InfoWatch Password Disclosure Adapter. Руководство по установке и конфигурированию

09/09/2025

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Введение 3

2 Общая информация об InfoWatch Password Disclosure Adapter 4

2.1 Функции InfoWatch Password Disclosure Adapter 4

2.2 Схема работы InfoWatch Password Disclosure Adapter 4

3 Аппаратное и программное обеспечение для InfoWatch Password Disclosure Adapter 8

4 Добавление лицензии и получение токена плагина для InfoWatch Traffic Monitor 10

5 Установка и запуск InfoWatch Password Disclosure Adapter 12

5.1 Установка адаптера на один сервер с Traffic Monitor 12

5.2 Установка адаптера на отдельный сервер 15

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 21

6 Обновление InfoWatch Password Disclosure Adapter 27

7 Настройки InfoWatch Password Disclosure Adapter 29

7.1 Настройки адаптера в файле pda.conf 29

7.2 Настройки адаптера в таблице setting базы данных 31

7.3 База паролей InfoWatch Password Disclosure Adapter 33

8 Настройка политики Traffic Monitor для работы InfoWatch Password Disclosure Adapter 34

9 Диагностика и удаление InfoWatch Password Disclosure Adapter 41

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 TM, 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 PostreSQL.

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:

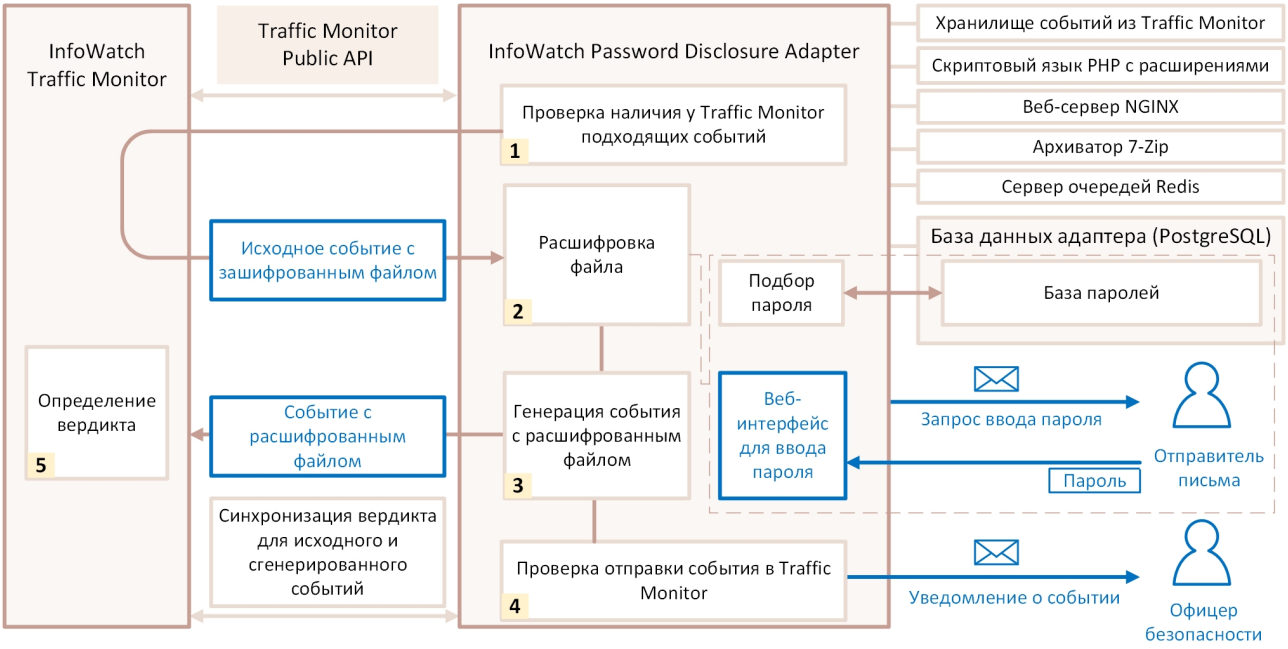
- обработка событий типа *Электронная почта* и зашифрованных файлов форматов:
  - RAR, ZIP, 7ZIP;
  - DOC, PPT, XLS, в том числе с надстройкой IRM Client for Office;
  - DOCX, PPTX, XLSX, XLSM, XLSB;
  - PDF.
- в случае неподдерживаемого формата зашифрованного вложения – уведомление отправителя о том, что отправка письма была приостановлена;
- 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.



