ООО «Газинформсервис»

УТВЕРЖДАЮ
Заместитель генерального директора –
технический директор
ООО «Газинформсервис»

_____Н.В. Нашивочников

«____» _____ 20___ г.

ПРОГРАММНЫЙ КОМПЛЕКС
SafeERP Platform Security Extension Module

Руководство администратора

Представители предприятия-разработчика

Руководитель проекта/Начальник отдела РБППО

_____С.В. Устенко

Исполнитель

_____Е.А. Жданова

Нормоконтролер

_____И.Л. Крылова

2023

ООО «Газинформсервис»

Утвержден

Программный комплекс
SafeERP Platform Security Extension Module

Описание применения

Листов 27

2023

АННОТАЦИЯ

Данное руководство является программным документом, определяющим порядок установки расширения программного комплекса (далее – ПК) SafeERP Platform Security Extension Module (далее – SafeERP PS EM).

Настоящее руководство состоит из информационной части (аннотации и листа содержания) и разделов основной части, включающих в себя:

- сведения о назначении расширения ПК SafeERP PS EM;
- условия работы расширения ПК SafeERP PS EM;
- порядок установки расширения ПК SafeERP PS EM;
- порядок запуска web-интерфейса расширения ПК SafeERP PS EM.

СОДЕРЖАНИЕ

1. Назначение ПК SafeERP PS EM

Расширение ПК SafeERP PS EM предназначено для проведения автоматизированного тестирования на проникновение сервисов и другого распространенного ПО.

Расширение ПК SafeERP PS EM реализует следующие функциональные возможности:

- проверку доступности целевых серверов;
- определение состояния указанных портов на целевых серверах;
- идентификацию запущенных на открытых портах сервисов, ПО и его версии (при наличии возможности такого определения);
- обнаружение уязвимостей (CVE) для идентифицированного ПО (при наличии уязвимого ПО);
- поиск известных эксплойтов для обнаруженных уязвимостей (CVE) (при наличии уязвимого ПО);
- применение подготовленных пентестов для идентифицированных сервисов;
- генерацию отчета в формате PDF, содержащего информацию, перечисленную выше.

2. Общая схема работы ПК SafeERP PS EM

2.1. Компоненты ПК SafeERP PS EM

Расширение состоит из нескольких компонентов – одного сервера управления ПК SafeERP PS EM и одного агента сканирования по умолчанию. Это расширение содержит весь необходимый функционал для сбора и обработки информации, проведения автоматизированного тестирования на проникновение, генерации отчета и отображения web-интерфейса.

Общая схема работы расширения представлена на (рис. 1).

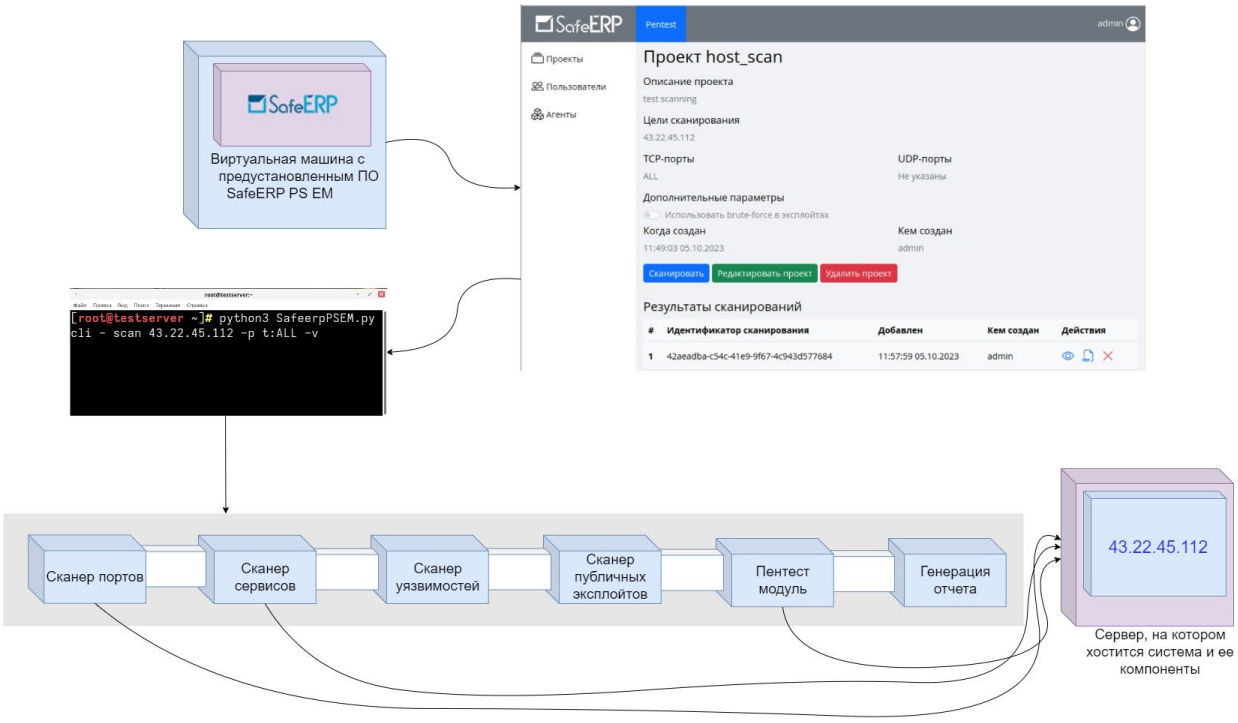


Рисунок 1 – Общая схема работы расширения ПК SafeERP PS EM

2.2. Технические средства, обеспечивающие работу ПК SafeERP PS EM

Control Server

Сервер, на котором развернуто расширение ПК SafeERP PS EM, должен соответствовать следующим требованиям:

- четырехъядерный процессор Intel с частотой не менее 2,5 ГГц;
- оперативное запоминающее устройство с объемом памяти не менее 8 Гбайт;
- жесткий диск объемом не менее 100 Гбайт;
- встроенный сетевой адаптер.

