A KASPERSKY LAB'S COMPANY

INFOWATCH

InfoWatch Traffic Monitor Enterprise 3.5

Методика проведения расследований

INFOWATCH TRAFFIC MONITOR ENTERPRISE 3.5

Методика проведения расследований

© ЗАО “ИнфоВотч”
Тел. +7 (495) 229-00-22 • Факс +7 (495) 229-00-22
http://www.infowatch.com
Дата редакции: март 2011 года

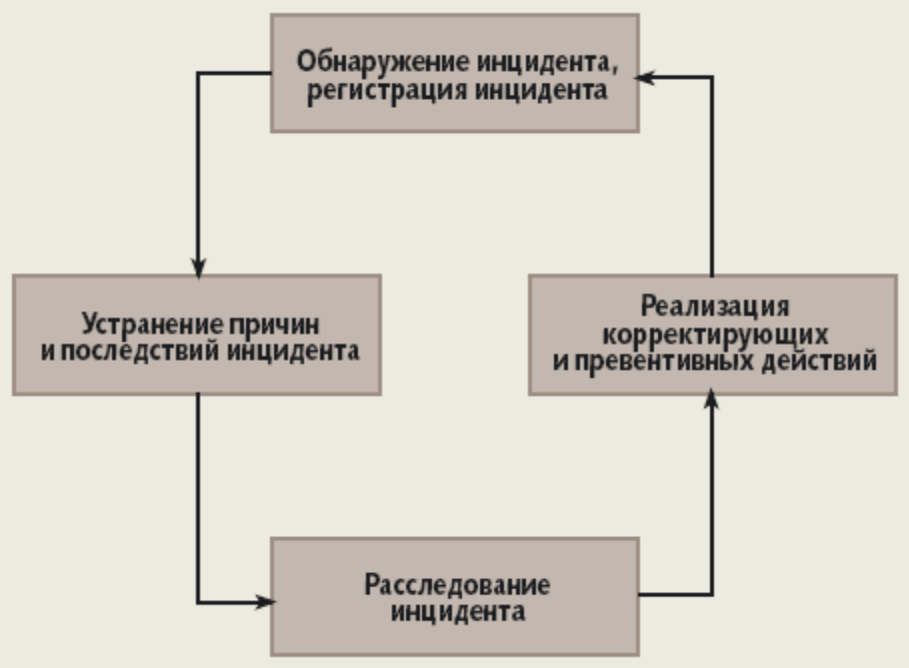
СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Основной задачей Системы InfoWatch Traffic Monitor является контроль[1] исходящего трафика и автоматическое выявление фактов нарушения политики информационной безопасности.

Частота появления и количество нарушений, связанных с информационной безопасностью, — один из наглядных показателей того, правильно ли функционирует система управления безопасностью.

Международный стандарт ISO 27001:2005 обращает особое внимание на необходимость создания процедуры управления инцидентами информационной безопасности. Как правило, такая процедура разрабатывается в рамках общей системы управления информационной безопасностью и описывается классической моделью непрерывного улучшения процессов, получившей название от цикла Шухарта-Деминга — модель PDCA (Plan – Планируй, Do – Выполняй, Check – Проверяй, Act – Действуй).



Стандарт ISO 27001 описывает модель PDCA как основу функционирования всех процессов системы управления информационной безопасностью.

Для того чтобы процедура выполнялась правильно и эффективно, все эти этапы должны непрерывно и последовательно повторяться. Через определенное время необходимо заново пересмотреть перечень событий, называемых инцидентами, внедрить обновленную процедуру, проверить ее функционирование и эффективность. Таким образом, цикл модели PDCA будет непрерывно повторяться, гарантируя ее четкое функционирование и постоянное улучшение.

[1] Контроль осуществляется только над технических каналами утечки, такими как электронная почта, веб, ICQ-сообщения, периферийные устройства, локальные и сетевые принтеры.

ГЛАВА 1. ОБНАРУЖЕНИЕ ИНЦИДЕНТА

В общем случае инцидент информационной безопасности определяется как единичное, нежелательное или неожиданное событие информационной безопасности (или совокупность таких событий), которое может скомпрометировать бизнес-процессы компании или угрожает ее информационной безопасности (ISO/IEC TR 18044:2004).

В терминах Системы Traffic Monitor под инцидентом понимается событие, признанное Системой нарушением, и подтвержденное таковым, офицером безопасности, по факту проведения расследования.

Предполагается, что в процессе внедрения Система была настроена в соответствии с политикой безопасности Компании, что, в частности, означает, что были созданы специализированные БКФ, определены эталонные документы, списки пользователей, зоны ответственности, теги, скрипт.

В скрипте определен перечень событий, являющихся нарушениями политики ИБ, и описана реакция Системы на наличие в трафике таких событий. Следует понимать, что все события, которые не были определены в скрипте как нарушения, будут рассматриваться как штатные (даже если они несут угрозу информационной безопасности).

Обнаружение нарушений политики информационной безопасности выполняется Системой в автоматическом режиме.

Система осуществляет архивирование информации, проходящей через технические каналы утечки. В архиве хранятся копии закачанных в интернет документов и текста, электронных писем, распечатанных документов и файлов, записанных на периферийные устройства.

ГЛАВА 2. УСТРАНЕНИЕ ПОСЛЕДСТВИЙ И ПРИЧИН ИНЦИДЕНТА

Предполагается, что в процессе внедрения политики информационной безопасности была разработана инструкция по устранению причин и последствий инцидента, включающая описание общих действий, которые необходимо предпринять, сроки, в течение которых следует устранить последствия и причины инцидента, а также указание на ответственность за несоблюдение инструкции. Предпринимаемые действия и сроки устранения зависят от специфики работы конкретной Компании.

