

Программный комплекс

Руководство пользователя

Аннотация

Данный документ представляет собой руководство пользователя для работы с программным комплексом по защите системно-технической инфраструктуры «SimuStrike» (далее – ПК «SimuStrike», комплекс). Руководство содержит сведения, необходимые пользователям для установки и настройки работы комплекса. Пользователь должен знать стандартные программные средства (операционные системы, утилиты, офисные пакеты, антивирусные пакеты), а также обладать общими знаниями по администрированию сетевых устройств.

ПК «SimuStrike» служит для специалистов следующих направлений:

- по информационной безопасности (ИБ). Позволяет использовать комплекс для регулярного тестирования устойчивости информационной инфраструктуры и проверки наличия уязвимостей;
- центра мониторинга и реагирования на киберугрозы, которые занимаются обеспечением кибербезопасности. Комплекс позволяет оценить, что центр отслеживает все атаки на инфраструктуру, а также для оценить реакцию установленных продуктов ИБ на угрозы;
- групп инженеров по тестированию на проникновение. Использование комплекса для автоматизации проверки инфраструктуры позволяет повысить эффективность тестирования.

Содержание

1	Сведения о комплексе, технические и программные средства, обеспечивающие выполнение функций программы	4
1.1	Общие сведения о комплексе	4
1.2	Требования к составу и параметрам технических средств.....	5
1.3	Требования к сетевым портам ПК «Simustrike»	6
1.4	Рекомендуемая последовательность действий при работе с комплексом	6
2	Площадки и агенты.....	8
2.1	Добавление нового агента.....	17
3	Кампании.....	25
3.1	Основные настройки кампании	25
3.2	Разведка	27
3.2.1	Сканирование сети	27
3.2.2	Web сканирование	36
3.2.3	Сканирование инфраструктуры	49
3.2.4	Локальная разведка.....	64
3.3	Эксплуатация.....	75
3.3.1	Фишинг.....	86
3.4	Перемещение в сети.....	86
3.4.1	Перебор УЗ.....	97
4	Фишинг	105
4.1	Мониторинг	105
4.2	Задания	106
4.3	Шаблоны писем	110
4.4	Группы рассылки	111
4.5	Целевые страницы.....	121
4.6	Профили отправителей	122
5	Карточка кампании	127
5.1	Сводка	128
5.2	Карта	128
5.3	Агенты	130
5.4	Задания.....	134
5.5	Объекты	138
6	Библиотека.....	141
6.1.1	Словари	142
6.1.2	Эксплойты	146
6.1.3	Инструментальные модули	148
7	Администрирование	149
7.1	Настройки	149
7.2	Лицензия	150
8	Уведомления.....	152
9	Отчеты.....	154
	Перечень терминов и определений.....	156
	Перечень сокращений	159

1 Сведения о комплексе, технические и программные средства, обеспечивающие выполнение функций программы

1.1 Общие сведения о комплексе

ПК «SimuStrike» является продуктом класса Breach and Attack Simulation (BAS) и предназначен для специалистов по ИБ для регулярного тестирования устойчивости информационной инфраструктуры и проверки наличия уязвимостей.

ПК предназначен для использования в составе программно-технических средств (ПТС) защиты информации, подсистем обеспечения информационной безопасности, а также как отдельное средство для автоматизации тестирования существующих процессов с целью выявления уязвимостей в ИТ-инфраструктуре организации. Решение обеспечивает последовательную и непрерывную проверку защищенности, имитируя различные варианты атак и позволяет осуществлять наблюдение за реагированием ИТ-инфраструктуры организации на угрозы.

ПК расширяет классическое представление о системах симуляции атак, предоставляя не только инструменты для оценки уязвимости инфраструктуры, но также и систему сбора обратной связи от средств защиты, обеспечивая непрерывную информационную поддержку для инженеров ИБ и операторов «Центров Мониторинга».

ПК «SimuStrike» служит для:

- специалистов по информационной безопасности. Использование ПК для регулярного тестирования устойчивости информационной инфраструктуры и проверки наличия уязвимостей;
- специалистов центра мониторинга и реагирования на киберугрозы, которые занимаются обеспечением кибербезопасности. Использование ПК для проверки того, что центр действительно видит все атаки на инфраструктуру, а также для оценки реакции установленных продуктов информационной безопасности на угрозы;
- групп инженеров на исследование на проникновение. Использование ПК для автоматизации проверки инфраструктуры, что позволяет повысить эффективность тестирования.

Более подробно класс решаемых задач рассмотрен в документе «Описание применения».

ПК «SimuStrike» состоит из централизованного сервера и веб-интерфейса. Сервер отвечает за запуск автоматизированных сценариев кибератак, а интерфейс позволяет конфигурировать многоэтапные атаки, собирая их из готовых модулей, и отслеживать реакцию систем защиты в реальном времени.

Ниже представлена схема основных компонентов ПК «SimuStrike» (рис. 1).

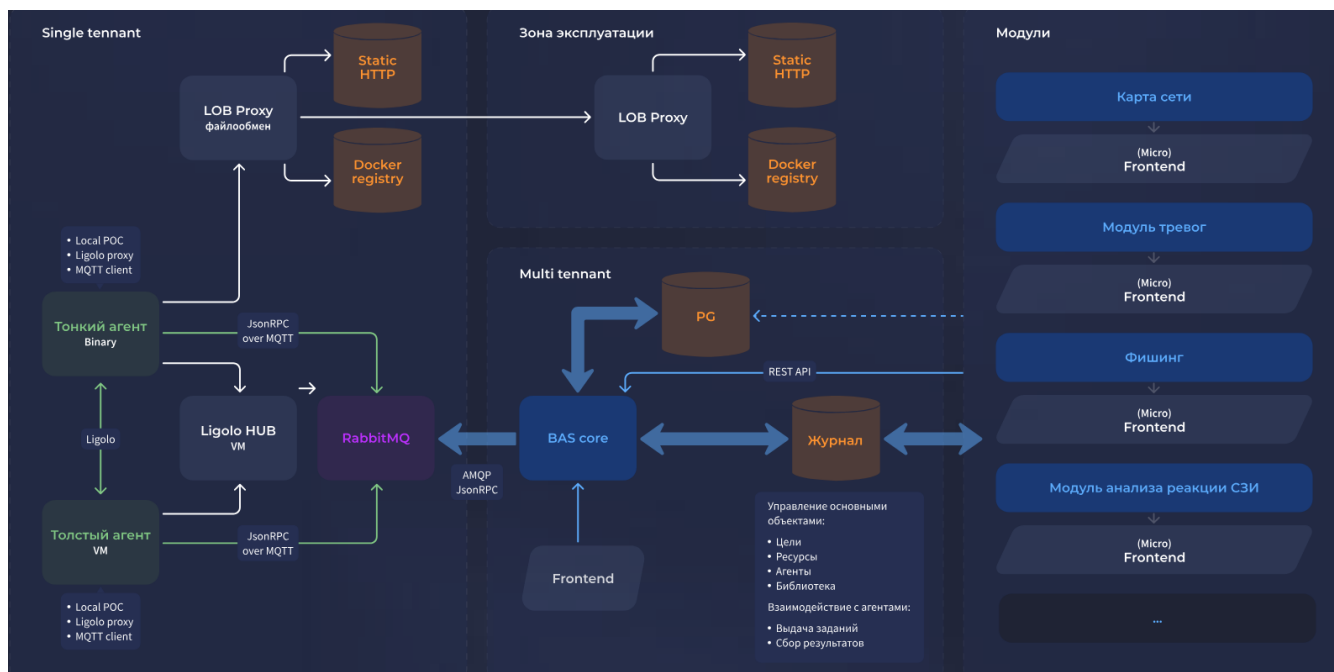


Рисунок 1 – Схема основных компонентов ПК «SimuStrike»

Примечание. В текущем релизе функциональные возможности комплекса работают в тестовом режиме, поэтому реализован доступ с ограниченной функциональностью.

1.2 Требования к составу и параметрам технических средств

Технические характеристики электронных вычислительных машин (ЭВМ), на базе которых созданы автоматизированные рабочие места (АРМ) оператора и администратора ПК, должны иметь характеристики, приведенные ниже.

Для АРМ ПК не ниже:

- процессор с частотой не менее 1,8 ГГц;
- оперативное запоминающее устройство (ОЗУ) с объемом памяти не менее 8 Гбайт;
- жесткий диск объемом не менее 100 Гбайт;
- сетевой адаптер с пропускной способностью не менее 100Мбит/1Гбит/с.

Для сервера ПК не ниже:

- 8-и ядерный процессор с частотой не менее 1.8 ГГц;
- ОЗУ с объемом памяти не менее 16 Гбайт;
- жесткий диск объемом не менее 500 Гбайт;
- сетевой адаптер с пропускной способностью не менее 1Гбит/с.

Для корректной работы сервера управления ПК необходимы следующие программные средства:

- операционная система: ОС семейства Linux (версия ядра 5.19 и выше).

- СУБД:
 - PostgreSQL 13 и выше;
 - Jatoba, сертификат соответствия № 4327 (выдан ФСТЭК России 19.11.2020 г.);
- программное обеспечение Docker Engine актуальной версии.

1.3 Требования к сетевым портам ПК «Simustrike»

- 1) Платформа
 - Подключение к внешней СУБД PSGr – порт 5432/TCP;
 - Синхронизация времени (NTP) – порт 123/UDP;
 - Подключение к почтовым серверам SMTP – порт 25/TCP;
 - Удалённое управление комплексом SSH – порт 22/TCP;
 - Веб-интерфейс пользователя:
 - HTTP – порт 80/TCP;
 - HTTPS – порт 443/TCP.
 - Подключение к подсистеме LOB – порт 8444/TCP.
- 2) Резидент
 - Подключение платформы и агентов к резиденту – порт 1884/TCP;
 - Подключение агентов к системе LOB на резиденте – порт 8888/TCP.

1.4 Рекомендуемая последовательность действий при работе с комплексом

- 1) Аутентифицироваться в ПК «SimuStrike» под своим логином и паролем, выданным администратором. Для этого необходимо в веб-браузере перейти по сетевому адресу приложения и войти в комплекс, используя выданные уникальные логин и пароль, чтобы получить авторизованный доступ к личному рабочему пространству.
- 2) Создать площадку. Для этого необходимо в главном меню последовательно выбрать в разделе «Администрирование» подраздел «Агенты», нажать кнопку «Добавить площадку», заполнить форму требуемыми параметрами и нажать кнопку «Добавить».
- 3) Установить резидента в соответствии с выбранным сценарием в инфраструктуру:
 - Моделирование атаки внешнего нарушителя. Находясь во внешней сети, BAS подключается к резиденту по внешнему адресу, передавая ему задачи по атаке внутренних ресурсов организации; резидент, в свою очередь, выполняет эти задачи (сканирование, распространение, сбор данных) изнутри сети, а развёрнутые в ней агенты подключаются к резиденту по указанному адресу для получения исполняемых модулей.
 - Моделирование атаки внутреннего нарушителя. Находясь внутри сети, BAS подключается к резиденту по внутреннему адресу, ставит ему задачи на атаку других внутренних ресурсов (например, перемещение по сети и поиск ценных

данных), после чего резидент выполняет эти задачи, а агенты, как и сам BAS, подключаются к нему для дальнейшей работы.

- 4) Создать кампанию и заполнить «Основные настройки». Для создания кампании необходимо в разделе «Кампании» главного меню нажать кнопку «Добавить кампанию», перейти в блок «Основные настройки» и заполнить обязательные поля.
- 5) В созданной кампании выбрать, настроить и активировать необходимые целевые модули. Выбрать из предложенного списка и детально настроить конкретные методы атаки (модули), которые резидент будет выполнять в рамках сценария.
- 6) Сохранить и запустить созданную кампанию. После активации всех нужных модулей нажать кнопку «Завершить создание кампании», после чего резидент начнет выполнять все активированные и настроенные модули атаки.
- 7) Осуществить мониторинг на странице карточки кампании. Для осуществления мониторинга необходимо открыть соответствующую кампанию в разделе «Кампании» и выбрать нужную вкладку.
- 8) Завершить кампанию в случае необходимости. Для завершения кампании с целью сбора финальных логов и освобождения ресурсов комплекса при достижении целей или возникновении такой необходимости следует в разделе «Кампании» открыть нужную кампанию, нажать кнопку «Управление» и выбрать опцию «Завершить кампанию».

2 Площадки и агенты

Примечание. Работа с комплексом начинается с установки резидента, который служит основным агентом в процессе атаки. Резидент является агентом ПК, который выполняет задачи по проведению кибератак в рамках заданных сценариев.

Площадка — это часть поверхности атаки, доступная резиденту. Например, если резидент установлен удаленно от инфраструктуры, он может начать атаку с внешнего веб-сервера. В случае, когда резидент установлен внутри инфраструктуры, он имитирует внутреннего нарушителя. Резидент, являясь важнейшим элементом комплекса и обладая всеми необходимыми инструментами для проведения атак, обязателен для функционирования комплекса, поскольку без него невозможно задействовать основные функции.

Для добавления площадки и основного агента необходимо:

- 1) Запустить веб-браузер и ввести в адресной строке открывшегося окна сетевой адрес приложения. Сетевой адрес приложения пользователю должен сообщить администратор, занимающийся обслуживанием комплекса, например, <https://bas.ru/login>.
- 2) На экране монитора откроется страница авторизации пользователя. Необходимо указать имя учетной записи пользователя, пароль и нажать кнопку «Войти в систему».
- 3) В главном меню перейти в раздел «Администрирование», затем в раздел «Агенты» (рис. 2).

Площадка	Адрес для агентов	Адрес для ВАС адреса	Статус	Агенты/онлайн
Площадка_2Площадка_2Площадка_2...	212.199.35.545835	melton.com:53636	Не установлен	8/0
12345678901234567890123456789012...	160.38.139.1.14634	valdez.com:23563	Не установлен	6/0
f93be69-b17e-4ef6-bb8e-c1fc812fd398	15.79.253.177.8017	palmer-dean.biz:56780	Не установлен	1/0
79a846d2-b873-4a11-8d21-08ac799d26...	23.112.113.61.5783	brooks.org:62457	Не установлен	4/0
Площадка11	127.0.0.2.443	127.0.0.1:9000	Не установлен	1/0
Площадка22	127.0.0.2.443	10.5.25.5.65535	Не установлен	1/0
111-22.04.2025	rabbitmq:1884	10.116.231.28:1884	Не установлен	2/0
a4909920-3a12-4d48-ad57-eb187ed13bf2	212.158.240.136:47572	mcbride-carroll.biz:26521	Не установлен	1/0
70c4c81f-e796-4f69-b71e-52755a7c0ea1	170.122.52.168:65535	jimenez.com:65535	Не установлен	1/0
f3bdcd8d-229a-4fa0-8ac8-998b61a7dfab	197.1.244.172:37969	smith.com:32726	Не установлен	1/0
58f0713f-380d-4ed5-a79e-1f6811095b62	105.4.119.87:65535	gordon.com:65535	Не установлен	1/0
c52fd4e7-7357-48be-ad50-c02af5b27ae9	159.108.234.4:15559	ryan.com:54878	Не установлен	1/0
e972b1a4-126b-49a1-8cac-dbd05e2ca02	179.105.249.112:65535	lee.com:65535	Не установлен	1/0
22345678901234567890123456789012...	76.33.87.33:6905	lowe-esparza.com:1406	Не установлен	1/0
22222	102.9.226.88:37470	munoz.com:7457	Не установлен	1/0
A18q9H1U5agxGwMMLh6RjzKjRkydL...	146.147.125.151:11046	shaw-dominguez.biz:25...	Не установлен	1/0
a7WNkbiU7zENZ35jEKTevyKAdom4g...	104.51.53.77:4136	turner.com:10400	Не установлен	1/0

Рисунок 2 – Раздел «Агенты»

- 4) Настроить площадки и агенты. Для этого в правом верхнем углу нажать кнопку «Добавить площадку».
- 5) Заполнить форму добавления площадки требуемыми параметрами (рис. 3):
 - название площадки – генерируется автоматически (например «Площадка-29.07.2025»). При необходимости название площадки можно изменить;
 - комментарий – поле для указания дополнительной информации;
 - переключатели:
 - использовать порты по умолчанию – включен/выключен (по умолчанию включен);
 - общий адрес агента и модуля обновления – включен/выключен (по умолчанию включен);
 - адрес для площадки – IP-адрес (IPv4, IPv6) или доменное имя, которое будет использоваться ПК «SimuStrike» для обращения к резиденту. В зависимости от настроек сети, может быть внешним (белым) или внутренним (серым) адресом. Необходимо учитывать маршрутизацию и сетевой адрес (NA). Указывается в формате: IP-адрес 10.5.25.5, порт 1884.
 - адрес для агента – IP-адрес (IPv4, IPv6) или доменное имя, которое будет использоваться для настройки сетевого подключения агентов к резидент-агенту (площадке). В зависимости от настроек сети, может быть внешним (белым) или внутренним (серым) адресом. Необходимо учитывать маршрутизацию и NA;
 - адрес обновления модулей – IP-адрес (IPv4, IPv6) или доменное имя, которое будет использоваться для обращения за модулями для агентов. Сетевое взаимодействие осуществляется от агента к резидент-агенту

(площадке). Чаще всего, этот адрес совпадает с полем «Адрес для Агента». Может быть изменен, если это необходимо.

- 6) Нажать кнопку «Добавить».

Примечание. При отключении параметра «Использовать порты по умолчанию» появляется возможность вручную указать порты подключения. Если отключить параметр «Общий адрес агента и модуля обновления», поле «Адрес обновления модулей» станет доступным для редактирования.

× Добавить площадку

Подготовка:

1. Выделите физическую или виртуальную машину на ОС RedOS 7.3+
2. Настройте сетевую доступность и маршрутизацию, в зависимости от целей площадки (внешний доступ, локальная сеть, контейнер)
- 2.a (Опционально) Присвойте FQDN и проверьте его доступность в целевой сети
3. Запишите или скопируйте сетевые параметры (IP-Адрес или FQDN)
4. Заполните необходимые настройки в форме и нажмите **Добавить**

Дополнительная информация приведена в подсказках к полям, а также в документации.

Название площадки

Площадка-29.07.2025

Комментарий

Добавьте комментарий

Использовать порты по умолчанию



Общий адрес агента и модуля обновления



Адрес для площадки ⓘ

Укажите адрес для площадки

1884

Адрес для Агента ⓘ

Укажите адрес для агента

1884

Адрес обновления модулей ⓘ

8888

Добавить

Отменить

Рисунок 3 – Окно «Добавить площадку»

- 7) После добавления площадки необходимо в диалоговом окне «Агенты» выбрать ее в списке (рис. 4).

Площадка-тестдок	111.111.111.111:440	10.5.25.4:440	Не установлен	1/0			
Тест							
Название агента	Тип	Статус	IP адрес	Последнее соединение	Привилегии агента	Сетевые интерфейсы	Исполнение задачи
Master-a960e702	Резидент	offline	-	-	-	-	-

Рисунок 4 – Созданная площадка

- 8) Для установки агента развернуть созданную площадку и нажать кнопку .
- 9) В открывшемся окне «Установка резидента» скопировать скрипт с помощью кнопки «Копировать в буфер». Перейти на электронно-вычислительную машину (ЭВМ), планируемую для установки агента, запустить терминал с правами администратора и выполнить скрипт (рис. 5).

×

Установка резидента

Название агента

Master-a960e702

Тип агента

Резидент

UUID агента

e80f9cd5-299d-4c9c-8445-d656718a8460

Вид загрузки

Bash скрипт

Отключить проверку SSL ⓘ

☐

Установить tar ⓘ

☐

Скрипт установки

```
curl -location -X POST -d '{"token": "XXX"}' "https://core.dev-1.bas.dev.da.lan/api/v1/core/agents/e80f9cd5-299d-4c9c-8445-d656718a8460/package" -o resident-e80f9cd5-299d-4c9c-8445-
```

Копировать в буфер

Скрипт нужно скопировать

ⓘ На хосте должен быть docker Linux

Заккрыть

Рисунок 5 – Окно «Установка резидента»

- 10) После успешной установки резидента на хосте в веб-интерфейсе отобразится резидент со статусом «Онлайн». После выполнения всех обязательных шагов можно приступить к созданию и настройке кампании (рис. 6).

Агенты

🔍 Введите запрос для поиска

+ Добавить площадку

Площадка	Адрес для агентов	Address for BAS core	Статус	Агенты/онлайн			
▼ Площадка-30.07.2025	192.168.223.133:1884	192.168.223.133:1884	✓ online	1/1			
Название агента	Тип	Статус	IP адрес	Последнее соединение	Привилегии агента	Сетевые интерфейсы	Исполнение задачи
Master-Seed564bc	Резидент	✓ online	-	30.07.2025 15:37	-	-	-

Рисунок 6 – Резидент со статусом онлайн

Для просмотра карточки площадки необходимо:

- 1) В разделе «Агенты» в перечне площадок выбрать требуемую и нажать на ее название, после чего откроется карточка площадки (рис. 7).

✕ Площадка-04.07.2025

Статус

✓ online

Описание

тест тонкий агент новые настройки площадки

Параметры

Адрес для агентов

10.116.231.28:1884

Адрес для площадки

10.116.231.28:1884

Адрес обновления модулей

test:1884

Площадка создана

04.07.2025 11:40

Агенты

Название агента	Тип	Статус	IP адрес
Master-52a1e1f5	Резидент	✓ online	-
Агент-b363509b	Тонкий	✓ online	-
Агент-7152a6f1	Тонкий	⊗ offline	-
Агент-bfea13d6	Толстый	⊗ offline	-
Агент-475c298f	Тонкий	⊗ offline	-

Заккрыть

Рисунок 7 – Окно «Площадка»

- 2) Просмотреть информацию карточки площадки. Описание полей приведено в таблице 1.

Таблица 1 – Карточка площадки

Элемент	Описание
Название площадки	Текстовое поле для указания названия площадки
Статус площадки	Текущее состояние площадки. Отображает два статуса: онлайн (активен), офлайн (неактивен)
Описание	Комментарий к площадке
Параметры	
Адрес для агентов	IP-адрес и порт для подключения агентов
Адрес для площадки	IP-адрес и порт для самой площадки
Адрес обновления модулей	IP-адрес для загрузки обновлений
Дата создания	Дата и время создания площадки
Агенты	Приводится перечень агентов для площадки
Название агента	Имя агента
Тип агента	«Резидент», «Тонкий», «Толстый»
Статус агента	«онлайн» или «офлайн»
IP-адрес	IP-адрес агента

3) Нажать кнопку «Заккрыть» для завершения работы с окном.

Для редактирования или удаления площадки необходимо:

- 1) Для редактирования площадки нажать кнопку .
- 2) В открывшемся окне «Редактировать площадку» (рис. 8) внести изменения и нажать «Сохранить».

✕ Редактировать площадку

Название площадки	Площадка-30.07.2025	
Комментарий	Добавьте комментарий	
Использовать порты по умолчанию	☒	
Общий адрес агента и модуля обновления	☒	
Адрес для площадки ⓘ	192.168.223.133	1884
Адрес для Агента ⓘ	192.168.223.133	1884
Адрес обновления модулей ⓘ	192.168.223.133	8888

Рисунок 8 – Окно «Редактировать площадку»

- 3) Для удаления площадки нажать кнопку . Удаление площадки возможно только после удаления всех связанных агентов.
- 4) В открывшемся окне «Удалить площадку» (рис. 9) нажать кнопку «Скачать информацию», а затем нажать кнопку «Удалить». Скачивание информации обязательно для завершения процесса.

Удалить площадку: **Площадка22**

Агенты будут удалены только из интерфейса. Для полного удаления
① необходимо остановить все контейнеры и запущенные сервисы на хосте, а также удалить скачанные архивы самостоятельно

1. Скачайте информацию по резиденту, после можно будет удалить площадку

↓ Скачать информацию

Удалить

Отменить

Рисунок 9 – Окно «Удалить площадку»

2.1 Добавление нового агента

На первом этапе устанавливается резидент, который служит основным агентом в процессе атаки. После его установки можно добавлять тонкие агенты на любое количество ЭВМ без необходимости проведения активной атаки. Это позволяет расширить контроль над инфраструктурой.

В ПК выделяются следующие типы агентов:

- тонкий агент;
- толстый агент;
- умный агент.

Тонкий агент используют для закрепления и распространения в инфраструктуре, он не содержит большого количества инструментов, но способен выполнять скрипты и при необходимости загружать дополнительные инструменты. Это позволяет таким агентам быть гибкими и адаптивными в процессе атаки, обеспечивая возможность быстрого реагирования на изменяющиеся условия.

Толстый агент необходим для выполнения ряда ключевых задач в комплексе и является основным агентом. Он содержит все необходимые инструменты и функции для проведения проверок, сканирования и анализа, что позволяет эффективно выявлять уязвимости и угрозы. Кроме того, толстый агент способен запускать Proof of Concept (PoC) скрипты и инструменты для анализа защищенности, что позволяет тестировать решения в реальных условиях. Толстый агент обрабатывает и анализирует большие объемы данных, что способствует более глубокому пониманию состояния безопасности системы. Он способен функционировать независимо, что позволяет ему выполнять задачи даже в условиях ограниченной сетевой связи. Дополнительно, толстый агент может взаимодействовать с другими компонентами и системами безопасности, обеспечивая комплексный подход к защите информации. Таким образом, толстый агент играет ключевую роль в обеспечении безопасности и эффективности работы комплекса.

Умный агент предоставляет необходимые вычислительные мощности «bare metal» для выполнения ресурсоемких операций, включая перебор хеш-сумм паролей и потенциальные атаки методом полного перебора (брутфорса).

Администратор инфраструктуры может использовать тонкие агенты для имитации внутреннего нарушителя или для распространения в сети без эксплуатации уязвимостей. Такой подход обеспечивает гибкость и возможность скрытого мониторинга, что делает его эффективным инструментом для анализа безопасности и выявления потенциальных угроз.

Для добавления нового агента необходимо:

- 1) Открыть веб-интерфейс и перейти на вкладку «Агенты».
- 2) Выбрать необходимую площадку из доступного списка (рис. 10).

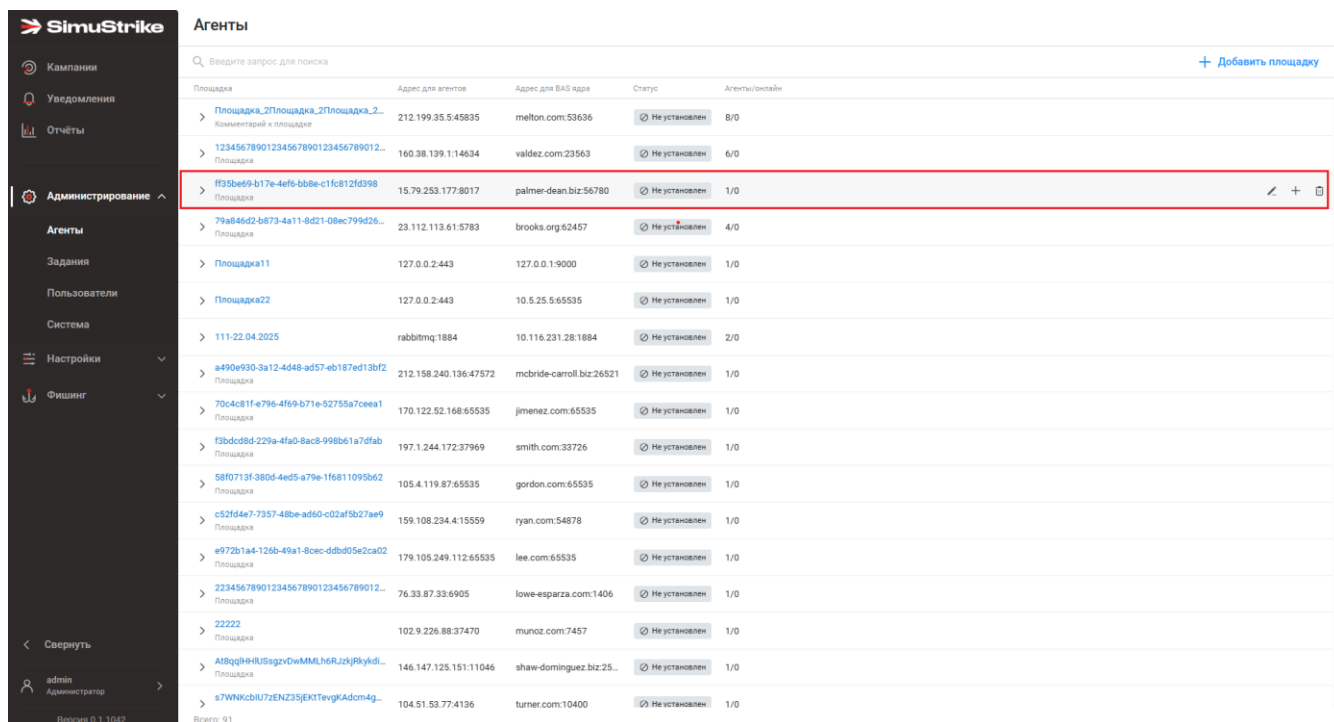


Рисунок 10 – Вкладка «Агенты»

- 3) В строке с выбранной площадкой нажать кнопку .
- 4) В открывшейся форме добавления агента заполнить обязательные поля (рис. 11):
 - выбрать тип агента (толстый/тонкий);
 - ввести название агента. Допускается использование латинского алфавита, кириллицы и цифр. К указанному названию автоматически добавляются 8 случайных символов латинского алфавита и цифр для обеспечения уникальности;
 - добавить комментарий при необходимости.

× Добавить агента

Тип агента ⓘ

Тонкий

Толстый

Площадка

bbb

Название агента

Агент

-f245b534

Комментарий

Добавьте комментарий

Добавить

Отменить

Рисунок 11 – Окно «Добавить агента»

- 5) После заполнения всех обязательных полей нажать кнопку «Добавить» для добавления нового агента на площадку.

Для просмотра карточки агента необходимо:

- 1) Раскрыть выбранную площадку при помощи кнопки ▼ и найти установленного агента. Нажать на имя агента, чтобы открыть его карточку (рис. 12).

✕ Агент-b363509b

Статус агента	✓ online
Описание	-
Последнее соединение	31.07.2025 16:01

Площадка

Название площадки	Площадка-04.07.2025
Описание	тест тонкий агент новые настройки площадки

Параметры

Идентификатор агента	b363509b-32b1-4c3f-9263-4795aca063f9
Архитектура процессора	x86
Операционная система	linux
Тип агента	Тонкий
Версия агента	SOME VERSION
Пользователь ОС агента	-
Агент создан	04.07.2025 12:30

Сетевые интерфейсы

Сетевые интерфейсы не найдены

Маршруты

Сеть	Шлюз	Iface	Приоритет	Тип
0.0.0.0/0	10.116.231.1	eth0	-	Unicast

[Заккрыть](#)

Рисунок 12 – Окно «Агент»

- 2) Просмотреть информацию карточки агента. Описание полей приведено в таблице 2.

Таблица 2 – Карточка агента

Элемент	Описание
Агент	Уникальный идентификатор агента в системе
Статус	Текущее состояние агента: online (активен) или offline (недоступен)
Описание	Текстовое поле для добавления комментария
Последнее соединение	Дата и время последней успешной связи агента с сервером
Площадка	Площадка, к которой привязан агент
Название	Имя площадки
Описание	Детали конфигурации или тестового окружения
Параметры агента	Технические характеристики агента
Идентификатор	Уникальный UUID агента для системного отслеживания
Архитектура процессора	Тип процессора: x86 (32-бит) или x64 (64-бит)
ОС	Операционная система агента (Linux, Windows и т.д.)
Тип агента	Тип агента с минимальными ресурсами
Версия	Версия ПО агента
Пользователь ОС	Учётная запись, от которой работает агент (если доступно)
Дата создания	Дата развёртывания агента
Сетевые интерфейсы	Список сетевых адаптеров
Маршруты	Правила маршрутизации сетевого трафика
Сеть	Диапазон IP-адресов
Шлюз	IP-адрес шлюза для выхода во внешнюю сеть
Интерфейс	Имя сетевого интерфейса
Приоритет	Приоритет маршрута
Тип	Тип передачи данных

3) Нажать кнопку «Заккрыть» для завершения работы с окном.

Для редактирования агента необходимо:

- 1) Раскрыть выбранную площадку при помощи кнопки  и найти установленного агента (рис. 13).

Агенты

Введите запрос для поиска

Добавить площадку

Площадка	Адрес для агентов	Адрес для BAS ядра	Статус	Агенты/онлайн			
Площадка_2Площадка_2Площадка_2... Комментарий к площадке	212.199.35.545835	melton.com:53636	Не установлен	8/0			
12345678901234567890123456789012... Площадка	160.38.139.1:14634	valdez.com:23563	Не установлен	6/0			
f35be69-b17e-4ef6-bb8e-c1fc812fd398 Площадка	15.79.253.177:8017	palmer-dean.biz:56780	Не установлен	1/0			
Название агента	Тип	Статус	IP адрес	Последнее соединение	Привилегии агента	Сетевые интерфейсы	Исполнение задачи
Master-e51c346c	Резидент	offline	-	-	-	-	-
79a846d2-b873-4a11-8d21-08ec799d26... Площадка	23.112.113.61:5783	brooks.org:62457	Не установлен	4/0			
Название агента	Тип	Статус	IP адрес	Последнее соединение	Привилегии агента	Сетевые интерфейсы	Исполнение задачи
Master-b5a16d23	Резидент	offline	-	-	-	-	-
Агент1-34616c57	Тонкий	offline	-	-	-	-	-
Агент2-61140d8d	Тонкий	offline	-	-	-	-	-
Агент3-356623db	Тонкий	offline	-	-	-	-	-

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали площадки

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d

Агент3-356623db

Детали агента

79a846d2-b873-4a11-8d21-08ec799d26...

Площадка

Название агента

Master-b5a16d23

Агент1-34616c57

Агент2-61140d8d</

Рисунок 13 – Окно «Агенты»

- 2) Нажать кнопку  для редактирования агента.
- 3) В открывшемся окне «Редактировать агента» внести нужные изменения и нажать кнопку «Сохранить» (рис. 14).

