RT Protect EDR

Руководство пользователя

Версия 1.0.9 от 20 августа 2024
Разработано компанией АО «РТ-Информационная безопасность»

RT Protect

1. Общие положения

1.1 *Идентификация документа*

Данное руководство кратко можно идентифицировать согласно таблице 1.

Таблица 1 – Идентификация документа

Название документа	«RT Protect EDR» Руководство пользователя
Версия документа	Версия 1.0.22 (актуально для версии агента 2.0.162.2662, версии фронтенда 2.39.36, версии бекенда 1.21.1)
Идентификация программы	«RT Protect EDR»
Идентификация разработчика	АО «РТ-Информационная безопасность»
Уровень доверия	Оценочный уровень доверия 4 (ОУД4)
Идентификация ПЗ	Профиль защиты систем обнаружения вторжений уровня узла типа «У» четвертого класса защиты. ИТ.СОВ.У4.ПЗ. Утвержден ФСТЭК России от 3.02.2012г. Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты ИТ.СКН.П4.ПЗ (утвержден ФСТЭК России от 01.12.2014)
Идентификация ОК	«Требования к системам обнаружения вторжений, утвержденные приказом ФСТЭК России от 6 декабря 2011 г. № 638. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»
Ключевые слова	Система обнаружения вторжений, СОВ, ОУД4

1.2 *Аннотация документа*

Настоящий документ является руководством пользователя программы «RT Protect EDR» (далее Программа).

В документе приведены общие сведения, сведения об установке и первоначальной настройке Программы, а также рекомендации по использованию Программы и решению типичных проблем, связанных с вирусными угрозами.

2. Общие сведения

Программа имеет клиент-серверную архитектуру и предназначена для выявления и предотвращения кибератак на различные информационные системы – от отдельно взятых компьютеров до корпоративных систем.

Программа включает в себя как функции классического антивируса, так и передовые технологии по выявлению и предотвращению атак «нулевого» дня.

Программа базируется на следующих современных подходах и технологиях в области информационной безопасности:

1) EDR (Endpoint Detection and Response) – единый центр расследования и реагирования на инциденты информационной безопасности в корпоративных информационных системах;

2) Классический антивирус – поиск известных вирусных сигнатур в информационных потоках;

3) Машинное обучение – технология выявления похожести поведения программ, установленных на агенте, на нежелательное или содержимого исполняемого файла на нежелательное;

4) Anti-Ransomware – защита от вирусов-вымогателей;

5) Поведенческая эвристика – выявление и сдерживание известных вредоносных техник в поведении программ;

6) IOCs (Indicator of Compromise) и IOAs (Indicator of Attacks) – индикаторы компрометации и атак.

3. Назначение программы

3.1 *Основные задачи и возможности*

Основные задачи и возможности Программы можно кратко описать согласно следующему списку:

1) Быстрое реагирование на сложные и скрытые угрозы, предотвращение их дальнейшего развития;

2) Автоматическое детектирование и быстрое реагирование на сложные угрозы, пропущенные превентивными средствами защиты;

3) Сбор и хранение информации о событиях ИБ в течение установленного времени хранения;

4) Выборка записей событий ИБ на основе предустановленных и пользовательских фильтров;

5) Обнаружение, идентификация и регистрация инцидентов ИБ;

6) Генерация отчетов о возникших инцидентах ИБ;

7) Своевременное информирование о возникновении инцидентов лиц, ответственных за выявление инцидентов и реагирование на них;

8) Мониторинг доступности технических средств по протоколам ICMP, SSH, HTTP, HTTPS, SMTP;

9) Управление (администрирование) комплексом;

10) Автоматическая генерация индикаторов и правил компрометации из обнаруженных угроз;

11) Визуализация пути атаки и построение всех событий, связанных с инцидентом, таких как:

- обнаружение угрозы на конечном устройстве;
- извлечение кода;
- процесс, порождающий другие процессы;
- создание файла;
- сетевые соединения;
- модификация реестра и т.д.;

12) Подробное описание артефактов в информационной карточке инцидента для анализа первопричин;

13) Возможность выявления всех затронутых серверов и рабочих станций.

3.2 *Способы отражения предметной области в программе*

Программа предназначена для выявления киберугроз и борьбы со сложными APT-атаками.

Чтобы защитить корпоративную сеть от различных угроз, многие организации применяют классические средства: антивирусные решения, сканеры безопасности, а также системы обнаружения и предотвращения вторжений. Однако указанные системы не всегда в состоянии обнаружить сложные целевые атаки или предоставить достаточное количество информации для приоритизации и расследования инцидентов ИБ, которые были обнаружены. Для этого сотрудники, отвечающие за информационную безопасность, должны использовать целый комплекс средств, чтобы обеспечить защиту ИС и ускорить расследование инцидентов ИБ, которые все же могут возникнуть.

К таким средствам относятся:

— антивирусы на компьютерах и мобильных устройствах всех сотрудников;

— SIEM-системы, в которые интегрированы потоки данных об угрозах;

— анти-APT-системы, обеспечивающие обнаружение сложных угроз и целевых атак;

— системы исследования образцов программного обеспечения и поиска подробной информации о характеристиках вредоносного программного обеспечения по индикаторам компрометации.

В момент возникновения инцидента от сотрудников, ответственных за ИБ, требуются быстрые и точные шаги, которые позволят минимизировать ущерб от инцидента.