ГЛАВА 3. РАССЛЕДОВАНИЕ ИНЦИДЕНТА

Расследование инцидента – это процесс, целью которого является сбор доказательной базы, подтверждающей или опровергающей факт нарушения политики информационной безопасности, а также определение виновных в его возникновении.

В общем случае факт передачи информации характеризуется следующими параметрами:

- **КТО** – сотрудник, выполнивший передачу
- **ЧТО** – состав передаваемой информации
- **ГДЕ** – канал передачи
- **КОГДА** – дата передачи
- **ОТКУДА** – откуда была выполнена передача информации (например, рабочая станция сотрудника, и т.д.)
- **КУДА** – получатель

В терминах Системы Traffic Monitor проведение расследования означает:

- в случае если известны условия поиска – поиск в хранилище событий, удовлетворяющих заданному набору условий
- в случае если не известны условия поиска – анализ Событий, отмеченных Системой как нарушения

  и вынесение пользовательского решения о наличии, либо отсутствии нарушения.

Процесс расследования инцидентов является сложно формализуемой задачей, так как зависит от специфики работы в конкретной Компании. Однако можно определить общий подход к ее решению. Схематично процесс расследования инцидентов можно описать следующим образом:

Последние два этапа в общем случае сильно зависят как от специфики деятельности компании, так и от характера самой утечки и целиком и полностью ложатся на Офицера безопасности.

Однако первые два этапа в меньшей степени зависят от рода деятельности компании и позволяют использовать некие общие принципы, которые будут рассмотрены далее в этом разделе.

3.1. Общий подход к выявлению потенциальных нарушений

Очевидно, что подход к расследованию инцидентов напрямую зависит от того, какой информацией об инциденте обладает Офицер безопасности.

С точки зрения полноты известной информации можно выделить следующие подходы:

- **Выявление инцидентов «с нуля».**

  Дополнительная информация об участниках и составе передаваемых данных отсутствует.

  В этой ситуации отправной точкой для проведения расследования является определение и анализ фактов пересылки подозрительной информации.

- **Контроль контента**.

  Известен состав передаваемой информации. Например:

  – публикация в прессе конфиденциальных материалов;

  – конкурент получил секретные данные;

  – в компании в скором времени должна стартовать маркетинговая программа. Необходимо контролировать перемещение информации, связанной с этой программой.

  В данной ситуации в процессе проведения расследования необходимо установить источник утечки – кто осуществил передачу данных, и, если необходимо, кому данные были переданы.

- **Контроль активности сотрудников.**

  Состав передаваемой информации в общем случае не известен, но известен ее потенциальный отправитель и/или получатель. Например:

  – в компании работает сотрудник, который подозревается в подобных действиях в прошлом и есть вероятность их повторения;

  – из компании был уволен сотрудник, который может попытаться получить от бывших коллег конфиденциальную информацию;

  – в силу объективных причин идет обмен информации с конкурентами, вероятна утечка информации по халатности.

  В данной ситуации процесс расследования заключается в наблюдении за трафиком подозрительных сотрудников и выявлении фактов передачи конфиденциальной информации.

Если содержимое передаваемых данных не известно (как, например, в случае контроля за активностью сотрудника или при выявления инцидента «с нуля»), то особенное внимание при анализе перехваченного трафика следует уделить потенциально опасным ситуациям. В этом случае Вы можете использовать следующие критерии для выявления потенциальных нарушений:

- Пересылка любой **информации конфиденциального характера**. В терминах Системы это означает, что необходимо проанализировать объекты, в которых в процессе лингвистического анализа были обнаружены категории БКФ.
- Пересылка копий или частей **известных конфиденциальных документов**. В терминах Системы это означает, что необходимо проанализировать объекты, для которых были обнаружены совпадения с эталонными документами.
- Пересылка **зашифрованного контента** (если шифрование не является корпоративным стандартом) и/или архивов, закрытых паролем.
- Пересылка файлов **неизвестных форматов** (потенциальная угроза передачи конфиденциальной информации, так как Система не может проверить содержимое перехваченного файла).

В некоторых случаях, как, например, при расследовании инцидентов «с нуля», к потенциально опасным ситуациям можно также отнести пересылку графической информации (потенциальная возможность сокрытия конфиденциальной информации, например, с помощью стеганографии).

Ниже мы рассмотрим каждый из описанных подходов к расследованию инцидентов более подробно.

Все типовые настройки, описанные далее, Вы можете найти в консоли управления в разделах:

- **Отчеты –> Типовые отчеты версии 3.4 –> Расследование инцидентов.**
- **Запросы –> Типовые запросы версии 3.4.**

3.2. Выявление инцидентов «с нуля»

Если не известен ни маршрут передачи данных, ни состав передаваемой информации, то расследование инцидента потребует анализа всего перехваченного трафика. При этом особенное внимание следует уделить потенциально опасным ситуациям.

В общем случае при проведении расследования «с нуля» Вы можете выполнить следующие действия:

1. **Просмотреть все события, перехваченные Системой.**

   Для этого Вы можете воспользоваться следующими типовыми настройками:

   Запросы –> Типовые запросы версии 3.4 -> (или канал перехвата) -> Все события за период

   Запросы –> Типовые запросы версии 3.4 -> Все каналы перехвата -> Все события за текущий день

2. **Проверить, была ли в течение текущего дня подозрительная активность**, и сузить временные рамки для выполнения поиска в хранилище.

