InfoWatch Password Disclosure Adapter. Руководство по установке и конфигурированию

20/08/2026

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Введение 4

2 Общая информация об InfoWatch Password Disclosure Adapter 5

2.1 Функции InfoWatch Password Disclosure Adapter 5

2.2 Схема работы InfoWatch Password Disclosure Adapter 5

2.2.1 Статусы файлов и событий 7

2.2.2 Назначение вердикта и отправка уведомлений 7

3 Аппаратное и программное обеспечение для InfoWatch Password Disclosure Adapter 9

4 Добавление лицензии и получение токена плагина для InfoWatch Traffic Monitor 11

5 Установка и запуск InfoWatch Password Disclosure Adapter 13

5.1 Установка адаптера на один сервер с Traffic Monitor 13

5.2 Установка адаптера на отдельный сервер 16

5.2.1 Установка адаптера на отдельный сервер под управлением ОС RHEL или РЕД ОС 16

5.2.2 Установка адаптера на отдельный сервер под управлением ОС Astra Linux 22

6 Обновление InfoWatch Password Disclosure Adapter 27

7 Настройки InfoWatch Password Disclosure Adapter 29

7.1 Настройки адаптера в файле pda.conf 29

7.1.1 Подключение к серверу Traffic Monitor 29

Раздел TM 29

Раздел Pushapi 30

7.1.2 Подключение к базе данных PostgreSQL 31

Раздел Database 31

7.1.3 Подключение к серверу очередей Redis 32

Раздел Redis 32

7.1.4 Почтовые уведомления 32

Раздел SMTP 32

Раздел Templates 33

7.1.5 Синхронизация и быстродействие 34

Раздел Worker 34

7.1.6 Логирование 35

Раздел Logging 35

7.1.7 Хранение расшифрованных данных 35
Раздел ContentStorage 35
7.2 База паролей InfoWatch Password Disclosure Adapter 36
7.3 Настройки шаблонов уведомлений 36
7.3.1 Параметры, используемые в шаблонах уведомлений 37
7.4 Настройки страницы ввода пароля 38
8 Настройка политики Traffic Monitor для работы InfoWatch Password Disclosure Adapter 40
8.1 Правила пересылки защищенных и незащищенных данных 44
9 Диагностика и удаление InfoWatch Password Disclosure Adapter 46

1 Введение

В настоящем руководстве представлены сведения по установке, настройке, администрированию, обновлению и удалению InfoWatch Password Disclosure Adapter (далее также PDA, адаптер).

Аудитория

Информация, содержащаяся в руководстве, предназначена для администраторов InfoWatch Traffic Monitor (далее также Система), которые хотят оптимизировать работу по расшифровке в случае перехвата писем с зашифрованными файлами.

Руководство рассчитано на пользователей, имеющих навыки администрирования в среде операционных систем Microsoft Windows и Linux, а также навыки работы с СУБД PostgreSQL.

2 Общая информация об InfoWatch Password Disclosure Adapter

Пересылка файлов – потенциальная угроза утечки конфиденциальной информации. В случае шифрования файлов отправителем Офицер безопасности вынужден расшифровывать файлы вручную. InfoWatch Password Disclosure Adapter позволяет автоматизировать расшифровку файлов, защищенных паролем.

Адаптер получает из Traffic Monitor события с перехваченными письмами, к которым прикреплены зашифрованные файлы, расшифровывает их и отправляет обратно в Traffic Monitor для вынесения вердикта.

В этой главе представлены:

- Функции InfoWatch Password Disclosure Adapter
- Схема работы InfoWatch Password Disclosure Adapter

2.1 Функции InfoWatch Password Disclosure Adapter

InfoWatch Password Disclosure Adapter предназначен для автоматической расшифровки зашифрованных файлов, прикрепленных к перехваченному письму. При этом осуществляется:

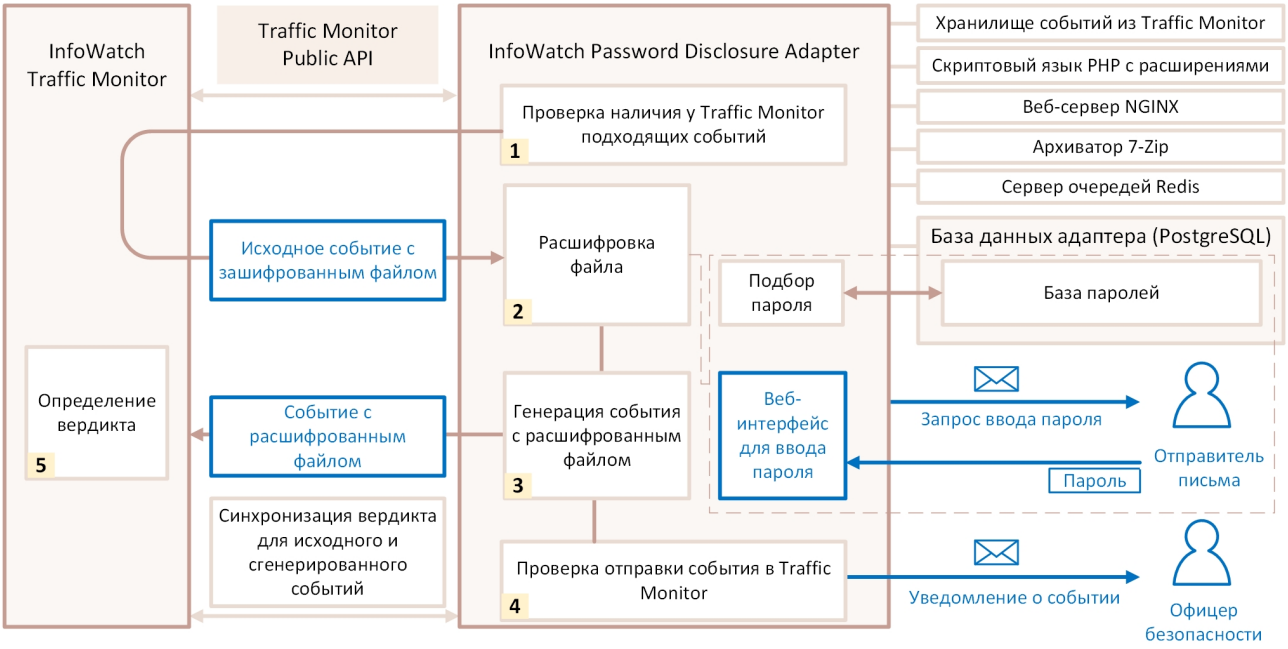
- обработка событий типа *Электронная почта* и зашифрованных файлов форматов:
  - RAR, ZIP, 7ZIP;
  - DOC, PPT, XLS, в том числе с надстройкой IRM Client for Office;
  - DOCX, PPTX, XLSX, XLSM, XLSB;
  - PDF;
  - EML.
- в случае неподдерживаемого формата зашифрованного вложения – уведомление отправителя по электронной почте о невозможности обработки файла;
- в случае поддерживаемого формата зашифрованного вложения – подбор пароля из базы паролей;
- при отсутствии подходящего пароля в базе – уведомление отправителя о необходимости предоставить пароль;
- уведомление Офицера безопасности об успешно расшифрованных событиях;
- досылка оригинальных писем получателю при положительном результате проверки расшифрованного контента;
- повторное использование и шифрованное хранение введенных отправителем паролей.

Кроме того, поддерживается возможность:

- фильтрации событий, получаемых из Traffic Monitor;
- ручного изменения вердикта Офицером безопасности;
- расшифровки вложенных архивов;
- работы с несколькими зашифрованными файлами, прикрепленными к одному письму.

2.2 Схема работы InfoWatch Password Disclosure Adapter

На схеме ниже показан принцип работы InfoWatch Password Disclosure Adapter.



Если перехват трафика осуществляется в режиме **блокировки "в разрыв"**[1], InfoWatch Password Disclosure Adapter работает по следующему алгоритму:

1. Адаптер обращается к Traffic Monitor, чтобы получить почтовые события с зашифрованными файлами из карантина[2].
2. В случае, если обработка файла данного типа не поддерживается, адаптер оповещает об этом отправителя уведомлением по электронной почте. Письмо остается в карантине.
3. В случае, если обработка файла данного типа поддерживается, адаптер расшифровывает файл следующим образом:
   a. Подбирает пароль из базы паролей. Подробнее см. статью *База паролей InfoWatch Password Disclosure Adapter*.
   b. Если в базе нет подходящего пароля, адаптер оповещает отправителя уведомлением по электронной почте о необходимости перейти в веб-интерфейс и ввести пароль.
   c. Password Disclosure Adapter генерирует событие[3] с расшифрованным файлом и отправляет его с пользовательскими атрибутами и ID исходного события в Traffic Monitor.
   d. Адаптер отправляет уведомление Офицеру безопасности с информацией о событии, в котором содержится расшифрованный файл.
   e. На основании анализа расшифрованного файла Система определяет вердикт для события (см. *Назначение вердикта и отправка уведомлений*).

В случае пересылки **скрытой копии** почтового трафика[1]:

1. Адаптер обращается к Traffic Monitor, чтобы получить почтовые события с зашифрованными файлами из карантина[2].
2. В случае, если обработка файла данного типа поддерживается, адаптер расшифровывает файл следующим образом:
   a. Подбирает пароль из базы паролей. Подробнее см. статью *База паролей InfoWatch Password Disclosure Adapter*.

b. Если в базе нет подходящего пароля, адаптер оповещает отправителя уведомлением по электронной почте о необходимости перейти в веб-интерфейс и ввести пароль.
c. Password Disclosure Adapter генерирует событие[3] с расшифрованным файлом и отправляет его с пользовательскими атрибутами и ID исходного события в Traffic Monitor.
d. На основании анализа расшифрованного файла Система определяет вердикт для события (см. *Назначение вердикта и отправка уведомлений*).

Примечание:

[1] В режиме пересылки скрытой копии трафика вердикт *Карантин* не влияет на пересылку писем. Подробнее о режимах перехвата почтового трафика см. *InfoWatch Traffic Monitor. Руководство администратор. Настройка перехвата SMTP-трафика*.

