер безопасности может ***в режиме реального времени*** прицельно контролировать действия сотрудников, а значит, оперативно предотвращать возможные нарушения	Раздел 2.1.3
4	**Модуль Endpoint Agent**: контроль целостности	В Solar Dozor 7.4 офицер безопасности может легко настроить политику таким образом, чтобы при обнаружении нарушения целостности агента система создавала событие с высоким уровнем критичности. При этом в интерфейсе в разделе **Перехватчики** такой агент будет отображаться со статусом "Поврежден". Также можно настроить запись сообщения о нарушении	Раздел 2.1.4

№	Новый функционал	Краткое описание	Полное описание
		целостности агента в журнал syslog. Кроме того, в разделе **Система > Мониторинг** можно посмотреть сведения о количестве агентов (в графическом виде), сгруппированных по статусам, подстатусам и версиям агентов. Все это позволяет своевременно узнать о нарушении и принять соответствующие меры.	
5	**Модуль Endpoint Agent**: получение сведений о структуре внешнего носителя	Реализован механизм считывания структуры каталогов съемных носителей информации (флеш-накопителей, карт памяти и внешних жестких дисков), подключаемых через USB-порт к рабочим станциям сотрудников компании. Теперь можно контролировать содержимое внешних устройств, что позволяет своевременно выявлять нарушения, связанные с операциями, выполняемыми с данными на съемных носителях	Раздел 2.1.5

2.1.1. Модуль анализа поведения Dozor UBA: поддержка работы в территориально-распределенных организациях – Multi UBA

Функциональные возможности модуля Dozor UBA, задействованные в Solar Dozor 7.4, позволяют полноценно использовать его в территориально-распределенных организациях. При этом учитываются особенности работы каждой структурной единицы организации (филиала, дочернего предприятия, департамента и т.п.).

Multi UBA позволяет получить все доступные сведения о поведении сотрудников именно в разрезе отдельной организационной единицы (OE). Для этого офицеру безопасности достаточно в соответствующем разделе интерфейса выбрать OE из списка доступных (Рис. 1, Рис. 2).

В окне выбора OE можно просмотреть сводную статистику по всем доступным OE, где, помимо общего количества сотрудников в OE, отражены наиболее значимые с точки зрения безопасности показатели (Рис. 1):

- Количество типов поведения (паттернов) с опасными/подозрительными тенденциями (у таких паттернов цифры, показывающие прирост за неделю, отображаются красным/желтым цветом) – так можно сразу увидеть, на какие паттерны стоит обратить пристальное внимание;
- Количество сотрудников с серьезными аномалиями и их прирост за неделю.