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	**Запрос**
Отчеты –> Типовые отчеты версии 3.4 –> Расследование инцидентов –> Выявление подозрительной активности (текущий день)	
Информация с категориями – количество отправок в час	Оперативные запросы -> Типовые запросы -> Все каналы перехвата. По технологиям -> События, содержащие категории за период
Эталонные документы – количество отправок в час	Оперативные запросы -> Типовые запросы -> Все каналы перехвата. По технологиям -> События, содержащие эталонные документы за период
Файлы неизвестного формата – количество отправок в час	Оперативные запросы -> Типовые запросы -> Все каналы перехвата. События с вложениями -> События с файлами неизвестного формата за период
Зашифрованные объекты – количество отправок в час	Оперативные запросы -> Типовые запросы -> Все каналы перехвата. События с вложениями -> События с зашифрованными файлами за период
Файлы заданного типа – количество отправок в час	Оперативные запросы -> Типовые запросы -> Все каналы перехвата. События с вложениями -> События с заданным форматом файла за период

   Отчеты покажут, как в течение текущего дня изменялось количество подозрительных объектов, перехваченных Системой. В случае подозрительной активности Вам необходимо построить соответствующие запросы и проанализировать объекты, которые в них попали.

   Для уточнения результатов данных отчетов Вы можете выяснить, кто из сотрудников пересылал подозрительный контент, какие каналы передачи данных для этого использовались и кто являлся получателем.

3. **Определить контентные маршруты, по которым пересылалась потенциально опасная информаци**я, и тем самым сузить область поиска по каналу перехвата, отправителю и получателю.

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Отчеты –> Типовые отчеты версии 3.4 –> Расследование инцидентов –> Контентные маршруты (текущий день):	
Контентные маршруты информации с категориями	Оперативные запросы –> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие категории за период Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие определенную категорию за период Оперативные запросы -> Типовые запросы версии 3.4 -> Канал перехвата (необходимый канал) -> События, содержащие определенную категорию за период
Контентные маршруты эталонных документов	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие эталонные документы за период Оперативные запросы -> Типовые запросы версии 3.4 -> Канал перехвата (необходимый канал) -> События, содержащие эталонные документы за период
Контентные маршруты зашифрованных файлов и файлов неизвестного формата	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. События с вложениями -> События с зашифрованными файлами за период Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. События с вложениями -> События с файлами неизвестного формата за период

   Отчеты покажут наиболее популярные маршруты перемещения потенциально опасной информации: кто из сотрудников пересылал подозрительный контент, какие каналы передачи данных для этого использовались и кто являлся получателем.

3.3. Контроль контента

Если известен состав передаваемой информации, то в процессе проведения расследования Вам необходимо установить ее отправителя и получателей.

В общем случае при проведении расследования по пересылке известного контента Вы можете выполнить следующие действия:

1. **Определить наиболее популярные маршруты пересылки интересующей Вас информации** и, тем самым, сузить область дальнейшего поиска по отправителю, получателям и каналам передачи.

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Отчеты –> Типовые отчеты версии 3.4 –> Расследование инцидентов –> Контентные маршруты (текущий день):	
Контентные маршруты информации с категориями	Оперативные запросы –> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие категории за период Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие определенную категорию за период Оперативные запросы -> Типовые запросы версии 3.4 -> Канал перехвата (необходимый канал) -> События, содержащие определенную категорию за период
Контентные маршруты эталонных документов	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие эталонные документы за период Оперативные запросы -> Типовые запросы версии 3.4 -> Канал перехвата (необходимый канал) -> События, содержащие эталонные документы за период
Контентные маршруты по ключевым словам	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата -> События, содержащие "ключевую фразу" за период
Контентные маршруты заданного файла	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. События с вложениями -> События с заданным именем файла за период

Для уточнения результатов отчетов Вам необходимо задать требуемые категории информации, эталонные документы, ключевые слова или имена файлов, для которых Вы хотите определить наиболее популярные маршруты пересылки.

После того, как Вы сузите область поиска по отправителям или получателям интересующей Вас информации, Вы можете с помощью предустановленных отчетов, расположенных в папке **Отчеты –> Типовые отчеты версии 3.4 –> Расследование инцидентов –> Выявление подозрительных событий (текущий день)**, определить, в какое время были зафиксированы факты пересылки интересующего Вас контента.

2. **Определить, когда Система зафиксировала факт пересылки интересующего Вас контента** и, тем самым, сузить временные рамки для дальнейшего поиска.

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Отчеты –> Типовые отчеты версии 3.4 –> Расследование инцидентов –> Выявление подозрительных событий (текущий день)	
Выявление подозрительных событий по категориям	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие категории за период

Отчет	Запрос
Выявление подозрительных событий по эталонным документам	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие эталонные документы за период
Выявление подозрительных событий по ключевым словам	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата -> События, содержащие «ключевую фразу» за период
Выявление подозрительных событий по имени файла	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. События с вложениями -> События с заданным именем файла за период

Для выполнения типовых отчетов, перечисленных в таблице, Вам необходимо задать следующие условия:

- определить интересующий Вас контент (категории информации, эталонные документы, ключевые слова или имена файлов);
- задать отправителя и/или получателей, которых Вы определили как потенциальных подозреваемых на предыдущем шаге.

После того, как Вы сузили параметры поиска по отправителям/получателям и времени перехвата интересующей Вас информации, Вам необходимо выполнить соответствующие запросы и проанализировать объекты, которые в них попали.

3.4. Контроль активности сотрудников

Если известен круг потенциальных нарушителей политики безопасности, то процесс выявления инцидентов можно свести к решению следующих подзадач:

1. Определить, отправлял ли потенциальный нарушитель какую-либо подозрительную информацию.

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Отчеты –> Типовые отчеты версии 3.4 –> Расследование инцидентов –> Контроль активности сотрудника (текущий день) –> Сотрудник – отправка подозрительного контента	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие эталонные документы за период Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие категории за период Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. События с вложениями -> События с зашифрованными файлами за период Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. События с вложениями -> События с файлами неизвестного формата за период

   В качестве условия Вы должны указать сотрудника, по которому Вы хотите построить отчет.

   Отчет покажет, какое количество потенциально опасных объектов было перехвачено в течение текущего дня.

