

Киберполигон

Инструкция по работе с сервисом

1. Цели и назначения системы	3
2. Роли пользователей	3
3. Сценарии	4
3.1 Сценарии для всех пользователей	4
3.1.1. Авторизация	4
3.1.2. Настройка профиля	4
3.2. Суперадминистратор/Администратор	5
3.2.1. Авторизация	6
3.2.2. Добавление нового пользователя «Студент»	6
3.2.3. Добавление нового пользователя «Инструктор»	7
3.2.4. Добавление нового пользователя «Администратор»	8
3.2.5. Добавление нового пользователя «Суперадминистратор»	9
3.2.6. Редактирование пользователей	9
3.2.7. Настройка профиля (Недоступно для Суперадминистратора)	10
3.2.8. Загрузить файл CSV	10
3.2.9. Активация/Деактивация пользователей	10
3.2.10. Первостепенные функции	11
3.3. Инструктор	12
3.3.1. Авторизация	12
3.3.2. Настройка профиля	12
3.3.3. Создание рабочего окружения	13
3.3.4. Редактирования рабочего окружения	14
3.3.5. Приглашение в рабочее окружение по ссылке	14
3.3.6. Приглашение в рабочее окружение через инвайт	15
3.3.7. Активация/Деактивация пользователей внутри рабочего окружения	16
3.3.8. Создание учения	16
3.3.9. Редактирование учения	17
3.3.10. Удаление учения	18
3.3.11. Старт учения	19
3.3.12. Остановить учение	19
3.3.13. Завершения учения	20
3.3.14. Оценка отчетов (Red Team)	21
3.3.15. Чат	22
3.3.16. Комментарии к карточкам	23
3.3.17. Демонстрация учения	24
3.3.18. Просмотр статистики по учениям	25
3.3.19. Настройка столбцов со статистикой	26

3.3.20. Формирование отчета со статистикой	27
3.3.21. Управление скриптом атаки в конфигурации учения Blue Team vs Script	27
3.3.22. Первостепенные функции	28
3.4. Студент	29
3.4.1. Авторизация	30
3.4.2. Настройка профиля	30
3.4.3. Регистрация	30
3.4.4. Функционал зависящий от роли в учении	31
3.4.4.1. Blue Team	31
3.4.4.1.1. SOC	31
3.4.4.1.1.1. Создание инцидента	31
3.4.4.1.1.2. Написание комментария к карточке инцидента	31
3.4.4.1.1.3. Общение в чате	33
3.4.4.1.2. Leader	33
3.4.4.1.2.1. Назначение инцидента	33
3.4.4.1.2.2. Голосование за карточку инцидент	34
3.4.4.1.2.3. Обработка карточки инцидента	34
3.4.4.1.2.4. Написание комментария к карточке инцидента	35
3.4.4.1.2.5. Общение в чате	35
3.4.4.1.2.6. Оценка товарищей по команде после завершения учения	35
3.4.4.1.3. OPS	35
3.4.4.1.3.1. Голосование за карточку инцидента	35
3.4.4.1.3.2. Обработка карточки инцидента	35
3.4.4.1.3.3. Написание комментария к карточке инцидента	35
3.4.4.1.3.4. Общение в чате	35
3.4.4.2. Red Team	36
3.4.4.2.1. Attacking	36
3.4.4.2.1.1. Создание карточки взлома	36
3.4.4.2.1.2. Написание отчета для карточки взлома	36
3.4.4.2.1.3. Редактирование карточки уязвимости	38
3.4.4.2.1.4. Написание комментария к карточке взлома	39
3.4.4.2.1.5. Общение в чате	40
3.4.4.2.2. Leader	40
3.4.4.2.2.1. Назначение карточки взлома	40
3.4.4.2.2.2. Создание карточки взлома	40
3.4.4.2.2.3. Написание отчета для карточки взлома	40
3.4.4.2.2.4. Редактирование карточки уязвимости	40
3.4.4.2.2.5. Написание комментария к карточке взлома	41
3.4.4.2.2.6. Общение в чате	41
3.4.4.2.2.7. Оценка товарищей по команде после завершения учения	41
3.4.5. Первостепенные функции	41

1. Цели и назначения системы

Полное наименование: Программное обеспечение «Система моделирования киберугроз и ликвидации инцидентов безопасности в информационных инфраструктурах».

Краткое наименование: «Киберполигон».

Программное обеспечение «Киберполигон» представляет собой программную платформу для проведения занятий со специалистами по предотвращению, обнаружению, реагированию, расследованию и устранению последствий инцидентов.

Программное обеспечение ориентировано для обучения команды Blue Team и команды Red Team в формате киберучений под контролем руководителя процесса – Инструктора.

2. Роли пользователей

В системе пользователям можно присваивать разные роли. Каждая роль по умолчанию предоставляет пользователям доступ к определенным инструментам учетной записи. К тому же у ролей могут быть различные разрешения в зависимости от предоставленных им привилегий.

1. Суперадминистратор

Создается программно при развертке платформы

- Обладает всеми возможностями администратора
- Может наделять пользователей ролью «Администратор»

2. Администратор

Назначается суперадминистратором

- Имеет полный доступ ко всем разделам панели управления
- Может наделять пользователей ролью «Инструктор»
- Может добавлять пользователей с ролью «Студент»

3. Инструктор

Назначается администратором

- Может создавать и управлять своими рабочими окружениями
- Может приглашать пользователей в свои рабочие окружения
- Может создавать / редактировать / удалять / проводить учения в рамках своих рабочих окружений

4. Студент

Добавляется администратором или регистрируется самостоятельно

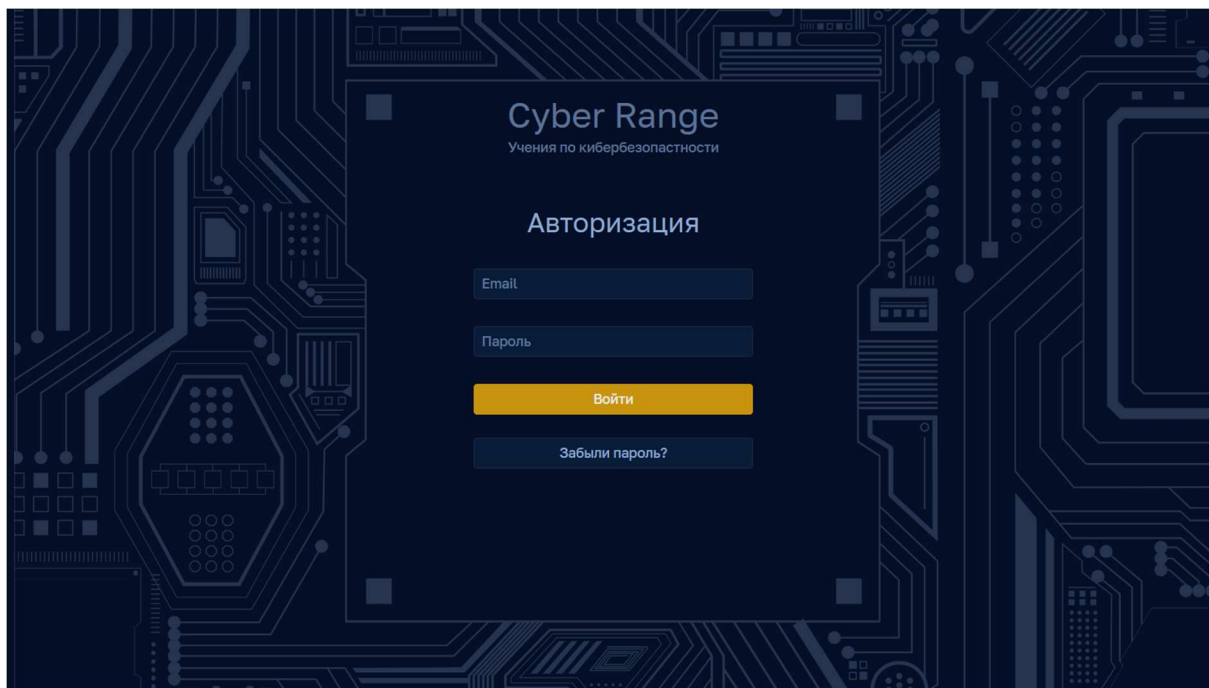
- Может просматривать список учений, в которых он участвует
- Может участвовать в учении в роли
 - Red Team
 - Leader
 - Attacking
 - Blue Team
 - Leader
 - OPS
 - SOC

3. Сценарии

3.1 Сценарии для всех пользователей

- [Авторизация](#)
- [Настройка профиля](#)

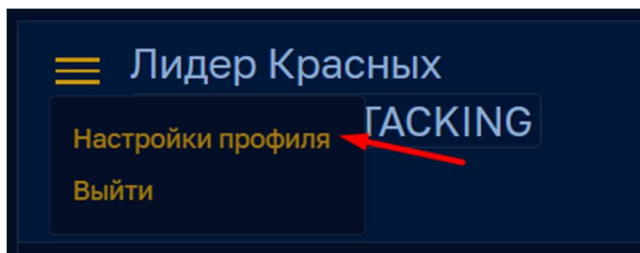
3.1.1. Авторизация



1. При открытии приложения система открывает страницу с обязательными полями:
 - a. Email.
 - b. Пароль.
2. Пользователь нажимает на кнопку «Войти». Далее перед пользователем открывается интерфейс приложения, следовательно пользователь авторизовался в системе.

3.1.2. Настройка профиля

Для того чтобы перейти к редактированию и настраиванию своего профиля необходимо нажать бургер-меню (три горизонтальные полосы) в левом верхнем углу.



1. Пользователь нажимает кнопку «Настройки профиля». Система открывает модальное окно с полями для редактирования:

- а. Имя.
 - б. Фамилия.
 - с. Email – недоступно для редактирования.
2. После редактирования полей необходимо нажать на кнопку «Сохранить». Далее система принимает или отклоняет редактирование данных.
 3. Пользователь также может изменить пароль, не изменяя остальные персональные данные аккаунта. Пользователю будут доступны поля для редактирования
 - а. Пароль – необходимо ввести старый пароль, который был привязан к данному аккаунту.
 - б. Новый пароль – пароль должен содержать минимум 8 символов.
 - с. Повторите пароль – должен полностью совпадать с полем «Новый пароль»
 4. После редактирования полей необходимо нажать на кнопку «Изменить пароль». Далее система принимает или отклоняет изменение пароля.
 5. Для того чтобы модальное окно закрыть, необходимо нажать крестик.

3.2. Суперадминистратор/Администратор

Основной функционал суперадминистратора/администратора:

- [Авторизация](#)
- Добавление нового пользователя
 - [Студент](#)
 - [Инструктор](#)
 - [Администратор](#)
 - [Суперадминистратор](#)
- [Редактирование пользователя](#)

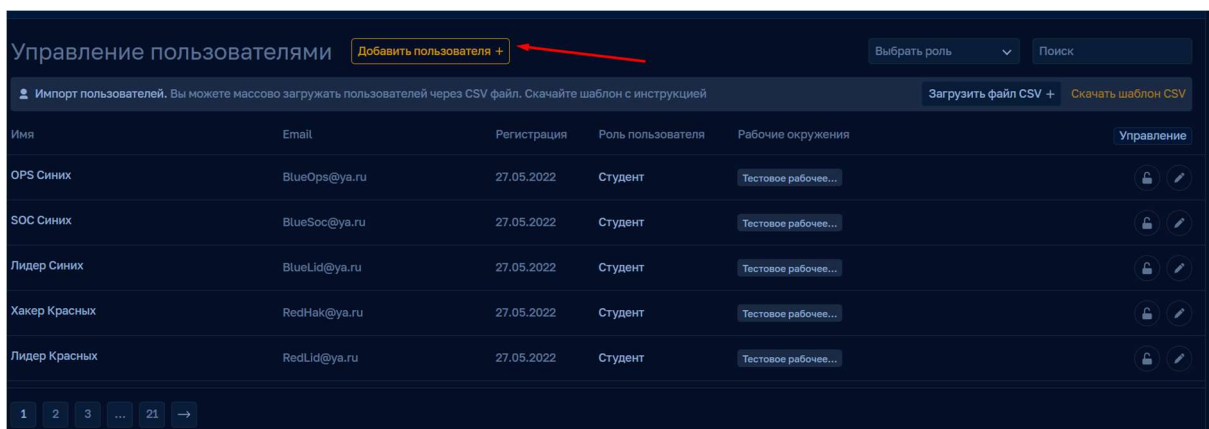
- [Настройка профиля](#)
- [Загрузить файл CSV](#)
- [Активация/Деактивация пользователей](#)
- [Первостепенные функции](#)

Во всем разделе 3.2. под термином **пользователь** будет использоваться роль суперадминистратор/администратор для упрощения написания.

3.2.1. Авторизация

Смотри пункт 3.1.1. – [авторизация](#)

3.2.2. Добавление нового пользователя «Студент»



Чтобы добавить пользователя, необходимо найти раздел «Управление пользователями» и справа от данного раздела кнопку «Добавить пользователя».

1. Пользователь нажимает на кнопку «Добавить пользователя». Система открывает модальное окно с обязательными полями для заполнения:
 - a. Имя
 - b. Фамилия
 - c. Email
 - d. Роль — нужно выбрать из выпадающего списка ролей системы: Инструктор, **Студент**, Суперадминистратор, Администратор.

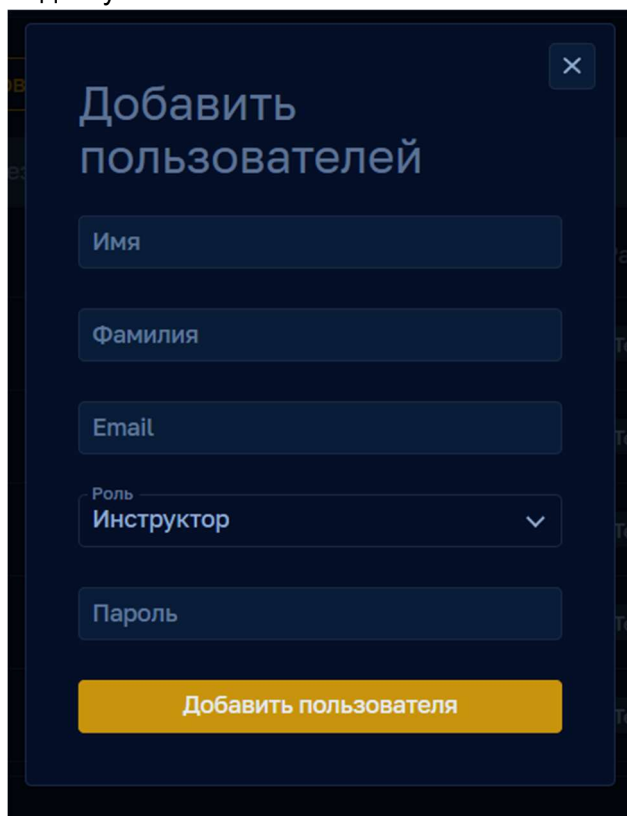
- е. Выберите рабочее окружение — нужно выбрать из выпадающего списка одно или несколько нужных рабочих окружений, которые будут доступны пользователю.
 - ф. Пароль
 2. После заполнения всех полей нужно нажать на кнопку «Добавить пользователя». Далее система отправляет на почту, указанную для создаваемого пользователя, ссылку для авторизации.

