

Программный  
«SimuStrike»

комплекс

Описание применения

## Аннотация

Настоящий документ содержит описание применения программного комплекса «SimuStrike» (далее – ПК, комплекс).

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.

## Содержание

1	Назначение ПК.....	4
1.1	Назначение ПК «SimuStrike» .....	4
1.2	Структура и компоненты ПК «SimuStrike» .....	4
1.3	Функциональные возможности ПК .....	5
1.4	Лицензии ПК «SimuStrike» .....	13
1.5	Роли пользователей .....	14
2	Условия применения ПК .....	16
2.1.1	Организация администрирования комплекса .....	16
2.1.2	Требования к составу и параметрам технических средств ПК.....	16
2.2	Требования к сетевым портам ПК «Simustrike» .....	17
2.3	Требования к браузерам.....	17
3	Задачи ПК.....	18
4	Входные и выходные данные .....	19
4.1	Входные данные.....	19
4.2	Выходные данные .....	19
	Перечень терминов и определений.....	21
	Перечень сокращений .....	24

# 1 Назначение ПК

## 1.1 Назначение ПК «SimuStrike»

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».

## 1.2 Структура и компоненты ПК «SimuStrike»

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).

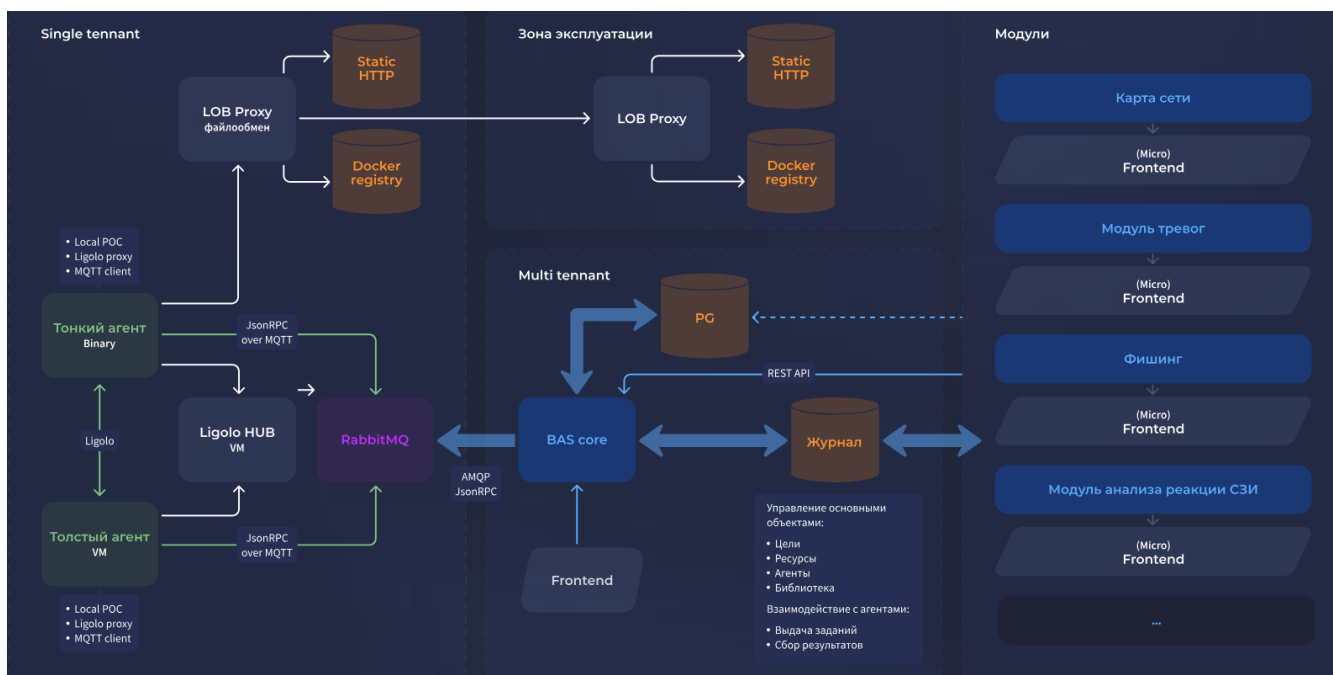


Рисунок 1 – Схема основных компонентов ПК «SimuStrike»

Компоненты, необходимые для работы ПК «Simustrike»:

- 1) Операционная система и необходимые пакеты

- Операционная система: Linux RED OS 7.3 или новее.