[2] За одно обращение считывается до 1000 событий. Офицер безопасности может задать периодичность получения событий в настройках.

[3] Если в исходном событии содержится:

- несколько зашифрованных файлов, включая вложенные архивы, то адаптер генерирует новое событие только после того, как все файлы расшифрованы;
- архив с несколькими уровнями вложенности, Система обрабатывает не более 100 уровней;
- архив, то после расшифровки адаптер распаковывает его и запаковывает обратно перед отправкой в Traffic Monitor;
- архив RAR-формата, то при генерации события адаптер меняет формат архива на ZIP.

2.2.1 Статусы файлов и событий

Адаптер присваивает статусы зашифрованным файлам и событиям, содержащим эти файлы.

Статусы файлов:

- *Расшифровано*
- *Ожидает пароль от пользователя*

Статусы событий:

- *Расшифровано* – когда расшифрованы все зашифрованные файлы в событии;
- *Отправлено в ТМ* – когда адаптер сгенерировал событие для Traffic Monitor;
- *Обработано* – когда адаптер отправил уведомление Офицеру безопасности с информацией о событии, в котором находится расшифрованный файл;
- *Ошибка.*

2.2.2 Назначение вердикта и отправка уведомлений

Traffic Monitor отправляет уведомления об изменении вердиктов согласно настроенным политикам. При этом исходное событие наследует вердикт сгенерированного. После анализа расшифрованных вложений возможна отправка уведомлений в следующих случаях:

- при попадании сгенерированного события в карантин (вердикт *Карантин*) – начиная с Traffic Monitor версии 7.15;
- при досылке письма из исходного события (вердикт *Разрешить*);
- при блокировке письма из исходного события (вердикт *Заблокировать*).

Доступно ручное изменение вердикта для исходного и сгенерированного событий. Например, если после анализа расшифрованных вложений Система назначила письму вердикт Карантин, Офицер безопасности может дослать письмо вручную.

Если Офицер безопасности назначил вердикт исходному событию раньше, чем его определила Система после анализа, то результаты анализа по сгенерированному событию не влияют на исходное событие.

О настройке политик Traffic Monitor см. *InfoWatch Traffic Monitor. Руководство пользователя. Создание политики защиты данных*.

О применении разных правил к пересылке одних и тех же данных в зашифрованном и открытом виде см. *Правила пересылки защищенных и незащищенных данных.*

3 Аппаратное и программное обеспечение для InfoWatch Password Disclosure Adapter

Требования к аппаратному обеспечению

Минимальные требования, необходимые для установки адаптера:

- количество ядер процессора: 2;
- ОЗУ: 1 ГБ;
- жесткий диск: 2 ГБ.

Требования к аппаратному обеспечению при предполагаемой нагрузке в 35000 пользователей (2000 событий в день):

- процессор: 8 CPU (2* CPU Xeon Gold 6230 @ 2.1 GHz);
- ОЗУ: 2 ГБ;
- диск: SSD (RAID1 1.5 TB).

Требования к программному обеспечению

Требования к ПО при установке адаптера на один сервер с Traffic Monitor отличаются от требований при распределенной установке адаптера.

ПО		При совместной установке	При распределенной установке
Операционная система	РЕД ОС	Версии 7.3.x	
	Red Hat Enterprise Linux	Версии 7.x	
	Astra Linux	Версии 1.7.5.16, 1.7.5.9, 1.8.6	
InfoWatch Traffic Monitor с СУБД PostgreSQL		Начиная с версии 7.9[1]	Начиная с версии 7.7.1[1]
Дополнительные пакеты[2]	Утилита QPDF	+	+
	Скриптовый язык PHP с расширениями PDO, PDO_PGSQL, Mailparse, Redis, PCNTL	–	Версии 7.4
	Сервер Redis	–	Версии 5.x
	Веб-сервер NGINX	–	Версии 1.x
	Архиватор 7-Zip (модуль P7zip-plugins)	–	+

Примечание:

[1] Работа адаптера на сервере под управлением ОС Astra Linux поддерживается только при использовании Traffic Monitor версии 7.10 и выше.

[2] Подробнее об установке зависимостей см. статьи раздела *Установка и запуск InfoWatch Password Disclosure Adapter*.

4 Добавление лицензии и получение токена плагина для InfoWatch Traffic Monitor

Важно!

Лицензию необходимо добавить до запуска адаптера во время подготовки Traffic Monitor. Подробнее см. статью *Установка и запуск InfoWatch Password Disclosure Adapter*.

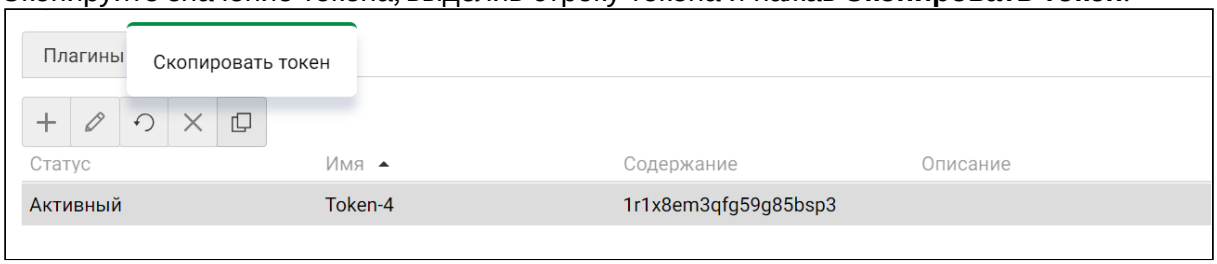
Также необходимо сохранить значение токена плагина, которое будет использовано позже для настройки подключения адаптера к Traffic Monitor. Подробнее см. статью *Настройка политики Traffic Monitor для работы InfoWatch Password Disclosure Adapter*.

Чтобы добавить лицензию:

1. В Консоли управления Traffic Monitor перейдите в раздел **Управление** → **Лицензии**.
2. Нажмите + **Создать**.
3. В диалоговом окне загрузки файла выберите поставляемый файл лицензии (`.license`) и нажмите **Открыть**.
4. В диалоговом окне **Добавление лицензии** отобразятся сведения о лицензии и лицензируемых технологиях и перехватчиках. Нажмите **Сохранить**.
5. В открывшемся диалоговом окне нажмите **Да**. Страница браузера будет перезагружена, и новая лицензия будет добавлена в список установленных лицензий.

Чтобы получить токен плагина:

1. В Консоли управления Traffic Monitor перейдите в раздел **Управление** → **Плагины**.
2. Выберите плагин *InfoWatch Password Disclosure Adapter* и перейдите на вкладку **Токены**.
3. Скопируйте значение токена, выделив строку токена и нажав **Скопировать токен**:



4. Сохраните значение токена.

Примечание:

В **Traffic Monitor 7.10 и более поздних версий** плагин предустановлен.

Плагин отображается, только если в Traffic Monitor установлена действующая лицензия.

Для взаимодействия с **Traffic Monitor 7.9** добавьте плагин вручную:

1. В Консоли управления Traffic Monitor перейдите в раздел **Управление** → **Плагины**.
2. Нажмите **Добавить плагин**.
3. В открывшемся диалоговом окне нажмите **Выбрать файл**.
4. В диалоговом окне загрузки файла выберите поставляемый файл плагина (`.zip`).

Теперь вы можете перейти к установке адаптера и его настройке перед запуском.

5 Установка и запуск InfoWatch Password Disclosure Adapter

> **Важно!**
>
> До начала установки:
>
> - Убедитесь, что версии ПО удовлетворяют требованиям, описанным в статье *Аппаратное и программное обеспечение для InfoWatch Password Disclosure Adapter*. Там же вы можете найти ссылки на официальную документацию ПО с инструкциями по его установке и настройке.
> - Сохраните токен плагина адаптера. Подробнее см. *Добавление лицензии и получение токена плагина для InfoWatch Traffic Monitor*.

Вы можете установить InfoWatch Password Disclosure Adapter:

- на сервер, где установлен Traffic Monitor, см. *Установка адаптера на один сервер с Traffic Monitor*;
- на отдельный сервер, см. *Установка адаптера на отдельный сервер*.

5.1 Установка адаптера на один сервер с Traffic Monitor

Чтобы установить адаптер и настроить его перед запуском:

1. Скопируйте поставляемые пакеты:
   - на сервере под управлением ОС RHEL и РЕД ОС в директорию `/root/rpms`:
     - `<iwtm-pda>.rpm`
     - `<iwtm-php-mailparse>.rpm`
     - `<iwtm-msoffcrypto-tool>.rpm`
   - на сервере под управлением ОС Astra Linux в директорию `/root/debs`:
     - `<iwtm-pda>.deb`
     - `<iwtm-php-mailparse>.deb`
     - `<iwtm-msoffcrypto-tool>.deb`

     > **Примечание:**
     >
     > Здесь и далее `<iwtm-pda>`, `<iwtm-php-mailparse>` и `<iwtm-msoffcrypto-tool>` – полные названия файлов.
     >
     > При наличии пакетов для разных ОС убедитесь, что вы используете файлы именно для вашей ОС.