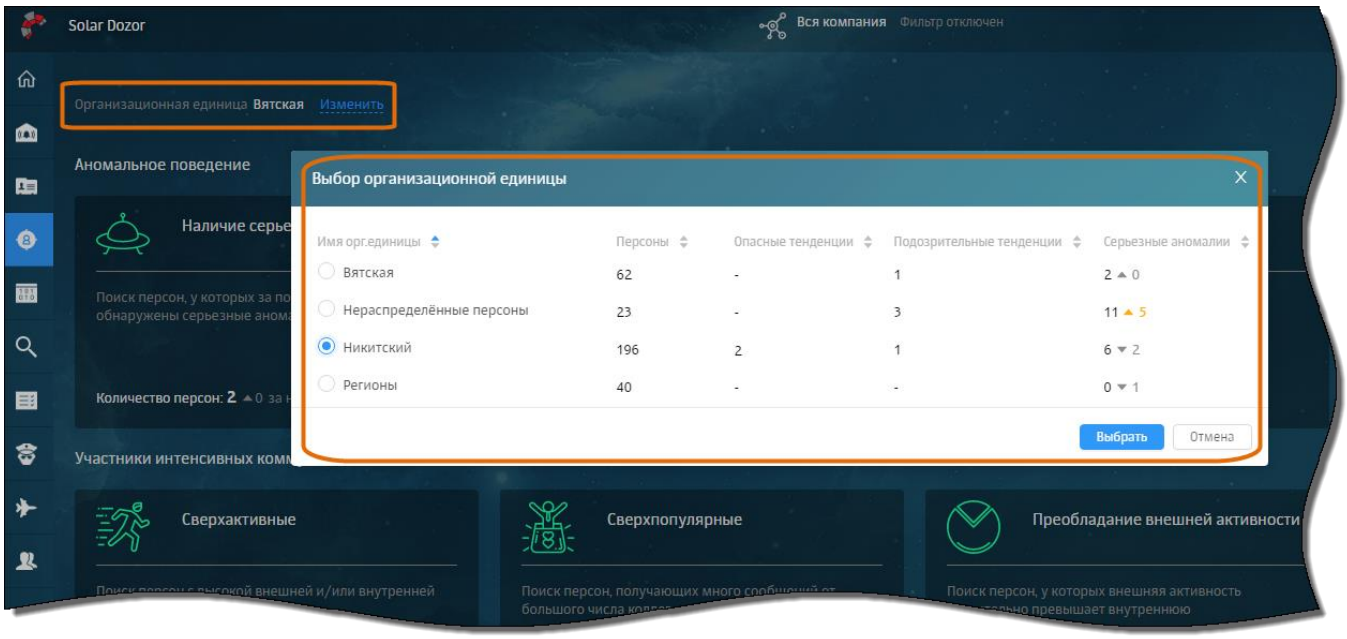


Рис. 1. Раздел «Анализ поведения (UBA)»: выбор ОЕ, сводная статистика по ОЕ

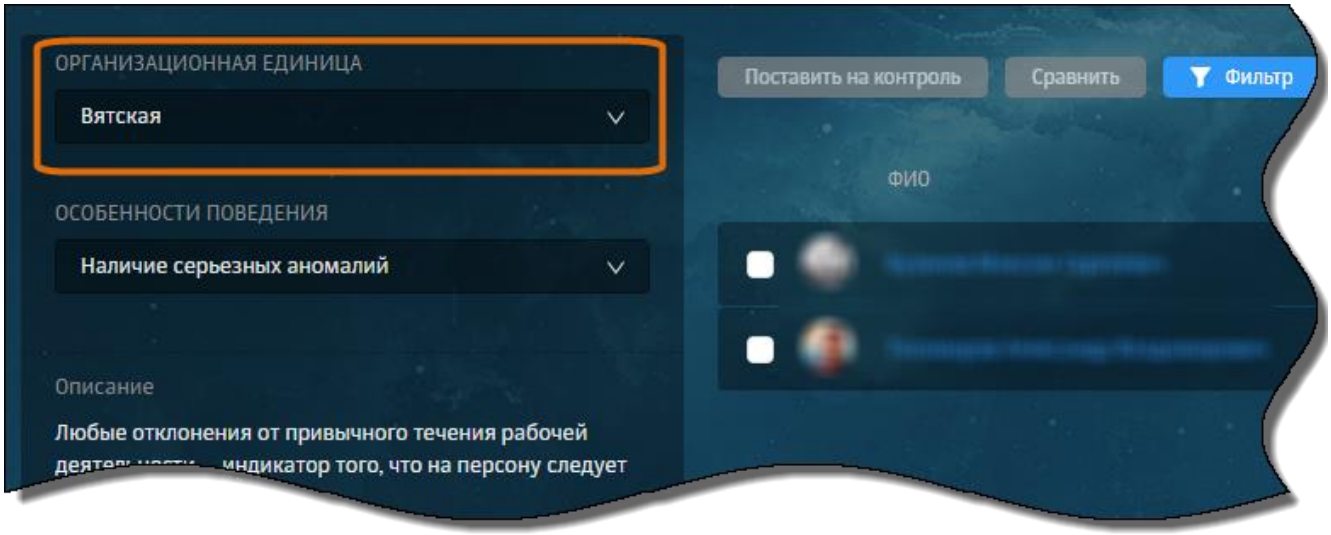


Рис. 2. Раздел «Анализ поведения (UBA) > список сотрудников»: выбор ОЕ – отображение списка сотрудников ОЕ

Также в карточке персоны можно просмотреть статистику переписки сотрудника с коллегами из определенной ОЕ – в карточке персоны на вкладке **Поведение и аномалии > Особые контакты > Внутренние коммуникации**) добавлен элемент, позволяющий фильтровать данные по ОЕ (Рис. 3).

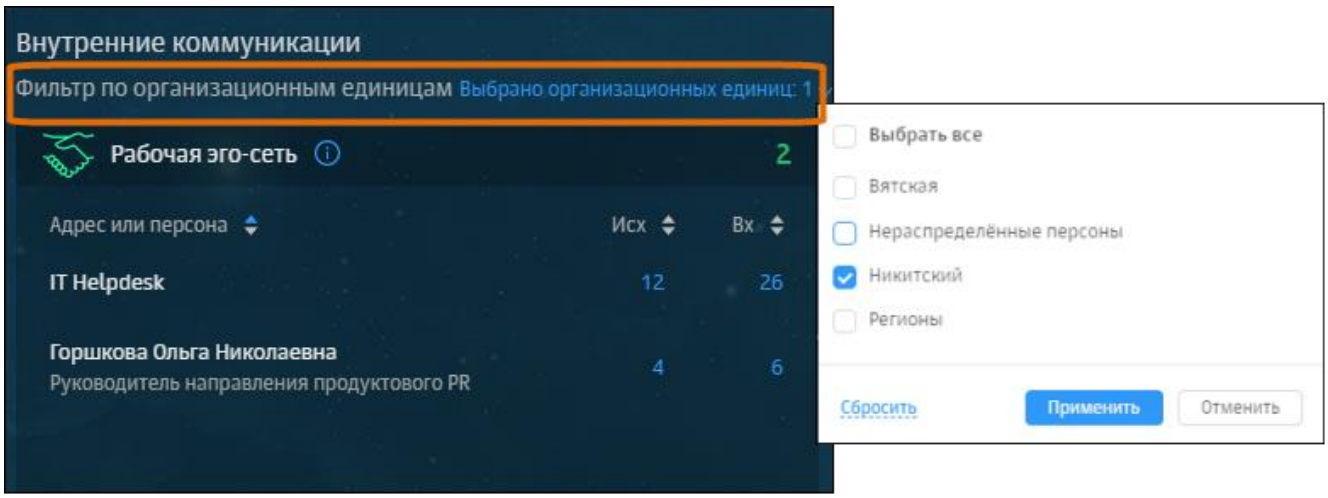


Рис. 3. Рабочая эго-сеть: количество сообщений, количество сообщений, которые сотрудник отправлял коллегам/получал от коллег из определенного филиала из определенного филиала

В расчетах, на основе которых строятся UBA-профили сотрудников в Solar Dozor версии 7.4, учитывается ***часовой пояс*** региона, где работает конкретный сотрудник. К примеру, часовые пояса учитываются в расчетах для определения типов поведения **Работа ночью**, **Работа в выходные дни** и **Признаки увольнения**, а также в статистике суточной активности сотрудников.

Офицер безопасности может задать часовые пояса при создании и настройке ОЕ (Рис. 4).