Технические характеристики компьютеров, на базе которых созданы автоматизированные рабочие места оператора и администратора расширения ПК SafeERP PS EM, должны иметь характеристики не ниже:

- процессор Intel с частотой не менее 1,5 ГГц;
- оперативное запоминающее устройство с объемом памяти не менее 1 Гбайт;
- жесткий диск объемом не менее 150 Гбайт;
- встроенный SVGA-адаптер с объемом памяти не менее 32 Мбайт;
- жидкокристаллический монитор с размером экрана не менее 15 дюймов и разрешением не менее 1024x768 пикселей;
- встроенный сетевой адаптер;
- клавиатура;
- мышь;
- источник бесперебойного питания.

2.3. Технические средства, обеспечивающие работу ПК SafeERP PS EM Agent

Сервер, на котором развернут агент расширения ПК SafeERP PS EM, должен соответствовать следующим требованиям:

- четырехъядерный процессор Intel с частотой не менее 2,5 ГГц;
- оперативное запоминающее устройство с объемом памяти не менее 8 Гбайт;
- жесткий диск объемом не менее 50 Гбайт;
- встроенный сетевой адаптер.

3. Запуск интерфейса настройки ПК

3.1. Запуск web-интерфейса

Для запуска web-интерфейса SafeERP PS EM необходимо в консоли сервера, на котором установлено расширение, выполнить следующую команду под учетной записью пользователя safeerp_ps_em:

```
docker compose up -d
```

Сканер будет доступен в браузере по следующим адресам:

```
https://<SEP_CONTROL_SERVER_HOST>:<SEP_CONTROL_SERVER_PORT>
```

3.2. Вход

Для первичного входа в сканер используются учётные данные по умолчанию (admin/admin) (рис. 2).

После успешного входа появится форма смены пароля – необходимо изменить пароль по умолчанию. До смены пароля по умолчанию другие действия на сервере управления **будут недоступны**.

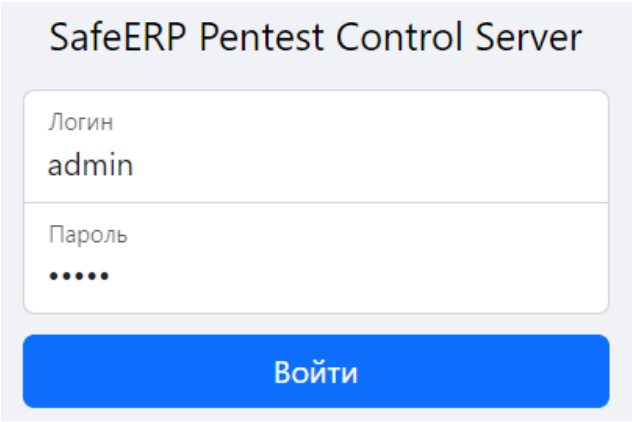


Рисунок 2 – Вход в сканер

4. Интерфейс модуля расширения ПК SafeERP PS EM

На первоначальном экране модуля «Pentest» (рис. 3) представлены следующие рабочие области:

– боковое меню;
– рабочая область, в соответствии с выбранным пунктом из бокового меню.

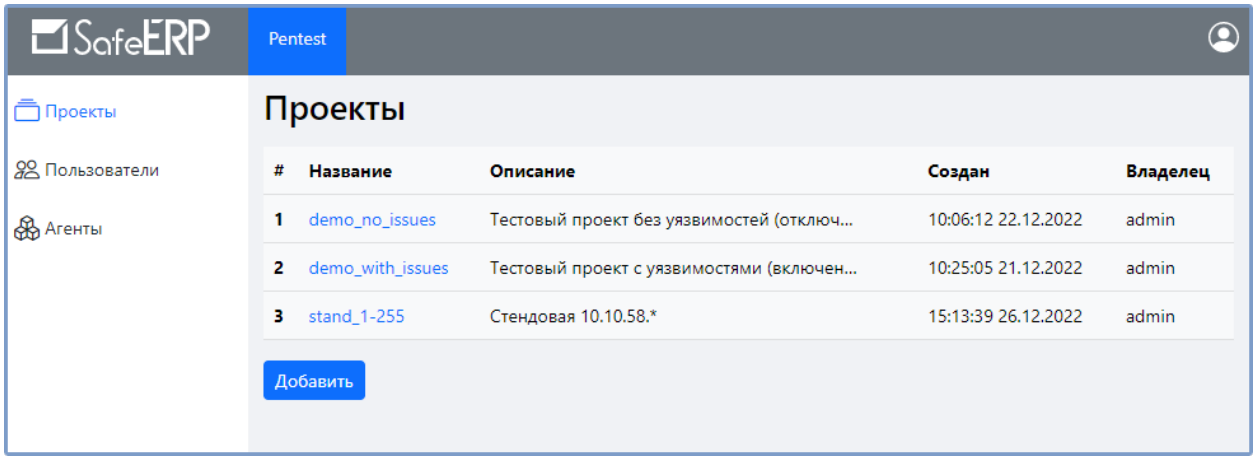


Рисунок 3 – Первоначальный экран модуля "Pentest"

4.1. Проекты

Подробные действия, связанные с проектами, приведены в пп. 4.1.1. – 4.1.4.

4.1.1 Создание проекта

Функция создания проекта предоставляется только пользователям с полномочиями на администрирование ПК SafeERP PS EM.