× Редактировать агента

Тип агента	Основной	
Площадка	79a846d2-b873-4a11-8d21-08ec799d2625	
Название агента	Master	-b5a16d23
Комментарий	Добавьте комментарий	

Сохранить

Отменить

Рисунок 14 – Окно «Редактировать агента»

Удаление происходит только из интерфейса, при необходимости полного удаления необходимо проделать следующие шаги:

- 1) Раскрыть выбранную площадку при помощи кнопки  и найти установленного агента.

- 2) Нажать кнопку .
- 3) В открывшемся окне «Удалить агента» нажать кнопку «Скачать информацию», а затем нажать кнопку «Удалить» для завершения процесса (рис. 15).

Удалить агента: **Агент1-34616c57**

Агенты будут удалены только из интерфейса. Для полного удаления
 необходимо остановить все контейнеры и запущенные сервисы на хосте, а также удалить скачанные архивы самостоятельно

1. Скачайте информацию по агенту, после можно будет удалить агента  [Скачать информацию](#)
2. Удалите агента из системы
3. Удалите агента на хосте (см. скаченный файл)

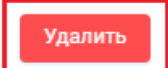
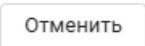
 

Рисунок 15 – Окно «Удалить агента»

3 Кампании

Кампании представляют собой имитацию многоступенчатых хакерских атак. Их можно настраивать различными способами, включая сценарии, которые моделируют действия только внутренних нарушителей. В таких случаях достаточно активировать модули эксплуатации, перемещения в сети и закрепления, в то время как разведка может не потребоваться.

Кампании имитируют модель Kill Chain, охватывающую любое количество этапов. Они могут варьироваться от сложных сценариев, в которых задействованы все доступные модули, до одноступенчатых атак, когда злонамеренный сотрудник предпринимает действия, превышающие его привилегии, что может привести к уничтожению информации или её утечке.

Кроме того, кампанию можно настроить на постоянную имитацию атак в течение длительного времени, что позволяет непрерывно контролировать эффективность средств защиты информации (СрЗИ). Кампании также можно комбинировать и чередовать. Например, фишинговую кампанию можно направить на один сегмент предприятия, в то время как атаки с эксплуатацией уязвимостей будут нацелены на другую часть компании.

Примечание. Для добавления кампании в комплекс необходимо предварительно добавить требуемые площадки и агенты. Модули в настройках кампании при необходимости настраиваются отдельно.

3.1 Основные настройки кампании

Основные настройки необходимы для обеспечения эффективного управления кампаниями, так как они позволяют ограничить временные рамки и определить целевые площадки.

Для указания основных настроек необходимо:

- 1) Перейти в раздел «Кампании» в главном меню комплекса.
- 2) В открывшемся разделе нажать кнопку «Добавить кампанию» (рис. 16).

Кампания	Статус	Площадки	Задачи	Дата создания	План, дата начала	План, дата завершения	Уведомления	Автор
Кампания-b7cc3f6c	Черновик	-	-	04.12.2025 23:54	-	∞∞	-	admin
Кампания-3e7c0108	Черновик	-	-	04.12.2025 20:53	-	∞∞	-	admin
Кампания-2d4547de	Черновик	-	-	04.12.2025 19:22	-	∞∞	-	admin
Кампания-faff5871	В работе	1	Task_bash+cred-checker-demo...	04.12.2025 19:12	-	∞∞	-	admin
Кампания-608b0b9d	Завершена	1	Task_m0-module-cve-2021-420...	04.12.2025 19:06	-	∞∞	-	admin
Кампания-1c92ae2e	Завершена	1	Task_m0-module-serp-vuln-sca...	04.12.2025 19:02	-	∞∞	-	admin
Кампания-ba93a5ff	Завершена	1	Task_m0-module-serp-vuln-sca...	04.12.2025 18:58	-	∞∞	-	admin
Кампания-f3bbae6f	Завершена	1	Task_m0-module-serp-vuln-sca...	04.12.2025 18:56	-	∞∞	-	admin
Кампания-516d3faa	Завершена	1	Task_m0-module-serp-vuln-sca...	04.12.2025 18:45	-	∞∞	-	admin
Кампания-e6767216	Черновик	-	-	04.12.2025 18:51	-	∞∞	-	admin
Кампания-0efba85f	Завершена	1	Task_m0-module-serp-vuln-sca...	04.12.2025 17:16	-	∞∞	-	admin
Кампания-e108110a	Черновик	-	-	04.12.2025 17:26	-	∞∞	-	admin
Кампания-d361896b	В работе	1	-	04.12.2025 16:12	-	∞∞	-	admin
Кампания-2a3260c9	Черновик	-	-	04.12.2025 12:34	-	∞∞	-	admin

Рисунок 16 – Раздел «Кампании»

3) В окне создания кампании перейти в блок «Основные настройки» (рис. 17).

Создать кампанию: Кампания-b7cc3f6c Черновик

Срок действия лицензии истек. Перейти на другую лицензию

Основные настройки (Настроен)

Разведка

- Сканирование сети
- Web сканирование
- Сканирование инфраструктуры
- Локальная разведка

Получение доступа

- Фишинг
- Эксплуатация

Общие настройки | Поверхность атаки | Объекты | Словари | Исключения | Расписание

Название кампании: Кампания -b7cc3f6c

Описание: Укажите описание

Выбор площадки: DA-Main

Рисунок 17 – Вкладка «Основные настройки»

- 4) Заполнить обязательные поля настроек во вкладке «Основные настройки»:
- указать название кампании;
 - ввести краткое описание кампании;
 - выбрать необходимую площадку из предложенного списка.
- 5) Во вкладке «Расписание» выбрать период и время запуска (рис. fig:pic11116?).

- 6) После указания всех необходимых полей в блоке «Основные настройки» появится надпись «Настроен». При необходимости внесения дальнейших изменений в кампанию перейти к следующим подразделам окна создания кампании. В случае, если на текущий момент настройки завершены, нажать кнопку «Завершить создание кампании».

Примечание. В дальнейшем в созданную кампанию можно внести изменения путем редактирования записи.

3.2 Разведка

Разведка требуется в процессе подготовки к атакам, так как она позволяет собирать дополнительную информацию об атакуемой инфраструктуре и оценивать наиболее подходящие векторы для осуществления атаки. Этот этап включает комплекс мер, реализуемых с помощью модулей сканирования сети и веб-сканирования, что позволяет выявить уязвимости и уязвимые места в системе. Эффективная разведка способствует более точному планированию атак и повышает вероятность успешного выполнения поставленных задач.

3.2.1 Сканирование сети

Сканирование сети участвует в обеспечении безопасности информационной инфраструктуры предприятия. Оно позволяет выявлять уязвимости как внутри сетевой инфраструктуры, так и в отдельных её элементах, таких как сетевые устройства, рабочие ЭВМ пользователей и серверы.

Добавление настроек по сканированию сети осуществляется после указания основных настроек кампании. Для этого необходимо:

- 1) Перейти в блок «Разведка» в окне «Создать кампанию».
- 2) Открыть подраздел «Сканирование сети» и перейти к заполнению настроек.

- 3) Установить переключатель в поле «Расширить поверхность атаки» (по умолчанию активирован). Активация данного параметра означает, что новые цели, найденные в ходе кампании будут использоваться модулем (рис. 18).

< Создать кампанию: Кампания-4fd43027 Черновик

 Основные настройки

✓ Настроен

 Разведка

Сканирование сети 

✓ Настроен  1

Web сканирование 

✓ Настроен  1

Сканирование инфраструктуры 

Локальная разведка 

 Получение доступа

Фишинг 

Эксплуатация 

Перебор УЗ 

Перемещение в сети 

 Постэксплуатация

Завершить создание кампании

Расширить поверхность атаки  

Выбрать проверки [Добавить](#)

Цели сканирования [Добавить](#)

Рисунок 18 – Переключатель «Расширить поверхность атаки»

- 4) В поле «Цель сканирования» нажать кнопку «Добавить» (рис. 19).

< Создать кампанию: Кампания-4fd43027 Черновик

 Основные настройки

✓ Настроен

 Разведка

Сканирование сети 

✓ Настроен  1

Web сканирование 

✓ Настроен  1

Сканирование инфраструктуры 

Локальная разведка 

 Получение доступа

Фишинг 

Эксплуатация 

Перебор УЗ 

Перемещение в сети 

 Постэксплуатация

Завершить создание кампании

Расширить поверхность атаки  

Выбрать проверки 5 проверок

Цели сканирования 

Рисунок 19 – Добавление цели сканирования

- 5) В открывшемся окне «Добавить цели сканирования» нажать кнопку «Цель сканирования» (рис. 20).

× Добавить цели сканирования

🔍 Введите запрос для поиска

☰ Фильтр

⬇ Загрузить цели

+ Цель сканирования



Список пуст

Сохранить

Отменить

Рисунок 20 – Окно «Цель сканирования»

- 6) Заполнить требуемые поля (рис. 21):
- выбрать тип ресурса из выпадающего списка (IP-адрес, подсеть, доменные имена, диапазон IP-адресов);
 - ввести адрес цели, исходя из указанного выше типа ресурса;

- отключить переключатель «Исключения», который включен по умолчанию. Включение переключателя обозначает, что выбранный тип ресурса будет исключен из списка целей сканирования. Выключение обозначает, что будет добавлен как обычная цель для сканирования.

× Добавить цели сканирования

Тип ресурса

Адрес

Исключение

IP адрес

IP адрес

Подсеть

Доменные имена

Диапазон IP адресов

Введите запрос для поиска

Фильтр

Загрузить цели

+ Цель сканирования



Список пуст

Сохранить

Отменить

Рисунок 21 – Ввод данных для целей сканирования

- 7) Нажать кнопку «Добавить». В список добавятся заданные цели сканирования или исключения (рис. 22).

× **Добавить цели сканирования**

Тип ресурса	IP адрес
Адрес	192.12.12.12
Исключение	☐
Добавить Отменить	

[+ Цель сканирования](#)



Список пуст

Сохранить

Отменить

Рисунок 22 – Список добавленных целей

- 8) Для загрузки перечня целей доступно два варианта: использовать готовый файл через опцию «Загрузить цели из файла» или предварительно скачать шаблон в формате .txt через «Скачать шаблон», заполнить его и затем выполнить загрузку (рис. 23).

× **Добавить цели сканирования**

Тип ресурса IP адрес ▾

Адрес 192.12.12.12

Исключение ☐

Добавить Отменить

🔍 Введите запрос для поиска ≡ Фильтр ↓ Загрузить цели + Цель сканирования

Загрузить цели из файла

Скачать шаблон

Рисунок 23 – Кнопка «Загрузить цели»

- 9) Для осуществления поиска необходимо перейти в поле «Введите запрос для поиска» для поиска записи в списке. Поиск выполняется по мере ввода символов. При нажатии кнопки «Фильтр» открывается окно для указания параметров фильтрации (рис. 24):
- тип ресурса – выпадающий список для выбора категории;
 - кнопка «IP-адрес» – фильтрация по конкретным IP-адресам;
 - кнопка «Подсеть» – фильтрация по диапазонам (например, 192.168.1.0/24);
 - кнопка «Доменные имена» – фильтрация по URL (например, example.com);
 - состояние – переключатели для отбора целей по статусу:
 - кнопка «Все» – показывать все ресурсы (включая обычные и исключённые);
 - кнопка «Только исключения» – отображать только адреса, помеченные как «исключённые»;
 - кнопка «Без исключений» – скрыть все исключённые ресурсы;
 - переключатель «Только новые» – используется для отображения только недавно добавленных целей (например, после последнего сканирования);
 - кнопка «Применить» – активирует выбранные фильтры;
 - кнопка «Закрыть» – закрывает окно без сохранения настроек.

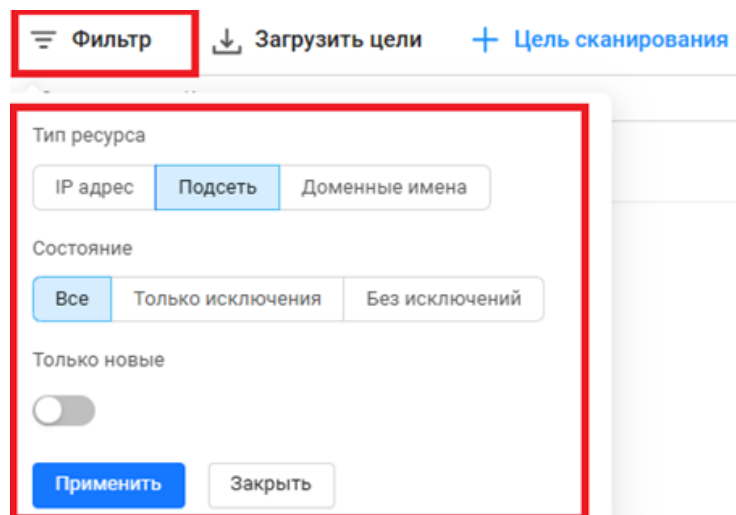


Рисунок 24 – Кнопка «Фильтр»

- 10) Выбрать цели из списка. При выборе целей из списка отображаются скрытые кнопки (рис. 25) для работы с выбранными целями:
- кнопка «Удалить» – для удаления выбранных ресурсов;
 - кнопка «Скачать» – для экспорта данных;
 - кнопка «Исключить» – выделяет ресурсы как исключенные из сканирования;
 - кнопка «Отменить исключение» – снимает отметку об исключении.

× **Добавить цели сканирования**

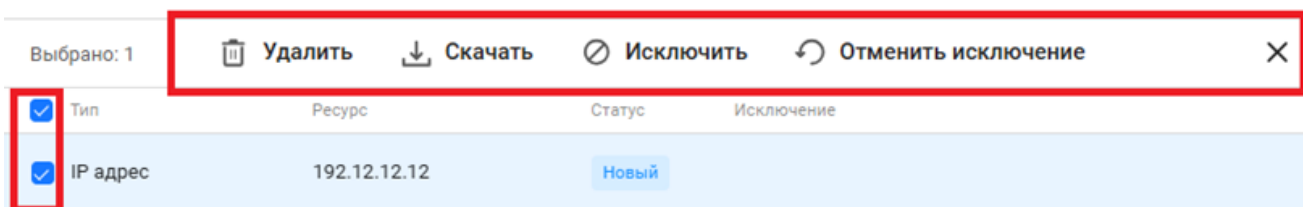


Рисунок 25 – Логика появления кнопок действий при выборе целей

Для исключения, удаления целей из списка возможно использование кнопок (рис. 26):

× **Добавить цели сканирования**

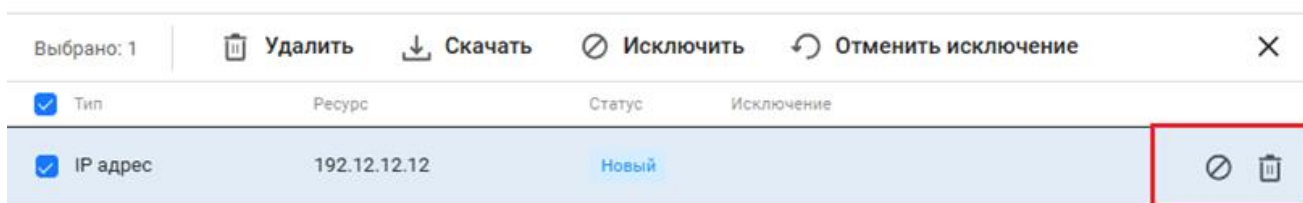


Рисунок 26 – Кнопки «Добавить в исключения» и «Удалить»

- 11) В окне «Добавить цели сканирования» после выбора целей нажать кнопку «Сохранить» для применения параметров (рис. 27). Для отмены настроек и выхода из окна нажать кнопку «Отменить».

× Добавить цели сканирования

Выбрано: 1



Удалить



Скачать



Исключить



Отменить исключение

☒ Тип

Ресурс

Статус

Исключение

☒ IP адрес

192.12.12.12

Новый

Всего: 1

Сохранить

Отменить

Рисунок 27 – Кнопка «Сохранить»

- 12) Активировать переключатель модуля «Сканирование сети» (рис. 28) и перейти к настройке модуля «Web сканирование».

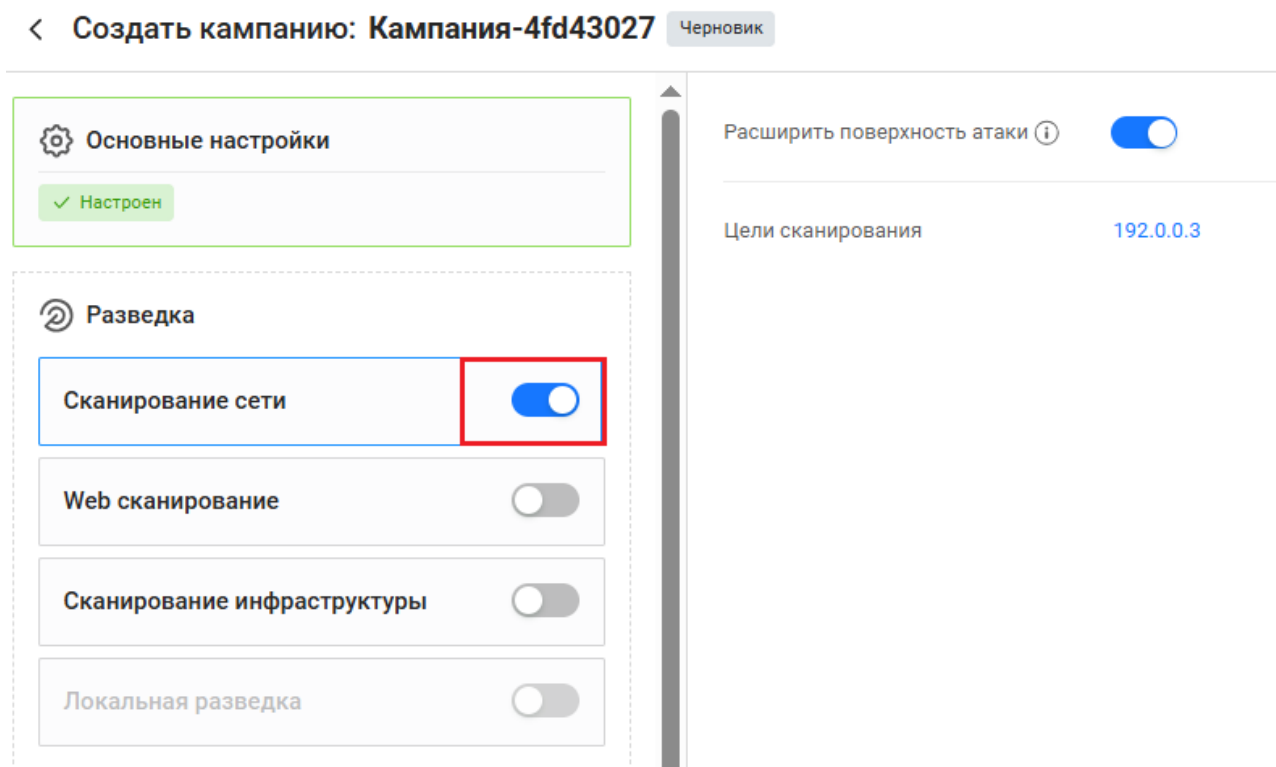


Рисунок 28 – Переключатель модуля «Сканирование сети»

Примечание. Некоторые тонкие настройки могут не работать в тестовом режиме.

3.2.2 Web сканирование

Web сканирование это процесс поиска уязвимостей веб-серверов, сервисов и приложений. Веб-сканер необходим для выявления возможных уязвимостей, которые могут быть использованы модулем эксплуатации. Кроме того, веб-сканер предоставляет информацию, такую как адреса электронной почты, которые могут быть использованы для фишинга.

Для добавления настроек веб-сканирования необходимо:

- 1) В блоке «Разведка» перейти к подразделу «Web сканирование» и заполнить настройки (рис. 29).

< Создать кампанию: Кампания-4fd43027 Черновик

⚙️ Основные настройки

✓ Настроен

🔍 Разведка

Сканирование сети

✓ Настроен 1

Web сканирование

Сканирование инфраструктуры

Локальная разведка

⚙️ Получение доступа

Фишинг

Эксплуатация

Перебор УЗ

Перемещение в сети

🔗 Постэксплуатация

Брутфорс

Завершить создание кампании

Расширить поверхность атаки ⓘ

Выбрать проверки

Добавить

Цели сканирования

Добавить

Рисунок 29 – Вкладка «Web сканирование»

- 2) Переключатель в поле «Расширить поверхность атаки» оставить без изменения (по умолчанию активирован). Это значит, что новые цели, найденные в ходе кампании, будут использоваться модулем (рис. 30).

< Создать кампанию: Кампания-4fd43027 Черновик

 Основные настройки

✓ Настроен

 Разведка

Сканирование сети 

✓ Настроен  1

Web сканирование 

Сканирование инфраструктуры 

Локальная разведка 

 Получение доступа

Фишинг 

Эксплуатация 

Перебор УЗ 

Перемещение в сети 

 Постэксплуатация

Брутфорс 

Расширить поверхность атаки  

Выбрать проверки [Добавить](#)

Цели сканирования [Добавить](#)

Завершить создание кампании

Рисунок 30 – Переключатель «Расширить поверхность атаки»

- 3) Указать проверки. Для этого в поле «Выбрать проверки» нажать кнопку «Добавить» (рис. 31).

< Создать кампанию: Кампания-4fd43027 Черновик

Основные настройки

✓ Настроен

Разведка

Сканирование сети

✓ Настроен 1

Web сканирование

Сканирование инфраструктуры

Локальная разведка

Получение доступа

Фишинг

Эксплуатация

Перебор УЗ

Перемещение в сети

Постэксплуатация

Брутфорс

Завершить создание кампании

Расширить поверхность атаки

Выбрать проверки

Добавить

Цели сканирования

Добавить

Рисунок 31 – Поле «Выбрать проверки»

- 4) В открывшемся окне «Добавить проверки» выбрать необходимые проверки из представленных в списке (рис. 32):
- поиск e-mail, телефонов, всех ссылок на сайте;
 - поиск используемых WEB технологий и CVE.

× Добавить проверки

☐ Описание	Название
☐ Поиск e-mail, телефонов, всех ссылок на сайте	btc-module-webserp-crawler-parser
☐ Поиск используемых WEB технологий и CVE	btc-module-webserp-wappalyzer

Всего: 2

Сохранить

Отменить

Рисунок 32 – Окно «Добавить проверки»

- 5) После выбора проверок нажать кнопку «Сохранить».
- 6) Доступна возможность указать цели сканирования. Для этого в поле «Цель сканирования» нажать кнопку «Добавить» (рис. 33).

< Создать кампанию: **Кампания-4fd43027** Черновик

 Основные настройки

✓ Настроен

 Разведка

Сканирование сети 

✓ Настроен  1

Web сканирование 

Сканирование инфраструктуры 

Локальная разведка 

 Получение доступа

Фишинг 

Эксплуатация 

Перебор УЗ 

Перемещение в сети 

 Постэксплуатация

Брутфорс 

Завершить создание кампании

Расширить поверхность атаки  

Выбрать проверки [Добавить](#)

Цели сканирования [Добавить](#)

Рисунок 33 – Поле «Цель сканирования»

7) В открывшемся окне «Добавить цели сканирования» (рис. 34), нажать кнопку «Цель сканирования».

× **Добавить цели сканирования**

🔍 Введите запрос для поиска

☰ Фильтр

⬇ Загрузить цели

+ **Цель сканирования**



Список пуст

Сохранить

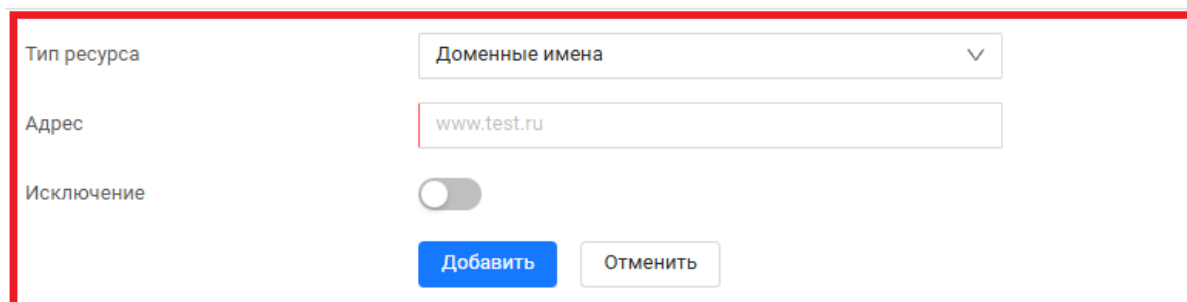
Отменить

Рисунок 34 – Окно «Добавить цели сканирования»

- 8) Заполнить требуемые поля (рис. 35):
- выбрать тип ресурса из выпадающего (доменные имена, URI, сервис);
 - ввести адрес цели, исходя из указанного выше типа ресурса;

- отключить переключатель «Исключения», который включен по умолчанию. Включение переключателя обозначает, что выбранный тип ресурса будет исключен из списка целей сканирования. Выключение обозначает, что будет добавлен как обычная цель для сканирования.

× Добавить цели сканирования



Тип ресурса	Доменные имена
Адрес	www.test.ru
Исключение	☐
<button>Добавить</button> <button>Отменить</button>	

🔍 Введите запрос для поиска

≡ Фильтр

⬇ Загрузить цели

+ Цель сканирования

Рисунок 35 – Ввод данных целей

- 9) Нажать кнопку «Добавить». В список добавятся заданные цели сканирования или исключения (рис. 36).

× Добавить цели сканирования

Тип ресурса

Адрес

Исключение ☐

Фильтр

Загрузить цели

+ Цель сканирования

☐ Тип	Ресурс	Статус	Исключение
☐ IP адрес	192.12.12.20	Новый	
☐ IP адрес	192.12.12.12	Новый	

Всего: 2

Рисунок 36 – Список добавленных целей

- 10) Для загрузки перечня целей можно сразу загрузить готовый файл через опцию «Загрузить цели из файла» или сначала скачать шаблон в формате .txt через «Скачать шаблон», заполнить его и затем загрузить (рис. 37).

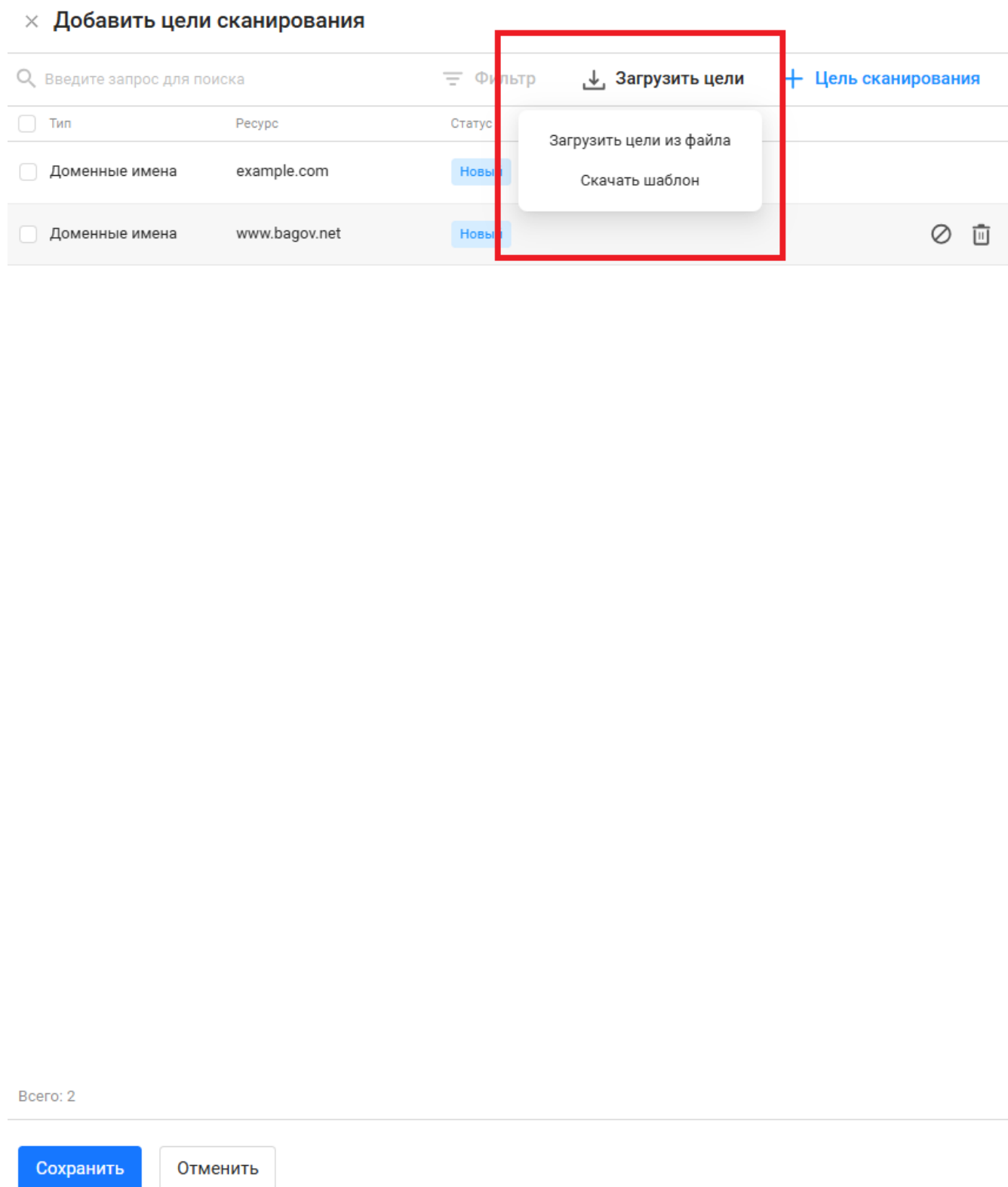


Рисунок 37 – Кнопка «Загрузить цели»

- 11) Выбрать цели из списка. При выборе целей из списка отображаются скрытые кнопки (рис. 38) для работы с выбранными целями:
- кнопка «Удалить» – для удаления выбранных ресурсов;
 - кнопка «Скачать» – для экспорта данных;
 - кнопка «Исключить» – выделяет ресурсы как исключенные из сканирования;

– кнопка «Отменить исключение» – снимает отметку об исключении.

× Добавить цели сканирования

Выбрано: 2	УдалитьСкачатьИсключитьОтменить исключение				×
☒	Тип	Ресурс	Статус	Исключение	
☒	Доменные имена	example.com	Новый		
☒	Доменные имена	www.bagov.net	Новый		

Всего: 2

Сохранить

Отменить

Рисунок 38 – Логика появления кнопок действий при выборе целей

Для исключения, удаления целей из списка возможно использование кнопок (рис. 39):

× Добавить цели сканирования

Выбрано: 2	Удалить	Скачать	Исключить	Отменить исключение	×
☒ Тип	Ресурс	Статус	Исключение		
☒ Доменные и...	htmlweb.ru				
☒ Подсеть	10.116.231.0/24				

Рисунок 39 – Кнопки «Добавить в исключения» и «Удалить»

- 12) В окне «Добавить цели сканирования» после выбора целей нажать кнопку «Сохранить» для применения параметров.
- 13) Активировать переключатель модуля «Web сканирование» (рис. 40) и перейти к настройке модуля «Сканирование инфраструктуры».

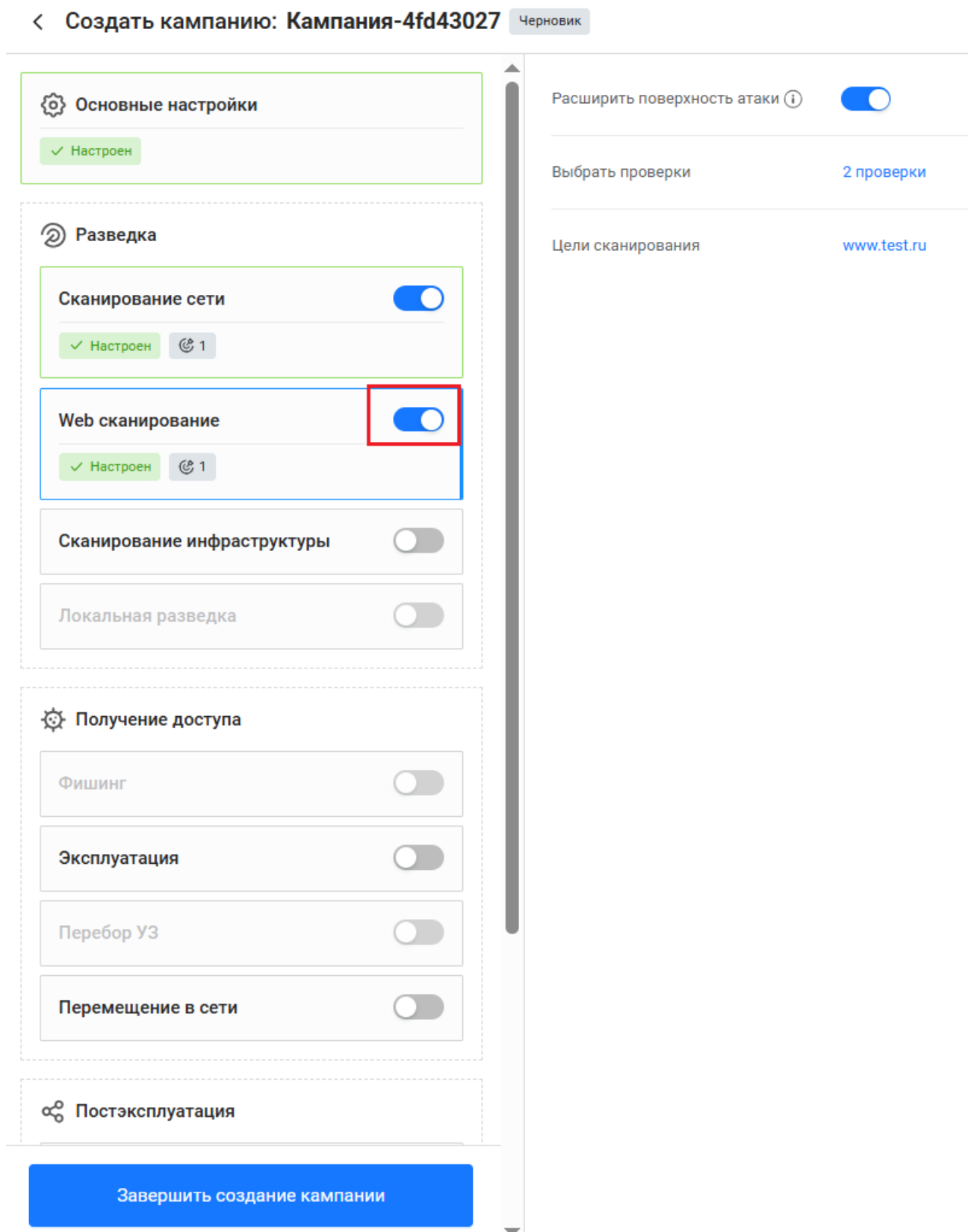


Рисунок 40 – Переключатель модуля «Web сканирование»

Примечание. Некоторые тонкие настройки могут не работать в тестовом режиме.