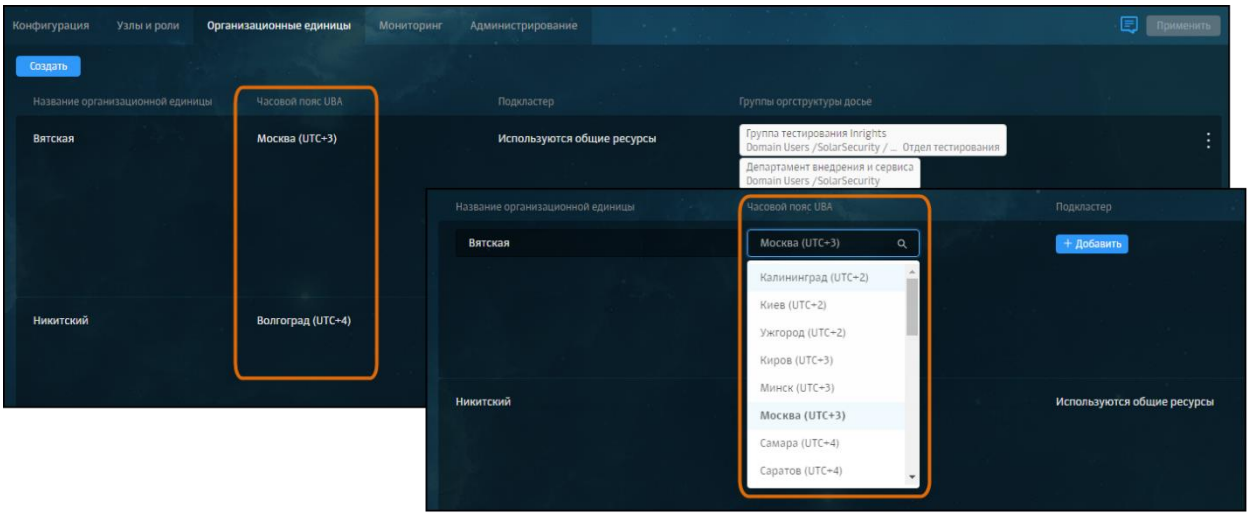


Рис. 4. Раздел «Система > Организационные единицы»: задание часовых поясов для ОЕ

Новая схема расчетов с учетом организационной единицы и часового пояса применяется:

- при формировании UBA-профиля сотрудника: в частности, при определении типов (паттернов) поведения сотрудника и обнаружении аномалий в его поведении;
- при формировании статистики – по особым контактам и показателям суточной активности.

2.1.2. Модуль File Crawler: поддержка работы в территориально-распределенных организациях – Multi Crawler

В Solar Dozor версии 7.4 реализована поддержка работы модуля File Crawler в территориально-распределенных организациях.

Теперь при создании задачи на сканирование определенных объектов ее можно связать с организационной единицей (Рис. 5). Далее параметры задачи задаются с учетом ресурсов ОЕ – сканирующий хост выбирается из списка относящихся к ОЕ, элементы карты сети также доступны из относящихся только к ОЕ.

Примечание. *Если ОЕ не указана, то задача выполняется общими для компании ресурсами и доступна пользователям, у которых нет ограничений по ОЕ.*

