

INFOWATCH

InfoWatch Vision 2.0. Руководство пользователя

09/09/2019

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 4

2 Комплект документов 5

3 Техническая поддержка пользователей 6

4 Интерфейс Vision 2.0 7

4.1 Единый фильтр 8

4.2 Раздел "Статистика" 11

4.2.1 Виджеты статистики 12

4.3 Раздел "События" 16

4.4 Раздел "Граф связей" 17

4.4.1 Общие сведения о графе 18

4.4.2 Принципы построения графа 21

4.5 Раздел "Досье" 26

4.5.1 Просмотр досье персоны 27

4.5.2 Виджеты досье 28

4.5.3 Добавление контактов персоны 29

4.5.4 Объединение досье 29

4.5.5 Создание, редактирование и удаление досье 29

4.5.6 Изменение руководителя персоны 30

4.5.7 Граф связей персоны 30

4.5.8 Комментирование в досье персоны 31

4.5.9 Добавление файла в досье 31

5 Примеры сценариев работы Офицера безопасности 32

5.1 Ежедневный анализ коммуникаций выбранных сотрудников 32

5.2 Анализ активности сотрудника 32

5.3 Выявление канала утечки 35

5.4 Анализ взаимодействий выбранного сотрудника 36

5.5 Анализ бизнес-процессов внутри компании 37

5.6 Быстрый поиск аномалий в поведении сотрудников 39

5.7 Сбор информации в досье 42

В настоящем руководстве вы сможете найти сведения по работе и решению задач в InfoWatch Vision 2.0 – программном обеспечении, предназначенном для визуализации расследования инцидентов на основе данных, полученных от InfoWatch Traffic Monitor.

1 Аудитория

Информация, содержащаяся в Руководстве, предназначена для пользователей, работающих с Системой (выполняющих настройку конфигурации, анализ информационных объектов и т. п.).

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционной системы Microsoft Windows.

2 Комплект документов

В комплект документации по InfoWatch Vision 2.0 входят:

- «InfoWatch Vision 2.0. Руководство по установке». Содержит описание процесса установки, обновления и удаления InfoWatch Vision 2.0.
- «InfoWatch Vision 2.0. Руководство администратора». Содержит информацию по настройке и подготовке к работе InfoWatch Vision 2.0.
- «InfoWatch Vision 2.0. Руководство пользователя». Содержит описание порядка работы и решения задач в InfoWatch Vision 2.0.

Сопутствующая документация по комплексу InfoWatch Traffic Monitor включает в себя:

- «InfoWatch Traffic Monitor. Руководство по установке». Содержит описание порядка установки, настройки, обновления и удаления системы InfoWatch Traffic Monitor.
- «InfoWatch Traffic Monitor. Руководство администратора». Содержит информацию по администрированию Системы (база данных, серверная часть).
- «InfoWatch Traffic Monitor. Руководство пользователя». Содержит описание порядка работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, составление политик для обработки объектов).
- «InfoWatch Traffic Monitor. Справочник по конфигурационным файлам». Содержит пояснения к часто используемым конфигурационным файлам.

3 Техническая поддержка пользователей

При возникновении проблем и вопросов, связанных с работой Системы, вы можете обратиться в службу технической поддержки:

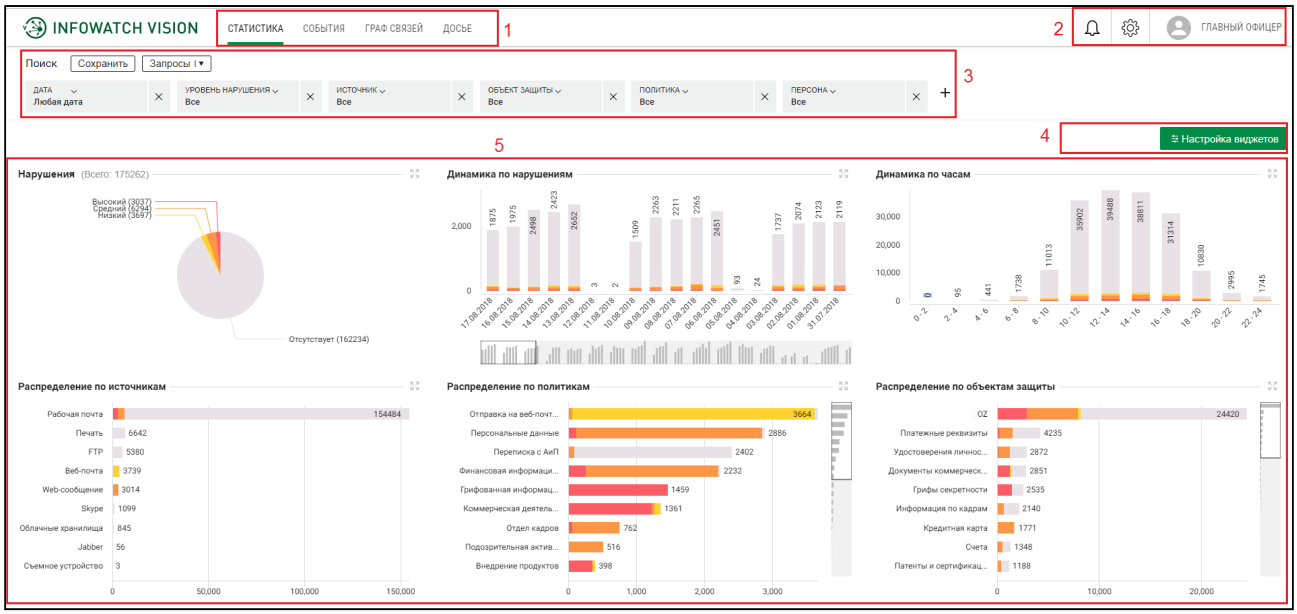
- если вы приобрели продукт у партнера компании InfoWatch, то обратитесь в службу технической поддержки партнера.
- если продукт приобретен у компании InfoWatch напрямую, то обратитесь в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

Часы работы Службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни в РФ. Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/support.

Перед обращением в службу технической поддержки рекомендуется посетить раздел База знаний на нашем сайте: https://kb.infowatch.com/. Возможно, там уже содержится ответ на интересующий вас вопрос или описано решение возникшей у вас проблемы.

4 Интерфейс Vision 2.0

Окна интерфейса InfoWatch Vision содержат ряд общих элементов (1-3), а также ряд специфичных элементов (4,5).



Элементы окна:

Номер на схеме	Элемент окна	Назначение элемента
1	Панель навигации	Отображение разделов Vision. При выборе раздела выполняется переход к нему.
2	Настройки Vision и меню пользователя	Отображение пользовательского меню. При нажатии раскрывается список, в котором пользователь может: • отредактировать свою учетную запись; • сменить пароль своей учетной записи; • сменить язык интерфейса; • выполнить выход.
3	Панель фильтрации (Единый фильтр)	Отображение примененных фильтров. Пользователь может отредактировать уже созданные фильтры и добавить новые.
4	Панель настроек рабочей области	Отображение пользователю доступных действий для этого раздела.
5	Рабочая область	Отображение элементов выбранного раздела Vision и работа с ними.

Работа в Vision ведется в тематических разделах:

Раздел	Описание
Статистика	Раздел содержит статистическую информацию о нарушениях/нарушителях согласно установленным фильтрам.
События	Раздел содержит список событий, согласно установленным фильтрам.
Граф связей	Раздел для визуализации событий в виде графа связей.
Досье	Раздел содержит справочник персон компании, а также внешних контактов.

4.1 Единый фильтр

Единый фильтр - универсальный инструмент, который используется во всех разделах. С его помощью Офицер безопасности может:

- проанализировать все взаимодействия персоны в рамках одного среза информации;
- сохранять различные наборы фильтров, для того чтобы быстро получать интересующие срезы информации;
- исключить из анализа часть событий, чтобы скрыть лишнюю информацию;
- отфильтровать части информации на графе связей, чтобы упростить анализ коммуникаций персоны.

Фильтр можно задать от одного атрибута и выбрать хотя бы одно значение. Фильтр доступен во всех разделах Системы: **Досье**, **События**, **Статистика**, **Граф связей** - и может быть настроен по различным атрибутам:

Название атрибута	Описание и возможные значения атрибута
Дата	Дата наступления события. Выберите период времени, данные за который вас интересуют: • Последние 7 дней; • Последние 30 дней; • Последние 90 дней; • Этот месяц; • Прошлый месяц; • Произвольный период (можно выбрать даты начала и окончания периода либо список произвольных дат).
Часы	Установите время наступления события.
Уровень нарушения	Выберите уровень нарушения (соответствует аналогичному в Traffic Monitor): • Высокий; • Средний; • Низкий; • Отсутствует.

Тип события	Создает выборку по типу события. Выберите тип события в Traffic Monitor: • WhatsApp; • Yahoo!; • Буфер обмена; • ВКонтакте; • Ввод с клавиатуры; • Веб-почта; • Краулер; • Облачные хранилища; • Печать; • Почта на Клиенте; • Сетевой ресурс; • Соцсеть; • Съемное устройство; • Терминальная сессия; • Фотосъемка.
Объект защиты	Выберите из списка объекты защиты, созданные в ТМ.
Политика	Выберите из списка политики, созданные в ТМ.
Вердикт	Выберите из списка интересующие вердикты событий ТМ: *Запрещен, Разрешен, На карантине.*
Нарушения	Укажите вариант поиска: искать события с нарушениями или без них.
Имя файла	Выберите файлы из загруженных файлов-вложений в событиях ТМ.
Тип файла	Выберите типы файлов-вложений в событиях ТМ.
Источник	Выберите источник из списка успешных интеграций, данные которых добавить в выборку: *Traffic Monitor* или *LDAP.*
Интеграция	Выберите интеграцию из списка имен успешных интеграций.
Контакты	Позволяет отсортировать идентифицированные и неидентифицированные контакты.
Тип контакта	Укажите вариант поиска: по известным контактам персон в системе или внешним контактам персоны.
Персона*	Укажите сотрудника из списка или введите в строке поиска.

Группы*	Создает выборку по группам AD и TM. Укажите группы в иерархии в компании, синхронизированные из TM или AD.
Должность*	Укажите все интересующие должности в компании, синхронизированные из TM или AD.
Отдел*	Укажите все интересующие отделы в компании, синхронизированные из TM или AD.
Статус*	Укажите все интересующие статусы сотрудников в компании, синхронизированные из TM или AD.

* - Для атрибутов, связанных с персонами, можно установить модификаторы:

- *Любой;*
- *Отправитель;*
- *Получатель.*

Если установить модификатор *Отправитель/Получатель*, то выбранные персоны или группы персон будут являться отправителями или получателями в событиях.
Если установить модификатор *Любой*, то будут выбраны все участники события: все персоны или группы персон.

После изменения значений атрибутов в фильтре автоматически перестраиваются:

- диаграммы, распределения и таблицы в разделе **Статистика**;
- таблица с данными событий в разделе **События**;
- графическое отображение в разделе **Граф связей**.

Чтобы сохранить установленные атрибуты фильтров для использования в дальнейшем:

1. Нажмите **Сохранить** в области Единого фильтра.
2. В открывшемся окне задайте имя нового фильтра.
3. Выберите тип фильтра:
    a. Личный - при этом фильтр будет доступен только Офицеру безопасности, который его создал
    b. Общий - фильтр будет доступен всем пользователям Системы
4. Нажмите **Сохранить**

Чтобы воспользоваться ранее созданным фильтром:

1. Нажмите **Запросы** в области Единого фильтра.
2. Щелкните на интересующий фильтр, чтобы его активировать. При этом Офицер безопасности может:
    a.  - отредактировать Личные фильтры и Общие фильтры.
    b.  - удалить Личные фильтры , а также Общие фильтры, при условии, что он создал их ранее.

Если требуется удалить один фильтр с панели Единого фильтра, нажмите  напротив него.

Если требуется очистить ранее введенные значения фильтра, раскройте фильтр, нажав на его имя, и затем **Очистить фильтр**.

Важно!

Необходимо учитывать, что:

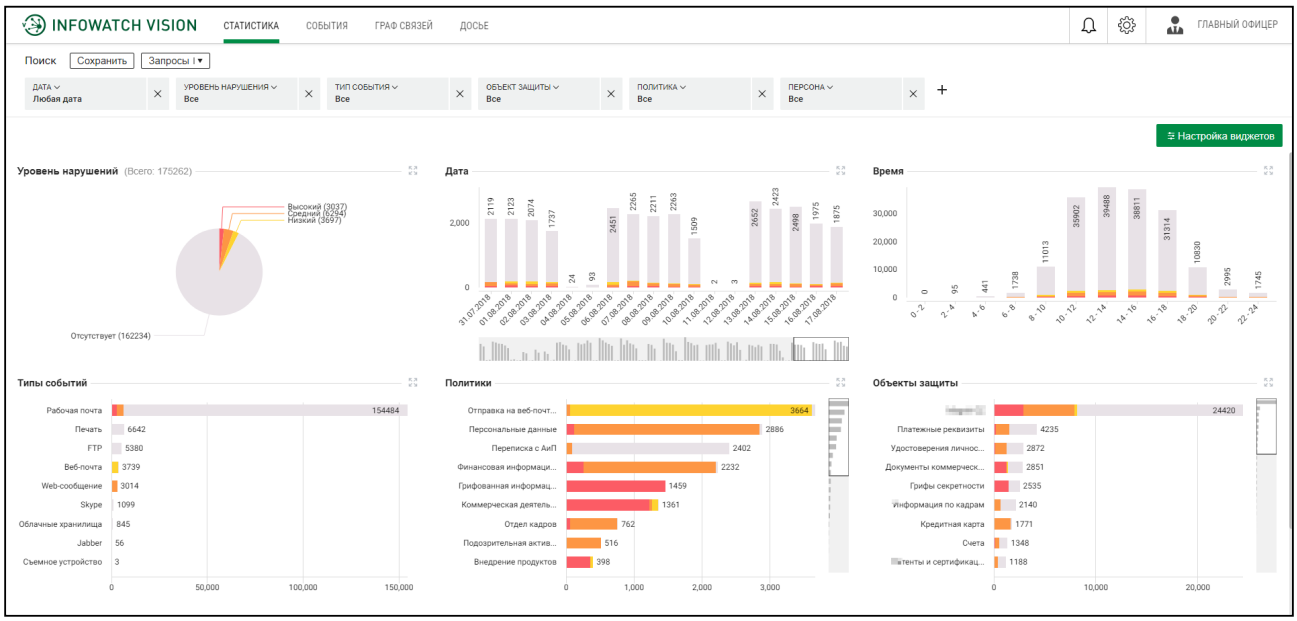
- все настройки Единого фильтра распространяются только в рамках одной вкладки в браузере;
- при перемещении на шаг назад или вперед (кнопка "Назад"/"Вперед" браузера) фильтр возвращается в то состояние, в каком он был на этом шаге;
- при выходе из Системы все атрибуты фильтра сбрасываются в исходное состояние.