3.2.3. Добавление нового пользователя «Инструктор»

Чтобы добавить пользователя, необходимо найти раздел «Управление пользователями» и справа от данного раздела кнопку «Добавить пользователя».

1. Пользователь нажимает на кнопку «Добавить пользователя». Система открывает модальное окно с обязательными полями для заполнения:
 - а. Имя.
 - б. Фамилия.
 - с. Email.
 - д. Роль — нужно выбрать из выпадающего списка ролей системы: **Инструктор**, Студент, Суперадминистратор, Администратор.
 - е. Выберите рабочее окружение— нужно выбрать из выпадающего списка одно или несколько нужных рабочих окружений, которые будут доступны пользователю.

- i. Для пользователя с ролью инструктор выбор рабочего окружения недоступно.



- f. Пароль.
2. После заполнения всех полей нужно нажать на кнопку «Добавить пользователя». Далее система отправляет на почту, указанную для создаваемого пользователя, ссылку для авторизации.

3.2.4. Добавление нового пользователя «Администратор»

Чтобы добавить пользователя, необходимо найти раздел «Управление пользователями» и справа от данного раздела кнопку «Добавить пользователя».

1. Пользователь нажимает на кнопку «Добавить пользователя». Система открывает модальное окно с обязательными полями для заполнения:
 - a. Имя.
 - b. Фамилия.
 - c. Email.
 - d. Роль — нужно выбрать из выпадающего списка ролей системы: Инструктор, Студент, Суперадминистратор, **Администратор**.
 - e. Выберите рабочее окружение — нужно выбрать из выпадающего списка одно или несколько нужных рабочих окружений, которые будут доступны пользователю.
 - i. Для пользователя с ролью администратор выбор рабочего окружения недоступно.
 - f. Пароль.

2. После заполнения всех полей нужно нажать на кнопку «Добавить пользователя». Далее система отправляет на почту, указанную для создаваемого пользователя, ссылку для авторизации.

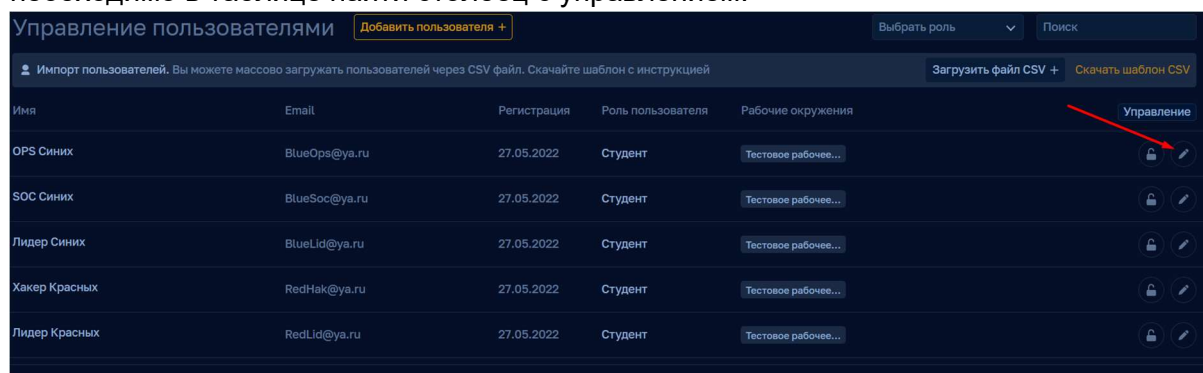
3.2.5. Добавление нового пользователя «Суперадминистратор»

Чтобы добавить пользователя, необходимо найти название раздела «Управления пользователями» правее от данного раздела находится кнопка «Добавить пользователя».

1. Пользователь нажимает на кнопку «Добавить пользователя». Система открывает модальное окно с обязательными полями для заполнения:
 - a. Имя.
 - b. Фамилия.
 - c. Email.
 - d. Роль — нужно выбрать из выпадающего списка ролей системы: Инструктор, Студент, **Суперадминистратор**, Администратор.
 - e. Выберите рабочее окружение — нужно выбрать из выпадающего списка одно или несколько нужных рабочих окружений, которые будут доступны пользователю.
 - i. Для пользователя с ролью суперадминистратор выбор рабочего окружения недоступно.
 - f. Пароль.
2. После заполнения всех полей нужно нажать на кнопку «Добавить пользователя». Далее система отправляет на почту, указанную для создаваемого пользователя, ссылку для авторизации.

3.2.6. Редактирование пользователей

Чтобы отредактировать пользователя, необходимо найти раздел «Управление пользователями». Данный раздел представляет из себя таблицу с полями. Далее необходимо в таблице найти столбец с управлением.



Имя	Email	Регистрация	Роль пользователя	Рабочие окружения	Управление
OPS Синих	BlueOps@ya.ru	27.05.2022	Студент	Тестовое рабочее...	🔒 ✎
SOC Синих	BlueSoc@ya.ru	27.05.2022	Студент	Тестовое рабочее...	🔒 ✎
Лидер Синих	BlueLid@ya.ru	27.05.2022	Студент	Тестовое рабочее...	🔒 ✎
Хакер Красных	RedHak@ya.ru	27.05.2022	Студент	Тестовое рабочее...	🔒 ✎
Лидер Красных	RedLid@ya.ru	27.05.2022	Студент	Тестовое рабочее...	🔒 ✎

1. Пользователю доступны две кнопки для редактирования:
 - a. Заблокировать пользователя — при нажатии на кнопку пользователю блокируется вход в систему.
 - b. Редактировать пользователя — при нажатии на кнопку пользователю открывается модальное окно с полями, доступные к редактированию.
 - i. Имя.

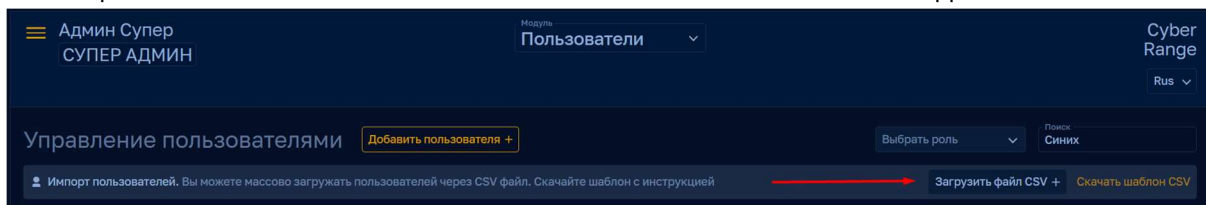
- ii. Фамилия.
- iii. Email — недоступно для редактирования.
- iv. Роль — можно сменить на другую роль из выпадающего списка ролей системы: Инструктор, Студент, Суперадминистратор, Администратор.
- v. Выберите рабочее окружение — можно добавить из выпадающего списка одно или несколько дополнительных рабочих окружений или вовсе их убрать.
 - 1. Для пользователя с ролью инструктор выбор рабочего окружения недоступно.
 - 2. Для пользователя с ролью администратор выбор рабочего окружения недоступно.
 - 3. Для пользователя с ролью суперадминистратор выбор рабочего окружения недоступно.
- vi. Пароль.
- vii. Чекбокс «Пользователь заблокирован» — если проставить галочку, пользователю, который подлежит редактированию, блокируется вход в систему.

3.2.7. Настройка профиля (Недоступно для Суперадминистратора)

Смотри пункт 3.1.2. – [настройка профиля](#)

3.2.8. Загрузить файл CSV

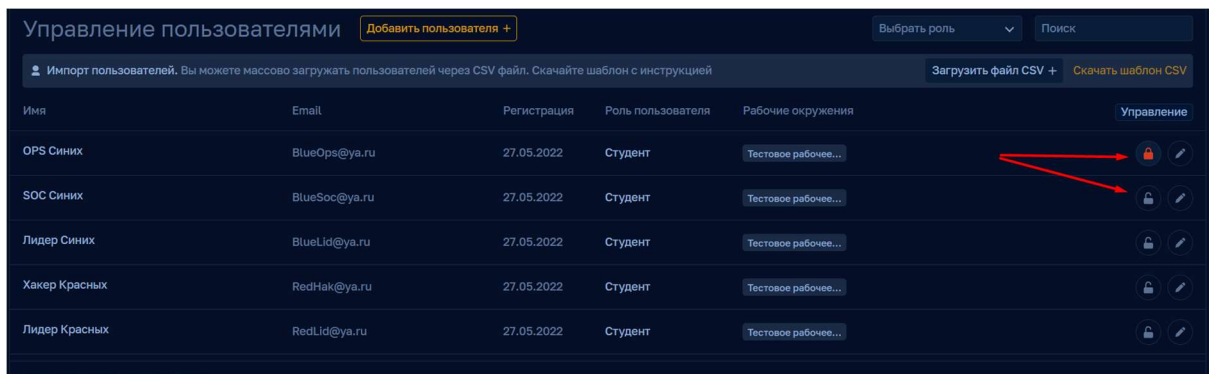
Данный функционал находится в разделе «Управление пользователями», чуть выше таблицы с пользователями есть две кнопки.



1. Пользователь нажимает на кнопку «Загрузить файл CSV», система открывает папку на рабочем компьютере пользователя.
2. Пользователю необходимо выбрать файл для загрузки.
3. Система автоматически регистрирует пользователей из файла.

3.2.9. Активация/Деактивация пользователей

Чтобы заблокировать или разблокировать пользователя, необходимо найти раздел «Управление пользователями». Данный раздел представляет из себя таблицу с полями. Далее необходимо в таблице найти столбец с управлением.

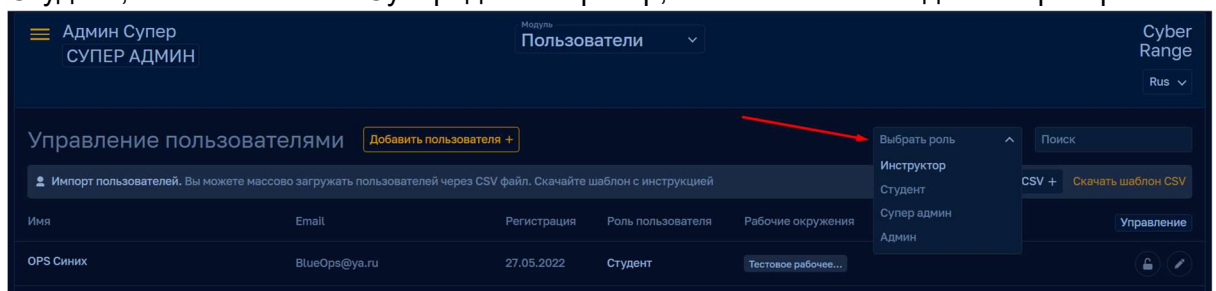


1. Пользователь нажимает на кнопку «Заблокировать пользователя». Система блокирует пользователя в системе.
2. Пользователь нажимает на ту же кнопку «Разблокировать пользователя». Система снова активизирует пользователя в системе.

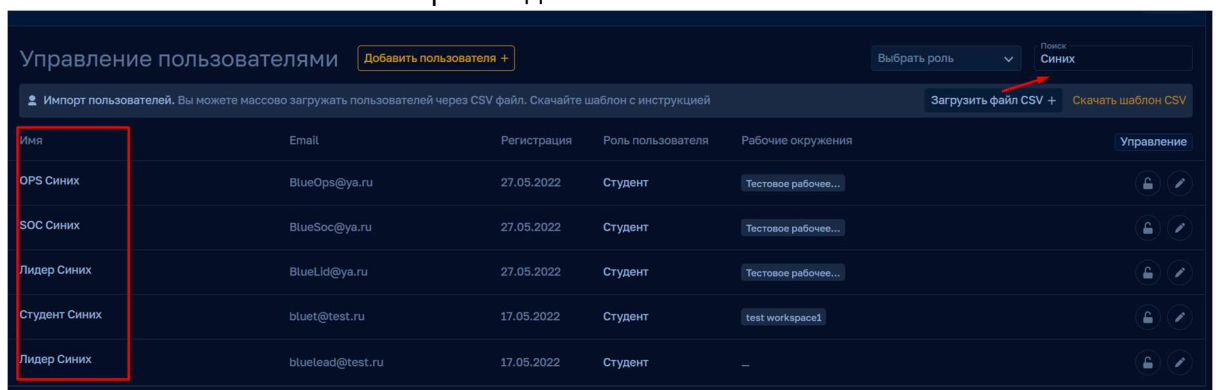
3.2.10. Первостепенные функции

Пользователю также доступны такие функции как:

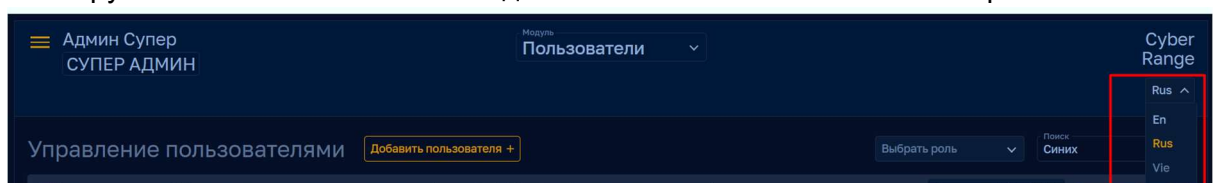
1. Фильтрация — фильтровать можно по ролям пользователей Инструктор, Студент, Суперадминистратор, Администратор



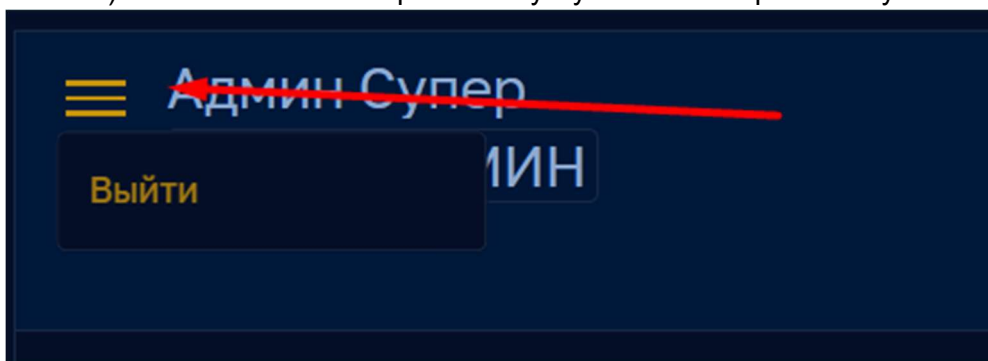
2. Поиск — поиск происходит по имени пользователей



3. Сменить язык — доступны три языка: Русский, Английский, Вьетнамский, планируется добавить Бирманский



4. Выйти из профиля — необходимо нажать бургер-меню (три горизонтальные полосы) в левом верхнем углу и выбрать пункт «Выйти».



3.3. Инструктор

Основной функционал инструктора:

- [Авторизация](#)
- [Настройка профиля](#)
- [Создание рабочего окружения](#)
- [Редактирование рабочего окружения](#)
- [Приглашение в рабочее окружение по ссылке](#)
- [Приглашение в рабочее окружение через инвайт](#)
- [Активация/Деактивация пользователей внутри рабочего окружения](#)
- [Создание учения](#)
- [Редактирование учения](#)
- [Удаление учения](#)
- [Старт учения](#)
- [Завершения учения](#)
- [Оценка отчетов](#)
 - [Red Team](#)
- [Проведение учения](#)
- [Чат](#)
- [Комментарии к карточкам](#)
- [Просмотр статистики по учениям](#)
- [Настройка столбцов со статистикой](#)
- [Формирование отчета со статистикой](#)
- [Управление скриптом атаки в конфигурации учения Blue Team vs Script](#)
- [Первостепенные функции](#)

Во всем разделе 3.3. под термином **пользователь** будет использоваться роль Инструктор для упрощения написания.