InfoWatch Password Disclosure Adapter работает по следующему алгоритму:

1. Адаптер обращается к Traffic Monitor, чтобы получить почтовые события с зашифрованными файлами из карантина. За одно обращение считывается до 1000 событий. Офицер безопасности может задать периодичность получения событий в настройках.
2. Адаптер расшифровывает файл следующим образом:
   a. Проверяет тип файла.
      - В случае, если обработка файла данного типа не поддерживается:
        i. Письмо остается в карантине;
        ii. Адаптер оповещает отправителя почтовым уведомлением о том, что письмо не было доставлено.
      - В случае, если обработка файла данного типа поддерживается:
        i. Подбирает пароль из базы паролей. Подробнее см. статью "База паролей InfoWatch Password Disclosure Adapter".
        ii. Если в базе нет подходящего пароля, адаптер оповещает отправителя почтовым уведомлением о необходимости перейти в веб-интерфейс и ввести пароль.
        iii. Password Disclosure Adapter генерирует событие с расшифрованным файлом и отправляет его с пользовательскими атрибутами и ID исходного события в Traffic Monitor.

> **Примечание:**
>
> 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.

iv. Адаптер отправляет уведомление Офицеру безопасности с информацией о событии, в котором содержится расшифрованный файл.
v. На основании анализа расшифрованного файла Система определяет вердикт для исходного события.

Статусы файлов и событий

Адаптер присваивает зашифрованным файлам и событиям, содержащим эти файлы, следующие статусы:

Статус	Присваивается файлу	Присваивается событию
Расшифровано	• Если подошел один из паролей, хранящихся в базе паролей • Если пользователь ввел подходящий пароль	Когда расшифрованы все зашифрованные файлы в событии
Ожидает пароль от пользователя	Если пользователь ввел неподходящий пароль	–
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	–	Если на одном из этапов работы адаптера с событием возникла ошибка

Вердикты

После анализа сгенерированного события Система определяет для исходного события тот же вердикт, что и для сгенерированного. На основании вердикта осуществляются следующие действия с исходным письмом:

Вердикт	Действие Системы
Разрешить	Исходное письмо досылается получателю.
Заблокировать	Исходное письмо не досылается получателю.

Вердикт	Действие Системы
Карантин	Исходное письмо не досылается автоматически, но Офицер безопасности может дослать его вручную.

Примечание:

Офицер безопасности может вручную изменить вердикт для исходного и сгенерированного событий.

Важно!

Если Офицер безопасности назначил вердикт исходному событию раньше, чем его определил адаптер после анализа Traffic Monitor, то результаты анализа по сгенерированному событию не влияют на исходное событие.

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 и 1.7.5.9	
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".

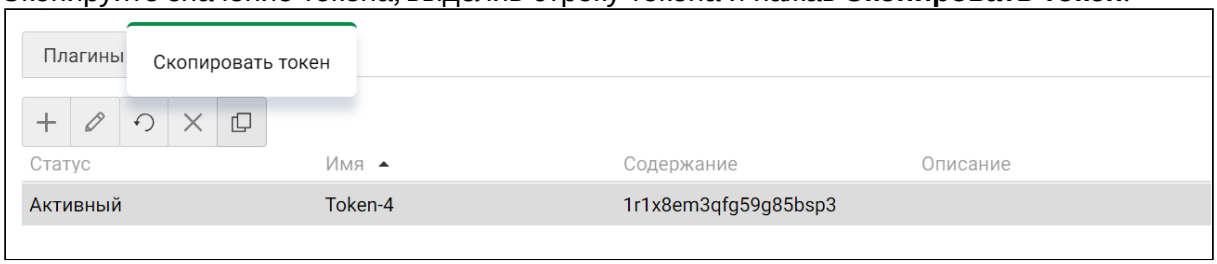
Также необходимо сохранить значение токена плагина, которое будет использовано позже для настройки подключения адаптера к Traffic Monitor. Подробнее см. статью "Настройка политики Traffic Monitor для работы InfoWatch Password Disclosure Adapter".

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 TM 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. Откройте на редактирование файл `/opt/iw/tm5/etc/pda.conf`. В файле укажите:
   - параметры подключения к Traffic Monitor;
   - параметры подключения к базе данных PostrgeSQL;
   - при необходимости – количество занимаемых потоков.

> **Примечание:**
>
> Подробнее о параметрах см. статью "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. Задайте настройки в таблицах базы данных:

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

a. В таблице `setting` введите:
   - параметры подключения к Traffic Monitor;
   - параметры подключения к почтовому серверу;
   - при необходимости – ID тега.

