



# **Программный комплекс кибертренировок «Солар Кибермир»**

**Руководство пользователя**

МОСКВА, 2023

## Содержание

<b>1. НАЗНАЧЕНИЕ ПРОГРАММЫ.....</b>	<b>3</b>
<b>2. УСЛОВИЯ ЭКСПЛУАТАЦИИ .....</b>	<b>4</b>
2.1. ТРЕБОВАНИЯ К СЕРВЕРУ ПРИЛОЖЕНИЯ .....	4
2.2. ТРЕБОВАНИЯ К АВТОМАТИЗИРОВАННОМУ РАБОЧЕМУ МЕСТУ ПОЛЬЗОВАТЕЛЯ.....	4
<b>3. ВЫПОЛНЕНИЕ ПРОГРАММЫ.....</b>	<b>4</b>
3.1. РАБОТА АДМИНИСТРАТОРА И ПРЕПОДАВАТЕЛЯ НА ПЛАТФОРМЕ .....	4
3.1.1. ВХОД В ПЛАТФОРМУ (АВТОРИЗАЦИЯ).....	4
3.1.2. СОЗДАНИЕ МЕРОПРИЯТИЯ.....	5
3.1.3. УПРАВЛЕНИЕ МЕРОПРИЯТИЕМ.....	29
3.1.4. УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ.....	37
3.1.5. УПРАВЛЕНИЕ ОРГАНИЗАЦИЯМИ .....	45
3.1.6. ПЕРЕЧЕНЬ МЕРОПРИЯТИЙ.....	48
3.1.7. СКОРИНГ ОТЧЕТОВ УЧАСТНИКОВ.....	49
3.1.8. НАСТРОЙКА СКОРБОРДА ПЛАТФОРМЫ.....	57
3.1.9. РЕДАКТОР ВИЗУАЛИЗАЦИИ .....	62
3.2. РАБОТА УЧАСТНИКА НА ПЛАТФОРМЕ.....	91
3.2.1. ВХОД В ПЛАТФОРМУ (АВТОРИЗАЦИЯ).....	91
3.2.2. ПОДКЛЮЧЕНИЕ К МЕРОПРИЯТИЮ .....	92
3.2.3. КАРТОЧКА МЕРОПРИЯТИЯ .....	94
3.2.4. ПОДКЛЮЧЕНИЕ К ВИРТУАЛЬНОМУ РАБОЧЕМУ МЕСТУ .....	96
3.2.5. ЗАПОЛНЕНИЕ ОТЧЕТА ОБ ОБНАРУЖЕННЫХ АТАКАХ .....	103
3.2.6. ДОБАВЛЕНИЕ ТЕХНИК .....	103
3.2.7. КОПИРОВАНИЕ ДАННЫХ ОБ ОБНАРУЖЕННЫХ ТЕХНИКАХ В ОТЧЕТ С ИСПОЛЬЗОВАНИЕМ БУФЕРА ОБМЕНА ВНУТРИ ВИРТУАЛЬНОЙ МАШИНЫ ПРИ РАБОТЕ В ОГРАНИЧЕННОМ РЕЖИМЕ УПРАВЛЕНИЯ РАБОЧИМ СТОЛОМ.....	108
<b>ПРИЛОЖЕНИЕ А. ФАЙЛ С ДАННЫМИ О ПОЛЬЗОВАТЕЛЯХ .XLSX.....</b>	<b>111</b>

# 1. Назначение программы

Программный комплекс кибертренировок «Солар Кибермир» (далее – Комплекс) предназначен для повышения уровня практической подготовки специалистов в области информационной безопасности по выявлению компьютерных атак, расследованию инцидентов информационной безопасности за счет автоматизации следующих процессов:

- проведение практических занятий по информационной безопасности (далее – ИБ): обнаружение, расследование и защита от кибератак (далее – КА);
- проведение учений и соревнований по информационной безопасности и защите от КА для специалистов по ИБ;
- оценка практических навыков специалистов в области ИБ;
- проведение исследований в области информационной безопасности программного обеспечения и автоматизированных систем (далее – ИС).

## 2. Условия эксплуатации

### 2.1. Требования к серверу приложения

Минимальные требования к аппаратному обеспечению сервера приложений:

- процессор не менее 12 ядер с тактовой частотой не менее 3 ГГц и поддержкой архитектуры x64;
- объем оперативной памяти не менее 32 ГБ;
- объем жесткого диска не менее 250 ГБ;
- сетевой адаптер Ethernet с пропускной способностью не ниже 100 Мбит/с.

Требования к программному обеспечению сервера:

- операционная система Linux x64 без графического интерфейса с установленными средствами защиты информации.

### 2.2. Требования к автоматизированному рабочему месту пользователя

Требования к аппаратному обеспечению:

- процессор не менее 4 ядер с тактовой частотой не менее 2,8 ГГц;
- объем оперативной памяти не менее 4 ГБ;
- объем жесткого диска не менее 128 ГБ;
- разрешение экрана при работе с интерфейсом не менее 1024x768 (интерфейс оптимизирован для разрешения 1920x1080);
- сетевой адаптер Ethernet с пропускной способностью не ниже 10 Мбит/с.

Требования к программному обеспечению:

- операционная система Linux x64 с установленным графическим интерфейсом;

## 3. Выполнение программы

### 3.1. Работа администратора и преподавателя на платформе

#### 3.1.1. Вход в платформу (авторизация)

Для доступа к платформе необходимо выполнить следующие действия:

- в адресной строке в браузере указать адрес платформы и перейти по ссылке;

- на форме входа в верхнем поле выбрать язык отображения интерфейса платформы, заполнить поля «Логин» и «Пароль», отметить галочкой пункт «Я принимаю условия пользовательского соглашения» и нажать кнопку «Войти» (Рис. 1).

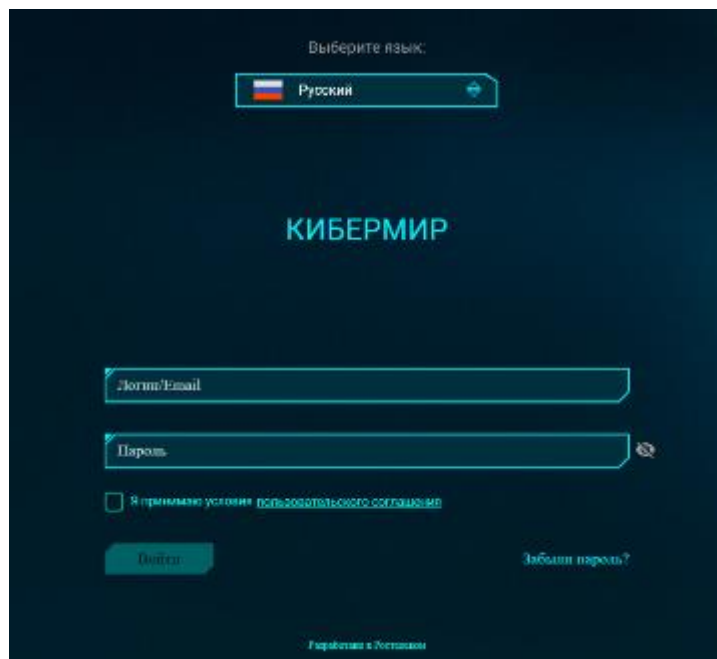


Рис. 1 – Форма входа на платформу

При вводе некорректного пароля более трех раз вход на платформу будет временно заблокирован.

### 3.1.2. Создание мероприятия

*Примечание. Возможность создавать и редактировать мероприятия есть только у администратора.*

После успешной авторизации выбрать из главного меню раздел «Миссии» и перейти на форму «Все миссии», где расположен список миссий (карточек с краткой информацией), на основе которых создаются мероприятия (Рис. 2).

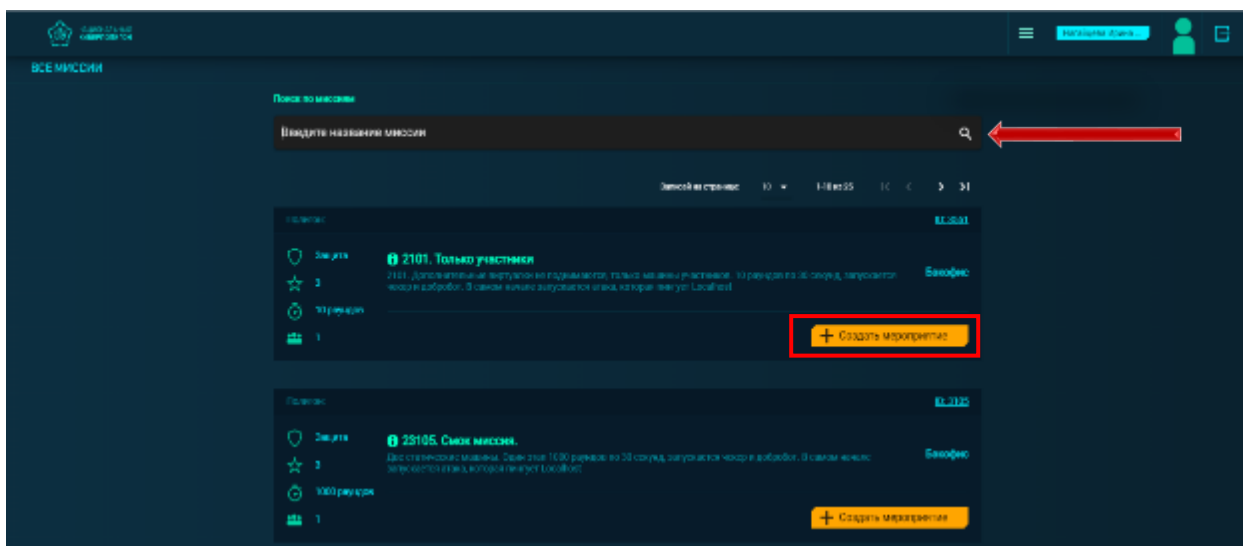


Рис. 2 – Форма «Все миссии»

Каждая миссия описывается конфигурационными файлами и материалами миссии.

Вся информация о миссии, отображенная в интерфейсе карточки миссии, содержится в конфигурационных файлах, которые расположены на стенде в папке с ID миссии. Доступ к стенду возможен только по ssh через VPN.

*Примечание. На форме «Все миссии» в списке миссий могут отображаться миссии, которые не прошли валидацию конфигурационных файлов на отсутствие ошибок (соответствие дистрибутивного состава: наличие всех необходимых полей в файлах (description, name, scenario, network и др.).*

Для поиска конкретной миссии в общем списке миссий по названию можно воспользоваться функцией поиска (Рис. 2).