3.3.1. Авторизация

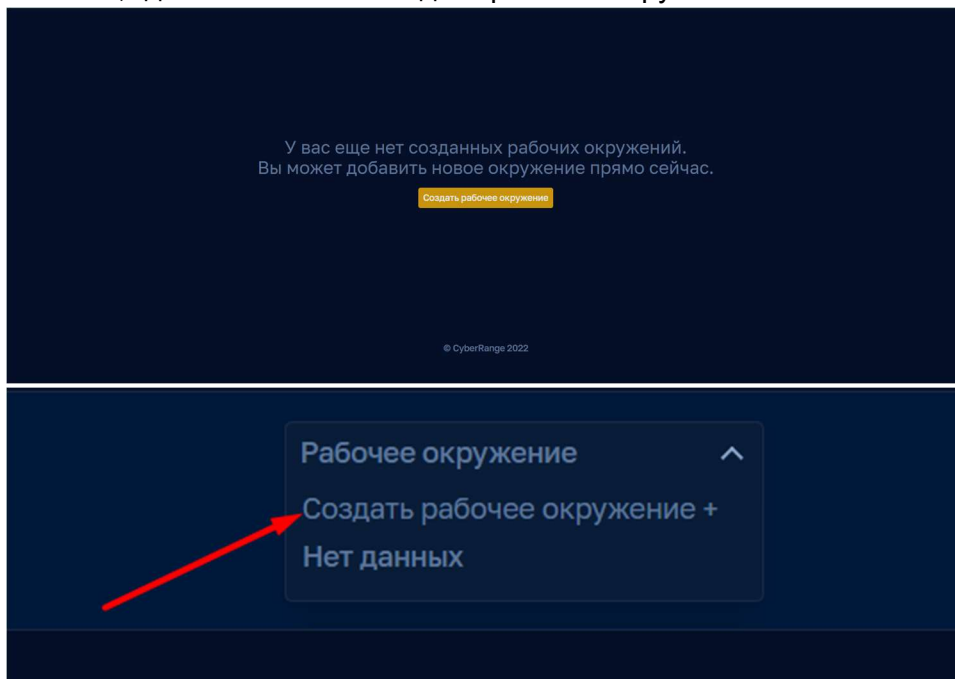
Смотри пункт 3.1.1. – [авторизация](#)

3.3.2. Настройка профиля

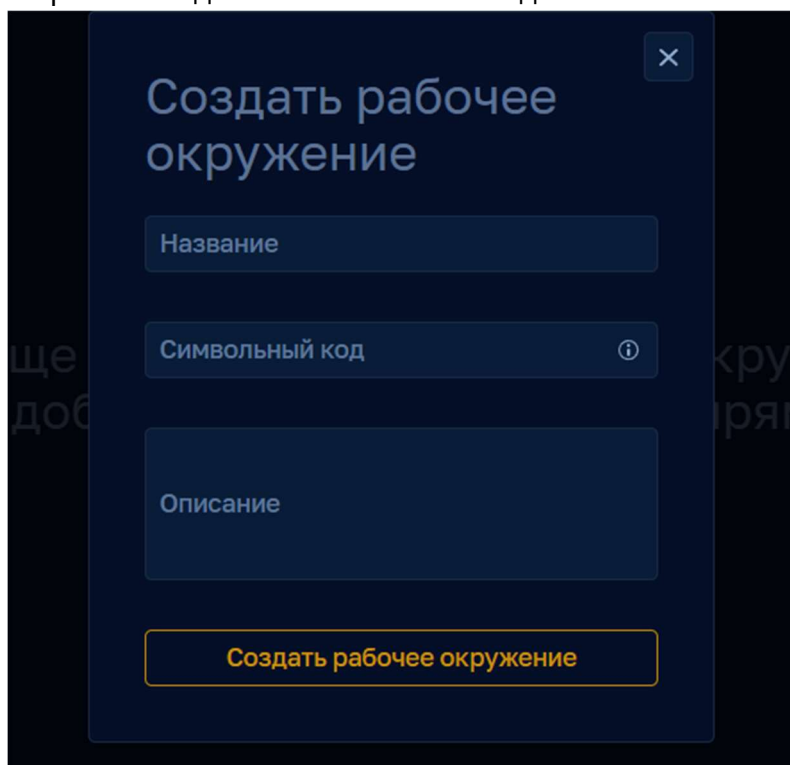
Смотри пункт 3.1.2. – [настройка профиля](#)

3.3.3. Создание рабочего окружения

Если пользователь заходит первый раз в систему, на стартовом экране ему доступна кнопка «Создать рабочее окружение». Если пользователь хочет добавить еще одно рабочее окружение, в шапке приложения по середине есть селект с выпадающим списком, где есть кнопка «Создать рабочее окружение +»



1. Пользователь нажимает на кнопку «Создать рабочее окружение». Система открывает модальное окно с полями для заполнения:



- а. Название – обязательное поле.
- б. Символьный код – обязательное поле.

- с. Описание – необязательное поле.
2. После заполнения полей нужно нажать на кнопку «Создать рабочее окружение».

3.3.4. Редактирования рабочего окружения

Чтобы отредактировать рабочее окружение, необходимо находиться в нем. Редактирование находится во вкладке «Настройки и инвайты». Справа находится раздел «Рабочее окружение».

1. Пользователь может редактировать рабочее окружения и ему доступны поля для регистрации:
 - a. Название.
 - b. Описание.
 - c. Язык интерфейса по умолчанию — нужно выбрать из выпадающего списка язык: Английский язык, Русский язык, Вьетнамский язык, планируется добавить Бирманский.
 - d. Чекбокс «Разрешить регистрацию пользователей по ссылке» – если проставить галочку, пользователь сможет приглашать студентов в данное рабочее окружение.
2. Для того, чтобы все изменения вступили в силу, необходимо нажать кнопку «Сохранить».

3.3.5. Приглашение в рабочее окружение по ссылке

Чтобы выслать ссылку на рабочее окружение, необходимо находиться в нем. Приглашения по ссылке находится во вкладке «Настройки и инвайты». Находим раздел инвайты и после раздела добавления пользователей есть активная ссылка «Пригласить по ссылке».

1. Пользователь нажимает на активную ссылку «Пригласить по ссылке». Система генерирует рабочую ссылку на рабочее окружение. *Время жизни ссылки составляет 24 часа, с момента нажатия на активную ссылку.*
 - a. **Важно:** Для того, чтобы неактивный пользователь (тот, который отсутствует в приложении) мог зарегистрироваться в приложении и стать участником рабочего окружения, необходимо, чтобы был проставлен чек-бокс «Разрешить регистрацию пользователей по ссылке», который находится в [Редактировании рабочего окружения](#).

3.3.6. Приглашение в рабочее окружение через инвайт

Для того, чтобы выслать инвайт на рабочее окружение, необходимо находится в нем. Приглашения через инвайт находится во вкладке «Настройки и инвайт». Находим раздел инвайты.

1. Чтобы пользователю отправить инвайт студенту, ему необходимо заполнить обязательные поля:
 - a. Имя.
 - b. Фамилия.
 - c. Email.
2. После заполнения всех полей нужно нажать на кнопку «Добавить пользователя». Далее система отправляет на почту, указанную для создаваемого пользователя, ссылку для авторизации.
 - a. **Важно:** Для того, чтобы неактивный пользователь (тот, который отсутствует в приложении) мог зарегистрироваться в приложении и стать участником рабочего окружения, необходимо, чтобы был проставлен чек-бокс «Разрешить регистрацию пользователей по ссылке», который находится в [Редактировании рабочего окружения](#).

3.3.7. Активация/Деактивация пользователей внутри рабочего окружения

Чтобы заблокировать или разблокировать пользователя в рабочем окружении, необходимо найти раздел «Пользователи окружения». Данный раздел представляет из себя таблицу с полями. Далее необходимо в таблице найти столбец с управлением пользователями.

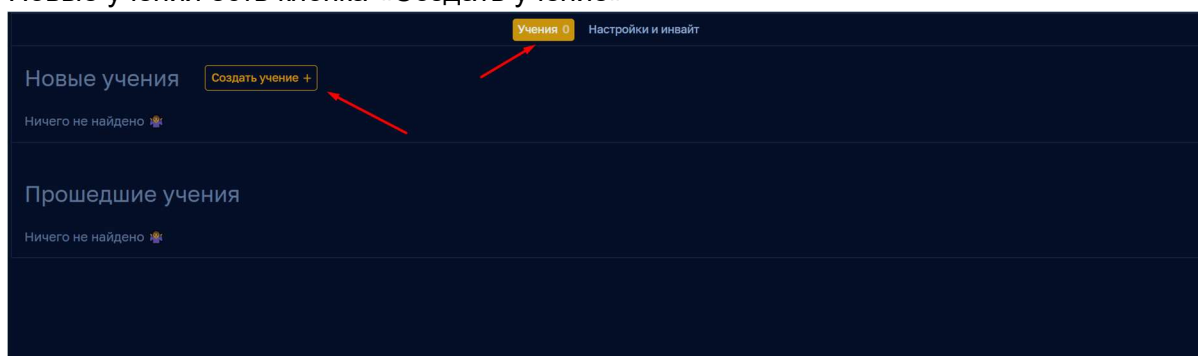
1. Пользователь нажимает на кнопку «Заблокировать». Система блокирует пользователя в системе.
2. Пользователь нажимает на кнопку ту же кнопку «Разблокировать». Система снова активирует пользователя в системе.

Пользователи окружения 5		
Имя	Email	Управление пользователями
OPS Синих	BlueOps@ya.ru	 Разблокировать
SOC Синих	BlueSoc@ya.ru	 Заблокировать
Лидер Синих	BlueLid@ya.ru	 Заблокировать
Хакер Красных	RedHak@ya.ru	 Заблокировать
Лидер Красных	RedLid@ya.ru	 Заблокировать

© CyberRange 2022

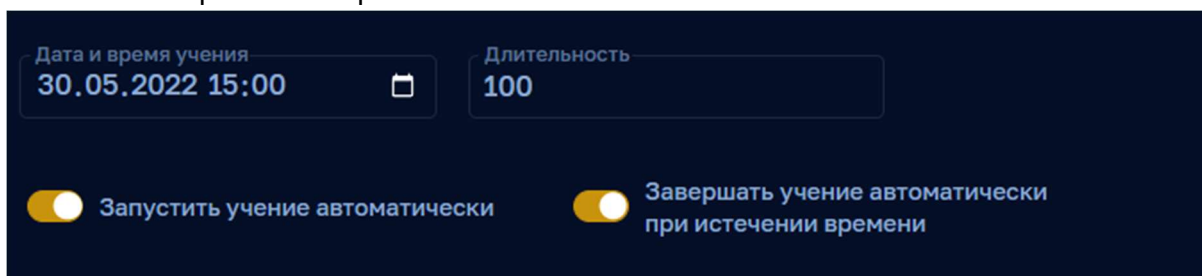
3.3.8. Создание учения

Для того чтобы создать учение, необходимо находиться в рабочем окружении, где необходимо создать само учение, далее нужно перейти во вкладку «Учения». Страница разделена на 2 логических раздела: Новые учения и Прошедшие учения. Около раздела Новые учения есть кнопка «Создать учение»



1. Пользователь нажимает на кнопку «Создать учение». Система открывает страницу для создания учения с обязательными полями:
 - a. Название.
 - b. Описание – необязательное поле.
 - c. Дата и время учения – записывается в определенном порядке (Дата.Месяц.Год Часы:Минуты).

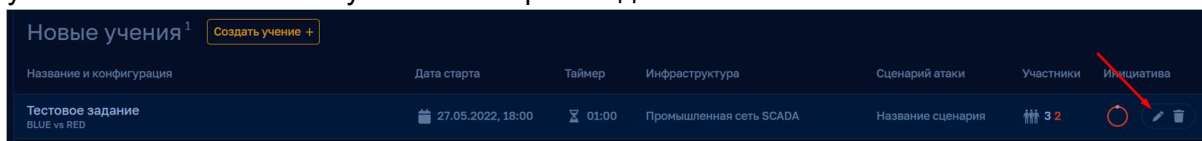
- i. **Важно:** дата и время предстоящего учения должны быть корректны, то есть дата и время учения не могут быть в прошлом времени.
- d. Длительность – необходимо записать сколько по времени будет длиться учение, время обязательно записывать в минутах.
- e. Автоматический запуск/завершение учения – учение также можно запустить и завершить автоматически, если выбраны оба пункта, если же пункты не будут выбраны, то пользователь управляет учением в реальном времени.



- i. Переключатель «Запустить учение автоматически».
 - ii. Переключатель «Завершать учение автоматически при истечении времени»
 - f. Инфраструктура – нужно выбрать инфраструктуру, которые заложены внутри системы.
 - g. Конфигурация учения – нужно выбрать из выпадающего списка вид учения:
 - i. Blue Team vs Red Team – нужно распределить студентов из рабочего окружения по командам.
 - 1. **Важно:** Обязательно в голубой команде должны быть роли: Лидер и SOC, а в красной команде обязательно присутствие Лидера.
 - ii. Red Team only – нужно выбрать студентов из рабочего окружения.
 - 1. **Важно:** Обязательно нужно выбрать Лидера команды.
 - iii. Blue Team vs Script – нужно выбрать студентов из рабочего окружения.
 - 1. **Важно:** Обязательно в команде должны быть роли: Лидер и SOC.
 - h. Выбрать сценарий атак – выбирается из предустановленного списка атак.
 - i. Переключатель включить генерацию трафика.
2. После заполнения всех полей, необходимо нажать кнопку «Создать учение».

3.3.9. Редактирование учения

Редактировать учения можно только те, которые находятся в разделе «Будущее учение» и не имеют статус «Сейчас происходит».



Новые учения ¹	Создать учение +						
Название и конфигурация	Дата старта	Таймер	Инфраструктура	Сценарий атаки	Участники	Инициатива	
Тестовое задание BLUE vs RED	27.05.2022, 18:00	01:00	Промышленная сеть SCADA	Название сценария	3 2		

1. Пользователь нажимает на кнопку «Редактировать учение». Система открывает страницу для редактирования учения с обязательными полями:
 - a. Название.
 - b. Описание – необязательное поле.
 - c. Дата и время учения – записывается в определенном порядке (Дата.Месяц.Год Часы:Минуты).
 - i. **Важно:** дата и время предстоящего учения должны быть корректны, то есть дата и время учения не могут быть в прошлом времени.
 - d. Длительность – необходимо записать сколько по времени будет длиться учение, время обязательно записывать в минутах.
 - e. Автоматический запуск/завершение учения – учение также можно запустить и завершить автоматически, если выбраны оба пункта, если же пункты не будут выбраны, то пользователь управляет учением в реальном времени.
 - i. Переключатель «Запустить учение автоматически».
 - ii. Переключатель «Завершать учение автоматически при истечении времени».
 - f. Инфраструктура – нужно выбрать инфраструктуру, которые заложены внутри системы.
 - g. Конфигурация учения – нужно выбрать из выпадающего списка вид учения:
 - i. Blue Team vs Red Team – нужно распределить студентов из рабочего окружения по командам.
 1. **Важно:** Обязательно в голубой команде должны быть роли: Лидер и SOC, а в красной команде обязательно присутствие Лидера.
 - ii. Red Team only – нужно выбрать студентов из рабочего окружения.
 1. **Важно:** Обязательно нужно выбрать Лидера команды.
 - iii. Blue Team vs Script – нужно выбрать студентов из рабочего окружения.
 1. **Важно:** Обязательно в команде должны быть роли: Лидер и SOC.
 - h. Выбрать сценарий атак – выбирается из предустановленного списка атак.
 - i. Переключатель включить генерацию трафика.
2. После заполнения всех полей, необходимо нажать кнопку «Создать учение».