> **Примечание:**
>
> Подробнее о параметрах см. статью "Настройки адаптера в таблице `setting` базы данных".

b. Если вы хотите добавить пароли в базу паролей, внесите их в таблицу `custom_password`. Подробнее см. статью "База паролей InfoWatch Password Disclosure Adapter".

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

```
systemctl start iw_pda
```

9. Убедитесь, что адаптер запущен:

```
systemctl status iw_pda
```

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

10. 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. документ *"InfoWatch Traffic Monitor. Руководство по установке"*, статья "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. документ *"InfoWatch Traffic Monitor. Руководство по*

установке", статья "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. Установите дополнительные пакеты NGINX, Redis, QPDF и P7zip с плагинами при помощи команды:

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

3. 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.

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

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

5. Смените пользователя NGINX на `iwtm`. Для этого:
   a. Откройте на редактирование файл `/etc/nginx/nginx.conf`.
   b. Измените значение поля `user` на `iwtm`.
6. 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`.
7. 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
```

8. 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`.
9. Перезапустите PHP-FPM и проверьте, что сервис запустился. Используйте команду:

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

10. 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
```

11. 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.

12. 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
```

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

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

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

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

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

```
setsebool -P httpd_can_network_connect 1
```

17. Откройте на редактирование файл `/opt/iw/tm5/etc/pda.conf`. В файле укажите:
    - параметры подключения к Traffic Monitor;

- параметры подключения к базе данных PostrgeSQL;
- параметры подключения к серверу очередей Redis;
- при необходимости – количество занимаемых потоков.

> **Примечание:**
>
> Подробнее о параметрах см. статью "Настройки адаптера в файле `pda.conf`".

18. На сервере Traffic Monitor 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`.
19. 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.

20. Подключитесь к базе данных и задайте настройки в таблицах.

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

    a. В таблице `setting` введите:
        - параметры подключения к Traffic Monitor;
        - параметры подключения к почтовому серверу;
        - при необходимости – ID тега.

> **Примечание:**
>
> Подробнее о параметрах см. статью "Настройки адаптера в таблице `setting` базы данных".

b. Если вы хотите добавить пароли в базу паролей, внесите их в таблицу `custom_password`. Подробнее см. статью "База паролей InfoWatch Password Disclosure Adapter".

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)`.

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. Установите дополнительные пакеты NGINX, Redis, QPDF и P7zip с плагинами при помощи команды:

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

3. 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.

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

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

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

7. 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
```

8. 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`.
9. Перезапустите PHP-FPM и проверьте, что сервис запустился. Используйте команду:

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

10. 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
```

11. 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.
12. 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
```

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

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

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

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

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

16. Откройте на редактирование файл `/opt/iw/tm5/etc/pda.conf`. В файле укажите:
    - параметры подключения к Traffic Monitor;
    - параметры подключения к базе данных PostrgeSQL;
    - параметры подключения к серверу очередей Redis;
    - при необходимости – количество занимаемых потоков.

    > **Примечание:**
    >
    > Подробнее о параметрах см. статью "Настройки адаптера в файле `pda.conf`".

17. 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.

18. Подключитесь к базе данных и задайте настройки в таблицах.

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

    a. В таблице `setting` введите:
    - параметры подключения к Traffic Monitor;
    - параметры подключения к почтовому серверу;
    - при необходимости – ID тега.

    > **Примечание:**
    >
    > Подробнее о параметрах см. статью "Настройки адаптера в таблице `setting` базы данных".

    b. Если вы хотите добавить пароли в базу паролей, внесите их в таблицу `custom_password`. Подробнее см. статью "База паролей InfoWatch Password Disclosure Adapter".

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

```
systemctl start iw_pda
```

20. 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. Запустите команду обновления адаптера:

   На сервере под управлением ОС RHEL или РЕД ОС:

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

   На сервере под управлением ОС Astra Linux:

   ```
   sudo apt install ./<iwtm_pda>.deb
   ```

   > **Примечание:**
   >
   > В командах выше `<iwtm-pda>` – полное название пакета с адаптером.

3. 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.