3.2.3 Сканирование инфраструктуры

Модуль сканирования инфраструктуры — это инструмент, предназначенный для проверки безопасности AD (активный каталог), который выполняет:

- выявление ошибочных конфигураций;
- поиск учетных данных пользователей;
- обнаружение хостов домена;
- хеш-сумм и паролей;
- поиск уязвимостей в инфраструктуре AD.

Для добавления настроек сканирования инфраструктуры необходимо:

- 1) В блоке «Разведка» перейти в подраздел «Сканирование инфраструктуры».
- 2) Открыть подраздел «Сканирование инфраструктуры» и перейти к заполнению требуемых настроек.
- 3) Переключатель в поле «Расширить поверхность атаки» оставить без изменения (по умолчанию активирован). Это значит, что новые цели, найденные в ходе кампании, будут использоваться модулем (рис. 41).

< Создать кампанию: Кампания-4fd43027 Черновик

 Основные настройки

✓ Настроен

 Разведка

Сканирование сети 

✓ Настроен  1

Web сканирование 

✓ Настроен  1

Сканирование инфраструктуры 

Локальная разведка 

 Получение доступа

Фишинг 

Эксплуатация 

Перебор УЗ 

Перемещение в сети 

 Постэксплуатация

Завершить создание кампании

Расширить поверхность атаки  

Выбрать проверки [Добавить](#)

Цели сканирования [Добавить](#)

Рисунок 41 – Переключатель «Расширить поверхность атаки»

- 4) В поле «Выбрать проверки» нажать кнопку «Добавить» (рис. 42).

< Создать кампанию: Кампания-4fd43027 Черновик

 Основные настройки

✓ Настроен

 Разведка

Сканирование сети 

✓ Настроен  1

Web сканирование 

✓ Настроен  1

Сканирование инфраструктуры 

Локальная разведка 

 Получение доступа

Фишинг 

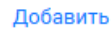
Эксплуатация 

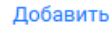
Перебор УЗ 

Перемещение в сети 

 Постэксплуатация

Расширить поверхность атаки  

Выбрать проверки 

Цели сканирования 

Завершить создание кампании

Рисунок 42 – Переключатель «Расширить поверхность атаки»

- 5) В открывшемся окне «Добавить проверки» выбрать необходимые проверки из представленных в списке (рис. 43):

- «Получение списка хостов подсети, дополнительной информации о хостах»;
- «Получение учетных данных в открытом виде из Credential Manager, Chrome, Edge, Firefox»;
- «Выгрузить базу хэшей пользователей (NTDS.dit)»;
- «Получение списка пользователей домена»;
- «Проверка контроллера домена на уязвимость Zerologon (cve-2020-1472)».

× Добавить проверки

☒ Описание	Название
☒ Получение списка хостов подсети, дополнительной информации о хостах	btc-module-nxc-smb-net
☒ Получение учетных данных в открытом виде из Credential Manager, Chrome, Edge, Firefox.	btc-module-nxc-smb-u-p-dpapi
☒ Выгрузить базу хэшей пользователей (NTDS.dit)	btc-module-nxc-smb-u-p-ntds
☒ Получение списка пользователей домена	btc-module-nxc-smb-u-p-users
☒ Проверка контроллера домена на уязвимость Zerologon (cve-2020-1472)	btc-module-nxc-smb-zerologon-check

Всего: 5

Сохранить

Отменить

Рисунок 43 – Окно «Добавить проверки»

- 6) Нажать кнопку «Сохранить» для применения настроек. Если необходимо отменить выбор проверок, то нажать кнопку «Отменить».
- 7) В поле «Цели сканирования» нажать кнопку «Добавить» (рис. 44).

< Создать кампанию: Кампания-4fd43027 Черновик

 Основные настройки

✓ Настроен

 Разведка

Сканирование сети

✓ Настроен  1

Web сканирование

✓ Настроен  1

Сканирование инфраструктуры



Локальная разведка



 Получение доступа

Фишинг



Эксплуатация



Перебор УЗ



Перемещение в сети



 Постэксплуатация

Расширить поверхность атаки 



Выбрать проверки

5 проверок

Цели сканирования

Добавить

Завершить создание кампании

Рисунок 44 – Поле «Цели сканирования»

- 8) В открывшемся окне «Добавить цели сканирования» нажать кнопку «Цель сканирования» (рис. 45).

× Добавить цели сканирования

🔍 Введите запрос для поиска

☰ Фильтр

⬇ Загрузить цели

+ Цель сканирования



Список пуст

Сохранить

Отменить

Рисунок 45 – Окно «Цель сканирования»

- 9) Заполнить требуемые поля (рис. 46):
- выбрать тип ресурса из выпадающего списка (IP-адрес, подсеть, сервис, диапазон IP-адресов, пользователь + пароль, хост + пароль) (рис. 47);
 - ввести адрес цели, исходя из указанного выше типа ресурса;

- отключить переключатель «Исключения», который включен по умолчанию. Включение переключателя обозначает, что выбранный тип ресурса будет исключен из списка целей сканирования. Выключение обозначает, что будет добавлен как обычная цель для сканирования.

× Добавить цели сканирования

Тип ресурса

IP адрес

Адрес

192.0.0.1

Исключение

☐

Добавить

Отменить

🔍 Введите запрос для поиска

☰ Фильтр

⬇️ Загрузить цели

+ Цель сканирования



Список пуст

Сохранить

Отменить

Рисунок 46 – Ввод данных целей

× Добавить цели сканирования

Тип ресурса	IP адрес
Адрес	
Исключение	
Введите запрос для поиска	
+ Цель сканирования	

IP адрес

IP адрес

Подсеть

Сервис

Диапазон IP адресов

Пользователь + Пароль

Хост + Пароль

Рисунок 47 – Выбор типа ресурса

- 10) Нажать кнопку «Добавить». В список добавятся заданные цели сканирования или исключения (рис. 48).

× Добавить цели сканирования

Тип ресурса

Адрес

Исключение ☐

Фильтр

Загрузить цели

+ Цель сканирования

☐ Тип	Ресурс	Статус	Исключение
☐ IP адрес	192.12.12.20	Новый	
☐ IP адрес	192.12.12.12	Новый	

Всего: 2

Рисунок 48 – Список добавленных целей

- 11) Для загрузки перечня целей можно сразу загрузить готовый файл через опцию «Загрузить цели из файла» или сначала скачать шаблон в формате .txt через «Скачать шаблон», заполнить его и затем загрузить (рис. 49)

× Добавить цели сканирования

Тип ресурса

Сервис

Адрес

http

10.116.231.11

80

Введите корректный IPv4-адрес

Исключение



Добавить

Отменить

Введите запрос для поиска

Фильтр

Загрузить цели

+ Цель сканирования



Тип

Ресурс

Статус



URI

sub-domain.example.co.uk

Новый



Доменные имена

example.com

Новый

Загрузить цели из файла

Скачать шаблон

Всего: 2

Сохранить

Отменить

Рисунок 49 – Кнопка «Загрузить цели»

- 12) Для осуществления поиска необходимо перейти в поле «Введите запрос для поиска» для поиска записи в списке. Поиск выполняется по мере ввода символов. При нажатии кнопки «Фильтр» открывается окно для указания параметров фильтрации (рис. 50):

- тип ресурса – выпадающий список для выбора категории;
- IP-адрес – фильтр по конкретному IP-адресу устройства;
- подсеть – фильтр по диапазону IP-адресов (подсети);
- сервис – фильтр по сетевым сервисам;
- пользователь + пароль – фильтр по учётным данным (логин/пароль);
- хост + пароль – фильтр по связке «хост + учётные данные»;
- состояние – переключатели для отбора целей по статусу:
- кнопка «Все» – показывать все ресурсы (включая обычные и исключённые);
- кнопка «Только исключения» – показывать только те ресурсы, которые были помечены как исключения;
- кнопка «Без исключений» – показывать только ресурсы, которые находятся в обычном состоянии, не являясь исключениями;
- переключатель «Только новые» – отображения только недавно добавленных целей (например, после последнего сканирования);
- кнопка «Применить» – активирует выбранные фильтры;
- кнопка «Закрыть» – закрывает окно фильтрации без применения изменений.

× Добавить цели сканирования

Тип ресурса

Адрес

Исключение ☐

≡ Фильтр

⬇ Загрузить цели

+ Цель сканирования

☐	Тип	Ресурс
☐	IP адрес	192.12.12.20
☐	IP адрес	192.12.12.12

Тип ресурса

Состояние

Все

Только исключения

Без исключений

Только новые

☐

Применить

Закрыть

Всего: 2

Рисунок 50 – Кнопка «Фильтр»

13) Выбрать цели из списка. При выборе целей из списка отображаются скрытые кнопки (рис. 51) для работы с выбранными целями:

- кнопка «Удалить» – для удаления выбранных ресурсов;
- кнопка «Скачать» – для экспорта данных;
- кнопка «Исключить» – помечает ресурсы как исключенные из сканирования;

– кнопка «Отменить исключение» – снимает отметку об исключении.

× **Добавить цели сканирования**

Тип ресурса

IP адрес

Адрес

192.0.0.1

Исключение

☐

Добавить

Отменить

Выбрано: 2

Удалить

Скачать

Исключить

Отменить исключение

×

☒	Тип	Ресурс	Статус	Исключение
☒	IP адрес	192.12.12.20	Новый	
☒	IP адрес	192.12.12.12	Новый	

Всего: 2

Сохранить

Отменить

Рисунок 51 – Логика появления кнопок действий при выборе целей

Для исключения, удаления целей из списка возможно использование кнопок (рис. 52):

× Добавить цели сканирования

Выбрано: 2	Удалить	Скачать	Исключить	Отменить исключение	×
☒ Тип	Ресурс	Статус	Исключение		
☒ Доменные и...	htmlweb.ru				
☒ Подсеть	10.116.231.0/24				

Рисунок 52 – Кнопки «Добавить в исключения» и «Удалить»

- 14) В окне «Добавить цели сканирования» после выбора целей нажать кнопку «Сохранить» для применения параметров.
- 15) Активировать переключатель модуля «Сканирование инфраструктуры» (рис. 53).

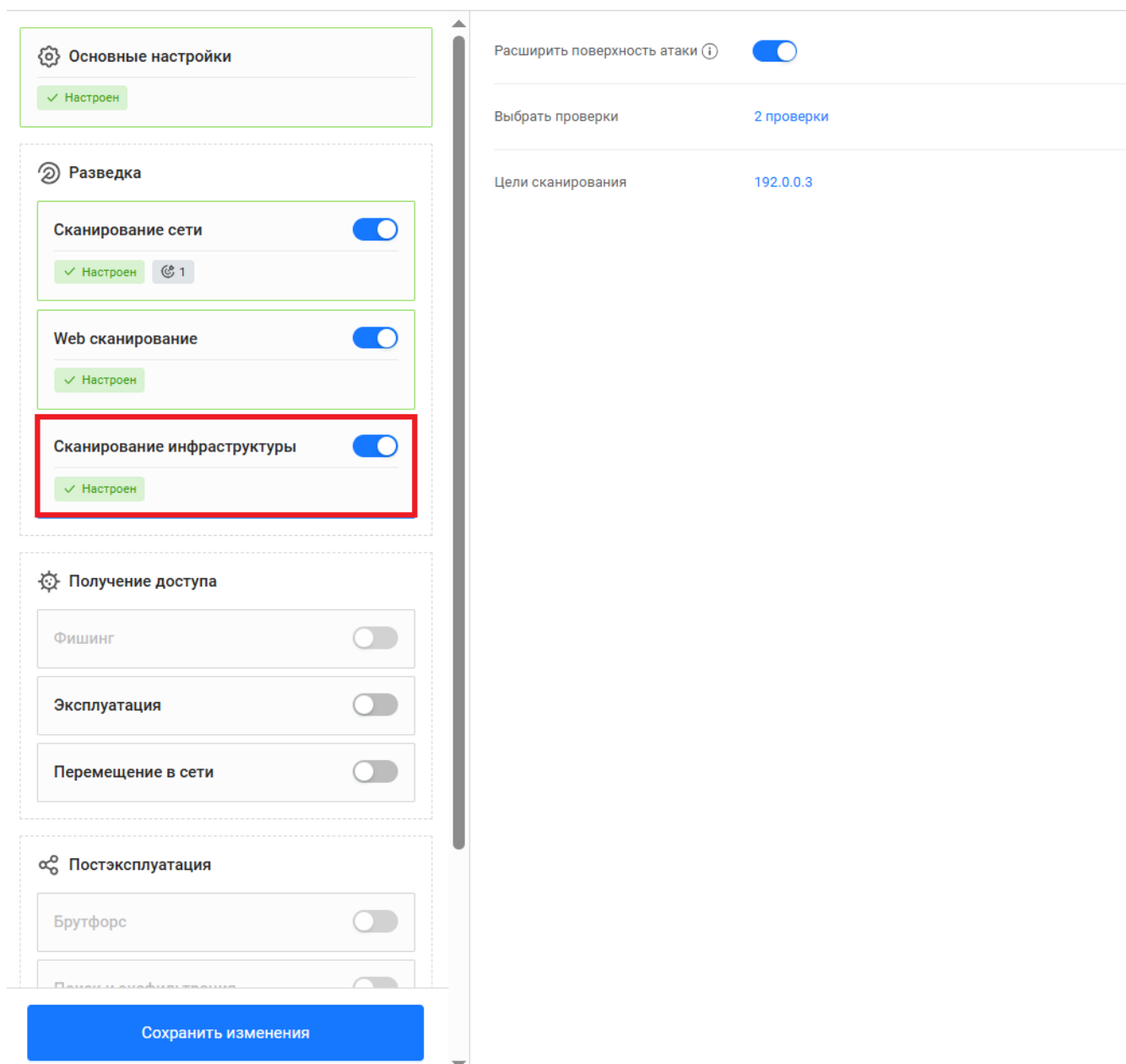


Рисунок 53 – Переключатель модуля «Сканирование инфраструктуры»

Примечание. Некоторые тонкие настройки могут не работать в тестовом режиме.

3.2.4 Локальная разведка

Функциональный компонент тонкого агента, выполняющий сканирование внутреннего состояния хоста.

Для добавления настроек локальной разведке необходимо:

- 1) В блоке «Разведка» перейти в подраздел «Локальная разведка».
- 2) Открыть подраздел «Локальная разведка» и перейти к заполнению требуемых настроек.

- 3) Переключатель в поле «Расширить поверхность атаки» оставить без изменения (по умолчанию активирован). Это значит, что новые цели, найденные в ходе кампании, будут использоваться модулем (рис. 54).

The screenshot displays the configuration interface of the SimuStrike software. On the left, there are four main sections of settings, each with a dashed border and a title icon:

- Основные настройки (Main Settings):** Contains a green status indicator 'Настроен' (Configured).
- Разведка (Reconnaissance):** Includes four toggle switches:
 - Сканирование сети (Network Scanning)
 - Web сканирование (Web Scanning)
 - Сканирование инфраструктуры (Infrastructure Scanning)
 - Локальная разведка (Local Reconnaissance) - This toggle is highlighted with a blue border.
- Получение доступа (Access):** Includes four toggle switches:
 - Фишинг (Phishing)
 - Эксплуатация (Exploitation)
 - Перебор УЗ (Brute Force)
 - Перемещение в сети (Network Movement)
- Постэксплуатация (Post-exploitation):** Includes three toggle switches:
 - Закрепление (Privilege Escalation)
 - Брутфорс хэшей (Hash Brute Force)
 - Эксфильтрация (Exfiltration)

On the right side, there is a sidebar with a vertical scrollbar. At the top of the sidebar, the option 'Расширить поверхность атаки' (Expand attack surface) is shown with an information icon and a blue toggle switch, which is highlighted by a red rectangular box. Below this, there are two sections: 'Выбрать проверки' (Select checks) with a 'Добавить' (Add) button, and 'Цели модуля' (Module targets) with a 'Добавить' (Add) button.

At the bottom of the main configuration area, there is a blue button labeled 'Завершить создание кампании' (Finish creating campaign).

Рисунок 54 – Переключатель «Расширить поверхность атаки»

- 4) В поле «Выбрать проверки» нажать кнопку «Добавить» (рис. 55).

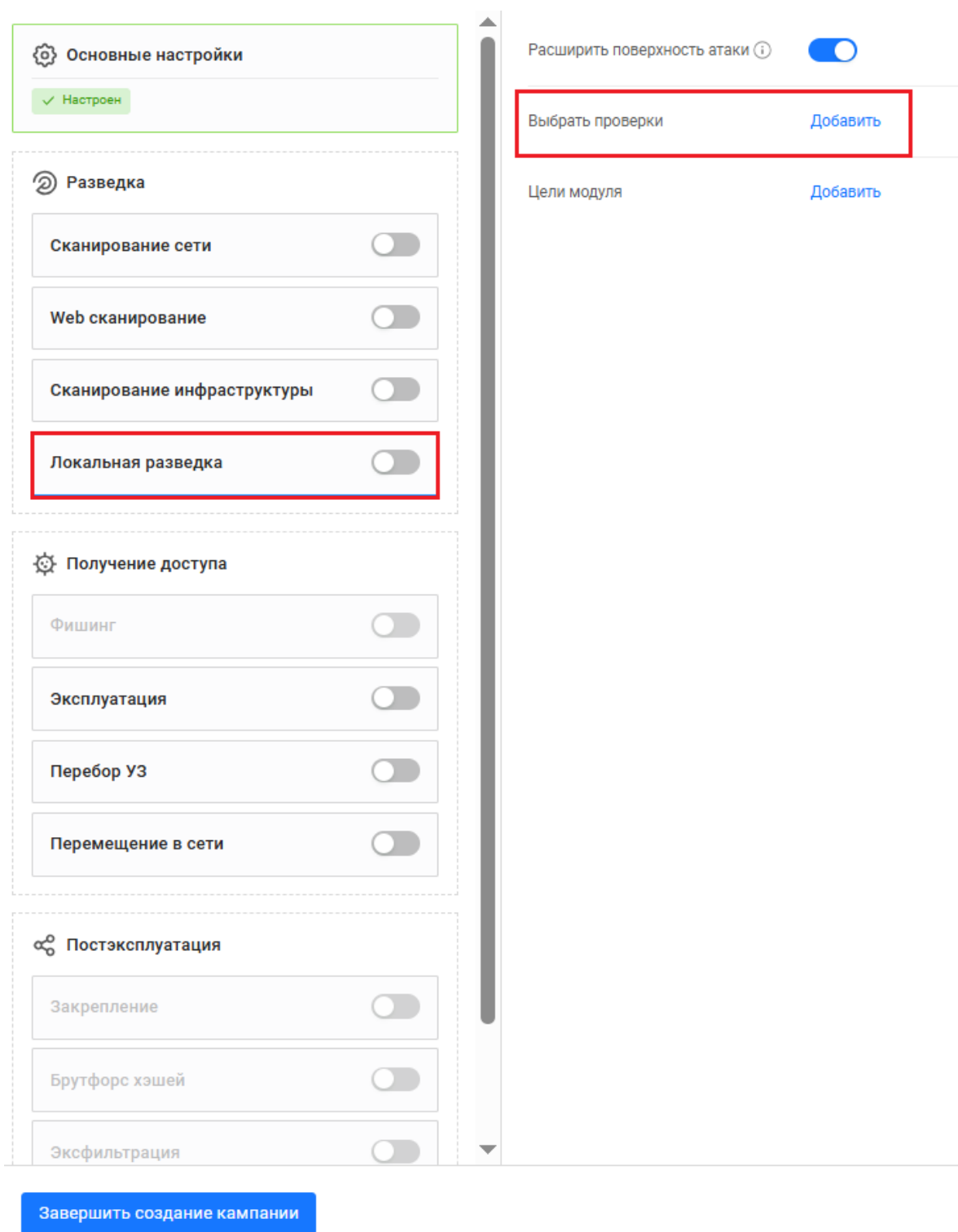


Рисунок 55 – Поле «Выбрать проверки»

- 5) В открывшемся окне «Добавить проверки» выбрать необходимые проверки из представленных в списке (рис. 56):
 - «Поиск чувствительных данных по ключам в "*.txt" файлах Linux»;
 - «Агрессивный поиск локальных файлов Linux»;
 - «Проверка прав на чтение в /etc/shadow»;
 - «Агрессивный поиск локальных файлов Windows».

× **Добавить проверки**

🔍 Введите запрос для поиска

✓ Описание	Название
✓ Поиск чувствительных данных по ключам в *.txt файлах Linux	btc-local-module-bash-cred-checker-demo
✓ Агрессивный поиск локальных файлов Linux	btc-local-module-bash-find-txt-yml-size
✓ Проверка прав на чтение в /etc/shadow	btc-local-module-bash-shadow-read-check
✓ Агрессивный поиск локальных файлов Windows	btc-local-module-posh-g-ch-p-txt-yml-size

Всего: 4

Сохранить

Рисунок 56 – Окно «Добавить проверки»

- 6) Нажать кнопку «Сохранить» для применения настроек. Если необходимо отменить выбор проверок, то нажать кнопку «Отменить».
- 7) В поле «Цели модуля» нажать кнопку «Добавить» (рис. 57).

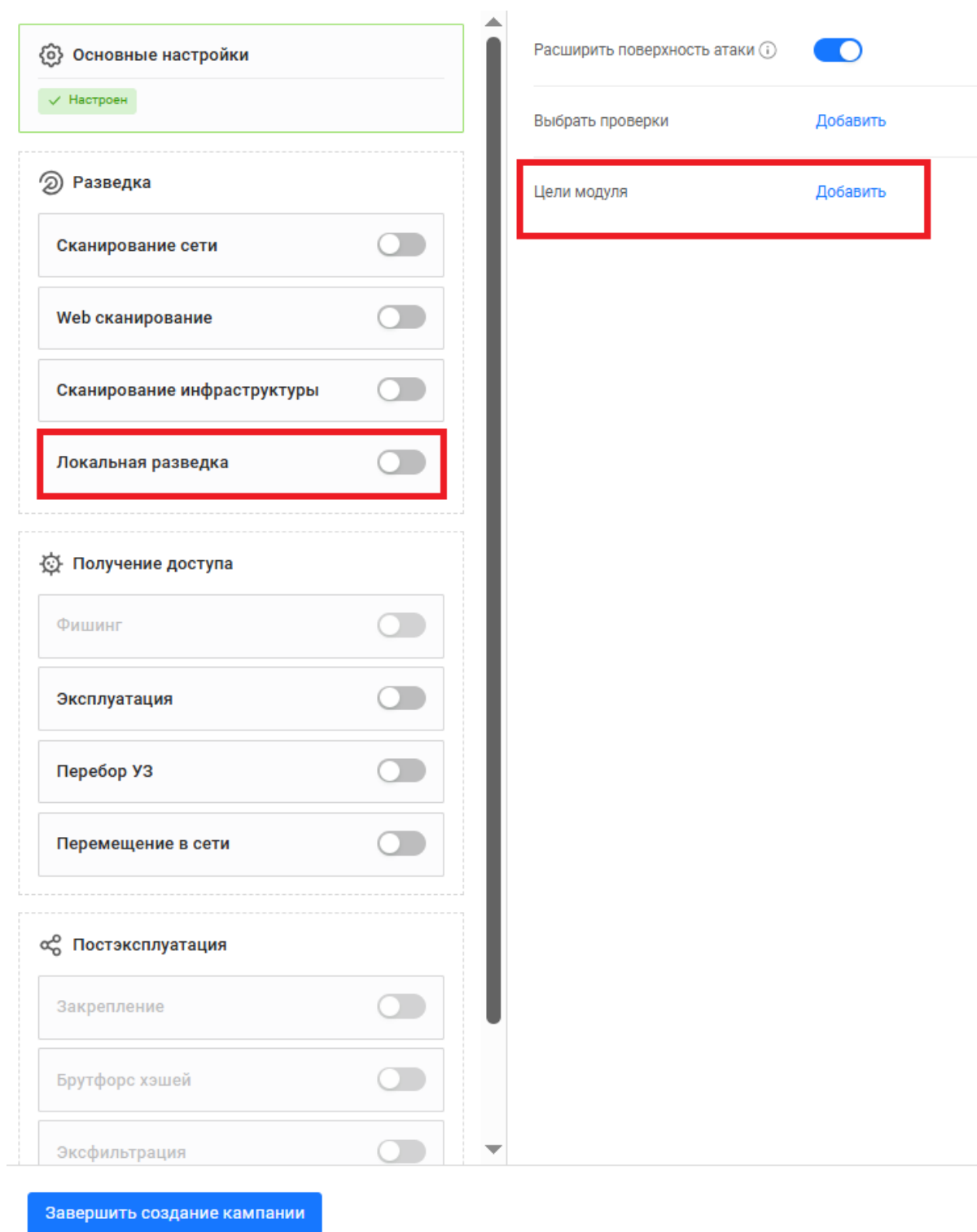


Рисунок 57 – Поле «Цели модуля»

- 8) В открывшемся окне «Добавить цели» нажать кнопку «Цель» (рис. 58).



Рисунок 58 – Окно «Цель сканирования»

- 9) Заполнить требуемые поля (рис. 59):
- выбрать тип ресурса из выпадающего списка (каталог, файл) (рис. 60); – ввести адрес цели, исходя из указанного выше типа ресурса;
 - отключить переключатель «Исключения», который включен по умолчанию. Включение переключателя обозначает, что выбранный тип ресурса будет исключен из списка целей сканирования. Выключение обозначает, что будет добавлен как обычная цель для сканирования.

The image shows the main form of the 'Добавить цели' (Add Goals) window. The form is enclosed in a red rectangular box. It contains the following elements: a dropdown menu for 'Тип ресурса' (Resource Type) with 'Каталог' (Catalog) selected; a text input field for 'Каталог' (Catalog) containing the path 'C:\Program files\data'; a toggle switch for 'Исключение' (Exclusion) which is currently turned off; two buttons, 'Добавить' (Add) and 'Отменить' (Cancel); and a search bar at the bottom with the placeholder 'Введите запрос для поиска'. Below the search bar are icons for 'Фильтр' (Filter), 'Загрузить цели' (Load Goals), and '+ Цель' (Add Goal). A dropdown menu is open below the search bar, showing two options: 'Загрузить цели из файла' (Load Goals from File) and 'Скачать шаблон' (Download Template).

Рисунок 59 – Ввод данных целей

× **Добавить цели**

Тип ресурса

Каталог

Исключение ☐

Введите запрос для поиска

Загрузить цели из файла
Скачать шаблон

Рисунок 60 – Выбор типа ресурса

- 10) Нажать кнопку «Добавить». В список добавятся заданные цели сканирования или исключения (рис. 61).

× **Добавить цели**

Тип ресурса

Каталог

Исключение ☐

Введите запрос для поиска

☐	Тип	Ресурс	Статус	Исключение
☐	Каталог	C:\Users\test	Новый	
☐	Каталог	C:\Users\	Новый	

Рисунок 61 – Список добавленных целей

- 11) Для загрузки перечня целей можно сразу загрузить готовый файл через опцию «Загрузить цели из файла» или сначала скачать шаблон в формате .txt через «Скачать шаблон», заполнить его и затем загрузить.
- 12) Для осуществления поиска необходимо перейти в поле «Введите запрос для поиска» для поиска записи в списке. Поиск выполняется по мере ввода символов. При нажатии кнопки «Фильтр» открывается окно для указания параметров фильтрации (рис. 62):
 - тип ресурса – выпадающий список для выбора категории:
 - каталог – фильтр для выбора папок и каталогов файловой системы;
 - файл – фильтр для выбора отдельных файлов;;
 - состояние – переключатели для отбора целей по статусу:
 - кнопка «Все» – показывать все ресурсы (включая обычные и исключённые);
 - кнопка «Только исключения» – показывать только те ресурсы, которые были помечены как исключения;
 - кнопка «Без исключений» – показывать только ресурсы, которые находятся в обычном состоянии, не являясь исключениями;
 - переключатель «Только новые» – отображения только недавно добавленных целей (например, после последнего сканирования);
 - кнопка «Применить» – активирует выбранные фильтры;
 - кнопка «Закрыть» – закрывает окно фильтрации без применения изменений.

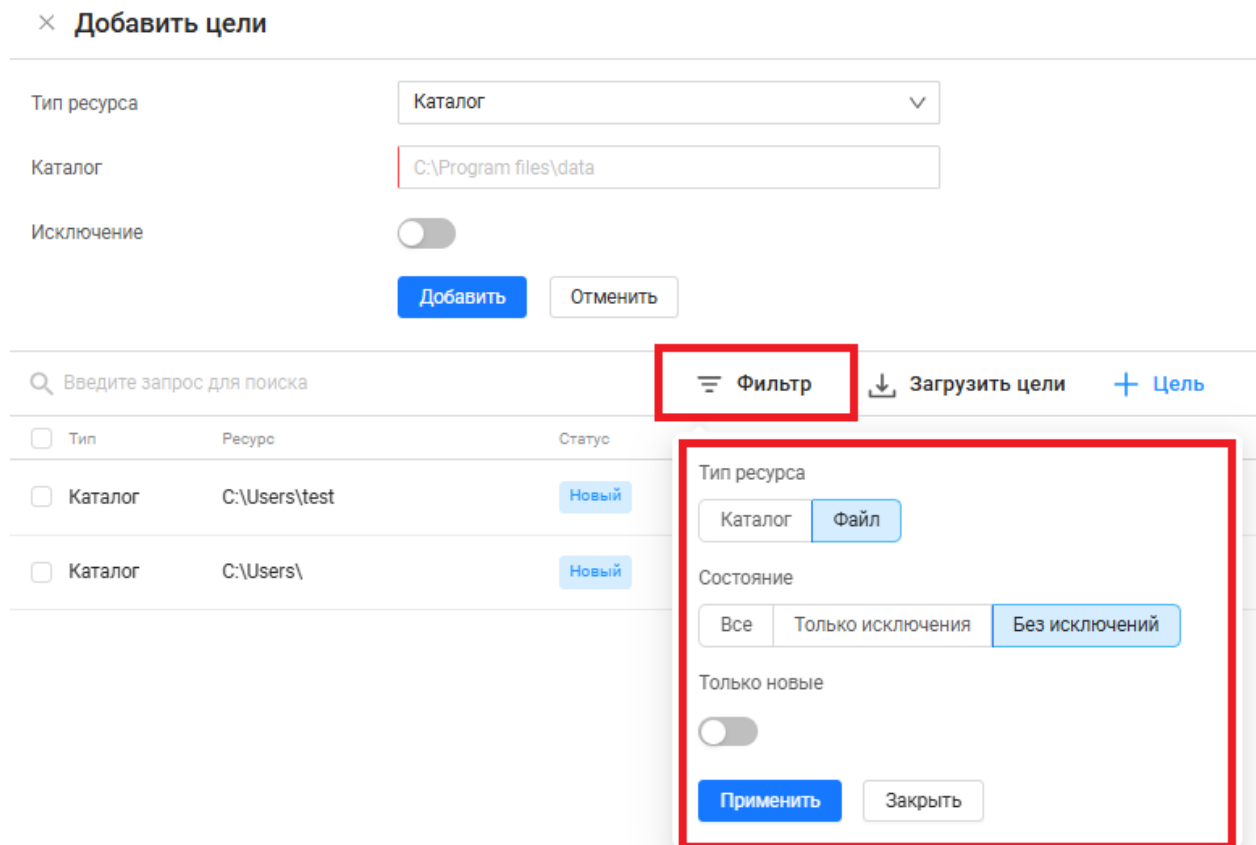


Рисунок 62 – Кнопка «Фильтр»

- 13) Выбрать цели из списка. При выборе целей из списка отображаются скрытые кнопки (рис. 63) для работы с выбранными целями:
- кнопка «Удалить» – для удаления выбранных ресурсов;
 - кнопка «Скачать» – для экспорта данных;
 - кнопка «Исключить» – помечает ресурсы как исключенные из сканирования;
 - кнопка «Отменить исключение» – снимает отметку об исключении.

× **Добавить цели**

Тип ресурса

Каталог

Исключение ☐

Выбрано: 2 |

☒	Тип	Ресурс	Статус	Исключение
☒	Каталог	C:\Users\test	Новый	Исключить Удалить
☒	Каталог	C:\Users\	Новый	

Рисунок 63 – Логика появления кнопок действий при выборе целей

Для исключения, удаления целей из списка возможно использование кнопок (рис. 64):

× **Добавить цели**

Тип ресурса

Каталог

Исключение ☐

Выбрано: 2 | ×

☒	Тип	Ресурс	Статус	Исключение
☒	Каталог	C:\Users\test	Новый	
☒	Каталог	C:\Users\	Новый	Исключить Удалить

Рисунок 64 – Кнопки «Добавить в исключения» и «Удалить»

- 14) В окне «Добавить цели» после выбора целей нажать кнопку «Сохранить» для применения параметров.
- 15) Активировать переключатель модуля «Локальная разведка» (рис. 65).