Для создания проекта необходимо выполнить следующие действия:

1) Выбрать раздел «Проекты».
2) Нажать кнопку Добавить.
3) Заполнить поля (рис. 4, 5)
4) Нажать на кнопку Добавить.

Появится окно «Создать проект», в котором следует определить (рис. 4, *5*):

– название отчета;
– описание проекта;
– цели сканирования;

– TCP и/или UDP порты;

– дополнительные параметры (активация brute-force в эксплойтах).

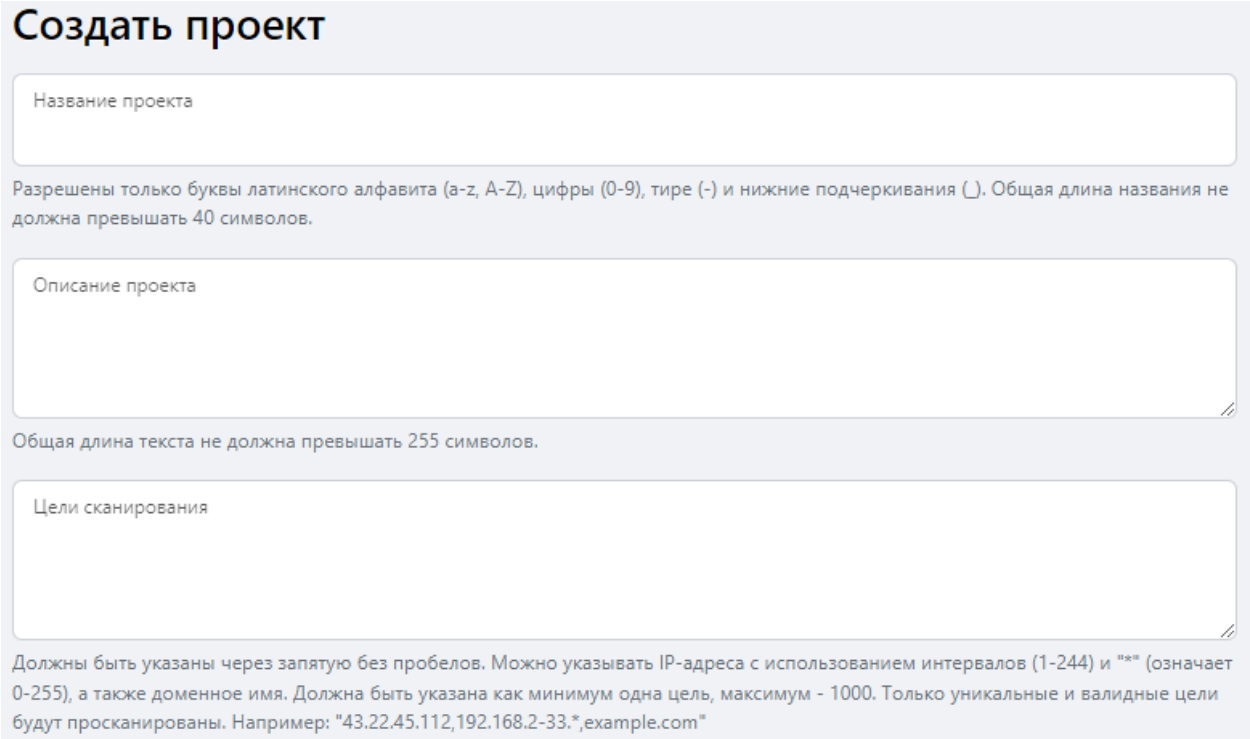


Рисунок 4 – Создание проекта. Название, описание, цели сканирования

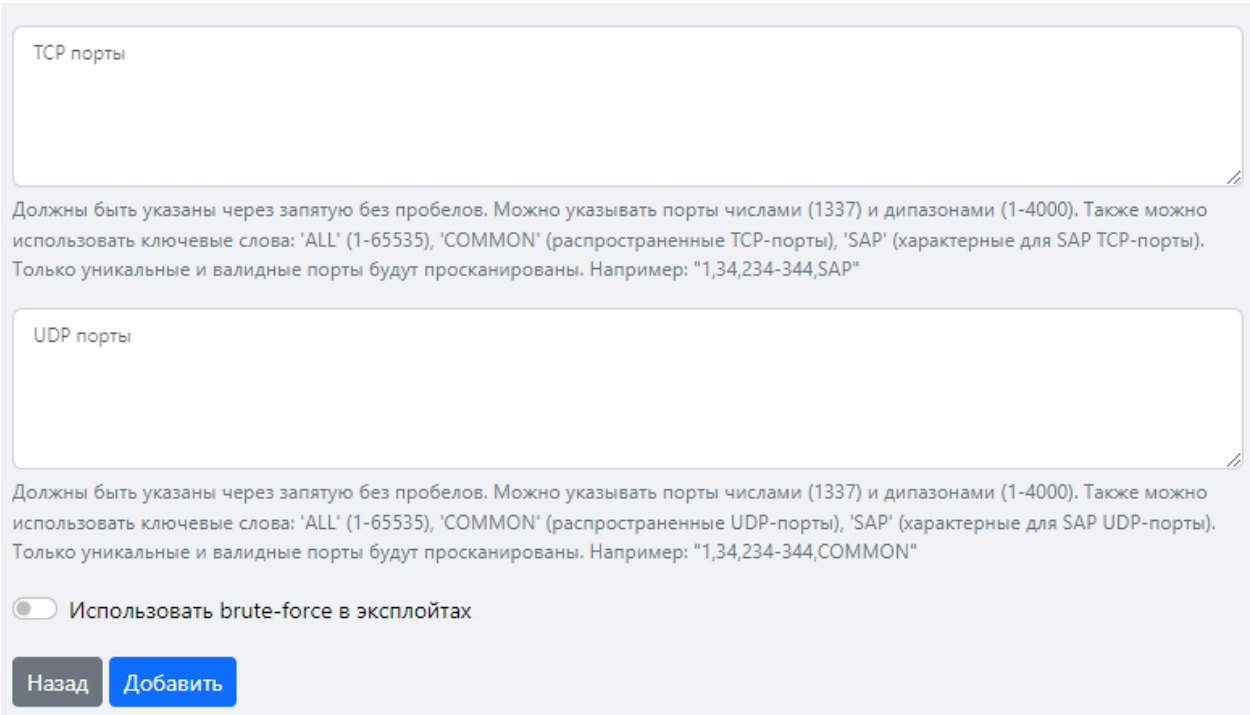


Рисунок 5 – Создание проекта. TCP порты, UDP порты, brute-force

Дальнейшее описание настроек изложены в подпунктах 4.1.1.1. - 4.1.1.4.

4.1.1.1. Название проекта

В названии проекта допускается использовать следующие символы:

- Прописные и строчные буквы латиницы;
- Цифры;
- Разрешенные символы (точка «.», тире «-», нижнее подчеркивание «_»).

Максимальное количество знаков в названии отчета 40 символов.

4.1.1.2. Цели сканирования

В данном окне ввести целевые сервисы для сканирования. В качестве целевого сервера можно указать:

- полное доменное имя (FQDN, например «example.com»);
- IPv4-адрес (например «192.168.0.1»);
- Шаблон IPv4-адресов для указания нескольких серверов(например, «192.168.2-34.*»).

Шаблон IPv4-адресов поддерживает следующие специальные обозначения:

- 2-34 – список номеров от 2 до 34;
- * – список номеров от 0 до 255.

Как минимум один сервер должен быть указан в качестве цели. При указании нескольких серверов только уникальные сервера будут просканированы. Целевые сервера, не попадающие в разрешенные лицензией цели сканирования, сканироваться не будут.

4.1.1.3. Порты

Номера портов необходимо указывать через запятую без пробелов («22,80-100,COMMON»). Поддерживаются следующие специальные обозначения**:**

1) Перечисление номеров портов от 1 до 65535;
2) Диапазон;
3) ALL – аналогично указанию TCP-портов с 1 по 65535 и/или UDP-портов с 1 по 65535;
4) Common – список распространенных портов, отличающийся для каждого протокола:

- COMMON в TCP – список распространенных TCP-портов. Список можно посмотреть и, при необходимости скорректировать, в файле «safeerp_pentest-master/data/ports/common_tcp.txt»;