4. 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
```

5. Запустите адаптер с помощью команды:

```
systemctl start iw_pda
```

7 Настройки InfoWatch Password Disclosure Adapter

Вы можете задать следующие настройки адаптера:

- настройка подключения к Traffic Monitor;
- настройка подключения к базе данных адаптера;
- настройка подключения к серверу очередей Redis;
- настройка SMTP-подключения для отправки уведомлений адаптером;
- настройка количества процессов и другие.

Описание настроек представлено в статьях раздела:

- Настройки адаптера в файле `pda.conf`
- Настройки адаптера в таблице `setting` базы данных
- База паролей InfoWatch Password Disclosure Adapter

> **Важно!**
>
> Перед запуском адаптера требуется определить значения обязательных параметров и при необходимости изменить значения по умолчанию. Подробнее см. статьи раздела "Установка и запуск InfoWatch Password Disclosure Adapter".

7.1 Настройки адаптера в файле pda.conf

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

- настройка подключения к Traffic Monitor;
- настройка подключения к базе данных PostgreSQL;
- настройка подключения к серверу очередей Redis;
- настройка количества занимаемых потоков.

Подключение к серверу Traffic Monitor

В секции `Pushapi` указаны параметры подключения к серверу, на котором установлен Traffic Monitor и на который адаптер будет присылать события. Большинство значений заданы по умолчанию; вам необходимо ввести корректные значения для параметров `Host` и `Token`.

Поле	Значение	Описание
`Host`	`127.0.0.1`	IP-адрес или имя хоста сервера Traffic Monitor, на который адаптер отправляет события
`Name`	`iw-xapi-puppy`	Имя сервиса
`Port`	`9101`	Порт сервера
`Token`	`-`	Токен доступа в Traffic Monitor

Поле	Значение	Описание
		Примечание: Токен отображается при подключении плагина в Консоли управления ТМ. Подробнее см. статью "Добавление лицензии и получение токена плагина для InfoWatch Traffic Monitor".
`UserName`	`consul_client`	Имя пользователя для входа в службу Consul **Примечание:** Подробнее о службе см. документ *"InfoWatch Traffic Monitor. Руководство администратора"*, раздел "Настройка Системы после установки", статья "Настройка межсервисного взаимодействия (служба Consul)".

Подключение к базе данных PostgreSQL

Чтобы установить соединение адаптера с базой данных, необходимо ввести значения всех полей секции `Database`, как представлено в таблице ниже:

Поле	Значение	Описание
`Database`	`postgres`	Используемая СУБД
`Driver`	`pgsql`	Драйвер для взаимодействия с СУБД
`Host`	`<IP-адрес>`	IP-адрес базы данных
`Password`	`xxXX1234`	Пароль пользователя
`Port`	`5433`	Порт базы данных
`Schema`	`pda`	Схема базы данных, используемая адаптером
`UserName`	`iwtm`	Имя пользователя в базе данных

Подключение к серверу очередей Redis

Чтобы установить соединение адаптера с сервером очередей Redis, необходимо ввести значения всех полей секции `Redis`:

Поле	Описание
`Host`	IP-адрес сервера Redis
`Port`	Порт подключения к Redis

Количество занимаемых потоков

Если требуется повысить скорость работы адаптера, настройте параметр `ParallelCount` в секции `Worker`. В параметре записывается количество потоков, которые занимает адаптер. Значение по умолчанию – `8`. Увеличение количества занимаемых потоков ведет к ускорению адаптера. Количество потоков не должно превышать количество ядер или быть слишком малым.

7.2 Настройки адаптера в таблице setting базы данных

Данная статья описывает настройки адаптера, которые содержатся в таблице `setting` базы данных:

- Настройка подключения адаптера к Traffic Monitor
- Настройка почтового сервера для отправки адаптером уведомлений офицеру безопасности
- Прочие параметры адаптера

Настройка подключения к Traffic Monitor

Все параметры подключения к Traffic Monitor обязательны. Большинство значений заданы по умолчанию; вам необходимо ввести корректные значения для параметров `tm_dataexport_api` и `tm_token`.

Параметр	Значение по умолчанию	Описание
`request_timeout`	`900` (в секундах)	Интервал времени обращения адаптера к TM для того, чтобы получить события
`audit_last_time`	Одно из значений в формате `timestamp`: • текущее время на сервере, если адаптер устанавливается впервые и в нем нет событий • время самого первого события, если адаптер был установлен ранее и в нем есть события	Время последней считанной записи аудита **Примечание:** Параметр необходим для прослушивания аудита TM на предмет изменений пользовательского решения по исходному или сгенерированному адаптером событиям.
`verification_timeout`	`60` (в секундах)	Интервал времени, в течение которого адаптер проверяет, пришло ли сгенерированное адаптером событие на анализ в TM **Примечание:** Параметр необходим для прослушивания аудита TM на предмет изменений пользовательского решения по исходному или сгенерированному адаптером событиям.