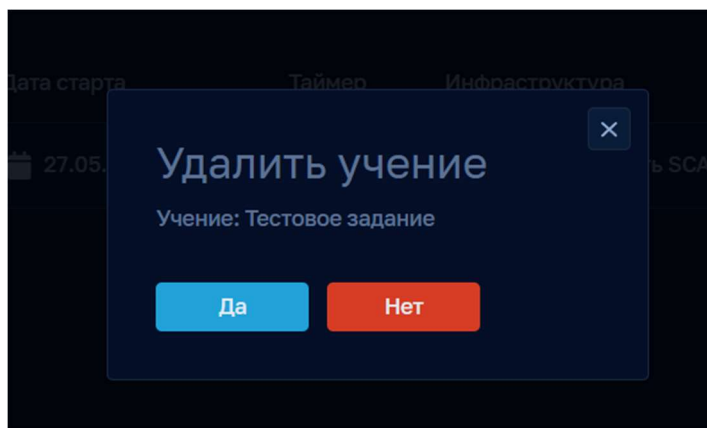
3.3.10. Удаление учения

Удалять учения можно только те, которые находятся в разделе «Будущее учение» и не имеют статус «Сейчас происходит».



1. Пользователь нажимает на кнопку «Удалить учение». Система открывает модальное окно с двумя ответами:
 - a. Да.

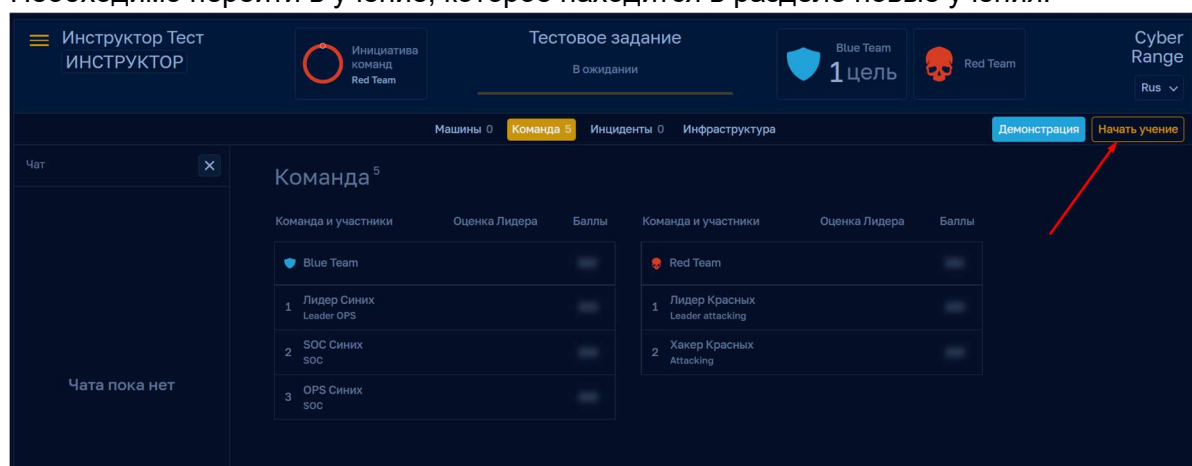
b. Нет.



2. Пользователь подтверждает удаление учения, нажимая кнопку да. Система удаляет учение из базы.

3.3.11. Старт учения

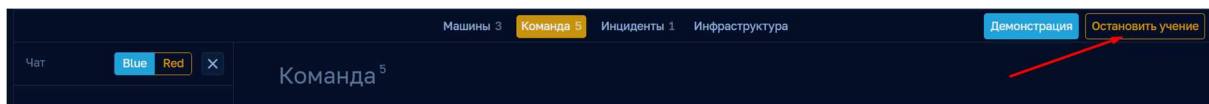
Старт учения может происходить по разному. Если пользователь выбрал автоматический запуск учения, то старт учения начинается в дату и время, которое установил пользователь. Если же пользователь не выбрал автоматический запуск учения, то поле дата и время несет только информационный характер. Необходимо перейти в учение, которое находится в разделе новые учения.



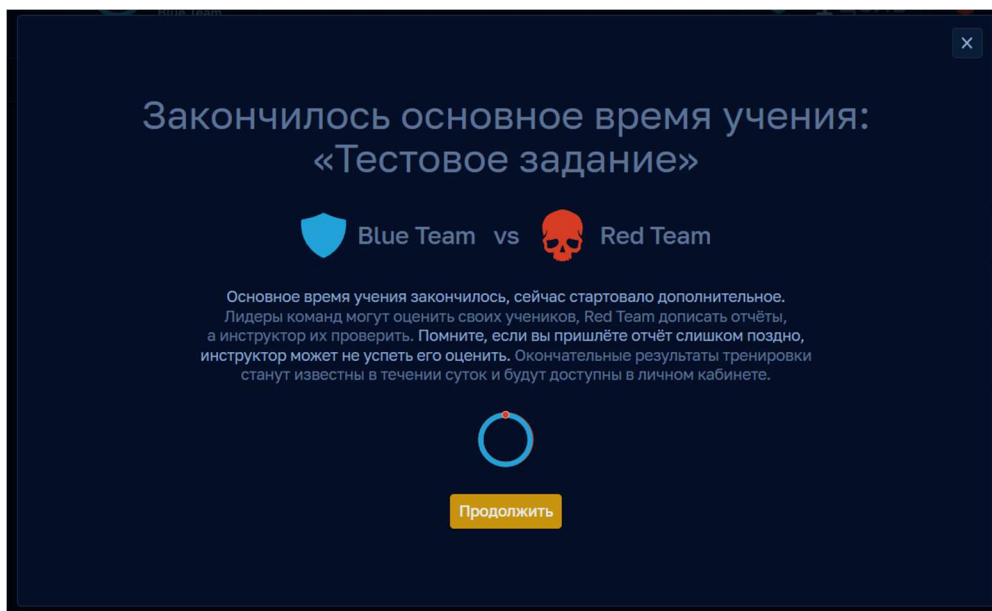
1. Пользователь нажимает на кнопку «Начать учение». Система открывает модальное окно с двумя ответами:
 - a. Да.
 - b. Нет.
2. Пользователь подтверждает о начале учения, нажимая кнопку «Да». Система активирует учение для студентов.

3.3.12. Остановить учение

Остановить учение можно только то, которое имеет статус «Сейчас происходит». Чтобы остановить учение, необходимо перейти в само учение.

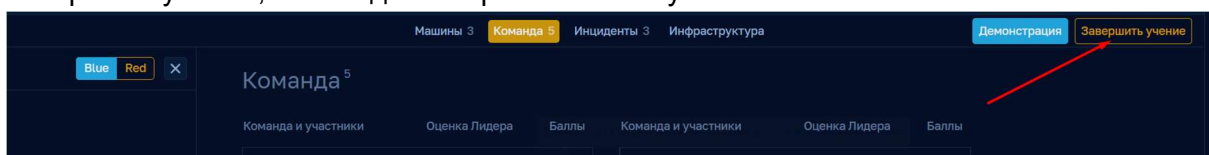


1. Пользователь нажимает на кнопку «Остановить учение». система открывает модальное окно с двумя ответами:
 - a. Да.
 - b. Нет.
2. Пользователь подтверждает об остановке учения, нажимая кнопку да. Система останавливает учение для студентов и открывает модальное окно с предупреждением.
 - a. **Важно:** Остановка учения это не пауза, это завершение основного обучения. Остановка учения нужна для написания отчетов и оценки работы. После остановки, продолжить учение невозможно, только завершить.



3.3.13. Завершения учения

Завершить учение можно только то, которое имеет статус «Остановлено». Чтобы завершить учение, необходимо перейти в само учение.



1. Пользователь нажимает на кнопку «Завершить учение». Система открывает модальное окно с двумя ответами:
 - a. Да.
 - b. Нет.

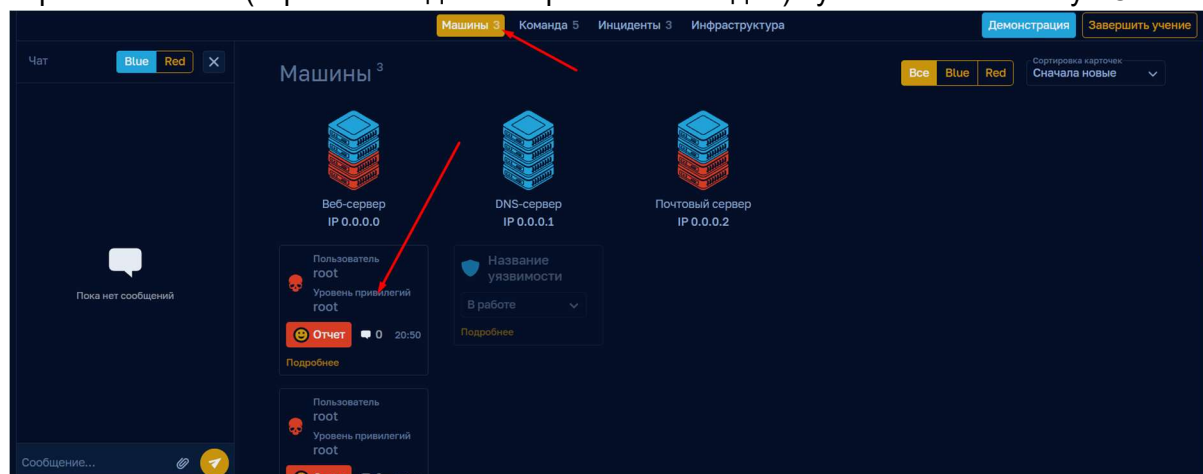
2. Пользователь подтверждает об остановке учения, нажимая кнопку «Да». Система завершает учение для студентов и демонстрирует для студентов их баллы.
3. После завершения учения никаких действий в учении произвести нельзя (выставить оценки, проверить отчеты и т.д.).

3.3.14. Оценка отчетов (Red Team)

Пользователь может оценивать только карточки взломов — карточки красной команды. Во вкладке «Команда», появится информация о проверке отчетов.

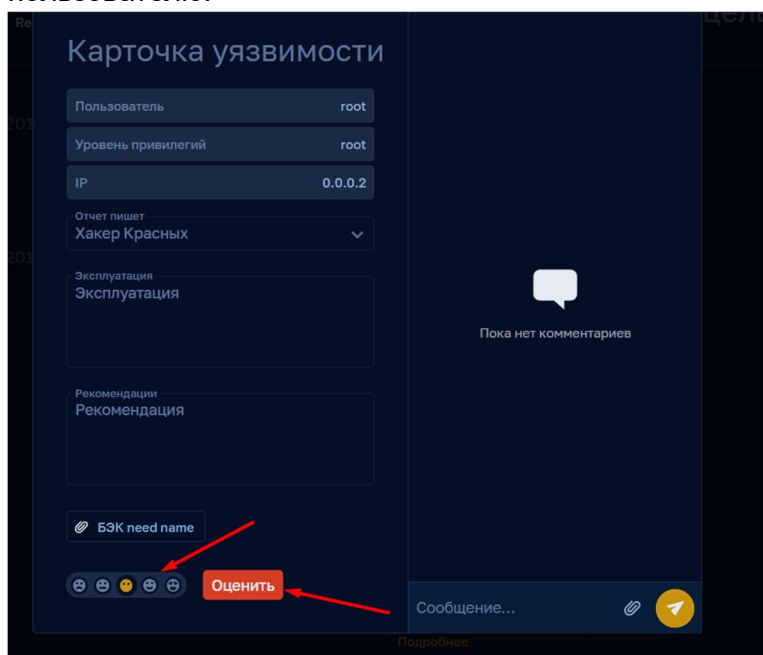


Также оценить карточки взломов можно, если перейти во вкладку «Машины». Далее на карточке взлома (карточка созданная красной командой) нужно нажать кнопку «Отчет».



1. Пользователь нажимает на кнопку «Отчет». Система открывает модальное окно с полями, которые недоступны для редактирования.
 - a. Пользователь.
 - b. Уровень привилегий.
 - c. IP.
 - d. Отчет пишет – в окне будет описан какой студент писал отчет по карточке.
 - e. Эксплуатация.
 - f. Рекомендации.

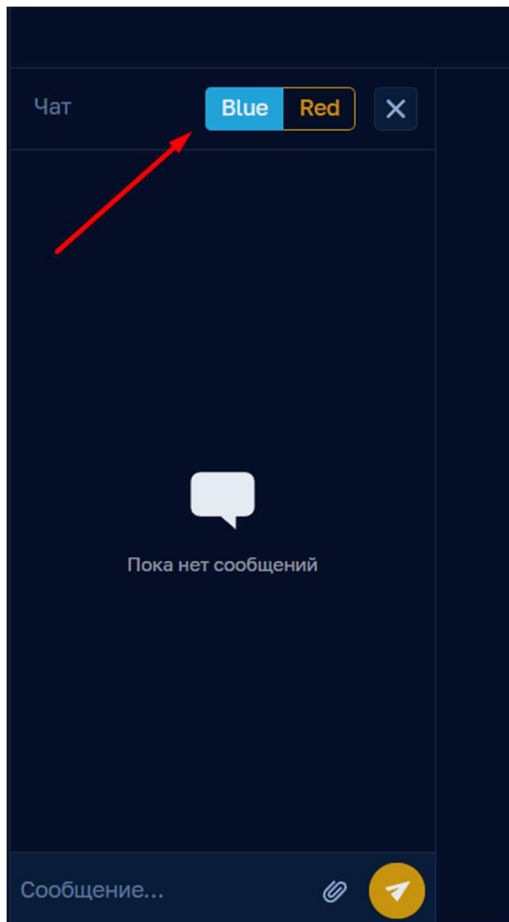
- g. Оценка в эмодзи – поле, которое доступно для редактирования пользователю.



- h. Чат – доступен пользователю как во время учения, так и после завершения.
2. Пользователь выбирает один из 5 эмодзи, тем самым оценивая карточку. Далее пользователь нажимает кнопку «Оценить». Система сохраняет ответ.
- a. **Важно:** После нажатия на кнопку «Оценить», оценку нельзя изменить.