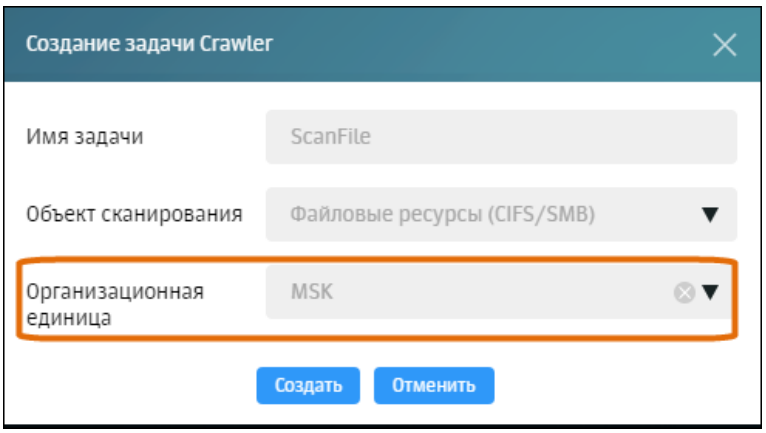


Рис. 5. Создание задачи на сканирование файловых ресурсов: задание ОЕ

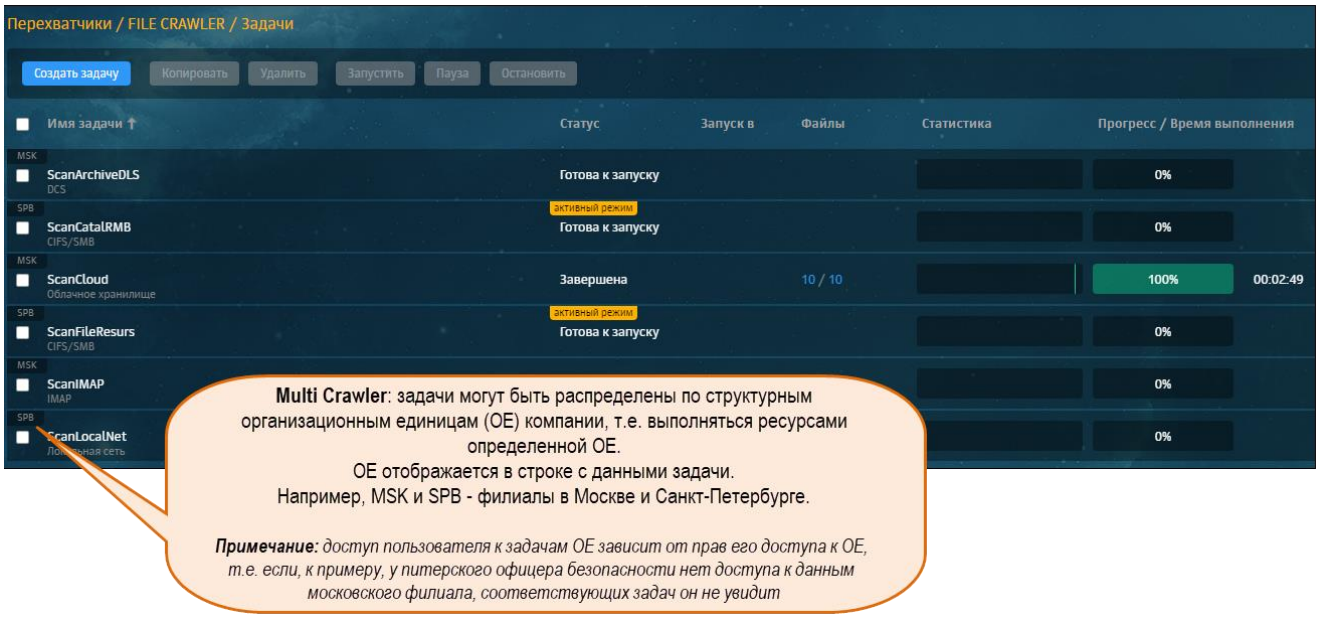


Рис. 6. File Crawler: список задач на сканирование

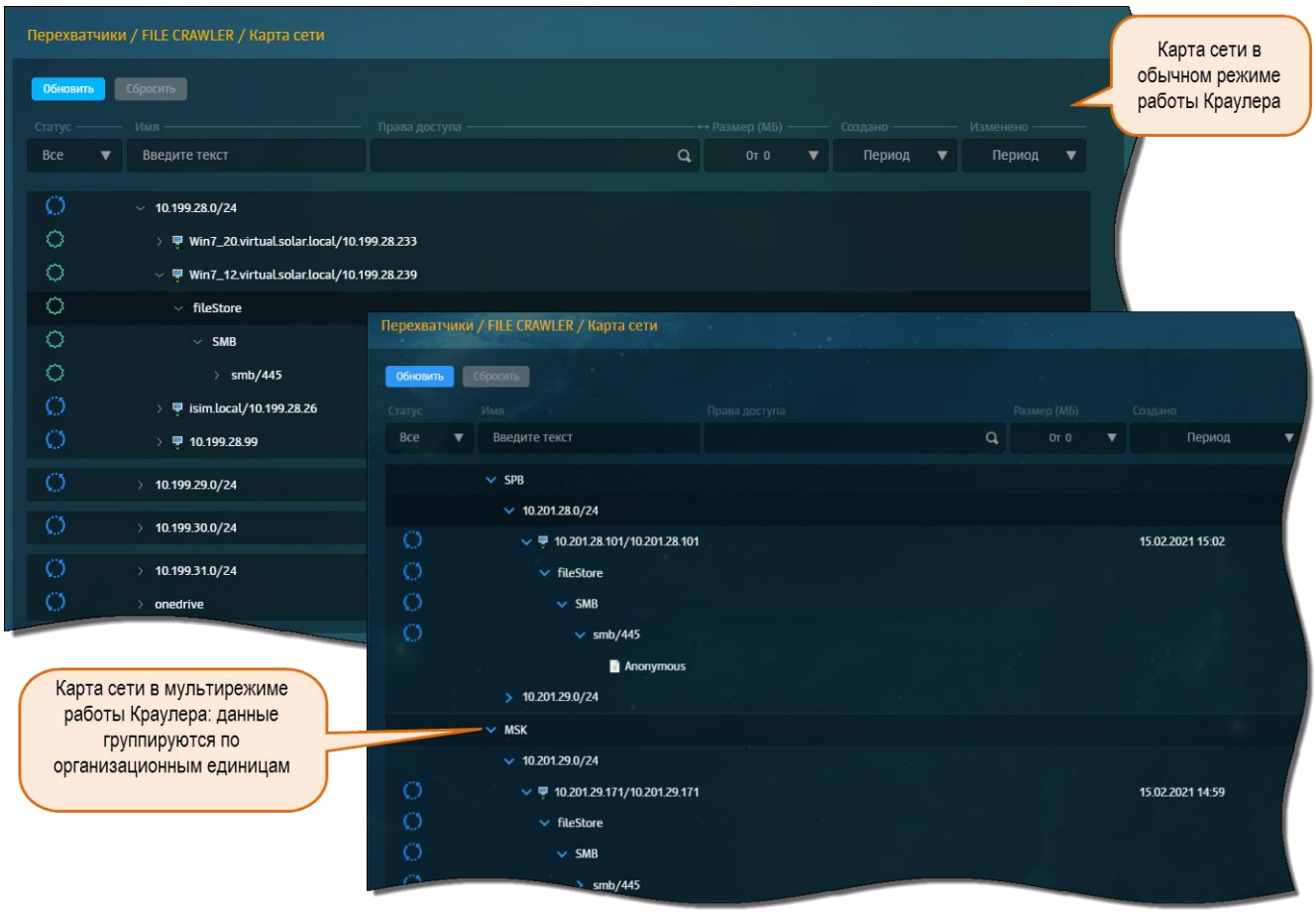


Рис. 7. File Crawler: карта сети

Таким образом, **Multi Crawler** позволяет:

- сканировать файловые/облачные хранилища, локальную сеть и почтовые серверы ресурсами определенных структурно-организационных единиц (филиалов, дочерних организаций и т.п.), что способствует оптимальной нагрузке;
- разграничивать доступ к задачам сканирования и отображаемым на карте сети ресурсам – в соответствии с разрешенными для офицера безопасности организационными единицами.

2.1.3. Трансляция экрана рабочих станций: режим реального времени

В Solar Dozor версии 7.4 офицер безопасности может просмотреть видеотрансляцию того, что в данный момент происходит на рабочем компьютере/ноутбуке интересующего сотрудника.

Трансляция возможна только в том случае, если установленный на рабочей станции агент работает в полнофункциональном режиме.

Запуск видеотрансляции доступен из краткой и полной карточек персоны (Рис. 8). По умолчанию видео открывается в окне-миниатюре, при этом интерфейс Solar Dozor остается доступным для работы. При необходимости видео можно раскрыть на весь экран.