Необходимые пакеты:

- docker – платформа контейнеризации;
- docker-compose – оркестрация многоконтейнерных приложений Docker;
- openssl – криптографический инструментарий и библиотеки TLS;
- openresty – веб-платформа на основе Nginx с расширенными возможностями;
- easysrsa – утилита для управления инфраструктурой открытых ключей (PKI);
- postgresql – система управления реляционными базами данных.

## 2) Основные сервисы и компоненты

Системы обмена сообщениями и потоковой обработки данных:

- Kafka – распределённая платформа потоковой обработки данных и передачи сообщений;
- RabbitMQ – брокер сообщений.

Реестр контейнеров:

- Docker Registry – приватный реестр для хранения образов Docker.

Базы данных:

- PostgreSQL – основная реляционная СУБД;
- MongoDB 5 – документоориентированная NoSQL база данных.

## 1.3 Функциональные возможности ПК

ПК реализует следующие функциональные возможности:

- сбор данных об информационных ресурсах сетевой ИТ-инфраструктуры организации;
- выявление информации о возможных уязвимостях и векторах возможных атак;
- проверка срабатывания средств защиты информации (СрЗИ) ИТ-инфраструктуры организации на генерируемые инциденты;
- проверка времени отклика СрЗИ объекта оценки на генерируемые инциденты;
- формирование отчетов и рекомендаций по результатам выполненных проверок.

Программная структура комплекса включает программные модули, представленные в таблице 1.

Таблица 1 – Описание модулей и их функциональных возможностей

Название	Описание	Функциональные возможности
Модуль Фишинга	Метод, заключающийся в рассылке фишинговых писем целевым группам пользователей. Цель — фиксация реакции пользователей и анализ результатов фишинговых кампаний. Данный подход	<ul style="list-style-type: none"> <li>• Создание и настройка фишинговых кампаний.</li> <li>• Просмотр и редактирование параметров заданий.</li> </ul>

Название	Описание	Функциональные возможности
	позволяет получить первоначальный доступ к инфраструктуре или завладеть учётными данными. Модуль включает функции создания целевых страниц, имитирующих легитимные веб-ресурсы.	<ul style="list-style-type: none"> <li>• Управление статусом заданий.</li> <li>• Организация повторной отправки недоставленных писем.</li> <li>• Запуск атак в ручном и автоматическом режимах.</li> <li>• Настройка IMAP-профиля для мониторинга ответов.</li> <li>• Конфигурация SMTP-профиля для ретрансляции.</li> <li>• Визуализация результатов кампаний на дашборде.</li> <li>• Анализ эффективности по метрикам: доставка, открытия, переходы, ввод данных.</li> <li>• Мониторинг выполнения заданий в реальном времени.</li> </ul>
Модуль сканирования сети	Модуль для обеспечения безопасности информационной инфраструктуры предприятия. Позволяет выявлять уязвимости во внутрисетевой инфраструктуре, сетевых устройствах, рабочих станциях и серверах.	<ul style="list-style-type: none"> <li>• Создание заданий для сканирования сетевой инфраструктуры.</li> <li>• Просмотр и редактирование параметров заданий.</li> <li>• Управление статусом заданий.</li> <li>• Запуск и остановка процессов сканирования.</li> <li>• Выявление уязвимостей в сетевой инфраструктуре.</li> <li>• Обследование устройств, рабочих станций и серверов.</li> <li>• Анализ защищенности внутренней сетевой среды.</li> <li>• Формирование и экспорт результатов сканирования.</li> </ul>