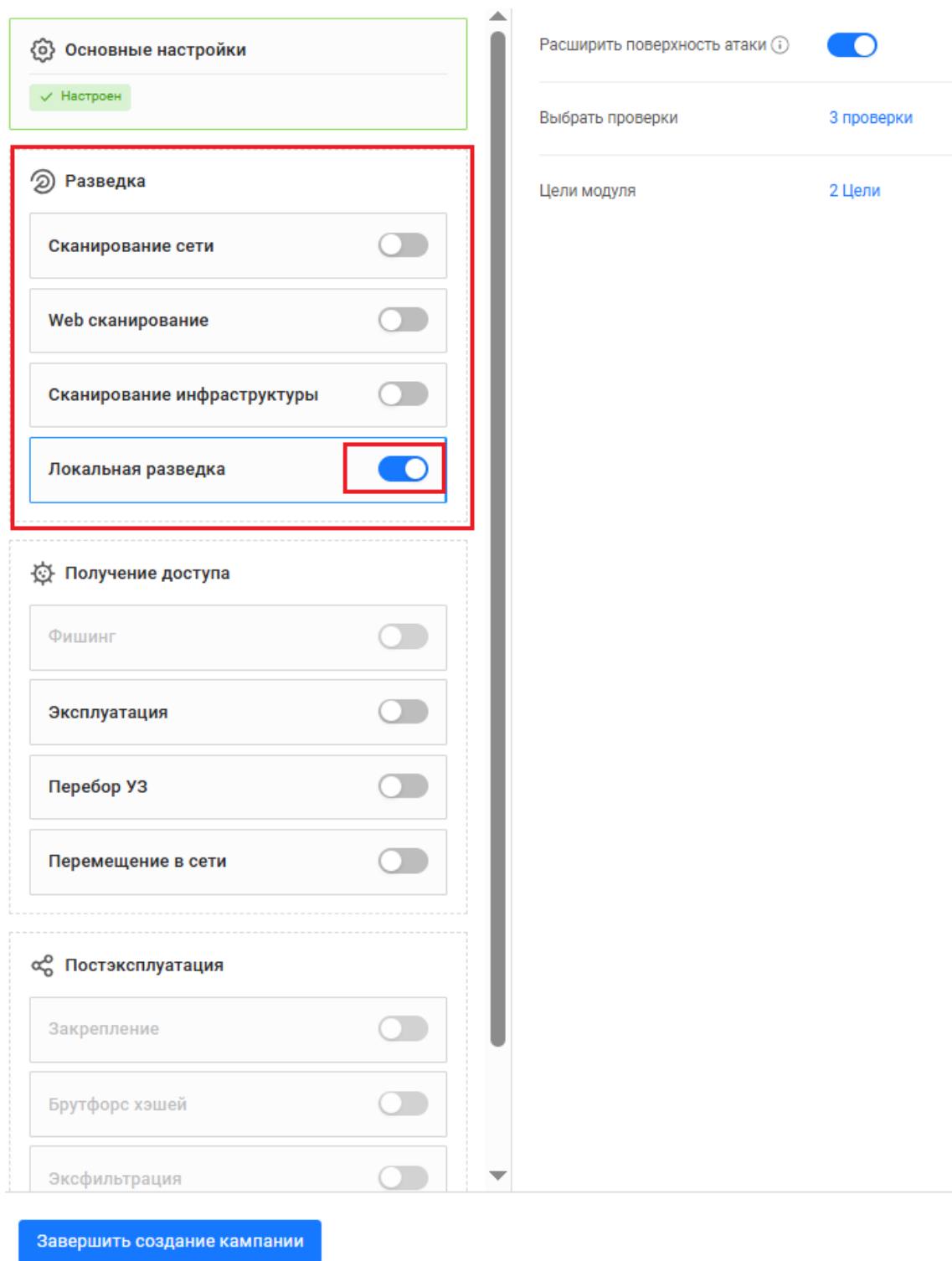


Рисунок 65 – Переключатель модуля «Локальная разведка»

Примечание. Некоторые тонкие настройки могут не работать в тестовом режиме.

3.3 Эксплуатация

Эксплуатация — это процесс запуска скрипта, который использует уязвимость программного обеспечения (ПО) без внедрения вредоносной полезной нагрузки. Такой

подход позволяет исследовать уязвимость без нанесения вреда системе. Модуль эксплуатации служит для подтверждения наличия уязвимости, что является важным шагом в процессе тестирования безопасности. После этого модули перемещения в сети и закрепления могут использовать уязвимости, подтвержденные модулем эксплуатации, для дальнейшего продвижения в системе и обеспечения устойчивого доступа к ней.

К настройке эксплуатации необходимо переходить после настройки модулей «Разведка» и «Фишинг». Для этого необходимо:

- 1) Перейти в блок «Получение доступа» в окне «Создать кампанию».
- 2) Открыть подраздел «Эксплуатация» и перейти к заполнению настроек (рис. 66).

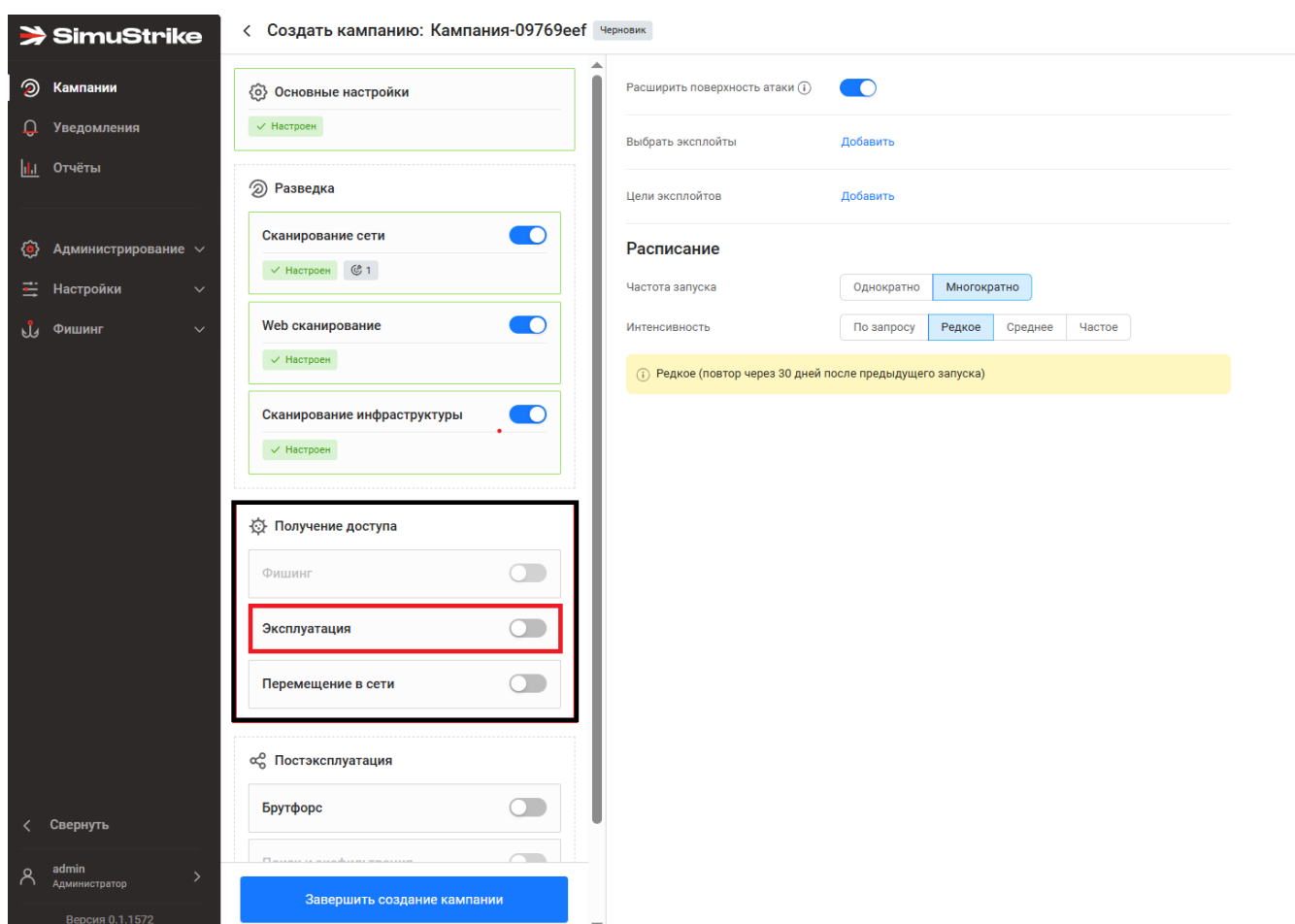


Рисунок 66 – Подраздел «Эксплуатация»

- 3) Переключатель в поле «Расширить поверхность атаки» оставить без изменения (по умолчанию активирован). Это значит, что новые цели найденные в ходе кампании будут использоваться модулем (рис. 67).

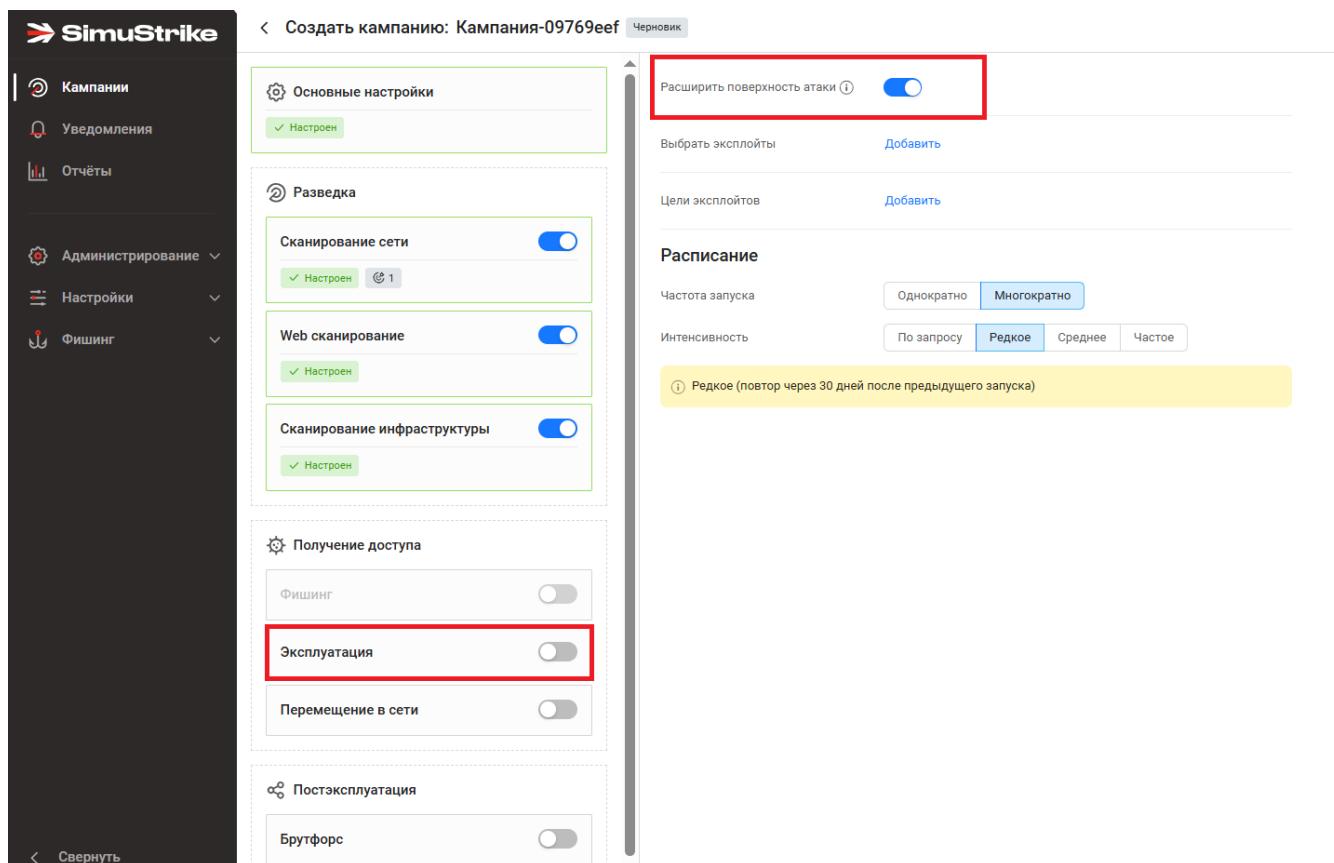


Рисунок 67 – Переключатель «Расширить поверхность атаки»

- 4) Выбрать эксплойты, для этого в поле нажать кнопку «Добавить» (рис. 68).

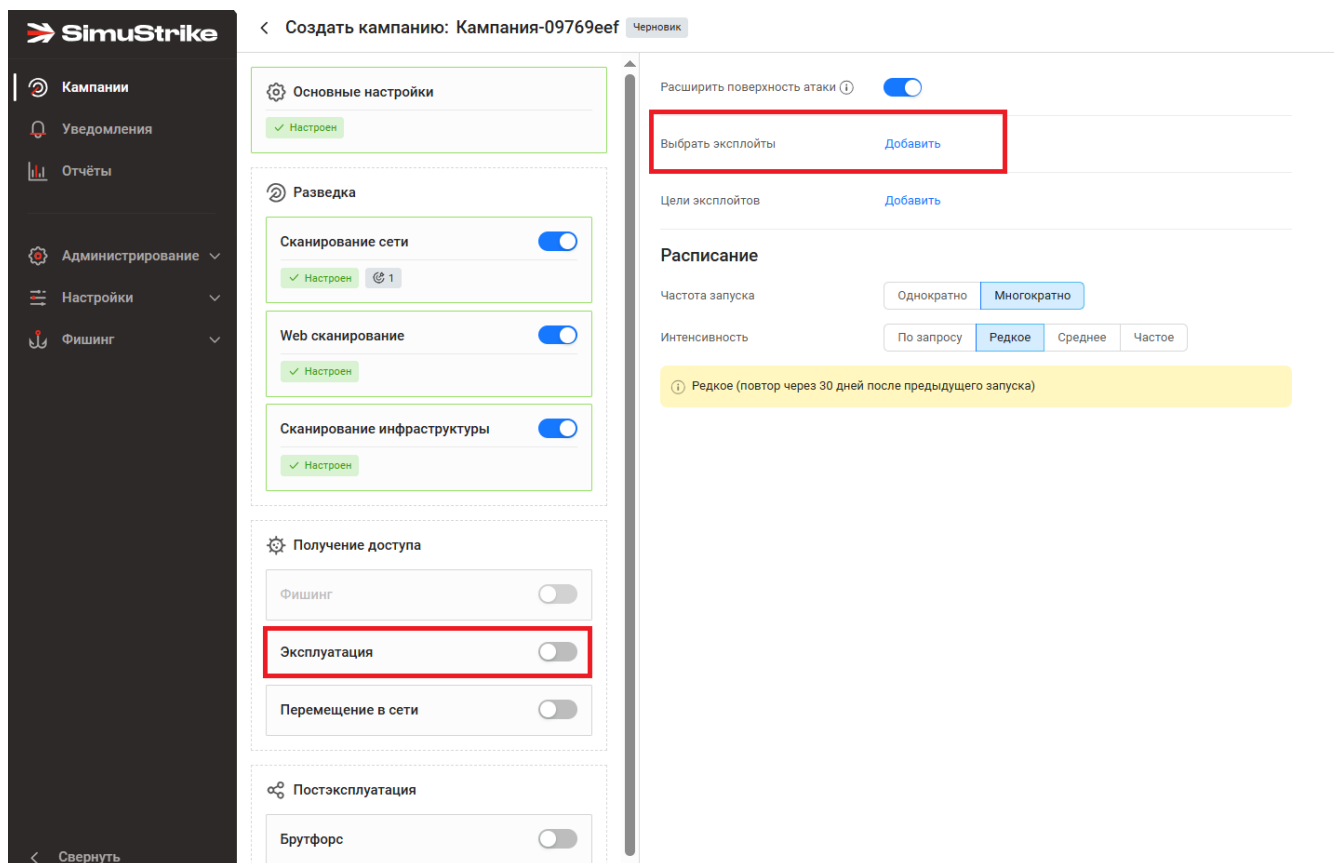


Рисунок 68 – Кнопка добавления эксплойтов

- 5) В открывшемся окне «Добавление эксплойтов» выбрать необходимые проверки из представленных в списке и нажать кнопку «Сохранить» (рис. 69).

× Добавление эксплойтов

🔍 Введите запрос для поиска

☰ Фильтр

☐	CVE	ОС	Класс ПО	CVSSv3	Наименование ПО	Тип атаки
☒	CVE-2024-28116	linux	Server Software	8.8 HIGH	Grav CMS	SSTI (RCE)
☒	CVE-2024-9264	linux	Server Software	9.9 CRITICAL	Grafana	Directory RCE
☒	CVE-2019-7609	linux	Server Software	9.8 CRITICAL	Kibana	RCE
☒	CVE-2015-3337	linux	Server Software	4.3 MEDIUM	ElasticSearch	Path Traversal
☒	CVE-2015-3306	linux	Server Software	10.0 CRITICAL	ProFTPD	RCE
☒	CVE-2020-1938	linux	Server Software	9.8 CRITICAL	Apache Tomcat	
☒	CVE-2014-3120	linux	Server Software	8.1 HIGH	ElasticSearch	RCE
☒	CVE-2025-3248	linux	Server Software	9.8 CRITICAL	Langflow	RCE
☒	CVE-2024-42327	linux	Server Software	9.9 CRITICAL	Zabbix Server	SQLi
☒	CVE-2021-43798	linux	Server Software	7.5 HIGH	Grafana	Directory RCE
☒	CVE-2019-20933	linux	Server Software	9.8 CRITICAL	InfluxDB	Broken Authentication
☒	CVE-2021-42013	linux	Server Software	9.8 CRITICAL	Apache HTTP Server	Path Traversal
☒	CVE-2019-9193	linux	Server Software	7.2 HIGH	Postgres	RCE
☒	CVE-2015-1427	linux	Server Software	9.8 CRITICAL	ElasticSearch	RCE
☒	CVE-2021-44521	linux	Server Software	9.1 CRITICAL	Apache Cassandra	RCE

Всего: 21

Сохранить

Отменить

Рисунок 69 – Окно «Добавление эксплойтов»

- 6) Доступна возможность указать цели эксплойтов. Для этого в поле «Цели эксплойтов» нажать кнопку «Добавить» (рис. 70).

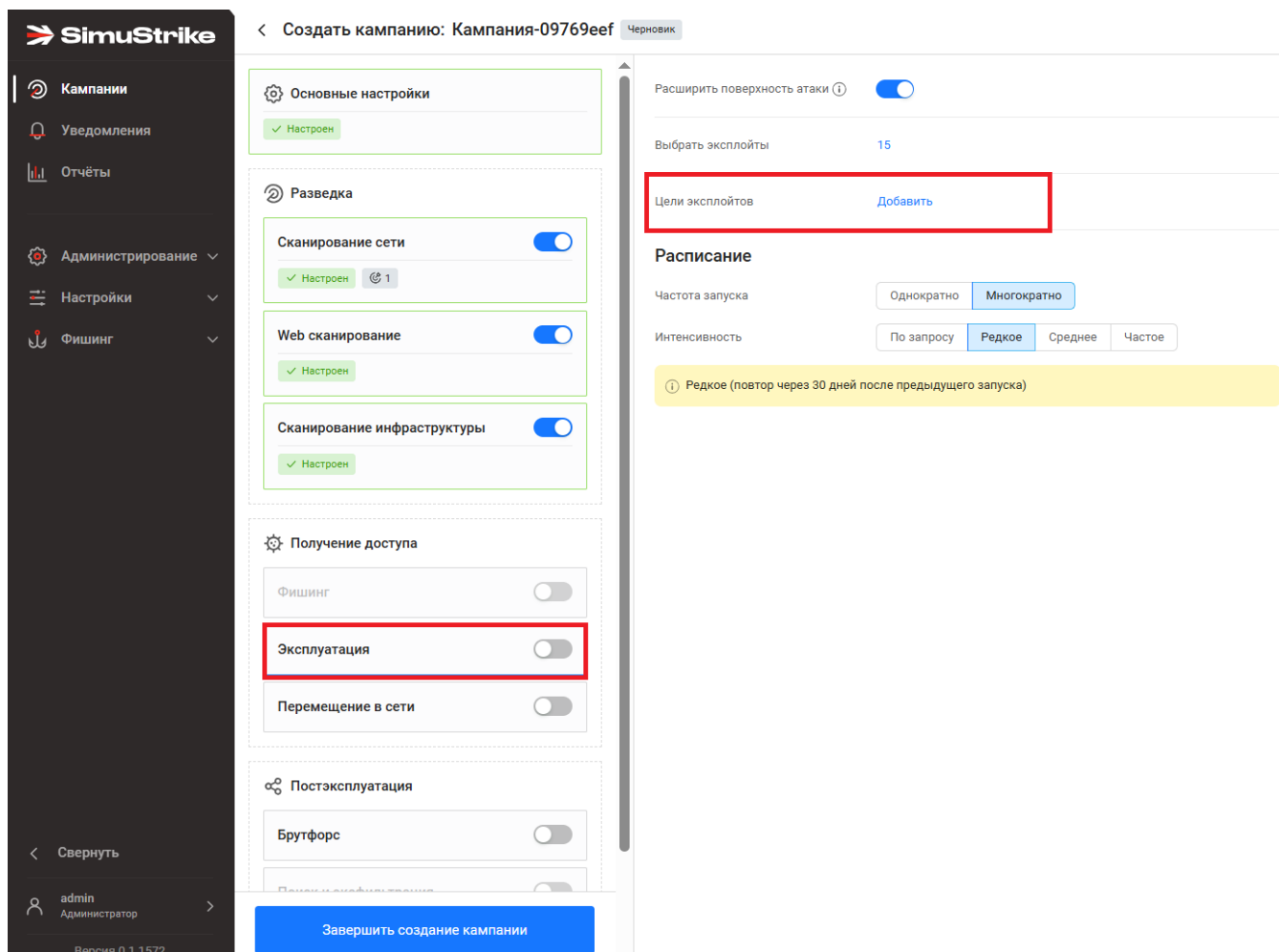


Рисунок 70 – Кнопка «Добавить»

- 7) В открывшемся окне «Добавить цели эксплойтов» (рис. 71), нажать кнопку «Цель эксплойта».

× **Добавить цели эксплойтов** Введите запрос для поиска Фильтр Загрузить цели эксплойтов **Цель эксплойта**

Список пуст

Сохранить

Отменить

Рисунок 71 – Окно «Добавить цели эксплойтов»

- 8) Заполнить требуемые поля в окне «Добавить цели эксплойтов» (рис. 72):
- выбрать тип ресурса из выпадающего списка;
 - сервис – указать протокол, IP-адрес, хост;
 - пользователь;
 - пароль;

- пользователь + пароль – учётные данные для доступа к ресурсу.
- ввести адрес цели, исходя из типа ресурса;
- переключатель «Исключения», отключён по умолчанию. Активация переключателя:
- если переключатель включен (отмечен), выбранный тип ресурса будет исключен из списка целей сканирования;
- если выключен (не отмечен), то будет добавлен как обычная цель для сканирования.

× Добавить цели эксплойтов

Тип ресурса	Сервис ▾		
Адрес	http ▾	10.116.231.11	: 80
Исключение	☐		
Добавить Отменить			

🔍 Введите запрос для поиска

☰ Фильтр

⬇ Загрузить цели эксплойтов

+ Цель эксплойта

Рисунок 72 – Ввод данных целей

- 9) Нажать кнопку «Добавить». В список добавятся заданные цели эксплойтов или исключения (рис. 73).

× Добавить цели эксплойтов

Тип ресурса

Пользователь

Исключение ☐

🔍 Введите запрос для поиска

☰ Фильтр

⬇️ Загрузить цели эксплойтов

+ Цель эксплойта

☐	Тип	Ресурс	Статус	Исключение
--------------------------	-----	--------	--------	------------

☐	Пароль	qwerty	Новый	
--------------------------	--------	--------	-------	--

☐	Пароль	йцукен	Новый	
--------------------------	--------	--------	-------	--

Рисунок 73 – Список добавленных целей

- 10) Для загрузки перечня целей можно сразу загрузить готовый файл через опцию «Загрузить цели из файла» или сначала скачать шаблон в формате .txt через «Скачать шаблон», заполнить его и затем загрузить (рис. 74).

× Добавить цели эксплойтов

Тип ресурса

Пользователь

Исключение ☐

🔍 Введите запрос для поиска

☰ Фильтр

⬇️ Загрузить цели эксплойтов

+ Цель эксплойта

☐	Тип	Ресурс	Статус	Исключение
--------------------------	-----	--------	--------	------------

☐	Пароль	qwerty	Новый	
--------------------------	--------	--------	-------	--

☐	Пароль	йцукен	Новый	
--------------------------	--------	--------	-------	--

Загрузить цели эксплойтов из файла

Скачать шаблон

Рисунок 74 – Кнопка «Загрузить цели»

- 11) Выбрать цели из списка. При выборе целей из списка отображаются скрытые кнопки (рис. 75) для работы с выбранными целями:
- кнопка «Удалить» – для удаления выбранных ресурсов;
 - кнопка «Скачать» – для экспорта данных;
 - кнопка «Исключить» – помечает ресурсы как исключенные из эксплойтов;
 - кнопка «Отменить исключение» – снимает отметку об исключении.

× Добавить цели эксплойтов

Тип ресурса

Пользователь
Обязательное поле

Исключение ☐

Выбрано: 3	Удалить	Скачать	Исключить	Отменить исключение	×
☒	Тип	Ресурс	Статус	Исключение	
☒	Пользователь	test@mail.ru	Новый		
☒	Пароль	qwerty	Новый		
☒	Пароль	йцукен	Новый		

Рисунок 75 – Логика появления кнопок действий при выборе целей

Для исключения, удаления целей из списка возможно использование кнопок (рис. 76):

- добавить в исключения;
- удалить из списка.

× Добавить цели эксплойтов

Тип ресурса	Пароль
Пользователь	qwerty Обязательное поле
Исключение	☐
Добавить Отменить	

Выбрано: 3	Удалить	Скачать	Исключить	Отменить исключение	×
☒ Тип	Ресурс	Статус	Исключение		
☒ Пользователь	test@mail.ru	Новый			
☒ Пароль	qwerty	Новый			
☒ Пароль	йцукен	Новый			

Рисунок 76 – Кнопки «Добавить в исключения» и «Удалить»

- В окне «Добавить цели эксплойтов» после выбора целей нажать кнопку «Сохранить» для применения параметров.
- Активировать переключатель модуля «Эксплуатация» (рис. 77).

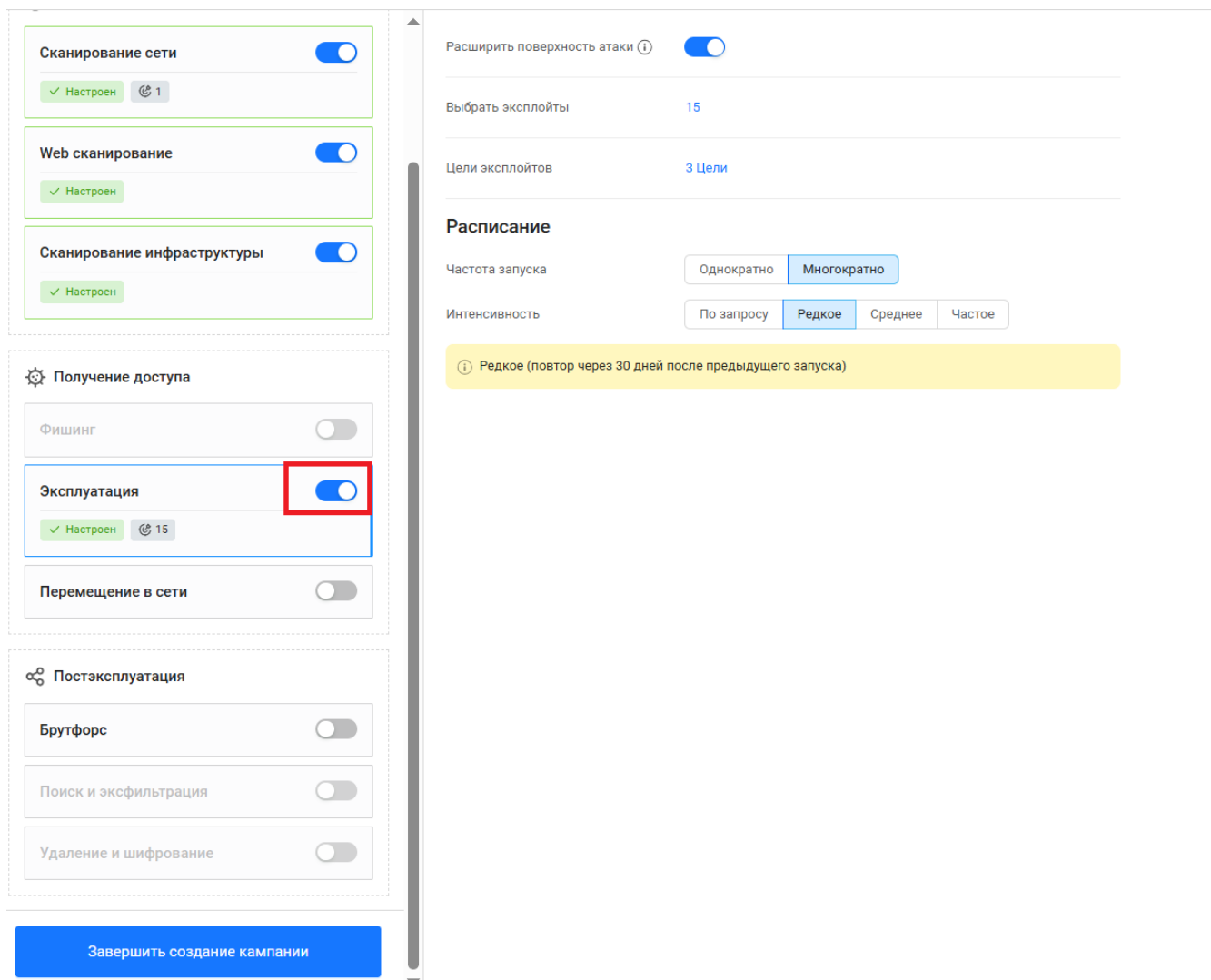


Рисунок 77 – Переключатель модуля «Эксплуатация»

Примечание. Некоторые тонкие настройки могут не работать в тестовом режиме.

3.3.1 Фишинг

Примечание. Настройка модуля «Фишинг» в рамках кампании будет доступна в версии 2.0. В данный момент модуль «Фишинг» настраивается в отдельном разделе главного меню.

3.4 Перемещение в сети

Перемещение в сети — это процесс поиска уязвимостей внутри инфраструктуры с использованием ранее заражённого хоста для дальнейшего перемещения и установки агента на другие хосты в той же сети. Этот модуль позволяет оценить максимальный ущерб, который могут причинить злоумышленники, находясь внутри инфраструктуры, и помогает проанализировать уязвимость системы в случае успешной атаки.

Для указания настроек перемещения в сети необходимо:

- 1) Перейти в блок «Получение доступа» в окне «Создать кампанию».
- 2) Открыть подраздел «Перемещение в сети» и перейти к заполнению требуемых настроек.
- 3) Переключатель в поле «Расширить поверхность атаки» оставить без изменения (по умолчанию активирован). Это значит, что новые цели найденные в ходе кампании будут использоваться модулем (рис. 78).

< Создать кампанию: Кампания-28a3ff0e Черновик

Сканирование инфраструктуры ☐

Локальная разведка ☐

⚙️ Получение доступа

Фишинг ☐

Эксплуатация ☐

Перебор УЗ ☐

Перемещение в сети ☐

🔗 Постэксплуатация

Закрепление ☐

Повышение привилегий ☐

Брутфорс хэшей ☐

Экспильтрация ☐

Удаление и шифрование ☐

Завершить создание кампании

Расширить поверхность атаки ⓘ ☒

Выбрать проверки [Добавить](#)

Цели модуля [Добавить](#)

Рисунок 78 – Переключатель «Расширить поверхность атаки»

- 4) В поле «Выбрать проверки» нажать кнопку «Добавить» (рис. 79).

< Создать кампанию: Кампания-28a3ff0e Черновик

Сканирование инфраструктуры	☐	Расширить поверхность атаки ⓘ	☒
Локальная разведка	☐	Выбрать проверки	Добавить
Получение доступа		Цели модуля	Добавить
Фишинг	☐		
Эксплуатация	☐		
Перебор УЗ	☐		
Перемещение в сети	☐		
Постэксплуатация			
Закрепление	☐		
Повышение привилегий	☐		
Брутфорс хэшей	☐		
Эксfiltrация	☐		
Удаление и шифрование	☐		

Завершить создание кампании

Рисунок 79 – Поле «Выбрать проверки»

- 5) В открывшемся окне «Добавить проверки» выбрать необходимые проверки из представленных в списке (рис. 80):
- «Поиск валидных учетных данных, методом перебора множества паролей и пользователей, по протоколу SSH»;

- «NXC (тихий режим) получение валидных имён пользователей FTP, и паролей в открытом виде»;
- «AS-Rep Roasting. Получение Kerberos AS-REP хэшей пользователей AD, с атрибутом DONT_REQ_PREAUTH»;
- «Получение валидных имён пользователей, и паролей в открытом виде»;
- «Установка агента Windows, загрузка с сервера метом PULL»;
- «NXC (тихий режим) получение валидных имён пользователей SSH, и паролей в открытом виде».

× Добавить проверки

🔍 Введите запрос для поиска

☐	Описание	Название
☐	Поиск валидных учетных данных, методом перебора множества паролей и пользователей, по протоколу SSH	btc-module-hydra-u...
☐	NXC (тихий режим) получение валидных имён пользователей FTP, и паролей в открытом виде	btc-module-nxc-ftp-...
☐	AS-Rep Roasting. Получение Kerberos AS-REP хэшей пользователей AD, с атрибутом DONT_REQ_PREAUTH	btc-module-nxc-lda...
☐	Получение валидных имён пользователей, и паролей в открытом виде	btc-module-nxc-sm...
☐	Установка агента Windows, загрузка с сервера метом PULL	btc-module-nxc-sm...
☐	NXC (тихий режим) получение валидных имён пользователей SSH, и паролей в открытом виде	btc-module-nxc-ssh...

Всего: 6

Сохранить

Отменить

Рисунок 80 – Окно «Добавить проверки»

- 6) Нажать кнопку «Сохранить» для применения настроек. Если необходимо отменить выбор проверок, то нажать кнопку «Отменить».
- 7) В поле «Цели модуля» нажать кнопку «Добавить» (рис. 81).

< Создать кампанию: Кампания-28a3ff0e Черновик

Разведка

Сканирование сети ☐

Web сканирование ☐

Сканирование инфраструктуры ☐

Локальная разведка ☐

Получение доступа

Фишинг ☐

Эксплуатация ☐

Перебор УЗ ☐

Перемещение в сети ☐

Постэксплуатация

Закрепление ☐

Повышение привилегий ☐

Расширить поверхность атаки ⓘ ☒

Выбрать проверки [Добавить](#)

Цели модуля [Добавить](#)

Завершить создание кампании

Рисунок 81 – Поле «Цели модуля»

- 8) В открывшемся окне «Добавить цели» нажать кнопку «Цель» (рис. 82).