*Важно! Редактирование конфигурационных файлов миссий вручную может привести к сбоям в работе, так как платформа не проводит валидацию конфигурационных файлов миссий.*

При нажатии на название конкретной миссии открывается карточка миссии (Рис. 3) на которой есть доступ к следующей информации:

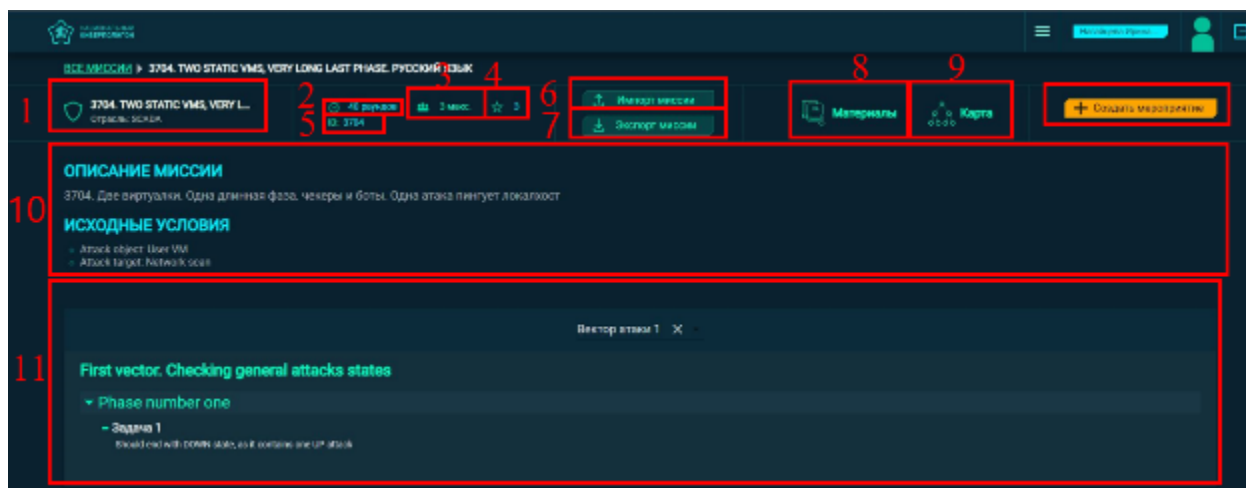


Рис. 3 – Карточка миссии

1. Название миссии и отрасль для которой создана миссия (Рис. 3 п. 1).
2. Количество раундов, из которых состоит миссия. Количество раундов миссии высчитывается из файла `scenario.yaml` (Рис. 3, п. 2).
3. Максимально возможное количество участников миссии (Рис. 3, п. 3).
4. Уровень сложности миссии (Рис. 3, п. 4).
5. Уникальный идентификатор миссии (Рис. 3, п. 5).
6. Кнопка **«Импорт миссии»** позволяет загрузить пакет конфигурационных файлов для выбранной миссии на сервер (Рис. 3, п. 6). Загружаемый пакет представляет собой ZIP-архив, содержащий в себе файлы миссии в соответствии со следующей структурой:

```

network-map.json
network.yaml
scenario.yaml
scoring_report.yaml
<language>
  attributes.yaml
  mission.yaml
  media
    <Mission manual 1>
    ...
    <Mission manual n>,

```

где:

- `network-map.json` – файл, содержащий визуализацию;
- `network.yaml` – файл, содержащий информацию об используемых машинах в данном мероприятии/сценарии;
- `scenario.yaml` – файл, содержащий сценарий атаки;
- `scoring_report.yaml` – файл, содержащий эталонный отчет;
- `<language>` – имя каталога с названием языка;
- `attributes.yaml` – файл с параметрами мероприятия;

- mission.yaml – файл, содержащий общую для всех типов миссий часть атрибутов;
- media – папка с материалами по миссии;
- <mission manual> – файл из материалов миссии (бриф, регламент и т. д.).

```
network-map.json
network.yaml
scenario.yaml
scoring_report.yaml

+---en
|   attributes.yaml
|   mission.yaml
|   \---media
|       Brief.pdf
|       network-map.png
|       Software list.pdf
|       User guide.pdf
|
|   \---ru
|       attributes.yaml
|       mission.yaml
|       \---media
|           Brief.pdf
|           network-map.png
|           Software list.pdf
|           User guide.pdf
```

Рис. 4 – Структура хранения файлов конфигурации

При инициации пользователем загрузки файлов на сервер система производит валидацию конфигурационных файлов миссии (как при создании мероприятия) на отсутствие ошибок (соответствие дистрибутивного состава: наличие всех необходимых полей в файлах, несовпадение названия машин, соответствие векторов и т. д.), и при успешной валидации производится загрузка файлов миссии (Рис. 4). Валидация не затрагивает содержимое папки с материалами миссии (папка «media»).

Система поддерживает импорт пакетов конфигурационных файлов размером до 50 Мбайт (52 428 800 байт). Если размер пакета превышает данное ограничение, то отобразится сообщение об ошибке (о превышении максимально допустимого размера пакета) (Рис. 5).

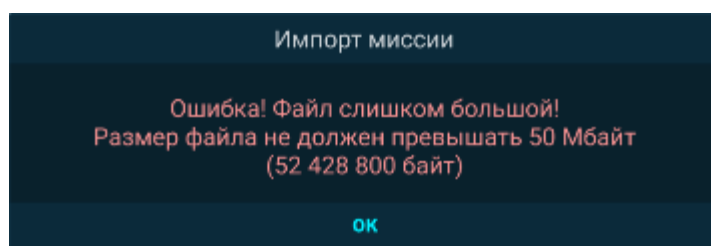


Рис. 5 – Сообщение о превышении максимально допустимого размера пакета при импорте миссии



Загружаемый ZIP-архив (пакет) должен формироваться из отдельно расположенных конфигурационных файлов и папок с файлами локализации, а не из одной папки, содержащей все конфигурационные файлы и папки локализации (Рис. 6). Если структура пакета ZIP-архива не совпадет с необходимой, то отобразится сообщение об ошибке и пакет файлов не загрузится.

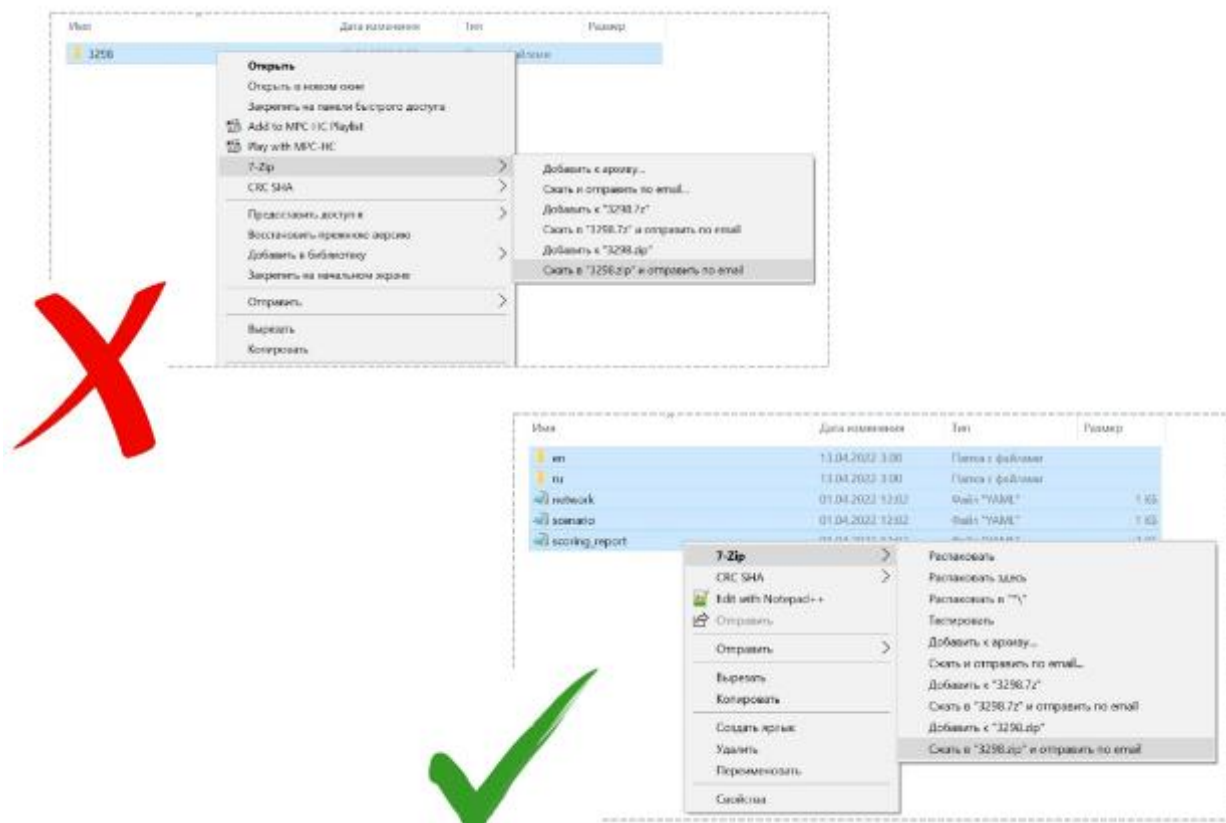


Рис. 6 – Архивация пакета конфигурационных файлов

Если при валидации возникнет одна или более ошибок, то система не загрузит для миссии конфигурационные файлы на сервер и проинформирует пользователя об ошибке (Рис. 7).

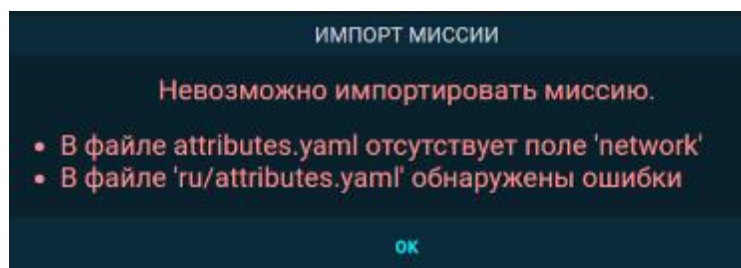


Рис. 7 – Пример сообщения об ошибке при импорте миссии

Если конфигурационные файлы миссии уже существовали на сервере, то при повторной загрузке очищаются все имеющиеся файлы на сервере и добавляются новые, при

этом система информирует пользователя с помощью всплывающего уведомления об успешной загрузке.

7. Кнопка «Экспорт миссии» позволяет выгрузить все файлы, находящиеся на сервере в папке с ID миссии, в виде ZIP-архива с сервера на ПК пользователя (Рис. 3, п. 7).