4.2 Раздел "Статистика"

О разделе:

Раздел содержит статистическую информацию о нарушениях/нарушителях. Она отображается на виджетах, которые:

- удобно использовать для ежедневного мониторинга;
- позволяют быстро просмотреть статистику по событиям.



С помощью кнопки **Открыть на весь экран** вы можете развернуть выбранный виджет на весь экран. Чтобы вернутся в нормальный режим, нажмите **Свернуть**.

Настройки рабочей области позволяют самостоятельно:

- установить размер виджета;
- выбрать расположение виджета на рабочей области.

Чтобы настроить отображение виджетов, нажмите **Настройка виджетов**, затем:

1. Если необходимо скрыть виджет с рабочей области, нажмите . Если необходимо расположить виджет на другом месте экрана, перетащите виджет в любое место рабочей области, нажав и удерживая указатель мыши на его названии.
2. Нажмите **Сохранить**, чтобы зафиксировать изменения.

Чтобы добавить виджет:

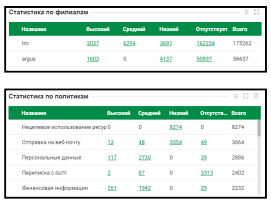
1. Нажмите **Настройка виджетов** -> **Добавить виджет** в правом верхнем углу рабочей области.
2. В открывшемся окне нажмите **Добавить виджет** напротив нужного виджета. Нажмите **Отменить**, если виджет был выбран ошибочно.
3. Подтвердите действие, нажав **Применить**, а затем **Закрыть**. Новый виджет будет добавлен на рабочую область. Если не требуется применять действия, нажмите **Отменить**.
4. Нажмите **Сохранить**, чтобы выйти из режима управления виджетами. Все внесенные изменения будут сохранены.

Чтобы отфильтровать информацию на виджете по нужному параметру:

1. Укажите нужный параметр на диаграмме либо кликните левой клавишей мыши на его описании.
2. Нажмите  в углу виджета. Параметры Единого фильтра будут изменены, и отображение на виджетах перестроится.

4.2.1 Виджеты статистики

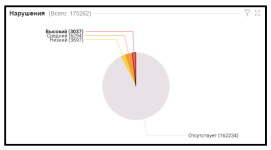
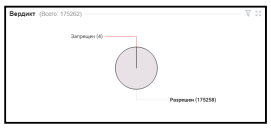
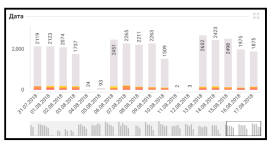
Виджеты в разделе **Статистика** наглядно отображают хранящиеся в Системе данные:

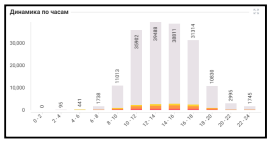
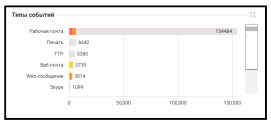
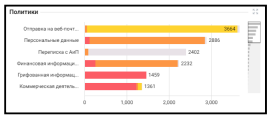
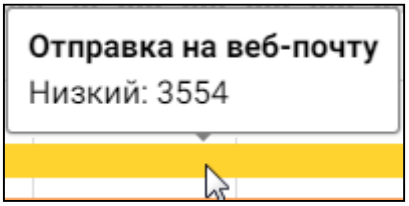
<table>
<tr><th>Название виджета</th><th>Описание</th></tr>
<tr><td>Статистика

</td><td>Отображает данные в виде таблицы. В настройках пользователь может выбрать тип статистики (по персонам, политикам, объектам защиты или филиалам), а также указать распределение событий (по источникам или по уровню нарушений).

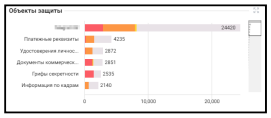
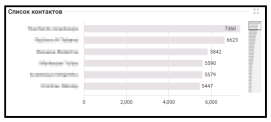
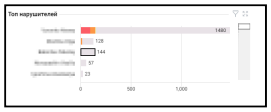
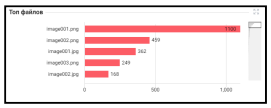
Чтобы установить настройки виджета:

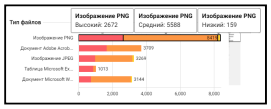
1. Нажмите  в правом верхнем углу виджета.
2. Задайте значения:

<table><tr><th>Параметр</th><th>Описание</th></tr><tr><td>Выберите значение для строки</td><td>Можно выбрать одно значение из предложенных:
- Персоны
- Политики
- Объекты защиты
- Филиалы</td></tr><tr><td>Выберите значение для столбца</td><td>Можно выбрать одно значение из предложенных:
- Источники
- Уровень нарушения</td></tr></table>
3. Установите флажок Показать суммарное количество событий, чтобы добавить в таблицу столбец Всего.
4. Нажмите Сформировать. Таблица будет сформирована заново.

Если требуется, можно добавить несколько виджетов Статистика с другими настройками.</td></tr>
<tr><td>Уровень нарушений
</td><td>Отображает распределение событий по уровням нарушений.</td></tr>
<tr><td>Вердикт
</td><td>Отображает информацию о распределении событий в Системе по вердиктам, назначенным этим событиям Офицером безопасности в Traffic Monitor. Рядом с каждым сектором указано, сколько событий с каким вердиктом загружено в Систему.</td></tr>
<tr><td>Дата
</td><td>Отображает распределение событий в Системе по датам. Можно выбрать одну или несколько дат и отфильтровать события за выбранный день.</td></tr>
</table>

Время 	Отображает распределение событий по часам суток (по два часа).
Типы событий 	Отображает распределение распределение событий Traffic Monitor по типам событий. Чтобы получить расширенную информацию: Если навести курсор на имя источника, выводится расширенная информация о количестве событий с разными уровнями нарушения в них: 
Политики 	Отображает распределение событий с разными уровнями нарушений по политикам. Чтобы получить расширенную информацию: Если навести указатель мыши на любую область столбцов диаграммы, отображается информация, сколько событий, с каким уровнем нарушения зарегистрировано в Системе и удовлетворяют выбранной политике.  **Примечание:** Если к событию применялось несколько политик, то оно учитывается несколько раз - для каждой из политик. На виджете отображаются все политики из отобранных с помощью единого фильтра событий. Поэтому при выборе одной из политик в качестве фильтра пользователь может увидеть на виджете и другие политики, которые также сработали на отобранных событиях.

Объекты защиты 	Отображает распределение событий с разными уровнями нарушений по объектам защиты. Событие отображается в статистике, если в нем присутствует какой-либо из выбранных объектов защиты. **Примечание:** Если в событии присутствуют несколько объектов защиты, то оно учитывается несколько раз - для каждого из найденных объектов защиты. На виджете отображаются все объекты защиты из отобранных с помощью единого фильтра событий. Поэтому при выборе одного из объектов защиты в качестве фильтра пользователь может увидеть на виджете и другие объекты защиты, которые также появлялись в отобранных событиях.
Список контактов 	Отображает круг общения персоны со всеми типами контактов: идентифицированными и неидентифицированными. Выводятся первые 50 наиболее популярных контактов.
События 	Отображает список событий, загруженных из ТМ и удовлетворяющих условиям фильтрации, в виде таблицы. Чтобы получить подробные данные о событии: 1. Выделите одно или несколько событий, зажав клавиши *Shift* или *Ctrl.* 2. Нажмите  справа в строке события или . 3. Нажмите **Перейти к событию в исходной системе**. В браузере откроется новая вкладка с Консолью управления ТМ, где отобразится событие, синхронизация с которым была осуществлена ранее.
Топ нарушителей 	Отображает список персон, нарушения которых встречаются в Системе наиболее часто. Выводятся первые 50 нарушителей, отсортированных по событиям с максимальным уровнем нарушений.
Топ файлов 	Отображает список файлов по нарушениям, перехваченных Traffic Monitor, с указанием количества упоминаний. Выводятся первые 50 наиболее встречаемых файлов.

Тип файлов 	Отображает статистику событий по различным типам файлов (например: графические, текстовые, медиа и т.д.). У столбца диаграммы указано общее количество событий с файлами данного типа.
Список событий (расширенный и краткий)	Отображают события в табличном представлении или в виде списка (подробнее см. Раздел "События")
Источник 	Отображает распределение событий по филиалам: показано, сколько событий загружено в Систему из разных филиалов компании.

Важно!

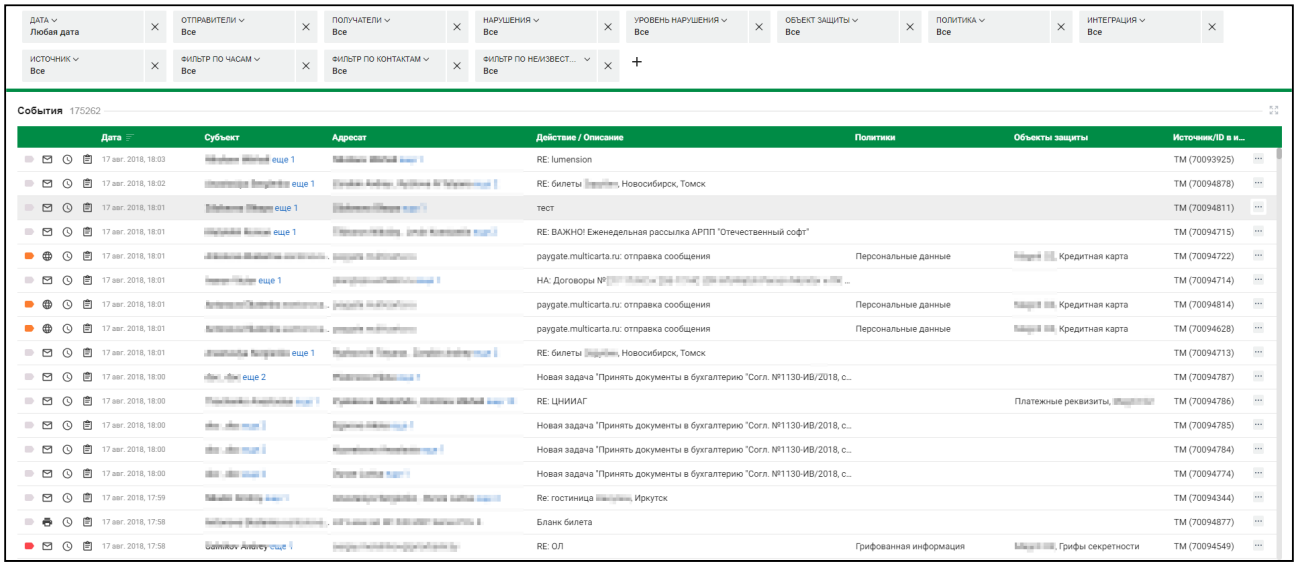
Для обеспечения стабильной работы виджетов рекомендуется избегать составления сложных запросов и применять дополнительные фильтры.

4.3 Раздел "События"

О разделе:

В разделе можно просмотреть данные всех событий, загруженных в Систему после синхронизации с Traffic Monitor:

- уровень нарушения в событии;
- тип события;
- решение Офицера безопасности по событию;
- статус отправки;
- дата создания события в ТМ;
- субъект - лицо, совершившее нарушение;
- адресат - лица, которым субъект передал данные;
- описание переданных данных;
- политики, сработавшие на данном виде нарушения;
- объекты защиты, которые были переданы;
- идентификатор события в ТМ.



Чтобы получить нужную выборку по событиям, ОБ настраивает фильтры на панели Единого фильтра (подробнее см. "Единый фильтр"). В полученном списке событий ОБ может выбрать несколько событий и перейти в исходную систему для более подробного анализа. Если события принадлежат нескольким источникам, то они будут открыты в разных вкладках браузера.

Чтобы ознакомиться с данными одного события в исходной системе:

1. Нажмите ... напротив нужного события.
2. Нажмите **Перейти к событию в исходной системе**.