2. Установите пакеты.
   - **На сервере под управлением ОС RHEL или РЕД ОС:**
     a. Перед установкой адаптера установите утилиту QPDF с помощью команды:

     ```
     yum install qpdf
     ```

     b. Перейдите в директорию с пакетами и установите их:

```
cd /root/rpms
rpm -i <iwtm-msoffcrypto-tool>.rpm <iwtm-pda>.rpm <iwtm-php-mailparse>.rpm
```

- **На сервере под управлением ОС Astra Linux:**
  a. Перед установкой адаптера установите дополнительный пакет с помощью команды:

```
sudo apt install python3-pip
```

  b. Перейдите в директорию с пакетами и установите их:

```
cd /root/debs
dpkg -i <iwtm-php-mailparse>.deb <iwtm-msoffcrypto-tool>.deb
sudo apt install ./<iwtm-pda>.deb
```

3. Перезапустите PHP-FPM. Для этого:
   a. Используйте команду:

```
systemctl restart iwtm-php-fpm
```

   b. Убедитесь, что PHP-FPM запустился:

```
systemctl status iwtm-php-fpm
```

4. В файле `/opt/iw/tm5/etc/pda.conf` укажите значения параметров согласно статье *Настройки адаптера в файле `pda.conf`*:
5. Запустите миграцию адаптера от имени пользователя `iwtm` с помощью команды:

```
su -c 'php /opt/iw/tm5/www/pda/pda migrate -p /opt/iw/tm5/etc' iwtm
```

6. В файле `override.conf` задайте параметр окружения. Для этого:
   a. Откройте на редактирование файл `/etc/systemd/system/iw_pda.service.d/override.conf`.
   b. В блоке `[Service]` укажите корректное значение переменной `Environment`, заменив `https://127.0.0.1` на внешний IP-адрес или доменное имя сервера.
   c. Если необходимо использовать более сложное шифрование паролей, используйте параметр `PDA_SALT`. Укажите в значении соль в формате строки произвольной длины, содержащей любые символы. Например:

```
Environment="PDA_SALT=P%gL1;T:9dR32M6n"
```

   d. Обновите сервис с помощью команды:

```
systemctl daemon-reload
```

7. Если необходимо, измените шаблоны почтовых уведомлений и отображение страницы ввода пароля. См. статьи *Настройки шаблонов уведомлений*, *Настройки страницы ввода пароля*.
8. Если вы хотите добавить пароли в базу паролей, внесите их в таблицу `custom_password` базы данных. Подробнее см. статью *База паролей InfoWatch Password Disclosure Adapter*.

   > **Примечание:**
   >
   > Для работы с базой данных рекомендуется использовать инструменты администрирования DBeaver или pgAdmin. При подключении к базе данных выберите схему `pda`.

9. Запустите прослушивание новых событий от имени системного администратора с помощью команды:

   ```
   systemctl start iw_pda
   ```

10. Убедитесь, что адаптер запущен:

    ```
    systemctl status iw_pda
    ```

    В случае успешного запуска отобразится статус `active (running)`.
11. Если необходимо включить автозапуск адаптера в случае перезагрузки сервера, переведите сервис в состояние `enabled`:

    ```
    systemctl enable iw_pda.service
    ```

После того, как прослушивание событий запущено, настройте политику Traffic Monitor для работы адаптера (подробнее см. *Настройка политики Traffic Monitor для работы InfoWatch Password Disclosure Adapter*).

> **Важно!**
>
> В дальнейшем при необходимости обновить Traffic Monitor, перед обновлением остановите адаптер. Используйте команду:
>
> ```
> systemctl stop iw_pda
> ```

Подробнее см. *InfoWatch Traffic Monitor. Руководство по установке. Обновление Системы*.

5.2 Установка адаптера на отдельный сервер

Перед установкой адаптера:

Необходимо проверить, что сервер очередей Redis доступен. Для этого подключитесь к Redis, используя команду:

```
redis-cli -h <server_IP> -p 6379 ping
```

В команде выше `<server_IP>` – IP-адрес сервера Redis.

При успешном подключении Redis отвечает сообщением `PONG`. Подробнее о взаимодействии с Redis см. официальную документацию Redis (доступна на английском языке).

Для установки адаптера используйте инструкции:

- Установка адаптера на отдельный сервер под управлением ОС RHEL или РЕД ОС
- Установка адаптера на отдельный сервер под управлением ОС Astra Linux

После установки адаптера и запуска прослушивания событий:

- Настройте политику Traffic Monitor для работы адаптера. Подробнее см. *Настройка политики Traffic Monitor для работы InfoWatch Password Disclosure Adapter*
- Если необходимо включить автозапуск служб в случае перезагрузки сервера, переведите все сервисы в состояние `enabled`:

  ```
  systemctl enable nginx.service redis.service php-fpm.service iw_pda.service
  ```

- При необходимости обновить Traffic Monitor в дальнейшем, перед обновлением остановите адаптер. Подробнее см. *InfoWatch Traffic Monitor. Руководство по установке. Обновление Системы*. Команды остановки и запуска адаптера см. в статье *Диагностика и удаление InfoWatch Password Disclosure Adapter*.

5.2.1 Установка адаптера на отдельный сервер под управлением ОС RHEL или РЕД ОС

Чтобы установить адаптер и настроить его перед запуском:

1. Установите скриптовый язык PHP с расширениями:
   На сервере под управлением ОС RHEL:
   a. Убедитесь, что менеджер пакетов `yum` настроен на репозиторий PHP 8.1.
   b. Установите PHP с расширениями при помощи команды:

   ```
   yum install php php-pdo php-cli php-pgsql php-pecl-redis php-fpm php-pecl-mailparse
   ```

   На сервере под управлением РЕД ОС:
   a. Скачайте репозиторий с PHP 8.1 при помощи команды:

```
yum install php81-release
```

b. Установите PHP с расширениями при помощи команды:

```
yum install php-8.1* php-pdo php-cli php-pgsql php-pecl-redis php-pecl-mailparse
```

> **Важно!**
>
> Если какой-либо пакет отсутствует в официальном репозитории, используйте пакет из внешнего дополнительного репозитория, предварительно подключив репозиторий к ОС.

2. Убедитесь, что вместе с PHP установлены модули:
   - `php-common`
   - `php-mbstring`
   - `php-process`
   - `php-curl`

   Чтобы проверить список установленных модулей, используйте команду:

```
php -m
```

   Если какой-то из модулей не был установлен, установите пакет отдельно.
3. Установите дополнительные пакеты NGINX, Redis, QPDF и P7zip с плагинами при помощи команды:

```
yum install nginx redis qpdf p7zip p7zip-plugins
```

4. Поместите на сервер в директорию `/root/rpms` поставляемые пакеты:
   - `<iwtm-pda>.rpm`
   - `<iwtm-msoffcrypto-tool>.rpm`

   > **Примечание:**
   >
   > Здесь и далее `<iwtm-pda>`, `<iwtm-msoffcrypto-tool>` – полные названия файлов.
   >
   > При наличии пакетов для разных ОС убедитесь, что вы используете файл именно для вашей ОС.

5. Перейдите в директорию с RPM-файлами и установите библиотеку `msoffcrypto` и адаптер. Используйте команду:

```
rpm -i <iwtm-msoffcrypto-tool>.rpm <iwtm-pda>.rpm
```

6. Смените пользователя NGINX на `iwtm`. Для этого:
   a. Откройте на редактирование файл `/etc/nginx/nginx.conf`.
   b. Измените значение поля `user` на `iwtm`.

7. Приведите порты PHP-FPM и Password Disclosure Adapter к одному значению или используйте Unix-сокет.

> **Примечание:**
>
> Для Password Disclosure Adapter по умолчанию используется 9001 порт. В зависимости от версии, для PHP-FPM по умолчанию может использоваться 9000 порт или Unix-сокет.

На сервере под управлением ОС Red Hat Enterprise Linux:

a. Перейдите в файл `/etc/php-fpm.d/www.conf`.
b. Выберите один из способов настройки:
   - Измените значение поля `listen` на `127.0.0.1:9001`.
     или
   - Скопируйте значение поля `listen` в файле `www.conf`.
     Если в поле listen указан порт:

     В файле `/etc/nginx/conf.d/iwtm-pda.location` измените значение поля `fastcgi_pass` на скопированное значение поля `listen`.

     Если в поле listen указан Unix-сокет:

     a. Удалите символ `;` в следующих строках, чтобы раскомментировать их:

     ```
     ;listen.owner = nobody
     ;listen.group = nobody
     ```

     b. Измените значения параметров `listen.owner` и `listen.group` на `iwtm`
     c. Закомментируйте строку `listen.acl_users = apache,nginx` при помощи символа `;`
     d. В файле `/etc/nginx/conf.d/iwtm-pda.location` измените значение поля `fastcgi_pass` на скопированное значение поля `listen`, вставив `unix:` перед значением:

     ```
     unix:/<ваш_путь>/<имя_сокета>.sock
     ```

На сервере под управлением РЕД ОС:

a. Перейдите в файл `/etc/php-fpm.d/www.conf`.
b. Измените значение поля `listen` на `127.0.0.1:9001`.

8. Настройте доступ PHP-FPM к общей временной директории `/tmp`. Для этого:
   a. Откройте на редактирование файл `/etc/systemd/system/php-fpm.service.d/override.conf`. Если файл отсутствует, создайте его.
   b. В блоке `[Service]` укажите значение `false` для параметра `PrivateTmp`. Если блок `[Service]` отсутствует, добавьте в файл следующие строки:

```
[Service]
PrivateTmp=false
```

9. Смените пользователя и группу PHP-FPM на `iwtm`. Для этого:
   a. Откройте на редактирование файл `/etc/php-fpm.d/www.conf`.
   b. Измените значения параметров `user` и `group` на `iwtm`.
10. Перезапустите PHP-FPM и проверьте, что сервис запустился. Используйте команду:

```
systemctl restart php-fpm && systemctl status php-fpm
```

11. В файле `override.conf` укажите корректный путь до PHP и задайте параметр окружения. Для этого:
    a. Откройте на редактирование файл `/etc/systemd/system/iw_pda.service.d/override.conf`.
    b. В указанной строке измените путь до PHP на используемый вашим сервером:

```
ExecStart=/opt/iw/tm5/bin/iw_pda -p /opt/iw/tm5/etc
```

    c. В блоке `[Service]` укажите корректное значение переменной `Environment`, заменив `https://127.0.0.1` на внешний IP-адрес или доменное имя сервера.
    d. Если необходимо использовать более сложное шифрование паролей, используйте параметр `PDA_SALT`. Укажите в значении соль в формате строки произвольной длины, содержащей любые символы. Например:

```
Environment="PDA_SALT=P%gL1;T:9dR32M6n"
```

    e. Сохраните изменения и обновите сервис с помощью команды:

```
systemctl daemon-reload
```

12. Настройте HTTPS-сервер:
    a. Откройте на редактирование файл `/etc/nginx/conf.d/nginx.pda.conf`.
    b. Раскомментируйте следующие строки, удалив символ `#`:

```
# ssl_certificate     /opt/iw/tm5/etc/certification/web-server.pem;
# ssl_certificate_key /opt/iw/tm5/etc/certification/web-server.key;
# listen 443 ssl;
```

    c. В раскомментированных строках для параметров `ssl_certificate` и `ssl_certificate_key` укажите полный путь до файлов с вашими сертификатом и ключом, используемых для работы веб-сервера NGINX по SSL.