4. Требования к аппаратному и программному обеспечению

Клиентская часть (далее Агент) работает на следующих ОС Windows:

1) Windows: 7, 8, 8.1, 10 (64-х и 32-х разрядной платформе);

2) Windows Server 2008, 2012, 2016, 2019.

Клиентская часть (далее Агент) работает на следующих ОС Linux:

1) Astra SE 1.6;

2) Astra SE 1.7 (поддерживаемые ядра):

– 5.10.142-1-generic;

– 5.15.0-33-generic;

– 5.4.0-110-generic;

– 5.4.0-54-generic.

3) Astra SE 1.8.

4) Debian 11:

– 5.10.0-19-amd64;

5) Debian 12.

6) Ubuntu 18.04:

– 4.15.0-163-generic

7) Ubuntu 20.04:

– 5.15.0-67-generic;

– 5.15.0-69-generic;

– 5.15.0-70-generic;

– 5.15.0-71-generic;

– 5.15.0-72-generic;

– 5.4.0-137-generic;

– 5.4.0-139-generic;

– 5.4.0-148-generic.

8) Ubuntu 22.04:

– 5.19.0-41-generic

9) Ubuntu 24.04.

10) RedOs 7.3:

– 5.10.29-3.el7.x86_64

Примечание

Требования Агента к аппаратуре совпадают с соответствующими требованиями Windows и Linux. Дополнительные требования не предъявляются.

Список ОС и ядер, поддерживаемых Агентом для Linux, в процессе разработки может уточняться и дополняться.

Сервер работает на 64-х разрядной платформе ОС Astra Linux SE 1.7. Аппаратная платформа сервера обеспечивает возможность выполнения функциональных требований, предъявляемых к серверу, с учетом технологии его построения, критериев производительности и отказоустойчивости.

Программа пригодна для функционирования на двух аппаратных платформах, приведенных в таблице 2.

Таблица 2 – Программно-аппаратное обеспечение и среда функционирования Программы

Характеристики	**Платформа 1 (клиентская часть)**		**Платформа 2 (серверная часть)**	
Операционная система	Windows/Linux		Linux	
	Минимальные требования	Рекомендуемые требования	Минимальные требования	Рекомендуемые требования
Процессор	Intel CoreTM I3 Duo 3.1 GHz или эквивалентный (с поддержкой SSE2)	2 ГГц и выше с поддержкой инструкций SSE2	Не менее 10 ядер частотой минимум 2,4 ГГц в 20 потоков	Три сервера с конфигурацией процессора не менее 10 ядер частотой минимум 2,4 ГГц в 20 потоков
Оперативная память	1 ГБ	2 ГБ	32ГБ	64 ГБ на каждом сервере
Жесткий диск (свободное пространство)	100 МБ	2ГБ	8 ТБ	Три жестких диска на каждый сервер по 8 ТБ каждый

5. Роли пользователей, взаимодействующих с Программой

Структура и конфигурация Программы спроектированы и реализованы таким образом, чтобы обеспечить оптимальный количественный состав персонала, который необходим для функционирования. Для функционирования Программы не требуется круглосуточного обслуживания и присутствия персонала.

Для обеспечения эффективного функционирования Программе необходимо наличие следующих групп пользователей, которые взаимодействуют с Программой:

— пользователь;

— аналитик;

— администратор.

Пользователь – сотрудник, выполняющий работу на персональном компьютере, на котором установлен модуль Агента. Пользователь не взаимодействует с Программой напрямую, ему доступны только оповещения в области уведомления панели задач ОС о состоянии защищаемой машины.

Примечание

При установке агента с помощью командной строки уведомления пользователю могут быть отключены администратором.

Аналитик – сотрудник отдела информационной безопасности (далее ИБ) или Центра обеспечения безопасности (SOC), который выполняет функцию экспертной оценки угроз, возникающих в отношении защищаемой Программой IT-инфраструктуры. Аналитик с помощью доступного для него функционала Программы (прежде всего это анализ карточек предупреждений) расследует события, которые потенциально могут нарушить работу защищаемых устройств или защищаемой сети в целом. В случае обнаружения вредоносной программы или атаки на инфраструктуру защищаемого объекта аналитик может оперативно отреагировать, к примеру, изолировав зараженный вредоносным файлом хост или заблокировав действие опасной программы.

Администратор – уполномоченный сотрудник организации Заказчика или Центра обеспечения безопасности. Администратор устанавливает серверный и агентский модули, а также настраивает Программу для ее корректной и полнофункциональной работы.

6. Установка и выполнение Программы

6.1 *Установка Агента в ОС Windows*

6.1.1. *Общие рекомендации по установке и удалению Агента*

Перед установкой Агента необходимо ознакомиться с требованиями к программному и аппаратному обеспечению, описанными в п.4.

Важно

Запуск инсталляции/деинсталляции Агента с помощью утилит с графическим интерфейсом осуществляется исключительно с помощью приложения Проводник.

Установка/удаление Агента другими средствами типа Total Commander не предусмотрено.

Установка/удаление Агента в режиме командной строки производится пользователем с правами Администратор с помощью интерпретатора командной строки cmd.exe.

6.1.2. *Установка Агента с помощью инсталлятора с графическим интерфейсом*

Инсталляционная версия Программы представлена в виде собственного инсталлятора.

Для установки необходимо выполнить следующие шаги:

1) Скачать инсталлятор последней версии ПО с сервера Предприятия-изготовителя (Сервер управления).