   Для анализа событий Вы можете использовать предлагаемые типовые запросы, задав в качестве дополнительного условия интересующего Вас сотрудника.

2. Определить, что именно отправлял потенциальный нарушитель.

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Отчеты –> Типовые отчеты версии 3.4 –> Расследование инцидентов –> Контроль активности сотрудника (текущий день)	
Сотрудник – отправляемые форматы файлов	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. События с вложениями -> События с заданным форматом файла за период
Сотрудник – отправляемые категории информации	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие категории за период
Сотрудник – отправляемые эталонные документы	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие эталонные документы за период

В качестве условия Вы должны указать сотрудника, по которому Вы хотите построить отчеты.

Данные отчеты покажут, какие типы файлов отправлял интересующий Вас сотрудник, а также какие категории информации и эталонные документы были обнаружены в пересылаемых им данных.

Для анализа событий Вы можете использовать предлагаемые типовые запросы, задав в качестве дополнительного условия интересующего Вас сотрудника.

3. Определить, кому сотрудник отправлял информацию.

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Отчеты –> Типовые отчеты версии 3.4 –> Расследование инцидентов –> Контроль активности сотрудника (текущий день)	
Сотрудник – получатели файлов неизвестного формата и зашифрованной информации	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. События с вложениями -> События с зашифрованными файлами за период Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. События с вложениями -> События с файлами неизвестного формата за период
Сотрудник – получатели информации с категориями	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие категории за период
Сотрудник – получатели эталонных документов	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие эталонные документы за период

Данные отчеты покажут, кому интересующий Вас сотрудник отправлял потенциально опасную информацию. В качестве условия Вы должны указать сотрудника, по которому Вы хотите построить отчеты.

Для анализа событий Вы можете использовать предлагаемые типовые запросы. Результаты запросов сгруппированы по сотрудникам. Если необходимо сформировать запрос по конкретному сотруднику, отредактируйте условия запроса.

После того как Вы сузили параметры поиска по получателям и содержимому пересылаемых данных, Вы можете уточнить время перехвата потенциально опасной информации. Для этого Вы можете воспользоваться предустановленными отчетами, расположенными в папке **Отчеты –> Типовые отчеты версии 3.4 –> Расследование инцидентов –> Выявление подозрительных событий (текущий день)**.

ГЛАВА 4. РЕАЛИЗАЦИЯ ДЕЙСТВИЙ, ПРЕДУПРЕЖДАЮЩИХ ПОВТОРНОЕ ВОЗНИКНОВЕНИЕ ИНЦИДЕНТА

После устранения последствий инцидента и восстановления нормального функционирования бизнес-процессов компании, возможно, потребуется выполнить действия по предотвращению повторного возникновения инцидента. Для определения необходимости реализации таких действий следует провести анализ рисков, в рамках которого определяется целесообразность корректирующих и превентивных действий. В некоторых случаях последствия инцидента незначительны по сравнению с корректирующими и превентивными действиями, и тогда целесообразно не совершать дальнейших шагов после устранения последствий инцидента.

Для внесения изменений, предупреждающих повторное возникновение инцидента, необходимо отредактировать скрипт, реализующий политику безопасности Компании.

ГЛАВА 5. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Помимо проведения расследования и выявления фактов утечки конфиденциальных данных, Система позволяет решать дополнительные задачи, такие как: предотвращение использования работниками ресурсов компании в личных целях; оптимизацию загрузки каналов за счет уменьшения нецелевого трафика; оценка статистики инцидентов как показателя эффективности функционирования Системы.

5.1. Нецелевое использование корпоративных ресурсов

Система предоставляет возможности для выявления фактов нецелевого использования корпоративных ресурсов.

В рамках данного документа под нецелевым использованием корпоративных ресурсов понимается посещение сайтов различной тематики (развлекательной тематики, агрессивной направленности, тематики для взрослых и т.д.) и рассылка развлекательного контента (музыка, изображения и видео).

Подход, описанный в данном разделе, поможет Вам ответить на следующие вопросы:

- Как используются корпоративные ресурсы (почта, доступ в интернет и т.д.).
- Кто из сотрудников использует корпоративные ресурсы не по назначению и каким образом.

Все предустановленные отчеты, встречающиеся в данном разделе, Вы можете найти в консоли управления в разделе **Отчеты –> Типовые отчеты версии 3.4 –> Стандартные отчеты –> Нецелевое использование корпоративных ресурсов**.

5.1.1. Оценка использования корпоративных ресурсов

Методы, описанные в данном разделе, позволяют оценить, насколько часто сотрудники Вашей компании используют не по назначению корпоративные ресурсы (такие, как почта или доступ в Интернет).

На основании информации, полученной на данном этапе, Вы сможете решить, требуется ли проводить дальнейший анализ или нет.

Все предустановленные отчеты, описанные в данном разделе, Вы можете найти в консоли управления в папке **Отчеты –> Типовые отчеты версии 3.4 –> Нецелевое использование корпоративных ресурсов -> Оценка использования корпоративных ресурсов**. Во всех случаях, если не указано иное, отчеты по умолчанию показывают статистику за текущую неделю.

С помощью предустановленных отчетов, входящих в комплект поставки Системы, вы можете:

1. Оценить объем и процентное соотношение объектов, свидетельствующих о пересылке файлов развлекательного содержания.

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Пересылка файлов за период	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. События с вложениями

   Отчет **Пересылка файлов** покажет Вам, какие типы файлов пересылали сотрудники Вашей компании и насколько часто.

   В качестве уточнения результатов данного отчета Вы можете использовать сужающие условия на канал перехвата.

Для того, чтобы просмотреть и проанализировать события, связанные с пересылкой файлов, Вы можете воспользоваться указанными запросами.

2. Оценить объем и процентное соотношение использования веб-ресурсов.