- COMMON в UDP – список распространенных UDP-портов. Список можно посмотреть и, при необходимости скорректировать, в файле «safeerp_pentest-master/data/ports/common_udp.txt».

При указании нескольких портов только уникальные порты будут просканированы.

4.1.1.4. Brute-force

В качестве дополнительных параметров используются Brute-force в эксплойтах.

Для активации brute-force необходимо изменить положение ползунка (см. рис. 5).

В случае сканирования систем с включенным параметром brute-force, стандартные учетные записи этой системы могут быть **заблокированы** со всеми действиями, которые они выполняют.

4.1.2 Журнал событий процесса сканирования

Для просмотра журнала событий процесса сканирования, необходимо перейти в окно «показать лог». В данном окне представлены результаты выполнения этапов сканирования.

4.1.3. Результаты сканирования

В данное окно входят отчеты по сканированию. По умолчанию сохраняются отчеты в папке «Загрузки».

Возможные действия с отчетами будут изложены в подпунктах 4.1.3.1. – 4.1.3.2.

4.1.3.1. Сохранение и просмотр отчета

Для сохранения и просмотра отчета необходимо нажать на кнопку 

. Место сохранения отчета настроено по умолчанию.

Примечание – Отчеты сохраняются в формате *pdf.

4.1.3.2. Удаления отчета

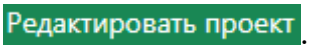
Для удаления отчета необходимо обратиться к полю «Недавние сканирования». Нажать на кнопку  .

4.1.4. Редактирование проекта

Вносить изменения в следующих полях:

- описание проекта;
- цели сканирования;
- TCP и UDP порты;
- дополнительные параметры.

Для редактирования проекта необходимо выполнить следующие действия:

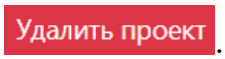
1) Выбрать раздел «Проекты».
2) Выбрать проект, нажать левой клавишей мышки в столбце «Название».
3) Нажать на кнопку 

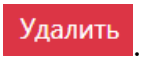
.
4) Внести изменения.
5) Нажать на кнопку 

.

4.1.5. Удаление проекта

Для удаления проекта требуется выполнить следующие действия:

1) Выбрать раздел «Проекты».
2) Выбрать проект, нажать левой клавишей мышки в столбце «Название».
3) Нажать на кнопку 

.
4) В открывшемся окне нажать кнопку 

.

4.2. Пользователи

В таблице 1 указаны полномочия пользователей ПК SafeERP PS EM.