3.3.15. Чат

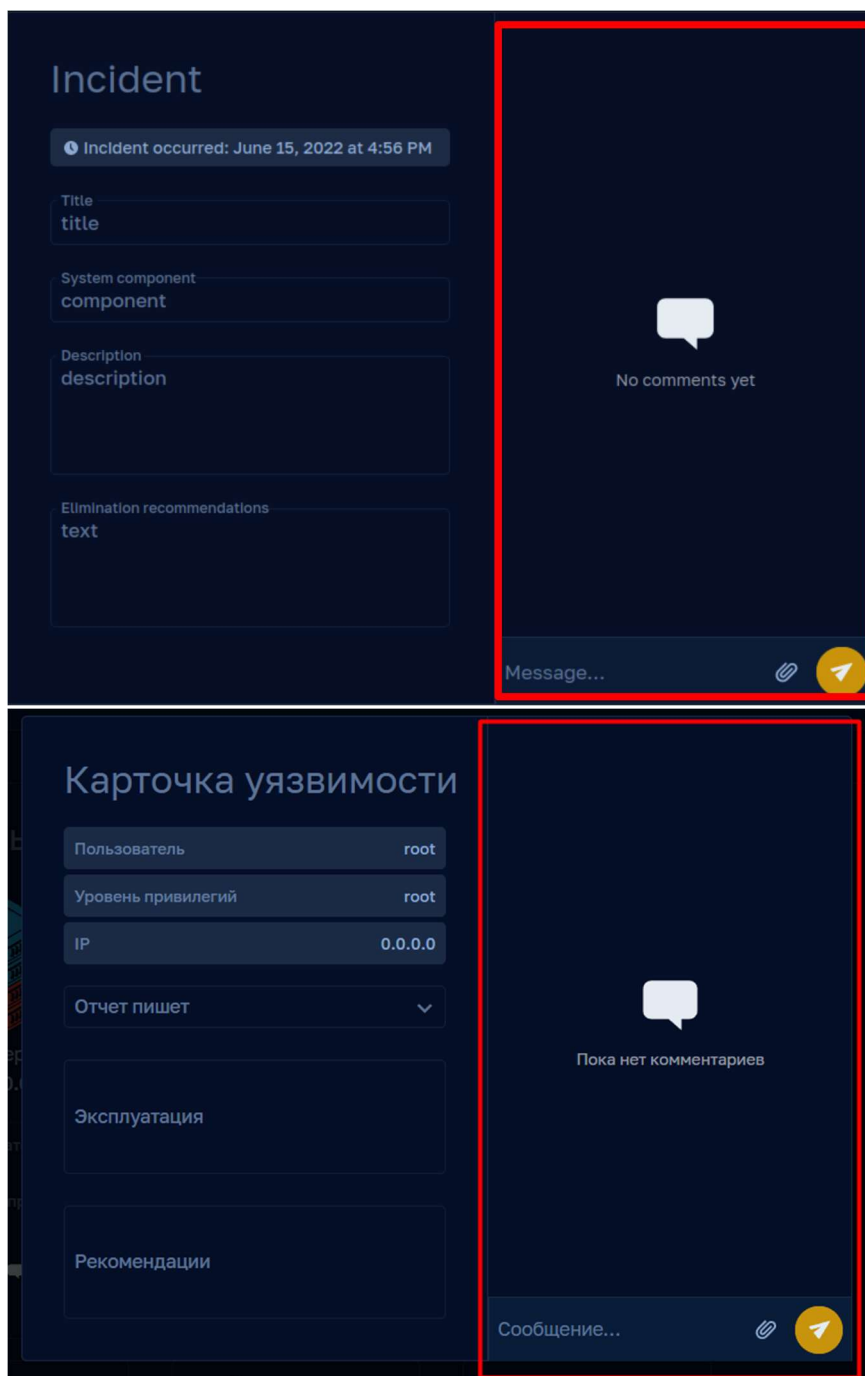
Пользователю доступны чаты обеих команд и с помощью переключения кнопок, пользователь видит чат обеих команд (Исключение, если тип учения выбран Red Team only или Blue Team vs Script, тогда доступен только чат для одной команды)



1. Пользователь может отвечать в чате обеим командам.
2. Пользователю доступен функционал добавления различных файлов в чат (Изображения/файлы различных расширений).
3. Пользователь также может скрыть чат.

3.3.16. Комментарии к карточкам

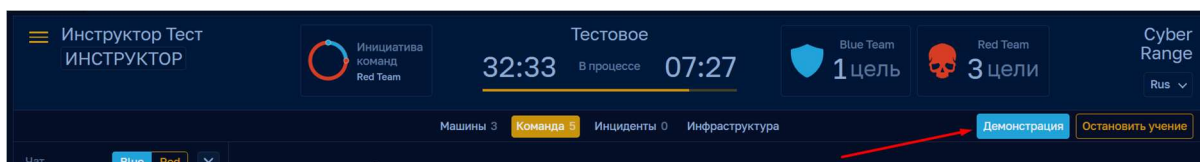
Пользователю доступны написания комментариев к карточкам взлома или инцидентов.



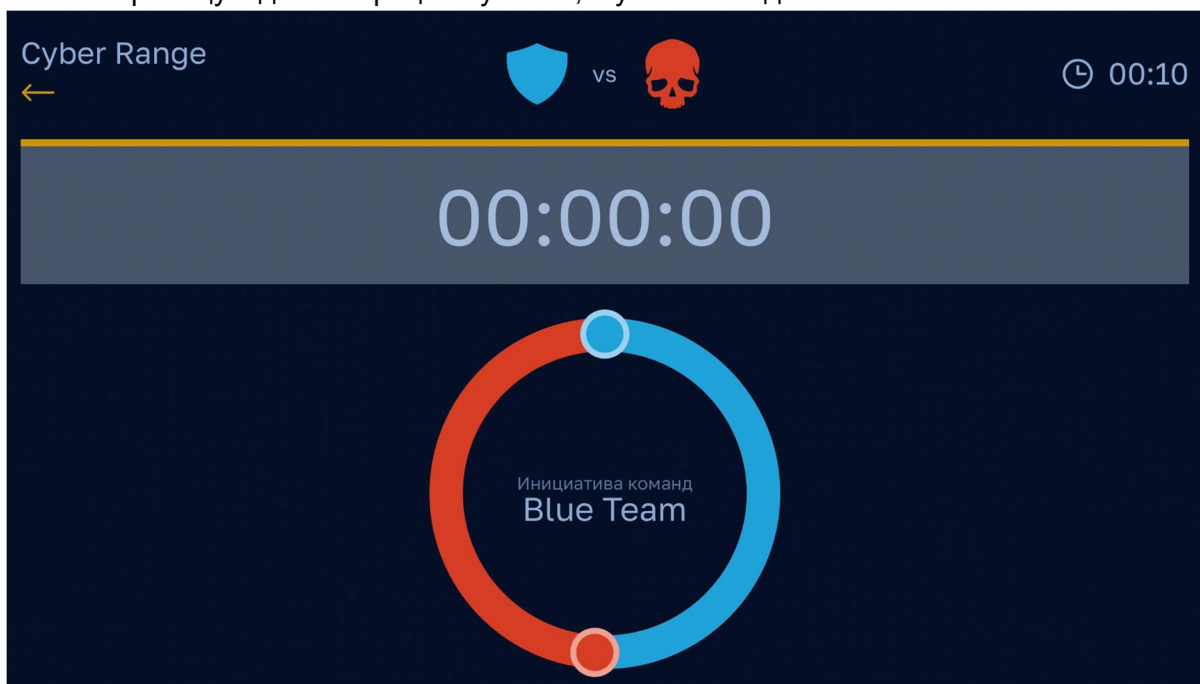
1. Пользователь открывает карточку инцидента/карточку взлома. Система открывает модальное окно с полями недоступные для редактирования.
2. Пользователь пишет комментарий к карточке.
 - a. **Важно:** Написание комментариев к карточкам доступно всегда. Даже после полного завершения учения.

3.3.17. Демонстрация учения

Пользователь может посмотреть демонстрацию по учению которое имеет статус «Сейчас происходит». Необходимо перейти в само учение, которое необходимо посмотреть.



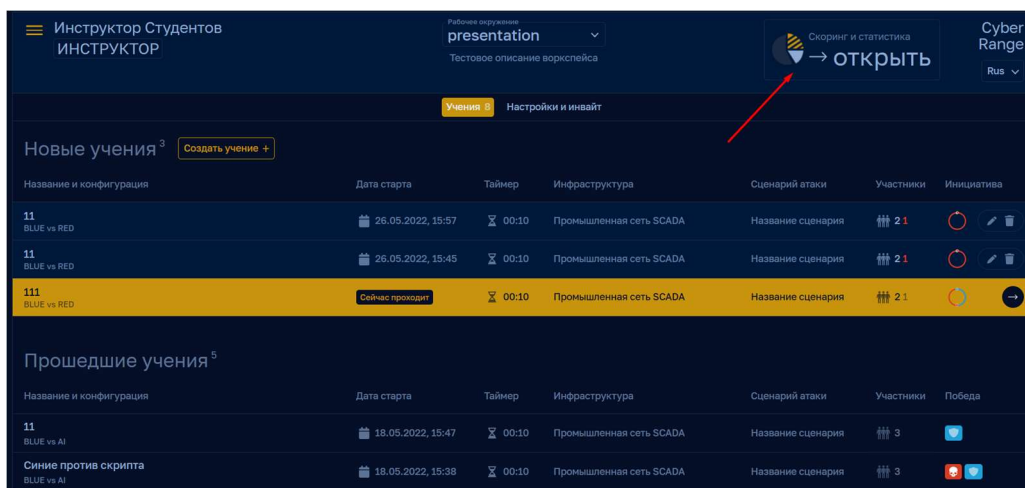
1. Пользователь нажимает на кнопку «Демонстрация». Система открывает страницу с демонстрацией учения, в учение входят такие поля:



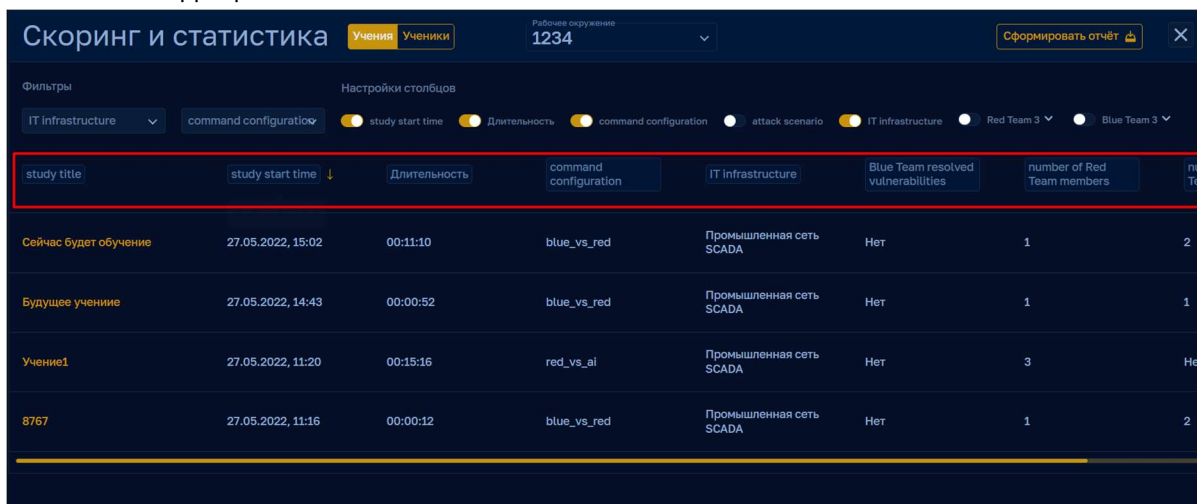
- a. Тип учения. Отображается в виде иконок команд:
 - i. Blue Team and Red Team.
 - ii. Blue Team only.
 - iii. Blue Team vs Script.
- b. Время сколько длится учения – пишется в верхнем правом углу.
- c. Время до окончания учения – время движется в обратном порядке.
- d. Индикатор прогресса между команд.
 - i. Исключение, если выбрана конфигурация учения Red Team only или Blue Team vs Scrip, тогда отображается количество хостов().
 - ii. Исключение, если учение не запущено, тогда отображается заглушка «Учение в режиме ожидания»

3.3.18. Просмотр статистики по учениям

Пользователь может просмотреть статистику по всем учениям или ученикам. Необходимо находиться в рабочем окружении, где проходили учения и нажать на кнопку «Скоринг и Статистика».



1. Пользователь нажимает на кнопку «Скоринг и Статистика». Система открывает страницу. По всем столбцам есть фильтрация и сортировка, где данные можно сортировать по любому столбцу в двух порядках: восходящий, нисходящий.



2. Пользователь нажимает на любой столбец. Система производит сортировку, без загрузки страницы.
3. Пользователь также может просмотреть статистику не только по учениям, но и по ученикам, с помощью переключения кнопок «Учение»/«Ученики». При переключении на учеников открывается таблица по ученикам.

3.3.19. Настройка столбцов со статистикой

Пользователь может настраивать статистику для своего удобства и отображать только те столбцы, которые ему необходимы для проверки. Пользователь с помощью переключателя может скрыть тот или иной столбец.

Скоринг и статистика

Учения

Ученики

Рабочее окружение

1234

Сформировать отчёт

✕

Фильтры

IT infrastructure

command configuration

Настройки столбцов

study start time

Длительность

command configuration

attack scenario

IT infrastructure

Red Team 3

Blue Team 3

study title

study start time

Длительность

command configuration

IT infrastructure

Blue Team resolved vulnerabilities

number of Red Team members

number of Blue Team members

Сейчас будет обучение	27.05.2022, 15:02	00:11:10	blue_vs_red	Промышленная сеть SCADA	Нет	1	2
Будущее учение	27.05.2022, 14:43	00:00:52	blue_vs_red	Промышленная сеть SCADA	Нет	1	1
Учение1	27.05.2022, 11:20	00:15:16	red_vs_ai	Промышленная сеть SCADA	Нет	3	Нет
8767	27.05.2022, 11:16	00:00:12	blue_vs_red	Промышленная сеть SCADA	Нет	1	2

1. Пользователь нажимает на переключатель любого столбца. Система скрывает/открывает столбец.

3.3.20. Формирование отчета со статистикой

Пользователю доступно формирование отчета по учениям, которые находятся в рабочем окружении. Для этого необходимо находиться в рабочем окружении, по которому хотим выгрузить отчет.

1. Пользователь переходит на страницу «Скоринг и статистика».
2. Настраивает статистику как ему удобно.
3. Нажимает на кнопку «Сформировать отчет». Система генерирует CSV файл и сохраняет на ПК пользователя.