8. Комплект сопроводительных материалов, которые могут пригодиться участнику мероприятия (Рис. 3, п. 8) для разных миссий может быть различным (Рис. 8). Сами файлы располагаются на сервере в папке с ID миссии в поддиректории **media** рядом с конфигурационными файлами.

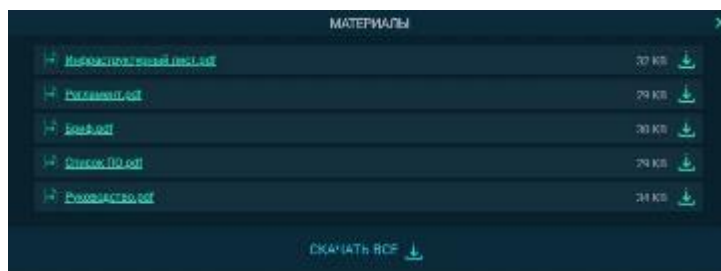


Рис. 8 – Комплект сопроводительных материалов для скачивания

9. Карта миссии – топология сети инфраструктуры миссии (Рис. 3, п. 9, 9). Для каждой миссии карта будет своя и сохранена на сервере в папке с ID миссии в поддиректории **media**.



Рис. 9 – Карта миссии

10. Описание и исходные условия миссии (Рис. 3, п. 10).

11. Векторы атаки, по которым представлена информация об этапах и задачах, предусмотренные в данной миссии (Рис. 3, п. 11).

Чтобы создать мероприятие на основе выбранной миссии, необходимо нажать на кнопку «Создать мероприятие» (Рис. 3).

Краткая информация о миссиях, а также кнопка **«Создать мероприятие»** доступна на форме «Все миссии» на карточках миссий (Рис. 2).

После нажатия на кнопку **«Создать мероприятие»** открывается форма **«Создание мероприятия»** (Рис. 3) со следующими полями:

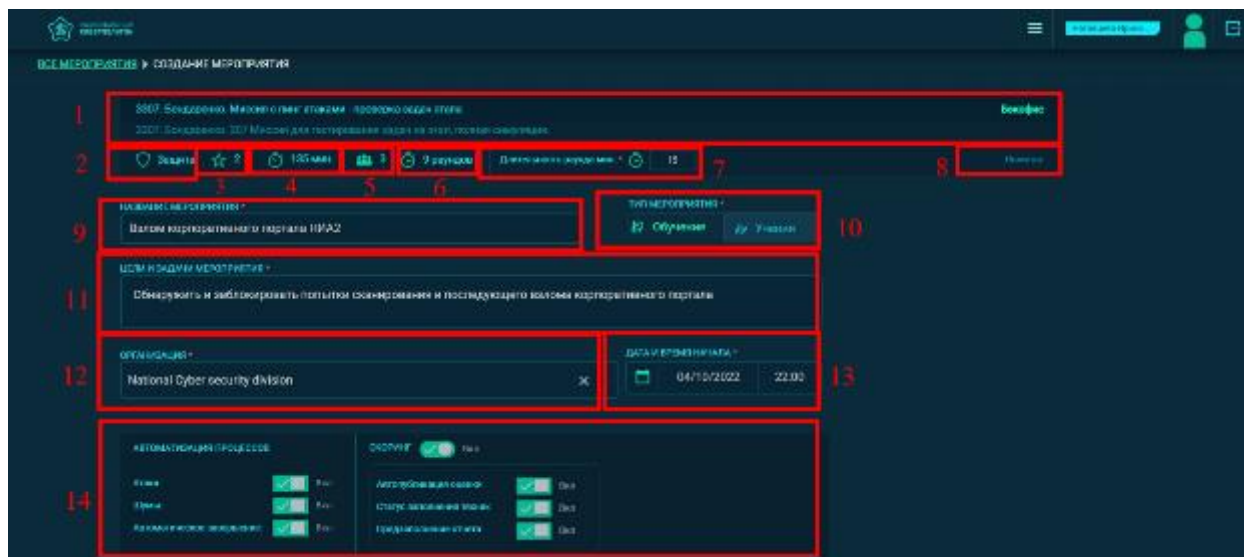


Рис. 10 – Форма «Создание мероприятия»

1. Название и описание миссии (Рис. 10, п. 1). Задается в карточке миссии. При клике на название миссии осуществляется переход на карточку миссии (Рис. 3).
2. Режим миссии. Задается в карточке миссии (Рис. 10, п. 2).
3. Уровень сложности миссии. Задается в карточке миссии (Рис. 10, п. 3).
4. Продолжительность мероприятия – максимально доступное время длительности мероприятия (Рис. 10, п. 4).
5. Максимальное количество участников. Задается в конфигурационных файлах (Рис. 10, п. 5).
6. Количество раундов мероприятия (Рис. 10, п. 6). Количество раундов миссии высчитывается из файла scenario.yaml по правилу MAX (rounds, SUM (durations)).
7. Длительность раунда в минутах (Рис. 10, п. 7). В данное поле необходимо вписать целое или десятичное число от 0,5 до 100 000. Поле является обязательным для заполнения.
8. Название полигона. Задается в конфигурационных файлах (Рис. 10, п. 8).
9. Название мероприятия (Рис. 10, п. 9). В данное поле необходимо вписать название планируемого мероприятия. Максимальная длина названия мероприятия – 255 символов. При превышении данного значения появляется сообщение: **«Введенное значение не должно быть более 255 символов»**. Поле является обязательным для заполнения.
10. Тип мероприятия – Учения/Обучение (Рис. 10, п. 10). При типе «Обучение» нет

ограничений по использованию платформы. При типе мероприятия «Учения» участнику недоступны подсказки в задачах этапа на форме проведения (при условии, что они прописаны в конфигурационных файлах).

11. Цели и задачи мероприятия (Рис. 10, п. 11). В данное поле необходимо вписать цели и задачи планируемого мероприятия. Поле является обязательным для заполнения. Максимальная длина названия мероприятия – 3000 символов. При превышении данного значения появляется сообщение: **«Введенное значение не должно быть более 3000 СИМВОЛОВ»**.

12. Организация – необходимо выбрать организацию для которой создается мероприятие из выпадающего списка (справочника) всех зарегистрированных на платформе организаций (Рис. 10, п. 12). Поле является обязательным для заполнения;

13. Дата и время начала – необходимо выбрать дату и время проведения мероприятия. Поле является обязательным для заполнения (Рис. 10, п. 13).

Дату необходимо выбрать из выпадающего календаря, но не раньше текущей даты (Рис. 11).



Рис. 11 – Выбор даты начала мероприятия

Время мероприятия необходимо проставить вручную. При установке времени система проводит проверку на ближайшее доступное время для создания мероприятия. Оно должно быть на 1 час и 1 минуту больше текущего времени для того, чтобы система успела подготовить инфраструктуру мероприятия до его начала, а администратор решить все вопросы в случае возникновения проблем. Если же проставляемое время не соответствует этому условию, то появится сообщение: **«Ближайшее доступное время начала: +1 час к текущему времени»** (Рис. 12).

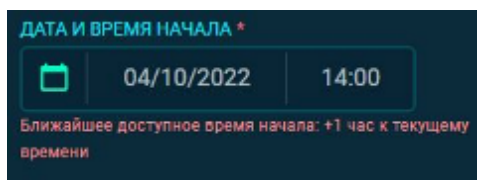


Рис. 12 – Выбор времени начала мероприятия

14. Блок настроек **«Автозапуск»** и **«Скоринг»** содержат переключатели, от комбинаций положений которых зависит сценарий будущего мероприятия (Рис. 10, п. 14). Необходимо проставить переключатели в позиции, соответствующие желаемому сценарию.

**В блоке «Автозапуск»** по умолчанию переключатели «Атаки», «Шумы» и «Автоматическое завершение» переведены в режим «Вкл» (Рис. 13).

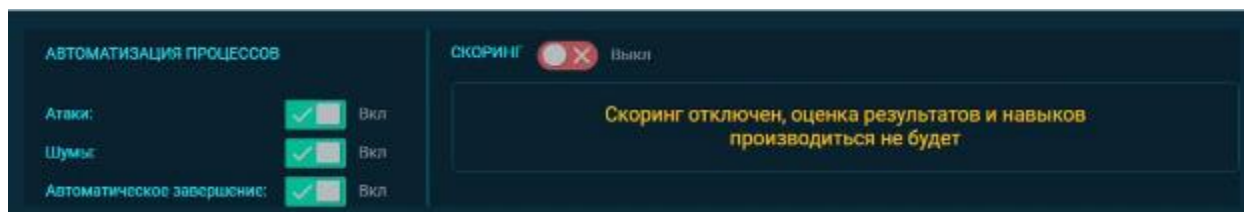


Рис. 13 – Блок «Автозапуск»

- Если переключатель **«Атаки»** перевести в режим «Выкл», то в мероприятии не будут проходить атаки и соответственно подсчет результатов участников (скоринг) невозможен.
- Если переключатель **«Шумы»** перевести в режим «Выкл», то в мероприятии не будут запускаться в работу доброты.
- Переключатель **«Автоматическое завершение»** может находиться в 2 режимах «Вкл»/«Выкл». В зависимости от комбинаций переключателей возможны следующие варианты проведения мероприятия:

1. Если переключатель «Автоматическое завершение» находится в режиме «Вкл», то мероприятие попадет в статус «Подведение итогов» (если переключатель блока «Скоринг» включен) или в статус Завершено (если переключатель блока «Скоринг» выключен).

2. Если переключатель «Автоматическое завершение» находится в режиме «Выкл», то после окончания сценария мероприятие перейдет в статус «Пауза» (независимо от положения переключателя блока «Скоринг»).

**Блок «Скоринг»** можно включить (Рис. 10, п. 14) или отключить (Рис. 13) в зависимости от необходимости оценки результатов участников мероприятия.

Перед созданием мероприятия со скорингом необходимо на стенд в папку с ID миссии, на основании которой планируется мероприятие, добавить конфигурационный файл

scoring\_report.yaml (эталонный отчет миссии). Без этого файла система не позволит включить скоринг в процессе создания мероприятия.

- Если общий переключатель блока «Скоринг» переведен в режим «Выкл», то после окончания сценария мероприятие переходит либо в статус «Пауза», либо в статус «Завершено» (зависит от положения переключателя «Автоматическое завершение»).
- Если общий переключатель блока «Скоринг» переведен в режим «Вкл», то при проведении мероприятия возможен скоринг 2 видов:

1. Общий переключатель блока «Скоринг» переведен в режим «Вкл», а переключатель «Автопубликация оценки» переведен в режим «Выкл» (Рис. 14).

При этом после окончания сценария мероприятие переходит в статус «Подведение итогов», при котором участники не могут отправлять новые отчеты.

Обновление табло с результатами участников происходит только после публикации оцененных/скорректированных отчетов преподавателем.