Таблица 1 - Полномочия для пользователей

Полномочия	Группа		
	Администратор	Оператор	Гость
Проекты			
- просмотр	+	+	+
- создание	+	–	–

- редактирование	+	–	–
- запуск	+	+	–
- удаление	+	–	–
Отчеты			
- просмотр	+	+	+
- удаление	+	+	–
Агенты			
- просмотр	+	+	+
- редактирование	+	–	–
- удаление	+	–	–
Лицензии			
- генерация запроса на получение лицензии	+	–	–
- добавление	+	–	–
- удаление	+	–	–
- просмотр	+	+	+

4.2.1. Создание пользователей

Для создания пользователя необходимо заполнить следующие поля (рис. 6, 7):

- логин – логин, с помощью которого будет осуществляться вход в систему;
- пароль – пароль, с помощью которого будет осуществляться вход в систему;
- email – электронная почта, которая привязана к системе;
- имя – имя пользователя, который будет авторизован в системе;
- фамилия – фамилия пользователя, который будет авторизован в системе;

– группа – группа полномочий, которая присваивается пользователю.

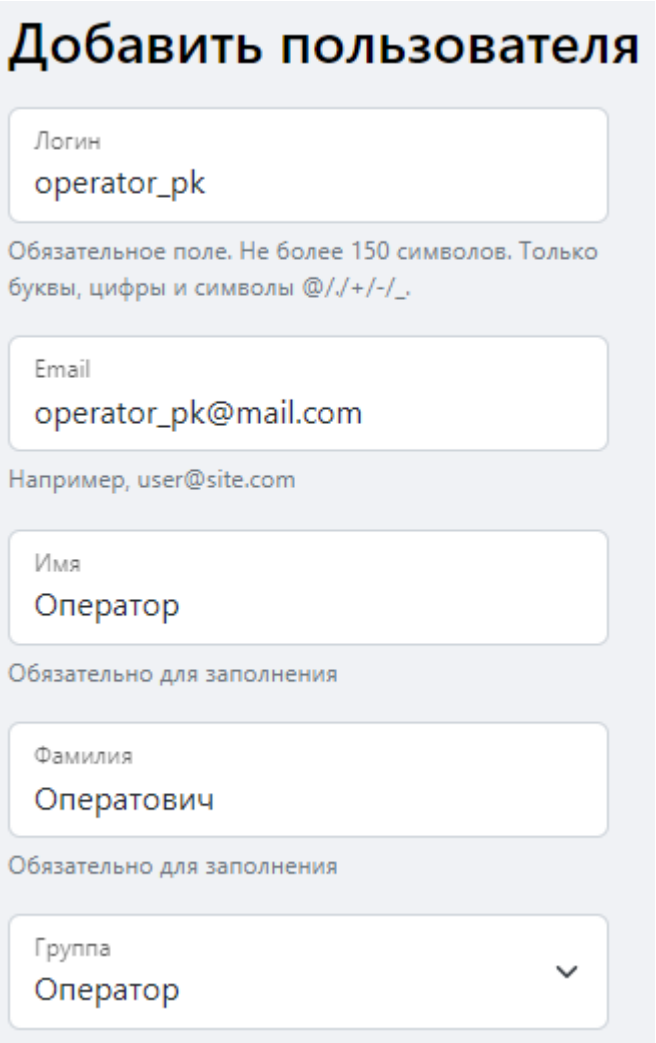


Рисунок 6 – Добавление пользователя. Логин, электронная почта, имя и фамилия пользователя

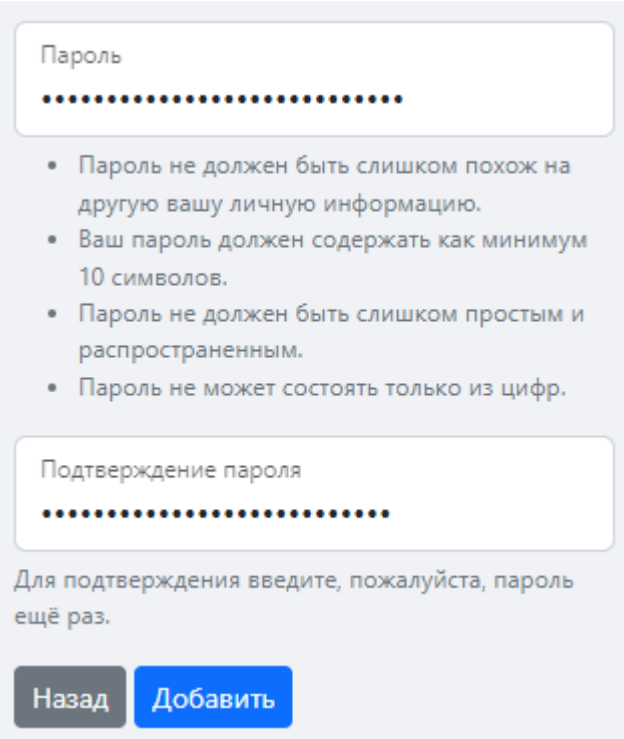


Рисунок 7 – Добавление пользователя. Пароль

Для создания пользователей необходимо выполнить следующие действия:

1) Выбрать раздел «Пользователи».
2) Нажать кнопку Добавить.
3) Заполнить поля (рис. 6, 7).
4) Нажать на кнопку Добавить.

4.2.2. Редактирование пользователей

Редактирование осуществляется в следующих полях:

- Логин;
- Email;
- Имя пользователя;
- Фамилия пользователя;
- Группа;
- Статус пользователя.

Для редактирования пользователя необходимо выполнить следующие действия:

1) Выбрать раздел «Пользователи».
2) Нажать на кнопку  .
3) Внести изменения.