13. Создайте symlink-файл из папки бинарных файлов Traffic Monitor на бинарный файл установленного 7-Zip:

```
ln -s /usr/bin/7z /opt/iw/tm5/bin/7zz
```

14. Перезапустите NGINX и убедитесь, что сервис запустился. Используйте команду:

```
systemctl restart nginx && systemctl status nginx
```

15. Смените владельца папки `/var/log/infowatch` на `iwtm` с помощью команды:

```
chown iwtm:iwtm /var/log/infowatch
```

16. В настройках сетевого экрана проверьте, что к нему можно подключаться по HTTP/HTTPS.
17. Разрешите подключение к HTTP-скриптам и модулям. Используйте команду:

```
setsebool -P httpd_can_network_connect 1
```

18. В файле `/opt/iw/tm5/etc/pda.conf` укажите значения параметров согласно статье *Настройки адаптера в файле `pda.conf`*.
19. На сервере с базой данных отредактируйте файлы:
    - В файле `/u01/postgres/pg_hba.conf` в поле `METHOD` укажите значения:
        - в разделе `# IPv4 local connections`:
            - значение `trust`;
        - в разделе `# IPv6 local connections`:
            - значение `md5`;
        - в разделе `# Allow replication connections from localhost, by a user with the replication privilege`:

        - в строке `host postgres` значение `trust`.
    - В файле `/u01/postgres/postgresql.conf` для параметра `password_encryption` укажите значение `md5`.
20. Запустите миграцию адаптера от имени пользователя `iwtm` с помощью команды:

```
su -c 'php /opt/iw/tm5/www/pda/pda migrate -p /opt/iw/tm5/etc' iwtm
```

> **Примечание:**
>
> Пользователь `iwtm` создается автоматически при установке RPM-пакета адаптера.

21. Если необходимо, измените шаблоны почтовых уведомлений отправителю письма и отображение страницы ввода пароля. См. статьи *Настройки шаблонов уведомлений*, *Настройки страницы ввода пароля*.
22. Если вы хотите добавить пароли в базу паролей, внесите их в таблицу `custom_password` базы данных. Подробнее см. статью *База паролей InfoWatch Password Disclosure Adapter*.

> **Примечание:**
>
> Для работы с базой данных рекомендуется использовать инструменты администрирования DBeaver или pgAdmin. При подключении к базе данных выберите схему `pda`.

23. Запустите прослушивание новых событий от имени системного администратора с помощью команды:

```
systemctl start iw_pda
```

24. Убедитесь, что адаптер запущен:

```
systemctl status iw_pda
```

В случае успешного запуска отобразится статус `active (running)`.

5.2.2 Установка адаптера на отдельный сервер под управлением ОС Astra Linux

Чтобы установить адаптер и настроить его перед запуском:

1. Установите скриптовый язык PHP с расширениями при помощи команды:

```
sudo apt install php8.1-common php8.1-cli php8.1-pgsql php8.1-xml php8.1-redis php8.1-phpdbg php8.1-mbstring php8.1-msgpack php8.1-fpm php-mailparse
```

> **Важно!**
>
> Если какой-либо пакет отсутствует в официальном репозитории, используйте пакет из внешнего дополнительного репозитория, предварительно подключив репозиторий к ОС.

2. Убедитесь, что вместе с PHP установлены модули:
   - `php-mbstring`
   - `php-process`
   - `php-curl`

   Чтобы проверить список установленных модулей, используйте команду:

```
php -m
```

   Если какой-то из модулей не был установлен, установите пакет отдельно.
3. Установите дополнительные пакеты NGINX, Redis, QPDF и P7zip с плагинами при помощи команды:

```
sudo apt install nginx redis qpdf p7zip python3-pip
```

4. Поместите на сервер в директорию `/root/debs` поставляемые пакеты:
   - `<iwtm-pda>.deb`
   - `<iwtm-msoffcrypto-tool>.deb`

   > **Примечание:**
   >
   > Здесь и далее `<iwtm-pda>`, `<iwtm-msoffcrypto-tool>` – полные названия файлов.

5. Перейдите в директорию с DEB-файлами и установите библиотеку `msoffcrypto` и адаптер. Используйте команду:

```
dpkg -i <iwtm-msoffcrypto-tool>.deb <iwtm-pda>.deb
```

6. Смените пользователя NGINX на `iwtm`. Для этого:
   a. Откройте на редактирование файл `/etc/nginx/nginx.conf`.
   b. Измените значение поля `user` на `iwtm`.

7. Приведите порты PHP-FPM и Password Disclosure Adapter к одному значению или используйте Unix-сокет.

> **Примечание:**
>
> Для Password Disclosure Adapter по умолчанию используется 9001 порт. В зависимости от версии, для PHP-FPM по умолчанию может использоваться 9000 порт или Unix-сокет.

   a. Перейдите в файл `/etc/php/8.1/fpm/pool.d/www.conf`.
   b. Выберите один из способов настройки:
      - Измените значение поля `listen` на `127.0.0.1:9001`.
        или
      - Скопируйте значение поля `listen` в файле `www.conf`.

      Если в поле listen указан Unix-сокет:

         i. Удалите символ `;` в следующих строках, чтобы раскомментировать их:

```
;listen.owner = nobody
;listen.group = nobody
```

         ii. Измените значения параметров `listen.owner` и `listen.group` на `iwtm`
         iii. Закомментируйте строку `listen.acl_users = apache,nginx` при помощи символа `;`
         iv. В файле `/etc/nginx/conf.d/iwtm-pda.location` измените значение поля `fastcgi_pass` на скопированное значение поля `listen`, вставив `unix:` перед значением:

```
unix:/<ваш_путь>/<имя_сокета>.sock
```

      Если в поле listen указан порт:

      В файле `/etc/nginx/conf.d/iwtm-pda.location` измените значение поля `fastcgi_pass` на скопированное значение поля `listen`.

8. Настройте доступ PHP-FPM к общей временной директории `/tmp`. Для этого:
   a. Откройте на редактирование файл `/etc/systemd/system/php-fpm.service.d/override.conf`. Если файл отсутствует, создайте его.
   b. В блоке `[Service]` укажите значение `false` для параметра `PrivateTmp`. Если блок `[Service]` отсутствует, добавьте в файл следующие строки:

```
[Service]
PrivateTmp=false
```

9. Смените пользователя и группу PHP-FPM на `iwtm`. Для этого:
   a. Откройте на редактирование файл `etc/php/8.1/fpm/pool.d/www.conf`.

b. Измените значения параметров `user` и `group` на `iwtm`.

10. Перезапустите PHP-FPM и проверьте, что сервис запустился. Используйте команду:

```
systemctl restart php8.1-fpm && systemctl status php8.1-fpm
```

11. В файле **`override.conf`** укажите корректный путь до PHP и задайте параметр окружения. Для этого:
    a. Откройте на редактирование файл `/etc/systemd/system/iw_pda.service.d/`**`override.conf`**.
    b. В указанной строке измените путь до PHP на используемый вашим сервером:

```
ExecStart=/opt/iw/tm5/bin/iw_pda -p /opt/iw/tm5/etc
```

    c. В блоке `[Service]` укажите корректное значение переменной `Environment`, заменив `https://127.0.0.1` на внешний IP-адрес или доменное имя сервера.
    d. Если необходимо использовать более сложное шифрование паролей, используйте параметр `PDA_SALT`. Укажите в значении соль в формате строки произвольной длины, содержащей любые символы. Например:

```
Environment="PDA_SALT=P%gL1;T:9dR32M6n"
```

    e. Сохраните изменения и обновите сервис с помощью команды:

```
systemctl daemon-reload
```

12. Настройте HTTPS-сервер:
    a. Откройте на редактирование файл `/etc/nginx/sites-enabled/`**`nginx.pda`**.
    b. Закомментируйте следующие строки при помощи символа `#`:

```
gzip on;
gzip_types application/javascript text/css text/xml application/octet-stream;
gzip_disable "msie6";
gzip_static on;
```

    c. Раскомментируйте следующие строки, удалив символ `#`:

```
# ssl_certificate     /opt/certification/web-server.pem;
# ssl_certificate_key /opt/certification/web-server.key;
# listen 443 ssl;
```

d. В раскомментированных строках для параметров `ssl_certificate` и `ssl_certificate_key` укажите полный путь до файлов с вашими сертификатом и ключом, используемых для работы веб-сервера NGINX по SSL.

13. Создайте symlink-файл из папки бинарных файлов Traffic Monitor на бинарный файл установленного 7-Zip:

```
ln -s /usr/bin/7z /opt/iw/tm5/bin/7zz
```

14. Перезапустите NGINX и убедитесь, что сервис запустился. Используйте команду:

```
systemctl restart nginx && systemctl status nginx
```

15. Смените владельца папки `/var/log/infowatch` на `iwtm` с помощью команды:

```
chown iwtm:iwtm /var/log/infowatch
```

16. В настройках сетевого экрана проверьте, что к нему можно подключаться по HTTP/HTTPS.

17. В файле `/opt/iw/tm5/etc/pda.conf` укажите значения параметров согласно статье *Настройки адаптера в файле `pda.conf`*.
18. Запустите миграцию адаптера от имени пользователя `iwtm` с помощью команды:

```
su -c 'php /opt/iw/tm5/www/pda/pda migrate -p /opt/iw/tm5/etc' iwtm
```

> **Примечание:**
>
> Пользователь `iwtm` создается автоматически при установке DEB-пакета адаптера.