× Добавить цели

Тип ресурса: Сервис

Адрес: http 10.116.231.11 : 80

Исключение: ☐

Добавить Отменить

Рисунок 82 – Окно «Цель сканирования»

9) Заполнить требуемые поля (рис. 83):

- выбрать тип ресурса из выпадающего списка (рис. 84):
- сервис – указать протокол, IP-адрес, хост;
- пользователь;
- пароль;
- пользователь + пароль – учётные данные для доступа к ресурсу.
- ввести адрес цели, исходя из типа ресурса;
- переключатель «Исключения», отключён по умолчанию. Активация переключателя:
- если переключатель включен (отмечен), выбранный тип ресурса будет исключен из списка целей сканирования;
- если выключен (не отмечен), то будет добавлен как обычная цель для сканирования.

× Добавить цели

Тип ресурса: Сервис

Адрес: http 10.116.231.11 : 80

Исключение: ☐

Добавить Отменить

Рисунок 83 – Ввод данных целей

× Добавить цели

Тип ресурса	Сервис Сервис Пользователь Пароль Пользователь + Пароль
Адрес	
Исключение	

🔍 Введите запрос для поиска

⌵ Фильтр

⬇️ Загрузить цели

+ Цель

Рисунок 84 – Выбор типа ресурса

- 10) Нажать кнопку «Добавить». В список добавятся заданные цели или исключения (рис. 85).

× Добавить цели

Тип ресурса	Сервис		
Адрес	http	10.116.231.11	: 80
Исключение			
Добавить		Отменить	

🔍 Введите запрос для поиска

☰ Фильтр

⬇️ Загрузить цели

+ Цель

☐ Тип	Ресурс	Статус	Исключение
☐ Пароль	qwqeqwew	Новый	
☐ Пароль	йцукен	Новый	

Рисунок 85 – Список добавленных целей

- 11) Для загрузки перечня целей можно сразу загрузить готовый файл через опцию «Загрузить цели из файла» или сначала скачать шаблон в формате .txt через «Скачать шаблон», заполнить его и затем загрузить (рис. 86).

× **Добавить цели**

Тип ресурса

Сервис

Адрес

http

10.116.231.11

80

Исключение

☐

Добавить

Отменить

Введите запрос для поиска

Фильтр

Загрузить цели

+ Цель

☐ Тип	Ресурс	Статус	Исключение
☐ Пароль	qwqeqwew	Новый	
☐ Пароль	йцукен	Новый	

Загрузить цели из файла

Скачать шаблон

Рисунок 86 – Кнопка «Загрузить цели»

- 12) В интерфейсе окна доступна возможность применить поиск при вводе в поле «Введите запрос для поиска», а также фильтры при нажатии кнопки «Фильтр» и последующем открытии окна фильтров с параметрами (рис. 87):
- тип ресурса – выпадающий список для выбора категории;
 - сервис – фильтр по сетевым сервисам;
 - пользователь;
 - пароль;
 - пользователь + пароль – фильтр по учётным данным (логин/пароль);
 - состояние – переключатели для отбора целей по статусу:
 - кнопка «Все» – показывать все ресурсы (включая обычные и исключённые);
 - кнопка «Только исключения» – показать только те ресурсы, которые были помечены как исключения;
 - кнопка «Без исключений» – показать только ресурсы, которые находятся в обычном состоянии, не являясь исключениями;
 - переключатель «Только новые» – отображения только недавно добавленных целей (например, после последнего сканирования);
 - кнопка «Применить» – активирует выбранные фильтры;
 - кнопка «Закрыть» – закрывает окно фильтрации без применения изменений.

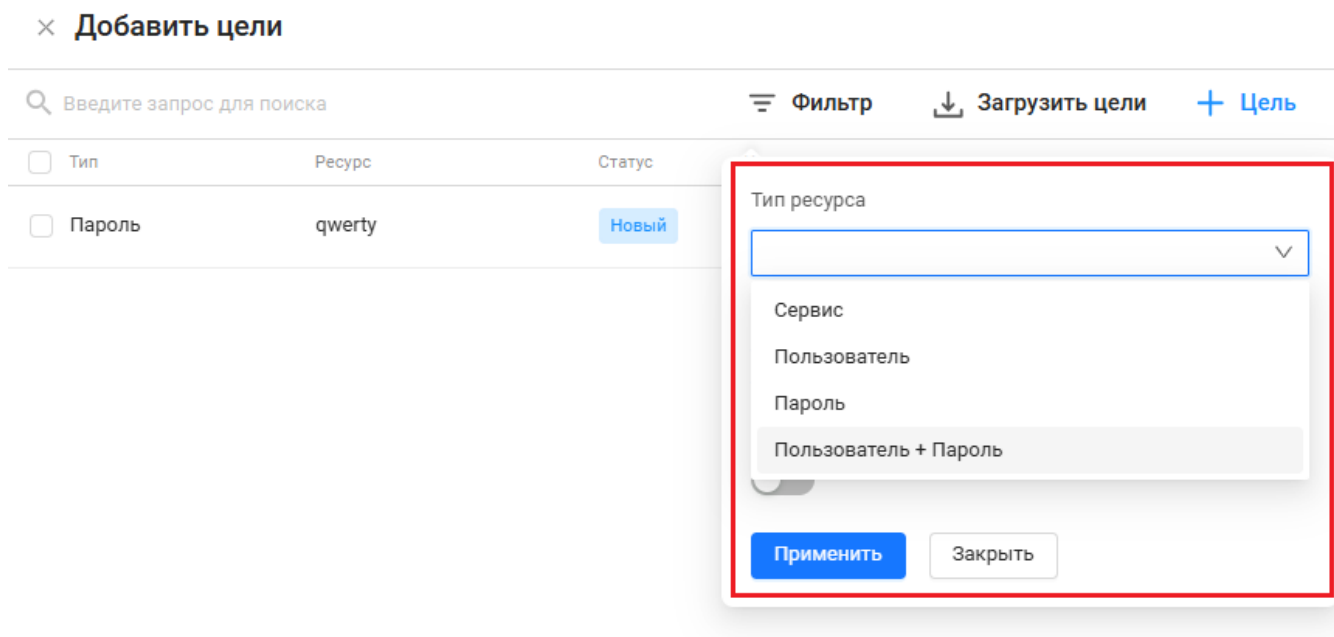


Рисунок 87 – Кнопка «Фильтр»

13) Выбрать цели из списка. При выборе целей из списка отображаются скрытые кнопки (рис. 88) для работы с выбранными целями:

- кнопка «Удалить» – для удаления выбранных ресурсов;
- кнопка «Скачать» – для экспорта данных;
- кнопка «Исключить» – помечает ресурсы как исключенные из сканирования;
- кнопка «Отменить исключение» – снимает отметку об исключении.

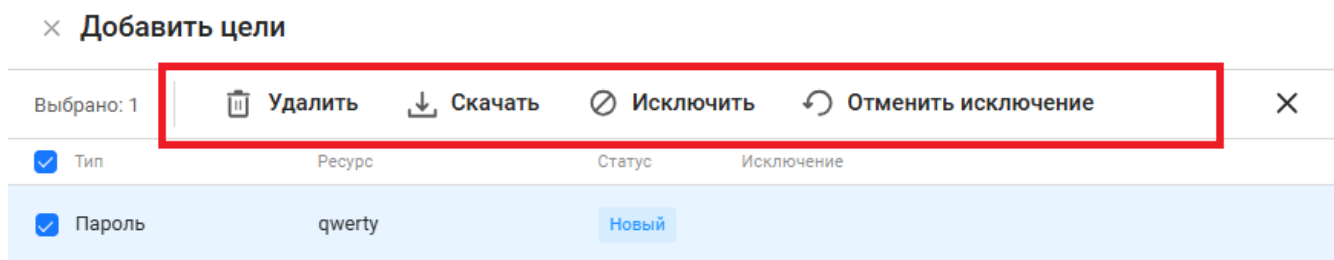


Рисунок 88 – Логика появления кнопок действий при выборе целей

Для исключения, удаления целей из списка возможно использование кнопок: - кнопка

 – добавить в исключения; - кнопка  – удалить из списка.

- 14) В окне «Добавить цели сканирования» после выбора целей нажать кнопку «Сохранить» для применения параметров.
- 15) Активировать переключатель модуля «Перемещение в сети» (рис. 89).

< Создать кампанию: Кампания-4a1e7010

Черновик

Сканирование инфраструктуры ☒

Локальная разведка ☐

Получение доступа

Фишинг ☐

Эксплуатация ☒

Перебор УЗ ☐

Перемещение в сети ☒

Постэксплуатация

Закрепление ☐

Повышение привилегий ☐

Брутфорс хэшей ☐

Экспфильтрация ☐

Удаление и шифрование ☐

Расширить поверхность атаки ⓘ ☒

Выбрать проверки 2 проверки

Цели модуля 2 Цели

Завершить создание кампании

Рисунок 89 – Переключатель модуля «Перемещение в сети»

Примечание. Некоторые тонкие настройки могут не работать в тестовом режиме.

3.4.1 Перебор УЗ

Для добавления настроек перебор УЗ необходимо:

- 1) В блоке «Получение доступа» перейти в подраздел «Перебор УЗ».
- 2) Открыть подраздел «Перебор УЗ» и перейти к заполнению требуемых настроек.
- 3) Переключатель в поле «Расширить поверхность атаки» оставить без изменения (по умолчанию активирован). Это значит, что новые цели, найденные в ходе кампании, будут использоваться модулем (рис. 90).

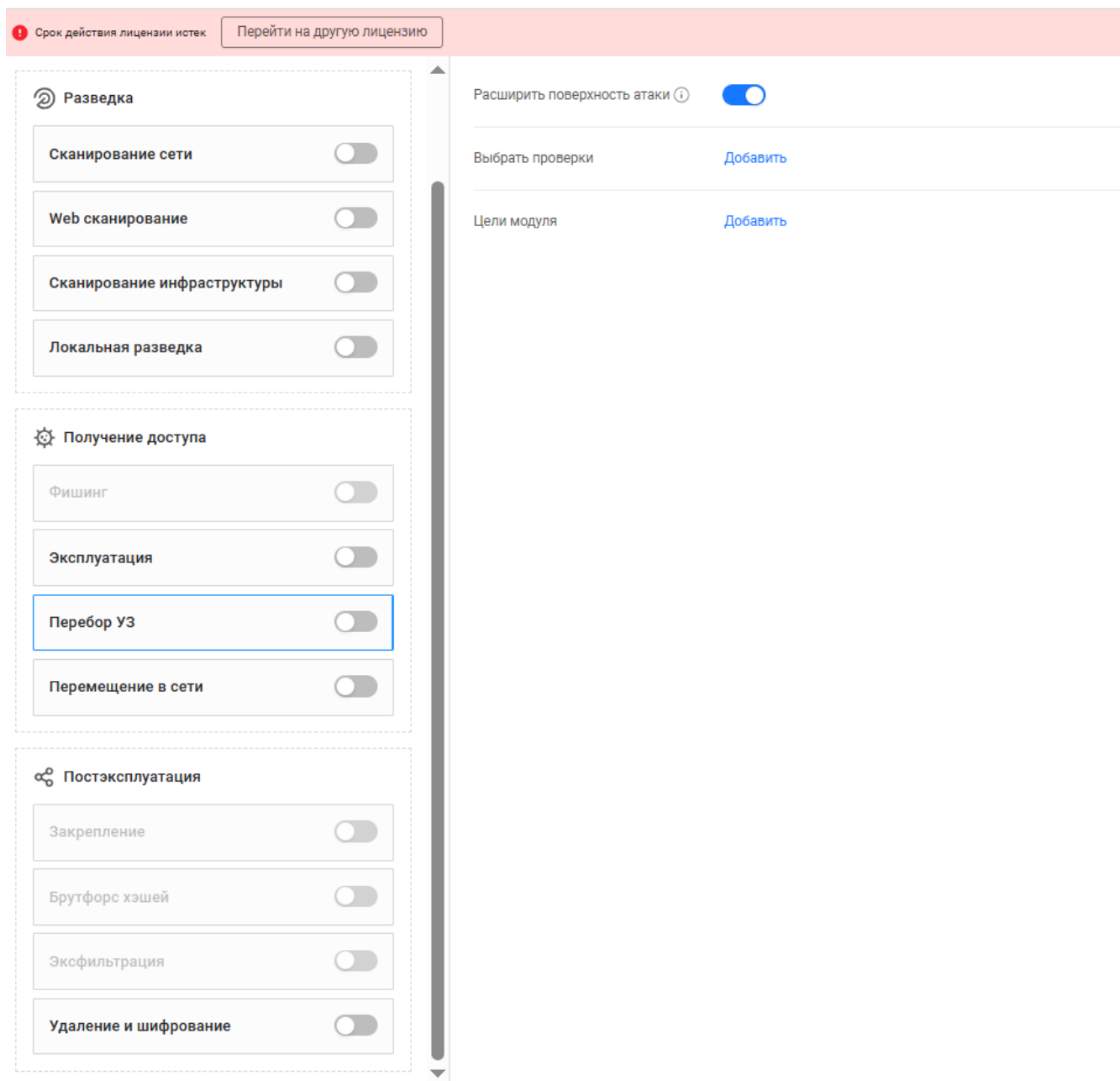


Рисунок 90 – Переключатель «Расширить поверхность атаки»

4) В поле «Выбрать проверки» нажать кнопку «Добавить» (рис. 91).

Срок действия лицензии истек. [Перейти на другую лицензию](#)

Разведка

- Сканирование сети ☐
- Web сканирование ☐
- Сканирование инфраструктуры ☐
- Локальная разведка ☐

Получение доступа

- Фишинг ☐
- Эксплуатация ☐
- Перебор УЗ ☐
- Перемещение в сети ☐

Постэксплуатация

- Закрепление ☐
- Брутфорс хэшей ☐
- Эксfiltrация ☐
- Удаление и шифрование ☐

Расширить поверхность атаки ☒

Выбрать проверки [Добавить](#)

Цели модуля [Добавить](#)

[Завершить создание кампании](#)

Рисунок 91 – Поле «Выбрать проверки»

5) В открывшемся окне «Добавить проверки» выбрать необходимые проверки из представленных в списке (рис. 92):

- «Поиск валидных учетных данных, методом перебора множества паролей и пользователей, по протоколу SSH»;
- «NXC (тихий режим) получение валидных имён пользователей FTP, и паролей в открытом виде»;
- «Получение валидных имён пользователей, и паролей в открытом виде»;

- «NXC (тихий режим) получение валидных имён пользователей SSH, и паролей в открытом виде».

× **Добавить проверки**

🔍 Введите запрос для поиска

☐ Описание

Название

☐ Поиск валидных учетных данных, методом перебора множеств... [btc-module-hydra-u-p-ssh](#)

☐ NXC (тихий режим) получение валидных имён пользователей F... [btc-module-nxc-ftp-u-p](#)

☐ Получение валидных имён пользователей, и паролей в открыт... [btc-module-nxc-smb-u-p-brute-cos](#)

☐ NXC (тихий режим) получение валидных имён пользователей S... [btc-module-nxc-ssh-u-p](#)

Всего: 4

Сохранить

Отменить

Рисунок 92 – Окно «Добавить проверки»

- 6) Нажать кнопку «Сохранить» для применения настроек. Если необходимо отменить выбор проверок, то нажать кнопку «Отменить».
- 7) В поле «Цели модуля» нажать кнопку «Добавить» (рис. 93).

! Срок действия лицензии истек Перейти на другую лицензию

Разведка

Сканирование сети ☐

Web сканирование ☐

Сканирование инфраструктуры ☐

Локальная разведка ☐

Получение доступа

Фишинг ☐

Эксплуатация ☐

Перебор УЗ ☐

Перемещение в сети ☐

Постэксплуатация

Закрепление ☐

Брутфорс хэшей ☐

Экспильтрация ☐

Удаление и шифрование ☐

Расширить поверхность атаки ☒

Выбрать проверки Добавить

Цели модуля Добавить

Завершить создание кампании

Рисунок 93 – Поле «Цели модуля»

- 8) В открывшемся окне «Добавить цели» нажать кнопку «Цель».
- 9) Заполнить требуемые поля (рис. 94):

- выбрать тип ресурса из выпадающего списка (сервис, пользователь + пароль, пользователь, пароль) (рис. 95); – ввести адрес цели, исходя из указанного выше типа ресурса;
- отключить переключатель «Исключения», который включен по умолчанию. Включение переключателя обозначает, что выбранный тип ресурса будет исключен из списка целей сканирования. Выключение обозначает, что будет добавлен как обычная цель для сканирования.

× **Добавить цели**

Тип ресурса

Адрес

Исключение ☐

🔍 Введите запрос для поиска ≡ Фильтр 📄 Загрузить цели + Цель

Рисунок 94 – Ввод данных целей

× **Добавить цели**

Тип ресурса

Адрес

Исключение ☐

🔍 Введите запрос для поиска ≡ Фильтр 📄 Загрузить цели + Цель

Рисунок 95 – Выбор типа ресурса

- 10) Нажать кнопку «Добавить». В список добавятся заданные цели сканирования или исключения.
- 11) Для загрузки перечня целей можно сразу загрузить готовый файл через опцию «Загрузить цели из файла» или сначала скачать шаблон в формате .txt через «Скачать шаблон», заполнить его и затем загрузить.
- 12) Для осуществления поиска необходимо перейти в поле «Введите запрос для поиска» для поиска записи в списке. Поиск выполняется по мере ввода

символов. При нажатии кнопки «Фильтр» открывается окно для указания параметров фильтрации (рис. 96):

- тип ресурса – выпадающий список для выбора категории;
- каталог – фильтр для выбора папок и каталогов файловой системы;
- файл – фильтр для выбора отдельных файлов;;
- состояние – переключатели для отбора целей по статусу:
- кнопка «Все» – показывать все ресурсы (включая обычные и исключённые);
- кнопка «Только исключения» – показывать только те ресурсы, которые были помечены как исключения;
- кнопка «Без исключений» – показывать только ресурсы, которые находятся в обычном состоянии, не являясь исключениями;
- переключатель «Только новые» – отображения только недавно добавленных целей (например, после последнего сканирования);
- кнопка «Применить» – активирует выбранные фильтры;
- кнопка «Закрыть» – закрывает окно фильтрации без применения изменений.

× **Добавить цели**

Тип ресурса

Адрес

Исключение ☐

🔍 Введите запрос для поиска

☐ Тип	Ресурс	Статус	Исключение
☐	Пароль йцуцуй	Новый	

☰ Фильтр ⬇ Загрузить цели + Цель

Загрузить цели из файла

Скачать шаблон

Рисунок 96 – Кнопка «Фильтр»

13) Выбрать цели из списка. При выборе целей из списка отображаются скрытые кнопки для работы с выбранными целями:

- кнопка «Удалить» – для удаления выбранных ресурсов;
- кнопка «Скачать» – для экспорта данных;
- кнопка «Исключить» – помечает ресурсы как исключённые из сканирования;
- кнопка «Отменить исключение» – снимает отметку об исключении.

Для исключения, удаления целей из списка возможно использование кнопок (рис. 97):

× **Добавить цели**

Тип ресурса

Адрес

Исключение ☐

🔍 Введите запрос для поиска ≡ Фильтр ⬇ Загрузить цели + Цель

☐	Тип	Ресурс	Статус	Исключение
☐	Пароль	йцуцуй	Новый	☐ Удалить

Рисунок 97 – Кнопки «Добавить в исключения» и «Удалить»

- 14) В окне «Добавить цели» после выбора целей нажать кнопку «Сохранить» для применения параметров.
- 15) Активировать переключатель модуля «Локальная разведка» (рис. 98).

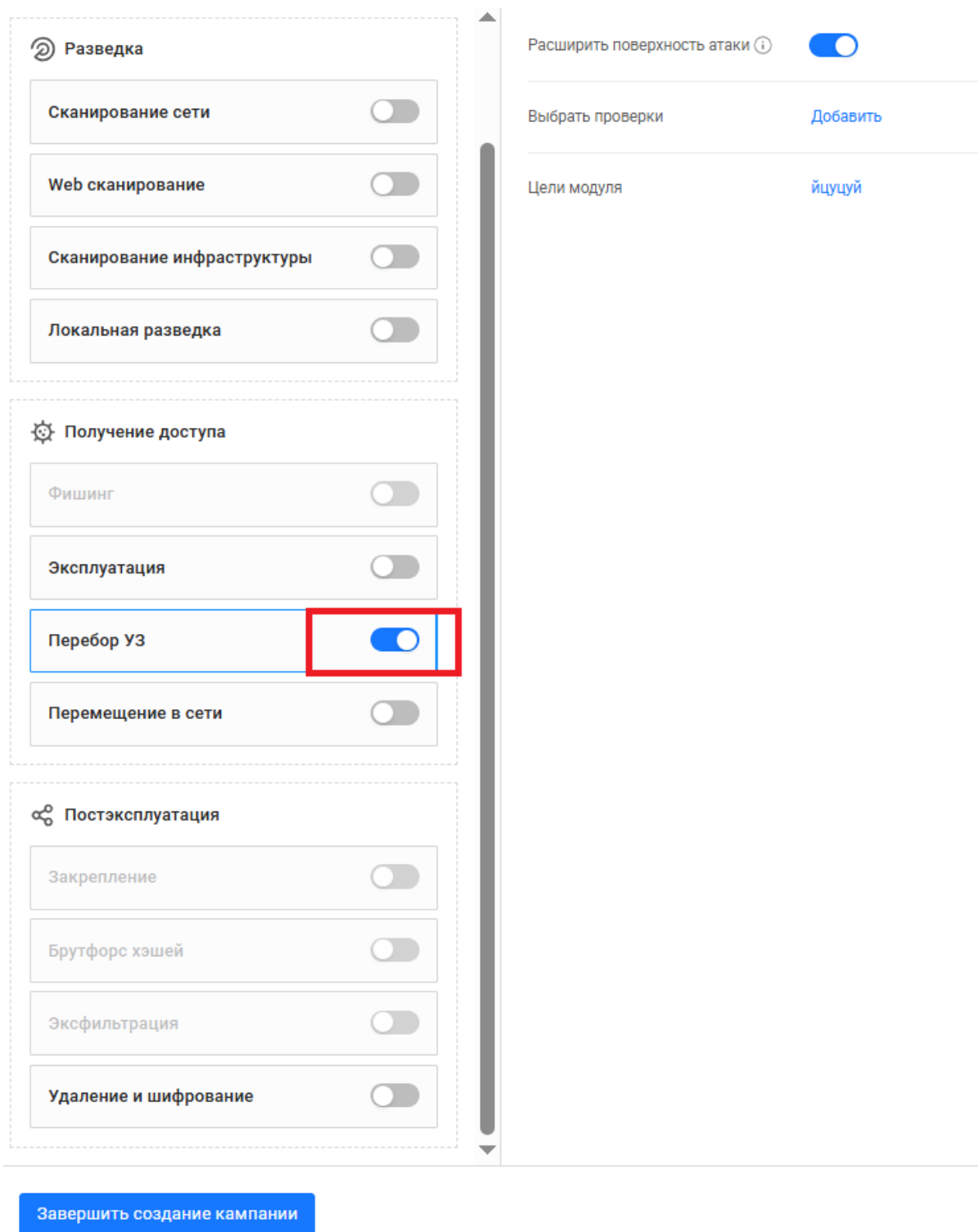


Рисунок 98 – Переключатель модуля «Перебор УЗ»

Примечание. Некоторые тонкие настройки могут не работать в тестовом режиме.

4 Фишинг

Фишинг — это метод, заключающийся в рассылке фишинговых писем целевым группам пользователей. Целью таких писем является фиксация реакции пользователей на их получение и анализ результатов фишинговых кампаний. Данный подход позволяет получить первоначальный доступ к атакуемой инфраструктуре или завладеть учётными данными конкретного пользователя внешнего сервиса. Модуль фишинга включает в себя функции для создания целевых страниц, которые имитируют легитимные веб-ресурсы, что увеличивает вероятность успешного обмана пользователей.

4.1 Мониторинг

Мониторинг результатов фишинговых атак — внутренний процесс, проводимый собственной командой безопасности. Он играет ключевую роль в оценке защищённости организации. Необходим для сбора и анализа общей информации о всех попытках мошенничества, что позволяет выявлять тенденции, оценивать уровень угроз и разрабатывать эффективные меры защиты. Предлагаемый подход позволяет осуществлять полный контроль над процессом за счёт определения параметров тестирования, анализа пользовательских реакций и немедленного получения результатов. Регулярный внутренний мониторинг позволяет оперативно выявлять проблемные зоны и вносить корректировки в стратегию защиты.

Для просмотра мониторинга в главном меню перейти в раздел «Фишинг», затем в подраздел «Мониторинг» (рис. 99) для просмотра хода и результатов выполнения заданий.

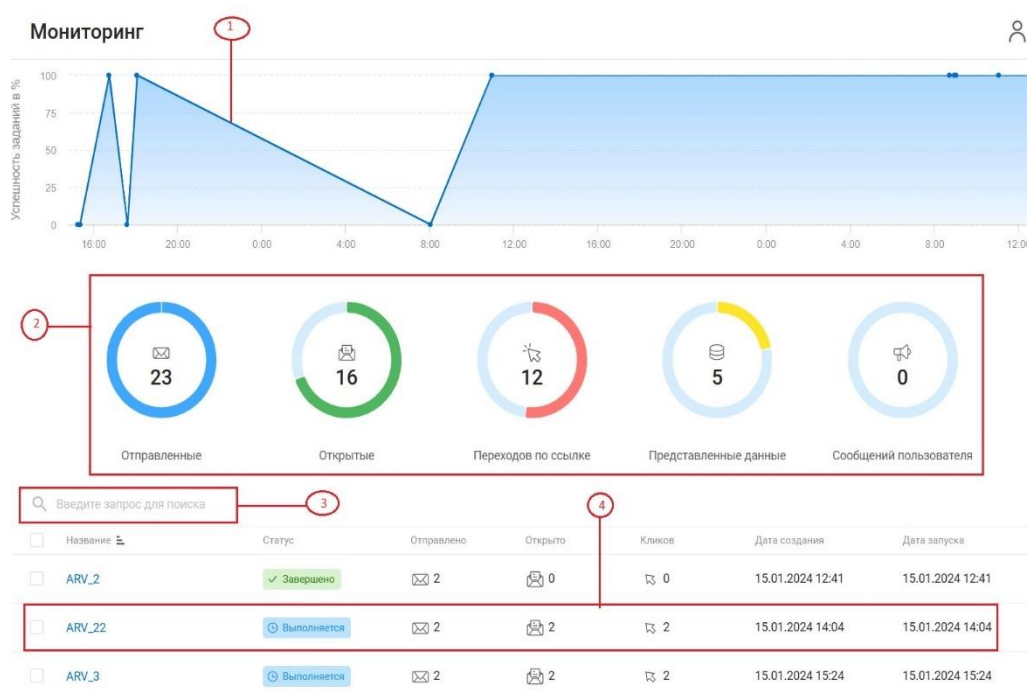


Рисунок 99 – Подраздел «Мониторинг»

В окне «Мониторинг» представлены следующие виджеты:

- 1) График успешности заданий в % (№ 1).
- 2) Круговые диаграммы (№ 2):
 - «Отправленные». Задание было создано, и письма успешно разосланы получателям.
 - «Открытые». Пользователь получил и открыл фишинговое письмо. В этом случае доступно уведомление о прочтении.
 - «Переход по ссылке». Пользователь осуществил переход по ссылке внутри письма и перешел на фишинговую страницу. Данные переходы фиксируются комплексом для отслеживания потенциальных угроз.
 - «Представленные данные». Статус активировался, если пользователь ввёл свои учётные данные на фишинговом сайте. В таком случае увеличился счётчик представленных данных.
 - «Сообщение пользователя». Пользователь ответил на фишинговое письмо, что также фиксируется для анализа.
- 3) Поисковая строка (№ 3).
- 4) Список заданий (№ 4).

Примечание. До момента, когда задания будут созданы и запущены, подраздел мониторинга останется пустой. После запуска заданий соответствующие виджеты, отвечающие за определенные показатели, будут заполнены данными.

4.2 Задания

На вкладке «Задания» настраиваются параметры фишинговой атаки.

Для указания настроек задания необходимо:

- 1) В главном меню перейти в разделе «Фишинг» в подраздел «Задания». При переходе в данный подраздел также будет отображен весь перечень заведенных заданий (рис. 100).
- 2) Нажать кнопку «Новое задание».

Фишинговые атаки / Задания



🔍 Введите запрос для поиска							🔽 Фильтр	+ Новое задание
☐ Название	Статус	Отправлено	Открыто	Кликов	Дата создания	Дата запуска		
☐ ARV_2	✓ Завершено	✉ 2	📧 0	👁 0	15.01.2024 12:41	15.01.2024 12:41		
☐ ARV_22	⌚ Выполняется	✉ 2	📧 2	👁 2	15.01.2024 14:04	15.01.2024 14:04		
☐ ARV_3	⌚ Выполняется	✉ 2	📧 2	👁 2	15.01.2024 15:24	15.01.2024 15:24		
☐ ARV_4	⌚ Выполняется	✉ 2	📧 2	👁 2	16.01.2024 08:15	16.01.2024 08:15		
☐ ARV_5	⌚ Выполняется	✉ 2	📧 2	👁 2	17.01.2024 06:03	17.01.2024 06:03		
☐ Test_1	✓ Завершено	✉ 1	📧 0	👁 0	15.01.2024 12:35	15.01.2024 12:35		
☐ Копия ARV_2	⌚ Выполняется	✉ 2	📧 0	👁 0	15.01.2024 14:56	15.01.2024 14:56		
☐ Копия ARV_3	⌚ Выполняется	✉ 2	📧 2	👁 1	17.01.2024 06:16	17.01.2024 06:16		
☐ Копия ARV_4	⌚ Выполняется	✉ 2	📧 2	👁 1	17.01.2024 06:21	17.01.2024 06:21		
☐ Копия ARV_7	⌚ Выполняется	✉ 2	📧 2	👁 1	17.01.2024 08:23	17.01.2024 08:23		
☐ Копия Копия ARV_2	⌚ Выполняется	✉ 2	📧 0	👁 0	16.01.2024 05:21	16.01.2024 05:21		

Рисунок 100 – Раздел «Задания»

- 3) В открывшемся окне «Создание задания» заполнить поля настроек формы (рис. 101):
- в поле «Название» указать название, которое однозначно идентифицирует конкретное задание;
 - в выпадающем списке «Шаблон письма» выбрать шаблон;
 - в выпадающем списке «Целевой сайт» выбрать сайт;
 - добавить URL выбранного сайта в поле «URL»;
 - в поле «Запуск задания» настроить дату и время запуска задания;
 - в поле «Равномерная рассылка писем» настроить дату и время запуска рассылки;
 - в выпадающем списке «Профиль отправителя писем» выбрать отправителя;
 - в выпадающем списке «Группы рассылки» выбрать одну или несколько групп.

← Создание задания

Название	Название
Шаблон письма	Health_Check
Целевой сайт	Testt
URL ⓘ	URL
Запуск задания	Запуск задания
Равномерная рассылка писем	Равномерная рассылка писем
Профиль отправителя писем	cred
Группы рассылки	Группы рассылки

Рисунок 101 – Окно «Создание задания»

- 4) При необходимости отправки нажать кнопку «Отправить тестовое письмо» для проверки настройки отправки.
- 5) В открывшемся окне «Тестовое письмо» заполнить поля настроек (рис. 102):
 - имя;
 - фамилию;
 - должность (необязательно);

- e-mail отправителя;
- e-mail получателя;
- URL.

✕ Тестовое письмо

Имя	Имя
Фамилия	Фамилия
Должность	Должность
E-mail отправителя	test@example.com
E-mail получателя	test@example.com
url	url

✓ Предварительный просмотр письма

Это электронное письмо, в котором вы узнаете, что настройка прошла успешно.

Подробности:

E-mail отправителя: {{ from_address }}

Кому вы отправили:

Имя: {{ first_name }}

Фамилия: {{ last_name }}

Должность: {{ position }}

фишинговый url

Отправить

Отменить

Рисунок 102 – Окно «Тестовое письмо»

- 6) Нажать кнопку «Отправить». В случае корректного указания настроек комплекс отправит тестовое письмо на указанный адрес и отобразит сообщение об успешной отправке.

- 7) В окне «Создание задания» нажать кнопку «Создать» для применения настроек задания.

4.3 Шаблоны писем

Шаблон письма — это текст, который будет направлен пользователю при массовой рассылке (фишинговой атаке). Как правило, информация в письме направлена на побуждение пользователя для перехода на сторонний ресурс. Например, сообщение может содержать фразу: «Срок действия вашего пароля истёк. Установите новый пароль». Шаблон письма необходим для имитации конкретного сервиса, которым пользуется целевая группа получателей. Например, если письма направляются сотрудникам отдела бухгалтерии, шаблон может быть оформлен в стиле банковского сайта, что увеличивает вероятность того, что получатели доверятся сообщению и перейдут по ссылке.

Для указания настроек шаблона писем необходимо:

- 1) В главном меню перейти в разделе «Фишинг» в подраздел «Шаблоны писем» (рис. 103). При переходе в подраздел отображен весь перечень заведённых шаблонов писем, дополнительно с этими письмами допустимы групповые операции.
- 2) Нажать кнопку «Новый шаблон».

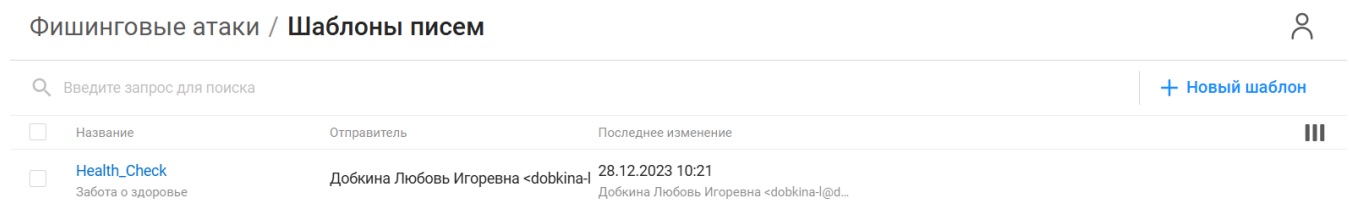


Рисунок 103 – Раздел «Шаблоны писем»

- 3) В открывшемся окне «Создание шаблона письма» заполнить поля настроек (рис. 104).
 - название;
 - доступна возможность добавления импорта шаблона при помощи кнопки «Импорт шаблона»;
 - отправитель;
 - тема письма;
 - текст. Есть вариант заполнить поле в виде текста или HTML разметки;
 - доступна возможность добавления файла, при помощи кнопки «Добавить файл»;
 - чекбокс «Добавить pixel». Добавление пикселя для отслеживания и регистрации факта открытия письма.