Скоринг и статистика

УченияУченики

Рабочее окружениеpresentation

Сформировать отчёт

Фильтры

Сбросить фильтры

IT infrastructure

command configuration

study start time

Длительность

command configuration

attack scenario

IT infrastructure

Red Team 3

Blue Team 3

study title

study start time

Длительность

command configuration

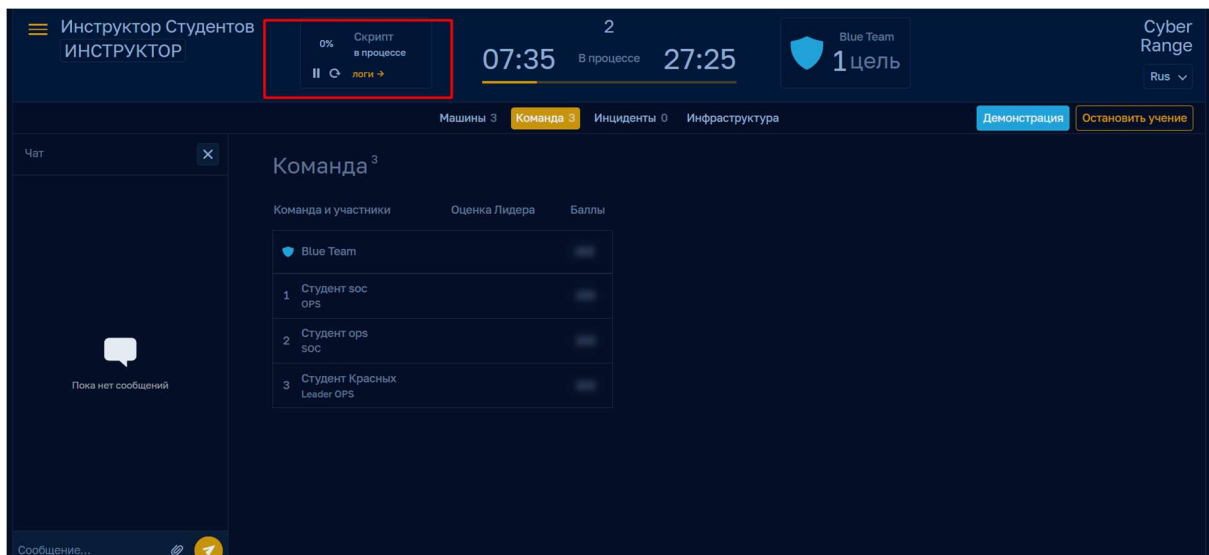
attack scenario

IT infrastructure

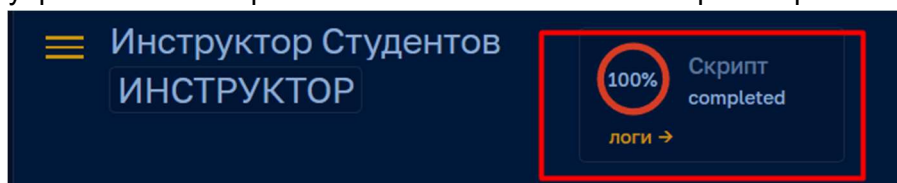
Тестовое учение	17.05.2022, 21:18	00:00:05	blue_vs_red	Название сценария	Промышленная сеть SCADA
Учение для презентации	17.05.2022, 21:44	00:00:10	blue_vs_red	Название сценария	Промышленная сеть SCADA
Учение по предотвращению хакерских атак	18.05.2022, 15:19	00:00:10	blue_vs_red	Название сценария	Промышленная сеть SCADA

3.3.21. Управление скриптом атаки в конфигурации учения Blue Team vs Script

Пользователь может управлять работой скрипта, когда конфигуратор учения выбран, как Blue Team vs Script. Для того, чтобы управлять скриптом, пользователь должен находиться в учении.



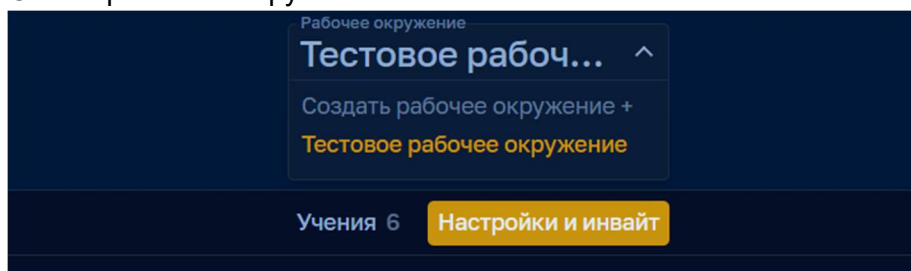
1. Пользователь может управлять скриптом:
 - a. Запустить скрипт.
 - b. Поставить на паузу.
 - c. Перезагрузить – при перезагрузке весь прогресс скрипта сбрасывается до нуля.
 - d. Посмотреть логи скрипта.
2. **Важно:** Если скрипт отработал до 100%, пользователь больше не может управлять скриптом и только просмотреть его логи.



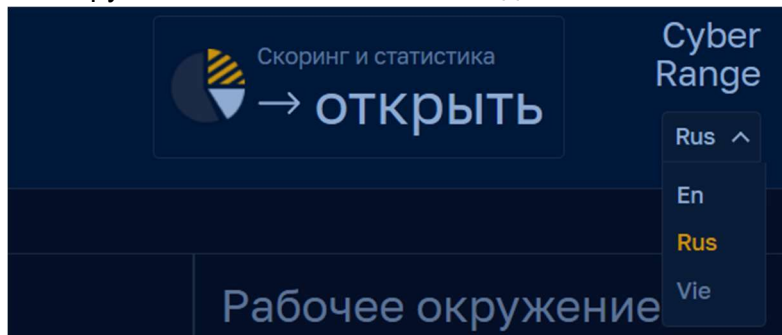
3.3.22. Первостепенные функции

Пользователю также доступны такие функции как:

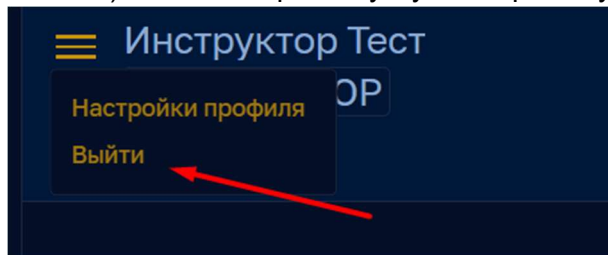
1. Смена рабочего окружения



2. Сменить язык – доступны три языка: Русский, Английский, Вьетнамский, планируется добавить Бирманский



3. Выйти из профиля – необходимо нажать бургер-меню (три горизонтальные полосы) в левом верхнем углу и выбрать пункт «Выйти».



3.4. Студент

Основной функционал студента:

- [Авторизация](#)
- [Настройка профиля](#)
- [Регистрация](#)
- [Функционал зависящий от роли в учении:](#)
 - [Blue Team](#)
 - [SOC](#)
 - [Создание инцидента](#)
 - [Написание комментария к карточке инцидента](#)
 - [Общение в чате](#)
 - [Leader](#)
 - [Назначение инцидента](#)
 - [Голосование за карточку инцидента](#)
 - [Обработка инцидента](#)
 - [Написание комментария к карточке инцидента](#)
 - [Общение в чате](#)
 - [Оценка товарищей по команде после завершения учения](#)
 - [OPS](#)
 - [Голосование за карточку инцидента](#)
 - [Обработка инцидента](#)
 - [Написание комментария к карточке инцидента](#)
 - [Общение в чате](#)
 - [Red Team](#)
 - [Attacking](#)
 - [Создание карточки взлома](#)

- [Написание отчета для карточки взлома](#)
- [Редактирование карточки уязвимости](#)
- [Написание комментария к карточке взлома](#)
- [Общение в чате](#)
- [Leader](#)
 - [Назначение карточки взлома](#)
 - [Создание карточки взлома](#)
 - [Написание отчета для карточки взлома](#)
 - [Редактирование карточки уязвимости](#)
 - [Написание комментария к карточке взлома](#)
 - [Общение в чате](#)
 - [Оценка товарищей по команде после завершения учения](#)
- [Первостепенные функции](#)

Во всем разделе 3.4. под термином пользователь будет использоваться роль Студента для упрощения написания.

3.4.1. Авторизация

Смотри пункт 3.1.1. – [авторизация](#)

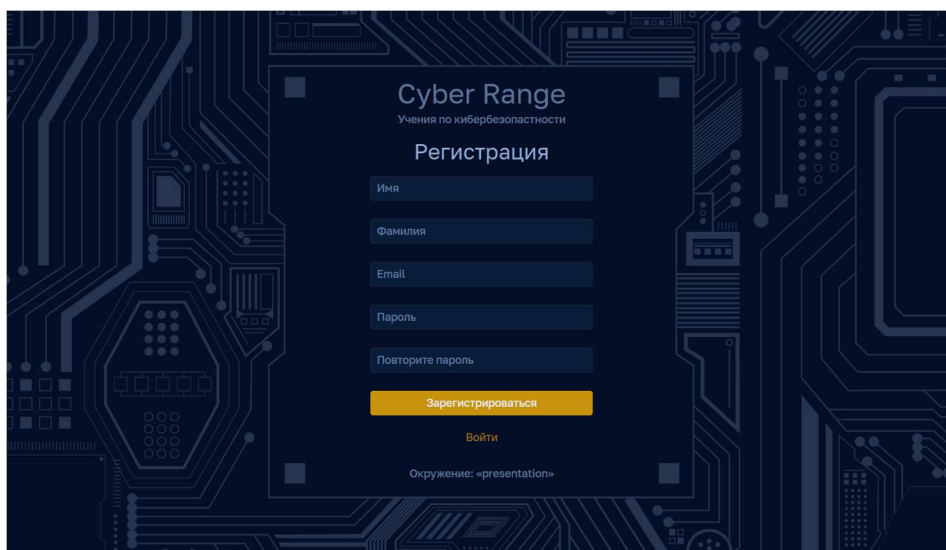
3.4.2. Настройка профиля

Смотри пункт 3.1.2. – [настройка профиля](#)

3.4.3. Регистрация

Пользователю доступна регистрация в приложении. На регистрацию пользователь может попасть только с помощью 2х случаев:

1. Ссылка на рабочее окружение.
2. Приглашение на почту в рабочее окружение.



1. При открытии приложения система открывает страницу с обязательными полями:

- a. Имя.
 - b. Фамилия.
 - c. Email.
 - d. Пароль.
 - e. Повторите пароль – должен полностью совпадать с полем «Пароль»
2. Пользователь нажимает на кнопку «Зарегистрироваться», Далее перед пользователем открывается интерфейс приложения, следовательно пользователь зарегистрировался в системе.
 - a. Если пользователь ранее был зарегистрирован в системе, есть кнопка Войти. При нажатии на нее открывается интерфейс [авторизации](#).

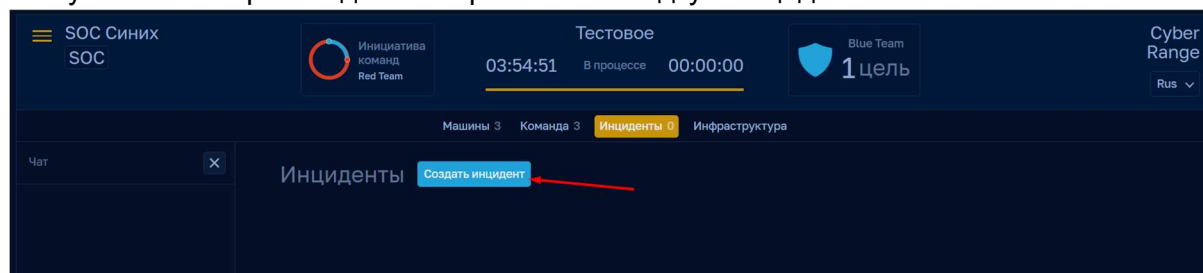
3.4.4. Функционал зависящий от роли в учении

3.4.4.1. Blue Team

3.4.4.1.1. SOC

3.4.4.1.1.1. Создание инцидента

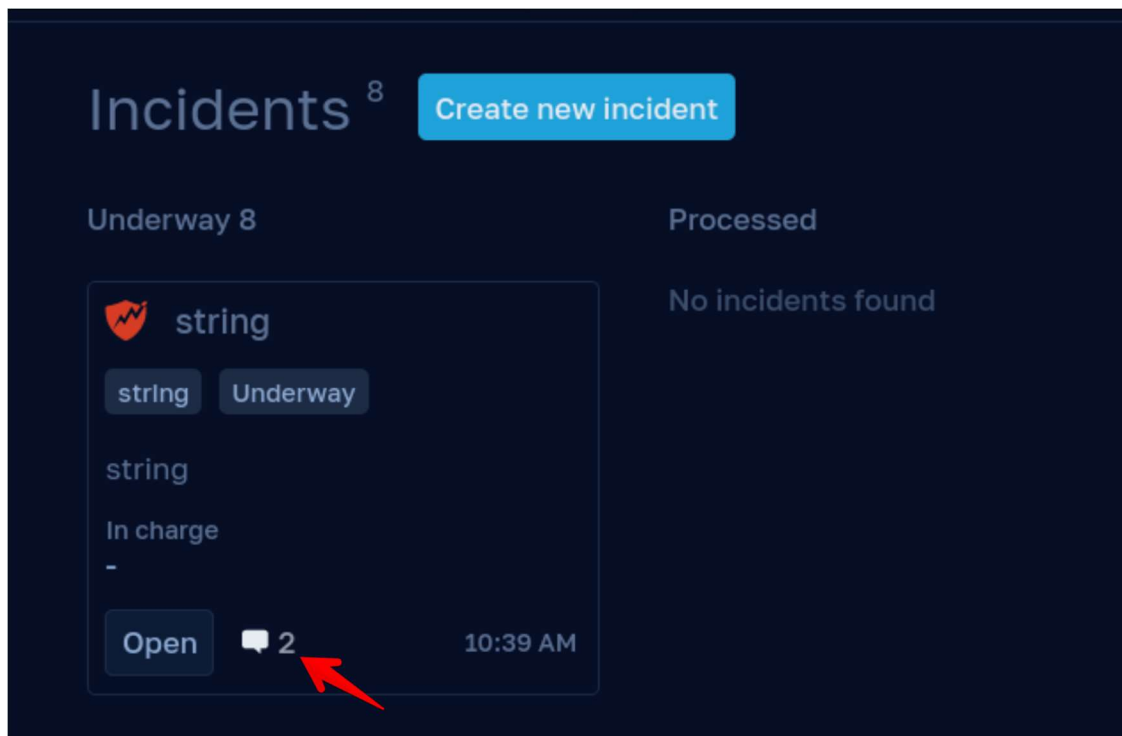
Пользователю с ролью SOC допущено только создание карточек инцидента. Для того чтобы создать карточку, пользователю необходимо находится в учении, которое имеет статус «Сейчас происходит» и перейти на вкладку «Инциденты» .