2) Запустить процесс установки двойным кликом по инсталлятору. Откроется окно, представленное на рисунке 1.

Рисунок 1 – Окно установки Программы

3) Заполнить поле ID клиента (не менее 8 символов) и адрес сервера. ID клиента берется из соответствующего поля после установки модуля администрирования в разделе **Лицензия/Информация о лицензии**.

4) При необходимости создания точки восстановления, отметить галочкой в строке напротив флага **Точка восстановления**.

5) Нажать **Установить**, появится окно **Индексирование файлов** (см. рис. 2).

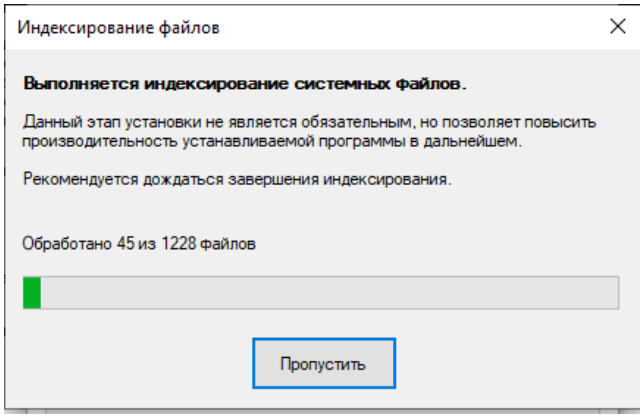

Рисунок 2 – Подтверждение установки

6) После окончания процесса установки появится окно (рисунок 3).

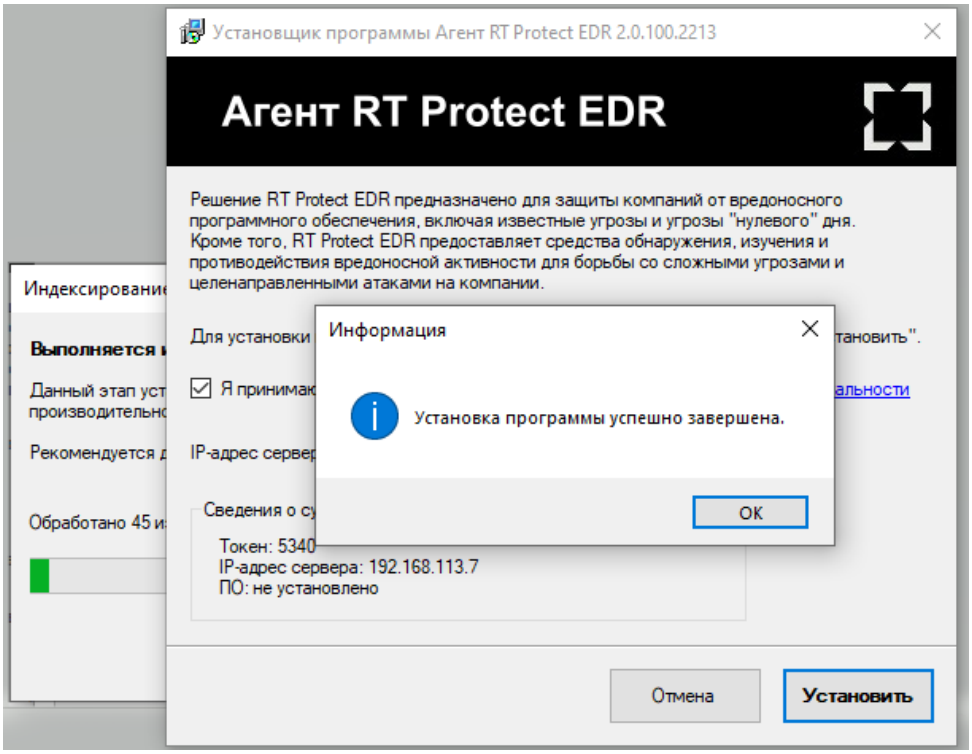

Рисунок 3 – Процесс установки

7) Дождаться завершения установки и нажать кнопку **OK**.

8) После завершения установки в правом углу экрана в системном трее появится иконка установленного антивируса **RT Protect EDR** (рисунок 4).

После завершения установки на диске С в папке Program Files создается папка **ИБ Реформ\Агент RT Protect EDR**\.

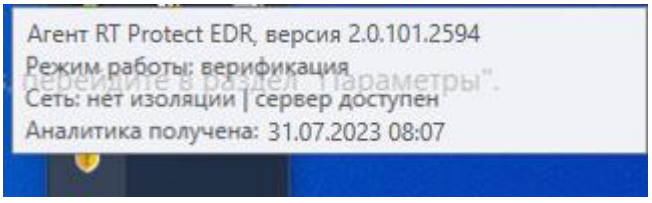

Рисунок 4 – Иконка установленного средства защиты

9) После первоначальной установки Агента его необходимо верифицировать. Операция доступна только пользователям системы с ролью **Администратор** на Сервере управления.

Подробную информацию о верификации агентов можно изучить в документе «Руководство администратора».

После верификации агента в трее появится сообщение, представленное на рисунке 5.