← Создание шаблона письма

Название	Название
Импорт шаблона ⓘ	Импорт шаблона
Отправитель ⓘ	Отправитель
Тема письма	Тема письма
Текст	<input checked="" type="button" value="Текст"/> HTML Текст письма
	☐ Добавить pixel ⓘ
Файл ⓘ	↑ Добавить файл или перетащите сюда файл
Создать	Отменить

Рисунок 104 – Окно «Создание шаблона письма»

- В окне «Создание шаблона письма» нажать кнопку «Создать» для применения настроек шаблона письма.

4.4 Группы рассылки

Группы рассылки — это набор адресов электронной почты, объединённых по определённому критерию. Например, можно создать группу для «Отдела маркетинга». Группировка получателей позволяет проводить более целенаправленные атаки,

адаптированные к конкретным организационным подразделениям компании. Это повышает вероятность успешного взаимодействия с целевой аудиторией и увеличивает шансы на достижение поставленных целей.

Для указания настроек группы рассылки необходимо:

- 1) В главном меню открыть раздел «Фишинг» и перейти в подраздел «Группы рассылки». Открыть вкладку «Получатели», чтобы завести учетные записи получателей (рис. 105).

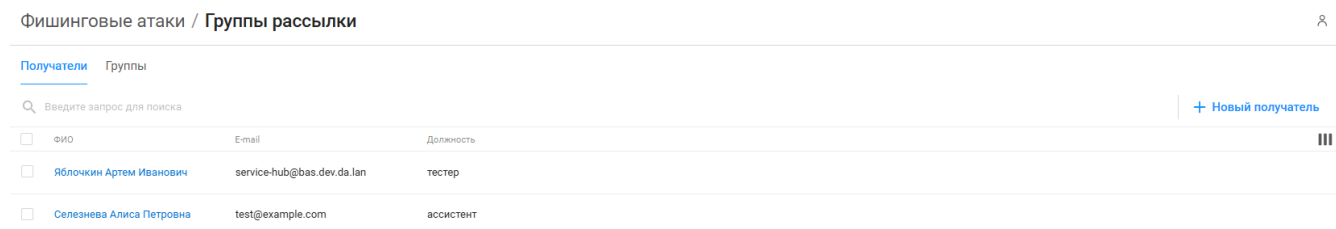


Рисунок 105 – Вкладка «Получатели»

- 2) На вкладке «Получатели» представлена информация о получателях с описанием полей:
 - поле поиска. Позволяет фильтровать список по имени, e-mail или должности;
 - кнопка «Новый получатель». Добавляет нового получателя в список вручную;
 - кнопка настройки отображения информации на странице . Позволяет убрать информацию по ФИО, электронными адресами, должностями или ролями пользователей (рис. 106);
 - кнопка удаления получателя . При нажатии происходит удаление получателя из списка;
 - таблица получателей:
 - ФИО. Полное имя получателя;
 - e-mail. Электронная почта получателя;
 - должность. Роль или должность сотрудника.

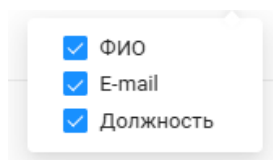


Рисунок 106 – Окно настройки отображения информации

- 3) Нажать кнопку «Новый получатель» (рис. 107).

☐	ФИО	E-mail	Должность
☐	Иванов Иван Иванович	test@example.com	Главный Иван
☐	Максимов Максим Максимович	info-hub@bas.dev.da.lan	info-hub
☐	Лопухов Иван Васильевич	service-hub@bas.dev.da.lan	повар

Рисунок 107 – Кнопка «Новый получатель»

- 4) В открывшемся окне «Добавить получателя» заполнить поля настроек (рис. 108):
- фамилия. Ввести фамилию пользователя;
 - имя. Ввести имя;
 - отчество. Ввести отчество;
 - e-mail. Ввести электронную почту;
 - должность пользователя. Ввести должность или роль;
 - доступна возможность добавления массового импорта получателей при помощи кнопки «Импорт получателей». Позволяет загрузить сразу нескольких пользователей;
 - ссылка «Скачать CSV-шаблон». Загружает шаблон таблицы, которую можно заполнить и использовать для импорта.

✕ Добавить получателя

Массовый импорт

Импорт получателей

[Скачать CSV-шаблон](#)

Фамилия

Фамилия

Имя

Имя

Отчество

Отчество

E-mail

test@example.com

Должность пользователя

Должность

Создать

Отменить

Рисунок 108 – Окно «Добавить получателя»

- 5) Нажать кнопку «Создать» для добавления нового пользователя в список получателей.

- 6) Выбрать получателей из списка (рис. 109). При выборе получателей отобразятся скрытые кнопки окна интерфейса:
- «Создать группу». Открывает новое окно «Создание группы рассылки». Ввести название группы и нажать кнопку «Создать» (рис. 110).
 - «Добавить в группу». Добавляет выбранных пользователей в существующую группу (рис. 111). Выбрать из выпадающего списка группу и нажать кнопку «Добавить».
 - «Удалить». Удаляет выбранных получателей из списка при нажатии на кнопку в новом окне «Удалить» (рис. 112).

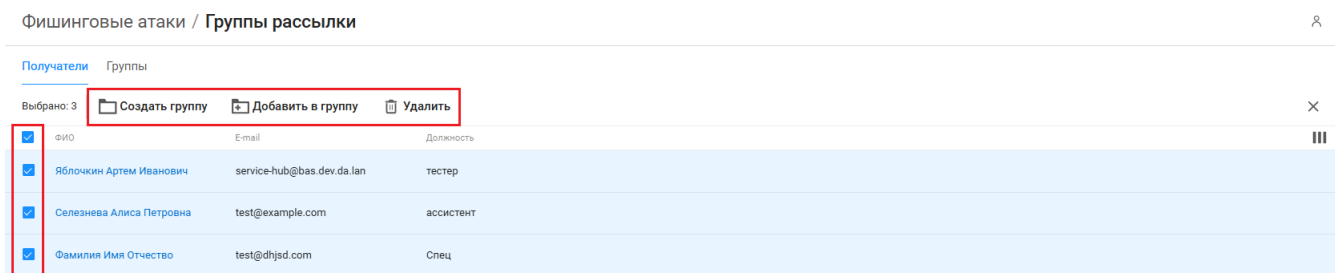


Рисунок 109 – Окно, в котором осуществлён групповой выбор

← Создание группы рассылки

Название группы	Площадка-23.04.2025
-----------------	--

🔍 Введите запрос для поиска

ФИО	E-mail	Должность
Яблочкин Артем Иванович	service-hub@bas.dev.da.lan	тестер
Селезнева Алиса Петровна	test@example.com	ассистент
Фамилия Имя Отчество	test@dhjsd.com	Спец

Создать

Отменить

Рисунок 110 – Окно «Создание группы рассылки»

[Добавить](#)[Сбросить](#)

Рисунок 111 – Окно «Добавить в группу»

Вы действительно хотите удалить 1 получателя?

[Удалить](#)[Отменить](#)

Рисунок 112 – Окно «Удалить»

- 7) В ПК имеется вкладка «Получатели», которая позволяет создавать новых пользователей и объединять их в группы. Также существует вкладка «Группы», основное назначение которой заключается в создании и редактировании групп пользователей. Для этого в главном меню перейти в разделе «Фишинг» в подраздел «Группы рассылки» и открыть вкладку «Группы» (рис. 113).

Фишинговые атаки / Группы рассылки

[Получатели](#) [Группы](#)[+ Новая группа](#)

☐	Название	Пользователи	Последнее изменение	
☐	Test_ARV	2 ▾	29.04.2025 10:00 SuperAdmin	
☐	Testt	1 ▾	29.04.2025 10:00 SuperAdmin	

Рисунок 113 – Вкладка «Группы»

- 8) Нажать кнопку «Новая группа».
- 9) В открывшемся окне ввести название группы и нажать кнопку «Добавить получателя» (рис. 114).

← Создание группы рассылки

Название группы



Введите запрос для поиска

[+ Добавить получателя](#)

Список пуст

Вы можете создать получателя при помощи кнопки ниже

[Добавить получателя](#)[Создать](#)[Отменить](#)

Рисунок 114 – Окно «Создание группы рассылки»

- 10) В окне «Выбор получателей» (рис. 115) нажать кнопку «Добавить получателей» или выбрать из списка уже добавленных.

✕ Выбор получателей

Введите запрос для поиска			+ Добавить получателей
☐	ФИО	E-mail	Должность
☐	Иван Иванович Иванов	test@mail.ru	Test
☐	Получатель Первый Один	incoming01@bas.mail.ru	ЗГД
☐	Получатель Второй Два	incoming02@bas.mail.ru	КМС
☐	Получателей Получатель Пол...	romay80092@darkse.com	великий и ужасный

Выбрать

Отменить

Рисунок 115 – Окно «Выбор получателей»

- 11) В новом окне «Добавить получателя» заполнить поля настроек формы (см. пункт 4)
- 12) Нажать кнопку «Создать» для добавления в список получателей.
- 13) Определить получателей из списка и нажать кнопку «Выбрать» (рис. 116).

✕ Выбор получателей

🔍 Введите запрос для поиска + Добавить получателей

☐	ФИО	E-mail	Должность	⋮
☒	Иван Иванович Иванов	test@mail.ru	Test	
☐	Получатель Первый Один	incoming01@bas.mail.ru	ЗГД	
☒	Получатель Второй Два	incoming02@bas.mail.ru	КМС	
☐	Получателев Получатель Пол...	romay80092@darkse.com	великий и ужасный	
☒	Фамилия Имя Отчество	test@dhjsd.com	Спец	

Выбрать Отменить

Рисунок 116 – Окно «Выбор получателей»

14) В окне «Создание группы рассылки» нажать кнопку «Создать» (рис. 117).

← Создание группы рассылки

Название группы Площадка-23.04.2025

🔍 Введите запрос для поиска + Добавить получателя

ФИО	E-mail	Должность	⋮
Фамилия Имя Отчество	test@dhjsd.com	Спец	
Получатель Второй Два	incoming02@bas.mail.ru	КМС	
Иван Иванович Иванов	test@mail.ru	Test	

Создать Отменить

Рисунок 117 – Окно «Создание группы рассылки»

15) В открывшемся окне «Группы рассылки» (рис. 118) созданная группа добавлена в перечень «Группы рассылки».

Фишинговые атаки / Группы рассылки 👤

Получатели Группы

🔍 Введите запрос для поиска + Новая группа

☐	Название	Пользователи	Последнее изменение	⋮
☐	Test_ARV	2 ▾	29.04.2025 11:08 SuperAdmin	
☐	Testt	1 ▾	29.04.2025 11:08 SuperAdmin	
☐	Площадка-23.04.2025	3 ▾	29.04.2025 11:08 SuperAdmin	

Рисунок 118 – Окно «Группы рассылки»

4.5 Целевые страницы

Целевая страница — это копия веб-ресурса, которая используется для имитирования целевого веб-ресурса. Такая страница подбирается с учётом адресной рассылки, что позволяет повысить вероятность того, что получатели доверятся сообщению и перейдут по ссылке.

Для указания настроек целевых страниц необходимо:

- 1) В главном меню перейти в разделе «Фишинг» в подраздел «Целевые страницы» (рис. 119).

Фишинговые атаки / Целевые страницы 👤

🔍 Введите запрос для поиска + Добавить страницу

☐	Название	Последнее изменение	⋮
☐	Testt	30.04.2025 14:05 SuperAdmin	
☐	Cloud_2_2	30.04.2025 14:05 SuperAdmin	✎ 📄 🗑

Рисунок 119 – Раздел «Целевые страницы»

- 2) Нажать кнопку «Добавить страницу».
- 3) В новом окне «Создание целевой страницы» (рис. 120) заполнить поля настроек формы:
 - название;
 - импорт страницы для добавления цели;
 - HTML-редактор для редактирования страницы;
 - чекбокс «Фиксация учётных данных», в случае необходимости сохранять введённые учётные данные;
 - чекбокс «Фиксация пароль», в случае необходимости сохранять введенный пароль;
 - поле «Перенаправить на» является опциональным, только при активации соответствующих чекбоксов.

← Создание целевой страницы

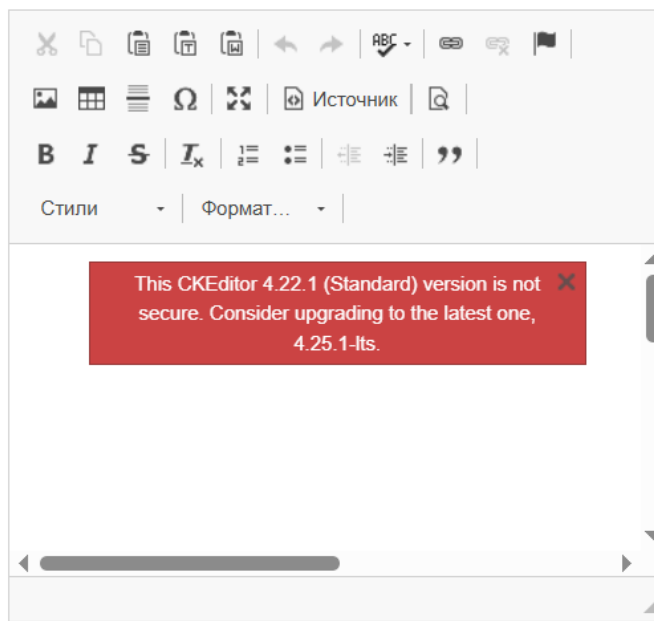
Название

test

Импорт страницы

Импорт страницы

HTML - редактор

☒ Фиксация учётных данных пользователя☒ Фиксация паролей

Перенаправить на ⓘ

http://example.com

Обязательное поле

Создать

Отменить

Рисунок 120 – Вкладка «Создание целевой страницы»

- 4) Нажать кнопку «Сохранить» для добавления целевой страницы.

4.6 Профили отправителей

Профиль отправителя создаётся и настраивается для отправки писем с определённого почтового сервера. Это позволяет обеспечить надёжность и безопасность коммуникации, а также повысить доверие получателей к отправляемым сообщениям. Правильная настройка профиля включает указание имени отправителя, адреса электронной почты и других параметров, что помогает избежать попадания писем в спам и улучшает их доставляемость.

Для указания настроек профилей отправителей необходимо:

- 1) В главном меню перейти в разделе «Фишинг» в подраздел «Профили отправителей» (рис. 121).

Фишинговые атаки / Профили отправителей 

 Введите запрос для поиска	+ Добавить профиль			
☐ Название	Почтовый протокол	E-mail	Адрес почтового сервера	Последнее изменение
☐ cred	SMTP	incoming01@bas.mail.ru	bas.mail.ru:25	05.05.2025 12:39 SuperAdmin
☐ Sender BAS Mail	SMTP	phisher@bas.mail.ru	bas.mail.ru:25	05.05.2025 12:39 SuperAdmin
☐ anon	SMTP	incoming01@bas.mail.ru	bas.mail.ru:25	05.05.2025 12:39 SuperAdmin

Рисунок 121 – Раздел «Профили отправителей»

- 2) Нажать кнопку «Добавить профиль».
- 3) В новом окне «Создание профиля отправителя» (рис. 122) заполнить поля настроек формы:
 - поле «Название профиля». Понятное название для удобной идентификации профиля отправителя;
 - поле «Почтовый протокол». Из выпадающего списка выбрать нужный почтовый протокол (например, SMTP). Определяет, какой протокол будет использоваться для отправки почты;
 - поле «Адрес почтового сервера» - указание адреса в формате «URL:порт»;
 - поле «Почтовый протокол». Из выпадающего списка выбрать нужный почтовый протокол (например, SMTP). Определяет, какой протокол будет использоваться для отправки почты;
 - поле «Логин» и «Пароль» для аутентификации на почтовом сервере;
 - чекбокс «Игнорирование ошибки сертификата», если это необходимо. Включает/отключает проверку сертификата почтового сервера;
 - чекбокс «Анонимный вход», если это требуется. Позволяет подключаться к серверу без ввода логина и пароля.

Название профиля	Sender BAS Mail
Почтовый протокол	SMTP ▼
Адрес почтового сервера	bas.mail.ru:25

Логин	phisher@bas.mail.ru
Пароль	 

☒ Игнорирование ошибки сертификата

☒ Анонимный вход

Рисунок 122 – Окно «Создание профиля отправителя»

- 4) Нажать кнопку «Отправить тестовое письмо» для проверки настройки отправки.
- 5) В новом окне «Тестовое письмо» (рис. 123) заполнить поля:
 - имя. В этом поле указывается имя отправителя письма;
 - фамилию. В этом поле указывается фамилия отправителя;
 - должность (необязательно). Это поле является необязательным и предназначено для указания должности отправителя;
 - e-mail отправителя. В этом поле вводится адрес электронной почты отправителя;

- e-mail получателя. В этом поле указывается адрес электронной почты получателя тестового письма;
- URL. Это поле используется для указания URL-ссылки, которая будет содержаться в тестовом письме.

✕ Тестовое письмо

Имя	Имя
Фамилия	Фамилия
Должность	Должность
E-mail отправителя	test@example.com
E-mail получателя	test@example.com
url	url

✓ Предварительный просмотр письма

Это электронное письмо, в котором вы узнаете, что настройка прошла успешно.

Подробности:

E-mail отправителя: {{ from_address }}

Кому вы отправили:

Имя: {{ first_name }}

Фамилия: {{ last_name }}

Должность: {{ position }}

фишинговый url

Отправить

Отменить

Рисунок 123 – Окно «Тестовое письмо»

- 6) Нажать кнопку «Отправить». Система отправит тестовое письмо на указанный адрес и отобразит сообщение об успешной отправке.

- 7) В окне «Создание профиля отправителя» нажать кнопку «Сохранить» для применения настроек.

5 Карточка кампании

Для просмотра карточки кампании необходимо:

- 1) В главном меню открыть раздел «Кампании» (рис. 124).

Кампания	Статус	Платформы	Задания	Дата создания	План, дата начала	План, дата завершения	Уведомления	Автор
Кампания-5204715	Завершена	1	Task_bash_cred-checker-demo...	17.11.2025 17:54	-	∞	-	Тест Т.
Кампания-2e531b0	Завершена	1	Task_btc-module-serp-vuln-sca...	17.11.2025 16:08	-	∞	-	Тест Т.
Кампания-abc1909	Завершена	1	Task_bash_cred-checker-demo...	18.11.2025 12:36	18.11.2025 12:37	∞	-	admin
Кампания-6263a86c	Завершена	1	Task_bash_cred-checker-demo...	18.11.2025 12:31	18.11.2025 12:32	∞	-	admin
checker-56e19a2c	Завершена	1	Task_bash-shadow-read-check...	18.11.2025 12:05	-	∞	-	Левченко О.
put agent 24706-33752e69	Завершена	1	put agent 24706-33752e69_btc...	18.11.2025 11:41	-	∞	-	Левченко О.
ssh test словарь-994007cd	Завершена	1	Task_btc-module-mtc-ssh-u-p...	18.11.2025 11:31	-	∞	-	Левченко О.
Кампания-372b54a4	Завершена	1	Task_btc-module-mtc-ssh-u-p...	18.11.2025 11:27	18.11.2025 11:29	∞	-	admin
ssh тикер 10.100.0.10-c63e1ef0	Завершена	1	Task_btc-module-mtc-ssh-u-p...	18.11.2025 10:47	-	∞	-	Левченко О.
Кампания-3c76a7c1	Завершена	-	-	18.11.2025 09:31	-	∞	-	Евгений К.
Кампания-c0fb6212	Завершена	-	-	18.11.2025 09:31	-	∞	-	Евгений К.
Кампания-022c24e1	Завершена	1	Кампания-022c24e1_mtc-local...	17.11.2025 16:05	-	∞	-	Тест Т.
Кампания-9c4a4528	Завершена	1	Task_btc-module-serp-vuln-sca...	17.11.2025 15:53	-	∞	-	Тест Т.
Кампания-356a0ea0	Завершена	1	Task_btc-module-serp-vuln-sca...	17.11.2025 15:49	-	∞	-	Тест Т.
Кампания-306e084a	Завершена	-	-	17.11.2025 15:42	-	∞	-	admin
Кампания-e67f0f4b	Завершена	-	-	17.11.2025 15:19	-	∞	-	Тест Т.
Кампания-eaf98187	Завершена	1	Task_btc-module-serp-vuln-sca...	17.11.2025 15:06	-	∞	-	Тест Т.
Кампания-89428b5b	Завершена	1	Task_btc-module-serp-vuln-sca...	17.11.2025 14:57	-	∞	-	Тест Т.

Рисунок 124 – Раздел «Кампании»

- 2) Навести курсор на интересующую кампанию и нажать левой кнопкой мыши по названию кампании, чтобы перейти в карточку кампании.
- 3) В открывшемся окне указана вся информация о ходе выполнения кампании (рис. 125).

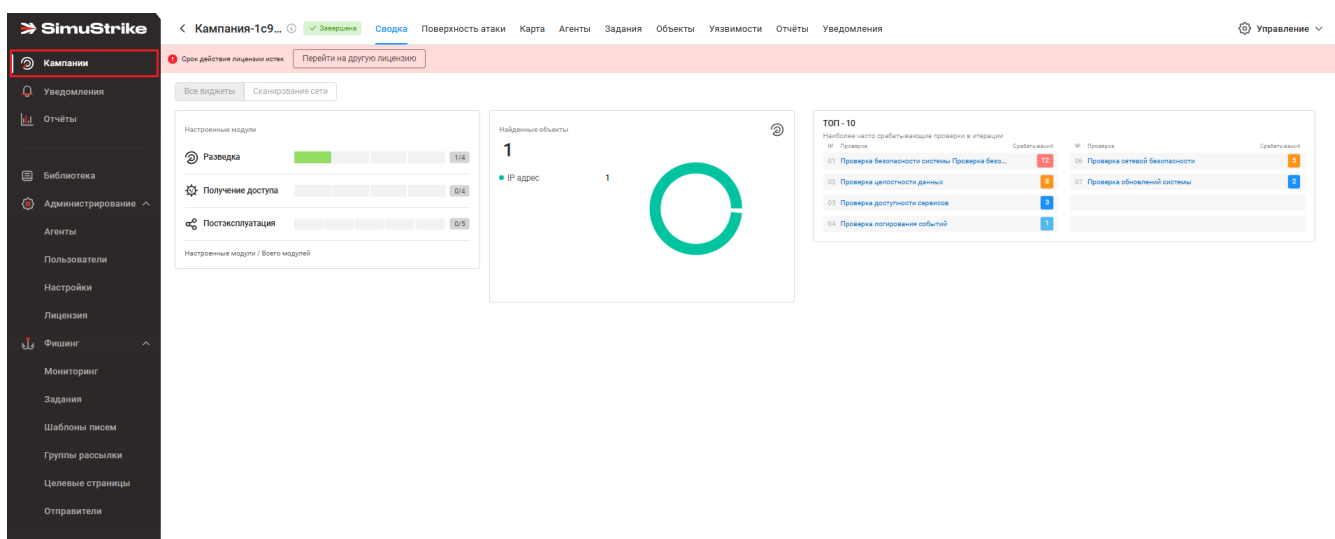


Рисунок 125 – Окно «Карточка кампании»

Примечание. Чтобы изменить параметры кампании, необходимо открыть её карточку, нажать кнопку «Управление» и выбрать в списке пункт «Настройки кампании» (рис.126). Если необходимо архивировать кампанию, то выбрать в списке пункт «Архивировать кампанию».

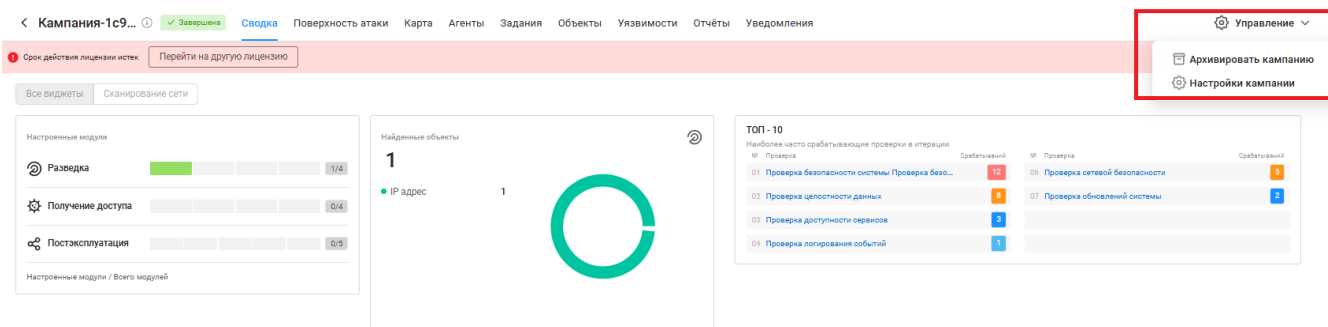


Рисунок 126 – Кнопка «Настройки кампании»

5.1 Сводка

Вкладка «Сводка» является рабочим пространством для мониторинга хода кампании. Здесь отображается сводная информация по всем активностям (виджеты/метрики).

Для просмотра объектов, участвующих в кампании необходимо:

- 1) В карточке кампании открыть вкладку «Сводка» (рис. 127).

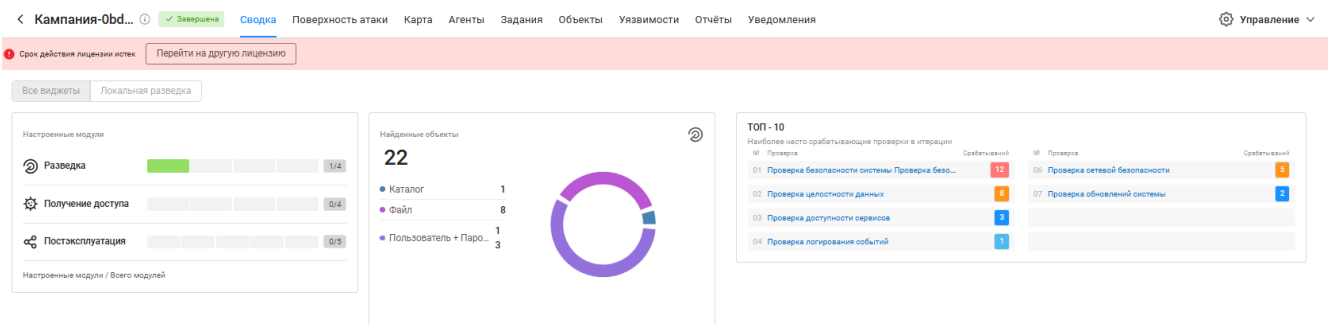


Рисунок 127 – Вкладка «Сводка»

В окне «Сводка» отображаются виджеты с информацией: - сети, IP-адреса, сервисы, доменные имена, веб-серверы; - сетевые директории, веб-приложения; - Контактные данные: e-mail, телефоны; - Локальные объекты: директории, версии программ, файлы, имена пользователей, пароли, хэши.

5.2 Карта

Карта сети — это интерактивный граф, который визуализирует структуру сети, статус безопасности каждого хоста и пути потенциального или реального распространения кибератак. Она предоставляет контекстную информацию об узлах (IP, ОС, уязвимости, компрометация) и связях между ними, позволяя фильтровать данные для анализа всей

сети, отслеживания атак по цепочке Kill Chain или мониторинга хостов с установленными агентами.

Для просмотра карты необходимо:

- 1) В карточке кампании открыть вкладку «Карта» (рис. 128).

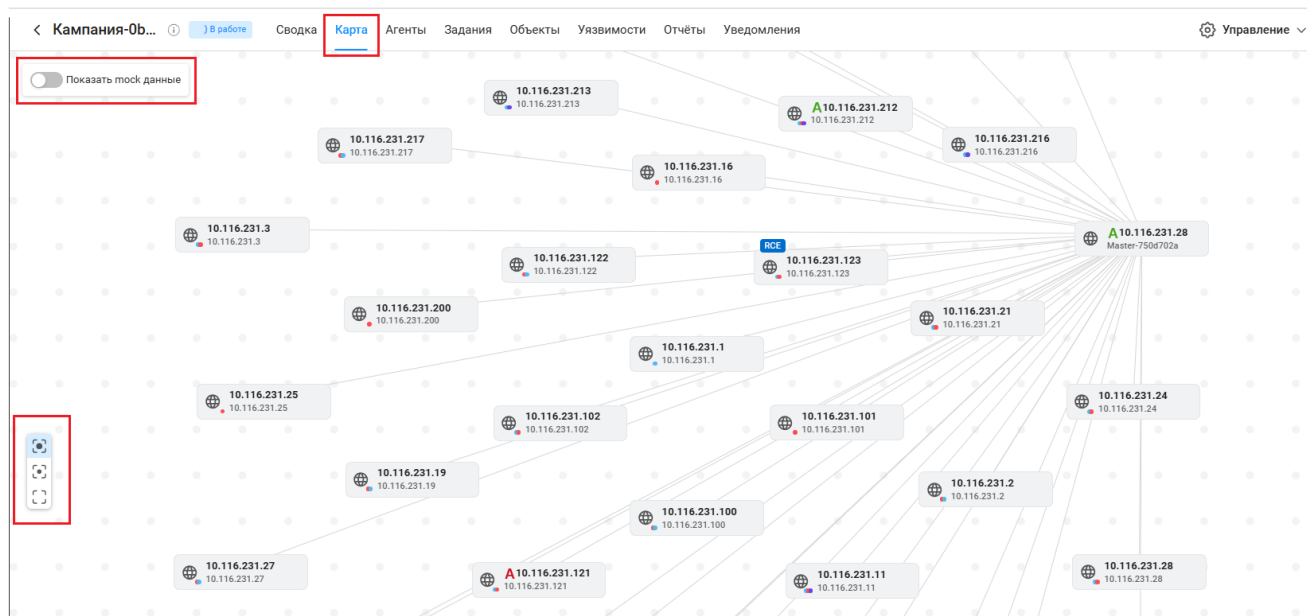


Рисунок 128 – Вкладка «Карта»

- 2) Для просмотра карточки с информацией необходимо выбрать интересующий узел (рис. 129):
 - вкладка «Общая информация» – отображает основные сведения;
 - вкладка «CVE» – отображает список уязвимостей;
 - вкладка «Порты» – информация об сетевых портах;
 - вкладка «Сводка» – обобщённый отчёт;
 - вкладка «Маршруты» – таблица маршрутизации;
 - вкладка «Процессы» – список запущенных процессов;
 - вкладка «Сетевые интерфейсы» – список сетевых интерфейсов;
 - вкладка «Логи» – просмотр прикладных логов.

×

10.116.231.122

Площадка: DA-Main

Общая информация

CVE

Порты

Сводка

Маршруты

Процессы

Сетевые интерфейсы

Логи

Дата создания

04.12.2025 17:16

Является исключением

Нет

Был доступен

-

Уязвимость

-

Добавлен пользователем

Да

Тип

IP адрес

Свойства объекта

-

Закреть

Рисунок 129 – Карточка с информацией

5.3 Агенты

Для просмотра площадок и агентов в карточке кампании необходимо:

- 1) В карточке кампании открыть вкладку «Агенты» для просмотра детальной информации обо всех агентах на выбранных площадках (рис. 130).

← Кампания-aa... ✓ Завершена Сводка Карта **Агенты** Задания Объекты Уязвимости Отчёты Уведомления Управление

🔍 Введите запрос для поиска

Площадка	Адрес для агентов	Адрес для площадки	Статус	Агенты/онлайн
DA-Main	10.116.231.28:1884	10.116.231.28:1884	✓ online	7/5
Название агента	Тип	Статус	Последнее соединение	Пользователь агента
Master-52a1e1f5	Резидент	✓ online	04.09.2025 15:42	root
Агент-b363509b	Тонкий	✓ online	04.09.2025 15:42	root
Новый-6b815170	Тонкий	⊗ offline	22.08.2025 17:04	root
новый_созданный-3ebf...	Тонкий	✓ online	04.09.2025 15:42	root
Агент-linux-42979a93	Тонкий	✓ online	04.09.2025 15:42	levchenko-o
Агент-475c298f	Тонкий	⊗ offline	22.08.2025 17:03	root
Агент-d7ab3d3c	Тонкий	✓ online	04.09.2025 15:42	root

Всего: 7

Рисунок 130 – Вкладка «Агенты»

- 2) На вкладке «Агенты» представлена информация о площадках (рис. 131):
- Площадка – название площадки. Есть возможность раскрыть для просмотра агентов;
 - Адрес для агентов – порт, через который агенты подключаются к площадке;
 - Адрес для площадки – порт для связи площадки с ядром системы;
 - Статус – указывает, доступна ли туннельная связь (онлайн, оффлайн);
 - Агенты/онлайн – количество активных агентов из общего числа (например, 7/5).