19. Если необходимо, измените шаблоны почтовых уведомлений отправителю письма и отображение страницы ввода пароля. См. статьи *Настройки шаблонов уведомлений*, *Настройки страницы ввода пароля*.
20. Если вы хотите добавить пароли в базу паролей, внесите их в таблицу `custom_password` базы данных. Подробнее см. статью *База паролей InfoWatch Password Disclosure Adapter*.

    > **Примечание:**
    >
    > Для работы с базой данных рекомендуется использовать инструменты администрирования DBeaver или pgAdmin. При подключении к базе данных выберите схему `pda`.

21. Запустите прослушивание новых событий от имени системного администратора с помощью команды:

    ```
    systemctl start iw_pda
    ```

22. Убедитесь, что адаптер запущен:

    ```
    systemctl status iw_pda
    ```

    В случае успешного запуска отобразится статус `active (running)`.

6 Обновление InfoWatch Password Disclosure Adapter

> **Важно!**
>
> Действия по обновлению адаптера выполняются от имени системного администратора.

Чтобы обновить адаптер:

1. Остановите процесс с помощью команды:

   ```
   systemctl stop iw_pda
   ```

2. Скопируйте новые версии пакетов `iwtm-pda` и `iwtm-msoffcrypto-tool`:

   > **Примечание:**
   >
   > Здесь и далее `<iwtm-pda>` и `<iwtm-msoffcrypto-tool>` – полные названия файлов.
   >
   > При наличии пакетов для разных ОС убедитесь, что вы используете файлы именно для вашей ОС.

   - на сервере под управлением ОС RHEL и РЕД ОС в директорию `/root/rpms`:
     - `<iwtm-pda>.rpm`
     - `<iwtm-msoffcrypto-tool>.rpm`
   - на сервере под управлением ОС Astra Linux в директорию `/root/debs`:
     - `<iwtm-pda>.deb`
     - `<iwtm-msoffcrypto-tool>.deb`

3. Запустите команду обновления адаптера и `iwtm-msoffcrypto-tool`:

   На сервере под управлением ОС RHEL или РЕД ОС:

   ```
   rpm -U <iwtm-msoffcrypto-tool>.rpm <iwtm-pda>.rpm
   ```

   На сервере под управлением ОС Astra Linux:

   ```
   sudo apt install ./<iwtm-msoffcrypto-tool>.deb ./<iwtm_pda>.deb
   ```

4. Если вы обновляете адаптер на сервере под управлением ОС RHEL или РЕД ОС, проверьте наличие файла `/opt/iw/tm5/etc/pda.conf.rpmnew`. Если:
   - файл отсутствует, то ваша версия файла `pda.conf` актуальна. Переходите к шагу 4;
   - файл присутствует, то в новой версии адаптера появились дополнительные настройки. Обновите файл `pda.conf`, создав резервную копию существующих настроек:
     a. Переименуйте файл `pda.conf` в `pda.conf.old`.
     b. Из файла `pda.conf.old` перенесите значения аналогичных полей настроек в новый файл `pda.conf.rpmnew`.

c. Переименуйте **`pda.conf.rpmnew`** в **`pda.conf`**.

> **Примечание:**
>
> Конфигурационный файл **`pda.conf.rpmnew`** создается автоматически после запуска команды обновления. Обязательное условие создания файла – наличие изменений в файле **`pda.conf`** новой версии адаптера.

5. Выполните миграцию от имени пользователя `iwtm`. В ходе миграции установятся схемы и таблицы и будут первоначально заполнены данные:

```
/opt/iw/tm5/bin/php /opt/iw/tm5/www/pda/pda migrate -p /opt/iw/tm5/etc
```

6. Убедитесь в корректности настроек HTTPS-сервера в файле `/etc/nginx/conf.d/` **`nginx.pda.conf`**.
7. Запустите адаптер с помощью команды:

```
systemctl start iw_pda
```

7 Настройки InfoWatch Password Disclosure Adapter

Вы можете задать следующие настройки адаптера:

- подключение к Traffic Monitor, базе данных адаптера и серверу очередей Redis;
- SMTP-подключение для отправки уведомлений адаптером, а также настройка шаблонов уведомлений;
- количество процессов и другие.

Описание представлено в статьях раздела:

- Обязательные настройки:
  - Настройки адаптера в файле `pda.conf`
- Опциональные настройки:
  - База паролей InfoWatch Password Disclosure Adapter
  - Настройки шаблонов уведомлений
  - Настройки страницы ввода пароля

7.1 Настройки адаптера в файле pda.conf

Данная статья описывает настройки адаптера, которые содержатся в файле `/opt/iw/tm5/etc/pda.conf`.

Обязательно укажите значения параметров в следующих разделах:

- Подключение к серверу Traffic Monitor – раздел `TM`
- Подключение к серверу Traffic Monitor – раздел `Pushapi` (в случае установки адаптера на отдельном сервере)
- Подключение к базе данных PostgreSQL – раздел `Database`
- Подключение к серверу очередей Redis – раздел `Redis`
- Почтовые уведомления – раздел `SMTP`
- Почтовые уведомления – раздел `Templates`

Опциональные настройки:

- Синхронизация и быстродействие – раздел `Worker`
- Логирование – раздел `Logging`
- Хранение расшифрованных данных – раздел `ContentStorage`

7.1.1 Подключение к серверу Traffic Monitor

Раздел `TM`

В разделе указаны настройки получения событий с сервера Traffic Monitor.

Необходимо ввести корректные значения параметров:

- `Url` (в случае установки адаптера на отдельном сервере)
- `Token`
- `Tags`

Поле	Описание
`Url`	Имя или IP-адрес хоста, на котором установлен TM и с которого адаптер получает события Значение по умолчанию: `https://127.0.0.1` **Примечание:** Ссылка на событие в письме Офицеру безопасности ведет на хост с этим адресом.
`Token`	Токен доступа в TM **Примечание:** Токен отображается при подключении плагина в Консоли управления Traffic Monitor. Подробнее см. статью *Добавление лицензии и получение токена плагина для InfoWatch Traffic Monitor*.
`Tags`	ID тега для фильтрации событий, получаемых адаптером. Вставьте ID всех тегов, при наличии которых адаптер должен получать события из Traffic Monitor. Чтобы добавить несколько тегов, перечислите их в массиве: • каждый тег указывайте в двойных кавычках; • используйте запятую в качестве разделителя. **Пример:** `"Tags": [ "3A912F1381B241CEA07CE1DA53EF552D00000000", "329573FF216C43B6B976808C73529B6300000000" ]` **Важно!** При работе с адаптером рекомендуется использовать теги. В случае, если не указан тег в политике Traffic Monitor и/или настройках PDA, адаптер получает из Traffic Monitor все события электронной почты с вердиктом *Карантин*, что может негативно влиять на производительность Системы. Подробнее о фильтрации событий см. *Настройка политики Traffic Monitor для работы InfoWatch Password Disclosure Adapter*.

Раздел `Pushapi`

В разделе указаны параметры подключения к серверу, на котором установлен Traffic Monitor и на который адаптер будет присылать события.

Большинство значений заданы по умолчанию. В случае установки адаптера на отдельном сервере, измените значение параметра `Host`.

Поле	Описание
`Host`	IP-адрес или имя хоста сервера Traffic Monitor, на который адаптер отправляет события Значение по умолчанию: `127.0.0.1`
`Name`	Имя сервиса Значение по умолчанию: `iw-xapi-puppy`

Поле	Описание
`Port`	Порт сервера Значение по умолчанию: `9101`
`UserName`	Имя пользователя для входа в службу Consul Значение по умолчанию: `consul_client` **Примечание:** Подробнее о службе см. *InfoWatch Traffic Monitor. Руководство администратора. Настройка межсервисного взаимодействия (служба Consul)*.

7.1.2 Подключение к базе данных PostgreSQL

Раздел `Database`

Необходимо ввести значения всех полей, как представлено в таблице ниже:

Поле	Описание
`Database`	Используемая СУБД Значение по умолчанию: `postgres`
`Driver`	Драйвер для взаимодействия с СУБД Значение по умолчанию: `pgsql`
`Host`	IP-адрес сервера, на котором развернута базы данных Значение по умолчанию: `127.0.0.1`
`Password`	Пароль пользователя
`Port`	Порт базы данных Значение по умолчанию: `5433`
`Schema`	Схема базы данных, используемая адаптером Значение по умолчанию: `pda`
`UserName`	Имя пользователя в базе данных

7.1.3 Подключение к серверу очередей Redis

Раздел `Redis`

Необходимо ввести значения всех полей:

Поле	Описание
`Host`	IP-адрес сервера Redis Значение по умолчанию: `127.0.0.1`
`Port`	Порт подключения к Redis Значение по умолчанию: `6379`

7.1.4 Почтовые уведомления

Раздел `SMTP`

Чтобы настроить почтовый сервер для отправки уведомлений, определите значения перечисленных параметров. Параметры `L ogin` и `Password` обязательны в случае шифрования SMTP-трафика, которое используется по умолчанию.

Поле	Описание
`Host`	SMTP-сервер, используемый для отправки уведомлений Значение по умолчанию: `127.0.0.1`
`Login`	Имя учетной записи, имеющей доступ к почтовому серверу. Знак обратного слэша необходимо экранировать **Пример:** `Login": "domain\\username"`
`Password`	Пароль учетной записи, имеющей доступ к почтовому серверу
`Port`	Порт, используемый для отправки уведомлений Значение по умолчанию: `25`
`Security`	Включить/выключить шифрование. Выбор из значений: • `1` – включить (по умолчанию) • `0` – выключить

Раздел `Templates`

Укажите адреса электронной почты Офицера безопасности и отправителя уведомлений, и, если вы настроили собственные шаблоны почтовых уведомлений, отправляемых адаптером, укажите пути до шаблонов. Если вы используете шаблоны уведомлений по умолчанию, указывать пути до них не требуется. О настройке шаблонов см. *Настройки шаблонов уведомлений*.