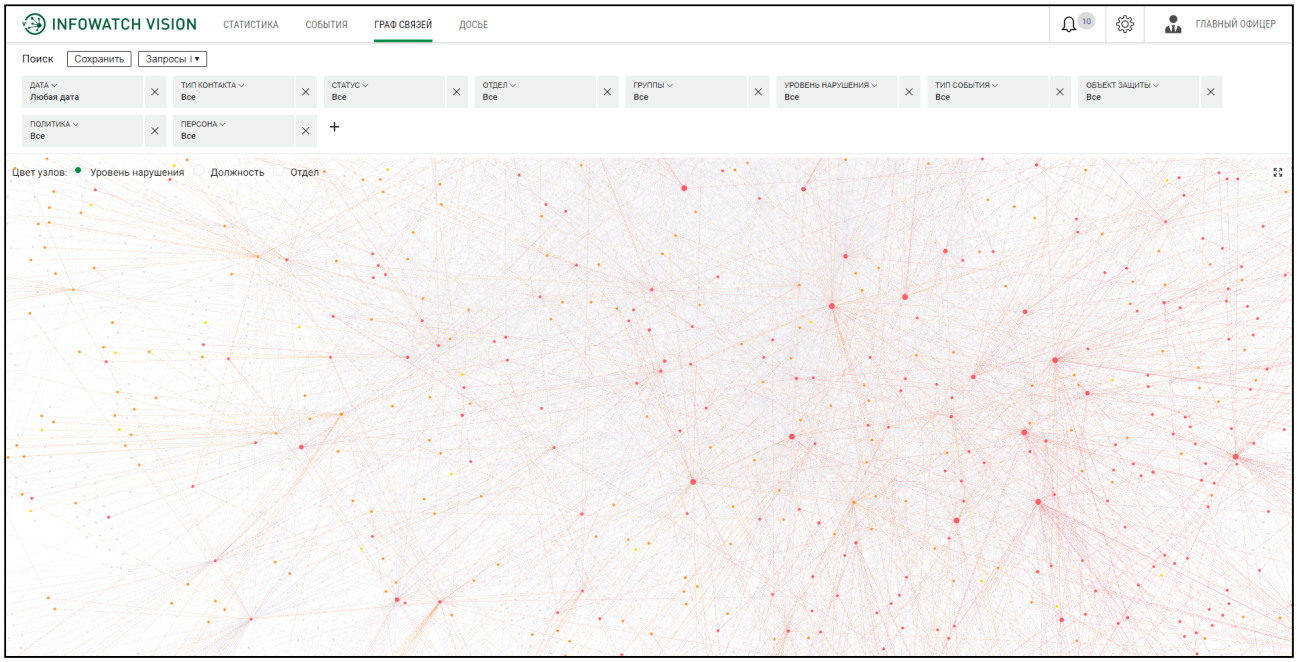
Чтобы ознакомиться с данными группы событий, выделите нужные события и нажмите .

> ⚠ **Примечание:**
>
> Для корректной работы необходимо разрешить открывать всплывающие окна с указанных источников в браузере.

4.4 Раздел "Граф связей"

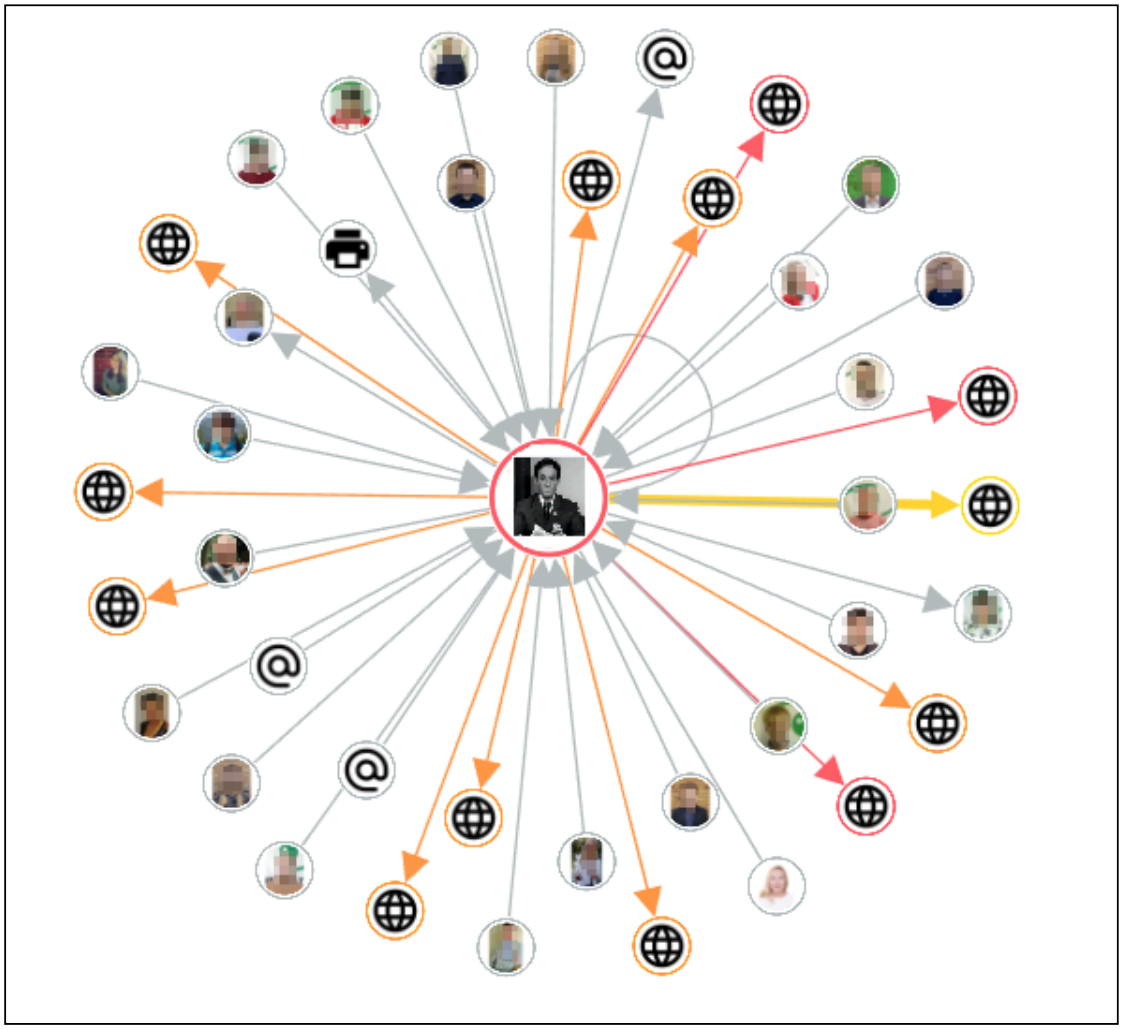
О разделе:

В разделе собранные в Системе данные визуализируются на экране в виде Графа связей, который строится на основании значений атрибутов Единого фильтра.

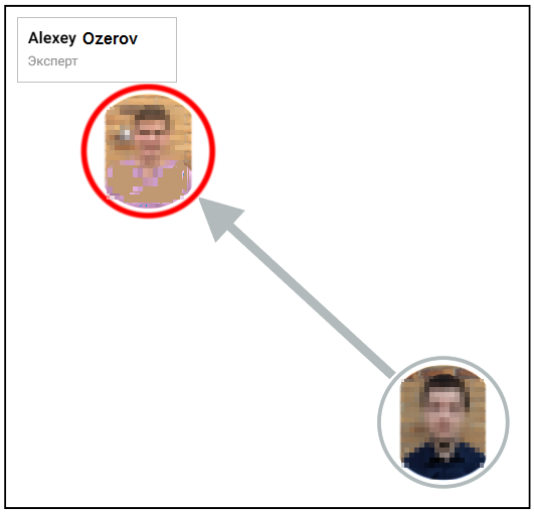


4.4.1 Общие сведения о графе

Граф связей в Досье сотрудника строится на основании событий, участником (отправителем/получателем) которых является сотрудник. Сотрудники компании или ресурсы показываются как узлы на графе, а их связи – как ребра.



Рядом с узлом указано его название, которое может содержать имя сотрудника, название ресурса и т.д. Узлы соединены между собой линиями разной толщины и цвета – связями. Узлы зафиксированы на графе и не зависят друг от друга. Если перемещать один узел на графе, то остальные узлы останутся на своих местах.



Цвет узла устанавливается с помощью дополнительного фильтра и определяется:

- максимальным уровнем нарушения среди всех связей узла, если выбрано "Уровень нарушения";
- принадлежностью разных персон к одному отделу в компании, если выбрано "Отдел";
- должностью, занимаемой персоной в компании, если выбрано "Должность".

Узлы соединены связями. Между двумя узлами всегда показывается только одна связь.

Параметр связи	Описание
Стрелка на линии связи	Показывает направление потока данных от узлов. Может быть: • направлена в одну сторону, если поток данных в одном направлении; • без указания направления, если был двусторонний обмен данными; • замкнутой петлей.
Толщина линии связи	Зависит от количества событий в связи: чем больше событий, тем толще линия связи
Цвет линии связи	Определяется максимальным уровнем нарушения в событиях связи. Цвета для связей определяются следующим образом: • Красный – высокий уровень; • Оранжевый – средний уровень; • Желтый – низкий уровень; • Серый – отсутствует.

При наведении курсора на линию связи можно узнать, сколько событий с разбивкой по уровням нарушений было зафиксировано Traffic Monitor:



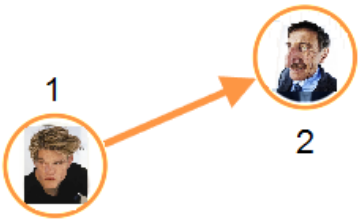
Типы событий отображаются на Графе связей в виде иконок:

Иконка	Описание
	Веб-сообщение
	Веб-почта
	Рабочая почта
	Ввод с клавиатуры, Буфер обмена
	Терминальная сессия
	Внешние устройства

	Принтеры
	Облачные хранилища
	FTP, Корпоративные сетевые ресурсы
	Мессенджеры

4.4.2 Принципы построения графа

В таблицы представлена схема построения Графа связей между сотрудниками компании от простого сценария (два сотрудника) к сложному (большое количество узлов и связей).

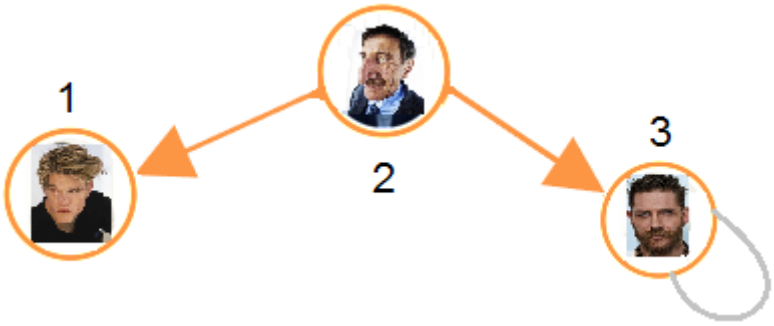
Действия сотрудников	Граф связей и описание
1. Сотрудник-1 направил Сотруднику-2 письмо с вложениями: 1.dwg, 2.jpeg. 2. Traffic Monitor зафиксировал для этого события нарушение политики "Отправка чертежей". Нарушению присвоен средний уровень.	 На графе отображены два узла, а также связь между ними. При наведении курсора на узел можно узнать фамилию и имя сотрудника. Внутри узлов показаны иконки сотрудников, согласно тому, как они идентифицированы в ТМ. Оранжевая линия связи между Сотрудник-1 и Сотрудник-2 обозначает, что уровень нарушения в связи – "Средний". Эта связь включает в себя пока только одно событие со средним уровнем нарушения. Узлы Сотрудник-1 и Сотрудник-2 также оранжевого цвета, так как максимальный уровень нарушения среди всех узлов на графе (в данном случае двух) – "Средний".

1. Сотрудник-2 переслал в Skype ответ Сотруднику-1: пустой бланк договора с печатью компании и два PDF-документа. Сотрудник-2 при отправке поставил в копию Сотрудника-3.
2. Traffic Monitor обнаружил в этом событии нарушение политики «Отправка юридической информации», а также отправку ОЗ «Договор с реквизитами», ОЗ «Соглашение с партнерами». Нарушению присвоен средний уровень.

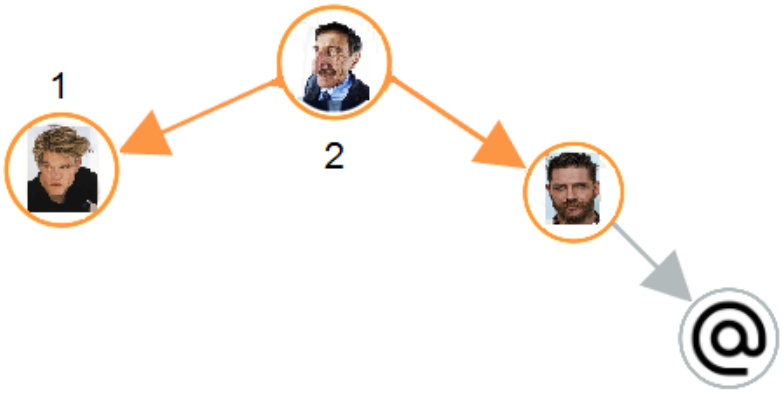


Добавился новый узел Сотрудник-3 и связь между ним и Сотрудником-2. Все связи и узлы на графе по-прежнему обозначаются оранжевым цветом, так как максимальный уровень нарушения в связях, с учетом добавившейся связи, не поменялся.

1. Сотрудник-3 оправляет себе с рабочей почты на домашнюю почту файл выгрузки из CRM.
2. Traffic Monitor зафиксировал нарушение политики «Отправка клиентской информации». Нарушению присвоен низкий уровень.