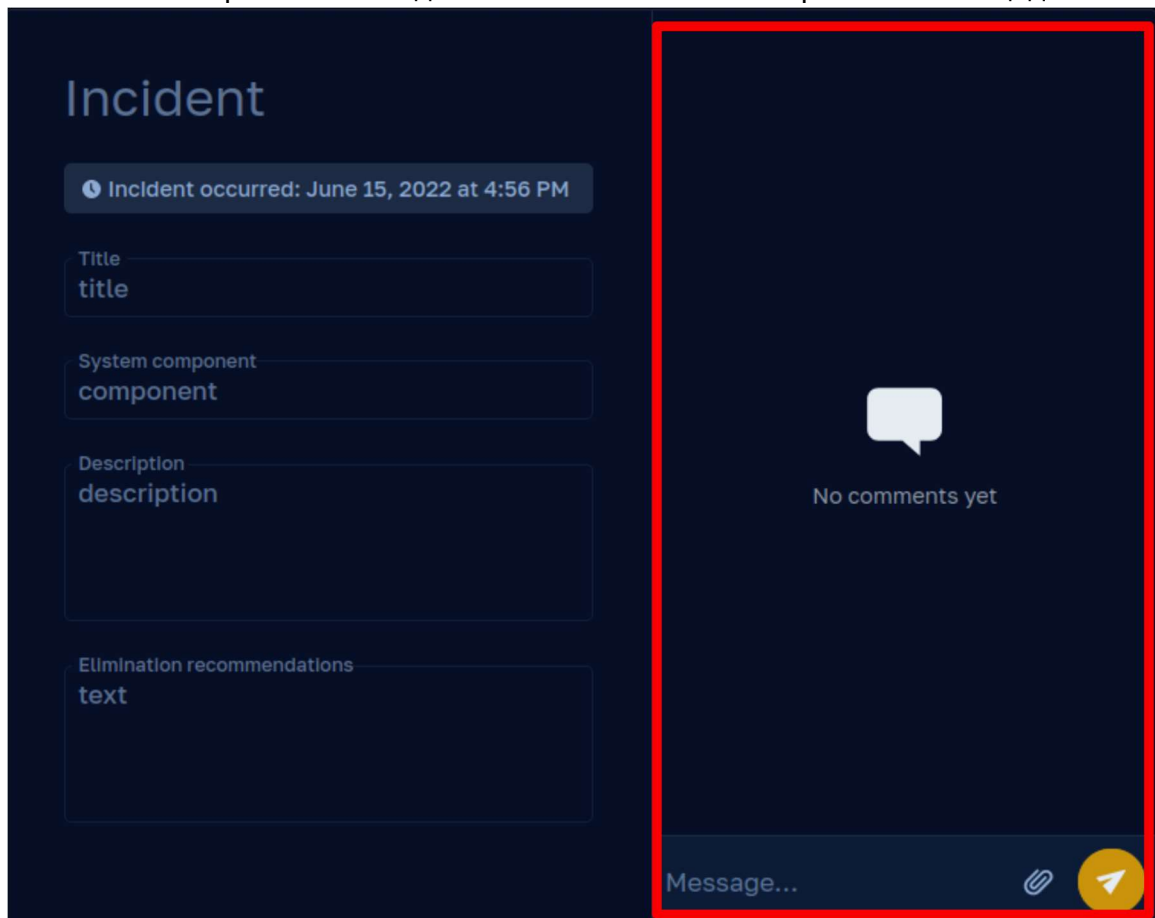
1. Пользователь нажимает на кнопку «Создать инцидент». Система открывает модальное окно с обязательными полями для заполнения:
 - a. Название.
 - b. Компонент системы.
 - c. Описание.
 - d. Рекомендации по устранению.
 - e. Приложить файл – дополнительный функционал, не обязателен к заполнению.
2. После заполнения всех полей нужно нажать на кнопку «Создать инцидент». Далее в системе появляется карточка инцидента и ей занимаются другие пользователи голубой команды.
 - a. **Важно:** После создания инцидента, его невозможно отредактировать.

3.4.4.1.1.2. Написание комментария к карточке инцидента

После создания инцидента, всей команде Blue Team доступно общение в комментариях карточки. Для того чтобы написать комментарий, пользователю необходимо находится в учении, которое имеет статус «Сейчас происходит» и перейти на вкладку «Инциденты».



1. Пользователь нажимает на кнопку «Открыть» или на значок комментария. Система открывает модальное окно с карточкой инцидента.

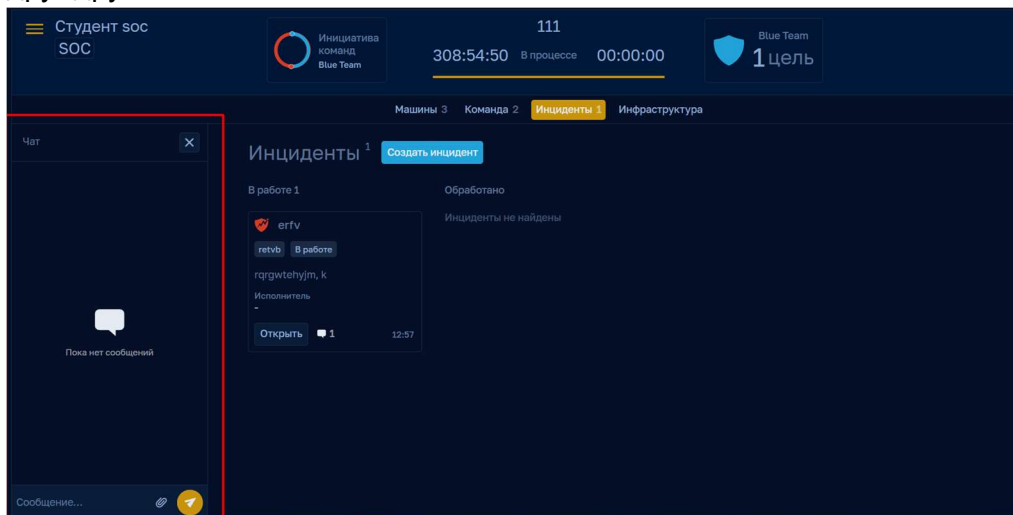


2. Пользователю доступно написание комментариев в карточке инцидента.

- а. **Важно:** Написание комментариев к карточкам доступно всегда. Даже после полного завершения учения.

3.4.4.1.1.3. Общение в чате

Любой команде доступен их группой чат, где они могут поддерживать общение. Чат находится внутри учения с левой стороны. Противоположные команды не видят чаты друг друга.



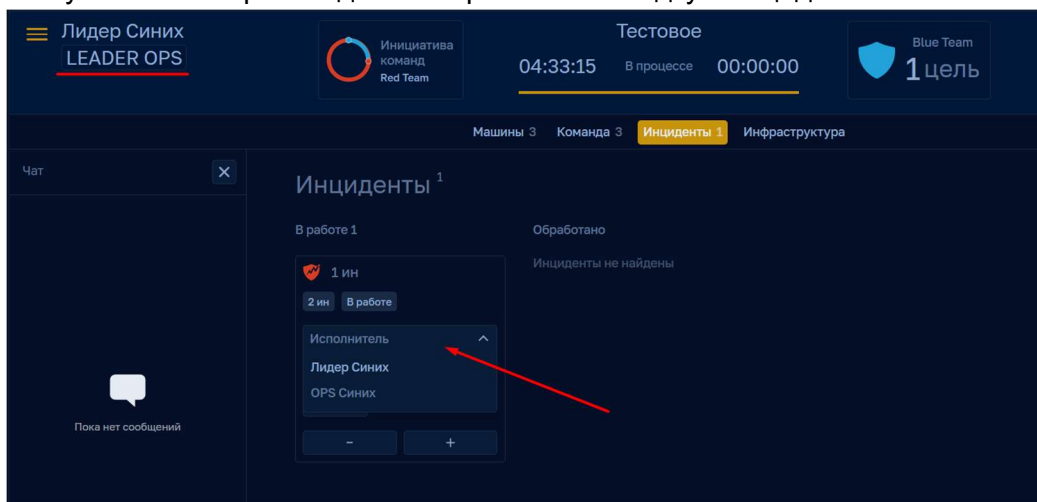
1. Пользователь пишет сообщение в чат. Система отображает сообщение пользователя всем сокомандникам.

- а. **Важно:** Чат учения доступен всем, даже после завершения полного учения.

3.4.4.1.2. Leader

3.4.4.1.2.1. Назначение инцидента

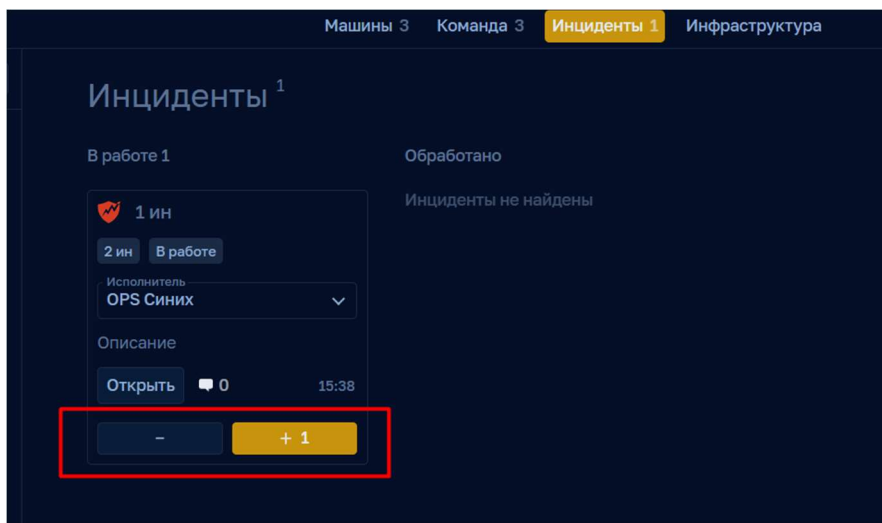
Лидер команды может назначать созданные инциденты на сокомандников (Пользователей с ролью OPS), либо назначить на самого себя. Для того чтобы назначить карточку, пользователю необходимо находиться в учении, которое имеет статус «Сейчас происходит» и перейти на вкладку «Инциденты».



1. Пользователь видит карточку инцидента и нажимает на селект, где выпадает список из сокомандников на кого можно назначить инцидент.
2. Пользователь выбирает пользователя на кого поставить инцидент, либо выбираем себя. Система назначает инцидент на выбранного пользователя.

3.4.4.1.2.2. Голосование за карточку инцидент

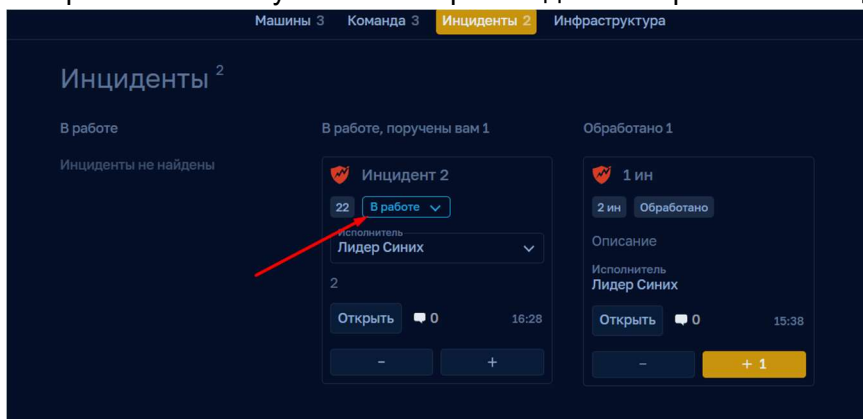
Пользователи с ролями Лидер и OPS, могут оценивать карточки инцидентов, тем самым голосуя за самые лучшие и худшие инциденты. Для того чтобы проголосовать за карточку, пользователю необходимо находится в учении, которое имеет статус «Сейчас происходит» и перейти на вкладку «Инциденты».



1. Пользователь видит карточку инцидента и нажимает на одну из кнопок «-» или «+». Система, тем самым считывает выбор пользователя и отображает на карточке голосование.
2. Голосовать за карточку можно только пока идет учение, после остановки учения голосовать за карточку нельзя.

3.4.4.1.2.3. Обработка карточки инцидента

Пользователи с ролями Лидер и OPS, могут обрабатывать карточки инцидентов. Для того чтобы обработать карточку, пользователю необходимо находится в учении, которое имеет статус «Сейчас происходит» и перейти на вкладку «Инциденты».



1. Пользователь видит карточку, которая поручена ему, если пользователь обработал карточку, он может изменить статус карточки на «Обработано».
2. Пользователь нажимает на селект и выбирает статус «Обработано». Система автоматически переносит карточку в колонку Обработано.
 - а. **Важно:** При изменении статуса карточки на «Обработано», изменить статус вновь невозможно.

3.4.4.1.2.4. Написание комментария к карточке инцидента

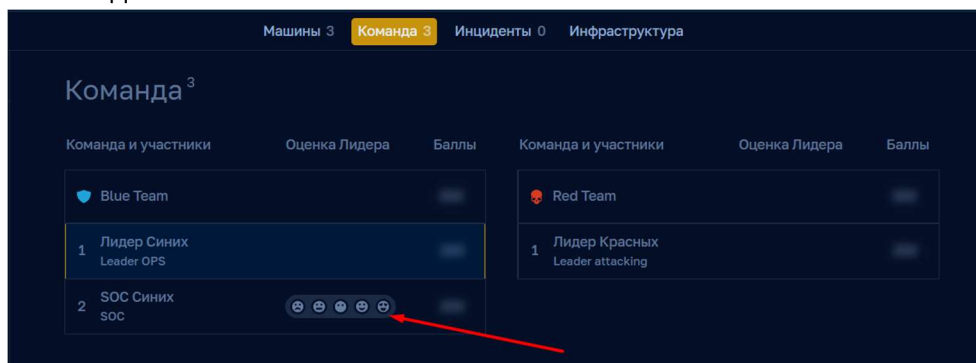
Смотри пункт 3.4.4.1.1.2. – [Написание комментария к карточке инцидента](#)

3.4.4.1.2.5. Общение в чате

Смотри пункт 3.4.4.1.1.3. – [Общение в чате](#)

3.4.4.1.2.6. Оценка товарищей по команде после завершения учения

После завершения учения, Лидер команды должен оценить работу своих сокомандников. Для того чтобы оценить сокомандника, пользователю необходимо находится в учении, которое имеет статус «Остановлено» и перейти на вкладку «Команда».



1. Пользователь видит оценочную шкалу напротив имени сокомандника и выбирает один из 5 эмодзи, тем самым оценивая работу во время учения.
 - а. Оценка сохранится только после завершения учения

3.4.4.1.3. OPS

3.4.4.1.3.1. Голосование за карточку инцидента

Смотри пункт 3.4.4.1.2.2. – [Голосование за карточку инцидента](#)

3.4.4.1.3.2. Обработка карточки инцидента

Смотри пункт 3.4.4.1.2.3. – [Обработка карточки инцидента](#)

3.4.4.1.3.3. Написание комментария к карточке инцидента

Смотри пункт 3.4.4.1.1.2. – [Написание комментария к карточке инцидента](#)

3.4.4.1.3.4. Общение в чате

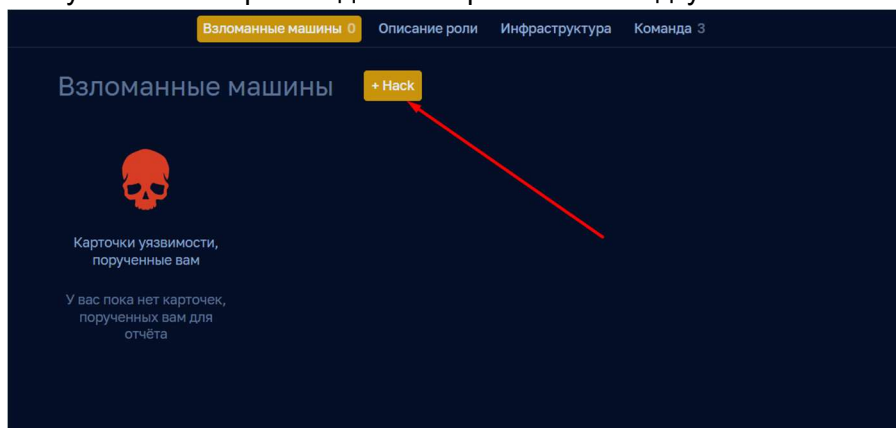
Смотри пункт 3.4.4.1.1.3. – [Общение в чате](#)

3.4.4.2. Red Team

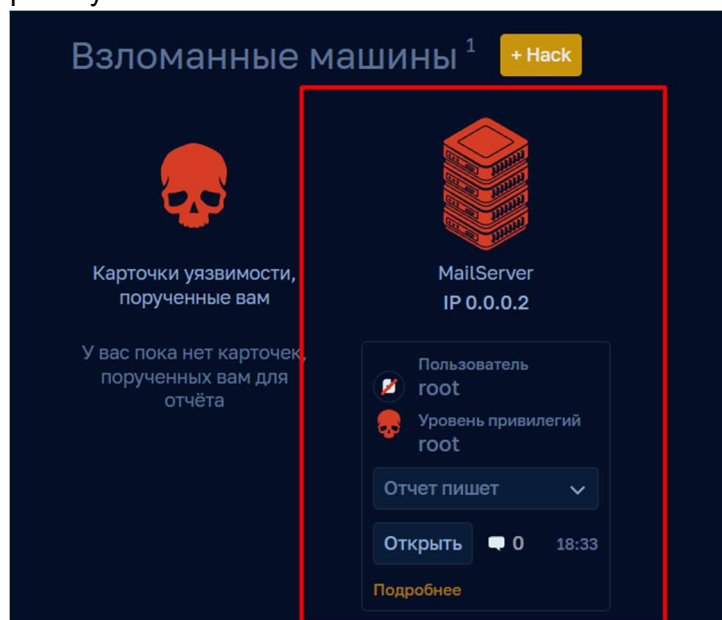
3.4.4.2.1. Attacking

3.4.4.2.1.1. Создание карточки взлома

Пользователю с ролью Лидер и Attacking могут создавать карточки взлома. Для того чтобы создать карточку, пользователю необходимо находиться в учении, которое имеет статус «Сейчас происходит» и перейти на вкладку «Взломанные машины».