Название	Описание	Функциональные возможности
		<ul style="list-style-type: none"> <li>• Обеспечение безопасности через регулярное обследование.</li> </ul>
Модуль веб-сканирования	Процесс поиска уязвимостей веб-серверов, сервисов и приложений. Необходим для выявления уязвимостей для последующей эксплуатации, а также сбора информации (например, email-адресов для фишинга).	<ul style="list-style-type: none"> <li>• Поиск уязвимостей веб-серверов, сервисов и приложений.</li> <li>• Создание и настройка заданий для сканирования веб-ресурсов.</li> <li>• Клонирование и редактирование существующих заданий.</li> <li>• Управление жизненным циклом заданий.</li> <li>• Поиск и фильтрация созданных заданий.</li> <li>• Выявление уязвимостей для эксплуатации.</li> <li>• Сбор дополнительной информации (например, email-адресов).</li> <li>• Формирование отчетов и выгрузка результатов.</li> </ul>
Модуль сканирования инфраструктуры	Инструмент для комплексной проверки безопасности Active Directory (AD). Выполняет аудит конфигураций, обнаружение хостов и учетных данных, поиск хеш-сумм и паролей, а также выявление уязвимостей в доменной среде.	<ul style="list-style-type: none"> <li>• Проверка безопасности AD.</li> <li>• Выявление ошибочных конфигураций (misconfigurations).</li> <li>• Поиск и анализ учетных данных пользователей.</li> <li>• Обнаружение хостов домена.</li> <li>• Сбор хеш-сумм и паролей.</li> <li>• Поиск уязвимостей в инфраструктуре AD.</li> <li>• Комплексный анализ защищенности AD.</li> <li>• Идентификация слабых мест в настройках доменной среды.</li> <li>• Обнаружение потенциальных векторов атаки.</li> </ul>

Название	Описание	Функциональные возможности
Модуль первоначального доступа	Процесс запуска скрипта, использующего уязвимость ПО без внедрения вредоносной нагрузки. Позволяет исследовать уязвимость без нанесения вреда и подтвердить её наличие для дальнейшего тестирования безопасности.	<ul style="list-style-type: none"> <li>• Эксплуатация уязвимостей ПО без внедрения вредоносной нагрузки.</li> <li>• Подтверждение наличия уязвимостей.</li> <li>• Автоматический подбор эксплойтов на основе данных о версиях ПО.</li> <li>• Поддержка сценариев внутреннего и внешнего нарушителя.</li> <li>• Создание заданий с настройкой списков хостов и режима работы.</li> <li>• Управление уведомлениями о возможности запуска.</li> <li>• Запуск и остановка заданий.</li> <li>• Разграничение прав доступа.</li> <li>• Автоматическое построение и выгрузка отчётов.</li> <li>• Визуализация результатов эксплуатации.</li> </ul>
Модуль перемещения в сети	Процесс поиска уязвимостей внутри инфраструктуры с использованием ранее заражённого хоста для дальнейшего перемещения и установки агента на другие хосты в сети. Позволяет оценить максимальный потенциальный ущерб от внутреннего нарушителя.	<ul style="list-style-type: none"> <li>• Поиск уязвимостей внутри инфраструктуры с заражённого хоста.</li> <li>• Перемещение между хостами через эксплуатацию уязвимостей.</li> <li>• Установка агента на уязвимые хосты.</li> <li>• Оценка потенциального ущерба.</li> <li>• Поддержка разных режимов работы.</li> <li>• Визуализация хостов с агентами на карте сети.</li> <li>• Логирование всех действий перемещения.</li> </ul>

Название	Описание	Функциональные возможности
		<ul style="list-style-type: none"> <li>• Автоматический переход к фазе поиска и эксфильтрации данных.</li> <li>• Разграничение прав доступа.</li> <li>• Управление заданиями.</li> </ul>
Модуль эксфильтрации данных	Обнаружение конфиденциальной информации внутри инфраструктуры компании и её отправка во внешнее хранилище в зашифрованном виде.	<ul style="list-style-type: none"> <li>• Обнаружение конфиденциальной информации во всей инфраструктуре.</li> <li>• Поиск чувствительных данных на всех доступных носителях.</li> <li>• Выявление архивов, репозиториев, БД, резервных копий и документов.</li> <li>• Настройка типов и расширений файлов для поиска.</li> <li>• Шифрование данных перед эксфильтрацией.</li> <li>• Создание и клонирование заданий поиска и выгрузки.</li> <li>• Настройка параметров заданий (типы файлов, хранилище, расписание).</li> <li>• Запуск заданий в ручном режиме или по расписанию.</li> <li>• Управление статусом заданий.</li> <li>• Автоматическое построение и выгрузка отчётов.</li> <li>• Визуализация результатов (найденные файлы, репозитории, адреса).</li> </ul>
Модуль удаления и шифрования данных	Проверка доступов к разделам и прав перезаписи файлов на указанных хостах. При наличии прав фиксируется событие о возможности шифрования хоста.	<ul style="list-style-type: none"> <li>• Проверка прав доступа к разделам и права перезаписи файлов.</li> <li>• Фиксация события о</li> </ul>