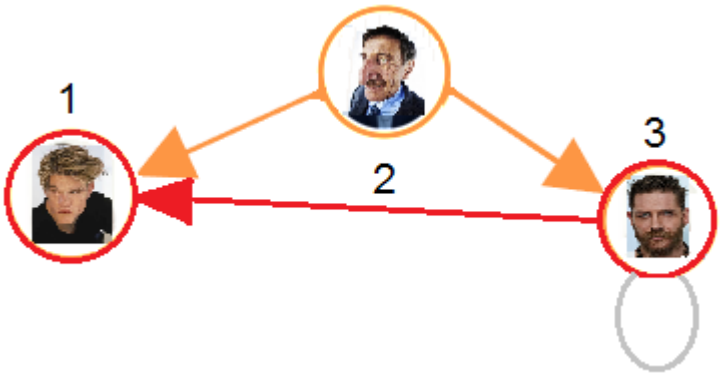


Если домашняя почта сотрудника идентифицирована в TM, то у Сотрудника-3 появляется связь – замыкающаяся петля. Петля (связь) отображается серым цветом, а узел Сотрудник-3 – оранжевым, так как за выбранный период у него есть связи средним уровнем нарушения (связь с Сотрудником-2).



Если его домашняя почта не идентифицирована в TM, то появляется новый узел с иконкой «Неидентифицированный контакт».

1. Сотрудник-3 отправил Сотруднику-1 письмо с вложением «база данных.xml».
2. Traffic Monitor обнаружил в этом событии нарушение политики «Отправка баз данных». Нарушению присвоен высокий уровень.

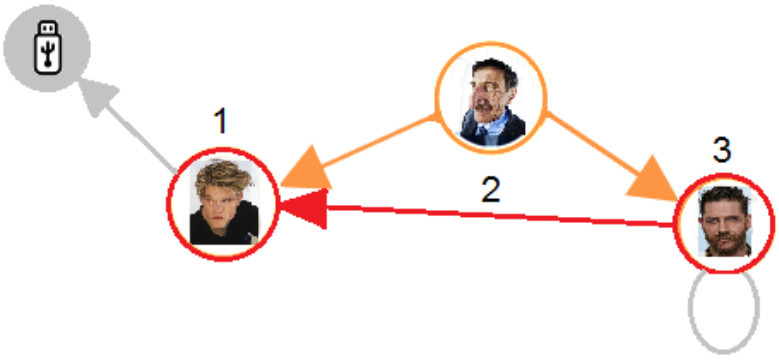


Узлы Сотрудник-3, Сотрудник-1 и их связи теперь отображаются красным цветом.
Если сейчас отфильтровать граф по уровню нарушения «Только средний», то на графе:

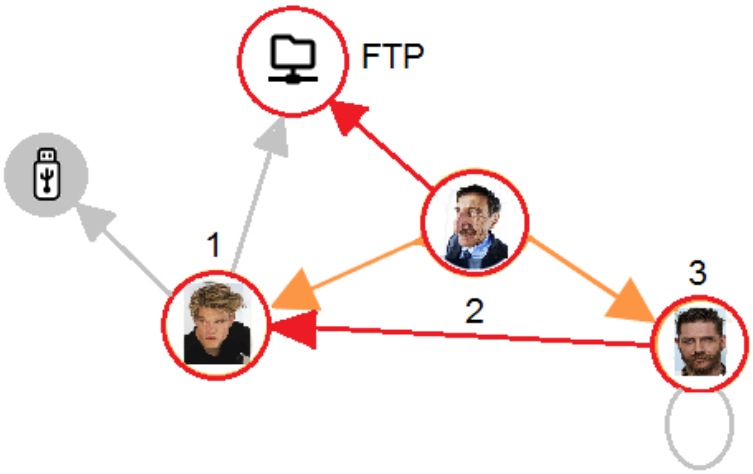
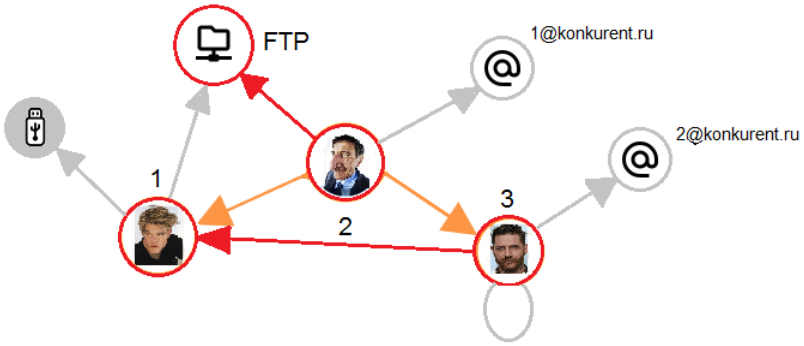
- останутся только оранжевые связи;
- замыкающаяся петля у Сотрудника-3 не отобразится;
- контуры узлов Сотрудник-3 и Сотрудник-1 останутся красными, так как у них за выбранный период есть связь с высоким уровнем нарушения.



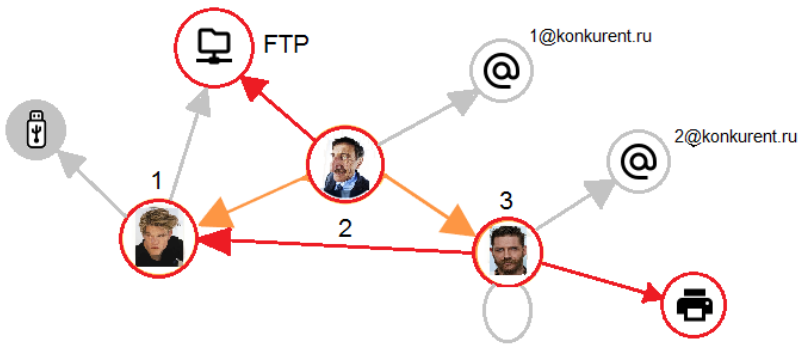
1. Сотрудник-1 копирует текстовой файл на внешнее устройство.
2. Traffic Monitor не обнаружил нарушения в этом событии



На графе у узла Сотрудник-1 появляется частный узел - "Внешнее устройство". Так как нарушения не обнаружено, связь показана серым цветом. Если Сотрудник-1 скопирует информацию на другое внешнее устройство, то новый узел на граф не добавится - у сотрудника всегда показывается только один частный узел "Внешнее устройство".

1. Сотрудник-1 копирует файл на FTP-сервер. 2. Сотрудник-2 копирует файл на FTP-сервер. 3. Traffic Monitor обнаружил у Сотрудника-2 нарушение высокого уровня.	 На Графе показывается Общий узел "FTP" и его связи с Сотрудником-1 и Сотрудником-2. Размер узла увеличивается по мере того, как на него копируют файлы сотрудники. Узел Сотрудника-2 и его связь с FTP становятся красного цвета. Сам узел "FTP" будет добавлен в Единый фильтр по типам события.
1. Сотрудник-1 написал письмо конкурентной организации на адрес 1@konkurent.ru. 2. Сотрудник-2 написал письмо конкурентной организации на адрес 2@konkurent.ru.	 На Графе показаны связи узлов Сотрудник-1 и 1@konkurent.ru, Сотрудник-2 и 2@konkurent.ru. Иконки узлов 1@konkurent.ru и 2@konkurent.ru показывают, что это "Неидентифицированные контакты".

1. Сотрудник-3 распечатывает файл с копией паспорта РФ.
2. Traffic Monitor в этом событии обнаружил нарушение политики «Печать персональных данных клиентов». Нарушению присвоен высокий уровень нарушения.

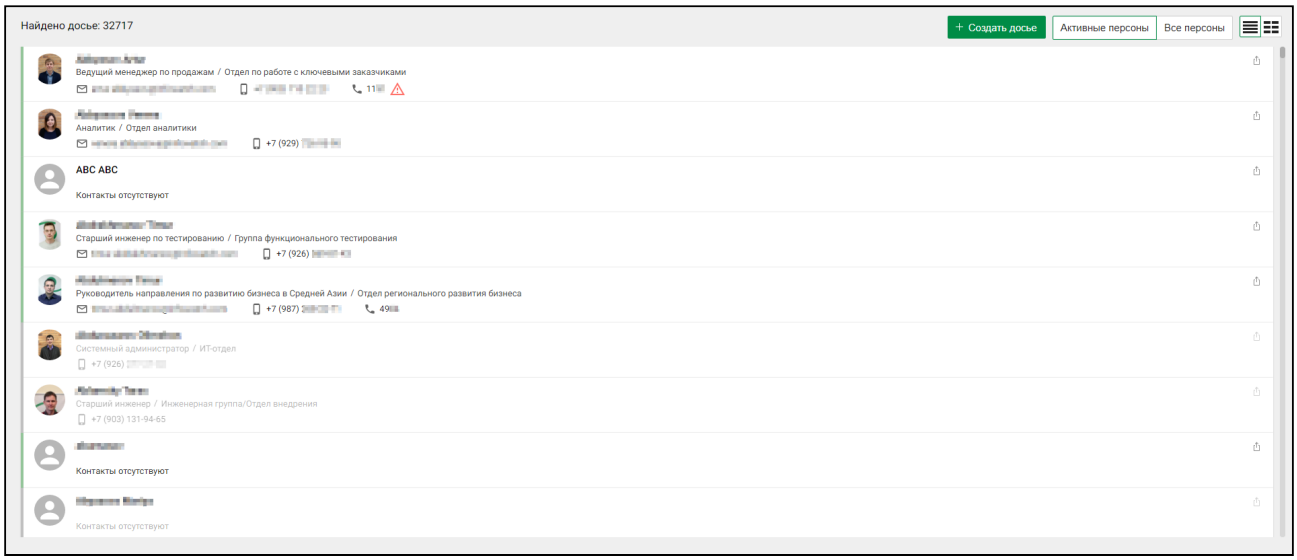


На графе у Сотрудника-3 проявляется частный узел "Принтер". Узлы Сотрудник-3 и Принтер отображаются красным цветом. Если Сотрудник-3 распечатает документ на другом принтере, то новый узел «Принтер» на граф связей не добавится – по мере увеличения событий печати связь «Принтер-Сотрудник-3» будет становиться толще.
У сотрудника всегда показывается только один частный узел "Принтер".

4.5 Раздел "Досье"

О разделе:

Раздел содержит справочник персон, загруженный в Систему при синхронизации с источниками: Active Directory и Traffic Monitor, а также персон, добавленных вручную.



В таблице персон отображаются только персоны, удовлетворяющие условиям единого фильтра. Для настройки отображения досье с персонами используйте панель инструментов в правой части рабочей области:

- **Активные персоны** - отобразить досье только сотрудников с активной учетной записью в ActiveDirectory;
- **Все персоны** - отобразить досье всех персон, в том числе когда-либо работавших в компании;

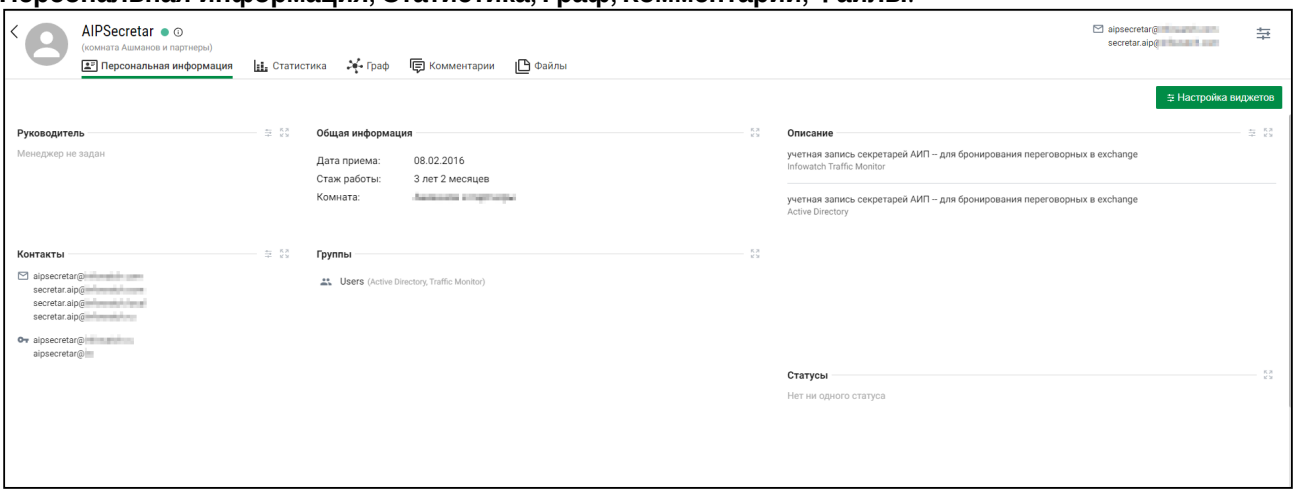
-  - отображать в виде списка;
-  - отображать в виде таблицы;

Целевые действия пользователя:

- Просмотр досье персоны
- Создание, редактирование и удаление досье
- Объединение досье
- Добавление контактов персоны
- Изменение руководителя персоны
- Граф связей персоны
- Добавление комментария в досье
- Добавление файла в досье
- Настройка виджетов досье

4.5.1 Просмотр досье персоны

Досье – инструмент сбора и анализа информации по конкретной персоне. Досье позволяет организовать совместную работу нескольких Офицеров безопасности путем обмена информацией в комментариях. Чтобы просмотреть досье персоны, щелкните левой кнопкой мыши по выбранной персоне в разделах **Досье** или **События**. Досье персоны содержит следующие вкладки: **Персональная информация**, **Статистика**, **Граф**, **Комментарии**, **Файлы**.



Страница досье персоны содержит личную информацию о сотруднике:

- ФИО сотрудника;
- Должность;
- Отдел;
- Контакты – личные или рабочие контакты персоны, включая адрес электронной почты, номер телефона, логин Skype, ICQ или адрес сайта в Интернете.

Для персон, данные которых импортированы из Active Directory, отображается цветовой индикатор в левом верхнем углу фотографии профиля:

-  – для активных сотрудников, в том числе с истекшим сроком действия учетной записи в ActiveDirectory;
-  – для сотрудников, отключенных в AD.