`tm_dataexport_api`	`https://127.0.0.1`	Имя или IP-адрес хоста, на котором установлен TM и с которого адаптер получает события **Примечание:** Ссылка на событие в письме Офицеру безопасности ведет на хост с этим адресом.

Параметр	Значение по умолчанию	Описание
`tm_token`	Отсутствует	Токен доступа в TM **Примечание:** Токен отображается при подключении плагина в Консоли управления TM. Подробнее см. статью "Добавление лицензии и получение токена плагина для InfoWatch Traffic Monitor".

Настройка почтового сервера

Чтобы настроить почтовый сервер для отправки уведомлений офицеру безопасности, определите значения перечисленных параметров. Параметры `smtp_login` и `smtp_password` обязательны в случае шифрования SMTP-трафика, которое используется по умолчанию.

Параметр	Описание
`smtp_host`	SMTP-сервер, используемый для отправки уведомлений
`smtp_port`	Порт, используемый для отправки уведомлений
`smtp_security`	Включить/выключить шифрование. Выбор из значений: • `1` – включить, по умолчанию • `0` – выключить
`smtp_login`	Имя учетной записи, имеющей доступ к почтовому серверу
`smtp_password`	Пароль учетной записи, имеющей доступ к почтовому серверу
`email_officer`	Адрес электронной почты Офицера безопасности, который получает уведомления от адаптера. При необходимости добавить несколько адресов используйте точку с запятой (`;`) в качестве разделителя **Пример:** `security.officer@company.ru; petr.ivanov@company.ru; viktor.evdokimov@company.ru`
`email_pda`	Адрес электронной почты, который используется в качестве отправителя уведомления

Прочие параметры адаптера

Значение параметра `enabled` задано по умолчанию. Вы можете задать значение опционального параметра `tags`.

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".

Параметр	Описание
`enabled`	Статус адаптера. Выбор из значений: • `1` – активный, по умолчанию. Адаптер запускается. • `0` – неактивный. Адаптер записывает в лог попытку запуска и завершает работу.

`tags`	ID тега для фильтрации событий, получаемых адаптером. Вставьте ID всех тегов, при наличии которых адаптер должен получать события из Traffic Monitor. При необходимости добавить несколько тегов используйте запятую (`,`) в качестве разделителя
	Пример:
	`3A912F1381B241CEA07CE1DA53EF552D00000000,`
	`329573FF216C43B6B976808C73529B6300000000`

7.3 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.