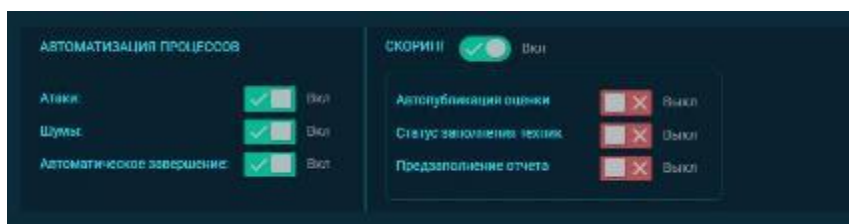


Рис. 14 – Блоки «Автозапуск» и «Скоринг»

2. Общий переключатель блока «Скоринг» и переключатель **«Автопубликация оценки»** переведены в режим «Вкл» (Рис. 10). По мере прохождения сценария система автоматически проводит оценку отчетов участников на базе эталонного отчета и публикует результаты оценки на табло результатов и после окончания сценария переводит мероприятие в статус «Завершено» или «Пауза» (если переключатель **«Автоматическое завершение»** переведен в режим «Выкл»).

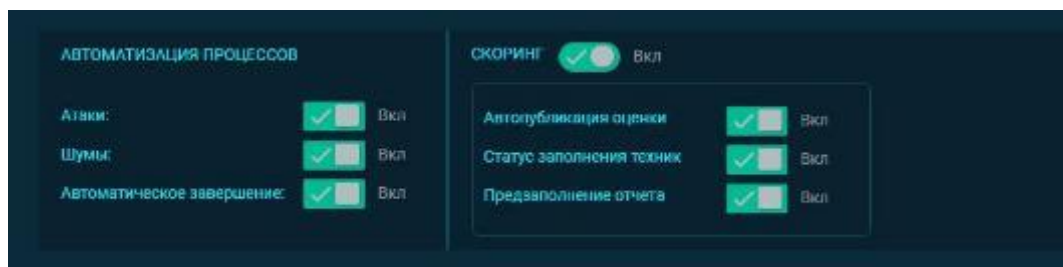



Рис. 15 – Блоки «Автозапуск» и «Скоринг»

Переключатель **«Статус заполнения техник»** позволяет включить/выключить отображение правильности заполнения техники в отчете участника. Правильность заполнения техники отображается в виде линейного индикатора с процентами.

Переключатель **«Предзаполнение отчета»** позволяет предварительно заполнить отчет участника и автоматически добавить в него одну или несколько техник. Такие техники будут помечены специальной иконкой. 

После заполнения всех обязательных полей и указания типа мероприятия, на форме **«Создание мероприятия»** появляются еще несколько полей для заполнения (Рис. 16).

Рис. 16 – Продолжение формы «Создание мероприятия»

15. Преподаватель – ФИО преподавателя (Рис. 10, п.15). Необходимо выбрать вручную из выпадающего списка (справочника) всех зарегистрированных на платформе преподавателей (Рис. 17). Поле не является обязательным для заполнения. Если его оставить пустым, то в качестве преподавателя будет назначен пользователь, создавший мероприятие.

Рис. 17 – Выбор преподавателя на форме «Создание мероприятия»

16. Участники – количество выбранных участников для данного мероприятия / максимально возможное количество участников для миссии (максимально возможное количество участников считается по числу машин участников, прописанных в конфигурационном файле network.yaml) (Рис. 10, п. 16).

Чтобы добавить участников к мероприятию, необходимо нажать кнопку **«Добавить»**.

В открывшемся окне со списком участников напротив фамилий необходимых участников проставить галочки в чекбоксах. Если необходимо выделить сразу всех участников из выбранной организации, то проставить галочку в верхнем чекбоксе (Рис. 18).

После чего у выбранных участников в столбце **«VM»** появятся поля для назначения им виртуальных машин, на которых им предстоит работать (Рис. 18).

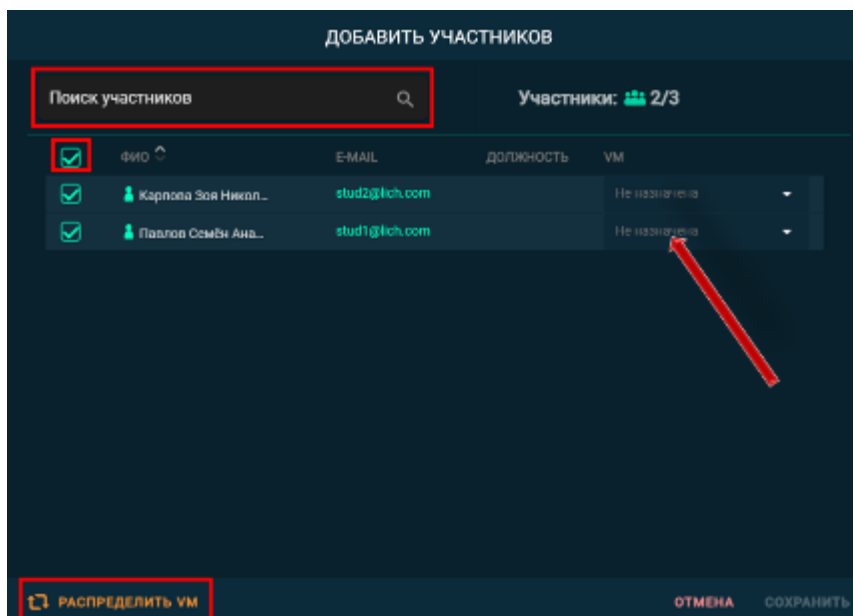


Рис. 18 – Форма «Добавить участников»

Назначить виртуальную машины участнику можно двумя способами:

- выбрать из выпадающего списка (справочника) всех виртуальных машин, которые прописаны в конфигурационном файле network.yaml для данной миссии (Рис. 18);
- нажать на **РАСПРЕДЕЛИТЬ VM** кнопку, и участнику автоматически будет назначена виртуальная машина.

Если участник ранее работал на определенной виртуальной машине, то при нажатии на кнопку **«Распределить VM»** ему будет назначена та виртуальная машина, которая была за ним закреплена на прошлом мероприятии. Это сделано для того, чтобы участники при проведении нескольких последовательных мероприятий работали на одной и той же виртуальной машине (Рис. 19).

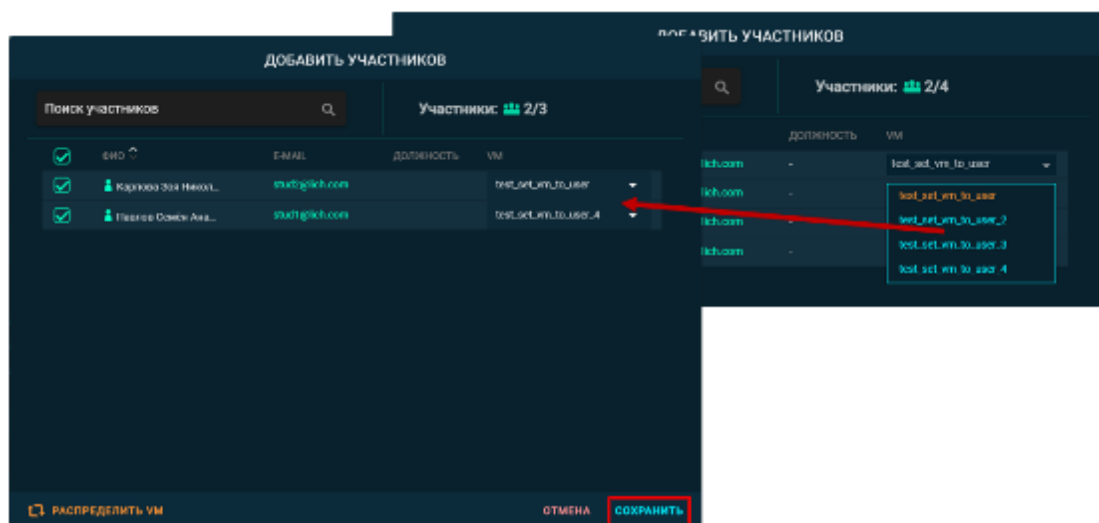


Рис. 19 – Выбор виртуальной машины на форме «Добавить участников»



Одна и та же машина не может быть одновременно назначена двум участникам.

Если разные участники мероприятия ранее пользовались одной и той же виртуальной машиной, то при автоматическом распределении данная машина будет назначена участнику, который последним ее использовал. Остальным участникам назначаются свободные виртуальные машины, прописанные в конфигурационном файле мероприятия.

Назначенные виртуальные машины подсвечиваются желтым цветом, а свободные – голубым (Рис. 19).

На форме «Добавить участников» можно воспользоваться функцией поиска участника по ФИО, а также сортировкой по столбцу с ФИО участника.

После назначения всем выбранным участникам виртуальных машин необходимо нажать на кнопку **«Сохранить»**.

17. Наблюдатели – количество выбранных наблюдателей мероприятия (Рис. 10, п. 17). Для добавления наблюдателей к мероприятию необходимо нажать кнопку **«Добавить»**.

В открывшемся окне со списком наблюдателей напротив фамилий необходимых наблюдателей проставить галочки и нажать кнопку **«Сохранить»**.

На форме можно воспользоваться функцией поиска наблюдателя по ФИО. А также сортировкой по столбцу с ФИО наблюдателя и фильтром по организации (Рис. 20).

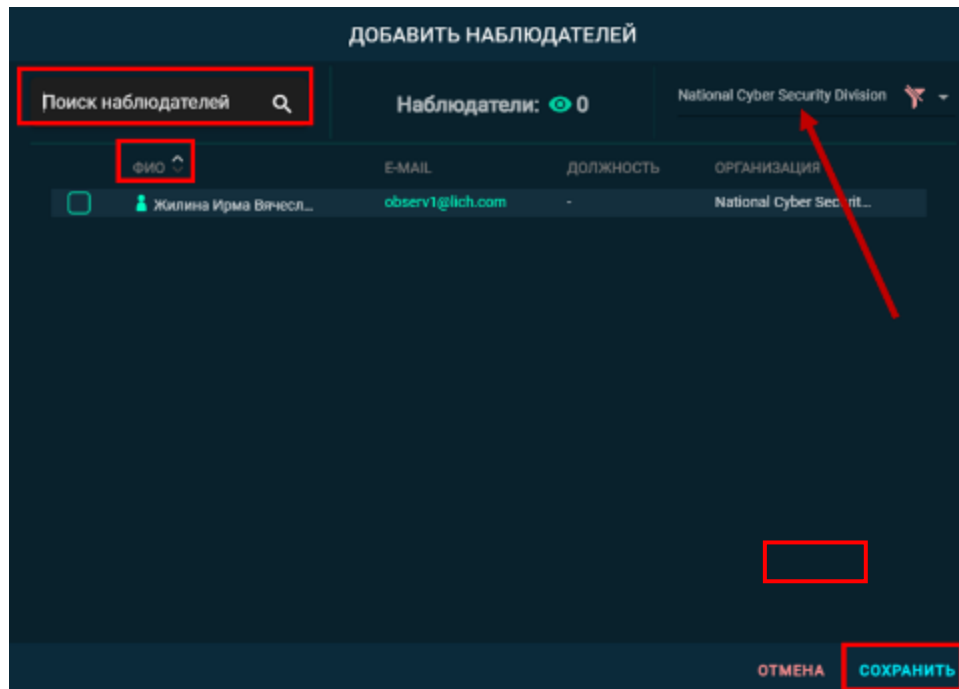



Рис. 20 – Форма «Добавить наблюдателей»

Состав участников и наблюдателей, добавленных к мероприятию, можно изменить или удалить, нажав на кнопки **«Изменить»** и на иконки  соответственно (Рис. 21).