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Типы веб-ресурсов за период	Оперативные запросы -> Типовые запросы версии 3.4 -> Интернет/HTTP -> Использование веб-ресурсов за текущий день

   Отчет **Типы веб-ресурсов за период** покажет Вам, насколько часто и на какие категории веб-ресурсов сотрудники Вашей компании отправляли запросы.

3. Оценить статистику обращений на веб-ресурсы в течение текущего дня.

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Статистика обращений на веб-ресуры за текущий день	Оперативные запросы -> Типовые запросы версии 3.4 -> Интернет/HTTP -> Использование веб-ресурсов за текущий день

   Отчет **Статистика обращений на веб-ресуры за текущий день** покажет Вам график обращений пользователей на веб-ресурсы в течение текущего дня. С помощью этого графика Вы можете определить часы, во время которых пользователи наиболее активно использую доступ в интернет. В качестве уточнения результатов данного отчета Вы можете указать только интересующие категории веб-ресурсов.

5.1.2. Выявление сотрудников

Все предустановленные отчеты, описанные в данном разделе, Вы можете найти в консоли управления в папке **Отчеты –> Типовые отчеты версии 3.4 –> Нецелевое использование корпоративных ресурсов –> Выявление сотрудников**. Во всех случаях, если не указано иное, отчеты показывают статистику за текущую неделю.

Чтобы определить сотрудников, использующих корпоративные ресурсы не по назначению, Вы можете с помощью штатных средств Системы выполнить следующие действия:

1. Определить сотрудников, наиболее активно использующих доступ в Интернет.

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Сотрудники – использование веб-ресурсов за период	Оперативные запросы -> Типовые запросы версии 3.4 -> Интернет/HTTP -> Использование веб-ресурсов за текущий день

   Отчет покажет сотрудников, от которых Система перехватила наибольшее количество запросов, с детализацией по категориям используемых сотрудником веб-ресурсов.

   Для уточнения результатов отчета **Сотрудники – использование веб-ресурсов** Вы можете определить наиболее активных пользователей, которые:

   - пересылали информацию через сервисы бесплатной веб-почты;
   - размещали информацию в блогах.

   Эта информация содержится в следующих предустановленных отчетах:

   - Сотрудники – использование веб-почты
   - Сотрудники – использование блогов

Помимо выявления нецелевого использования корпоративных ресурсов, эти отчеты покажут потенциальные места утечки конфиденциальной информации.

2. Определить пользователей, наиболее активно пересылавших файлы с содержимым развлекательного характера (музыка, видео, изображения).

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Сотрудники – пересылка файлов развлекательного характера за период	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. События с вложениями -> События с файлами развлекательного характера за период

   Отчет покажет пользователей, которые наиболее часто пересылали файлы, содержащие изображения, музыку или видео, с детализацией по каждой из указанных категорий файлов.

   Для уточнения результатов отчета Вы можете определить стандартные маршруты, по которым выполняются рассылки развлекательного характера. Эта информация доступна в предустановленном отчете **Маршруты пересылки файлов развлекательного характера за период**.

3. Определить рабочие часы, во время которых указанные сотрудники наиболее активно пользуются веб-ресурсами или рассылают сообщения развлекательного характера.

   Для этого Вы можете воспользоваться следующими предустановленными отчетами:

   - Активность сотрудника – использование веб-ресурсов за текущий день
   - Активность сотрудника – пересылка развлекательного контента за текущий день

   В качестве условий для данных отчетов Вы должны задать сотрудника, по которому Вы хотите построить отчет.

5.2. Аудит системы управления информационной безопасностью

5.2.1. Оценка эффективности работы Системы

Оценка эффективности работы системы – набор действий, который позволяет определить, работает ли настроенная система в соответствии с ожиданиями пользователя.

Схематично процесс оценки эффективности Системы, начиная с этапа анализа перехваченных объектов и заканчивая выявлением ошибочных настроек, можно представить в следующем виде:

Далее эти этапы будут рассмотрены более подробно.

Оценку эффективности стоит проводить в следующих случаях:

- при вводе в эксплуатацию новых правил обработки трафика – низкое качество работы системы будет говорить о том, что настройки заданы неполно и/или неправильно.
- на регулярной основе – снижение качества работы системы будет сигнализировать о том, что в компании изменились бизнес-процессы, и настройки системы необходимо адаптировать.

В результате оценки эффективности Системы Вы сможете выявить узкие места в заданных настройках и устранить их.

Все предустановленные отчеты, встречающиеся в данном разделе, Вы можете найти в консоли управления в разделе **Отчеты –> Типовые отчеты версии 3.4 –> Оценка эффективности Системы**. Во всех случаях, если не указано иное, отчеты показывают статистику за текущую неделю.

> **Важная информация!**
>
> Изложенный ниже метод предполагает, что при обработке перехваченных объектов Офицер безопасности использует штатную возможность Системы «Решение пользователя». «Решение пользователя» позволяет подтвердить или опровергнуть вердикт, вынесенный Системой.

5.2.1.1. Анализ вердиктов, вынесенных Системой

Анализ вердиктов, вынесенных Системой, является подготовительным этапом. Он выполняется в рамках проведения расследования инцидентов и заключается в том, что в процессе обработки объектов, перехваченных Системой, Офицер безопасности принимает решение, какие вердикты были вынесены Системой правильно, а какие – нет.

Для оценки общего количества перехваченных объектов и их распределения по вердиктам вы можете воспользоваться типовым отчетами и запросами из раздела **Отчеты –> Типовые отчеты версии 3.4 –> Статистика Системы –> Статистика инцидентов (текущий день)** (см. п. 5.2.2.2.1 на стр. 23).

Для более подробного анализа перехваченного трафика Вы можете воспользоваться подходом, описанным в разделе Глава 3 на стр. 7.