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 документ "*InfoWatch Traffic Monitor. Руководство пользователя*", глава "Решение задач при работе в консоли Traffic Monitor", раздел "Настройка реакций Системы", статья "Создание политики защиты данных".

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

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

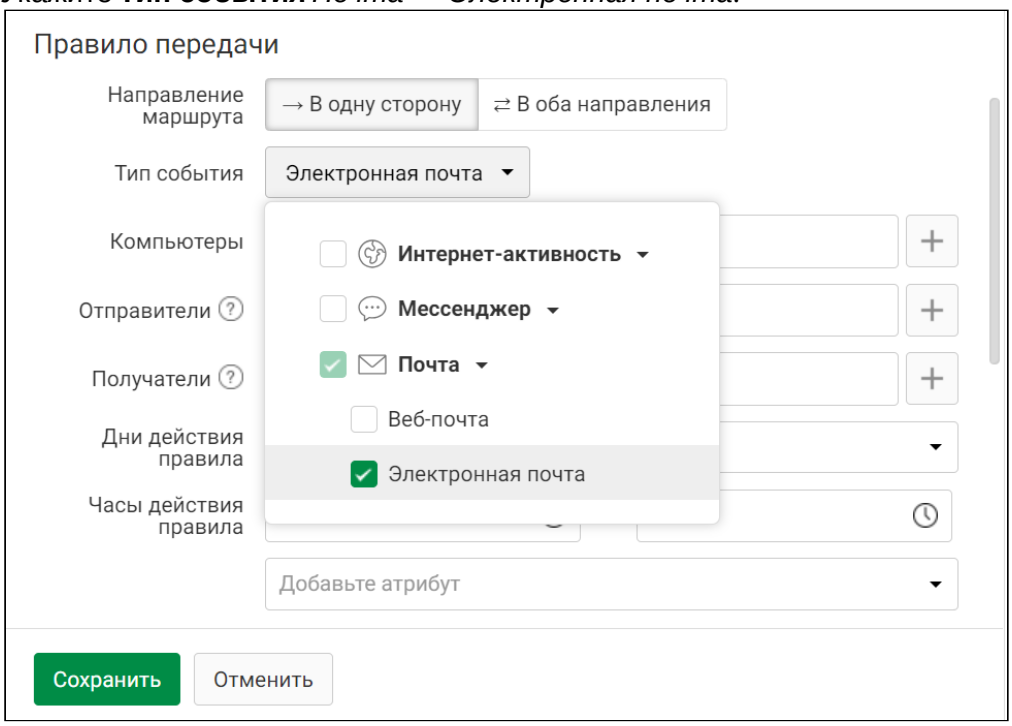
Важно!

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, попавшие в карантин, что может негативно влиять на производительность Системы.

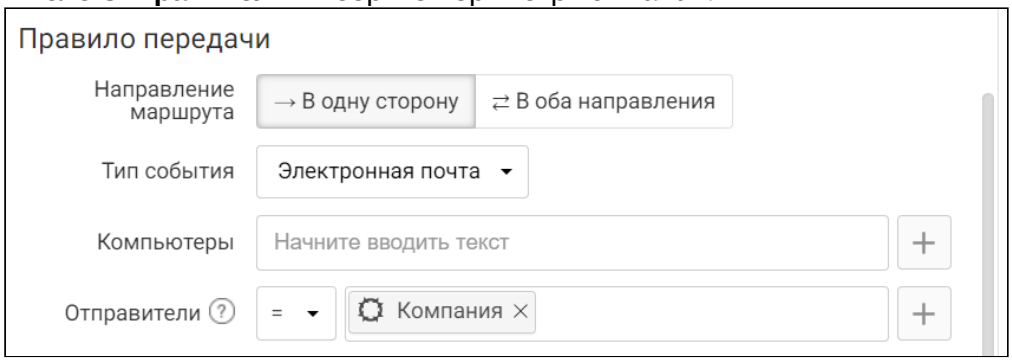
Чтобы настроить политику Traffic Monitor для перехвата событий с перечисленными условиями:

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**.

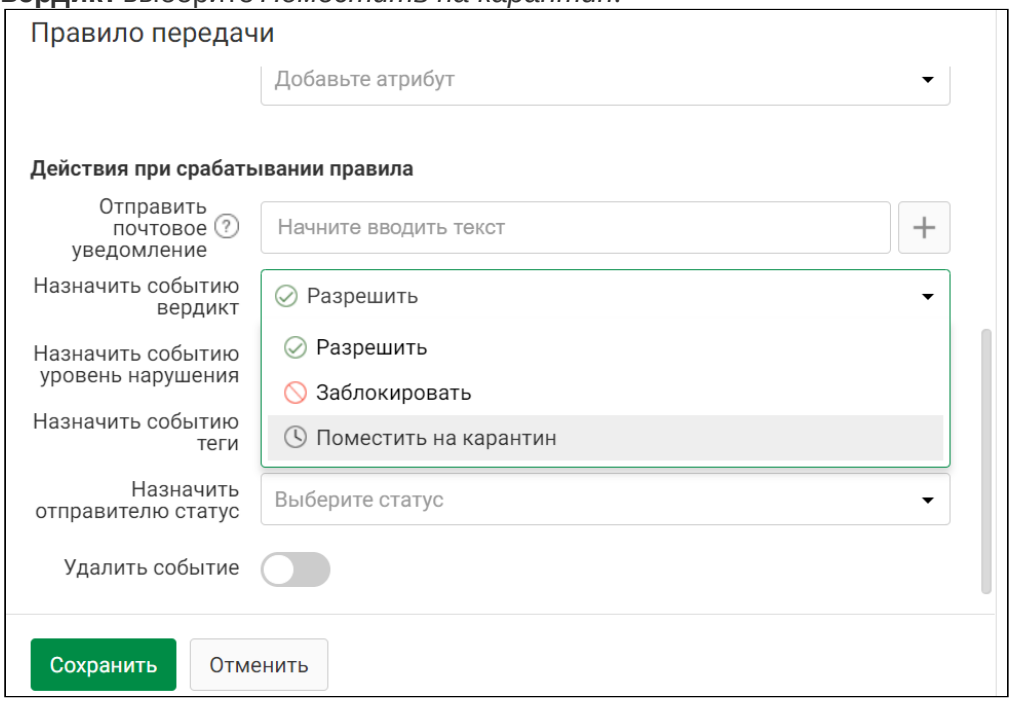
5. Укажите **Тип события** *Почта → Электронная почта*:



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



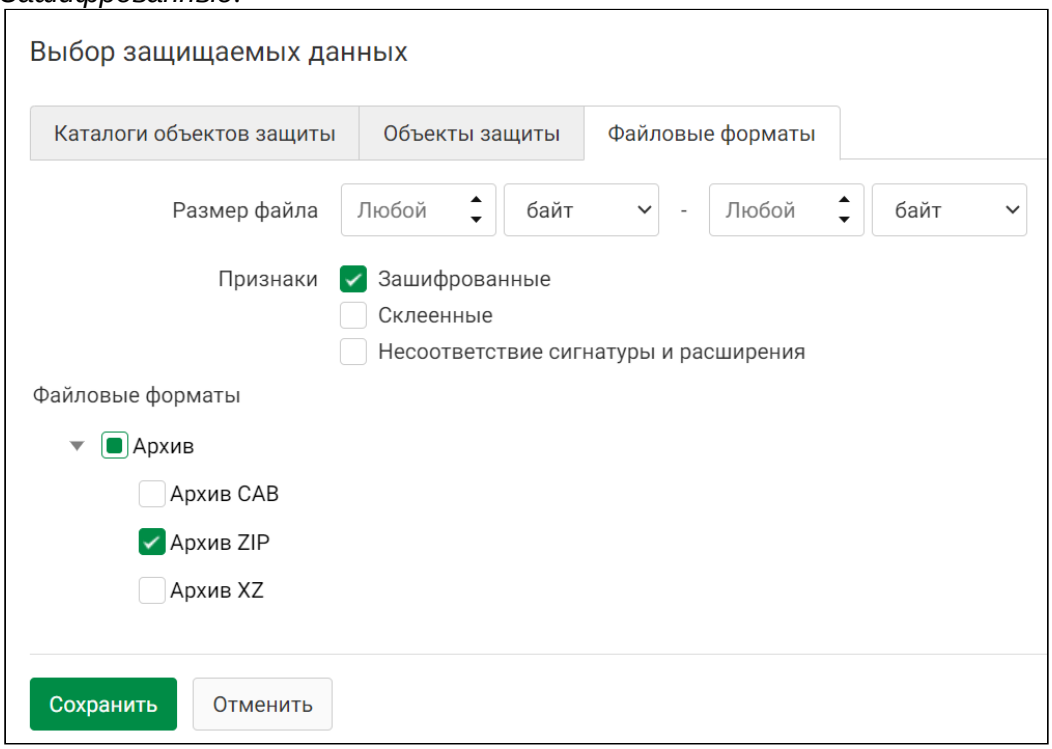
7. В разделе **Действия при срабатывании правила** в поле **Назначить событию вердикт** выберите *Поместить на карантин*:



> **Примечание:**
>
> Если 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*;
> - по завершении редактирования политики выполните действия из шага 14.
>
> Подробнее о настройке уведомлений см. документ "*InfoWatch Traffic Monitor. Руководство пользователя*", глава "Решение задач при работе в консоли Traffic Monitor", раздел "Управление Системой", статья "Настройка уведомлений".

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

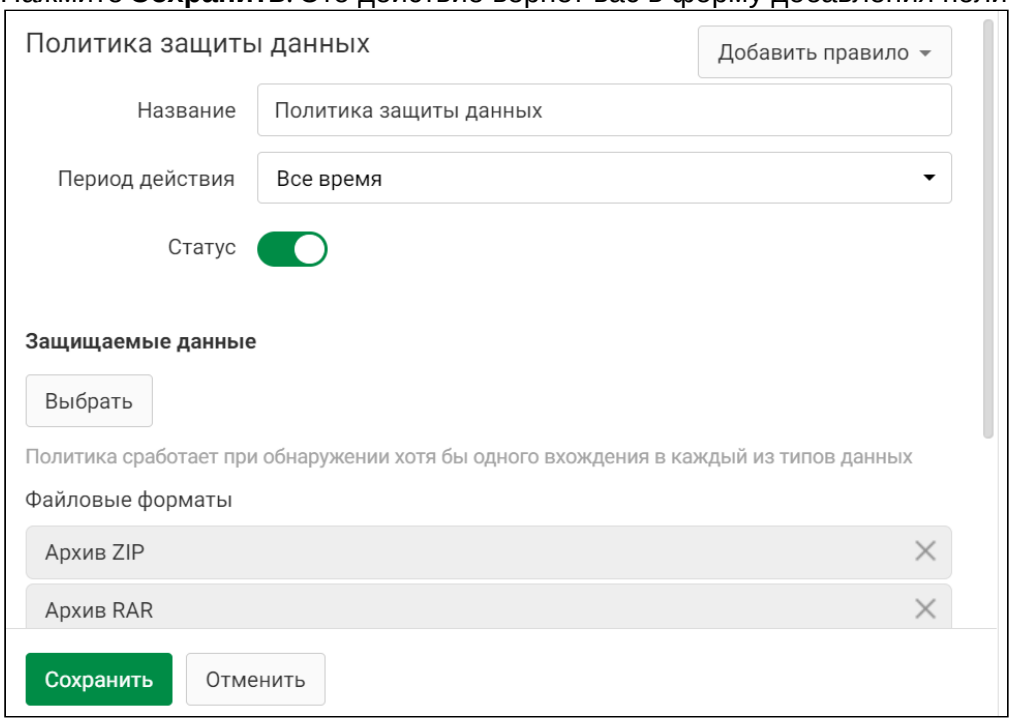
9. В разделе **Файловые форматы** в поле **Признаки** установите флажок для значения *Зашифрованные*:



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"*, глава "Решение задач при работе в консоли Traffic Monitor", раздел "Работа со справочниками", статья "Работа с тегами".
    b. Из колонки `tag_id` таблицы `tag` базы данных Traffic Monitor скопируйте ID добавленного тега.
    c. В поле `tags` таблицы `setting` базы данных адаптера вставьте ID тега.
    d. Укажите данный тег при настройке политики в разделе **Действия при срабатывании правила** в поле **Назначить событию теги**.
14. Чтобы Система уведомляла отправителя файла почтовыми сообщениями о том, что его письмо было помещено в карантин, заблокировано или покинуло карантин:
    a. Настройте блокировку SMTP-трафика "в разрыв". Подробнее см. документ "*InfoWatch Traffic Monitor. Руководство администратора*", глава "Настройка Системы после установки", раздел "Настройка перехвата трафика", подраздел "Настройка перехвата SMTP-трафика", статья "Блокировка "в разрыв".
    b. Задайте настройки подключения к почтовому серверу. Подробнее см. документ "*InfoWatch Traffic Monitor. Руководство пользователя*", глава "Решение задач при работе в консоли Traffic Monitor", раздел "Управление Системой", статья "Настройка подключения к почтовому серверу".
    c. Настройте отправку уведомлений при срабатывании политик на сгенерированные события.

> **Примечание:**

Система не отправляет уведомления для сгенерированных событий. При этом исходное событие наследует вердикт сгенерированного. Поэтому:

- При назначении сгенерированному событию вердикта *Разрешить* Система уведомляет отправителя о том, что письмо покинуло карантин.
- При назначении сгенерированному событию вердикта *Заблокировать* Система уведомляет отправителя о том, что письмо заблокировано после карантина.
- При назначении сгенерированному событию вердикта *Карантин* Система не уведомляет отправителя, т.к. уведомление о карантине было отправлено ранее при срабатывании политики на исходное событие.

Пример настройки:

i. Создайте текстовые объекты:

Название текстового объекта	*Разрешить*	*Заблокировать*	*Карантин*
Тип шаблона	строка		
Значение строки шаблона	*Разрешить*	*Заблокировать*	*Карантин*

ii. На основе этих текстовых объектов создайте объекты защиты:

Название объекта защиты	*Разрешить*	*Заблокировать*	*Карантин*
Элементы технологий	текстовый объект *Разрешить*	текстовый объект *Заблокировать*	текстовый объект *Карантин*
Условие обнаружения			

iii. Создайте политики защиты данных со указанными настройками:

Название политики		*Вердикт "Разрешить"*	*Вердикт "Заблокировать"*	*Вердикт "Карантин"*
Защищаемые данные	Объекты защиты	*Разрешить*	*Заблокировать*	*Карантин*
	Файловые форматы	Те же, что и файловые форматы в шаге 10 при настройке *Политики Password Disclosure Adapter*		

Правило передачи	Тип события	*Почта → Электронная почта*		
	Назначить событию вердикт	*Разрешить*	*Заблокировать*	*Поместить на карантин*
	Отправить почтовое уведомление	*Уведомление нарушителю*		

d. Примените конфигурацию.

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. документ "*InfoWatch Traffic Monitor. Руководство по установке*", статья "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.