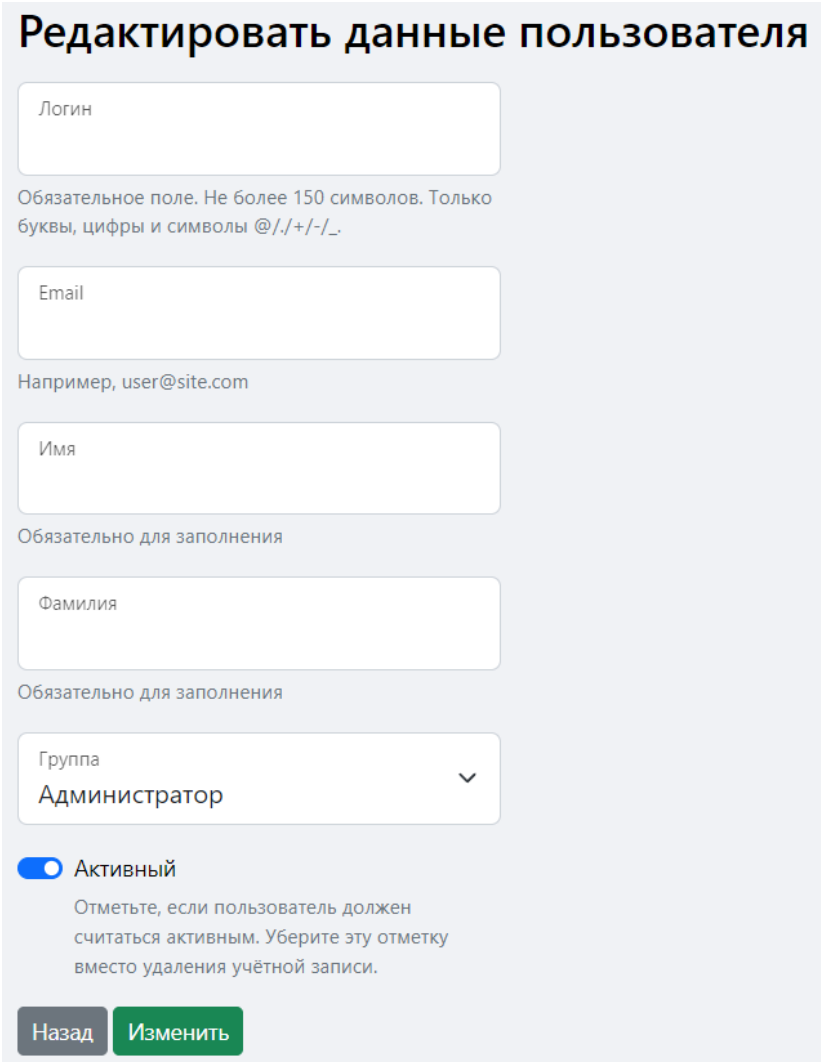


Рисунок 8 – Редактирование пользователей

4) Нажать на кнопку Изменить.

4.2.2.1. Смена пароля пользователей

Для смены пароля другого пользователя требуется выполнить следующие действия:

1) Выбрать раздел «Пользователи».
2) Нажать на кнопку  .
3) Заполнить поля.

4) Нажать на кнопку Сменить пароль.

4.2.3. Деактивация пользователей

Для деактивации пользователя необходимо выполнить следующие действия:

1) Выбрать раздел «Пользователи».
2) Нажать на кнопку  .
3) Изменить положение ползунка.
4) Нажать на кнопку Изменить.

4.2.4. Удаление пользователей

Для удаления другого пользователя необходимо выполнить следующие действия:

1) Выбрать раздел «Пользователи».
2) Нажать на кнопку  .
3) В открывшемся окне нажать на кнопку Удалить.

Пользователь с правами администратора не может удалить свой собственный профиль. Только деактивировать.

4.3. Агенты

4.3.1. Добавление агента

Для добавления агента необходимо заполнить следующие поля (Рисунок 9):

- Название – название агента, которое будет использоваться в проектах;
- IP-адрес – IP-адрес агента, с которого будут производиться сканирования;
- Порт – порт агента, с которого будут производиться сканирования.

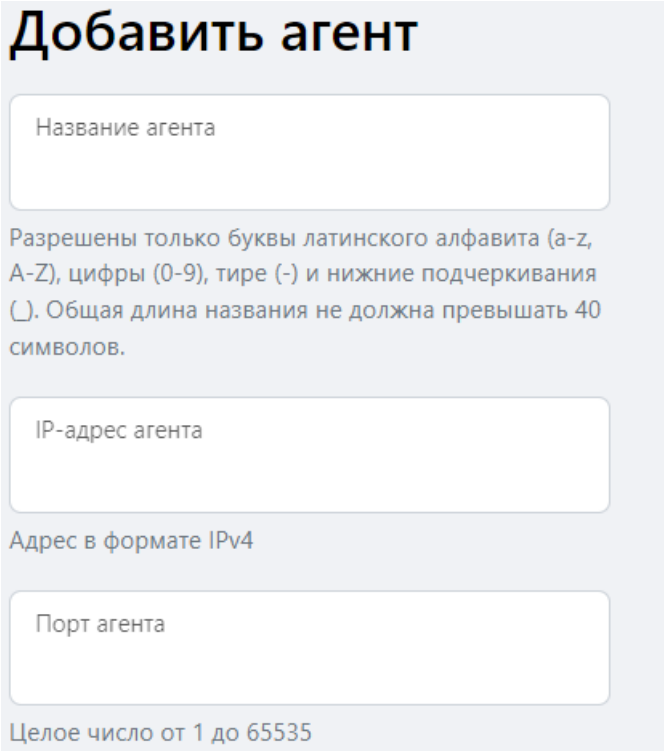


Рисунок 9 – добавление агента. Название, IP-адрес, порт агента

Для добавления агентов необходимо выполнить следующие действия:

1) Развернуть агента на необходимом сервере.
2) Выбрать раздел «Агенты».
3) Нажать кнопку Добавить.
4) Заполнить поля (Рисунок 9)
5) Нажать на кнопку Добавить.