Для изменения указанных атрибутов, а также атрибутов *Имя, Фамилия* и редактирования фотографии персоны используется кнопка  в правой части рабочей области (подробнее см. "Редактирование персоны").

На вкладке **Персональная информация** находятся Виджеты досье, специфичные для данной персоны. Также можно добавить общие Виджеты статистики.

На вкладке **Статистика** вы можете просмотреть виджеты статистики, относящиеся к данной персоне (см. "Виджеты статистики").

На вкладке **Граф** изображен Граф связей данной персоны (подробнее см. Граф связей персоны).

На вкладках **Комментарии** и **Файлы** вы можете оставить текстовые пометки и приложить файлы. Эта информация будет добавлена в досье персоны.

Для возврата к списку персон нажмите  в верхнем левом углу рабочей области.

4.5.2 Виджеты досье

Виджеты досье позволяют Офицеру безопасности просмотреть все хранящиеся в Системе данные по персоне. В таблице описаны виджеты, специфичные для раздела **Досье**. Также на вкладку **Статистика** в разделе **Досье** добавлять общие виджеты статистики (см. "Виджеты статистики").

Название виджета	Описание
Файлы	Показывает привязанные к персоне файлы и позволяет загружать новые файлы в досье
Руководитель	Отображает список руководителей персоны, а также позволяет задать руководителя вручную
Контакты	Позволяет управлять контактами персоны, а также отображает контакты, подгруженные из подключенных источников
Общая информация	Отображает состояние персоны в различных источниках
Описание	Отображает описания персоны, загруженные из источников, а также позволяет добавить пользовательское описание
Статусы	Отображает список статусов, присвоенных персоне в Traffic Monitor
Комментарии	Позволяет добавлять комментарии к досье
Группы	Отображает список групп из ActiveDirectory и Traffic Monitor, в которые входит персона.

Информацию с виджета можно сохранить в досье персоны. Для этого:

1. Нажмите  на интересующем виджете.
2. В открывшемся окне оставьте комментарий или прикрепите файл.

3. Нажмите **Сохранить**. Вся указанная информация теперь будет доступна на вкладке **Комментарии**.

4.5.3 Добавление контактов персоны

При синхронизации с Traffic Monitor или ActiveDirectoryустановятся доступны контакты персон: рабочие и личные номера телефона, адреса электронной почты, аккаунты в социальных сетях и др. Вы можете добавить дополнительные контакты вручную. Для этого:

1. Перейдите в досье персоны.
2. На виджете **Контакты** нажмите .
3. В открывшемся окне указаны все контакты и способы связи персоны. Нажмите **Добавить контакт**.
4. Укажите тип контакта (например, личный номер телефона) и введите его значение. Можно добавить несколько позиций или оставить комментарий к контакту.
5. Нажмите **Сохранить**. Новые контакты станут доступны в досье. Если вы оставили комментарий к контакту, напротив него будет стоять значок . Чтобы прочитать комментарий, щелкните по значку левой клавишей мыши.

4.5.4 Объединение досье

Для удобства Офицера безопасности можно объединить два или несколько досье в одно. При этом новое досье будет содержать всю информацию из прошлых досье. Для этого:

- Откройте первое досье, которое нужно объединить с другими.
- Нажмите  и выберите **Объединить досье с...**
- Выберите второе досье для объединения из списка. Если требуется, укажите несколько досье.
- Нажмите **Объединить**.

4.5.5 Создание, редактирование и удаление досье

Чтобы создать досье на новую персону, а также дополнительное досье на существующую в Системе персону:

1. Перейдите в раздел **Досье**.
2. Нажмите **+Создать досье**.
3. Заполните личные данные:

Графа	Описание
Фамилия	Фамилия персоны
Имя	Имя Персоны
Отчество	Отчество персоны (если есть)
Должность	Должность в организации
Отдел	Отдел, где работает персона

Описание	Дополнительное описание
Фотография	Прикрепите фотографию персоны

4. Добавьте контактные данные персоны. Это могут быть личный или рабочий номер телефона, адрес e-mail, аккаунт в социальных сетях.
5. Нажмите **Создать досье**. Новое досье будет доступно в списке всех досье сотрудников.

Чтобы внести изменения в досье:

1. Откройте нужное досье.
2. Нажмите  и выберите **Редактировать**.
3. Внесите изменения и нажмите **Сохранить**.

Чтобы удалить досье:

1. Откройте нужное досье
2. Нажмите  и выберите **Удалить**.
3. Нажмите **ОК**. Досье будет удалено без возможности восстановления.

4.5.6 Изменение руководителя персоны

На вкладке **Персональная информация** персоны на виджете **Руководитель** указан начальник персоны. Данная информация получается при синхронизации из карточки персоны в источнике: ActiveDirectory или Traffic Monitor.

Офицер безопасности может поменять руководителя персоны вручную. Для этого:

1. Нажмите .
2. В открывшемся окне **Изменение руководителя** в поле *Добавлено вручную* введите имя нового руководителя из числа персон, зарегистрированных в Системе. Можно ввести несколько имен.
3. Нажмите **Сохранить**. Теперь на виджете **Руководитель** отображаются указанные руководители.

Можно поочередно просмотреть всю цепочку руководителей в организации. Щелкните левой клавишей мыши на имени начальника персоны, и вы перейдете на страницу досье его руководителя.

4.5.7 Граф связей персоны

На вкладке **Граф** досье персоны отображается Граф связей, построенный на основании событий по данной персоне. Подробнее см. Раздел "Граф связей".

Офицер безопасности может сохранить граф связей персоны. Это может потребоваться для формирования отчета по сотруднику. Для этого:

1. Перейдите на вкладку **Граф** в досье персоны.
2. Если требуется, отредактируйте представленный Граф связей персоны.
3. Нажмите .
4. В открывшемся окне обязательно оставьте комментарий.
5. Если требуется, прикрепите дополнительные файлы. Для этого:
   a. Нажмите .

b. Выберите файлы или перетащите их в специальную область с помощью мыши.

6. Нажмите **Сохранить**. Граф связей персоны будет сохранен в виде отдельного файла. Ознакомиться с ним можно на вкладке **Персональная информация** на виджете **Комментарии**.

4.5.8 Комментирование в досье персоны

На вкладке **Комментарии** в досье персоны Офицер безопасности оставляет свои заметки о персоне, такие как файлы с данными в различных форматах или текст. Все эти данные могут потребоваться в будущем для расследования инцидентов или формирования отчетов.

Вкладка содержит список комментариев, которые можно отсортировать с помощью специального ключа. Для этого выберите **Сначала новые комментарии** или **Сначала старые комментарии**.

Чтобы внести новый комментарий:

1. Нажмите **Добавить комментарий**.
2. Внесите сведения. Если требуется, добавьте к комментарию вложение.
3. Нажмите **Сохранить**. Новый комментарий отобразится в списке, а также на виджете **Комментарии** вкладки **Персональная информация**.

Чтобы внести изменения в комментарий:

1. Нажмите  напротив файла.
2. Внесите изменения.
3. Нажмите **Сохранить**.

4.5.9 Добавление файла в досье

На вкладке **Файлы** в досье персоны Офицер безопасности может прикрепить файлы файлы с данными в различных форматах или текст. Все эти данные могут потребоваться в будущем для расследования инцидентов или формирования отчетов.

Вкладка содержит список файлов, которые можно отсортировать с помощью специального ключа. Для этого выберите **Первые добавленные** или **Последние добавленные**.

Чтобы загрузить новый файл в досье:

1. Нажмите **Добавить файл**.
2. Прикрепите файл. Файл будет добавлен в список вложений.

Любой Офицер безопасности может ознакомиться с ранее загруженными в Систему файлами. Для этого:

1. Нажмите  напротив файла.
2. Выберите **Скачать** либо откройте файл на просмотр, щелкнув левой клавишей мыши по его названию.

Если дальнейшее нахождение файла в досье нецелесообразно, удалите его:

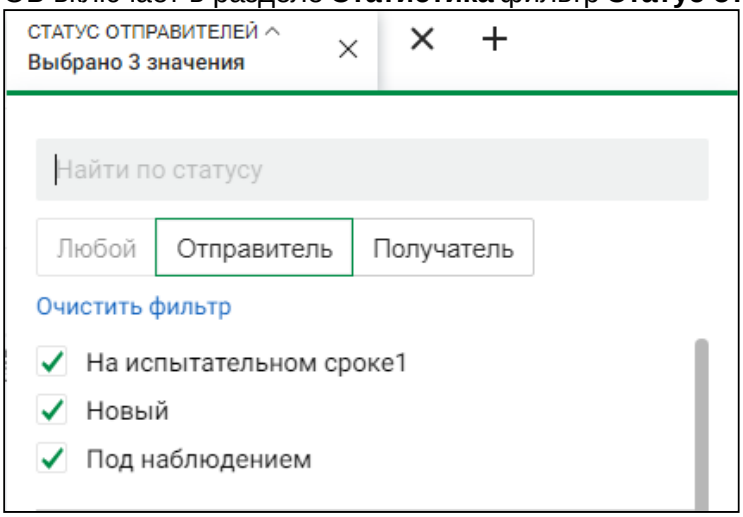
1. Нажмите  напротив файла.
2. Выберите **Удалить**.
3. В открывшемся окне нажмите **ОК**.

5 Примеры сценариев работы Офицера безопасности

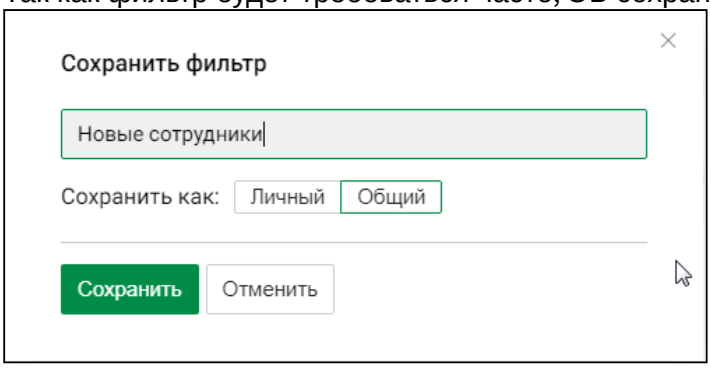
5.1 Ежедневный анализ коммуникаций выбранных сотрудников

ОБ необходимо ежедневно следить за действиями новых сотрудников компании. Для этого:

1. ОБ включает в разделе **Статистика** фильтр **Статус отправителей**.



2. Так как фильтр будет требоваться часто, ОБ сохраняет его.



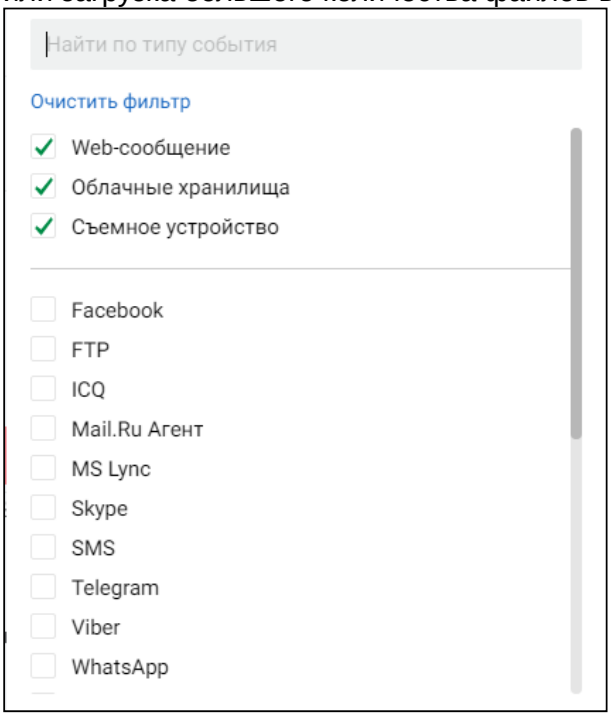
3. Сохраненный фильтр позволит быстро переключиться к нужной выборке событий и упростит регулярные операции офицеров безопасности.

5.2 Анализ активности сотрудника

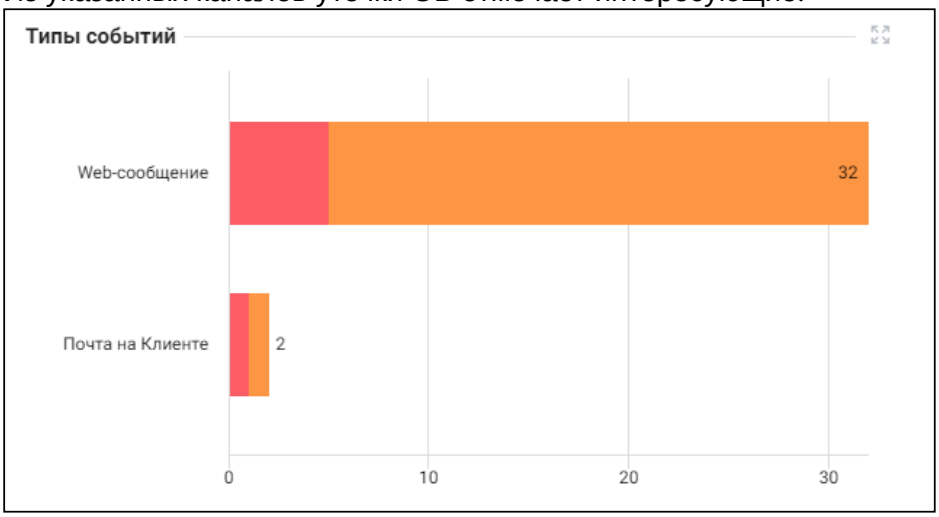
В компании есть сотрудник по подозрением. ОБ необходимо собрать максимум информации о нем. Для этого:

1. ОБ открывает досье сотрудника и анализирует его действия на предмет подозрительной активности: передача конфиденциальных данных на внешние почтовые адреса или сохранение их на съемные носители, контакты с конкурентами

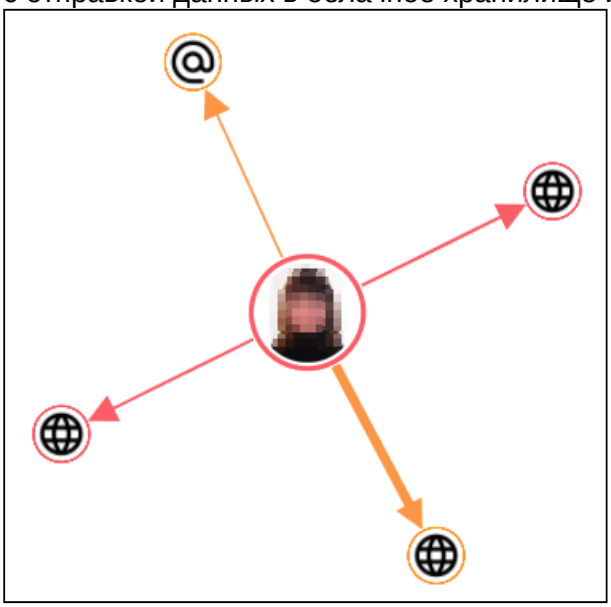
или загрузка большого количества файлов в облачные хранилища.