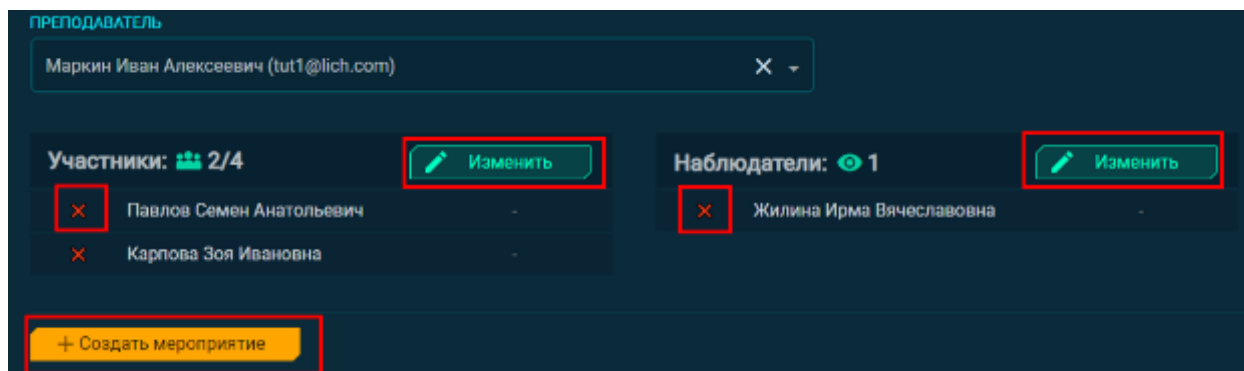


Рис. 21 – Продолжение формы «Создание мероприятия»

После заполнения всех полей и настроек формы необходимо нажать кнопку **«Создать мероприятие»** (Рис. 21) и откроется карточка мероприятия (Рис. 23).

### 3.1.2.1. Настройка инфраструктуры для работы с протоколом Guacamole

В «Тиониксе» для каждой виртуальной машины задаются метаданные, которые определяют параметры подключения к данной виртуальной машине.

Метаданные задаются средствами «Тионикса» в виде пары типа «ключ-значение», и задает их администратор с помощью скриптов подготовки виртуальных машин.

Метаданные:

- VM\_IP\_FOR\_GUACAMOLE='<vm ip address>' – IP-адрес виртуальной машины участника,
- VM\_USER\_FOR\_GUACAMOLE='<login>' – логин для подключения к виртуальной машине участника,
- VM\_PASS\_FOR\_GUACAMOLE='<password>' – пароль для подключения к виртуальной машине участника,

где:

VM\_IP\_FOR\_GUACAMOLE, VM\_USER\_FOR\_GUACAMOLE, VM\_PASS\_FOR\_GUACAMOLE)

– имена ключей, которые задаются в конфигурационных файлах ключами:

- cyberrange.guacamole.vm.meta-param-name-ip,
- cyberrange.guacamole.vm.meta-param-name-login,
- cyberrange.guacamole.vm.meta-param-name-password.

Конфигурационный файл, из которого платформа считывает необходимые метаданные:

- cyberrange.guacamole.vm.meta-param-name-ip=VM\_IP\_FOR\_GUACAMOLE,
- cyberrange.guacamole.vm.meta-param-name-login=VM\_USER\_FOR\_GUACAMOLE,

- cyberrange.guacamole.vm.meta-param-name=  
password=VM\_PASS\_FOR\_GUACAMOLE.

Данные параметры задаются в конфигурационном файле ~cyberrange/ng/configs/configs/cr-config/app/event/application.yaml.

Каталог с конфигурационными файлами расположен ~cyberrange/ng/configs.

Логин и пароль опциональны. В случае если они не указаны, то появится форма доступа к виртуальной машине (RDP), на которой необходимо ввести логин и пароль.

Автоматическое подключение под указанным профилем происходит, если заданы верные логин и пароль (Рис. 22).



Рис. 22 – Метаданные с прописанным логином и паролем

В работе платформы используется сторонний сервис guacamole-daemon (guacd), который проксирует guacamole-сессию в rdp и guacamole-proxy – разработанный компонент, который соединяет платформу с сервисом guacd (проксирует websocket-сессию от клиента (участника) в guacamole-сессию до guacd).

Настройка инфраструктуры включает в себя:

- параметры подключения к guacamole-proxy:
  - a) cyberrange.guacamole.base-uri=http://<host>:<port>,
    - б) cyberrange.guacamole.authn.basic.username=<login>,
      - в) cyberrange.guacamole.authn.basic.password=<password>;
  - параметры подключения к Тиониксу:
    - a) cyberrange.openstack.endpoint,
    - б) cyberrange.openstack.username,
    - в) cyberrange.openstack.password.

Данные параметры задаются в конфигурационном файле ~cyberrange/ng/configs/configs/cr-config/app/event/application.yaml.

### 3.1.2.2. Подготовка мероприятия

После создания мероприятие находится в разных состояниях:

- **Ожидание** – в данное состояние мероприятие переходит после завершения создания пользователем мероприятия.
- **Подготовка** – в данном состоянии система осуществляет подготовку необходимой инфраструктуры.
- **Ошибка** – в данное состояние мероприятие переходит, если в процессе подготовки или проведения мероприятия произошла ошибка. Если ошибку удалось исправить и инфраструктура вернула соответствующее состояние, то можно снова нажать на кнопку «Подготовить» и мероприятие вернется в статус «Подготовка». Если ошибка не исправлена, пользователь отменяет мероприятие, нажав на кнопку «Отмена», и оно переходит в статус «Отменено».
- **Скоро начнется** – данное состояние свидетельствует о том, что все подготовительные процедуры (развертывание инфраструктуры и др.) выполнены и мероприятие ожидает запуска вручную или согласно расписанию.
- **В процессе** – данное состояние является основным статусом мероприятия, в ходе которого пользователи реализуют свои основные функции и задачи, а система может выполнять сценарии атак и шумов.
- **Отменено** – мероприятие переходит в данное состояние при отмене мероприятия пользователем.
- **Пауза** – состояние, при котором мероприятие стоит на паузе. В этом состоянии не запускаются атаки и боты, но участники могут заполнять отчеты.
- **Пауза в конце раунда** – промежуточный статус перед постановкой мероприятия на паузу.
- **Подведение итогов** – данное состояние предназначено для финальной коррекции и утверждения оценок отчетов участников тренером мероприятия. В данном состоянии инфраструктура (виртуальные машины, выделенные подсети и др.) поднята и не разбирается, при этом участники не могут отправлять и корректировать свои отчеты.
- **Завершено** – данное состояние является завершающим для мероприятия. В этом состоянии доступны для просмотра многие данные, но нет возможности

подключиться к форме проведения, отредактировать мероприятие, отправить или оценить отчет.

Доступ к функциям на карточке мероприятия в разных ее статусах будет различным.

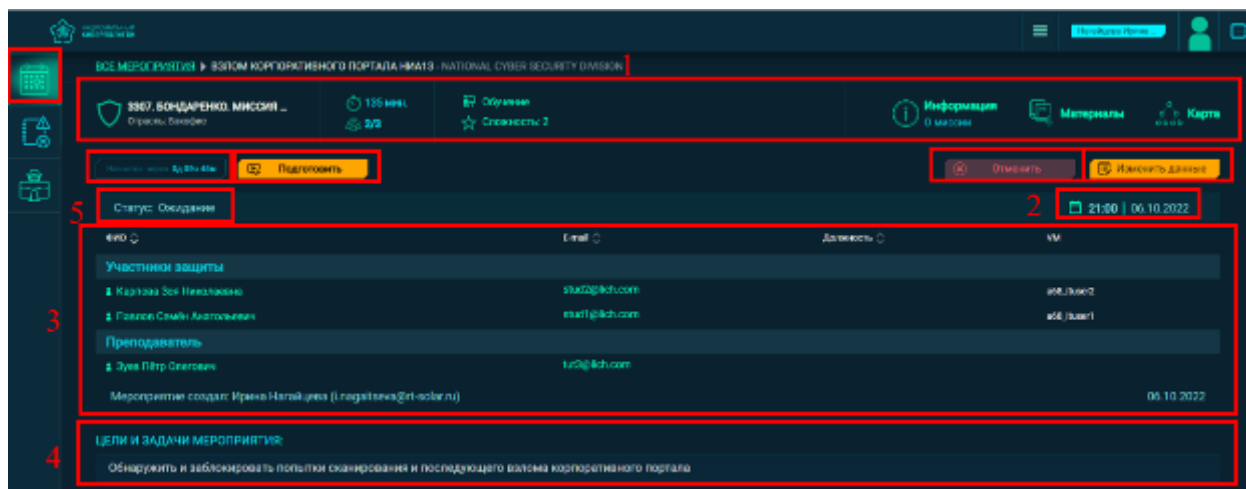



Рис. 23 – Карточка мероприятия без скоринга в статусе «Ожидание»

На карточке мероприятия отражена следующая информация (Рис. 23):

1. Общая информация о мероприятии (Рис. 23, п. 1).
2. Дата и время проведения мероприятия (Рис. 23, п. 2).
3. Таблица с информацией об участниках:

- ФИО;
- e-mail;
- должность;
- VM (виртуальные машины);

– кнопки  для перезапуска виртуальных машин участника (доступны начиная со статуса «Скоро начнется» (Рис. 23, п. 3).

В карточке мероприятия со скорингом таблица содержит большее количество информации (Рис. 27).

4. Цели и задачи мероприятия (Рис. 23, п. 4).
5. Статус мероприятия (Рис. 23, п. 5).