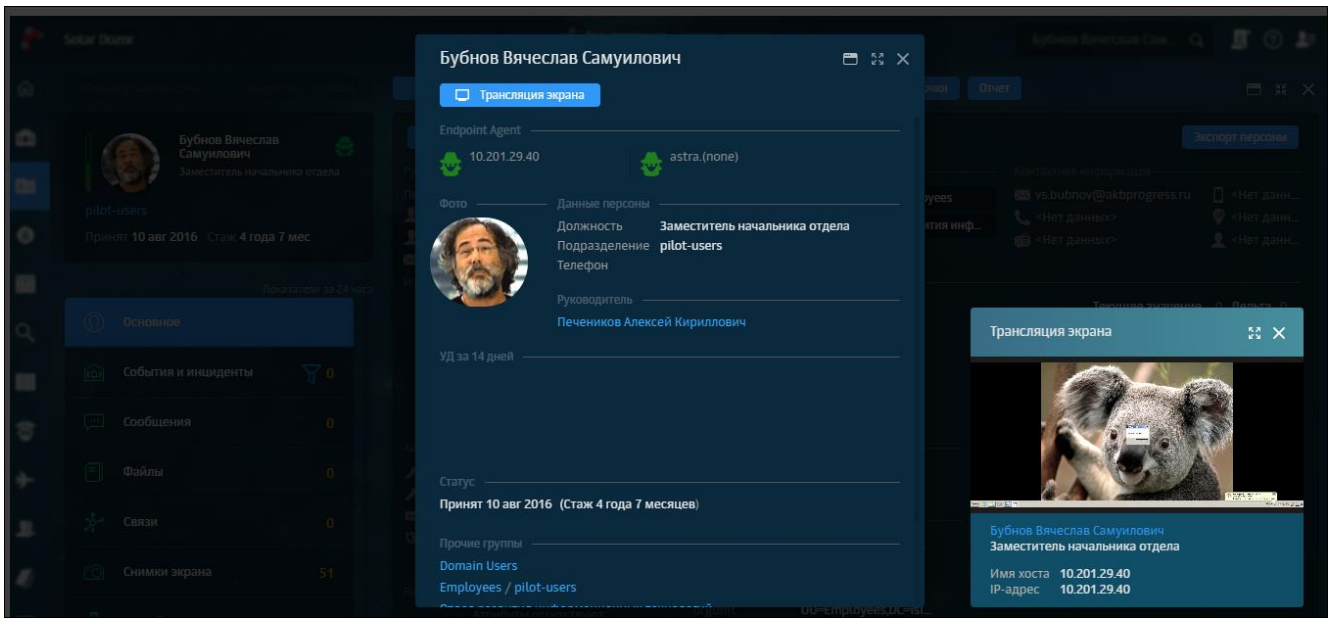


Рис. 8. Карточка персоны: трансляция экрана рабочего компьютера персоны

Если сотрудник использует несколько рабочих станций, можно попеременно просматривать трансляцию экрана каждой из них.

Таким образом, офицер безопасности может ***в режиме реального времени*** прицельно контролировать действия сотрудников, а значит, оперативнее предотвращать возможные нарушения.

2.1.4. Модуль Endpoint Agent: контроль целостности

В Solar Dozor 7.4 обеспечен контроль целостности модуля Endpoint Agent. В рамках реализации канал коммуникации «Действие пользователя» был дополнен информацией о типе сообщения *Endpoint/alert* – попытка нарушения целостности агента.

Теперь офицер безопасности может легко настроить политику таким образом, чтобы при обнаружении факта нарушения целостности агента система создавала событие с высоким уровнем критичности (Рис. 9, Рис. 10). При этом в интерфейсе в разделе **Перехватчики** такой агент будет отображаться со статусом **Поврежден**.

Под нарушением целостности понимается несанкционированное удаление и изменение исполняемых модулей или отключение агента.