Название	Описание	Функциональные возможности
	Имитирует шифрование различных типов данных.	возможности шифрования хостов. <ul style="list-style-type: none"> <li>• Имитация шифрования различных типов данных (архивы, БД, документы).</li> <li>• Создание заданий с выбором типов файлов для шифрования.</li> <li>• Настройка белых и черных списков активов.</li> <li>• Просмотр и редактирование параметров заданий.</li> <li>• Управление статусом заданий.</li> <li>• Запуск заданий в ручном или отложенном режиме.</li> <li>• Построение и выгрузка отчётов.</li> <li>• Фиксация результатов шифрования.</li> <li>• Разграничение прав доступа.</li> </ul>
Модуль перебора хешей	Метод перебора паролей, пользователей или извлечения паролей из хеш-сумм. Используется для получения первоначального доступа к серверам, оборудованию и рабочим станциям.	<ul style="list-style-type: none"> <li>• Автоматическое построение отчёта по результатам каждой итерации задания.</li> <li>• Отображение метаданных задания (название, автор, дата создания и запуска, статус).</li> <li>• Представление результатов выполнения: подобранные пароли, хеши с неудачными попытками.</li> <li>• Просмотр и выгрузка отчёта.</li> </ul>
Модуль локальной разведки	Функциональный компонент тонкого агента, выполняющий сканирование внутреннего состояния хоста.	<ul style="list-style-type: none"> <li>• Анализ ОС, прав доступа и привилегий.</li> <li>• Поиск чувствительных данных в файлах Linux и Windows.</li> </ul>

Название	Описание	Функциональные возможности
		<ul style="list-style-type: none"> <li>• Проверка прав доступа к системным файлам (/etc/shadow).</li> <li>• Инвентаризация установленного ПО и служб.</li> <li>• Сбор учетных данных и хешей паролей.</li> <li>• Обнаружение систем защиты и антивирусов.</li> <li>• Поиск векторов для эскалации привилегий.</li> <li>• Анализ автозагрузки и механизмов постоянства.</li> <li>• Выявление уязвимых конфигураций и служб.</li> <li>• Поиск возможностей для перемещения в сети.</li> </ul>
Модуль перебора УЗ	Компонент для автоматизированного обнаружения рабочих пар (логин/пароль) к внутренним сервисам методом комбинированного перебора и пассивного анализа.	<ul style="list-style-type: none"> <li>• Активный брутфорс учетных данных по SSH.</li> <li>• Пассивный сбор валидных логинов и паролей FTP через NXC.</li> <li>• Тихий сбор учетных данных SSH в режиме NXC.</li> <li>• Обнаружение паролей в открытом виде при FTP/SSH-аутентификации.</li> <li>• Анализ чистого текста в сетевых протоколах.</li> <li>• Поиск учетных данных в конфигурационных файлах.</li> <li>• Регулировка скорости перебора.</li> <li>• Приоритизация целей по критичности.</li> <li>• Комбинирование активных и пассивных методов.</li> <li>• Формирование базы валидных учетных записей.</li> </ul>

Название	Описание	Функциональные возможности
		<ul style="list-style-type: none"> <li>• Обеспечение скрытности операций.</li> <li>• Подготовка данных для горизонтального перемещения.</li> </ul>
Модуль закрепления	Обеспечение автоматического запуска агента после перезагрузки системы или ключевых служб для поддержания постоянного присутствия в инфраструктуре.	<ul style="list-style-type: none"> <li>• Создание автозагрузочных записей в реестре Windows.</li> <li>• Настройка заданий в планировщике задач Windows.</li> <li>• Регистрация в папке автозагрузки пользователя.</li> <li>• Установка в качестве системной службы (Windows/Linux).</li> <li>• Настройка планировщика заданий в Linux.</li> <li>• Создание файлов сервисов для systemd.</li> <li>• Добавление в автозагрузку через системные скрипты.</li> <li>• Изменение профилей оболочки.</li> <li>• Реализация множественных механизмов.</li> <li>• Обеспечение скрытности записей.</li> <li>• Автоматическое восстановление при сбое.</li> <li>• Адаптация под текущий уровень привилегий.</li> <li>• Кросс-платформенная поддержка.</li> <li>• Обход стандартных методов обнаружения.</li> </ul>
Модуль повышения привилегий	Функциональный компонент локального агента для эскалации прав доступа с пользовательского уровня до администраторского (root/sudo/system) на целевом хосте.	<ul style="list-style-type: none"> <li>• Повышение привилегий через эксплуатацию уязвимостей.</li> <li>• Обход механизмов sudo.</li> <li>• Поиск и использование</li> </ul>