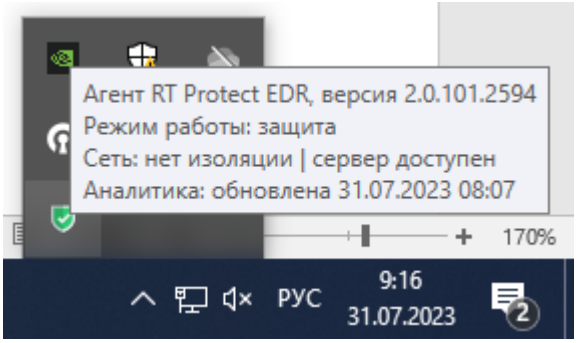

Рисунок 5 – Агент верифицирован

6.1.3. *Установка Агента с помощью инсталлятора в режиме командной строки*

Установка Агента с помощью инсталлятора setup.exe осуществляется пользователем с правами Администратора.

Типичные операции и соответствующие им комбинации командных строк:

1) Первоначальная установка Агента в silent-режиме с индексированием файлов:

Setup /noUI /server=192.168.77.77:5000 /customerId=12345678

2) Первоначальная установка Агента в silent-режиме с пропуском этапа индексирования файлов:

Setup /noUI /skipIndexing /server=192.168.77.77:5000 /customerId=12345678

Для разрешения перезагрузки (в случае необходимости) без запроса пользователя допускается указать параметр /canReboot.

В параметре customerId указывается действительный код клиента из лицензии.

3) Обновление установленного Агента:

Setup /noUI /update

4) Обновление установленного Агента с перезагрузкой:

Setup /noUI /updatesafe /canReboot

5) Обновление endpoint сервера:

Setup /noUI /update /server=192.168.77.77:5000

Примечание:

В параметре /server указывается endpoint сервера (допускается не указывать номер порта). Если требуется обновить только порт, то вместо IP-адреса сервера допускается указывать символ * (пример: /server=*:5000).

6) Обновление идентификатора клиента:

Setup /noUI /update /customerId=12345678

Интерфейс командной строки программы установки агента:

1) /noUI – запуск программы установки без показа пользовательского интерфейса;

2) /canReboot – разрешение перезагрузки без запроса к пользователю (если перезагрузка требуется);

3) /skipIndexing – пропуск этапа установки, связанного с индексированием файлов;

4) /update – режим «обновление на лету»;

5) /updatesafe – режиме «обновление с перезагрузкой»;

6) /server – идентификация серверной части;

7) /customerId – идентификатор клиента (выдается вместе с лицензией);

8) /restore_point – создание точки восстановления;

9) /tray=[<Уровень>] – управление значком и уведомлениями в трее.

Уровни:

— 0 – нет значка в трее, уведомления не выводятся;

— 1 – есть значок, уведомления не выводятся;

— 2 – есть значок, показывать только критические уведомления;

— 3 – есть значок, показывать все уведомления.

10) Пример записи: /tray=0 – установка агента без значка в трее, и без вывода уведомлений.

11) /no_driver – режим «без защиты».

12) /no_proxy – режим установки агента, при котором не использует системные настройки проксирования сетевого трафика при взаимодействии с сервером.

6.1.4. *Пользовательский интерфейс*

Агент, установленный на пользовательской машине, не имеет активного пользовательского интерфейса. Административный модуль управления Агентом находится на сервере и его пользовательский интерфейс не доступен для пользователя. Агент предоставляет пользователю/администратору информацию об угрозах и проблемах, обнаруженных в системе с помощью всплывающих окон.

На рисунках 6 - 11 показаны уведомления, генерируемые ARW-модулем Агента, касающиеся защиты от вредоносных действий.