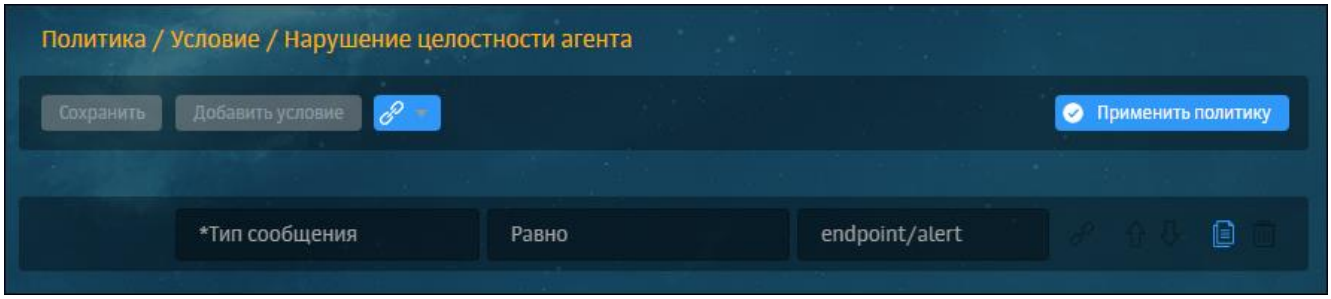


Рис. 9. Политика: условие проверки на нарушение целостности агента

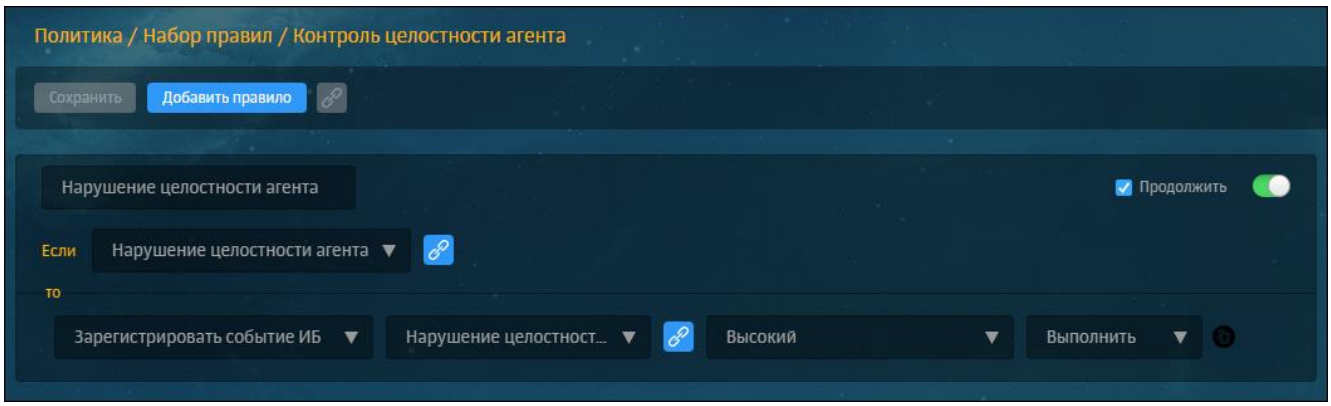


Рис. 10. Политика: набор правил, действующий при нарушении целостности агента

Также можно настроить запись сообщения о нарушении целостности агента в журнал syslog.

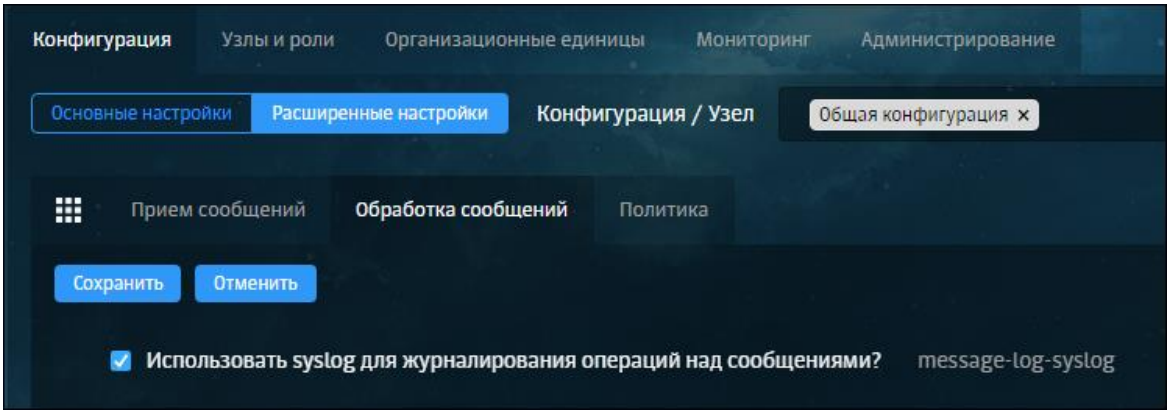


Рис. 11. Настройка журналирования событий в syslog

Кроме того, в разделе **Система > Мониторинг > Показатели Solar Dozor** можно посмотреть сведения о количестве агентов (в графическом виде), сгруппированных по статусам, подстатусам и версиям агентов.

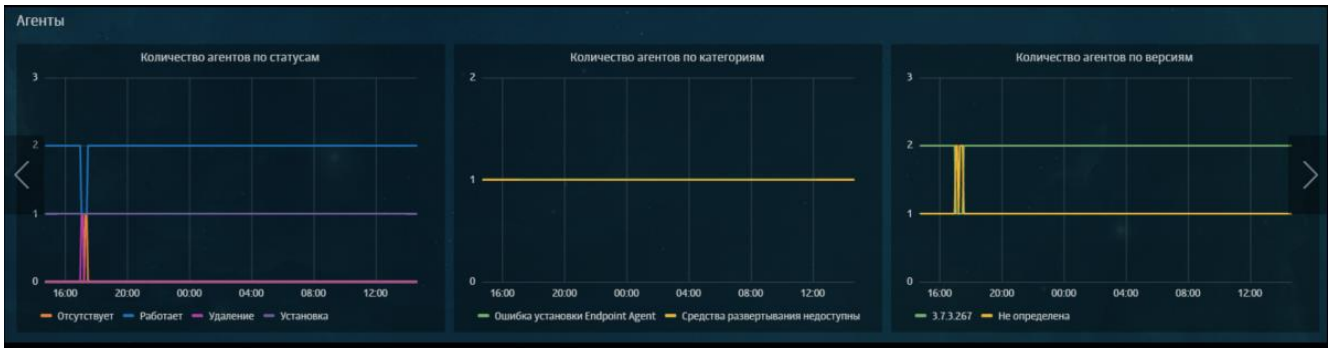


Рис. 12. Мониторинг количества агентов

Все это позволяет своевременно узнать о нарушении и принять соответствующие меры.

2.1.5. Модуль Endpoint Agent: получение сведений о структуре каталогов внешнего носителя

В Solar Dozor 7.4 реализован механизм считывания структуры каталогов съемных носителей информации (флеш-накопителей, карт памяти и внешних жестких дисков), подключенных через USB-порт к рабочим станциям сотрудников компании.

Офицер безопасности может:

- задавать параметры перехвата информации о структуре каталогов с рабочих станций.

  Достаточно установить флажок **Получение структуры каталогов со съемных носителей** и задать максимальное количество считываемых файлов, а также до какого уровня вложенности следует считывать структуру.

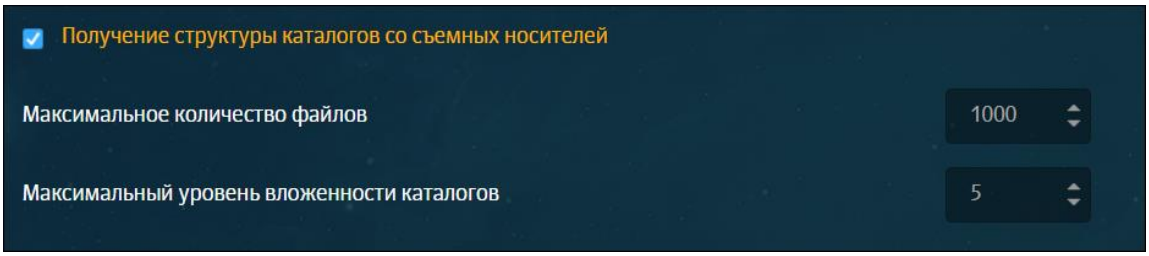


Рис. 13. Параметры перехвата данных о структуре каталогов

- просматривать информацию о структуре каталогов конкретного устройства в интерфейсе Solar Dozor в полной карточке персоны на вкладке **Устройства** (Рис. 14).