> **Примечание:**
>
> Пути до шаблонов необходимо указывать относительно директории `/opt/iw/tm5/www/pda/etc/templates/`. Например, если шаблоны расположены в директории `/opt/iw/tm5/www/pda/etc/templates/custom_notifications`, указывайте `custom_notifications/<имя_файла>.twig`.

Поле	Описание
`OfficerEmail`	Адрес электронной почты Офицера безопасности, который получает уведомления от адаптера. Чтобы добавить несколько адресов, перечислите их в массиве: • каждый адрес указывайте в двойных кавычках; • используйте запятую в качестве разделителя. **Пример:** `"OfficerEmail": [ "security.officer@company.ru", "petr.ivanov@company.ru", "viktor.evdokimov@company.ru" ]`
`OfficerSubjectTemplate`	Путь к тексту темы почтового уведомления, отправляемого Офицеру безопасности, с информацией о событии с расшифрованным файлом
`OfficerTemplate`	Путь к шаблону уведомления, отправляемого Офицеру безопасности, с информацией о событии с расшифрованным файлом
`PdaUrl`	Ссылка на страницу ввода пароля. Отображается в уведомлении отправителю. Значение по умолчанию: `https://127.0.0.1`
`SenderEmail`	Адрес электронной почты, который используется в качестве отправителя уведомления
`SenderSubjectTemplate`	Путь к тексту темы почтового уведомления о необходимости предоставить пароль, присылаемого отправителю письма с зашифрованными вложениями

Поле	Описание
`SenderTemplate`	Путь к шаблону почтового уведомления о необходимости предоставить пароль, присылаемого отправителю письма с зашифрованными вложениями
`UnsupportedSubjectTemplate`	Путь к тексту темы почтового уведомления, присылаемого отправителю письма с зашифрованными вложениями, о том, что письмо не было доставлено
`UnsupportedTemplate`	Путь к шаблону почтового уведомления, присылаемого отправителю письма с зашифрованными вложениями, о том, что письмо не было доставлено

7.1.5 Синхронизация и быстродействие

Раздел `Worker`

Значения параметров заданы по умолчанию. При необходимости вы можете изменить их.

Поле	Описание
`ListenTimeout`	Интервал времени обращения адаптера к Traffic Monitor для того, чтобы получить события Значение по умолчанию: `900` (в секундах)
`ParallelCount`	В параметре записывается количество потоков, которые занимает адаптер. Увеличение количества занимаемых потоков ведет к ускорению адаптера. Количество потоков не должно превышать количество ядер или быть слишком малым. Значение по умолчанию: `8`
`SyncTimeout`	Интервал времени, в течение которого адаптер проверяет, пришло ли сгенерированное адаптером событие на анализ в TM. Параметр необходим для прослушивания аудита Traffic Monitor на предмет изменений пользовательского решения по исходному или сгенерированному адаптером событиям. Значение по умолчанию: `60` (в секундах)
секция `RetryStrategy`	Повторная обработка операций, завершившихся с ошибкой (например, отправки письма отправителю)
`MaxRetries`	Максимальное количество попыток Значение по умолчанию: `10`
`Delay`	Длительность первого интервала перед следующей попыткой Значение по умолчанию: `5` (в секундах)

Поле	Описание
`Multiplier`	Во сколько раз увеличивается каждый следующий интервал. Например, при `"Delay": 5` и `"Multiplier": 2`, интервал ожидания перед каждой следующей попыткой возрастает в два раза: 5, 10, 20, 40 и т.д. Значение по умолчанию: `2`
`MaxDelay`	Максимальное значение интервала Значение по умолчанию: `3600` (в секундах)

7.1.6 Логирование

Раздел `Logging`

Значения параметров заданы по умолчанию. При необходимости вы можете изменить их.

Поле	Описание
`DefaultDirectory`	Директория файла с логами Значение по умолчанию: `/var/log/infowatch/`
`FileName`	Имя файла с логами Значение по умолчанию: `pda.log`
`GlobalLevel`	Выбор режима: • `warning` (по умолчанию) • `debug`

7.1.7 Хранение расшифрованных данных

Раздел `ContentStorage`

Значения параметров заданы по умолчанию. При необходимости вы можете изменить их.

Поле	Описание
`MinDiskFreeSize`	Количество дискового пространства, используемого для хранения расшифрованных данных. При достижении указанного числа удаляются более старые файлы. Значение по умолчанию: `1073741824` байт (1024 МБ)
`Path`	Директория с расшифрованными данными. По умолчанию данные хранятся в `/tmp`.

7.2 База паролей InfoWatch Password Disclosure Adapter

Адаптер использует базу паролей для подбора пароля к зашифрованному файлу. База паролей состоит из:

- паролей, внесенных Офицером безопасности. Такие пароли хранятся в открытом виде;
- паролей, введенных по запросу адаптера отправителями файлов. Адаптер сохраняет правильные пароли, применяя шифрование с привязкой к хешу файла, имени файла и отправителю.

Если в базе отсутствуют пароли, внесенные Офицером безопасности, то адаптер использует только сохраненные пароли, которые были введены отправителями ранее.

Чтобы добавить пароли в базу паролей, внесите их в таблицу `custom_password` базы данных по одному на строку перед запуском адаптера.

> **Важно!**
>
> Количество паролей, внесенных Офицером безопасности, влияет на производительность адаптера. Оптимальное число не должно превышать 1000.

7.3 Настройки шаблонов уведомлений

Шаблоны уведомлений по электронной почте, используемые Системой по умолчанию, доступны в директории `/opt/iw/tm5/www/pda/etc/templates/notifications/` :

- Тексты тем уведомлений:
  - `officer_subject.twig` – текст темы уведомления, отправляемого Офицеру безопасности, с информацией о событии с расшифрованным файлом;
  - `sender_subject.twig` – текст темы уведомления о необходимости предоставить пароль, присылаемого отправителю письма с зашифрованными вложениями;
  - `unsupported_subject.twig` – текст темы уведомления, присылаемого отправителю письма с зашифрованными вложениями, о том, что письмо не было доставлено.
- Шаблоны уведомлений:
  - `officer.twig` – шаблон уведомления, отправляемого Офицеру безопасности, с информацией о событии с расшифрованным файлом;
  - `sender.twig` – шаблон уведомления о необходимости предоставить пароль, присылаемого отправителю письма с зашифрованными вложениями;
  - `unsupported.twig` – шаблон уведомления, присылаемого отправителю письма с зашифрованными вложениями, о том, что письмо не было доставлено.

Вы можете изменить текст уведомлений, присылаемых адаптером Офицеру безопасности и отправителю письма с зашифрованным вложением. Для этого:

1. Создайте папку в директории `/opt/iw/tm5/www/pda/etc/templates/` , в нашем примере – `custom_notifications` .
2. Скопируйте файлы из папки `notifications` в папку `custom_notifications` .
3. Отредактируйте файлы. При этом учтите, что:
   - Тексты тем уведомлений содержат лишь текстовую строку.

- Шаблоны уведомлений представлены в формате HTML-файлов. В шаблонах используются параметры, чьи значения адаптер подставляет в текст сообщений при отправке.
  Вы можете отредактировать:
  - Оформление письма в секции `<head>` → `<style>`.
  - Текст и отображение значений параметров в секции `<body>`.

4. В файле `pda.conf` укажите пути к новым шаблонам относительно директории `/opt/iw/tm5/www/pda/etc/templates/`. Подробнее см. *Настройки адаптера в файле pda.conf*.

7.3.1 Параметры, используемые в шаблонах уведомлений

В таблице представлены используемые в тексте шаблонов параметры, которые адаптер заменяет на данные событий при отправке уведомления.

Параметр	Описание
`tm_url`	Адрес для просмотра расшифрованных событий в Консоли Traffic Monitor
`url`	Адрес веб-интерфейса для ввода пароля
`subject`	Тема письма
`date`	Дата письма
`filenames`	Приложенные зашифрованные файлы
`senders`	Отправители
`recipients`	Получатели
`object_id`	Событие
`new object_id`	Сгенерированное событие

Параметры `filenames`, `senders` и `recipients` – массивы. Их значения могут быть перечислены:

- Через запятую. Для этого используйте запись вида:

```
{{ <массив>|join(', ') }}
```

Пример:

- Фрагмент разметки в шаблоне:

```
Получатели письма: {{ recipients|join(', ') }}.
```

- Фрагмент текста в отправленном сообщении:

  Получатели письма: Контакт из события: petr.sorokin@company.com (Электронная почта), Контакт из события: vera.belova@company.com (Электронная почта).

- Списком. Для этого используйте запись вида:

```
<ul>
    {% for i in <массив> %}
        <li>{{ i }}</li>
    {% endfor %}
</ul>
```

Пример:

- Фрагмент разметки в шаблоне:

```
Вложения:
<ul>
    {% for filename in filenames %}
        <li>{{ filename }}</li>
    {% endfor %}
</ul>
```

- Фрагмент текста в отправленном сообщении:

  Вложения:

  - Расчетный счет.docx
  - номера-карт.zip
  - список_клиентов.rar
  - Годовой_план.pdf

7.4 Настройки страницы ввода пароля

Вы можете настроить отображение страницы ввода пароля: изменить акцентный цвет, добавить логотип и контактную информацию. Для этого:

1. В директории `/opt/iw/tm5/www/pda/frontend/custom/` создайте файл `config.json`.
2. Из файла `config.json.example`, расположенного в этой же директории, скопируйте в `config.json` блок с параметрами. Убедитесь, что вы не переносите в файл блок с комментарием.
3. Если необходимо добавить логотип, поместите файл с изображением в директорию `/opt/iw/tm5/www/pda/frontend/`.
4. В файле `config.json` измените значения параметров согласно таблице. Любой параметр опционален и может быть удален.