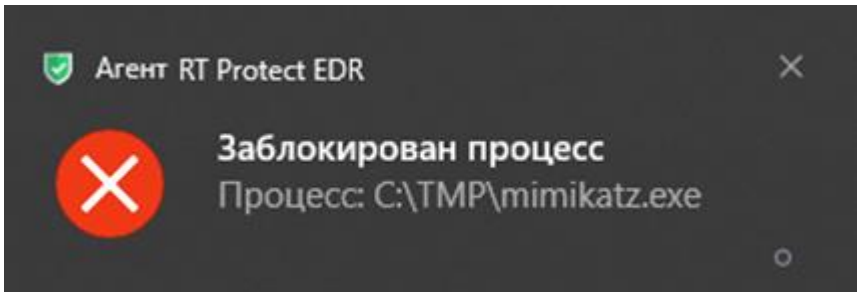

Рисунок 6 – Уведомление о блокировке процесса

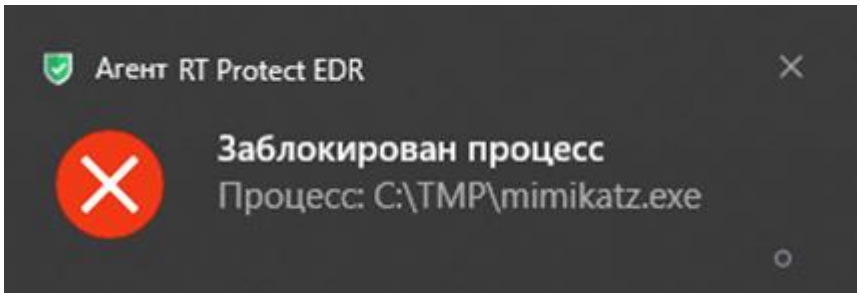

Рисунок 7 – Уведомление о блокировке доступа к диску на запись

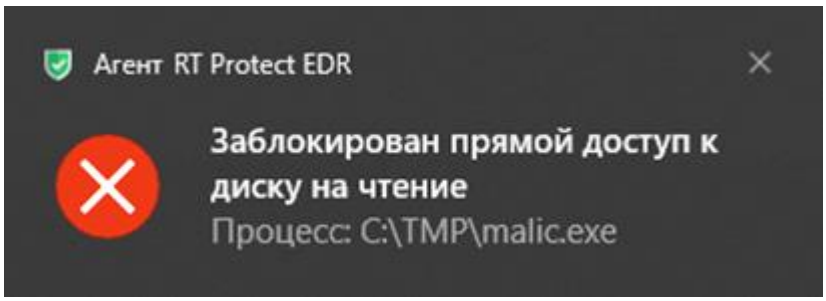

Рисунок 8 – Уведомление о блокировке доступа к диску на чтение

Рисунок 9 – Уведомление о блокировке файла

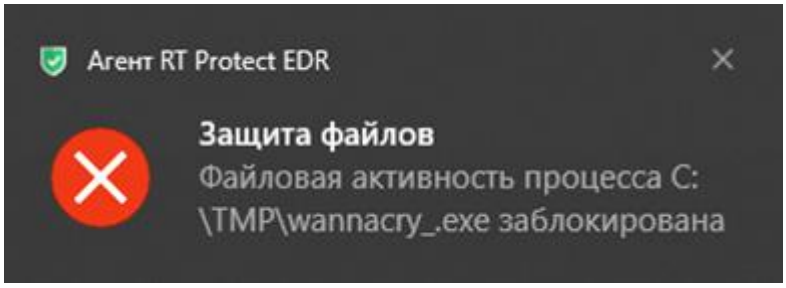

Рисунок 10 – Уведомление о блокировке файловой активности процесса

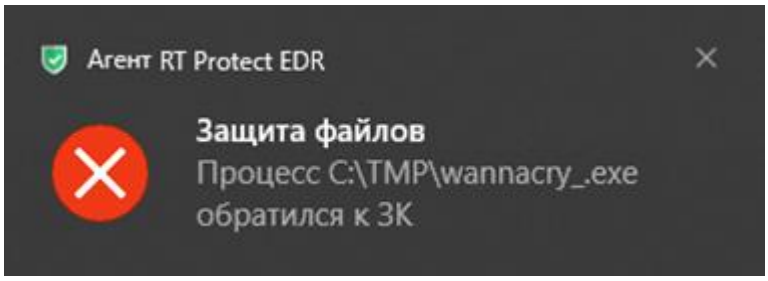

Рисунок 11 – Уведомление об обращении процесса к защищаемому каталогу

На рисунках 12 - 13 показаны уведомления, генерируемые Агентом при изоляции сети. Подробнее о событии изоляции Агента можно ознакомиться в документе «Руководство администратора».

Рисунок 12 – Включена изоляция сети

Рисунок 13 – Выключена изоляция сети

На рисунках 14 - 15 показаны сообщения, генерируемые Агентом при отсутствии/возобновлении связи с сервером.

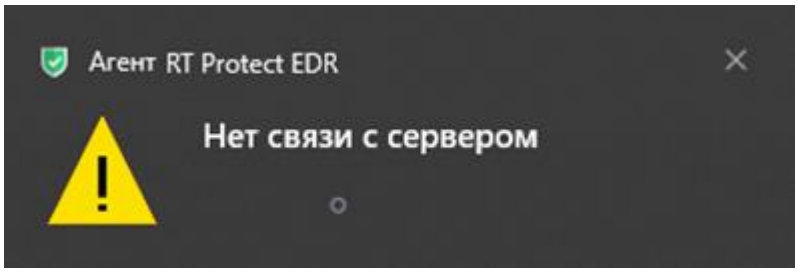

Рисунок 14 – Отсутствует связь с сервером

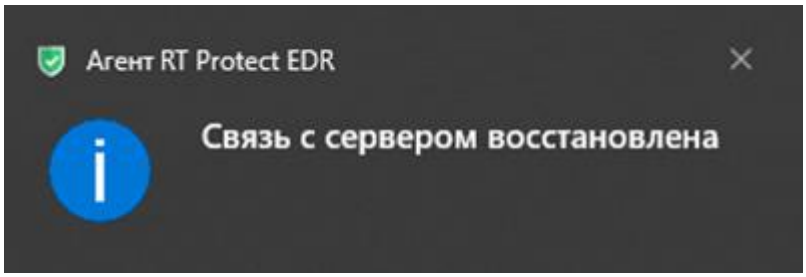

Рисунок 15 – Связь с сервером восстановлена

6.2 *Установка Агента в ОС Linux*

6.2.1. *Общие сведения*

Дистрибутив Агента EDR под Linux представлен в виде следующих пакетов:

– deb-пакет;

– rpm-пакет.

Агент EDR в формате deb-пакета, рассчитан на установку в следующих ОС:

– Astra SE 1.6 (64-х разрядная платформа);

– Astra SE 1.7 (64-х разрядная платформа);

– Astra SE 1.8 (64-х разрядная платформа);

– Debian-11 (64-х разрядная платформа);

– Debian-12 (64-х разрядная платформа);

– Ubuntu-18.04 (64-х разрядная платформа);

– Ubuntu-20.04 (64-х разрядная платформа);

– Ubuntu-22.04 (64-х разрядная платформа);

– Ubuntu-24.04 (64-х разрядная платформа);

– Alt Linux 10.