Название	Описание	Функциональные возможности
		уязвимостей ядра ОС. • Использование слабых разрешений файловой системы. • Эксплуатация уязвимостей в планировщике заданий ОС. • Обход механизмов защиты. • Автоматический подбор и проверка эксплойтов. • Подтверждение полученных привилегий администратора. • Кросс-платформенная поддержка.

Структура комплекса включает следующие основные подсистемы:

- 1) Подсистема хранения данных СУБД. Обеспечивает хранение служебных данных ПК, а также состояния модулей и ядра системы (задания, агенты, библиотека и т.д.) в соответствующей базе данных.
- 2) Подсистема авторизации и аутентификации. Обеспечивает аутентификацию и авторизацию пользователей, контроль и разграничение прав доступа пользователей к функциям ПК.
- 3) Интеграционная подсистема. Обеспечивает возможности лицензирования, обновления, доставки необходимых данных для работы ПК.
- 4) Клиентское веб-приложение. Обеспечивает веб-интерфейс пользователя для управления и запуска атак.

---

**Примечание.** По результатам атак в веб-интерфейсе отображаются успешность, затрагиваемые и зараженные узлы, а также оценка. По результатам проведения атак формируется отчет, содержащий информацию об используемых эксплойтах, адресах узлов и эксплуатируемое ПО, в котором были выявлены уязвимости.

---

## 1.4 Лицензии ПК «SimuStrike»

Лицензия на программный комплекс является срочной, она имеет определенный срок действия. В течение этого срока продукт может функционировать в полном объеме. При истечении срока лицензии или до его начала программный комплекс будет недоступен для использования.

В рамках лицензии предусмотрены различные уровни технической поддержки, которые включают:

- гарантийная поддержка. Обеспечивает пользователю услуги поддержки в течение установленного гарантийного периода;
- расширенная поддержка. Включает дополнительные услуги, такие как приоритетный доступ к технической поддержке.

Лицензия имеет ограничение на количество хостов и организаций, на которых может быть установлен и использован ПК.

---

**Примечание.** Комплект ПК будет поставляться с полным набором модулей. Однако использование некоторых модулей возможно только при наличии действующей лицензии на конкретные модули. При необходимости есть возможность активировать дополнительные модули. Без активной лицензии доступ к функциональности модулей будет ограничен. Подробная информация о лицензии приведена в описании документа «Руководство администратора».

---

## 1.5 Роли пользователей

При первоначальном доступе к интерфейсу ПК, выполняется аутентификация пользователей. В комплексе реализована ролевая модель доступа. Для разграничения доступа пользователей к функциональным возможностям в ПК «SimuStrike» предусмотрены следующие роли:

- Владелец;
- Администратор;
- Пользователь;
- Аудитор.

Каждой роли соответствует определенный набор прав и привилегий. Права доступа задаются при создании нового пользователя и по необходимости могут быть изменены пользователем с соответствующими привилегиями.

Владелец комплекса обладает полными правами и не имеет ограничений в доступе к функционалу и данным.

Администратор комплекса обладает правами на управление комплексом. Это позволяет ему эффективно управлять, обеспечивать безопасность и поддерживать работоспособность.

Пользователь комплекса имеет возможность создавать собственные кампании, что позволяет ему настраивать и управлять процессами в соответствии с его потребностями и целями. Эта функциональность предоставляет пользователю гибкость и контроль над выполнением задач, а также возможность адаптации кампаний под конкретные сценарии.

Аудитор в комплекса имеет ограниченные права доступа, которые позволяют ему только просматривать результаты выполнения задач, но не вносить изменения или

управлять процессами. Это ограничение обеспечивает высокий уровень безопасности и целостности данных, а также предотвращает несанкционированные действия, которые могут повлиять на работу ПК.