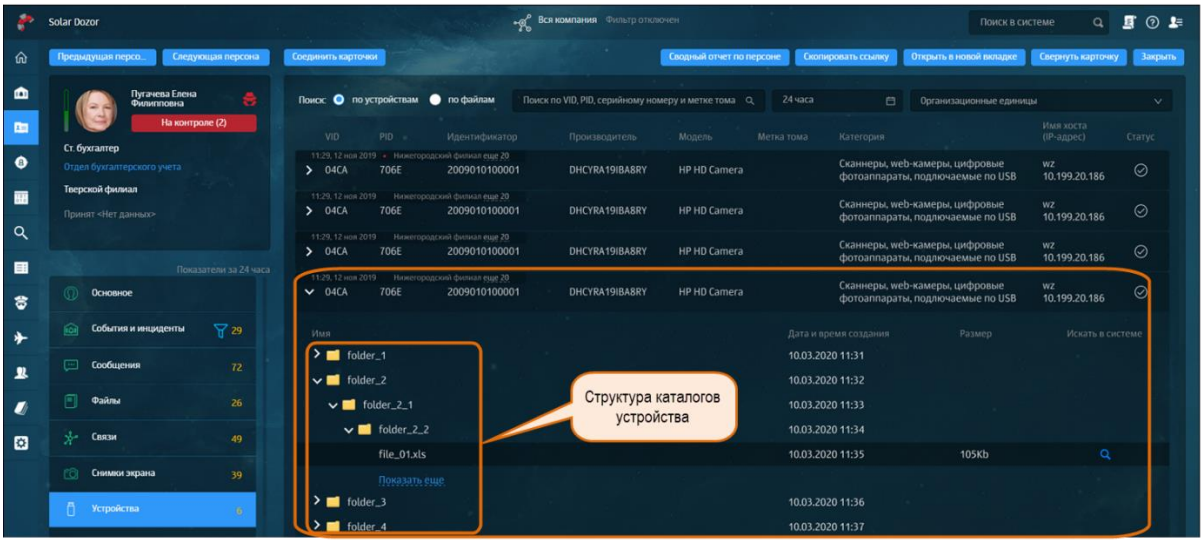


Рис. 14. Карточка персоны, вкладка «Устройства»: данные о структуре каталогов

Также организован поиск файлов по имени (Рис. 15).

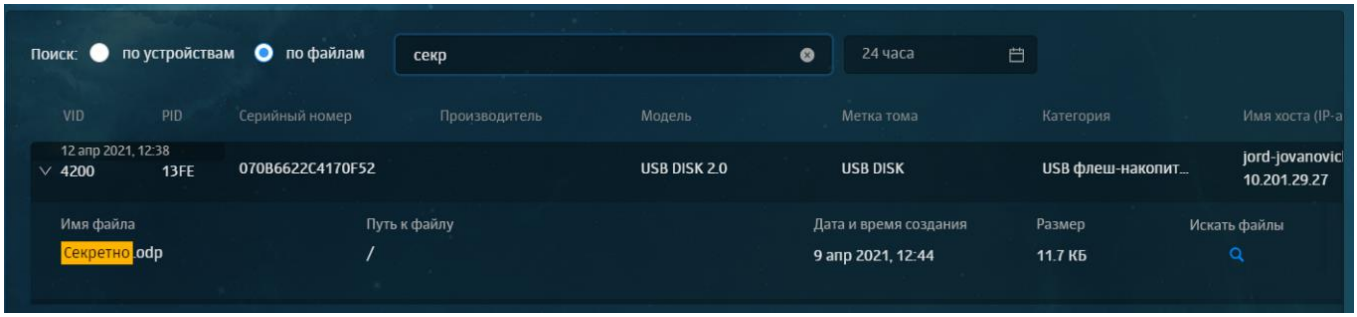


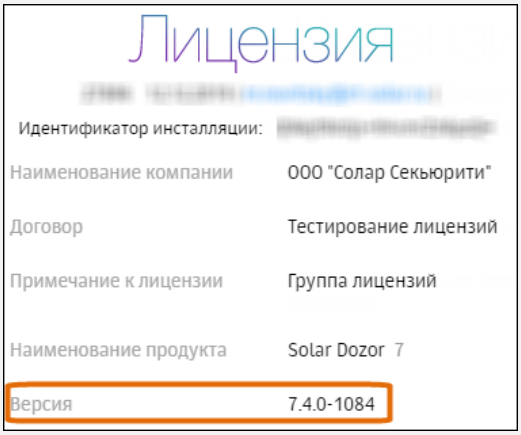
Рис. 15. Карточка персоны, вкладка «Устройства»: поиск файлов