Агент EDR в формате rpm-пакета, рассчитан на установку в следующих ОС:

– Red OS 7.3.

Для работы агента требуются следующие пакеты (большая часть из них входит в состав базовой части ОС):

1) libbrotli1 (>= 0.6.0)

2) libc6 (>= 2.22)

3) libcurl4 (>= 7.16.3)

4) libelf1 (>= 0.142)

5) libev4 (>= 4.04)

6) libgcc-s1 (>= 3.0)

7) libjansson4 (>= 2.1)

8) libsqlite3-0 (>= 3.5.9)

9) libssl1.1 (>= 1.1.0)

10) libstdc++6 (>= 7)

11) libsystemd 0

12) libuuid1 (>= 2.16)

13) zlib1g (>= 1.2.3.3)

6.2.2. *Порядок установки*

Установка агента в формате deb пакетов

1) Установить пакеты из зависимостей, выполнив в терминале в ОС (Ubuntu/ Debian/Astra) следующую команду:

«sudo apt install libbrotli1 libcurl3-gnutls libelf1 \ libev4 libjansson4 libsqlite3-0 \libssl1.1 libuuid1 zlib1g»

2) Установить deb-пакет агента EDR в ОС (Ubuntu/Debian/Astra), выполнив в терминале следующую команду:

«sudo dpkg -i avd_1.x.x_amd64.deb»

Установка агента в формате rpm пакетов

1) Для установки пакетов из зависимостей в ОС Red OS 7.3 в терминале выполнить следующие команды:

«sudo dnf install jansson-2.14-1.e17 .x86_64»

«sudo dnf install libev-4.33-1.e17. x86_64»

2) Установить rpm-пакет агента EDR в ОС ReD OS 7.3, выполнив в терминале следующую команду:

«sudo rpm –U avd-1.3.0-redos.x86_64.rpm»

6.2.3. *Первая настройка*

Указать в конфигурационном файле /opt/avd/etc/avd.conf актуальное значение для customerId, а также адрес сервера EDR - вместо localhost указать IP-адрес или доменное имя сервера, например:

```
customerId=9e391e34f921fa4e
http {
  ...
  server=edr.vr-protect.ru
  ...
}
```

Вместо имени можно указать адрес сервера:

```
  server=192.168.1.1
```

Генерация токена выполняется агентом автоматически при первом запуске, однако токен можно задать принудительно, указав в конфигурационном файле его значение в формате:

token=...

6.2.4. *Запуск*

Запустить сервис агента, выполнив в терминале следующую команду:

«sudo systemctl start avd»

В дальнейшем сервис будет стартовать автоматически при запуске ОС.

Примечание

После успешной первоначальной установки Агент должен появиться в списке верификации на сервере EDR. После обновления Агента верификация не требуется.

После установки DEB-пакета в системе появится systemd сервис avd.

Основные файлы (исполняемый модуль сервиса, динамические библиотеки, конфигурационные файлы) сохраняются в системе по пути:

/opt/avd/

Параметры работы сервиса агента могут быть заданы через конфигурационный файл:

/opt/avd/etc/avd.conf

6.3 *Точка восстановления ОС, созданная при установке агента*

Точка восстановления – специальная функция в операционной системе Windows, которая позволяет сохранить текущие настройки компьютера. После выполнения этой операции пользователь сможет без особого труда вернуться к рабочему состоянию устройства после появления неполадок или сбоя в работе системы.

Если при установке агента была создана точка восстановления, то для восстановления состояния системы в состояние, предшествующее установке агента, следует произвести следующие действия:

1) Нажать правой кнопкой мыши на меню **Пуск** и зайти в **Панель управления**.

2) Перейти в раздел **Система и безопасность** – **Система** – **Защита системы**.

3) В окне **Защита системы** нажать кнопку **Восстановить**.

4) В открывшемся окне **Восстановление системы** указать в поле выбора **Выбрать другую точку восстановления**. Откроется окно, представленное на рисунке 16.

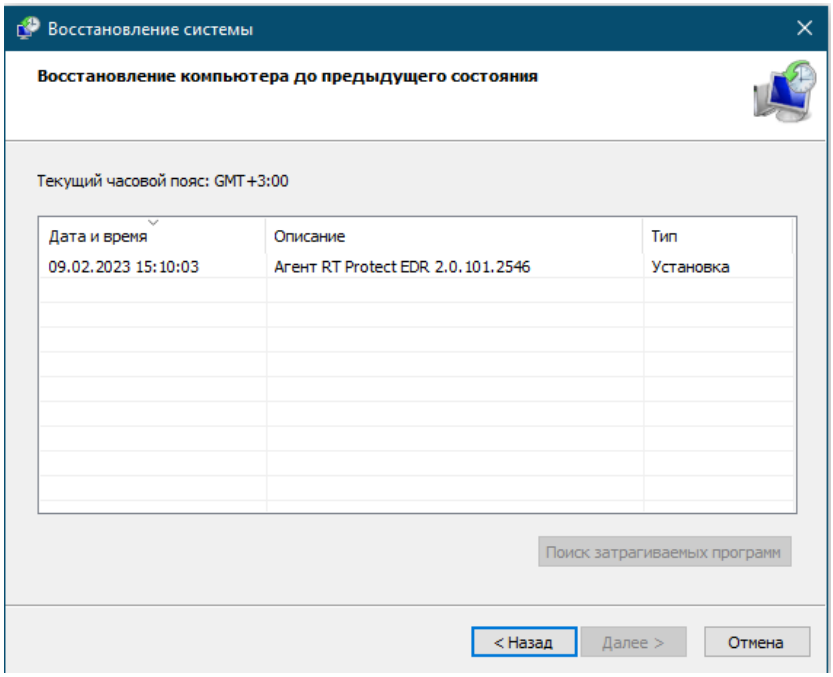

Рисунок 16 – Точка восстановления системы

5) Выбрать точку восстановления, созданную при установке Агента EDR, выделив соответствующую строчку из списка. Появится окно, представленное на рисунке 17.