**На вкладке «Log overmind»** в области с логами (overmind-процесс) можно наблюдать процесс подготовки инфраструктуры мероприятия (взаимодействие с «Тиониксом», запуск скриптов и получение от них данных и т. д., Рис. 24).

*Примечание. Вкладка «Log overmind» доступна только администратору.*

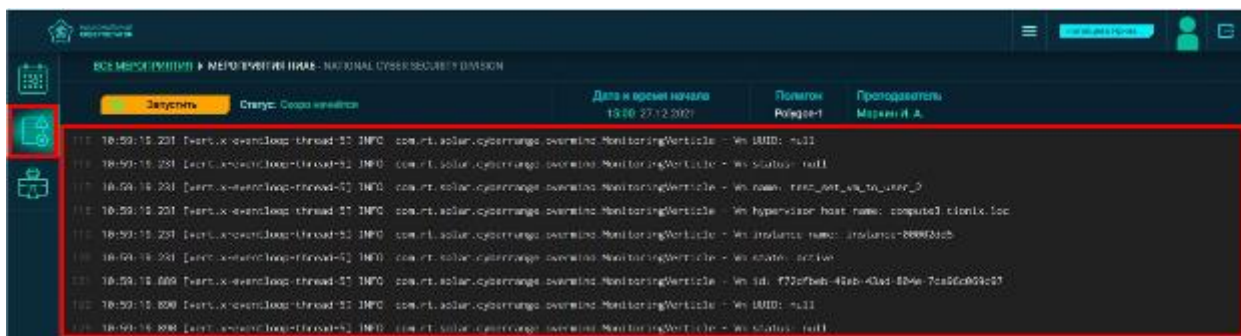


Рис. 24 – Вкладка «Log overmind»

Вкладка «**Управление атаками и шумами**» – форма с возможностью ручного запуска атак и шумов, которые были заданы при создании мероприятия (Рис. 25). В конфигурационном файле scenario.yaml шумовые атаки прописаны без конкретного расписания запуска. Для запуска шумовой атаки необходимо нажать на кнопки запуска рядом с каждой из атак (Рис. 25).



Рис. 25 – Вкладка «Управление атаками и шумами» для миссии с атаками и шумами

Если в миссии не предусмотрены атаки и шумы, то информация на этой складке может отсутствовать (Рис. 26).

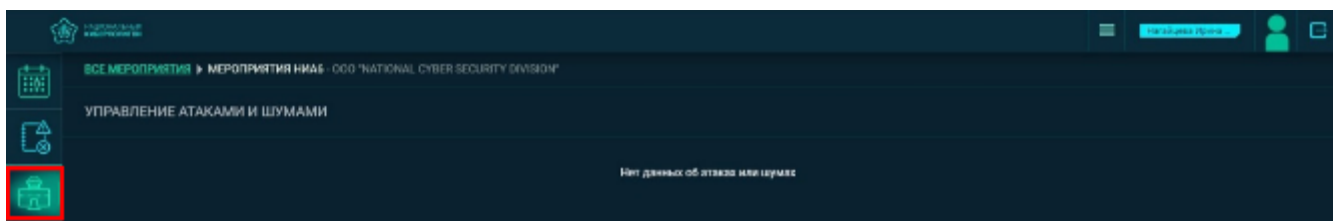


Рис. 26 – Вкладка «Управление атаками и шумами» для миссии без атак и шумов

Карточка мероприятия **со скорингом** содержит дополнительные поля и элементы управления (Рис. 27):

1. В блоке с общей информацией о мероприятии добавилась возможность воспользоваться шпаргалкой по эталонному отчету выбранного мероприятия. При нажатии на иконку открывается файл со шпаргалкой для использования при проверке отчетов участников на правильность заполнения.

2. В таблице с информацией об участниках добавились следующие столбцы:

- Статус – отображает состояние отправленного/неотправленного отчета участника;
- Обновлено мин.назад – показывает сколько минут назад был отправлен последний отчет участника;
- Отчеты – количество отправленных отчетов участника;
- Баллы (%) – количество баллов, набранных участником за заполнение отчета.

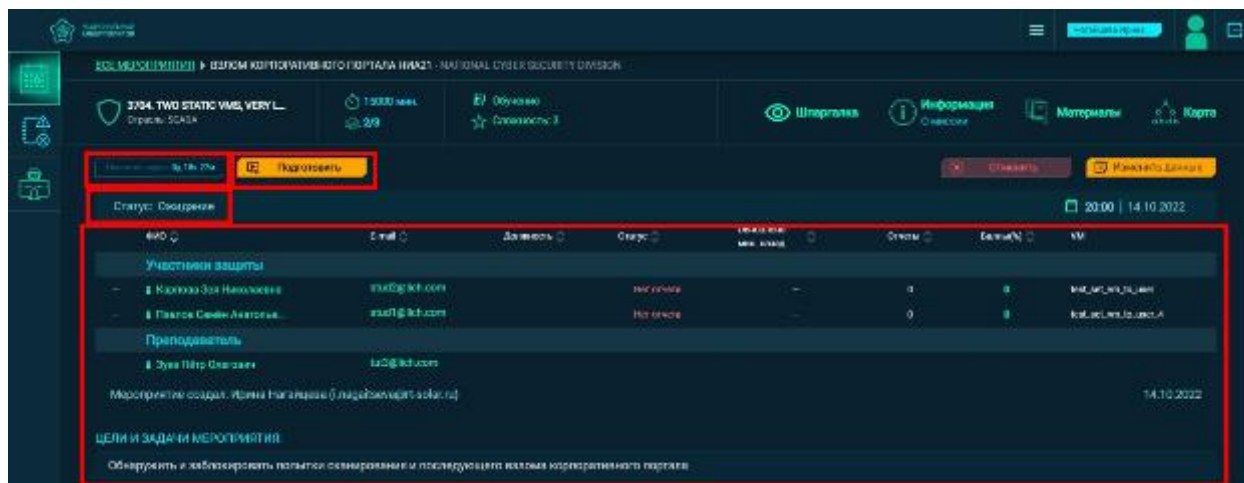


Рис. 27 – Карточка мероприятия со скорингом в статусе «Ожидание»

После завершения создания мероприятие переходит в статус **«Ожидание»**. При этом система производит регистрацию нового мероприятия. В данном состоянии есть возможность редактировать и отменить мероприятие.

На карточке мероприятия появляются функциональные элементы (Рис. 27):

3. Элемент «Начнется через...» – счетчик времени до начала мероприятия.
4. Кнопка «Подготовить» – для перевода мероприятия в следующее состояние «Подготовка» вручную.
5. Кнопка **«Шпаргалка»** по эталонному отчету – предоставляет информацию для использования при проверке отчетов участников на правильность заполнения (Рис. 28).



Рис. 28 – Шпаргалка по эталонному отчету

За 50 минут до планируемого начала мероприятия система автоматически переводит мероприятие в состояние **«Подготовка»** (если не был совершен принудительный запуск с помощью кнопки **«Подготовить»**).

Если время начала мероприятия наступило, но процесс подготовки инфраструктуры еще не завершился, то мероприятие остается в статусе **«Подготовка»**. В данном состоянии есть возможность редактировать некоторые свойства мероприятия и отменить мероприятие.

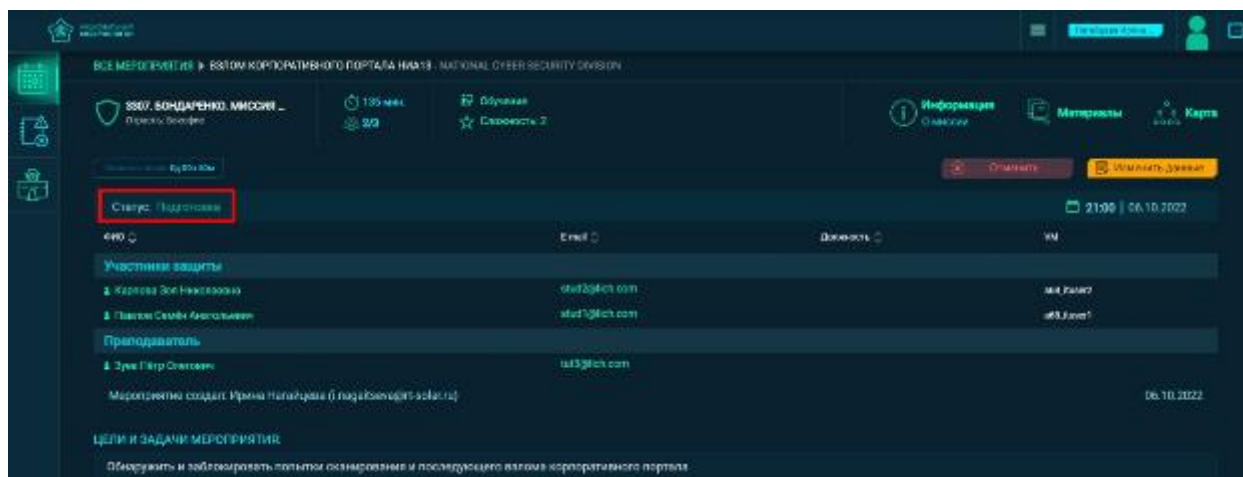


Рис. 29 – Карточка мероприятия без скоринга в статусе «Подготовка»



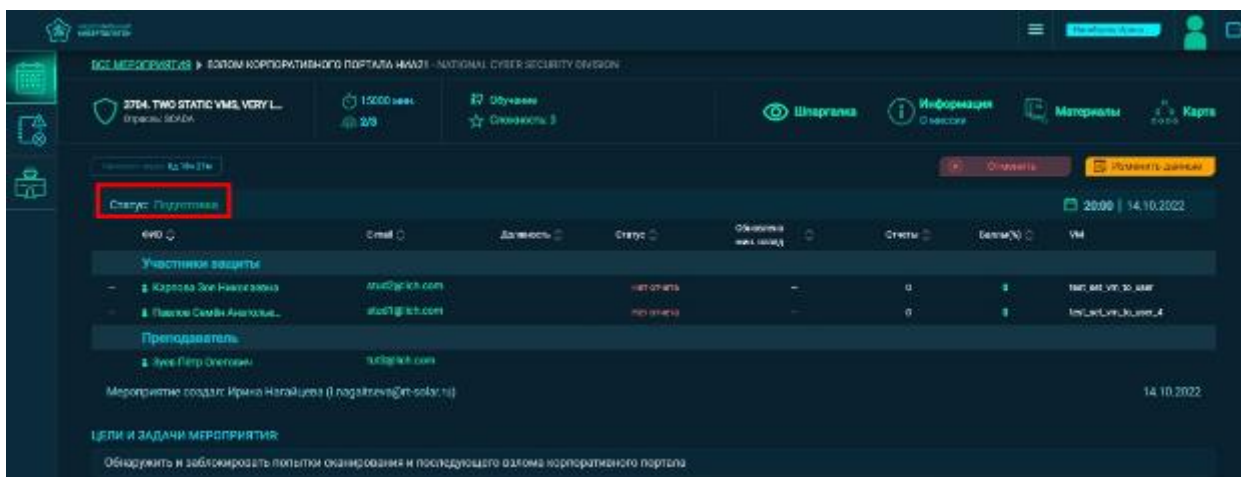



Рис. 30 – Карточка мероприятия со скорингом в статусе «Подготовка»

Мероприятие из статуса «Подготовка» после проведения всех подготовительных процедур (развертывание инфраструктуры и др.) автоматически перейдет в статус «Скоро начнется», и на карточке мероприятия появятся кнопки  для перезапуска виртуальных машин участников, а также кнопка «Запустить» (Рис. 31, 32), при нажатии на которую можно вручную запустить мероприятие, не дожидаясь его автоматического запуска в установленное время. В данном состоянии инфраструктура (виртуальные машины, выделенные подсети и др.) поднята и не разбирается.