← Кампания-аа... ✓ Завершена Сводка Карта **Агенты** Задания Объекты Уязвимости Отчёты Уведомления ⚙ Управление

🔍 Введите запрос для поиска

Площадка	Адрес для агентов	Адрес для площадки	Статус	Агенты/онлайн
▼ DA-Main	10.116.231.28:1884	10.116.231.28:1884	✓ online	7/5
Название агента	Тип	Статус	Последнее соединение	Пользователь агента
Master-52a1e1f5	Резидент	✓ online	04.09.2025 15:42	root
Агент-b363509b	Тонкий	✓ online	04.09.2025 15:42	root
Новый-6b815170	Тонкий	⊗ offline	22.08.2025 17:04	root
новый_созданный-3ebf...	Тонкий	✓ online	04.09.2025 15:42	root
Агент-linux-42979a93	Тонкий	✓ online	04.09.2025 15:42	levchenko-o
Агент-475c298f	Тонкий	⊗ offline	22.08.2025 17:03	root
Агент-d7ab3d3c	Тонкий	✓ online	04.09.2025 15:42	root

Всего: 7

Рисунок 131 – Таблица «Площадки»

- 3) Раскрыть площадку для просмотра информации об агентах (рис.132):
- Название агента – условное имя агента;
 - Тип – резидент/тонкий агент;
 - Статус – онлайн, оффлайн;
 - Последнее соединение – дата и время последней активности;
 - Пользователь агента – от какого пользователя работает агент;

← Кампания-аа... ① ✓ Завершена

Сводка

Карта

Агенты

Задания

Объекты

Уязвимости

Отчёты

Уведомления

⚙ Управление ▾

🔍 Введите запрос для поиска

Площадка	Адрес для агентов	Адрес для площадки	Статус	Агенты/онлайн
▼ DA-Main	10.116.231.28:1884	10.116.231.28:1884	✓ online	7/5
Название агента	Тип	Статус	Последнее соединение	Пользователь агента
Master-52a1e1f5	Резидент	✓ online	04.09.2025 15:42	root
Агент-b363509b	Тонкий	✓ online	04.09.2025 15:42	root
Новый-6b815170	Тонкий	⊗ offline	22.08.2025 17:04	root
новый_созданный-3ebf...	Тонкий	✓ online	04.09.2025 15:42	root
Агент-linux-42979a93	Тонкий	✓ online	04.09.2025 15:42	levchenko-o
Агент-475c298f	Тонкий	⊗ offline	22.08.2025 17:03	root
Агент-d7ab3d3c	Тонкий	✓ online	04.09.2025 15:42	root

Всего: 7

Рисунок 132 – Таблица «Агенты»

Примечание. Для просмотра карточки с информацией необходимо нажать на название интересующего агента (рис.133).

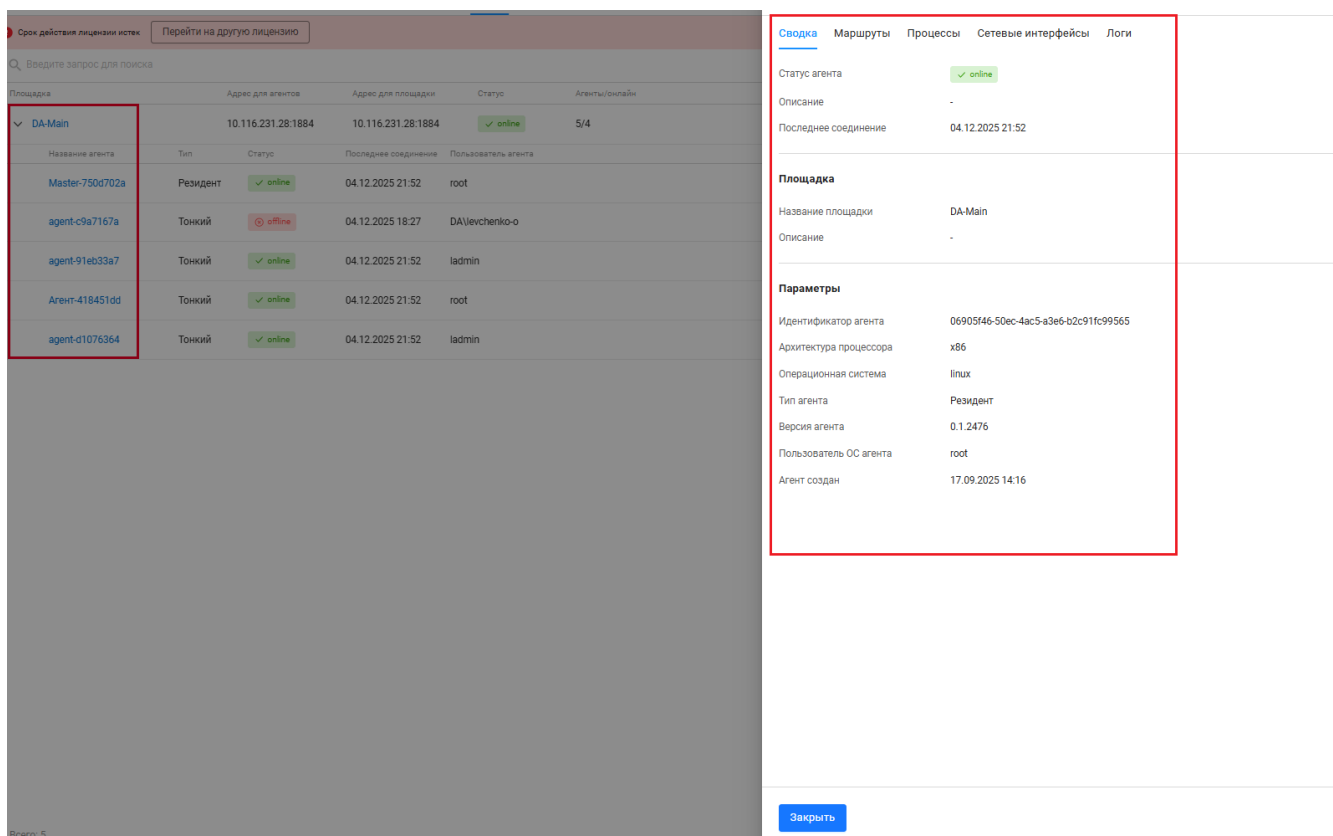


Рисунок 133 – Карточка агента

5.4 Задания

Каждый модуль может последовательно выполнять работу по нескольким целям. Каждое новое задание представляет собой один этап в очереди модуля. Например, сетевой сканер может находить новые объекты при работе с исходным объектом, и каждый из вновь найденных объектов становится целью как для этого модуля, так и для других модулей, порождая новые задания.

Для просмотра статуса и параметров каждого задания, а также координации их выполнения необходимо перейти в карточке кампании на вкладку «Задания» (рис. 134).

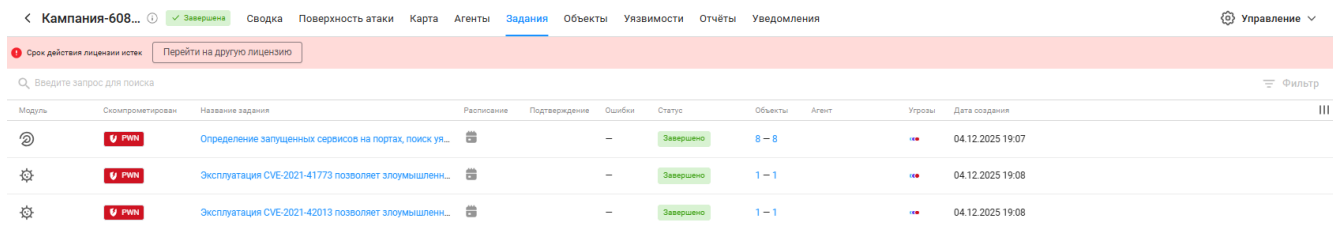


Рисунок 134 – Вкладка «Задания»

В окне представлена информация о заданиях:

- поле «Название задания» -- имя задачи;
- поле «Расписание» -- указывает дату и время запуска задания;
- поле «Статус» -- состояние выполнения задания;
- поле «Угрозы» -- тип обнаруженных угроз;
- поле «Объекты» -- количество задействованных объектов;
- поле «Последний запуск» -- указывает дату и время последнего запуска задания.

При нажатии на название задания отображается окно с полной информацией (рис. 135):

- вкладка «Сводка»:
 - блок «Основные сведения»:
 - поле «Задание создано» -- дата и время создания задания;
 - поле «Описание» -- описание задания;
 - поле «Переодичность» -- регулярность выполнения задания;
 - поле «Расписание» -- дата и время выполнения задания;
 - поле «Кампания» -- принадлежность к конкретной кампании;
 - блок «Параметры»:
 - поле «Запускать не раньше»;
 - поле «Запускать не позже»;
 - поле «Время последнего запуска»;
 - поле «Время завершения»;
 - блок «Подтверждение»:
 - поле «Необходимо подтверждение для запуска» -- определяет, требуется ли ручное подтверждение перед запуском;
- вкладка «Вх. объекты»:
 - поле «Объект» -- целевой ресурс;
 - поле «Последняя угроза» -- уровень обнаруженной угрозы;
 - поле «Статус» -- текущее состояние;
 - поле «Жизненный цикл» -- режим управления объектом;
 - поле «Исключение» -- наличие исключений;
- вкладка «Исх. объекты»:
 - поле «Объект» -- целевой ресурс;
 - поле «Последняя угроза» -- уровень обнаруженной угрозы;
 - поле «Статус» -- текущее состояние;
 - поле «Жизненный цикл» -- режим управления объектом;
 - поле «Исключение» -- наличие исключений;
- вкладка «Информация об ошибке».

Task_bash-cred-checker-demo_DIRECTORY_0bd685c5-4d58-4b42-a68f-
7237874f3b8c_agent_418451dd-e81a-47b6-9daa-6312fe3c3e09

Статус: Завершено

Сводка Вх. объекты Исх. объекты Информация об ошибке

Задание создано	03.12.2025 16:02
Описание	Auto-generated task for DIRECTORY resources using module btc-local-module-bash-cred-checker-de in campaign Кампания-0bd685c5
Периодичность	Однократно
Расписание	03.12.2025 16:02
Кампания	Кампания-0bd685c5

Параметры

Запускать не раньше	03.12.2025 16:02
Запускать не позже	04.12.2025 16:02
Время последнего запуска	-
Время завершения	03.12.2025 16:12

Подтверждение

Необходимо подтверждение для запуска	Нет
--------------------------------------	-----

Закрыть

Рисунок 135 – Карточка с информацией о задании

При наведении на задание доступна возможность копировать, добавить в архив или подтвердить задачу (рис. 136).

🔍 Введите запрос для поиска

Фильтр

Модуль	Скомпрометирован	Название задания	Расписание	Подтверждение	Ошибки	Статус	Объекты	Агент	Угрозы	Дата создания
🔗	—	Поиск чувствительных данных по ключам в *.txt файл...	📅	—	—	Завершено	1 – 22	—	🚨	03.12.2025 16:02
🔗	...	Поиск чувствительных данных по ключам в *.txt файл...	📅	—	—	Завершено	1 – 1	—	🚨	03.12.2025 16:02

Копировать
 Архив
 Подтвердить задачу

Рисунок 136 – Контекстное меню действий

5.5 Объекты

Объекты — это ресурсы, как физические (сетевое оборудование, серверы, АРМ), так и виртуальные, включая адреса электронной почты, номера телефонов, URL и любые другие ресурсы, входящие в список потенциальных целей для атаки в рамках кампании.

Для просмотра объектов, участвующих в кампании необходимо:

- 1) В карточке кампании открыть вкладку «Объекты» (рис. 137).

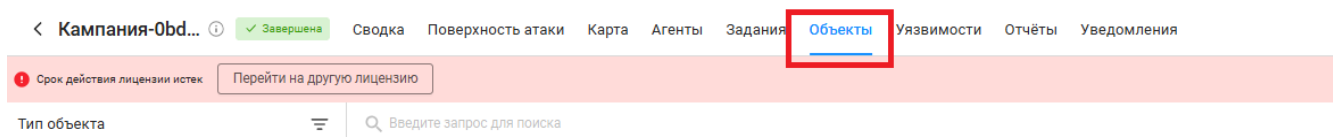


Рисунок 137 – Вкладка «Объекты»

- 2) В левой панели представлена классификация всех типов обнаруженных объектов (рис. 138):
 - Сети, IP-адреса, Сервисы, Доменные имена, Веб-серверы;
 - Сетевые директории, Веб-приложения;
 - Контактные данные: E-mail, Телефоны;
 - Локальные объекты: Директории, Версии программ, Файлы, Имена пользователей, Пароли, Хэши.

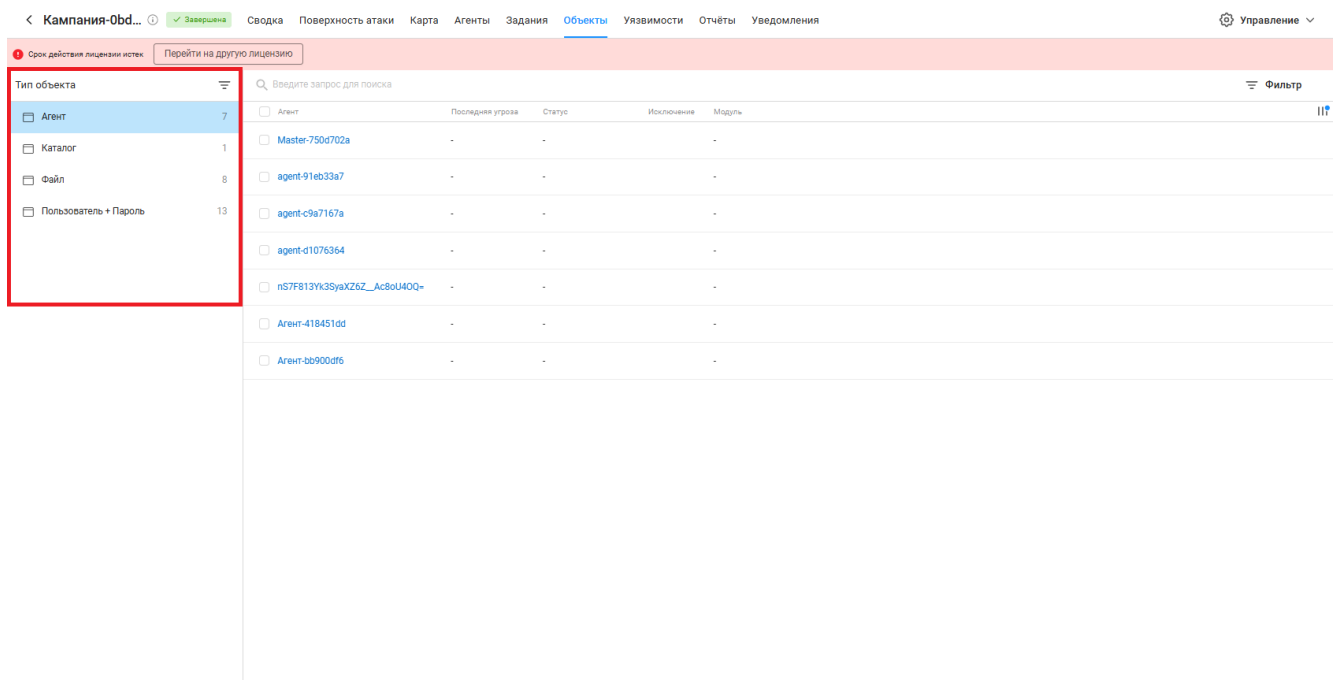


Рисунок 138 – Панель «Классификации объектов»

- 3) В правой панели представлены детали по объектам, входящим в выбранную категорию (рис. 139):
- тип объекта;
 - последняя угроза – отображается уровень риска (информация, низкая, средняя, высокая, критическая);
 - статус – текущее состояние указывает, что по данному объекту сейчас выполняется задача или анализ;
 - модуль;
 - исключение.

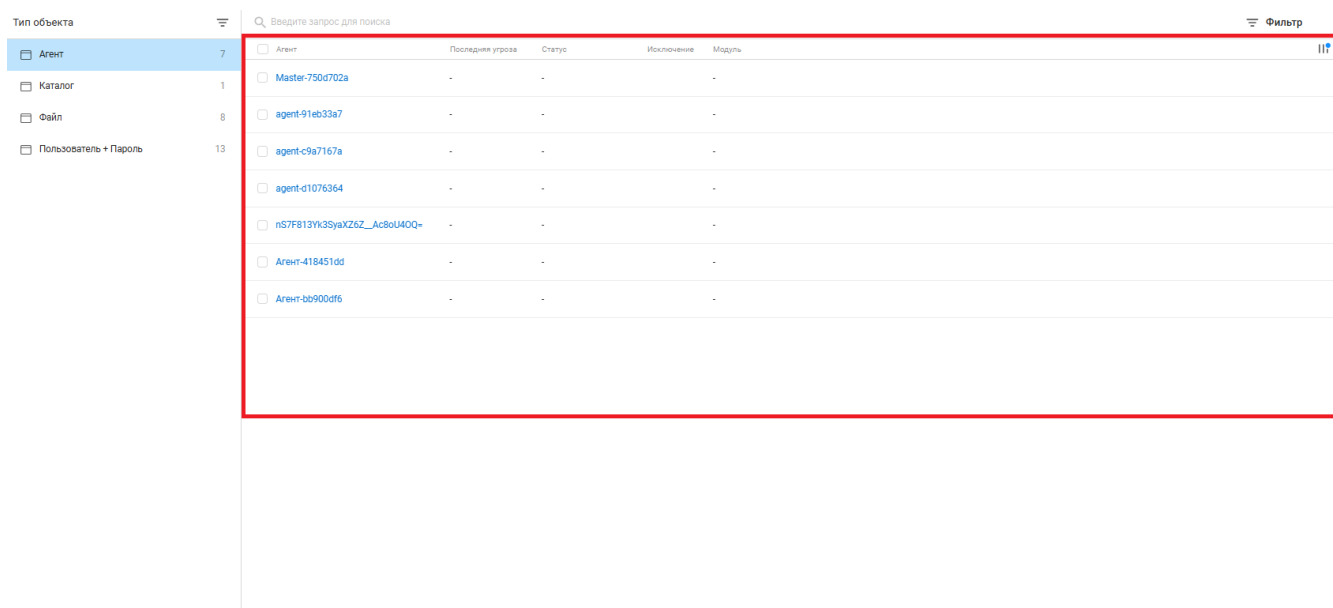


Рисунок 139 – Панель «Детали объектов»

- 4) Для просмотра информации о объектах необходимо выбрать тип объекта и нажать на название объекта (рис. 140).

The screenshot displays the 'Объекты' (Objects) section of the SimuStrike interface. On the left, a sidebar shows the object types: Агент (7), Каталог (1), Файл (8), and Пользователь + Пароль (13). The main table lists objects with columns for selection, name, last update, status, and exclusion. The object 'agent-c9a7167a' is selected and highlighted with a red box. To the right, a detailed view for this object is shown, also highlighted with a red box. It includes tabs for 'Общая информация' (General information), 'CVE', 'История' (History), and 'Модуль' (Module). The 'Общая информация' tab is active, displaying the following details:

- Дата создания** (Creation date): 03.12.2025 16:02
- Является исключением** (Is an exception): Нет (No)
- Был доступен** (Was accessible): -
- Уязвимость** (Vulnerability): -
- Добавлен пользователем** (Added by user): Да (Yes)
- Тип** (Type): Агент (Agent)
- Свойства объекта** (Object properties):
 - Операционная система (Operating system): windows

A 'Закреть' (Close) button is located at the bottom right of the details panel.

Рисунок 140 – Карточка информации о объектах

6 Библиотека

Библиотека — это специальное место, куда попадают различные ресурсы из инфраструктурных эксплуатационных сервисов. Она служит точкой входа и просмотра, позволяя пользователям взаимодействовать с элементами, которые могут быть как локальными, так и централизованными.

Основная цель библиотеки — предоставление возможности просмотра и добавления новых ресурсов, которые способствуют эффективной работе модулей. Например, в библиотеке могут храниться словари для брутфорса.

Библиотека выполняет важную роль в передаче информации между различными комплексами и кампаниями. Поскольку каждая кампания и комплекс являются обособленными, библиотека объединяет экспертизу и понимание, а также предоставляет доступ к первичным модулям, которые можно использовать в работе.

Для просмотра настроек подраздела «Библиотека» необходимо:

- 1) В главном меню перейти в раздел «Библиотека» (рис. 141).

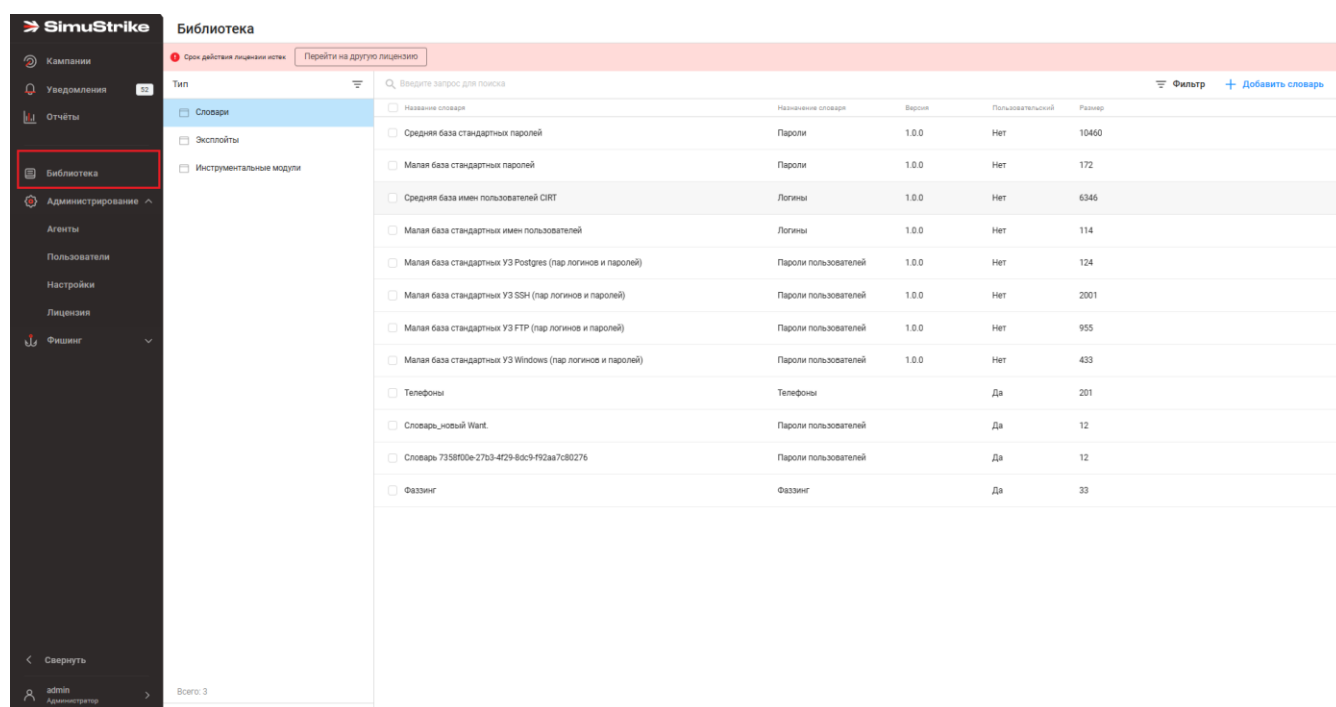


Рисунок 141 – Раздел «Библиотека»

- 2) В открывшемся окне «Библиотека» (рис. **fig:6322222?**) в левой области окна представлено содержимое библиотеки:
 - словари. Отображает словари, такие как словарь паролей, словарь пользователей, словарь фаззинга.
 - эксплойты. Отображает материалы, связанные с эксплойтами.
 - инструментальные модули. Отображает материалы, связанные с инструментальными модулями.

- фильтры . Предназначены для настройки фильтрации данных по типу.

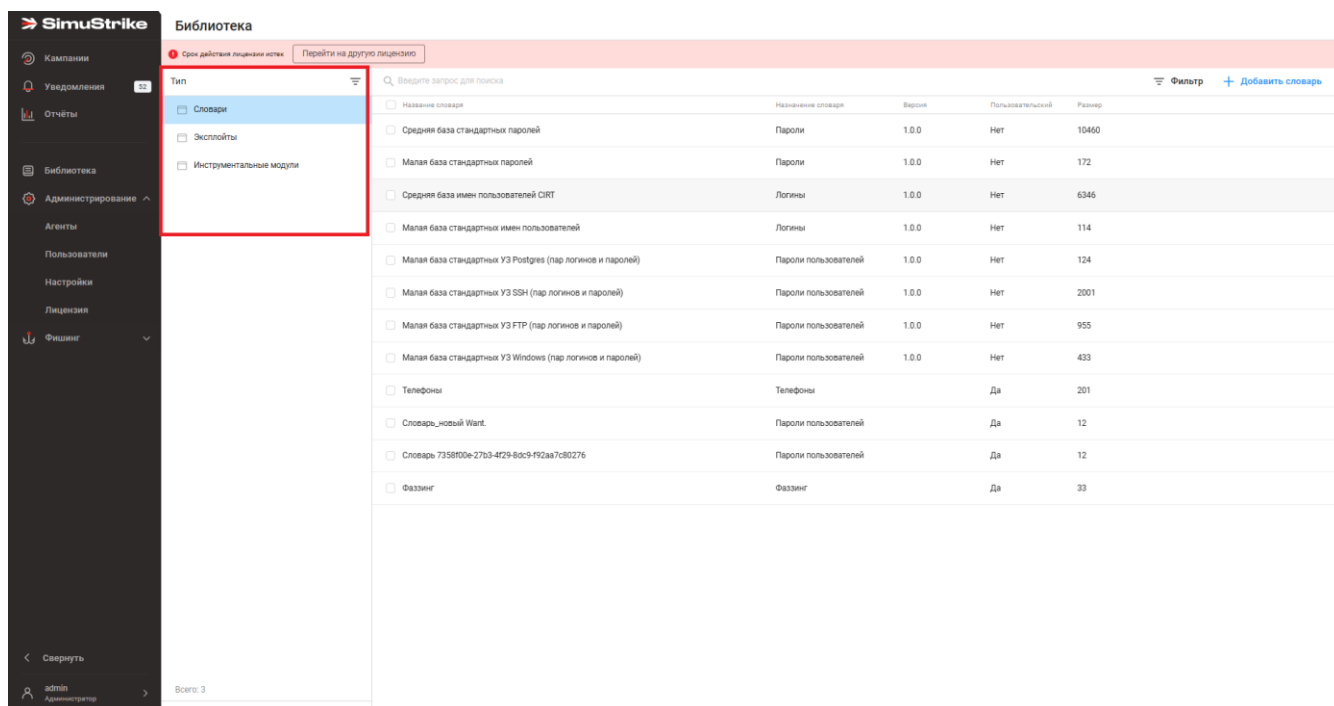


Рисунок 142 – Окно «Библиотека»

6.1.1 Словари

Словари могут быть различных типов, есть возможность добавлять новые словари, которые будут использоваться в зависимости от конкретных задач. Например, словари стандартных паролей, стандартных логинов, словари для фаззинга и многие другие. Словарь можно редактировать или удалять в случае необходимости. В библиотеке представлено множество типов словарей, что позволяет гибко настраивать их под целевое назначение.

Для просмотра интерфейса в окне «Библиотека» перейти на вкладку «Словари» в левой области окна. С правой стороны окна отображается состав полей и вкладок: - поле запроса для поиска; - кнопка . При нажатии вызывает окно «Фильтр» (рис. 143) с возможностью выбора указания назначения словаря (пароли, фаззинг, логины, E-mail адреса, телефоны, пароли пользователей, хеши пользователей, хеши). - кнопка «Добавить словарь».

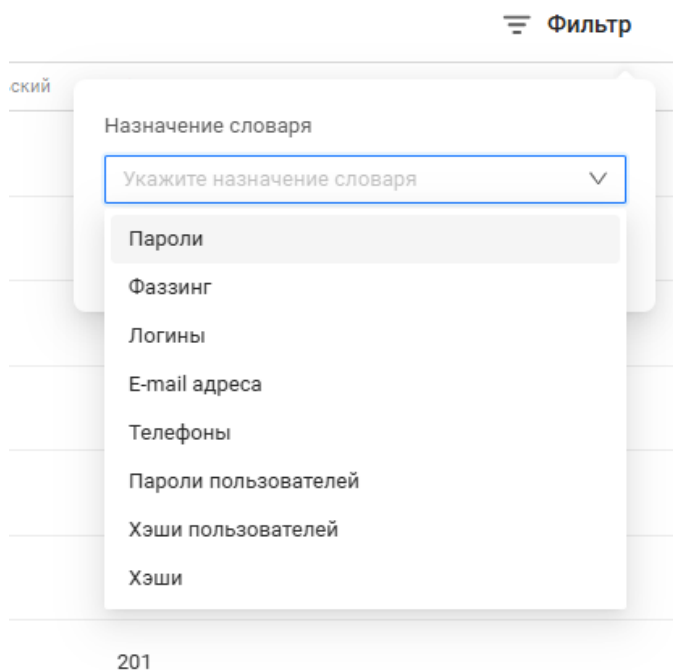


Рисунок 143 – Окно «Фильтр»

Ниже представлена полная информация с описанием каждого словаря (рис. 144):

- Средняя база стандартных паролей;
- Малая база стандартных паролей;
- Средняя база имен пользователей CIRT;
- Малая база стандартных имен пользователей;
- Малая база стандартных УЗ Postgres (пар логинов и паролей);
- Малая база стандартных УЗ SSH (пар логинов и паролей);
- Малая база стандартных УЗ FTP (пар логинов и паролей);
- Малая база стандартных УЗ Windows (пар логинов и паролей);
- Телефоны;
- Фаззинг.

Введите запрос для поиска						+ Добавить словарь
☐ Название словаря	Назначение словаря	Версия	Пользовательский	Размер		
☐ Средняя база стандартных паролей	Пароли	1.0.0	Нет	10460		
☐ Малая база стандартных паролей	Пароли	1.0.0	Нет	172		
☐ Средняя база имен пользователей ...	Логины	1.0.0	Нет	6346		
☐ Малая база стандартных имен поль...	Логины	1.0.0	Нет	114		
☐ Малая база стандартных Y3 Postgre...	Пароли пользователей	1.0.0	Нет	124		
☐ Малая база стандартных Y3 SSH (п...	Пароли пользователей	1.0.0	Нет	2001		
☐ Малая база стандартных Y3 FTP (п...	Пароли пользователей	1.0.0	Нет	955		
☐ Малая база стандартных Y3 Windo...	Пароли пользователей	1.0.0	Нет	433		
☐ Телефоны	Телефоны		Да	201		
☐ Словарь_новый Want.	Пароли пользователей		Да	12		
☐ Словарь 7358f00e-27b3-4f29-8dc9-f9...	Пароли пользователей		Да	12		
☐ Фаззинг	Фаззинг		Да	33		

Рисунок 144 – Окно «Словари»

Для добавления словаря нажать кнопку «Добавить словарь» и в открывшемся окне заполнить поля:

- ввести название;
- выбрать назначение словаря из предложенного списка (пароли, фаззинг, логины, e-mail адреса, телефоны, пароли пользователей, хэши, хэши пользователей);
- доступна возможность загрузки словаря из файла при помощи нажатия кнопки «Загрузить»;
- нажать кнопку «Добавить» для сохранения словаря (рис. 145).

× Добавить словарь

Название словаря	Название словаря
Назначение словаря	Назначение словаря ▼
Массовый импорт	Загрузить

Добавить	Отменить
---	---

Рисунок 145 – Окно «Добавить словарь»

6.1.2 Эксплойты

Эксплойты — это модули, которые предназначены для выполнения работы по эксплуатации уязвимостей в системах или приложениях. Эти модули отображаются в соответствующем разделе и не подлежат удалению.

Для просмотра интерфейса в окне «Библиотека» перейти на вкладку «Эксплойты» в левой области окна (рис. 146). С правой стороны окна отображается состав полей и вкладок:

- поле запроса для поиска. Позволяет искать по уязвимостям;
- список доступных эксплойтов. При нажатии на эксплойт доступен просмотр информации в карточке (рис. 147).

Тип	Введите запрос для поиска					
☐ Словари	CVE	ОС	Класс ПО	CVSSv3	Наименование ПО	Тип атаки
☒ Эксплойты	CVE-2011-2523	linux	Server Software	9.8 CRITICAL	vsftpd	RCE
☐ Инструментальные модули	CVE-2014-3120	linux	Server Software	8.1 HIGH	ElasticSearch	RCE
	CVE-2015-1427	linux	Server Software	9.8 CRITICAL	ElasticSearch	RCE
	CVE-2015-3306	linux	Server Software	10.0 CRITICAL	ProFTPD	RCE
	CVE-2015-3337	linux	Server Software	4.3 MEDIUM	ElasticSearch	Path Traversal
	CVE-2015-5531	linux	Server Software	5.0 MEDIUM	ElasticSearch	Path Traversal
	CVE-2017-12629	linux	Server Software	9.8 CRITICAL	Apache Solr	XXE
	CVE-2017-12635	linux	Server Software	9.8 CRITICAL	CouchDB	LPE
	CVE-2017-12636	linux	Server Software	7.2 HIGH	CouchDB	RCE
	CVE-2018-11409	linux	Server Software	5.3 MEDIUM	Splunk Enterprise	Information Disclosure
	CVE-2019-20933	linux	Server Software	9.8 CRITICAL	InfluxDB	Broken Authentication
	CVE-2019-7609	linux	Server Software	9.8 CRITICAL	Kibana	RCE
	CVE-2019-9193	linux	Server Software	7.2 HIGH	Postgres	RCE
	CVE-2020-1938	linux	Server Software	9.8 CRITICAL	Apache Tomcat	RCE
	CVE-2021-28164	linux	Server Software	5.3 MEDIUM	Jetty	Directory Traversal
	CVE-2021-41773	linux	Server Software	7.5 HIGH	Apache	Directory Traversal, RCE
	CVE-2021-42013	linux	Server Software	9.8 CRITICAL	Apache HTTP Server	Path Traversal + RCE
	CVE-2021-43798	linux	Server Software	7.5 HIGH	Grafana	Directory Traversal
Всего: 3						
Обновить библиотеку	Всего: 32					

Рисунок 146 – Список эксплойтов

× CVE-2014-3120

Модуль [Информация об уязвимости](#)

CVE ID	CVE-2014-3120
BDU ID	-
NCIRCC ID	-
Производитель	-
Дата публикации	28.07.2014 23:55
Дата последнего обновления	13.10.2025 21:36
Описание	The default configuration in Elasticsearch before 1.4.0.Beta1 enables dynamic scripting, which allows remote attackers to execute arbitrary MVEL expressions and Java code via the source parameter to _search. NOTE: this only violates the vendor's intended security policy if the user does not run Elasticsearch in its own independent virtual machine.
Оценка критичности	8.1 high
PoC	EXPLOIT_DB:33370 exploit/multi/elasticsearch/script_mvel_rce CVE-2014-3120 PACKETSTORM:127689 PACKETSTORM:128199 PACKETSTORM:128198 PACKETSTORM:128225 CVE-2014-3120

[Заккрыть](#)

Рисунок 147 – Информация об уязвимости

6.1.3 Инструментальные модули

Для просмотра информации в окне «Библиотека» перейти на вкладку «Инструментальные модули» в левой области окна (рис. 148). С правой стороны окна отображается состав полей и вкладок:

- поле запроса для поиска. Позволяет искать по описанию;
- список доступных инструментальных модулей.