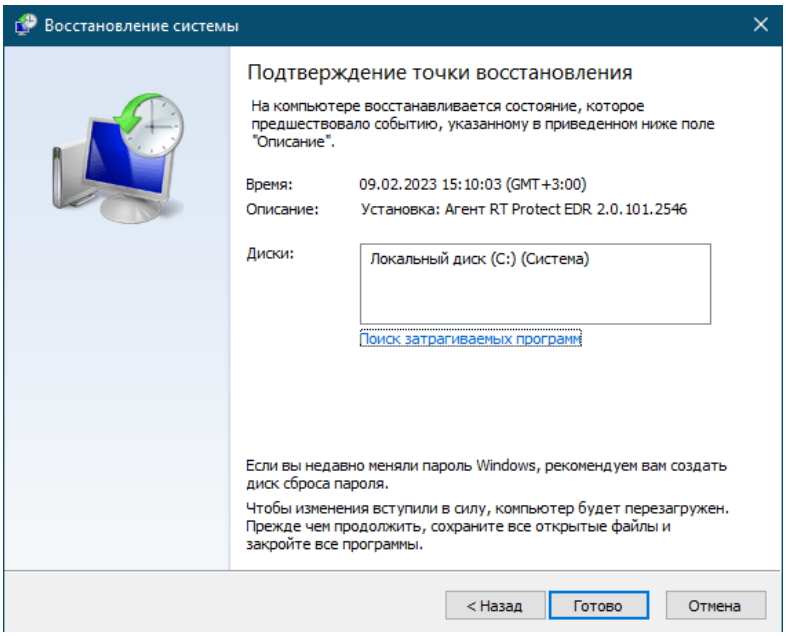

Рисунок 17 – Подтверждение точки восстановления

6) Подтвердить действие, нажав по кнопке **Готово**.

7. Удаление Агента

7.1 *Удаление агента в ОС Windows*

Удаление Агента (в ОС Windows) с конечной точки можно произвести следующими способами:

1) С помощью программы деинсталлятора - uninstall.exe, которая находится в папке: Program Files/ИБ Реформ/Agent_RT_Protect_EDR_;

2) Штатным способом удаления программ, через панель управления/установка и удаление программ;

3) В режиме командной строки, набрав команды:

– Uninstall/noUI – запуск удаления программы без показа пользовательского интерфейса;

– Uninstall/noUI/canReboot – запуск удаления программы без показа пользовательского интерфейса и разрешением перезагрузки без запроса к пользователю.

Примечание: Для удаления агента, с включенной опцией **Парольная защита от удаления** требуется ввести пароль, который сгенерирован на Сервере управления и доступен для копирования и просмотра пользователю с ролью **Администратор.**

7.2 *Удаление агента в ОС Linux*

Удаление Агента (в ОС Linux) с конечной точки можно произвести, набрав в терминале следующую команду:

«sudo dpkg -r avd»

Удаление Агента (в ОС RED OS) с конечной точки можно произвести, набрав в терминале следующую команду:

«sudo rpm –e avd»

8. Порядок решения основных пользовательских задач

8.1 Общие сведения

Система имеет клиент-серверную архитектуру. Программный компонент клиента (Агент), установленный на конечной точке, взаимодействует с серверной частью системы по защищенному TLS-каналу.

8.2 Состав компонентов агента EDR для ОС Windows

1) Компоненты ядра:

– драйвер агента, работающий в режиме ядра системы;

– драйвер контроля USB, работающий в режиме ядра системы.

2) Прикладные компоненты:

– служба, работающая в режиме пользователя;

– модуль системного трея (опционально).

Драйвер агента состоит из следующих модулей:

1) модуль контроля целостности компонентов агента;

2) модуль защиты файлов от программ-шифровальщиков;

3) модуль управления драйвером контроля USB;

4) модули мониторинга событий на конечной точке:

– монитор файловой системы;

– монитор реестра;

– монитор процессов;

– монитор сетевого взаимодействия;

– коррелятор правил обнаружения вредоносной активности.

Служба агента состоит из следующих модулей:

– модуль взаимодействия с сервером СОВ;

– модуль сбора статистики;

– модуль слежения за событиями системных журналов;

– модуль сканирования и анализа файлов;

– модуль исполнения команд, полученных от сервера СОВ;

– модуль работы с метаданными агента СОВ.

8.3 *Состав компонентов агента EDR для ОС Linux*

Агент состоит из трёх компонентов:

1) Исполняемый модуль - сервис «служба» systemd, запускаемый от имени суперпользователя при загрузке ОС. Название сервиса и исполняемого файла - avd.

2) BPF модули - набор BPF программ, загружаемый в ядро ОС по инициативе сервиса.

