**Описание функциональных характеристик**

**ПО «FINDLER»**

# 

# **Аннотация**

Настоящий документ содержит описание функциональных характеристик ПО «FINDLER», в том числе описание ПО, информацию о назначении ПО, описание основных функциональных характеристик и возможностей ПО, а также задачи, реализуемые при помощи платформы.

# **Содержание документа**

[Аннотация 2](#_6azvk1jd91d4)

[Содержание документа 3](#_ldxgxl3dcwxv)

[Описание и назначение ПО 4](#_n5qqbmh9pgg)

[Выполнение программы 4](#_x3rfcttfyq6n)

[Задача: “Изучение текущей статистики уровня защищенности” 4](#_51vhdvmvlgmm)

[Задача: “Анализ информации о текущих угрозах” 4](#_7xqpjhvkxqee)

[Задача: “Выгрузка информации об угрозах” 5](#_jn1oggp2ihvb)

[Задача: “Добавление комментариев к угрозам” 5](#_m7yfeoojhs8c)

[Задача: “Фильтр угроз” 6](#_e3s2f2qn63fp)

[Задача: “Добавление поддоменов” 6](#_sb2h6pn5j4sm)

[Задача: “Работа с доверенными сетями” 6](#_pamol7qb0eyc)

[Задача: “Работа с отчетом” 7](#_ggz8mkhbaunp)

[Задача: “Подключение Телеграма” 7](#_idiu4w3yhhiy)

[Информация для контактов 7](#_h3adh52sigm4)

# **Описание и назначение ПО**

ПО «FINDLER**»** — программное обеспечение, позволяющее анализировать и выявлять уязвимые точки системы пользователя в реальном времени. ПО “FINDLER” представляет собой SaaS решение.

ПО позволяет:

- выявлять угрозы;

- изучать статистику уровня защищенности;

- анализировать информацию о текущих угрозах;

- выгружать информацию об угрозах;

- добавлять комментарии к угрозам;

- фильтровать угрозы;

- добавлять поддомены;

- работать с доверенными сетями;

- изучать отчеты и выгружать информацию по ним;

- осуществлять взаимодействие с ботом Findler через Телеграм.

# **Выполнение программы**

ПО “FINDLER” работает на постоянной основе автоматически, ежедневно выявляет текущие угрозы. Следующие задачи пользователь должен выполнять вручную.

## **Задача: “Изучение текущей статистики уровня защищенности”**

Для выполнения данной задачи пользователю необходимо осуществить следующие действия:

1. Перейти главную страницу ПО “FINDLER”.
2. Изучить статистическую информацию в полях “Общий уровень защищенности”, “Все хосты”, “Общие показатели рисков по уровням”, “Обнаружено угроз”, “Обнаружено CVE, “Статистика CVE”, “Хосты с CVE”, “Опасные ссылки”, “Опасные порты”.
3. В случае необходимости, изменить временной промежуток для отображения статистики, нажав на кнопку с календарем, выбрав даты начала и конца периода, а затем нажав на кнопку “Применить”.

Выполнение задачи завершено.

## **Задача:** “**Анализ информации о текущих угрозах”**

Для выполнения данной задачи пользователю необходимо осуществить следующие действия:

1. Для анализа опасных ссылок по доменам необходимо перейти в раздел “Опасные ссылки по доменам”, нажав на ссылку “Опасные ссылки” и выбрав “По доменам”.
2. Для анализа опасных ссылок по ip необходимо перейти в раздел “Опасные ссылки по ip”, нажав на ссылку “Опасные ссылки” и выбрав “По IP”.
3. Для анализа опасных открытых портов необходимо перейти в раздел “Опасные открытые порты”.
4. Для анализа CVE необходимо перейти в раздел “Хосты с CVE”. Помимо прочего, пользователь может изучить рекомендации по устранению угроз, нажав на кнопку с тремя точками справа от хоста и изучив предложенную информацию в открывшемся подразделе.
5. Для анализа информации по хостам необходимо перейти в раздел “Все хосты”.
6. Обратить внимание на то, что низкий уровень угроз отмечен зеленым цветом, средний уровень угроз - оранжевым, высокий уровень угроз - красным, критический - бордовым, отсутствующий - серым.

Выполнение задачи завершено.

## **Задача: “Выгрузка информации об угрозах”**

Для выполнения данной задачи пользователю необходимо осуществить следующие действия:

1. Для выгрузки информации об опасных ссылках по доменам необходимо перейти в раздел “Опасные ссылки по доменам” и нажать кнопку со стрелкой, направленной вниз, или файла с форматом CSV.
2. Для выгрузки информации об опасных ссылках по ip необходимо перейти в раздел “Опасные ссылки по ip” и нажать кнопку со стрелкой, направленной вниз, или файла с форматом CSV.
3. Для выгрузки информации об опасных открытых портах необходимо перейти в раздел “Опасные открытые порты” и нажать кнопку со стрелкой, направленной вниз, или файла с форматом CSV.
4. Для выгрузки информации о CVE необходимо перейти в раздел “Хосты с CVE” и нажать кнопку со стрелкой, направленной вниз, или файла с форматом CSV.
5. Для выгрузки информации по хостам необходимо перейти в раздел “Все хосты” и нажать кнопку со стрелкой, направленной вниз, или файла с форматом CSV.