Матрица доступа к компонентам ПК «SimuStrike» представлена в таблице 2.

Таблица 2 – Матрица доступа к компонентам ПК

Функции	Пользователь с доступом к кампании (создатель)	Пользователь	Аудитор	Администратор	Владелец
Создание подзадания, задания и кампании	+	+	-	-	+
Просмотр подзадания, задания и кампании	+	-	+	-	+
Изменение подзадания, задания и кампании	+	-	-	-	+
Деактивация подзадания и задания	+	-	-	-	+
Удаление кампании	-	-	-	-	+
Доступ к уведомлениям кампании	+	-	-	-	+
Управление комплексом	-	-	-	+	+

Создатель – это пользователь создавший свою кампанию. Он имеет все права на изменения своей кампании и просмотра чужих.

Создание заданий – это процесс, в основе которого лежит анализ настроек кампании, найденных в рамках кампании объектов (ресурсов), а также в зависимости от расписания планировщика, который учитывает настройки запуска модулей в рамках кампании.

## 2 Условия применения ПК

Для эксплуатации и эффективного применения ПК «SimuStrike» необходимо использование на ЭВМ лицензионного системного программного обеспечения.

### 2.1.1 Организация администрирования комплекса

Администрирование комплекса осуществляет владелец и администратор ПК «SimuStrike».

При первоначальном доступе к веб-интерфейсу комплекса выполняется аутентификация пользователя.

Интерфейс сервера управления состоит из следующих разделов:

- Кампания – раздел для создания новой кампании и результат проведенных проверочных мероприятий по тестированию инфраструктуры;
- Уведомления – информационные сообщения от ПК (ошибки программного решения, информационные сообщения кампании и другие уведомления);
- Отчеты – формирование отчетов по проведенным мероприятиям компании;
- Администрирование – раздел, где выполняется настройка компонентов для правильного функционирования ПК;
- Библиотека – раздел предназначен для возможности просмотра и добавления новых ресурсов, которые способствуют эффективной работе модулей.

Установка и настройка сервера управления выполняется согласно документу «Программный комплекс ПК «SimuStrike». Руководство по установке и удалению комплекса».

После установки сервера управления необходимо активировать лицензию согласно документу «Программный комплекс ПК «SimuStrike».

### 2.1.2 Требования к составу и параметрам технических средств ПК

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.

## **2.2 Требования к сетевым портам ПК «Simustrike»**

- 1) Платформа
  - Подключение к внешней СУБД PostgreSQL – 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.

## **2.3 Требования к браузерам**

Единый интерактивный веб-интерфейс обеспечивает доступ пользователей к функциональности ПК «SimuStrike» с использованием следующих минимальных версий браузера:

- веб-браузер Chrome (версий 89 и выше);
- Яндекс Браузер (версии 21 и выше).

### 3 Задачи ПК

ПК «SimuStrike» расширяет классическое представление о системах симуляции атак, предлагая инструменты для оценки уязвимости инфраструктуры и систему сбора обратной связи от систем защиты, что обеспечивает непрерывную поддержку для инженеров ИБ и операторов SOC.

ПК решает следующие задачи в области информационной безопасности (ИБ):

- 1) Оценка уязвимостей. Программный комплекс помогает IT-специалистам и администраторам выявлять уязвимости и слабые места в сетевой инфраструктуре, что позволяет своевременно принимать меры по их устранению.
- 2) Проведение атак. Программный комплекс предоставляет обширный набор инструментов для симуляции различных типов атак, что позволяет пользователям оценивать уровень безопасности своей системы.
- 3) Анализ эффективности. Программный комплекс позволяет анализировать эффективность проведенных атак в реальном времени, что помогает в выявлении недостатков в защите и в планировании дальнейших действий.
- 4) Тестирование защитных мер. Программный комплекс дает возможность эффективно тестировать существующие защитные меры и планы реагирования на кибератаки, обеспечивая уверенность в их работоспособности и эффективности.
- 5) Улучшение реагирования на инциденты. Программный комплекс способствует улучшению процессов реагирования на кибератаки, позволяя организациям адаптировать свои стратегии безопасности на основе полученных данных и результатов тестирования.