Информация по добавленным агентам будет доступна в разделе «Агенты». Для каждого агента будет доступна следующая информация:

- Номер – порядковый номер созданного агента;
- Хост – ip-адрес агента;
- Порт – порт агента;
- Версия агента;
- Доступность – статус доступа к агенту;
- Лицензия – состояние лицензии агента;
- Статус – статус готовности агента к сканированию.

4.3.2 Лицензирование агента

Для добавления лицензии требуется выполнить следующие действия:

1) Войти в раздел «Агенты».
2) Нажать на название агента.
3) Нажать на кнопку Сгенерировать запрос на лицензию.
4) Заполнить поле ключа лицензии полученного от вендора, e-mail, на который будет отправлен ключ активации (рис. 10).

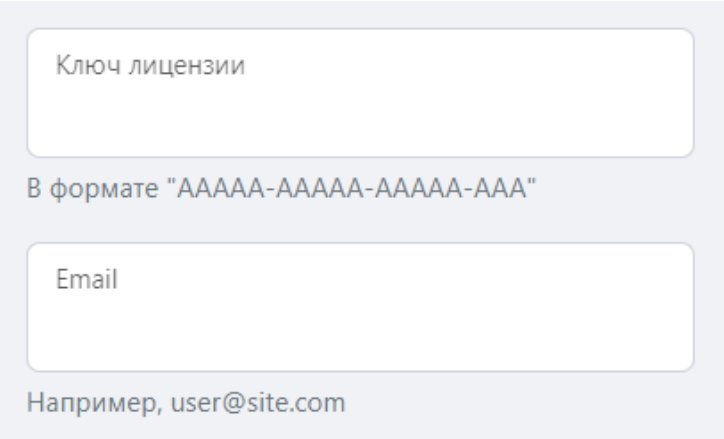


Рисунок 10 – Ключ лицензии, e-mail

5) Нажать на кнопку Сгенерировать запрос.
6) Перейти по ссылке https://license.gaz-is.ru/offlineActivate/
7) Нажать на кнопку Выбор файла.
8) Загрузить автоматически скачанный файл после выполнения пункта 5.
9) Нажать на кнопку Активировать.
10) Заполнить поле (рис. 11).

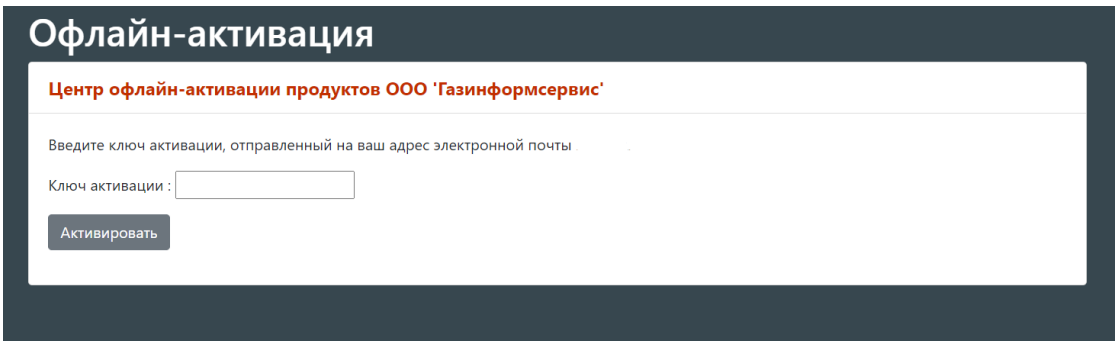


Рисунок 11 – Офлайн-активатор. Ключ активации

11) Нажать на кнопку Активировать.

12) После успешной активации нажать на кнопку Сохранить в файл.

13) Вернуться в рабочую область агента.

14) Нажать на кнопку Загрузить лицензию.

15) Нажать на кнопку Выбор файла.

16) Загрузить файл, полученный после выполнения пункта 12.

17) Нажать на кнопку Загрузить лицензию.

Подробная информация о лицензии агента будет доступна в разделе «Агенты». Для каждого агента будет доступна следующая информация:

- Статус действительности лицензии;
- Разрешенные цели агента;
- Количество сканирований;
- Период лицензии агента.

4.3.3. Редактирование агента

На странице редактирования агента возможно заполнить следующие поля (рис. 12):

- Название агента;
- IP-адрес агента;
- Порт агента;

Для редактирования агента требуется выполнить следующие действия:

1) Войти в раздел «Агенты».
2) Нажать на название агента.
3) Нажать на кнопку Редактировать данные агента.
4) Внести изменения.

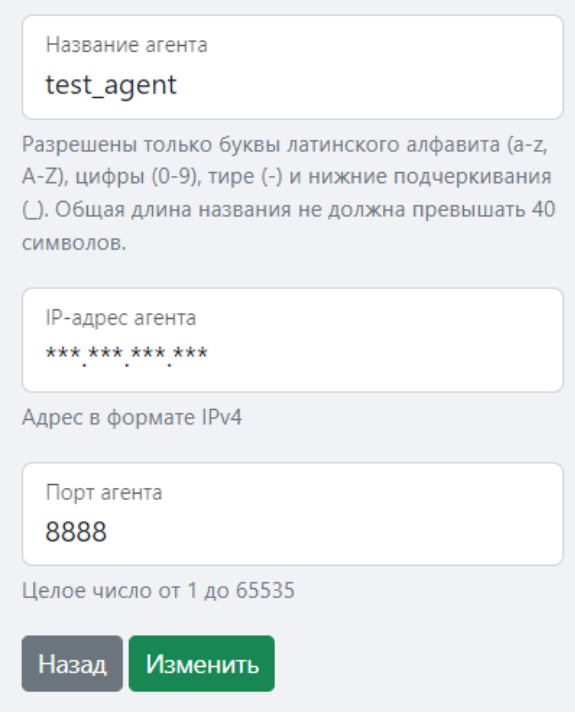


Рисунок 12 – Название агента, IP-адрес, порт

5) Нажать на кнопку Изменить.