Тип	Q. Введите запрос для поиска	Фильтр
Словари		
Эксплойты		
Инструментальные модули		

Описание	Название	Модуль
Поиск чувствительных данных по ключам в *.txt файлах Linux	btc-local-module-bash-cred...	Локальная разведка
Повышение привилегий через CVE-2025-32463	btc-local-module-bash-cve...	Повышение привилегий
Агрессивный поиск локальных файлов Linux	btc-local-module-bash-find...	Локальная разведка
Проверка прав на чтение в /etc/shadow	btc-local-module-bash-shad...	Локальная разведка
Повышение привилегий через sudo	btc-local-module-bash-sudo...	Повышение привилегий
Агрессивный поиск локальных файлов Windows	btc-local-module-posh-g-ch...	Локальная разведка
Установка агента через CVE-2011-2523	btc-module-cve-2011-2523...	Перемещение в сети
Установка агента через CVE-2019-9193	btc-module-cve-2019-9193...	Перемещение в сети
Установка агента через CVE-2022-24706	btc-module-cve-2022-24706...	Перемещение в сети
Поиск валидных учетных данных, методом перебора множества паролей и пользователе...	btc-module-hydra-u-p-ssh	Перебор УЗ
NXC (тихий режим) получение валидных имён пользователей FTP, и паролей в открытом ...	btc-module-nxc-ftp-u-p	Перебор УЗ
AS-Rep Roasting. Получение Kerberos AS-REP хэшей пользователей AD, с атрибутом DONT...	btc-module-nxc-ldap-u-p-asr...	Сканирование инфраструктуры
Получение списка хостов подсети, дополнительной информации о хостах	btc-module-nxc-smb-net	Сканирование инфраструктуры
Получение валидных имён пользователей, и паролей в открытом виде	btc-module-nxc-smb-u-p-bru...	Перебор УЗ
Получение учетных данных в открытом виде из Credential Manager, Chrome, Edge, Firefox.	btc-module-nxc-smb-u-p-dp...	Сканирование инфраструктуры
Выгрузить базу хэшей пользователей (NTDS.dit)	btc-module-nxc-smb-u-p-ntds	Сканирование инфраструктуры
Имитация шифрования файлов C:\CLOP_TARGET	btc-module-nxc-smb-u-p-put...	Удаление и шифрование
Установка агента Windows, загрузка с сервера метом PULL	btc-module-nxc-smb-u-p-put...	Перемещение в сети

Всего: 3

Рисунок 148 – Список инструментальных модулей

Примечание. В дальнейшем планируется интеграция с внешним сервисом, который будет предоставлять новые словари и эксплойты для использования в рамках комплекса при нажатии кнопки «Обновить библиотеку».

7 Администрирование

Раздел «Администрирование» обеспечивает администраторов необходимой информацией для эффективного управления ПК, что способствует её стабильной и безопасной работе.

7.1 Настройки

Для добавления настроек администрирования необходимо:

- 1) Перейти в разделе «Администрирование» в подраздел «Настройки» (рис. 149).

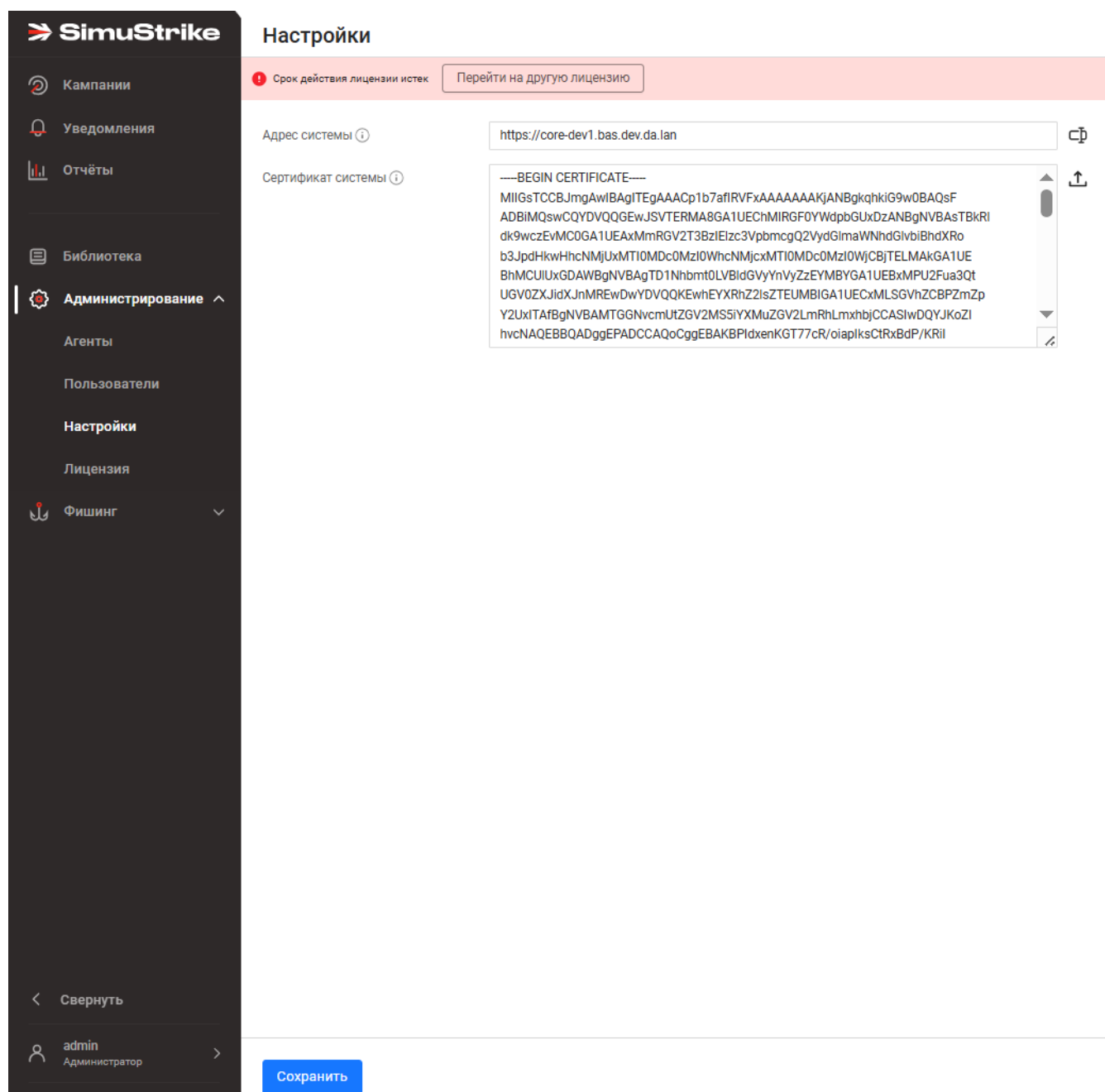


Рисунок 149 – Подраздел «Настройки»

- 2) Заполнить поле «Адрес системы» для этого указать адрес из адресной строки.

- 3) Заполнить поле «Сертификат системы» для этого ввести содержимое сертификата вручную или загрузите файл при помощи кнопки «Загрузить» (рис. 150).

SimuStrike Настройки

Срок действия лицензии истек [Перейти на другую лицензию](#)

Адрес системы [i](#)

Сертификат системы [i](#)

-----BEGIN CERTIFICATE-----
MIIGsTCCBJmgAwIBAgITEgAAACp1b7afIRVFxAAAAAAKJANBgkqhkiG9w0BAQsF
ADBIMQswCQYDVQQGEwJSVTERMA8GA1UEChMIRGF0YWdpbGUxLWZANBgNVBAsTBkRI
dk9wc2EvMCOGA1UEAxMmRGV2T3BzIElzc3VpbmcgQ2VydGhmaWNhdGlvbiBhdXR0
b3JpdHkwHhcNMjI0MDc0MzI0WhcNMjc0MTI0MDc0MzI0WjCBJTELMAkGA1UE
BhMCUlxGDAWBgNVBAgTD1NhbmtdLVBldGVyYnVyZzEYMBYGA1UEBxMPU2Fua3Qt
UGV0ZXJidXJnMREwDwYDVQQKEwhEYXRhZ2lsZTEUMBIGA1UECzMlSGVhZCBPZmZp
Y2UxIHRfBgNVBAMTGGNvcmUtZGV2MS5iYXMuZGV2LmRhLmxbjCCAsiwdQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAKBPIdxenKGT77cR/oiaplksCtRxBdP/KRil

[Загрузить](#)

[Сохранить](#)

Рисунок 150 – Поле «Адрес системы» и «Сертификат системы»

7.2 Лицензия

Для просмотра и обновления лицензии необходимо:

- 1) Перейти в разделе «Администрирование» в подраздел «Лицензия» (рис. 151).

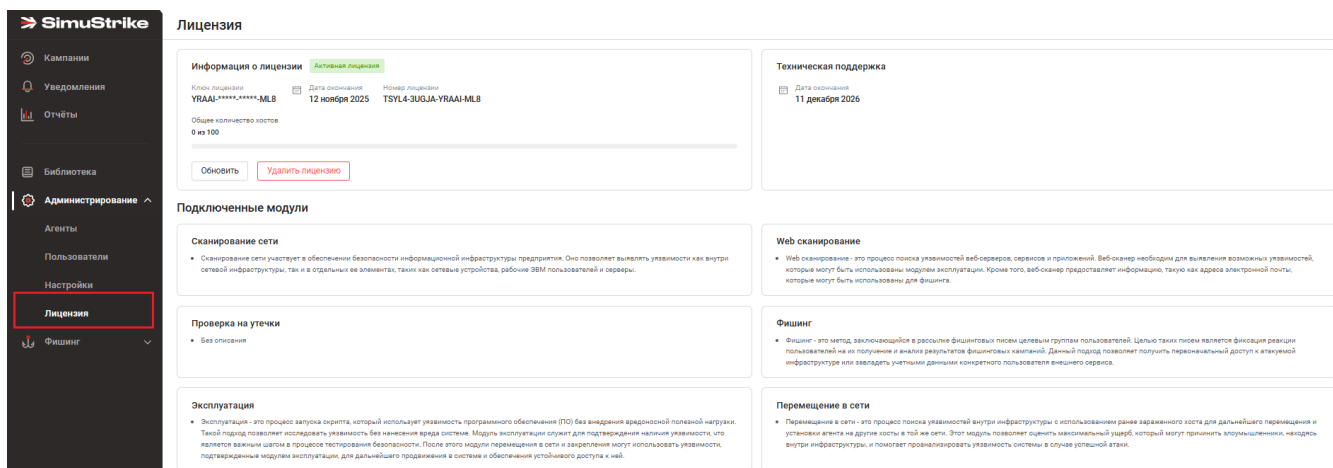


Рисунок 151 – Подраздел «Лицензия»

2) В окне «Лицензия» представлена информации о действии лицензии, технической поддержки и подключенных модулях (рис. 152).

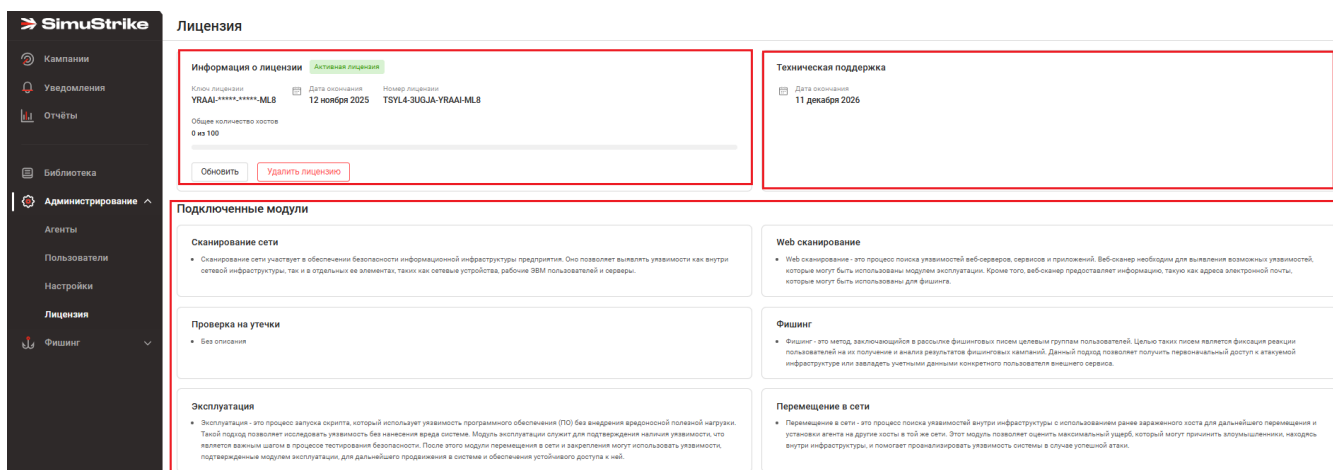


Рисунок 152 – Информация о лицензии

3) Для обновления лицензии необходимо нажать кнопку «Обновить», а для удаления нажать кнопку «Удалить» .

8 Уведомления

Для просмотра уведомлений необходимо:

- 1) В главном меню перейти в раздел «Уведомления». Уведомления делятся на две группы «Уведомления по кампаниям» и «Системные уведомления» (рис. 153).

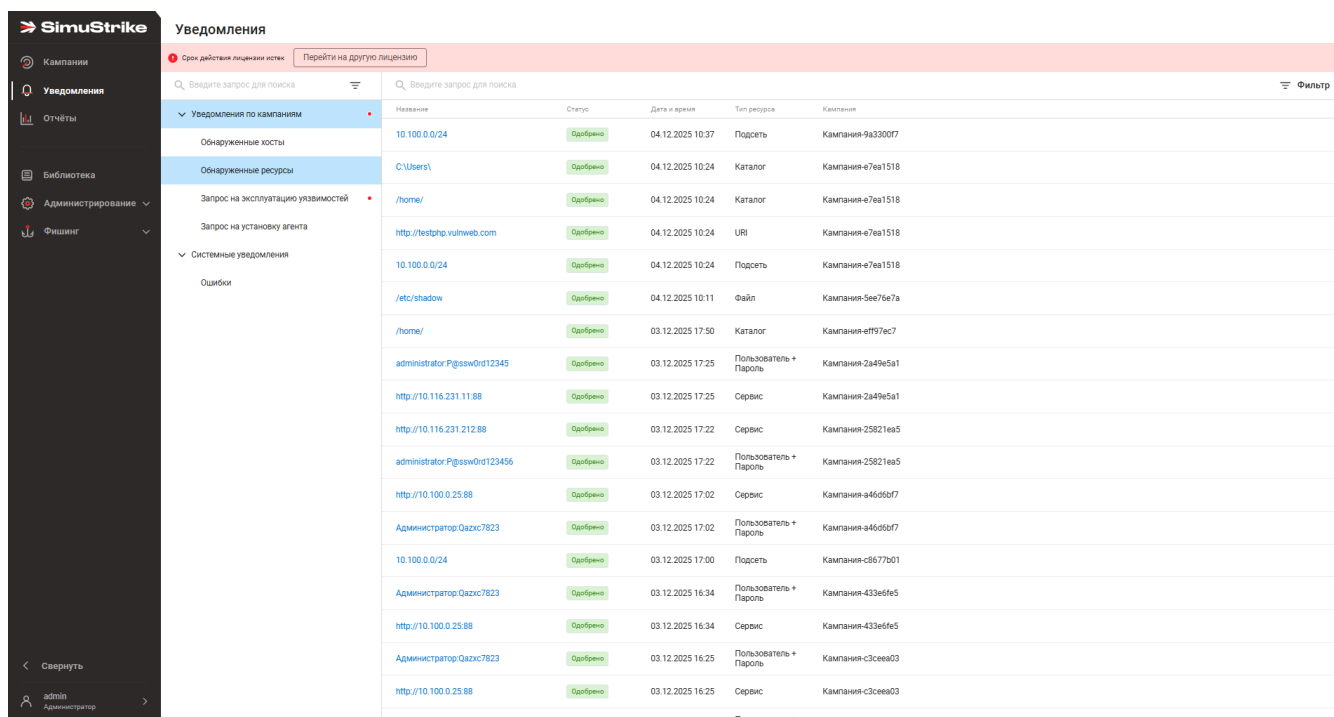


Рисунок 153 – Раздел «Уведомления»

- 2) Для просмотра уведомлений выбрать одну из групп:
 - «Уведомления по кампаниям»;
 - «Обнаруженные хосты»;
 - «Обнаруженные ресурсы»;
 - «Запрос на эксплуатацию уязвимостей»;
 - «Запрос на установку агента»;
 - «Системные уведомления»;
 - Ошибки.
- 3) Доступна возможность просмотра карточки уведомления при нажатии на его название (рис. 154).

- Кампания
- Уведомления**
- Отчеты
- Библиотека
- Администрирование
- Фишинг

Срок действия лицензии истекает

Перейти на другую лицензию

Введите запрос для поиска

Введите запрос для поиска

Уведомления по кампаниям

Обнаруженные хосты

Обнаруженные ресурсы

Запрос на эксплуатацию уязвимостей

Запрос на установку агента

Системные уведомления

Ошибки

10.100.0.0/24

C:\Users\

/home/

http://testphp.vulnweb.com

10.100.0.0/24

/etc/shadow

/home/

administrator:P@ssw0rd12345

http://10.116.231.11.88

http://10.116.231.212.88

administrator:P@ssw0rd123456

http://10.100.0.25.88

Администратор:Qazxc7823

10.100.0.0/24

Администратор:Qazxc7823

http://10.100.0.25.88

Администратор:Qazxc7823

http://10.100.0.25.88

Имя ресурса	Статус	Дата и время	Тип ресурса	Кампания
10.100.0.0/24	Одобрено	04.12.2025 10:37	Подсеть	Кампания-9a3300f7
C:\Users\	Одобрено	04.12.2025 10:24	Каталог	Кампания-e7ea1518
/home/	Одобрено	04.12.2025 10:24	Каталог	Кампания-e7ea1518
http://testphp.vulnweb.com	Одобрено	04.12.2025 10:24	URL	Кампания-e7ea1518
10.100.0.0/24	Одобрено	04.12.2025 10:24	Подсеть	Кампания-e7ea1518
/etc/shadow	Одобрено	04.12.2025 10:11	Файл	Кампания-5ee76e7a
/home/	Одобрено	03.12.2025 17:50	Каталог	Кампания-eff97ec7
administrator:P@ssw0rd12345	Одобрено	03.12.2025 17:25	Пользователь + Пароль	Кампания-2a49e5a1
http://10.116.231.11.88	Одобрено	03.12.2025 17:25	Сервис	Кампания-2a49e5a1
http://10.116.231.212.88	Одобрено	03.12.2025 17:22	Сервис	Кампания-25821ea5
administrator:P@ssw0rd123456	Одобрено	03.12.2025 17:22	Пользователь + Пароль	Кампания-25821ea5
http://10.100.0.25.88	Одобрено	03.12.2025 17:02	Сервис	Кампания-a46c5bf7
Администратор:Qazxc7823	Одобрено	03.12.2025 17:02	Пользователь + Пароль	Кампания-a46c5bf7
10.100.0.0/24	Одобрено	03.12.2025 17:00	Подсеть	Кампания-c8677b01
Администратор:Qazxc7823	Одобрено	03.12.2025 16:34	Пользователь + Пароль	Кампания-433e6fe5
http://10.100.0.25.88	Одобрено	03.12.2025 16:34	Сервис	Кампания-433e6fe5
Администратор:Qazxc7823	Одобрено	03.12.2025 16:25	Пользователь + Пароль	Кампания-с3ee603
http://10.100.0.25.88	Одобрено	03.12.2025 16:25	Сервис	Кампания-с3ee603

Рисунок 154 – Вызов карточки уведомлений

9 Отчеты

Для просмотра отчетов необходимо:

- 1) В главном меню перейти в раздел «Отчеты». (рис. 155).

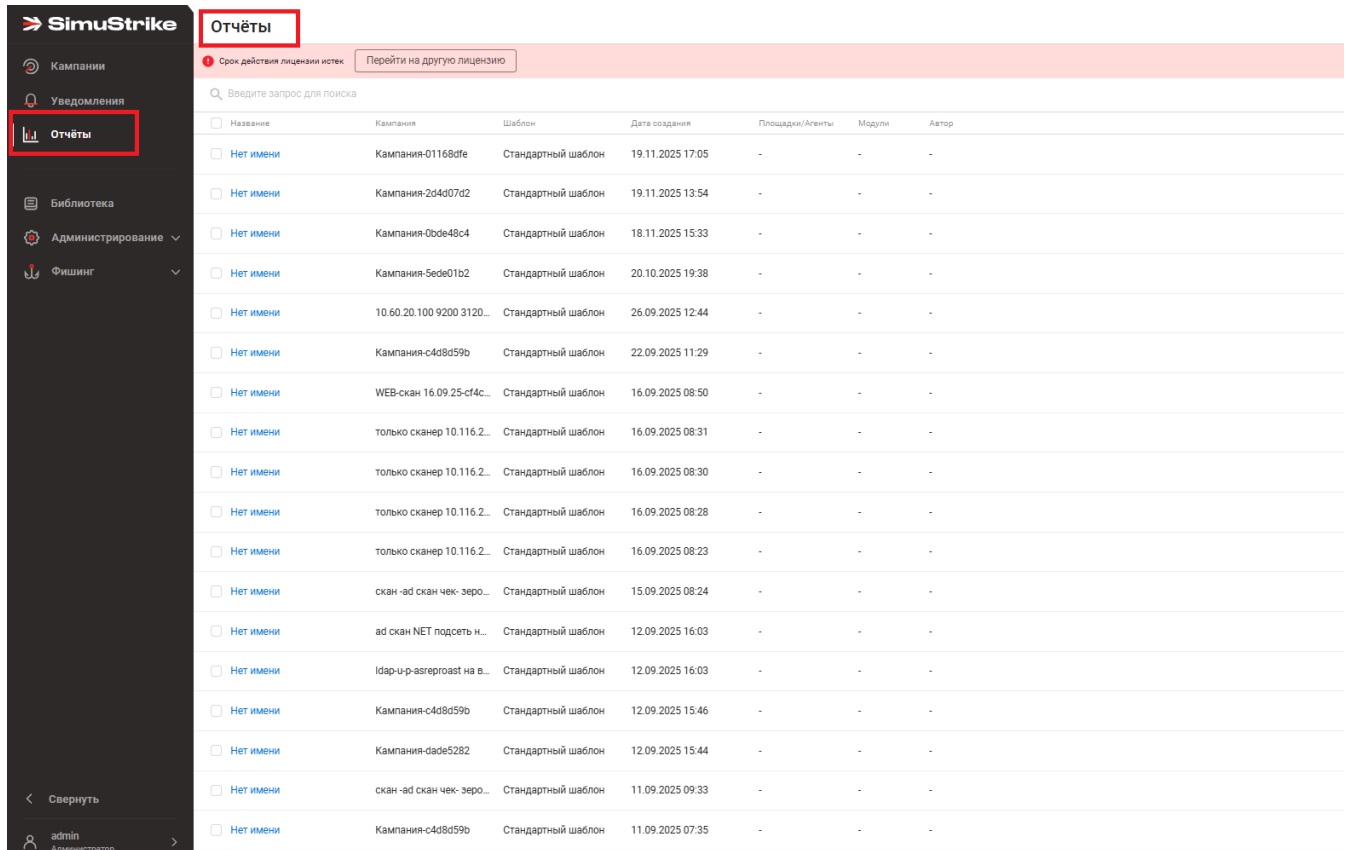


Рисунок 155 – Раздел «Отчеты»

- 2) Доступна возможность скачать или удалить отчет (рис. 156).

Отчёты

Срок действия лицензии истек

Перейти на другую лицензию

Введите запрос для поиска

Фильтр

☐	Название	Кампания	Шаблон	Дата создания	Площадки/Агенты	Модули	Автор	
☐	Нет имени	Кампания-01168dfe	Стандартный шаблон	19.11.2025 17:05	-	-	-	
☐	Нет имени	Кампания-2d4d07d2	Стандартный шаблон	19.11.2025 13:54	-	-	-	
☐	Нет имени	Кампания-0bde48c4	Стандартный шаблон	18.11.2025 15:33	-	-	-	
☐	Нет имени	Кампания-5ede01b2	Стандартный шаблон	20.10.2025 19:38	-	-	-	↓ ✕
☐	Нет имени	10.60.20.100 9200 3120...	Стандартный шаблон	26.09.2025 12:44	-	-	-	
☐	Нет имени	Кампания-c4d8d59b	Стандартный шаблон	22.09.2025 11:29	-	-	-	
☐	Нет имени	WEB-скан 16.09.25 cf4c...	Стандартный шаблон	16.09.2025 08:50	-	-	-	
☐	Нет имени	только сканер 10.116.2...	Стандартный шаблон	16.09.2025 08:31	-	-	-	
☐	Нет имени	только сканер 10.116.2...	Стандартный шаблон	16.09.2025 08:30	-	-	-	
☐	Нет имени	только сканер 10.116.2...	Стандартный шаблон	16.09.2025 08:28	-	-	-	
☐	Нет имени	только сканер 10.116.2...	Стандартный шаблон	16.09.2025 08:23	-	-	-	
☐	Нет имени	скан -ad скан чек-зеро...	Стандартный шаблон	15.09.2025 08:24	-	-	-	
☐	Нет имени	ad скан NET подсеть н...	Стандартный шаблон	12.09.2025 16:03	-	-	-	
☐	Нет имени	Idar-ч-р-asgerproast на в...	Стандартный шаблон	12.09.2025 16:03	-	-	-	
☐	Нет имени	Кампания-c4d8d59b	Стандартный шаблон	12.09.2025 15:46	-	-	-	
☐	Нет имени	Кампания-dade5282	Стандартный шаблон	12.09.2025 15:44	-	-	-	
☐	Нет имени	скан -ad скан чек-зеро...	Стандартный шаблон	11.09.2025 09:33	-	-	-	

Рисунок 156 – Кнопки «Скачать» и «Удалить»

3) Пример отчета в формате .html (рис. 157).

Кампания-2d4d07d2

Отчёт сформирован: 2025-11-19 13:54:27

Основная информация

Описание:

Владелец: Тест

Отчёт сформировал: Костенко

Период кампании: 0001-01-01 00:00:00 —

Период отчёта: 2025-11-18 20:28:20 — 2025-11-19 13:54:27

Модули

cred_brute_force

Статистика

4

1

1

1

1

Рисунок 157 – Отчет в браузере

Перечень терминов и определений

Кампании	– Представляют собой имитацию многоступенчатых хакерских атак. Их можно настраивать различными способами, включая сценарии, которые моделируют действия только внутренних нарушителей. В таких случаях достаточно активировать модули эксплуатации, перемещения в сети и закрепления, в то время как разведка может не потребоваться.
Фишинг	– Метод, заключающийся в рассылке фишинговых писем целевым группам пользователей. Целью таких писем является фиксация реакции пользователей на их получение и анализ результатов фишинговых кампаний. Данный подход позволяет получить первоначальный доступ к атакуемой инфраструктуре или завладеть учётными данными конкретного пользователя внешнего сервиса. Модуль фишинга включает в себя функции для создания целевых страниц, которые имитируют легитимные веб-ресурсы, что увеличивает вероятность успешного обмана пользователей.
Площадка	– Часть поверхности атаки, доступная основному агенту (резиденту). Например, если резидент установлен удалённо от инфраструктуры, он может начать атаку с внешнего веб-сервера. В случае, когда резидент установлен внутри инфраструктуры, он имитирует внутреннего нарушителя. Резидент обладает всеми необходимыми инструментами для проведения атак.
Резидент	– Ключевой компонент, необходимый для пользования ПК. Для корректного функционирования системы требуется наличие как минимум одного резидента.
Агентская система	– Предназначена для распространения функциональных возможностей программы по всей сети, включая подсети, DMZ и изолированные VLAN, при наличии как минимум одной сетевой связи с сегментом сети, в котором уже присутствует агент.
Тонкий агент	– Используются для закрепления и распространения в инфраструктуре: «не содержат большого количества инструментов, но способны выполнять скрипты и при необходимости загружать дополнительные инструменты». Это позволяет им быть гибкими и адаптивными в процессе атаки, обеспечивая возможность быстрого реагирования на изменяющиеся условия.
Толстый агент	– Необходим для выполнения ряда ключевых задач в системе BAS. Он содержит все необходимые инструменты и функции для проведения проверок, сканирования и анализа, что позволяет эффективно выявлять уязвимости и угрозы. Кроме того, толстый агент способен запускать скрипты (POC) и инструменты для анализа защищенности, что позволяет тестировать новые идеи и решения в реальных условиях. Толстый агент также может обрабатывать и анализировать большие объёмы данных, что способствует более глубокому пониманию состояния безопасности системы. Он способен функционировать независимо, что позволяет ему выполнять задачи даже в условиях ограниченной сетевой связи. Наконец, толстый агент может

взаимодействовать с другими компонентами BAS и системами безопасности, обеспечивая комплексный подход к защите информации. Таким образом, толстый агент играет ключевую роль в обеспечении безопасности и эффективности работы системы.

- | | |
|----------------------------------|--|
| Web-сканирование | – Процесс поиска уязвимостей веб-серверов, сервисов и приложений. Веб-сканер необходим для выявления возможных уязвимостей, которые могут быть использованы модулем эксплуатации. Кроме того, веб-сканер предоставляет информацию, такую как адреса электронной почты, которые могут быть использованы для фишинга. |
| Эксплуатация | – Процесс запуска скрипта, который использует уязвимость программного обеспечения (ПО) без внедрения вредоносной полезной нагрузки. Такой подход позволяет исследовать уязвимость без нанесения вреда системе. Модуль эксплуатации служит для подтверждения наличия уязвимости, что является важным шагом в процессе тестирования безопасности. После этого модули перемещения в сети и закрепления могут использовать уязвимости, подтвержденные модулем эксплуатации, для дальнейшего продвижения в системе и обеспечения устойчивого доступа к ней. |
| Перемещение в сети и закрепление | – Процесс поиска уязвимостей внутри инфраструктуры с использованием ранее заражённого хоста для дальнейшего перемещения и установки агента на другие хосты в той же сети. Этот модуль позволяет оценить максимальный ущерб, который могут причинить злоумышленники, находясь внутри инфраструктуры, и помогает понять, насколько уязвима система в случае успешной атаки. |
| Брутфорс | – Метод, заключающийся в переборе паролей, пользователей или извлечении паролей в открытом виде из хешей. Этот подход часто используется для получения первоначального доступа к серверам, сетевому оборудованию и рабочим станциям пользователей. Брутфорс может быть эффективным, особенно в случаях, когда пароли являются слабыми или предсказуемыми. |
| Шаблон письма | – Текст, который соответствует содержанию целевой страницы и побуждает получателя перейти по ссылке. Шаблон письма необходим для имитации конкретного сервиса, которым пользуется целевая группа получателей. |
| Мониторинг | – Необходим для сбора и анализа общей информации о всех попытках мошенничества, что позволяет выявлять тенденции, оценивать уровень угроз и разрабатывать эффективные меры защиты. Регулярный мониторинг помогает организациям своевременно реагировать на инциденты и минимизировать потенциальные риски. |
| Профиль отправителя | – Позволяет обеспечить надёжность и безопасность коммуникации, а также повысить доверие получателей к отправляемым сообщениям. Правильная настройка профиля включает указание имени отправителя, адреса электронной почты и других параметров, что помогает избежать попадания писем в спам и улучшает их доставляемость. |
| Целевая страница | – Копия веб-ресурса, которая может имитировать корпоративный сайт, сайт финансового учреждения или любой другой сервис. URL, указанный в письме, ведёт на заранее подготовленную целевую |

страницу. Такая страница подбирается с учётом адресной рассылки, что позволяет повысить вероятность того, что получатели доверятся сообщению и перейдут по ссылке.

- | | |
|-----------------------------|--|
| Библиотека | – Специальное место, куда попадают различные ресурсы из инфраструктурных эксплуатационных сервисов. Она служит точкой входа и просмотра, позволяя пользователям взаимодействовать с элементами, которые могут быть как локальными, так и централизованными. |
| XSS (Cross-Site Scripting) | – Уязвимость веб-приложений, позволяющая злоумышленникам внедрять вредоносные скрипты на страницы, которые просматривают пользователи. Это может привести к кражам данных, таким как куки и токены сессий, а также к другим атакам на пользователей и системы. |
| RCE (Remote Code Execution) | – Тип уязвимости, позволяющий злоумышленнику выполнять произвольный код на удаленной системе. При наличии такой уязвимости атакующий может получить доступ к системе, управлять ею и выполнять команды, что может привести к серьезным последствиям, таким как утечка данных, повреждение файлов или полный контроль над системой. |
| Эксплойты | – Модули, которые предназначены для выполнения работы по эксплуатации уязвимостей в системах или приложениях. Эти модули отображаются в соответствующем разделе и не подлежат удалению. |

Перечень сокращений

AD	–	Active Directory
API	–	Application Programming Interface
CVE	–	Common Vulnerabilities and Exposures
HTTP	–	HyperText Transfer Protocol
HTTPS	–	HyperText Transfer Protocol Secure
IP	–	Internet Protocol
LDAP	–	Lightweight Directory Access Protocol
MAC	–	Media Access Control
NA	–	Network Address
SNMP	–	Simple Network Management Protocol
SQL	–	Structured Query Language
SSH	–	Secure Shell
TI	–	Threat Intellegence
TTP	–	Tactics Technics Protocols
TLS	–	Transport Layer Security
БД	–	База данных
БДУ	–	База данных уязвимостей
ИБ	–	Информационная безопасность
КО	–	Клиентское оборудование
МЭ	–	Межсетевой экран
ОС	–	Операционная система
ПК	–	Программный комплекс
ПО	–	Программное обеспечение
ПТС	–	Программно-технические средства
СрЗИ	–	Средства защиты информации
СЗИ	–	Система защиты информации
ТУ	–	Технические условия
ИБ	–	Информационная безопасность