Эти задачи помогают организациям повысить уровень безопасности своей сетевой инфраструктуры и подготовленность к потенциальным киберугрозам.

## 4 Входные и выходные данные

### 4.1 Входные данные

Входными данными для ПК являются:

- значения управляющих параметров, задаваемых администратором ПК;
- сформированные задания в кампании;
- базы данных которые формируют на основании найденных или из произвольного списка электронных адресов и номеров телефонов в базах утечек НКЦКИ [(<https://chk.safe-surf.ru/>)] или других подключаемых по API;
- данные, собираемые при сканировании в проектах, состав которых определяется произведенными настройками управляющих параметров функциональных модулей ПК.

Входные ресурсы функциональных модулей ПК «SimuStrike» приведены в таблице 3.

Таблица 3 – Входные ресурсы

Название	Входные ресурсы
Модуль горизонтального перемещения	Сетевой сервис, IP
Модуль сканирования Web	Сетевой сервис, URI, FQDN
Модуль удаления и шифрования данных	Сетевой сервис
Модуль эксфильтрации данных	Директория, агент, файл
Модуль первоначального доступа	Сетевой сервис, пара логин и пароль
Модуль сканирования AD	Сеть, IP, сетевой сервис,
Модуль сетевого сканирования	IP, FQDN, сервис

### 4.2 Выходные данные

Обогащённые данными входные объекты. Например, IP адрес в ходе сканирования дополняется наличием сетевых сервисов, программным обеспечением и уязвимостями в нем. В ходе дальнейшей работы ПК в таких модулях, как эксплуатация уязвимостей определяется возможность компрометации входного объекта.

Выходными данными для ПК являются:

- автоматически строится отчет по результатам каждой итерации в ходе выполнения задания фаззинга, парсинга и поиска в базах утечек;
- отчет по результатам каждой итерации в ходе выполнения задания по имитации доступа к ресурсам из потока данных TI;
- результаты выполнения задания формируются для каждого агента. Возможна выгрузка отчета в формате Excel или CSV;
- отчеты по результатам фишинговых атак;
- отчеты по результатам сканирования ресурса в кампании;
- отчеты по результатам сканирования веб-ресурсов. Возможна выгрузка отчета в формате Excel или CSV;

- выгрузка отчета в формате Excel или CSV;
- графическое представление построения карты сети;
- данные, экспортируемые подсистемой отображения собранных данных, в файлы формата «PDF» по запросам оператора ПК.

Выходные ресурсы функциональных модулей ПК «SimuStrike» приведены в таблице 4.

Таблица 4 – Выходные ресурсы

Название	Выходные ресурсы
Модуль горизонтального перемещения	Агент, пара пользователь и пароль, пара логин и пароль, пара пользователь и хеш, пара хост и пароль
Модуль сканирования Web	URI, e-mail, телефон, сетевой сервис, пара ПО и хост, пара ПО и URI
Модуль удаления и шифрования данных	Файл
Модуль эксфильтрации данных	Файл, пользователь, хеш, пара пользователь и хеш
Модуль первоначального доступа	Сетевой сервис, пара хост и пароль, пара логин и пароль, пара пользователь и пароль
Модуль сканирования AD	Сеть, сетевой сервис, IP, пользователь, пароль, пара пользователь и пароль, пара хост и хеш, пара пароль и хост, пара пользователь и хеш
Модуль сетевого сканирования	IP, сетевой сервис, пара ПО и хост, пара ПО и URI

## 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 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. 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
SOC	–	Security Operations Center
SNMP	–	Simple Network Management Protocol
SMTP	–	Simple Mail Transfer Protocol
SSH	–	Secure Shell
TI	–	Threat Intellegence
TTP	–	Tactics Technics Protocols
TLS	–	Transport Layer Security
АРМ	–	Автоматизированное рабочее место
БД	–	База данных
БДУ	–	База данных уязвимостей
ИБ	–	Информационная безопасность
КО	–	Клиентское оборудование
ОС	–	Операционная система
ПК	–	Программный комплекс
ПО	–	Программное обеспечение
ППО	–	Программное программное обеспечение
ПТС	–	Программно-технические средства
СрЗИ	–	Средства защиты информации
ТУ	–	Технические условия
ИБ	–	Информационная безопасность