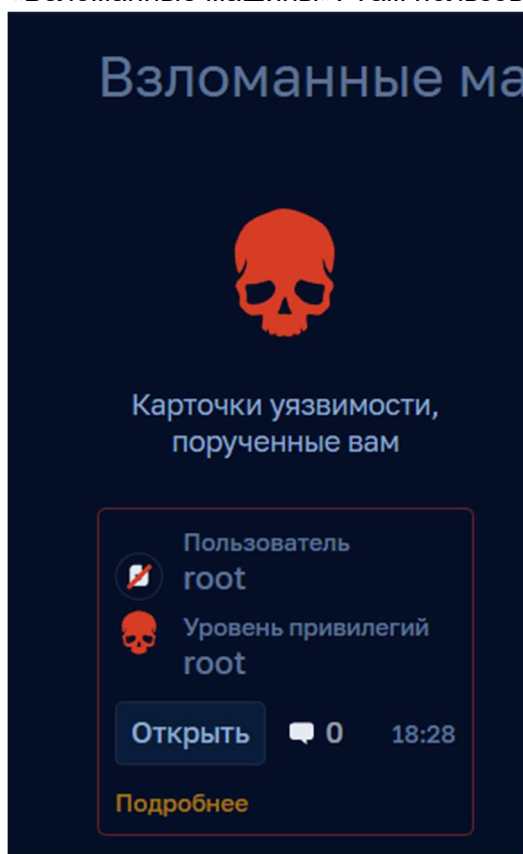
1. Пользователь нажимает на кнопку «Hack». Система создает карточку, которую необходимо кому-то обработать. Это временная кнопка, созданная для тестирования. В реальных условиях пользователю необходимо загрузить на взламываемую машину файл .md.
2. Пока лидер не назначит карточку на участника команды, ее нельзя взять в работу.



3.4.4.2.1.2. Написание отчета для карточки взлома

Пользователи с ролями Лидер и Attacking, могут обрабатывать карточки взломов. Для того чтобы обработать карточку, пользователю необходимо находиться в учении,

которое имеет статус «Сейчас происходит» или «Остановлено» и перейти на вкладку «Взломанные машины». Там пользователь увидит карточки назначенные ему.



1. Пользователь нажимает внутри карточки на кнопку «Открыть». Система открывает модальное окно с обязательными полями для заполнения отчета:
 - a. Пользователь – не редактируется.
 - b. Уровень привилегий – не редактируется.
 - c. IP – не редактируется.
 - d. Отчет пишет – не редактируется.
 - i. Исключение, если выбрана роль лидера, он может назначить отчет на другого пользователя.
 - e. Эксплуатация – обязательное поле для сохранения отчета.
 - f. Рекомендации – обязательное поле для сохранения отчета.
 - g. Приложить файл – дополнительный функционал, не обязателен к заполнению.

Карточка уязвимости

Пользователь root

Уровень привилегий root

IP 0.0.0.2

Отчет пишет
Хакер Красных

Эксплуатация

Рекомендации

Приложить файлы

Сохранить

Пока нет комментариев

Сообщение...

2. После заполнения всех полей нужно нажать на кнопку «Сохранить».

3.4.4.2.1.3. Редактирование карточки уязвимости

Пользователи с ролями Лидер и Attacking, могут редактировать карточки взломов. Для того чтобы отредактировать карточку, пользователю необходимо находится в учении, которое имеет статус «Сейчас происходит» и перейти на вкладку «Взломанные машины». Там пользователь увидит карточки назначенные ему.

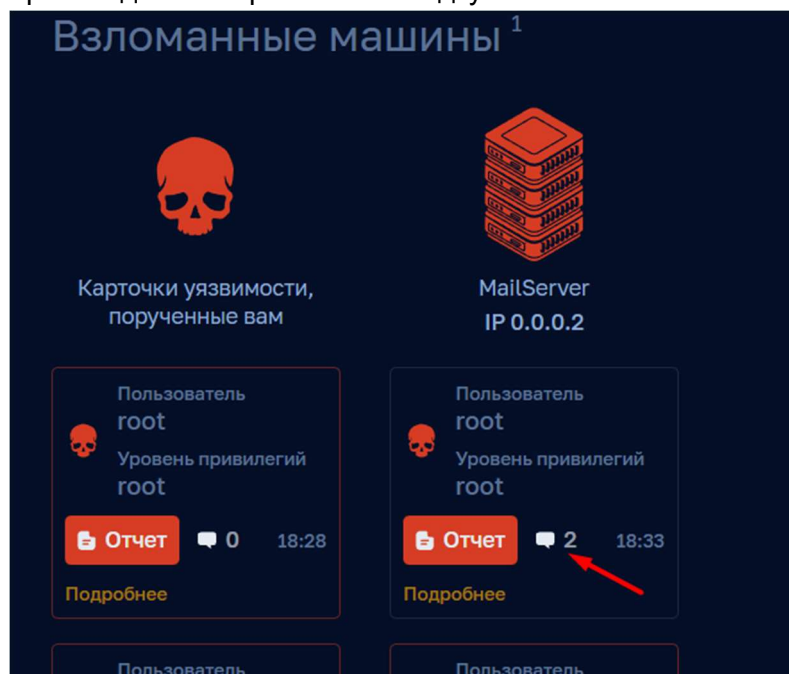
Пользователь на которого была назначена карточка взлома, может ее отредактировать.

Важно: Лидер может редактировать все карточки.

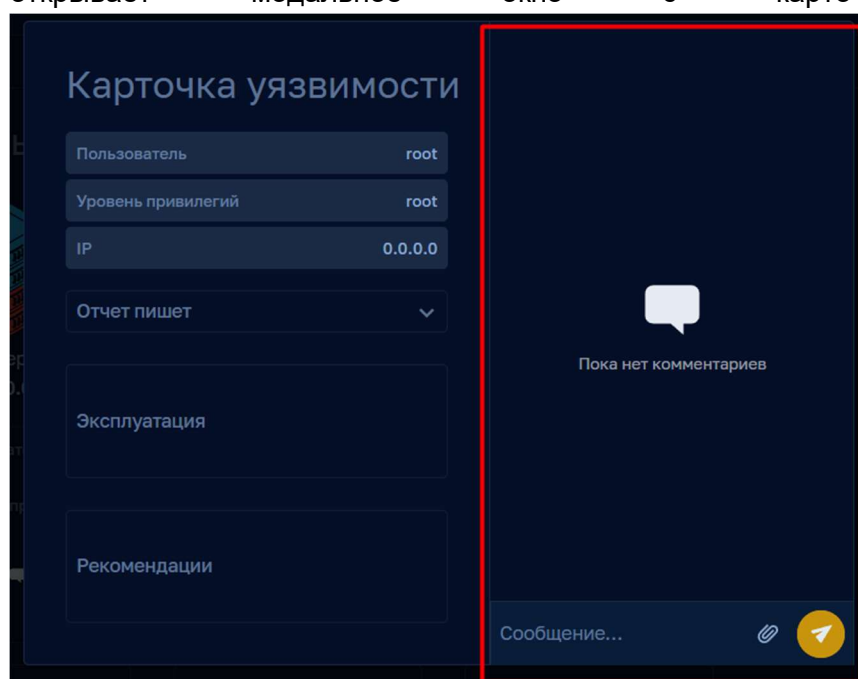
1. Пользователь нажимает внутри карточки на кнопку «Отчет». Система открывает модальное окно с обязательными полями для редактирования:
 - a. Пользователь – не редактируется.
 - b. Уровень привилегий – не редактируется.
 - c. IP – не редактируется.
 - d. Отчет пишет – не редактируется.
 - i. Исключение, если выбрана роль лидера, он может назначить отчет на другого пользователя.
 - e. Эксплуатация – доступна для редакции и является обязательным полем для сохранения отчета.
 - f. Рекомендации – доступна для редакции и является обязательным полем для сохранения отчета.
 - g. Приложить файл – доступно для редактирования и является дополнительным функционалом, не обязателен к заполнению.
2. После заполнения всех полей нужно нажать на кнопку «Сохранить». Система вносит изменения в отчет карточки взлома.

3.4.4.2.1.4. Написание комментария к карточке взлома

После создания карточки взлома, всей команде Red Team доступно общение в комментариях карточки. Для того чтобы написать комментарий к карточке, пользователю необходимо находиться в учении, которое имеет статус «Сейчас происходит» и перейти на вкладку «Взломанные машины».



1. Пользователь нажимает на кнопку «Отчет» или на значок комментария. Система открывает модальное окно с карточкой взлома.



2. Пользователю доступно написание комментариев в карточке взлома.
 - а. **Важно:** Написание комментариев к карточкам доступно всегда. Даже после полного завершения учения.

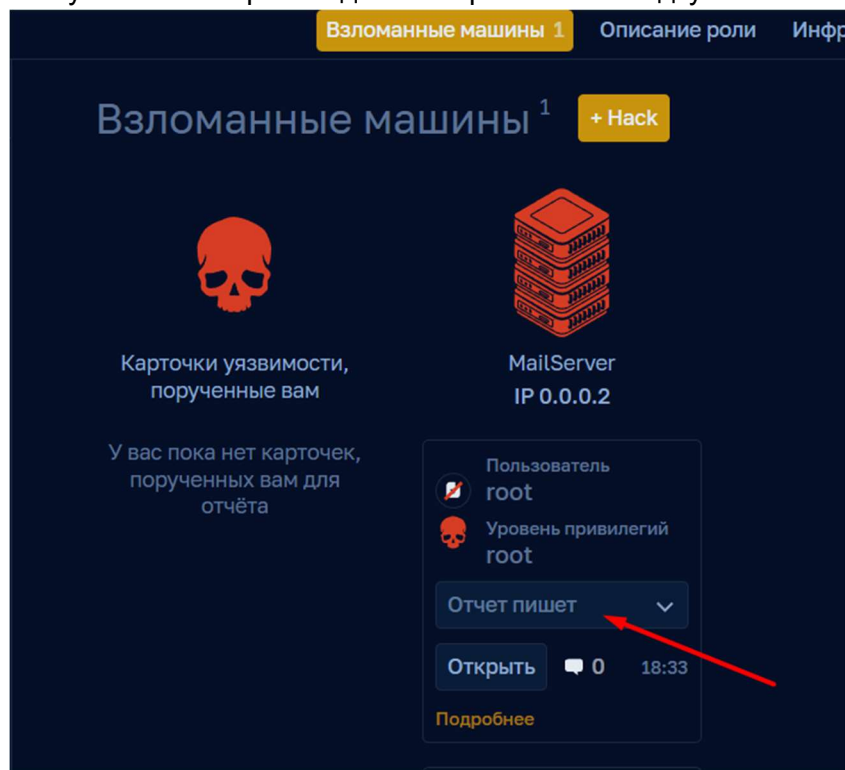
3.4.4.2.1.5. Общение в чате

Смотри пункт 3.4.4.1.1.3. – [Общение в чате](#)

3.4.4.2.2. Leader

3.4.4.2.2.1. Назначение карточки взлома

Лидер команды может назначать созданные карточки взлома на сокомандников (Пользователей с ролью Attacking), либо назначить на самого себя. Для того чтобы назначить карточку, пользователю необходимо находиться в учении, которое имеет статус «Сейчас происходит» и перейти на вкладку «Взломанные машины».



1. Пользователь видит карточку взлома и нажимает на селект, где выпадает список из сокомандников на кого можно назначить писать отчет.
2. Пользователь выбирает пользователя на кого поставить написание отчета, либо выбирает себя. Система назначает отчет на выбранного пользователя.
3. Создание карточки взлома

3.4.4.2.2.2. Создание карточки взлома

Смотри пункт 3.4.4.2.1.1. – [Создание карточки взлома](#)

3.4.4.2.2.3. Написание отчета для карточки взлома

Смотри пункт 3.4.4.2.1.2 – [Написание отчета для карточки взлома](#)

3.4.4.2.2.4. Редактирование карточки уязвимости

Смотри пункт 3.4.4.2.1.3 – [Редактирование карточки уязвимости](#)

3.4.4.2.2.5. Написание комментария к карточке взлома

Смотри пункт 3.4.4.2.1.4. – [Написание комментария к карточке взлома](#)

3.4.4.2.2.6. Общение в чате

Смотри пункт 3.4.4.1.1.3. – [Общение в чате](#)

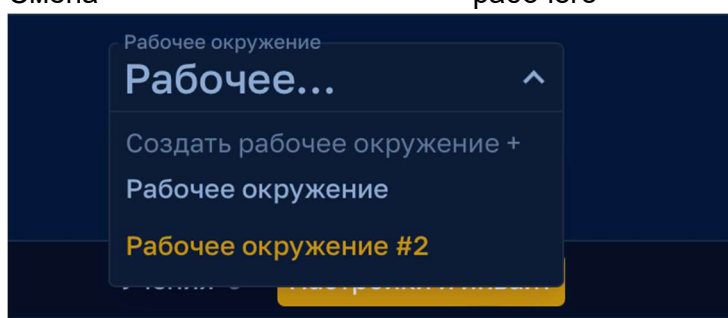
3.4.4.2.2.7. Оценка товарищей по команде после завершения учения

Смотри пункт 3.4.4.1.2.6. – [Оценка товарищей по команде после завершения учения](#)

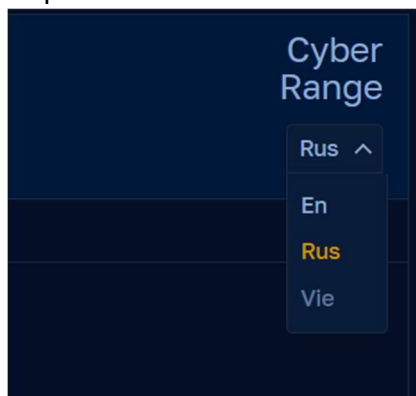
3.4.5. Первостепенные функции

Пользователю также доступны такие функции как:

1. Смена рабочего окружения



2. Сменить язык – доступны три языка Русский, Английский, Вьетнамский, Бирманский (планируется добавление).



3. Выйти из профиля – необходимо нажать бургер-меню (три горизонтальные полосы) в левом верхнем углу и выбрать пункт «Выйти».