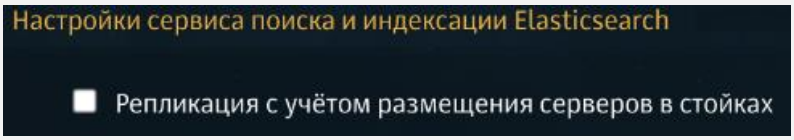
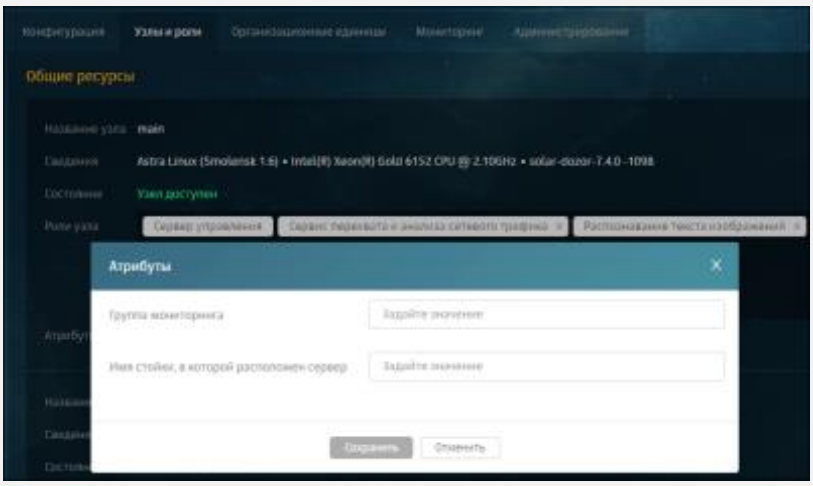
Так можно контролировать содержимое внешних устройств, что позволяет своевременно выявлять нарушения, связанные с операциями, выполняемыми с данными, хранящимися на съемных носителях.

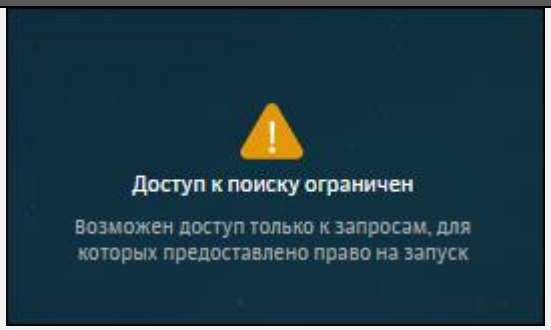
2.2. Улучшение функционала

В Табл. 2 приведен обзор доработок системы, реализованных в Solar Dozor версии 7.4.

Табл. 2. Обзор доработок системы

№	Доработка	Краткое описание
1	Контроль рабочего времени: учет использования клавиатуры и мыши при определении статуса активности сотрудника	В предыдущих версиях Solar Dozor в тех случаях, когда сотрудник оставлял свой компьютер незаблокированным или не отключался от терминальной сессии, считалось, что он активен. В итоге создавалось впечатление, что сотрудник работает круглые сутки, что не соответствовало реальности. Теперь система считает сотрудника 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)
2	Единый для всей системы формат времени и даты	Выработаны общие правила для отображения даты и времени в системе. Теперь вместо различных вариантов отображается, например, дата в формате *<число> <название месяца (максимум 4 символа)> <год>.* Примеры: 18 янв 2017, 10 мая 1999
3	Отображение сведений о версии продукта в окне с информацией о лицензии	Теперь сведения о версии продукта можно посмотреть не только в разделе **Система**, доступ к которому может быть ограничен, но и в окне с информацией о лицензии: 
4	Модуль Endpoint Agent: комплексная проверка банковских карт	В предыдущих версиях системы контроль банковских карт на агенте состоял только из определения номера карты. В версии 7.4 реализована возможность комплексной проверки номеров банковских карт – проверяется: • наличие номера карты в тексте сообщения и/или файла; • контрольная сумма найденных номеров карт (для подсчета контрольной суммы используется специальный алгоритм Луна). В структуру условия политики добавлены: • атрибут **Агент: перехват: текст содержит номера банковских карт**, который применяется только для агентской политики; • операция сравнения **удовлетворяет рег. выражению с учетом алгоритма Луна**", которая доступна только для указанного выше атрибута. Использование комплексной проверки повышает качество срабатывания правила политики при обнаружении номеров банковских карт

№	Доработка	Краткое описание
5	Модуль Endpoint Agent (ОС Windows): информирование о необходимости перезагрузки рабочей станции	Теперь система уведомляет пользователя о том, что после настройки определенных каналов перехвата требуется перезагрузка рабочей станции – в интерфейсе при изменении конкретных настроек отображается соответствующая надпись
6	Модуль Endpoint Agent: отключение перехвата данных нажатием кнопки в интерфейсе	Штатный механизм отключения агентского перехвата информации предполагает настройку – перевод агентов в режим "Без перехвата". Это занимает время, что в аварийных ситуациях может быть достаточно критично. В новой версии разработан механизм оперативного отключения перехвата – теперь отключить перехват (и обратно восстановить нормальную работу агентов) можно нажатием одной кнопки в интерфейсе. Таким образом, при конфликтах со сторонним ПО можно временно деактивировать агент, не удаляя его с рабочей станции. При этом все настройки сохраняются и при обратной активации агента нет необходимости снова его настраивать
7	Мониторинг работы системы: объединение серверов в группы и отображение информации о работе групп серверов	Реализована возможность создавать и выбирать группы серверов, по которым нужно отобразить информацию. Так можно отобразить, например, 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
8	Оптимизация индексирования в Elasticsearch: репликация с учетом распределения узлов по стойкам	Реализована возможность репликации Elasticsearch с учетом распределения узлов по стойкам. Пользователь может: • подключать/отключать репликацию:  • задавать расположение реплик, указав для узла имя стойки, в которой находится сервер: 
9	Поиск: выдача прав доступа на выполнение поисковых запросов	Теперь офицер безопасности может предоставлять другим пользователям доступ на выполнение созданных им поисковых запросов. Такие пользователи смогут выполнять запросы, а также просматривать их параметры и результат выполнения.

№	Доработка	Краткое описание
		 Такая – более гибкая – настройка доступа к данным системы для сотрудников младшего звена позволит снизить риск утечки ценных сведений
10	Пополнение справочника приложений	Теперь контролируемых приложений стало больше – в системный справочник приложений добавлены сведения о новых приложениях и их процессах
11	Модуль Endpoint Agent (ОС Windows): добавлен канал перехвата Dropbox	Агент 4.0 для ОС Windows, синхронизированный с 7.4, может перехватывать материалы, передаваемые по Dropbox (desktop)