Параметр	Описание
`accentColor`	Акцентный цвет страницы в формате HEX Пример: `#3f51b5`

`phones`
`emails`
	Список телефонных номеров/электронных адресов для связи. Вы можете указать несколько значений в виде массива строк. В качестве разделителя используйте запятую
	Примеры:
	`["+1 (234) 56-789-01", "+1 (234) 56-789-02"]`
	`["support@support.example", "support1@support.example"]`

`logo`	Путь к файлу с логотипом. Укажите путь относительно директории `/opt/iw/tm5/www/pda/frontend/` Пример: `/custom/logo.svg`

5. Сохраните изменения.

8 Настройка политики Traffic Monitor для работы InfoWatch Password Disclosure Adapter

Примечание:

В статье представлены настройки, имеющие непосредственное отношение к перехвату зашифрованных данных. Чтобы задать дополнительные настройки, смотрите *InfoWatch Traffic Monitor. Руководство пользователя. Создание политики защиты данных*.

Пример условий, при которых адаптер получает события из Traffic Monitor:

- тип *Электронная почта*;
- отправитель входит в периметр *Компания*;
- вердикт *Карантин*[1];
- добавленный тег[2];
- зашифрованный файл поддерживаемого формата во вложении.

Важно!

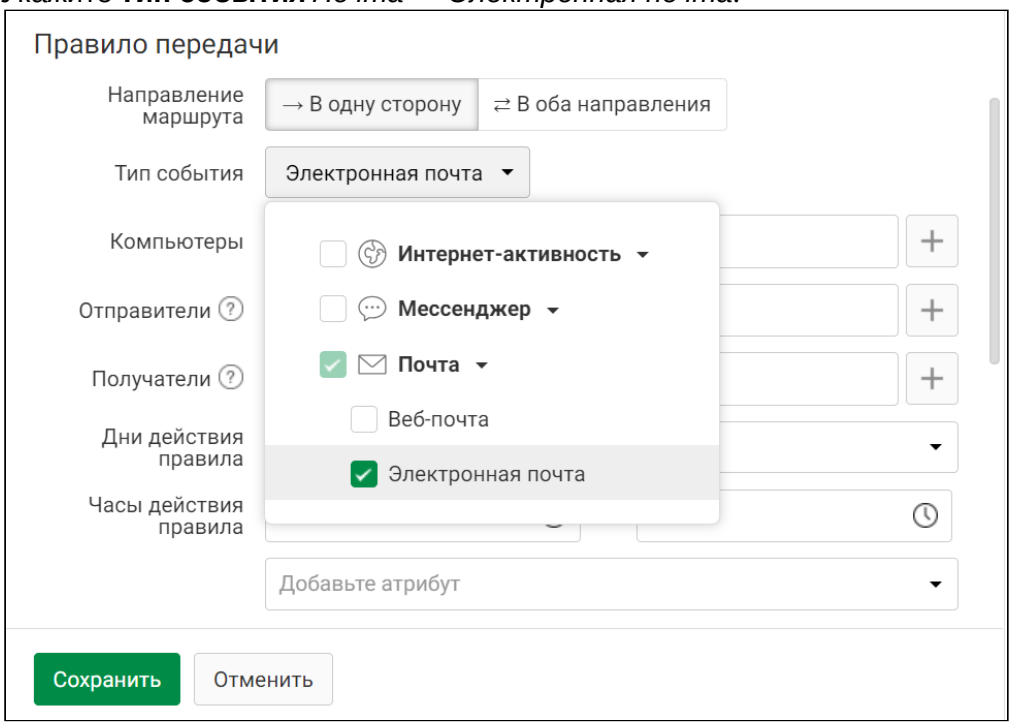
[1] Для корректной работы адаптера необходимо указать вердикт *Карантин* как при перехвате трафика в режиме блокировки "в разрыв", так и при режиме скрытых копий. В последнем случае вердикт не влияет на пересылку трафика. См. *Схема работы InfoWatch Password Disclosure Adapter*.

[2] При работе с адаптером рекомендуется использовать теги. В случае, если не указан тег в политике Traffic Monitor и/или настройках PDA, адаптер получает из Traffic Monitor все события электронной почты, попавшие в карантин, что может негативно влиять на производительность Системы.

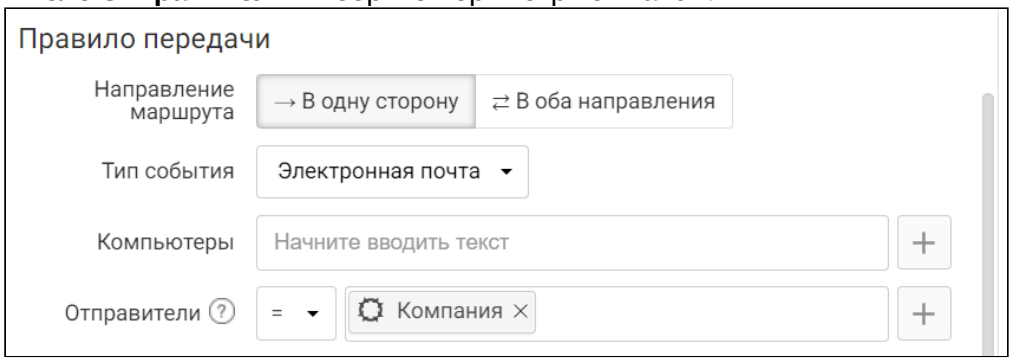
Чтобы настроить политику Traffic Monitor для перехвата событий с перечисленными условиями:

1. Войдите в Консоль управления Traffic Monitor.
2. Перейдите в раздел **Политики**.
3. В верхней части рабочей области нажмите **Добавить политику** и в раскрывающемся списке выберите **Политика защиты данных**. Новая политика будет добавлена в группу **Политики защиты данных**, а в правой части рабочей области отобразится форма добавления политики. В панели редактирования справа измените имя политики, например, на *Политика Password Disclosure Adapte*r.
4. В панели редактирования политики нажмите **Добавить правило** и выберите **Правило передачи**.

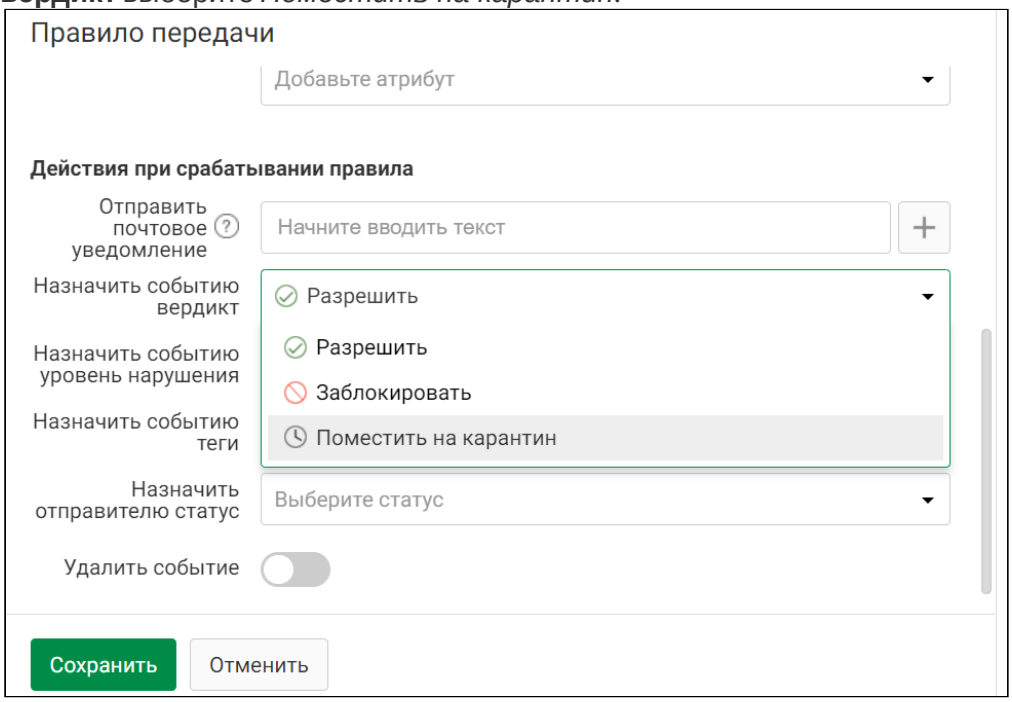
5. Укажите **Тип события** *Почта → Электронная почта*:



6. В поле **Отправители** выберите периметр *Компания*:



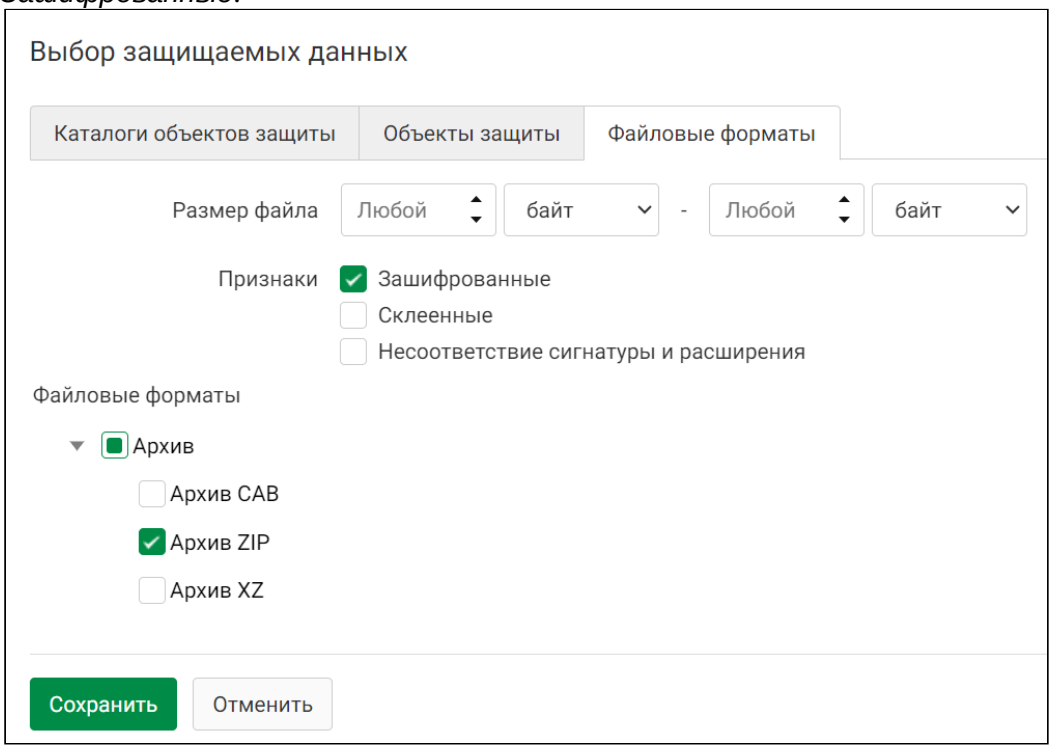
7. В разделе **Действия при срабатывании правила** в поле **Назначить событию вердикт** выберите *Поместить на карантин*:



> **Примечание:**
>
> Если настроена блокировка почтового трафика "в разрыв", и вы хотите, чтобы Система уведомляла отправителя письма о том, что письмо было помещено в карантин, заблокировано или покинуло карантин, в поле **Отправить почтовое уведомление** выберите *Уведомление отправителю.*
>
> Подробнее о настройке уведомлений см. *InfoWatch Traffic Monitor. Руководство пользователя. Настройка уведомлений*.

8. Нажмите **Сохранить**. В поле **Защищаемые данные** нажмите **Выбрать**.

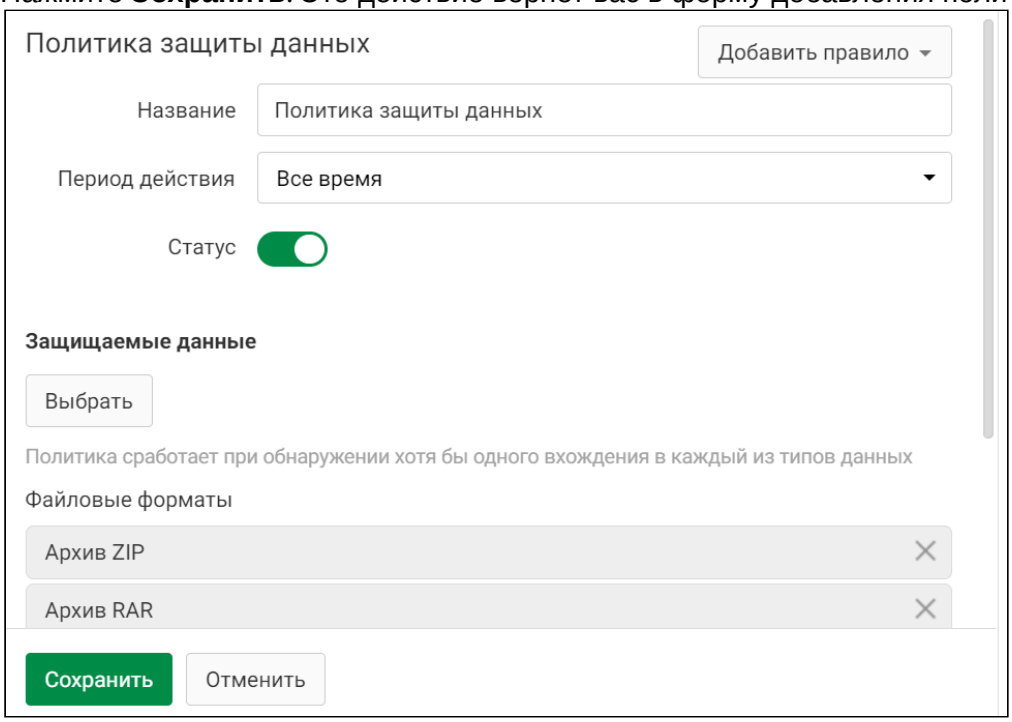
9. В разделе **Файловые форматы** в поле **Признаки** установите флажок для значения *Зашифрованные*:



10. В поле **Файловые форматы** установите флажки:
    - в секции *Архив* для значений *Архив ZIP*, *Архив RAR*, *Архив 7zip*;
    - в секции *Другие форматы* для значения *Файл-контейнер Microsoft*;
    - в секции *Текст* для значения *Документ Adobe Acrobat*.

> **Примечание:**
>
> Значение *Файл-контейнер Microsoft* используется для форматов DOC, DOCX, PPT, PPTX, XLS, XLSX, XLSM и XLSB.
>
> Значение *Документ Adobe Acrobat* используется для формата PDF.

11. Нажмите **Сохранить**. Это действие вернет вас в форму добавления политики:



12. Нажмите **Сохранить**.
13. Настройте фильтрацию получаемых событий по тегу:
    a. В Консоли управления Traffic Monitor добавьте новый тег. Подробнее см. документ *InfoWatch Traffic Monitor. Руководство пользователя. Работа с тегами*.
    b. Из колонки `tag_id` таблицы `tag` базы данных Traffic Monitor скопируйте ID добавленного тега.
    c. В файле `/opt/iw/tm5/etc/pda.conf` вставьте ID тега в качестве значения параметра `Tags` в разделе `TM`.
    d. Укажите данный тег при настройке политики в разделе **Действия при срабатывании правила** в поле **Назначить событию теги**.

8.1 Правила пересылки защищенных и незащищенных данных

Если настроена блокировка почтового трафика "в разрыв", Traffic Monitor может применять разные правила к событиям с одними и теми же данными, пересылаемыми в защищенном и открытом виде. Для этого используйте атрибут *Расшифрованные данные*.

Например, необходимо:

- Разрешать пересылку информации по счетам в файлах, защищенных паролем;
- Запрещать пересылку информации по счетам в открытом виде;
- Запрещать пересылку стратегии компании в любом виде.

Для этого:

1. Создайте политику для адаптера и настройте ее таким образом, чтобы Система отправляла события с зашифрованными вложениями в карантин, откуда бы их получал адаптер Password Disclosure Adapter. См. пример в статье *Настройка политики Traffic Monitor для работы InfoWatch Password Disclosure Adapter*.
2. Создайте политику для контроля пересылки информации по счетам:

a. В качестве защищаемых данных выберите объект защиты *Информация по счетам*.
b. Создайте правило передачи, разрешающее пересылку данных в защищенном виде (*Правило 1*):
   - Тип события: *Электронная почта*
   - Атрибут: *Расшифрованные данные* (значение *Да*)
   - Вердикт: *Разрешить*
c. Создайте правило передачи, запрещающее пересылку данных в незащищенном виде (*Правило 2*):
   - Тип события: *Электронная почта*
   - Вердикт: *Заблокировать*

3. Создайте политику для контроля пересылки стратегии компании:
   a. В качестве защищаемых данных выберите объект защиты *Стратегия компании*.
   b. Создайте правило передачи, запрещающее пересылку данных в незащищенном виде:
      - Тип события: *Электронная почта*
      - Вердикт: *Заблокировать*
4. Примените конфигурацию.

Примечание:

Поскольку в *Правиле 1* указан пользовательский атрибут, вес такого правила больше, чем вес *Правила 2*. Поэтому, несмотря на то, что *Правило 2* применимо к данным как в защищенном, так и в открытом виде, Система применит к данным в защищенном виде *Правило 1* как более приоритетное для них. Подробнее о пользовательских атрибутах и приоритетах правил см.:

- *InfoWatch Traffic Monitor. Руководство пользователя. Обычный режим создания запроса*;
- *InfoWatch Traffic Monitor. Руководство пользователя. Общие сведения о политиках*.

9 Диагностика и удаление InfoWatch Password Disclosure Adapter

Диагностика

Ошибки записываются в строках с префиксом `ERROR` в файле журнала `var/log/infowatch/pda.log`. При проблемах взаимодействия с PHP-FPM рекомендуется обратиться к журналам NGINX-сервера, которые можно найти в файле `/var/log/nginx/error.log`.

Если адаптер и Traffic Monitor установлены на отдельных серверах, осуществляется ежедневная ротация журналов службой `logrotate`. По умолчанию служба сохраняет последние 7 файлов. Настройки ротации заданы в файле `/etc/logrotate.d/pda`.

Чтобы запустить, остановить или перезапустить адаптер, используйте команды:

- ```
  systemctl start iw_pda
  ```
- ```
  systemctl stop iw_pda
  ```
- ```
  systemctl restart iw_pda
  ```

> **Примечание:**
>
> Остановка адаптера необходима перед:
>
> - обновлением адаптера;
> - удалением адаптера;
> - обновлением Traffic Monitor (подробнее см. *InfoWatch Traffic Monitor. Руководство по установке. Обновление Системы*).

Чтобы удалить адаптер:

> **Важно!**
>
> Действия по удалению адаптера выполняются от имени системного администратора.

1. Остановите адаптер.
2. Удалите папку с адаптером `/opt/iw/tm5/www/pda`.
3. В базе данных удалите схему `pda`.
4. Удалите конфигурационные файлы:
   - `/opt/iw/tm5/etc/pda.conf`;
   - `/etc/nginx/conf.d/iwtm-pda.location`.
5. Удалите пакет с адаптером из директории, использованной при установке PDA.
6. В Консоли управления Traffic Monitor:
   a. Удалите лицензию:
      i. Перейдите в раздел **Управление** → **Лицензии**.
  ```

ii. Выберите лицензию из списка слева.
iii. Нажмите **Удалить**.
iv. Нажмите **Да**, чтобы подтвердить удаление.
v. Нажмите **Да**, чтобы обновить страницу.

b. В случае работы с Traffic Monitor 7.9, удалите плагин:
i. Перейдите в раздел **Управление** → **Плагины**.
ii. Выберите плагин из списка слева.
iii. Нажмите **Удалить плагин**.
iv. Нажмите **Да**, чтобы подтвердить удаление.