При этом в первую очередь необходимо обратить внимание на те объекты, которым Система вынесла вердикт «Запрещено». С одной стороны, такие объекты являются потенциальными кандидатами для дальнейшего расследования. С другой стороны, большое количество объектов с запрещающим вердиктом может свидетельствовать о неполной или неправильно настройке Системы.

5.2.1.2. Оценка количества ошибочных вердиктов системы

Общая оценка настройки дает представление о количестве ошибочных вердиктов, вынесенных Системой. На основании информации, полученной на данном этапе, Вы сможете решить, требуется ли проводить дальнейший анализ поведения Системы или нет.

Для оценки количества ошибочных вердиктов, вынесенных Системой, Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Статистика – ложные срабатывания	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. Оценка эффективности Системы -> События, для которых были зафиксированы ложные срабатывания за период

Для оценки ошибок системы используется следующая классификация:

- Ложноположительный вердикт – Система признала объект потенциально опасным и вынесла запрещающий вердикт, однако Офицер безопасности, рассматривая данный инцидент, принял решение о том, что объект не является нарушением.
- Ложноотрицательный вердикт – Система не признала объект потенциально опасным, но Офицер безопасности принял решение, что объект является нарушением.

Наличие большого количества ложных вердиктов системы (как ложноположительных, так и ложноотрицательных) будет говорить о низком качестве настройки Системы. В этом случае Вам необходимо определить, какие именно настройки Системы некорректны, и попытаться их исправить. Общие рекомендации по выявлению и устранению некорректных настроек Системы описаны в п. 5.2.1.3 на стр. 20.

5.2.1.3. Выявление узких мест в настройках

В данном разделе описаны общие рекомендации, направленные на разрешение типовых проблем в настройке правил фильтрации трафика. В каждом конкретном случае выявление узких мест в настройках Системы будет зависеть от специфики корпоративной политики безопасности. Тем не менее, в качестве отправной точки Вы можете использовать описанные ниже типовые настройки Системы.

В общем случае Вы можете выполнить следующие действия для выявления узких мест в настройках Системы:

1. Определить категории БКФ, нуждающиеся в корректировке.

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Категории, для которых были зафиксированы ложные срабатывания	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. Оценка эффективности Системы -> События, для которых были зафиксированы ложные срабатывания за период (дополнительные сужающие условия на интересующие Вас категории, показанные в отчете)

   Отчет покажет категории БКФ, по которым было зафиксировано наибольшее количество ложных срабатываний Системы. Для прояснения ситуации Вам необходимо построить запросы для данных категорий БКФ и проанализировать объекты, которые в них попали.

   В результате анализа таких объектов Вы должны определить документы, которые были ошибочно категоризованы Системой, и скорректировать БКФ (добавить или удалить термины и соответствующие категории).

Отчет	Запрос
События, пропущенные при лингвистическом анализе	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. Оценка эффективности Системы -> События, пропущенные при лингвистическом анализе за период

Отчет покажет, для какого количества объектов Система не смогла определить категории. В качестве условий для данного отчета Вы должны задать ключевые слова, по которым Вы хотите выполнять поиск.

По результатам обработки объектов, пропущенных при лингвистическом анализе, Вам необходимо определить, какие рубрики БКФ нуждаются в корректировке, и скорректировать их.

2. Скорректировать базу эталонных документов.

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Эталонные документы, для которых были зафиксированы ложные срабатывания	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. Оценка эффективности Системы -> События, для которых были зафиксированы ложные срабатывания за период (дополнительные сужающие условия на интересующие Вас эталонные документы, показанные в отчете)

Отчет покажет эталонные документы, по которым было зафиксировано наибольшее количество ложных срабатываний Системы. Как и в случае анализа категорий, Вам необходимо будет построить соответствующие запросы для данных эталонных документов и проанализировать объекты, которые в них попали.

В результате анализа таких событий Вы должны определить, какие документы требуется исключить из базы эталонных документов, а какие, наоборот, добавить.

Отчет	Запрос
События, пропущенные анализом по цифровым отпечаткам	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. Оценка эффективности Системы -> Все каналы перехвата. Оценка эффективности Системы -> События, пропущенные анализом по цифровым отпечаткам за период

Отчет покажет, для какого количества объектов Система не смогла найти совпадения с эталонными документами. В качестве условий для данного отчета Вы должны задать имена файлов, по которым Вы хотите выполнить поиск.

По результатам обработки событий, пропущенных анализом по цифровым отпечаткам, Вам необходимо определить, какие документы требуется добавить в базу эталонных документов.

3. Актуализировать белые/черные списки отправителей и получателей, уточнить разрешенные контентные маршруты.

   Для этого Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Отправители, для которых были зафиксированы ложные срабатывания	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. Оценка эффективности Системы -> События, для которых были зафиксированы ложные срабатывания за период (дополнительные сужающие условия на отправителей)

Отчет	Запрос
Получатели, для которых были зафиксированы ложные срабатывания	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. Оценка эффективности Системы -> События, для которых были зафиксированы ложные срабатывания за период (дополнительные сужающие условия на получателей)

Данные отчеты покажут отправителей и получателей, для которых было зафиксировано наибольшее количество объектов с ложным вердиктом. Для анализа ситуации Вам необходимо выполнить запросы с соответствующими условиями на отправителей и получателей и проанализировать события, которые в них попали.

По результатам анализа Вы можете уточнить правила пересылки информации между сотрудниками, например:

- сотруднику Иванову запрещено отправлять любые письма на внешние адреса;
- сотруднику Петрову в силу производственной необходимости нужно разрешить отправку документов рекламного характера внешним контрагентам;
- и т.д.

5.2.2. Статистика Системы

Статистика является одним из ключевых показателей эффективности действующей в Компании системы безопасности.

Подход, описанный ниже, позволит Вам оценить:

- работу компонентов Системы (см. п. 5.2.2.1 на стр. 22);
- общую статистику выявления инцидентов (см. п. 5.2.2.2 на стр. 23).