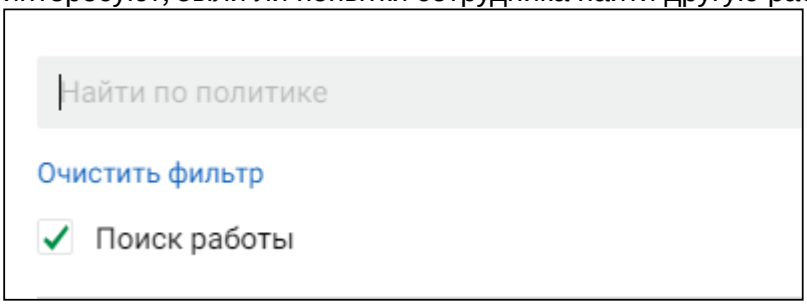
2. Из указанных каналов утечки ОБ отмечает интересующие.



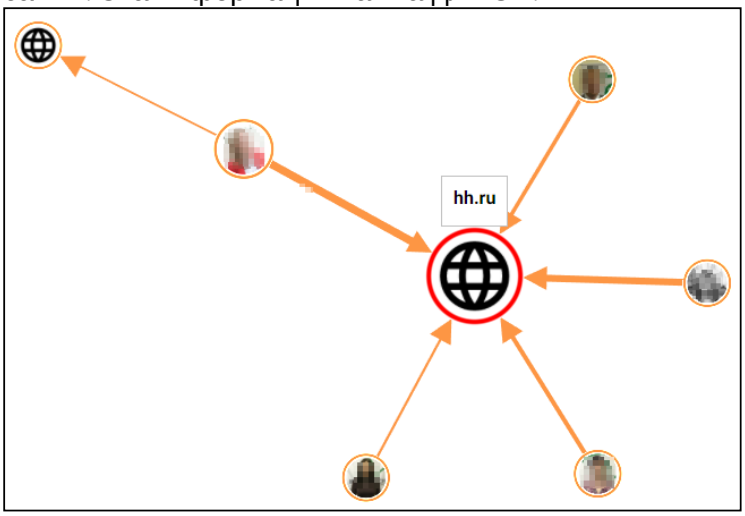
3. ОБ обнаружил, что данные события с высоким и среднем уровнем нарушения связаны с отправкой данных в облачное хранилище и на внешний email-адрес.



4. Дополнительно ОБ решает проверить сотрудника на лояльность компании. Его интересуют, были ли попытки сотрудника найти другую работу.



5. По политике ТМ "Поиск работы" ОБ находит несколько персон, посещавших подобные сайты. Эта информация важна для ОБ.

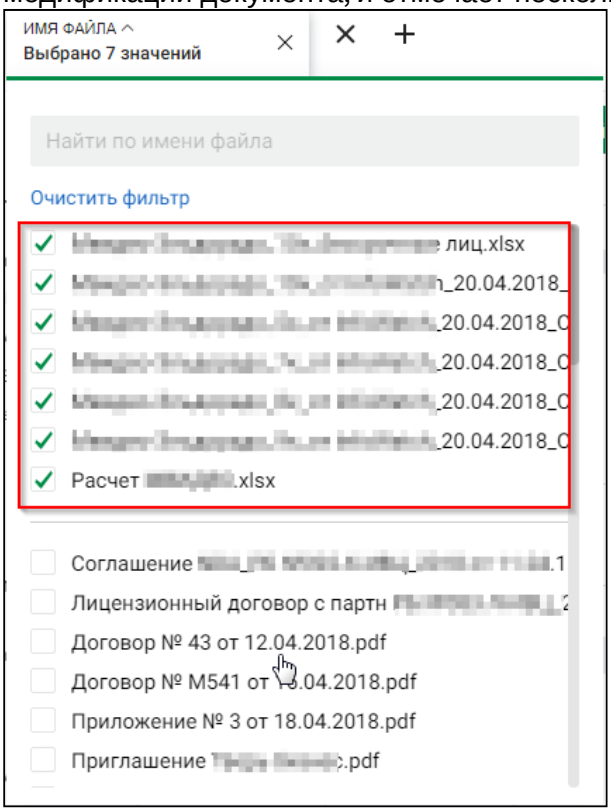


6. ОБ переходит в раздел **Досье** на вкладку **Граф** и сохраняет его, прикладывая к досье ( ).

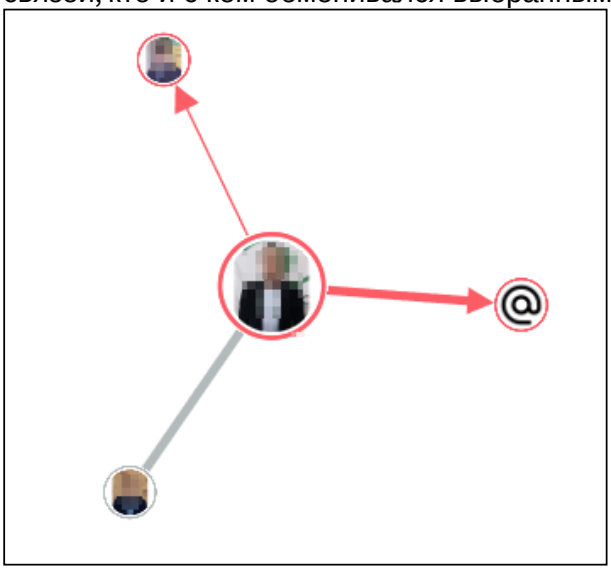
5.3 Выявление канала утечки

На публичном ресурсе в текущем месяце был обнаружен конфиденциальный документ. ОБ инициирует расследование, чтобы определить сотрудника – организатора утечки. Для этого:

1. Проанализировав содержание документа, ОБ вводит в фильтре **Имя файла** примерное название документа. Он видит все похожие файлы, которые могут означать различные модификации документа, и отмечает несколько файлов.



2. ОБ устанавливает в фильтре временной интервал, а затем анализирует на Графе связей, кто и с кем обменивался выбранными файлами.



3. Установив, что была утечка на внешний почтовый адрес, ОБ переходит в раздел **События**, а затем приступает к детальному изучению события в источнике.

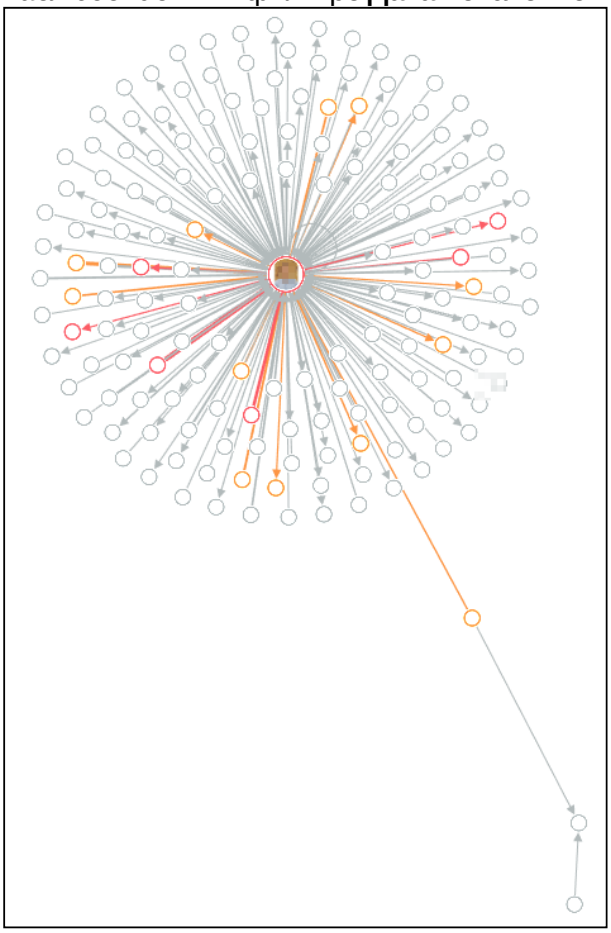
5.4 Анализ взаимодействий выбранного сотрудника

В обязанности Офицера безопасности входит постоянный контроль над сотрудниками, которые:

- недавно устроились на работу в организацию и находятся на испытательном сроке;
- ранее попадали под подозрение;
- в скором времени покинут компанию.

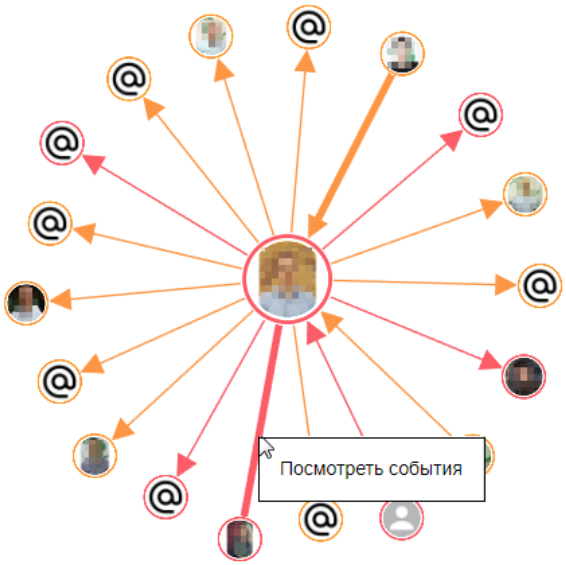
Для этого:

1. ОБ заходит в раздел **Граф связей**, выбирает в фильтре **Статус** значение *Под наблюдением* и в фильтре **Дата** – значение *Последние 7 дней.*

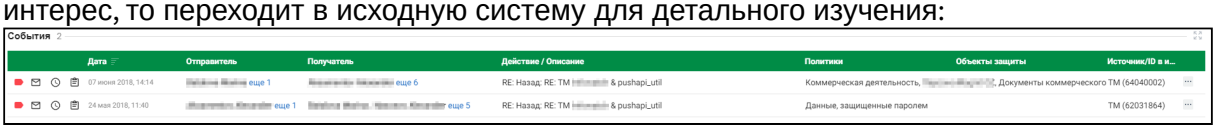


2. ОБ дополнительно применяет фильтр **Уровень нарушения** по значениям *Высокий, Низкий* и *Средний.* Граф перестраивается согласно фильтру. ОБ находит наиболее

серьезные нарушения и инициирует просмотр событий.



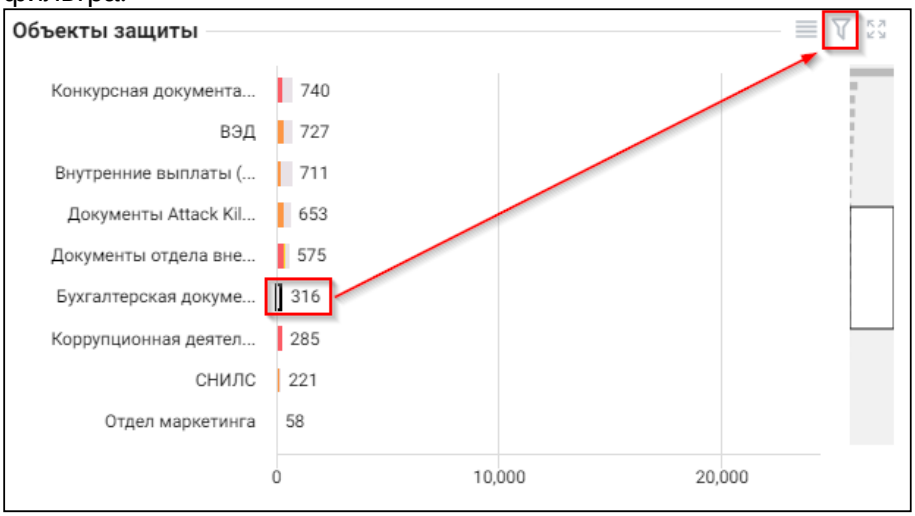
3. В разделе **События** ОБ просматривает описание событий и, если они вызывают у него интерес, то переходит в исходную систему для детального изучения:



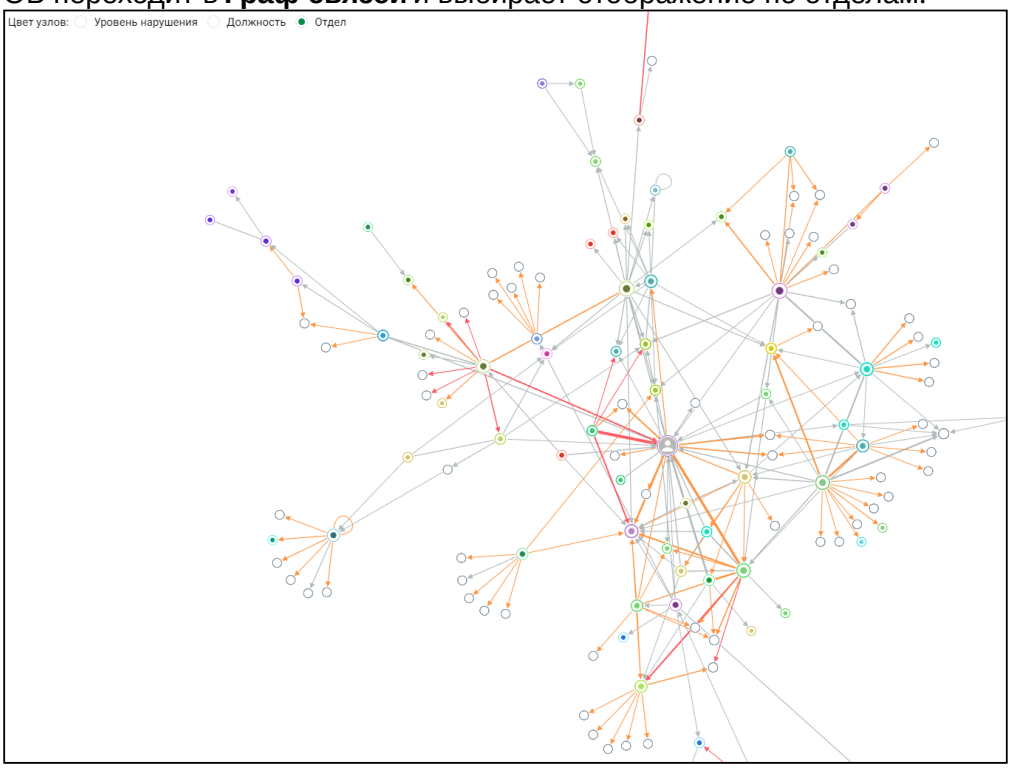
5.5 Анализ бизнес-процессов внутри компании

Офицер безопасности хочет проанализировать, как выбранный тип информации (например, Бухгалтерская документация) распространяется внутри компании, для того чтобы правильно настроить политики безопасности:

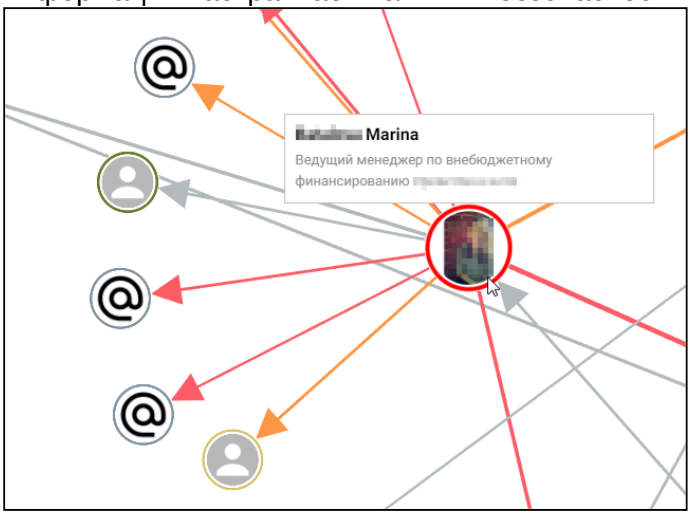
1. ОБ выбирает в объектах защиты **Бухгалтерская информация** и применяет в качестве фильтра.



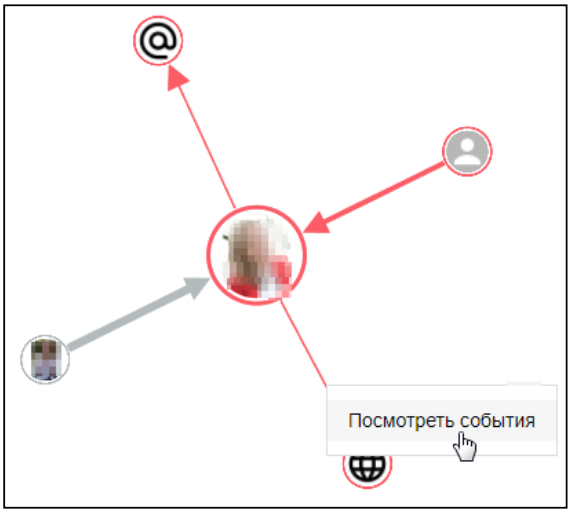
2. ОБ переходит в **Граф связей** и выбирает отображение по отделам.



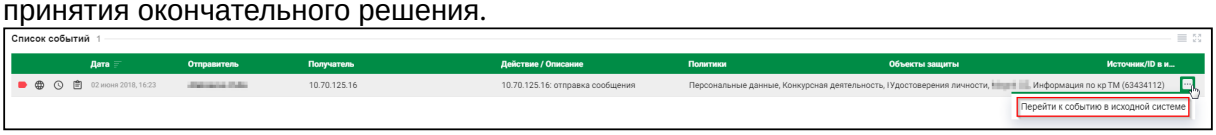
3. ОБ анализирует основных участников взаимодействия и на основании этой информации настраивает политики безопасности в TrafficMonitor.



4. Офицер безопасности анализирует получателей информации, не встроенных в общее взаимодействие, для того чтобы выявить нелегитимную пересылку информации. Для этого он просматривает все элементы графа, которые связаны только с одним отправителем и имеют только входящие события. В результате он выявляет подозрительную пересылку бухгалтерской документации на внешний сервер. ОБ выбирает заинтересовавшее его ребро графа и переходит к просмотру событий.



5. На вкладке **События** ОБ видит в теме письма, что на внешний сервер было переслано сообщение. Поэтому он переходит в TrafficMonitor для просмотра сообщений и принятия окончательного решения.

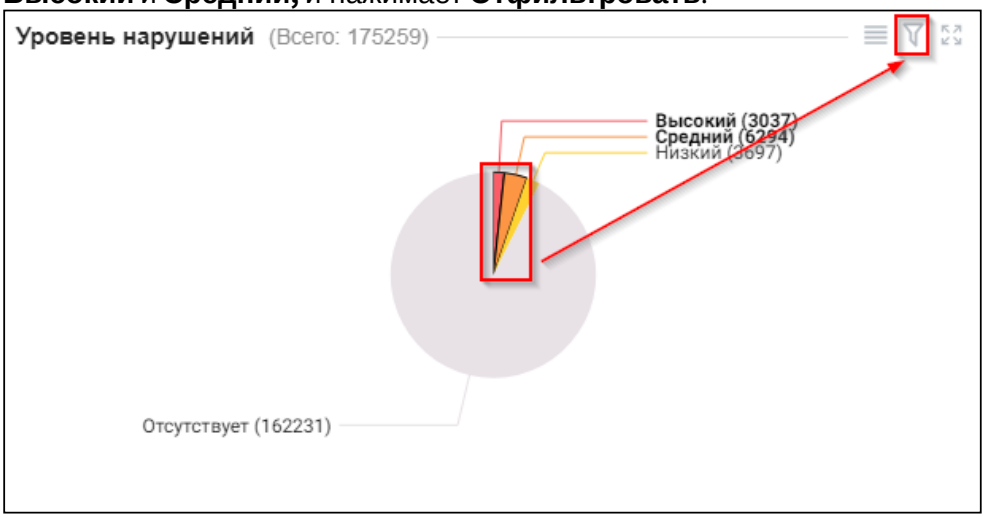


5.6 Быстрый поиск аномалий в поведении сотрудников

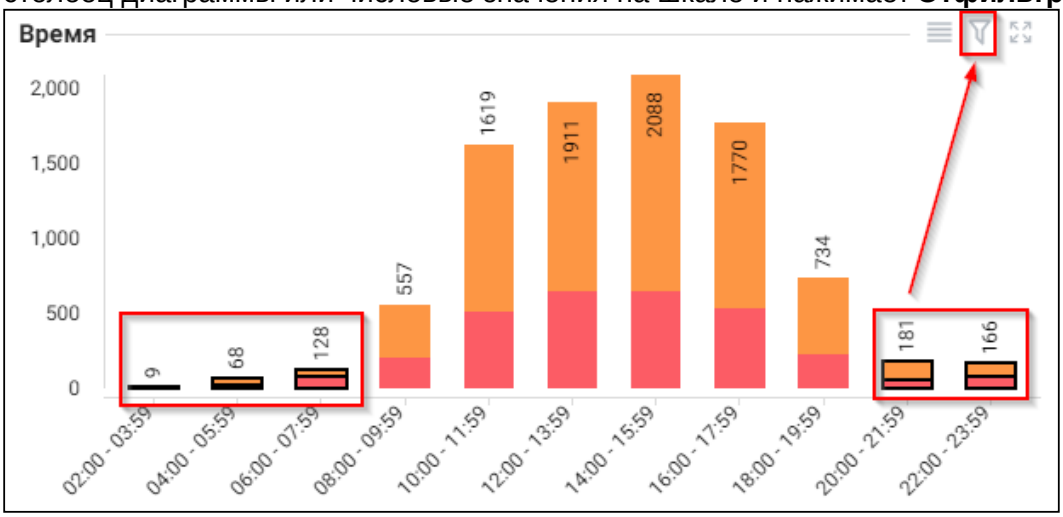
Существуют ситуации, когда Traffic Monitor фиксирует события, связанные с нетипичным поведением сотрудников.

Чтобы просмотреть такие случаи и отследить аномалии:

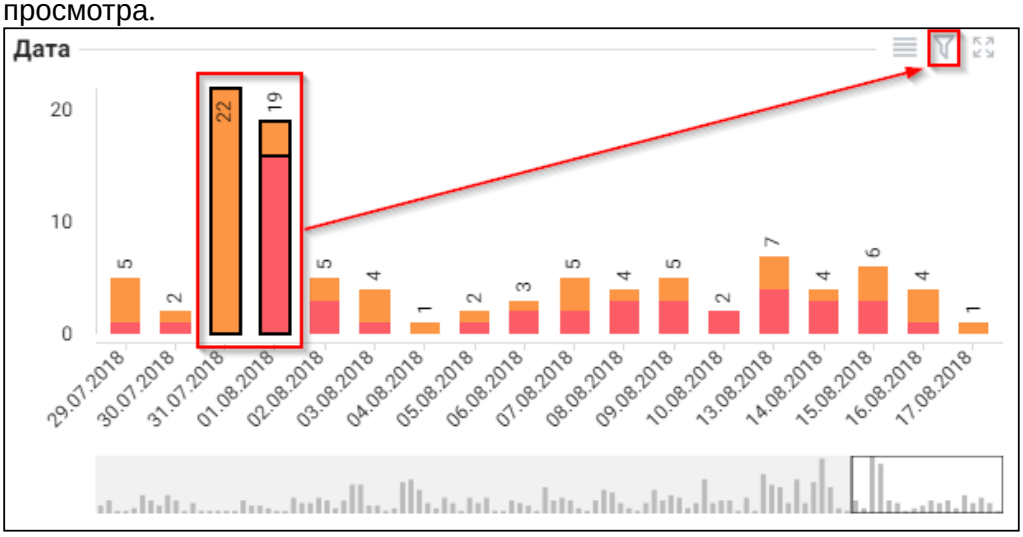
1. ОБ заходит в раздел **Статистика** и на виджете **Уровень нарушений** выбирает **Высокий** и **Средний,** и нажимает **Отфильтровать**.



2. ОБ заходит в раздел **Статистика,** на виджете статистики **Время** выбирает нужный столбец диаграммы или числовые значения на шкале и нажимает **Отфильтровать**.



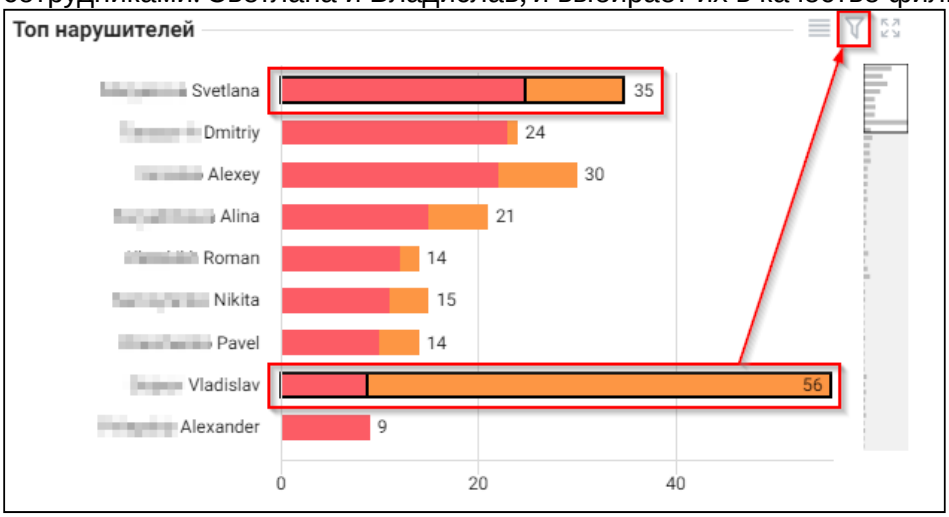
3. Статистика перестраивается, согласно новому фильтру. Офицер безопасности видит резкое увеличение количества событий в определенные дни и выбирает их для просмотра.