3) Модуль ядра. Загружается в ядро ОС по инициативе сервиса.

8.4 *Состав компонентов серверной части*

Серверная часть Программы состоит из следующих компонентов:

1) Балансировщик нагрузки (реализован на Nginx);

2) Веб-сервер (реализован на OpenResty);

3) Кеш-сервис (реализован на Redis);

4) Буфер для поступающих событий (реализован на Redis);

5) БД (база данных) для Django-приложения (реализована на PostgreSQL);

6) Объектное хранилище (хранилище файлов) с API (реализовано на Minio);

7) БД для событий и инцидентов (реализована на Elasticsearch);

8) Воркеры (записывают поступающие события в БД Elasticsearch) – проприетарный компонент, разработанный на языке Python;

9) Веб-приложение на Django – основной проприетарный компонент, реализующий бизнес-логику системы (разработан на языке Python).

Компоненты 1-7 являются известными общедоступными решениями, поддерживаемыми сообществом Open Source разработчиков и интегрированными в разрабатываемую систему.

Компоненты 8-9 собираются из исходного кода, разработанного на предприятии-изготовителе Изделия.

8.5 *Обобщённый алгоритм работы*

Клиент осуществляет мониторинг системной активности с целью выявления вредоносного поведения согласно правилам поведенческого анализа, полученным им от сервера. Клиент собирает статистику системной активности и периодически отправляет ее на сервер.

Сервер имеет административный модуль (frontend) для визуального представления профиля агента, его состояния, статистических данных, обнаруженных инцидентов безопасности и прочей информации, которая может быть полезна Администратору для наблюдения за Агентом в динамике.

Административный модуль сервера имеет функции управления Агентом – блокирования сети, отправления скрипта на выполнение и так далее.

8.6 *Порядок получения обновлений Программы и антивирусных баз*

Программа поставляется пользователю на основании договора о поставке, заключенного между Пользователем и Предприятием-изготовителем.

Программа поставляется в комплектности согласно документу «RT Protect EDR. Формуляр».

Указания по эксплуатации, применению, установке и направлению рекламаций на Программу содержатся в документах «Руководство Администратора» и «Формуляр». Обновление версии дистрибутива Агента производится Администратором.

9. Сообщения об ошибках

Большинство ошибок можно разделить на следующие типы:

1) Ошибки конфигурации:

– некорректные настройки параметров безопасности;

– некорректная установка компонентов Программы;

– некорректные действие со стороны Пользователя/Администратора;

– критические ошибки.

2) Ошибки оборудования:

– выход из строя аппаратных средств, на которых установлена Программа;

– выход из строя Сервера (или компонентов на Сервере), с которыми взаимодействуют компоненты Программы, установленные на оборудовании Пользователя;

– перебои питания со стороны клиентской или серверной части.

При возникновении ошибки Пользователю не следует самостоятельно заниматься устранением ошибки. Пользователь обращается к Администратору, который согласно процедурам, описанным в документе «Руководство администратора», устраняет выявленные ошибки.

10. Термины и определения

Перечень терминов и определений указан в таблице 2.

Таблица 3 – Термины и определения

Реагирование на инцидент ИБ	Структурированная совокупность действий, направленная на установление деталей инцидента, минимизацию ущерба от инцидента и предотвращение повторения инцидента ИБ
Целевая атака	Атака, нацеленная на одного человека, компанию или группу. В процессе атаки может использоваться различное вредоносное программное обеспечение и методы социальной инженерии
APT-Атака (ADVANCED PERSISTENT THREAT)	Сложная, продолжительная, хорошо спланированная многоходовая атака, использующая сложное вредоносное ПО, методы социальной инженерии и данные об информационной инфраструктуре атакуемого
БД	База данных
БД ПКВ	Базы данных признаков компьютерных вирусов
Индикаторы компрометации (IOC)	Наблюдаемая в компьютерной сети или на одном из компьютеров сущность, наличие которой может свидетельствовать о компрометации ИС. Обычно под такими индикаторами понимают IP-адреса, URL-адреса, хеши файлов
Информационная безопасность (ИБ)	Сфера науки и техники, охватывающая совокупность проблем, связанных с обеспечением защищенности объектов информационной сферы в условиях существования угроз. Под информационной безопасностью также понимают защищенность информации от несанкционированного ознакомления, преобразования и уничтожения, защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности
Инцидент ИБ	Нарушение или угроза нарушения ИБ компании
ИС	Информационная система
ИТ	Информационная технология
КВ	Компьютерные вирусы
Машинное обучение	Класс методов искусственного интеллекта, характерной чертой которых является не прямое решение задачи, а обучение в процессе применения решений множества сходных задач. Для построения таких методов используются средства математической статистики, численных методов, математического анализа, методов оптимизации, теории вероятностей, теории графов, различные техники работы с данными в цифровой форме
ОС	Операционная система
ПБ	Политика безопасности

ПО	Программное обеспечение
САВЗ	Средства антивирусной защиты
Событие ИБ	Любое идентифицированное явление в системе или сети
СУБД	Система управления базой данных
Угроза ИБ	Потенциально возможное событие, действие (воздействие), процесс или явление, создающее опасность возникновения инцидента ИБ
УД	Уровень доверия
Уязвимость информационной системы (ИС)	Недостаток в ИС, используя который внешний злоумышленник может намеренно реализовать угрозу ИБ
Эксплоит (EXPLOIT)	Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на ИС