5.2.2.1. Активность Системы

Методы, описанные в данном разделе, позволят Вам проверить работу компонентов Системы, отвечающих за перехват и анализ трафика.

Все предустановленные отчеты, описанные в данном разделе, Вы можете найти в консоли управления в папке **Отчеты –> Типовые отчеты версии 3.4 –> Статистика Системы –> Активность Системы (текущий день)**.

5.2.2.1.1. Проверка активности перехватчиков

Для получения статистики об активности перехватчиков Системы и анализа событий, перехваченных по каждому из каналов, Вы можете воспользоваться следующими типовыми отчетами и запросами:

Отчет	Запрос
Device Monitor – активность за текущий день **DeviceLock Monitor – активность за текущий день**	Оперативные запросы → Типовые запросы версии 3.4 → Устройства/ Device Monitor/ Device Lock Monitor
HTTP Monitor – активность за текущий день	Оперативные запросы → Типовые запросы версии 3.4 → Интернет/ HTTP
ICQ Monitor – активность за текущий день	Оперативные запросы → Типовые запросы версии 3.4 → Мгновенные сообщения/ ICQ

Отчет	Запрос
Print Monitor – активность за текущий день **Print Monitor Server – активность за текущий день**	Оперативные запросы → Типовые запросы версии 3.4 → Печать/ Print Monitor/ Print Monitor Server
SMTP Monitor – активность за текущий день	Оперативные запросы → Типовые запросы версии 3.4 → Электронная почта/ SMTP

Каждый из приведенных выше отчетов покажет, как в течение текущего дня изменялось количество объектов, перехваченных соответствующим перехватчиком. Нулевая активность в течение некоторого периода времени может говорить о том, что данный перехватчик не работает.

5.2.2.1.2. Ошибки применения правил обработки

Для получения статистики о работе правил обработки объектов Вы можете воспользоваться следующими типовыми настройками:

Отчет	Запрос
Ошибки выполнения пользовательского скрипта за текущий день	Оперативные запросы → Типовые запросы версии 3.4 → Все каналы перехвата. Статистика Системы → Ошибки выполнения пользовательского скрипта за текущий день

Отчет покажет, как в течение текущего дня изменялось количество объектов, при обработке которых произошли ошибки выполнения пользовательского скрипта. Это означает, что по тем или иным причинам скрипт задан некорректно. Для исправления сложившейся ситуации Вам необходимо проанализировать результаты соответствующего запроса и внести исправления в скрипт.

5.2.2.1.3. Статистика выполнения контентного анализа

Для получения статистики о работе контентного анализа Вы можете воспользоваться следующим типовым отчетом: **Статистика выполнения контентного анализа за текущий день**

Отчет покажет, как в течение текущего дня изменялось количество объектов, в которых были обнаружены хотя бы одна категория, эталонный документ или текстовый объект. Если в Системе заданы соответствующие параметры контентного анализа (загружены БКФ и эталонные документы или выбраны типы текстовых объектов), то продолжительная нулевая активность на графике может говорить о том, что контентный анализ по тем или иным причинам не выполняется.

5.2.2.2. Статистика инцидентов

Подход, описанный в данном разделе, позволит Вам оценить общую статистику работы Системы.

Все предустановленные отчеты, описанные в данном разделе, Вы можете найти в консоли управления в папке **Отчеты –> Типовые отчеты версии 3.4 –> Статистика Системы –> Статистика инцидентов (текущий день)**.

5.2.2.2.1. Общее количество инцидентов

Приведенные ниже типовые настройки позволяют сравнить количество потенциальных нарушений (т.е. событий, которые Система признала нарушениями) и «реальных» инцидентов (нарушений, которые были выявлены Офицером безопасности). Статистика приведена в разбивке по вердиктам, вынесенным Системой, для анализа событий Вы можете воспользоваться соответствующими запросами:

1. Общее количество нарушений, выявленных Системой, по отношению ко всем перехваченным объектам.

   Для получения данной статистики предназначены следующие типовые настройки:

Отчет	Запрос
Общее количество инцидентов, выявленных Системой	Оперативные запросы -> Типовые запросы версии 3.4 -> (канал перехвата) -> Инциденты, выявленные Системой, за текущий день

Отчет покажет количество объектов, которым Система вынесла вердикт «Нарушение», по отношению к объектам, признанным Системой «безопасными». Статистика приведена за текущий день.

В отличие от отчета, описанного ниже, данная статистика показывает количество предполагаемых нарушений.

Для уточнения результатов данного отчета Вы можете использовать дополнительные сужающие условия на каналы перехвата.

2. Общее количество инцидентов, выявленных Офицером безопасности.

   Для получения данной статистики предназначен предустановленный отчет **Общее количество инцидентов, выявленных Офицером безопасности**.

   Данный отчет покажет количество инцидентов, выявленных Офицером безопасности, в разбивке по вердиктам, вынесенным Системой. Статистика приведена за текущую неделю.

   > **Важная информация!**
   >
   > Данный отчет предполагает, что при обработке перехваченных объектов Офицер безопасности использует штатную возможность Системы «Решение пользователя». «Решение пользователя» позволяет подтвердить или опровергнуть вердикт, вынесенный Системой.

   В отличие от предыдущего отчета, данная статистика показывает количество «реальных» инцидентов, обнаруженных Офицером безопасности в процессе анализа перехваченного трафика.

   Для уточнения результатов данного отчета Вы можете использовать дополнительные сужающие условия на каналы перехвата.

5.2.2.2.2. Количество инцидентов по перехватчикам

Приведенные ниже отчеты позволяют сравнить количество потенциальных инцидентов (т.е. событий, которые Система признала нарушениями) и «реальных» инцидентов (нарушений, которые были выявлены Офицером безопасности в процессе анализа перехваченных Системой объектов). Статистика приведена в разбивке по каналам перехвата:

1. Количество нарушений, выявленных Системой, по перехватчикам.