4.3.4. Удаление агента

Для удаления агента на сервере управления необходимо выполнить следующие действия:

1) Выбрать раздел «Агенты».
2) Выбрать пользователя, нажав на столбец «Название».
3) Нажать на кнопку Удалить данные агента.

Агент будет удален с сервера управления, но на сервере, на котором он развернут – останется запущенным.

4.4. Личный кабинет пользователя

Подробные действия, связанные с личным кабинетом, изложены в пп. 4.4.1. – 4.4.3.

4.4.1. Профиль

Во вкладке «Профиль» есть возможность увидеть следующую информацию о пользователе:

- логин – логин, с помощью которого осуществляется вход в систему;
- email – электронная почта, которая привязана к системе;
- имя – имя пользователя, который авторизируется в системе;
- фамилия – фамилия пользователя, который авторизируется в системе;
- группа – группа полномочий, которая присваивается пользователю;
- токен авторизации – токен авторизации, использующийся для запуска сканирования из SDLC.

Для просмотра информации по своей личной учетной записи необходимо выполнить следующие действия:

1) Нажать на свой логин в левом верхнем углу экрана.
2) Нажать на вкладку «Профиль».

4.4.2. Смена пароля

Для смены пароля пользователя требуется выполнить следующие действия (рис. 13):

1) Нажать на свой логин в верхнем углу экрана.
2) Нажать на вкладку «Сменить пароль».
3) Ввести данные.

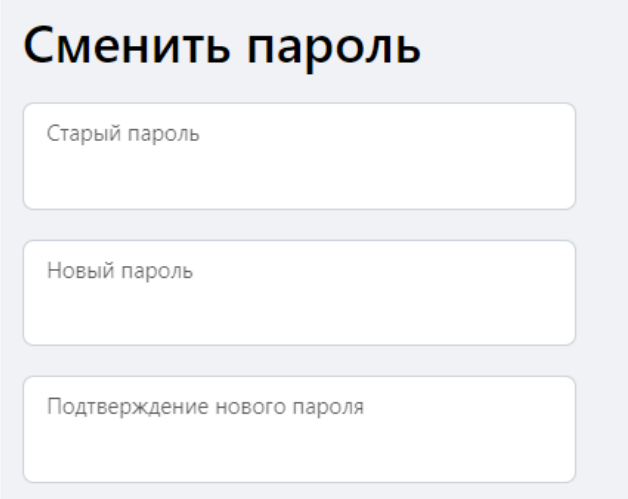


Рисунок 13 – Смена пароля

4) Нажать на кнопку Сменить пароль.

4.4.3. Смена пользователя

Чтобы сменить пользователя необходимо выполнить следующие действия:

1) Нажать на свой логин в правом верхнем углу экрана.
2) Нажать на кнопку «Выйти».
3) Ввести нужные учетные данные в открывшемся окне входа.
4) Нажать на кнопку Войти.

5. Интеграция SDLC

Интеграция и ведение SDLC модуля в ПК SafeERP PS EM возможно двумя способами: с помощью бинарного файла, либо docker-образа. Подробная информация представлена в пп. 5.1. – 5.2.

5.1. Интеграция SDLC по средствам бинарного файла

SDLC модуль использует данные аргументы:

- token – токен авторизации пользователя в ПК SafeERP PS EM;
- server – URL используемый для сканера;
- agent – название агента, связанное со сканером;
- project – название проекта, применяемого для сканирования в ПК SafeERP PS EM.

Пример использования модуля в .gitlab-ci.yml

```
variables:
    TOKEN: "00ea1da4192a2030f9ae023de3b3143ed647bbab"
    SERVER: "https://192.168.0.127"
    AGENT: "agent_name"
    PROJECT: "project_name"

safeerp_ps_em_sdlc:
    stage: safeerp_ps_em_sdlc
    script:
        - ./safeerp_ps_em_sdlc -token $TOKEN -server $SERVER -
agent $AGENT -project $PROJECT
    allow_failure: false
    tags:
        - shell
        - preprod
    only:
        - master
```

5.2. Интеграция SDLC по средствам Docker-образа

SDLC модуль использует данные аргументы:

- token – токен авторизации пользователя в ПК SafeERP PS EM;
- server – URL используемый для сканера;

– agent – название агента, связанное со сканером;
– project – название проекта, применяемого для сканирования в ПК SafeERP PS EM.

Пример использования модуля в .gitlab-ci.yml

```
variables:
    TOKEN: "00ea1da4192a2030f9ae023de3b3143ed647bbab"
    SERVER: "https://192.168.0.127"
    AGENT: "agent_name"
    PROJECT: "project_name"

safeerp_ps_em_sdlc:
    stage: safeerp_ps_em_sdlc
    script:
        - docker run --rm serp_ps_em_sdlc:latest
./safeerp_ps_em_sdlc -token $TOKEN -server $SERVER -agent
$AGENT -project $PROJECT
    allow_failure: false
    tags:
        - shell
        - preprod
    only:
        - master
```

Перечень сокращений

ПК	–	программный комплекс
ПО	–	программное обеспечение
CVE	–	Common Vulnerabilities and Exposures
FQDN	–	Fully Qualified Domain Name
PDF	–	Portable Document Format
PS EM	–	Platform Security Extension Module
SDLC	–	Software development lifecycle
TCP	–	Transmission Control Protocol
UDP	–	User Datagram Protocol