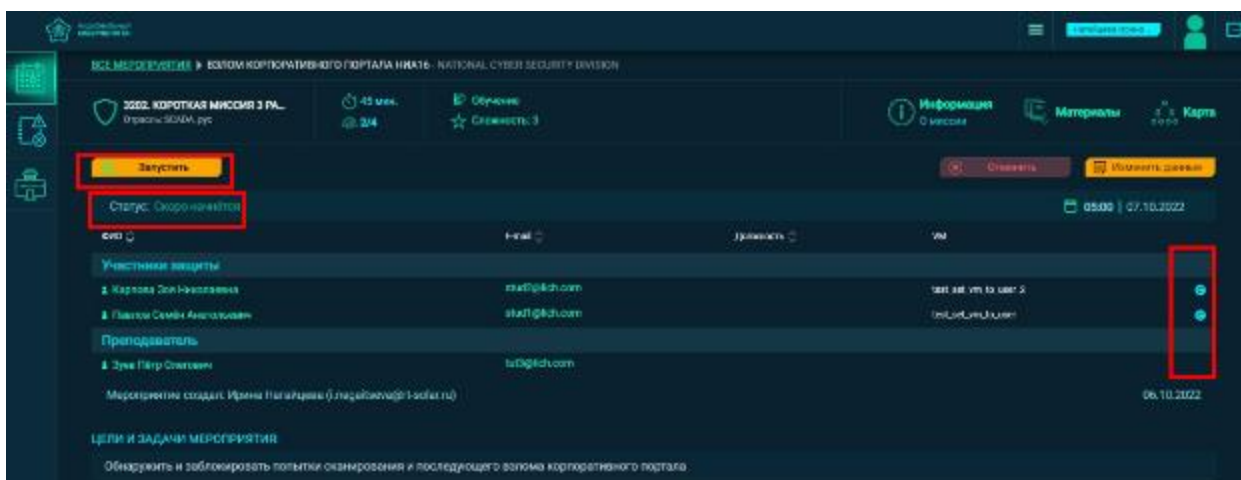


Рис. 31 – Карточка мероприятия без скоринга в статусе «Скоро начнется»

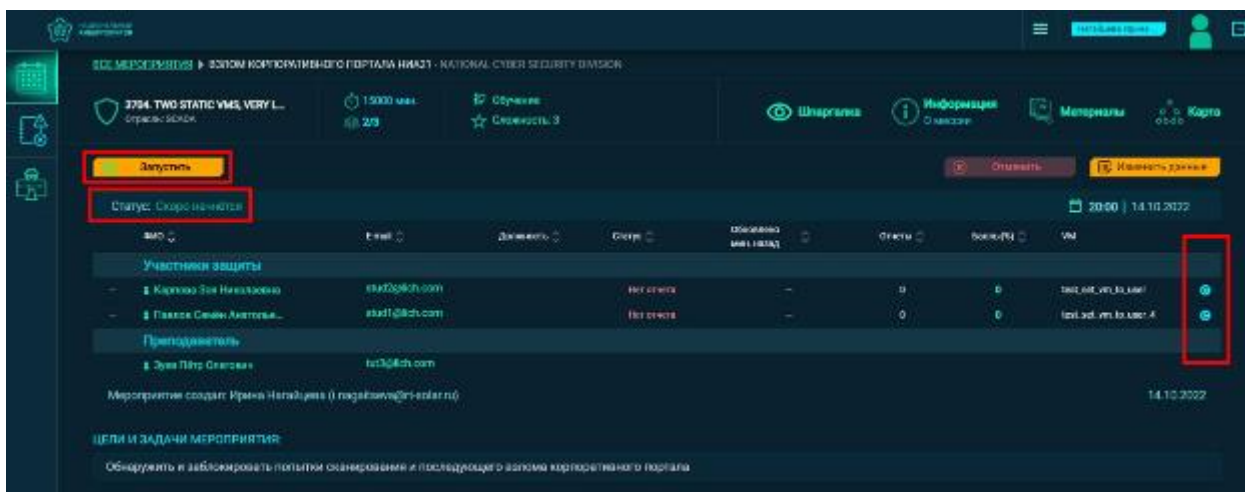


Рис. 32 – Карточка мероприятия со скорингом в статусе «Скоро начнется»

После запуска мероприятие переходит в статус «**В процессе**» и на карточке мероприятия появляется кнопка «**Присоединиться**», с помощью которой можно перейти на форму проведения данного мероприятия (Рис. 33, 34).

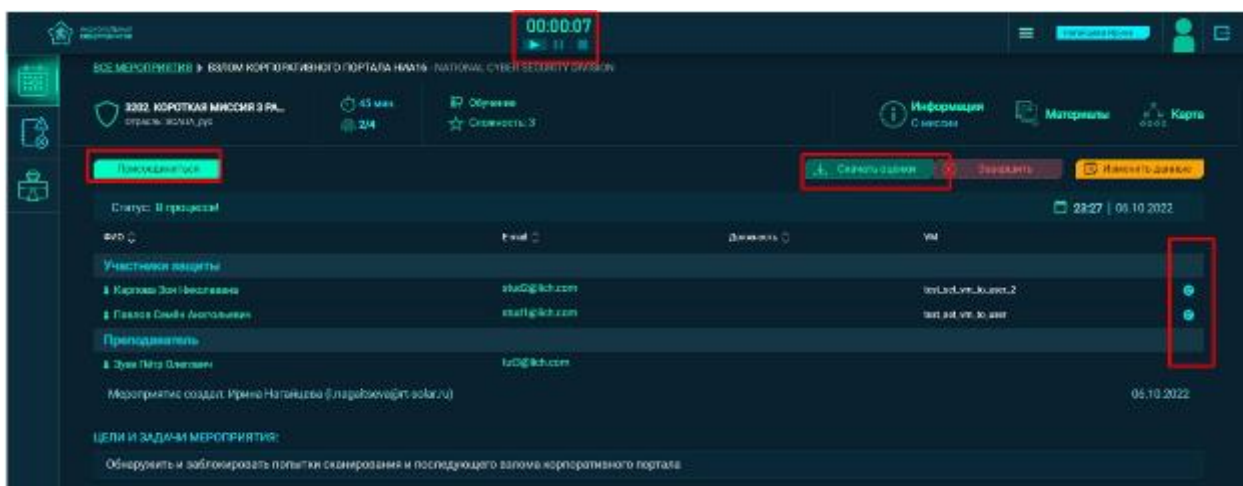



Рис. 33 – Карточка мероприятия без скоринга в статусе «Присоединиться»

На карточке мероприятия появляются:

1. Кнопка «**Скачать оценки**», позволяющая скачать оценки отчетов участников (только для мероприятий со скорингом).
2. Таймер мероприятия, отсчитывающий время от начала мероприятия, и кнопки, позволяющие начать, поставить на паузу, отменить или завершить мероприятие (Рис. 33, 34).
3. Кнопки , позволяющие перейти на форму оценки отчетов участников, которые они заполняют по мере прохождения мероприятия (Рис. 34).

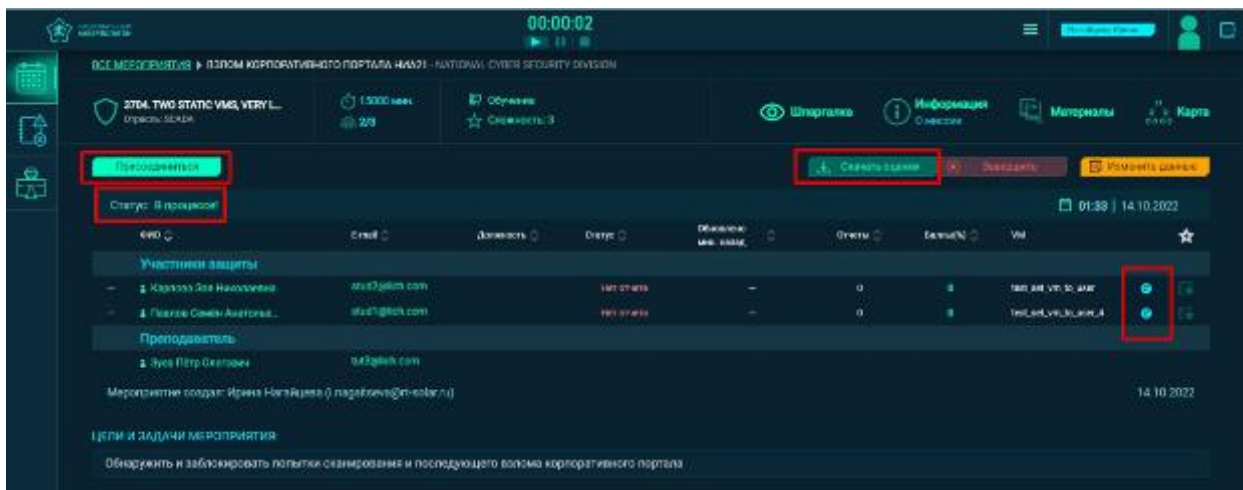


Рис. 34 – Карточка мероприятия со скорингом в статусе «Присоединиться»

В данном состоянии начинает работать счетчик раундов и запускаются атаки и боты в соответствии со сценарием.

### 3.1.2.3. Редактирование мероприятия

Если на этапе создания и подготовки появилась необходимость отредактировать данные мероприятия, то для этого на карточке мероприятия нужно нажать на кнопку «Изменить данные», после чего осуществится переход на форму «Редактирование мероприятия», где можно внести изменения (Рис. 35, 36).