   Для получения данной статистики предназначены следующие типовые настройки:

Отчет	Запрос
Количество инцидентов, выявленных Системой, по перехватчикам	Оперативные запросы -> Типовые запросы версии 3.4 -> (канал перехвата) -> Инциденты, выявленные Системой, за текущий день

   Данный отчет покажет количество объектов, перехваченных каждым монитором Системы, для которых Система вынесла вердикт «Нарушение». Статистика приведена за текущий день.

   В отличие от следующего отчета, данный предустановленный отчет показывает количество потенциальных нарушений, выявленных Системой, по каждому из каналов перехвата.

2. Количество подтвержденных нарушений по перехватчикам.

   Для получения данной статистики предназначен предустановленный отчет Количество инцидентов, выявленных Офицером безопасности, по перехватчикам.

   Данный отчет покажет количество инцидентов, выявленных Офицером безопасности, для каждого канала перехвата. Статистика приведена за текущий день.

Важная информация!

Данный отчет предполагает, что при обработке перехваченных объектов Офицер безопасности использует штатную возможность Системы «Решение пользователя». «Решение пользователя» позволяет подтвердить или опровергнуть вердикт, вынесенный Системой.

В отличие от предыдущего отчета, данная статистика показывает количество «реальных» инцидентов – подтвержденных нарушений, обнаруженных Офицером безопасности в процессе анализа перехваченного трафика.

5.2.2.2.3. Динамика количества инцидентов

Приведенные в этом разделе отчеты показывают, как изменялось количество перехваченных событий в течение текущего дня, и позволяют сравнить динамику количества потенциальных инцидентов (т.е. событий, которые Система признала нарушениями) и «реальных» инцидентов (нарушений, которые были выявлены Офицером безопасности). Для анализа событий, на основании которых построены отчеты, Вы можете использовать соответствующие запросы.

1. Динамика количества потенциальных инцидентов.

   Для получения и анализа данной статистики предназначены следующие типовые настройки:

Отчет	Запрос
Динамика количества инцидентов, выявленных Системой	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата -> Все события за текущий день
	Оперативные запросы -> Типовые запросы версии 3.4 -> (канал перехвата) -> Инциденты, выявленные Системой, за текущий день

   Данный отчет покажет, как в течение текущего дня изменялось количество всех перехваченных Системой объектов, а также какому количеству из них Система вынесла вердикт «Запрещено», а какому – «Разрешено».

   Для уточнения результатов данного отчета Вы можете использовать дополнительные сужающие условия на каналы перехвата.

2. Динамика подтвержденных нарушений.

   Для получения данной статистики предназначен предустановленный отчет **Динамика количества инцидентов, выявленных Офицером безопасности**.

   Важная информация!

   Данный отчет предполагает, что при обработке перехваченных объектов Офицер безопасности использует штатную возможность Системы «Решение пользователя». «Решение пользователя» позволяет подтвердить или опровергнуть вердикт, вынесенный Системой.

   Данный отчет покажет, как в течение текущего дня изменялось количество инцидентов, выявленных Офицером безопасности в процессе анализа перехваченного трафика.

5.2.2.2.4. Эффективность работы Офицера безопасности

Важная информация!

Изложенный ниже метод предполагает, что при обработке перехваченных объектов Офицер безопасности использует штатную возможность Системы «Решение пользователя». «Решение пользователя» позволяет подтвердить или опровергнуть вердикт, вынесенный Системой.

Для оценки эффективности работы Офицера безопасности Вы можете воспользоваться предустановленным отчетом **Обработка событий Офицером безопасности**.

Для уточнения результатов отчета Вы можете задать сужающие условия по зонам ответственности – если в вашей компании используется разделение доступа Офицеров безопасности к перехваченным объектам с помощью зон ответственности.

5.2.2.2.5. Рейтинг инцидентов по содержимому

Все предустановленные отчеты, описанные в данном разделе, Вы можете найти в консоли управления в папке Отчеты –> Типовые отчеты версии 3.4 –>Статистика Системы / Рейтинг инцидентов по содержимому (текущая неделя).

> **Важная информация!**
>
> Приведенные в этом разделе отчеты предполагают, что при обработке перехваченных объектов Офицер безопасности использует штатную возможность Системы «Решение пользователя».
>
> Если Вы не используете решение пользователя для обработки перехваченных объектов, то Вы можете воспользоваться аналогичными отчетами, но по вердиктам, вынесенным Системой[2].

Приведенные ниже отчеты показывают, какая информация (категории или эталонные документы) чаще всего встречается в инцидентах, выявленных Офицером безопасности в процессе анализа перехваченного трафика. Для анализа событий, содержащих интересующую Вас информацию, Вы можете использовать соответствующие запросы.

1. Категории информации, которые «утекают» чаще всего.

   Отчет покажет наиболее часто встречающиеся категории, которые были обнаружены в объектах, признанных Офицером безопасности как нарушение.

Отчет	Запрос
Инциденты – рейтинг категорий информации	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие определенную Категорию за период

2. Эталонные документы, которые «утекают» чаще всего.

   Отчет покажет наиболее часто встречающиеся эталонные документы, которые были обнаружены в объектах, признанных Офицером безопасности как нарушение.

Отчет	Запрос
Инциденты – рейтинг эталонных документов	Оперативные запросы -> Типовые запросы версии 3.4 -> Все каналы перехвата. По технологиям -> События, содержащие эталонные документы за период

[2] Чтобы заменить сужающие условия на вердикт «Запрещено», Вам необходимо в предустановленных отчетах удалить условие «Решение пользователя = Нарушение» и добавить условие «Вердикт = Запрещено».