Выполнение задачи завершено.

## **Задача: “Добавление комментариев к угрозам”**

Для выполнения данной задачи пользователю необходимо осуществить следующие действия:

1. Для добавления комментариев к опасным ссылкам по доменам необходимо перейти в раздел “Опасные ссылки по доменам” и добавить комментарий, нажав на кнопку с тремя точками справа от угрозы, введя комментарий в соответствующее поле и нажав после этого кнопку со стрелкой, направленной вверх;
2. Для добавления комментариев к опасным ссылкам по ip необходимо перейти в раздел “Опасные ссылки по ip” и добавить комментарий, нажав на кнопку с тремя точками справа от угрозы, введя комментарий в соответствующее поле и нажав после этого кнопку со стрелкой, направленной вверх;
3. Для добавления комментариев к CVE необходимо перейти в раздел “Хосты с CVE” и добавить комментарий, нажав на кнопку с тремя точками справа от хоста и перейдя в подраздел “Комментарии”, введя комментарий в соответствующее поле и нажав после этого кнопку со стрелкой, направленной вверх;
4. Для добавления комментариев к хостам необходимо перейти в раздел “Все хосты” и добавить комментарий, нажав на кнопку с тремя точками справа от хоста и введя комментарий в соответствующее поле и нажав после этого кнопку со стрелкой, направленной вверх;

Выполнение задачи завершено.

## **Задача: “Фильтр угроз”**

Для выполнения данной задачи пользователю необходимо осуществить следующие действия:

1. Для фильтра опасных ссылок по доменам необходимо перейти в раздел “Опасные ссылки по доменам”, нажать кнопку с ползунками и выбрать необходимые критерии.
2. Для фильтра ссылок по ip необходимо перейти в раздел “Опасные ссылки по ip”, нажать кнопку с ползунками и выбрать необходимые критерии.
3. Для фильтра опасных открытых портов необходимо перейти в раздел “Опасные открытые порты”, нажать кнопку с ползунками и выбрать необходимые критерии.
4. Для фильтра CVE необходимо перейти в раздел “Хосты с CVE”, нажать кнопку с ползунками и выбрать необходимые критерии.
5. Для фильтра хостов необходимо перейти в раздел “Все хосты”, нажать кнопку с ползунками и выбрать необходимые критерии.

Выполнение задачи завершено.

## **Задача: “Добавление поддоменов”**

Для выполнения данной задачи пользователю необходимо осуществить следующие действия:

1. Нажать на кнопку “+” справа от ссылки на раздел “Все хосты” (находится в левой части интерфейса).
2. Ввести в пустое поле домены (по одному на строку)
3. Добавить поддомен, нажав на синюю кнопку “Добавить”.

Выполнение задачи завершено.

## **Задача: “Работа с доверенными сетями”**

Для выполнения данной задачи пользователю необходимо осуществить следующие действия:

1. Перейти в поле настроек, нажав на кнопку, расположенную в правом верхнем углу, и выбрать раздел “Доверенные сети”.
2. Изучить текущие доверенные сети.
3. Добавить доверенную сеть, реализовав следующие действия:

* нажать кнопку “Добавить” в разделе “Доверенные сети”;
* ввести доверенные ip адреса или подсети в формате "x.x.x.x/m название";
* нажать кнопку “Добавить” внизу.

1. Удалить доверенную сеть, нажав на крестик справа от нее.

Выполнение задачи завершено.

## **Задача: “Работа с отчетом”**

Для выполнения данной задачи пользователю необходимо осуществить следующие действия:

1. Перейти в поле настроек, нажав на кнопку, расположенную в правом верхнем углу, и выбрать раздел “Отчет”.
2. Изучить текущие отчет.
3. Выбрать промежуток отчета, нажав на поле “Период” и выбрав необходимый период времени.
4. Выгрузить информацию, нажав на кнопку с направленной вниз стрелкой.
5. Существует возможность загрузки отчета с помощью нажатия на функцию “Отчет” в левом поле интерфейса.

Выполнение задачи завершено.

## **Задача: “Подключение Телеграма”**

Для выполнения данной задачи пользователю необходимо осуществить следующие действия:

1. Перейти в поле настроек, нажав на кнопку, расположенную в правом верхнем углу, и выбрать функцию “Подключить Телеграм”.
2. Осуществлять взаимодействие через Телеграм с ботом Findler.

Выполнение задачи завершено.

# **Информация для контактов**

Для контактов с командой разработчиков просьба обращаться по следующим контактам:

Email:

[a.tomilov@rebrandy.co](mailto:a.tomilov@rebrandy.co)

[a.orlov@rebrandy.co](mailto:a.orlov@rebrandy.co)

[info@rebrandy.co](mailto:info@rebrandy.co)

Телефон: +79220020942