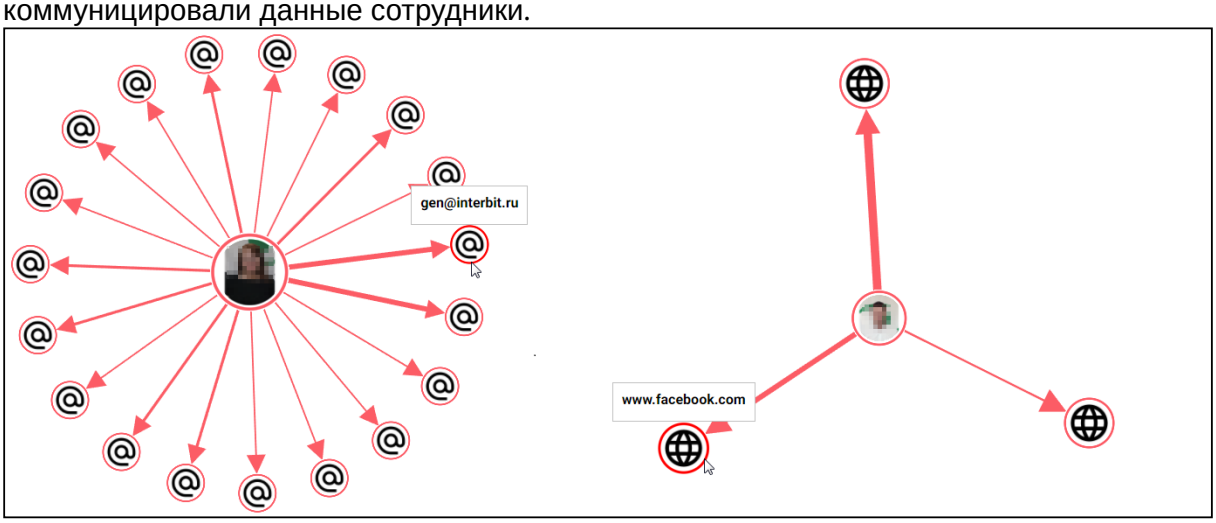
4. На виджете **Политики** ОБ видит, что в это время передавалась информация с грифами секретности и персональные данные.



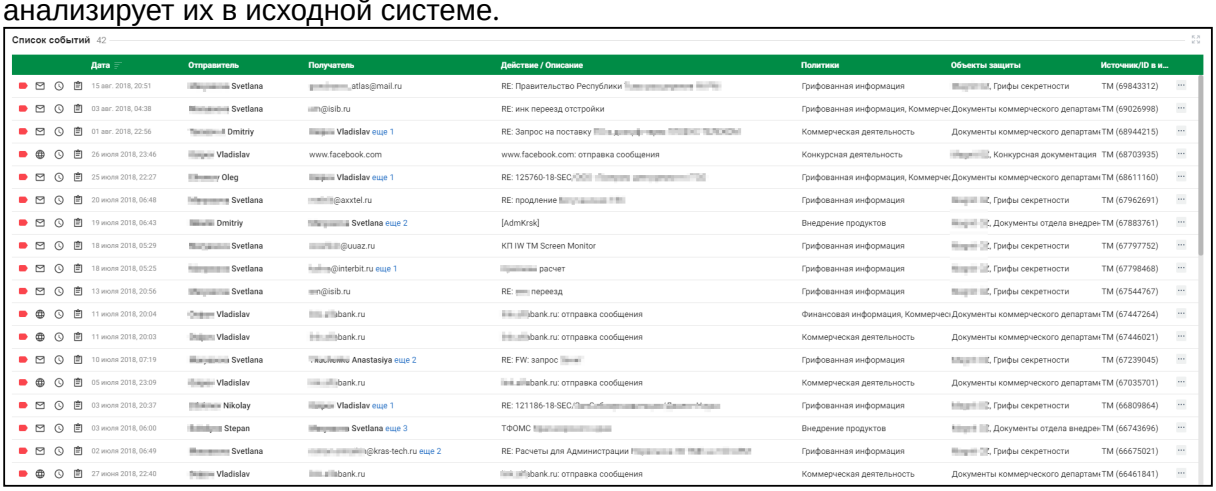
5. На виджете **Топ Нарушителей** ОБ видит, что большая часть событий связана с двумя сотрудниками: Светлана и Владислав, и выбирает их в качестве фильтра.



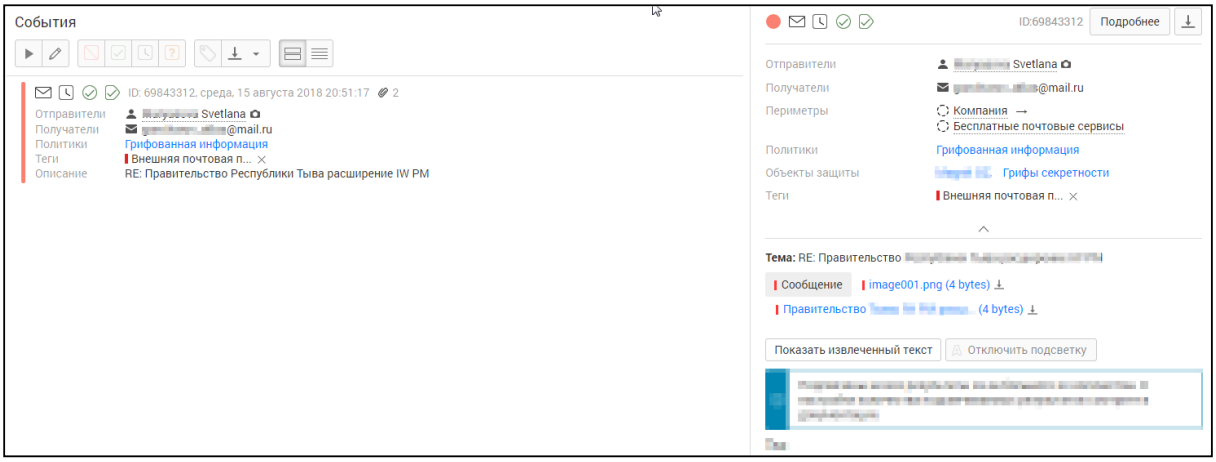
6. Офицер безопасности переходит в раздел **Граф связей** и находит, с кем коммуницировали данные сотрудники.



7. Поскольку отправка грифованной и персональной информации в нерабочее время по указанным адресам выглядит подозрительно, то ОБ переходит в раздел **События** и анализирует их в исходной системе.



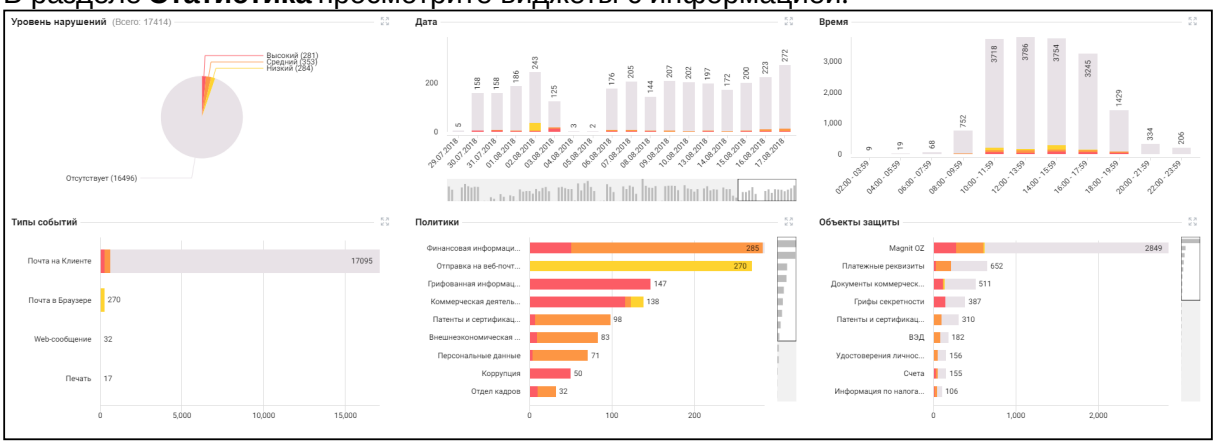
8. Выбранный список событий отображается в стандартном интерфейсе Traffic Monitor, ОБ может проанализировать детали событий и принять по ним решение.



5.7 Сбор информации в досье

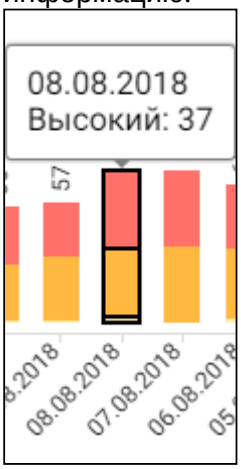
Сбор информации требуется для проведения расследования и составления отчетов по сотрудникам. В досье сотрудника ОБ может сохранять нужные данные.

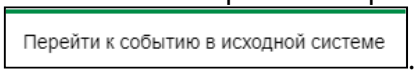
1. В разделе **Статистика** просмотрите виджеты с информацией.



2. Найдите подозрительную информацию или серьезные нарушения на одном из графиков.

3. Выделите ее. Нажмите  чтобы отфильтровать по ней всю статистическую информацию.



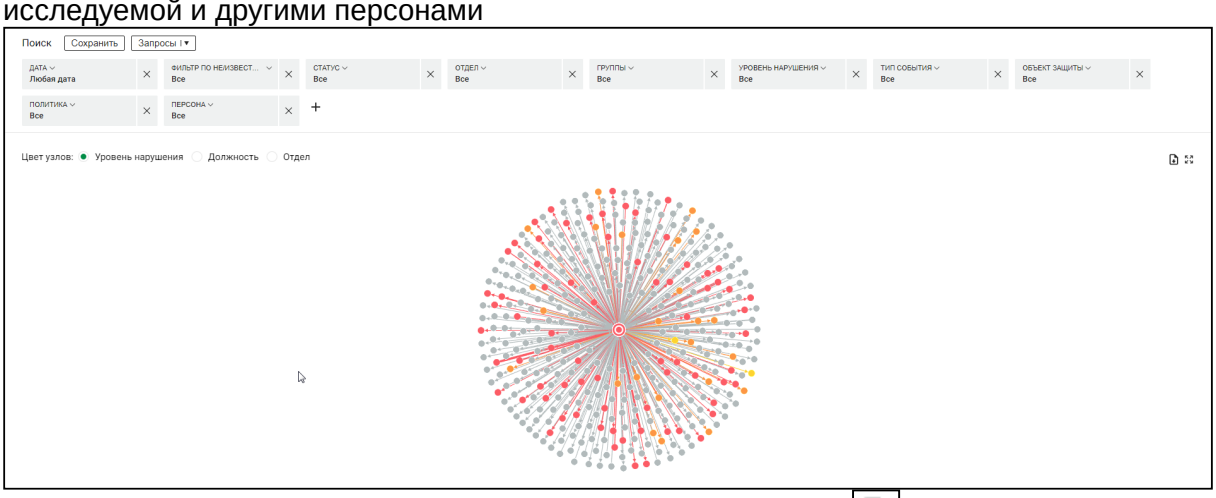
4. После тогда, как Система представит уже отфильтрованные данные, перейдите в раздел **События**.
5. Для детального просмотра события можно перейти в первоисточник, в данном случае Traffic Monitor. Нажмите  и 

. Можно просмотреть сразу все отфильтрованные события, нажав .
6. После самостоятельного анализа события перейдите в досье интересующей вас персоны. Для этого нажмите **Досье**.
7. На странице досье на вкладке **Комментарии** оставьте нужную информацию о сотруднике в текстовом виде или приложите файл. Для этого нажмите **Добавить комментарий**, а затем **Сохранить**.

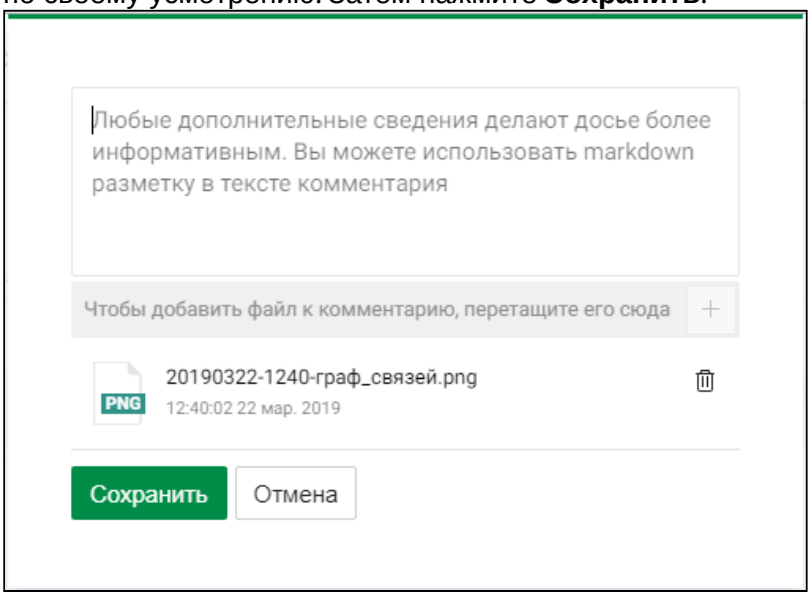


8. Перейдите на вкладку **Статистика**. Чтобы сохранить виджет в досье, нажмите  и заполните данные. Затем нажмите **Сохранить**.

9. Перейдите на вкладку **Граф**, чтобы увидеть информационные потоки между исследуемой и другими персонами



10. Чтобы приложить к досье полученную информацию, нажмите  и заполните данные по своему усмотрению. Затем нажмите **Сохранить**.



11. Чтобы добавить файл к досье, перейдите на вкладку **Файлы**. Нажмите **Добавить файл** и с помощью Проводника прикрепите нужный файл.
12. Система загрузит скриншот в досье персоны.