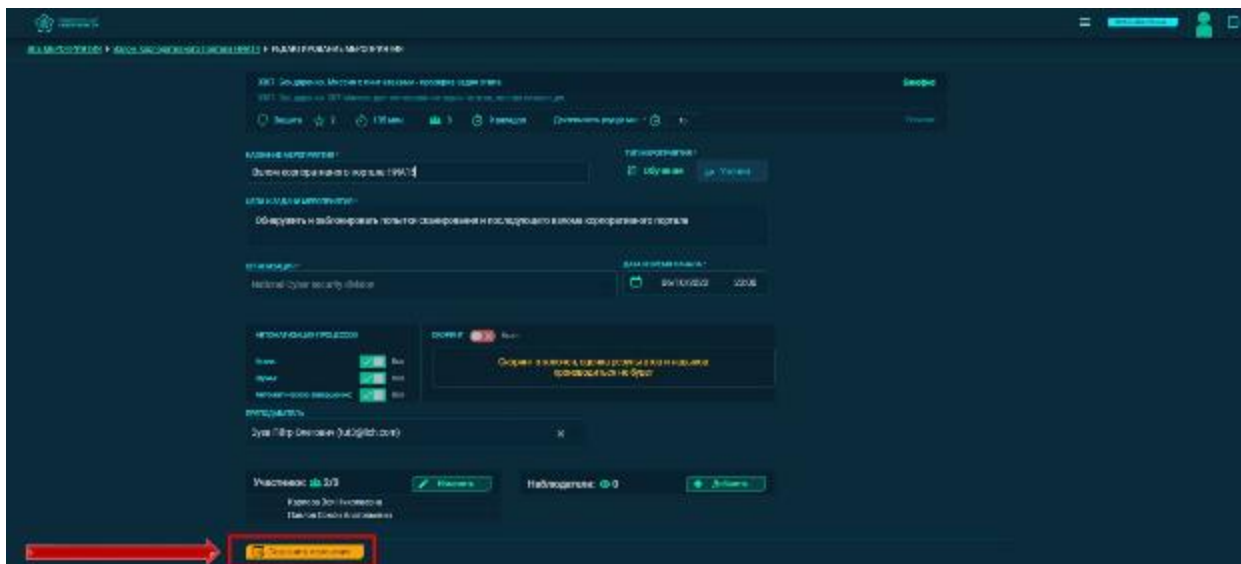


Рис. 35 – Форма «Редактирование мероприятия» без скоринга

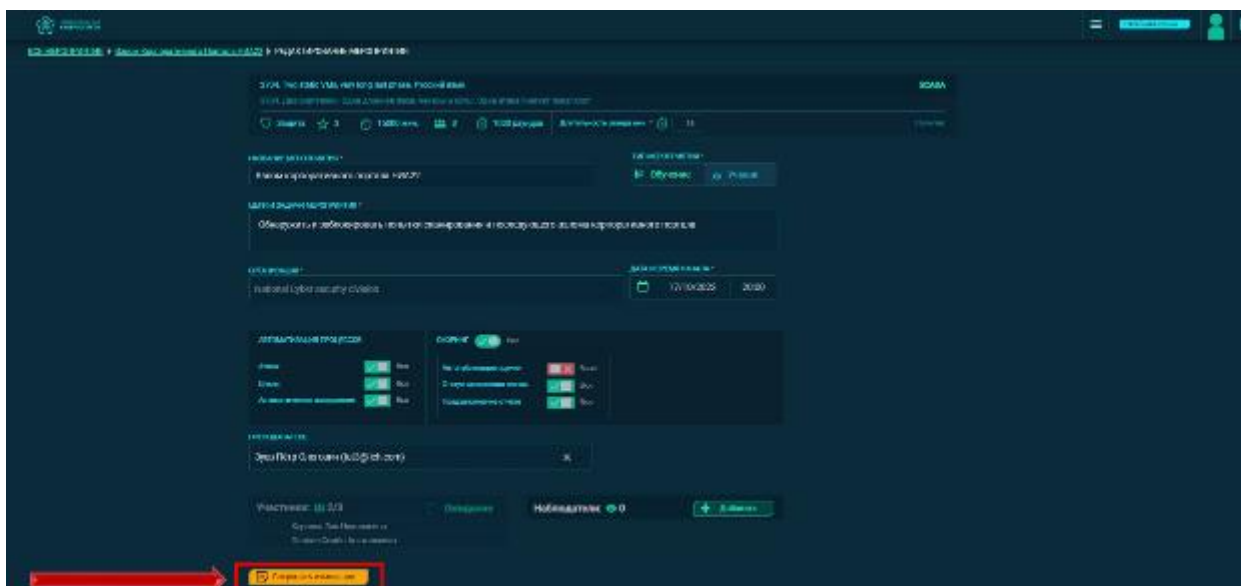


Рис. 36 – Форма «Редактирование мероприятия» со скорингом

Не все данные мероприятия доступны для изменения, когда процесс подготовки инфраструктуры мероприятия запущен. Элементы, не подлежащие изменению, не выделены цветом и не доступны для редактирования.

Если во время внесения изменений мероприятие изменило статус, то при попытке сохранить внесенные изменения в элементы, которые недоступны в новом статусе, появится уведомление о невозможности сохранить изменения (Рис. 37).

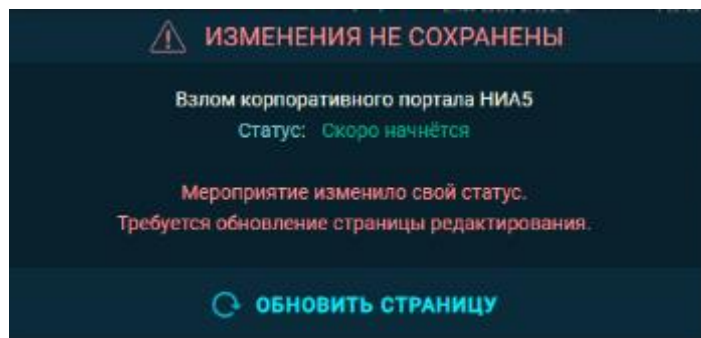


Рис. 37 – Уведомление о невозможности сохранить изменения в мероприятии

Изменить количество участников мероприятия возможно, только когда мероприятие находится в статусе **«Ожидание»** и процесс подготовки инфраструктуры мероприятия еще не запущен.

Отредактировать назначенную участнику виртуальную машину можно:

- когда мероприятие находится в статусе **«Ожидание»**;
- когда мероприятие находится в статусах **«Скоро начнется»**, **«Ошибка»**, **«В процессе»**, **«Пауза»**. При этом для выбора доступны развернутые для мероприятия

пользовательские виртуальные машины, заданные в конфигурационном файле мероприятия network.yaml (все статические и поднятые по количеству участников мероприятия динамические).

Если одному участнику назначается виртуальная машина, которая была ранее закреплена за другим участником, то в результате данная виртуальная машина закрепится за новым участником и сбросится у ранее назначенного участника (Рис. 38).

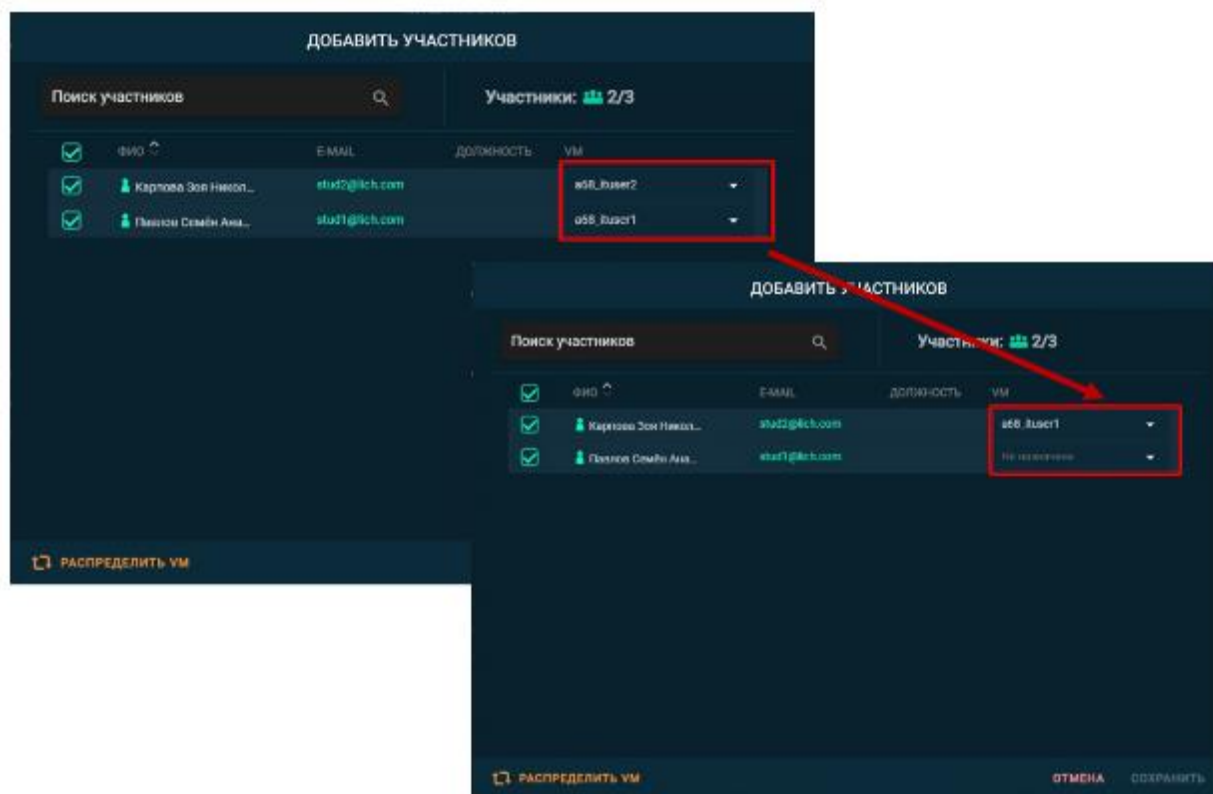


Рис. 38 – Замена виртуальной машины участнику

### 3.1.3. Управление мероприятием

#### 3.1.3.1. Отмена мероприятия

Если возникла необходимость отменить мероприятие, то на карточке мероприятия с момента начала подготовки и до его завершения доступна кнопка **«Отменить»**, которая позволяет отменить мероприятие и перевести его в статус **«Отменено»** (в случае, если мероприятие подготавливалось, но еще не запущено, Рис. 23, 27–33) и перевести в статус **«Завершено»**, если мероприятие уже началось (Рис. 33). После начала мероприятия появляется еще одна возможность отменить мероприятие через кнопку **«Стоп»** на таймере карточки мероприятия (Рис. 33, 34).

*Примечание. Кнопка «Отменить» доступна только администратору.*

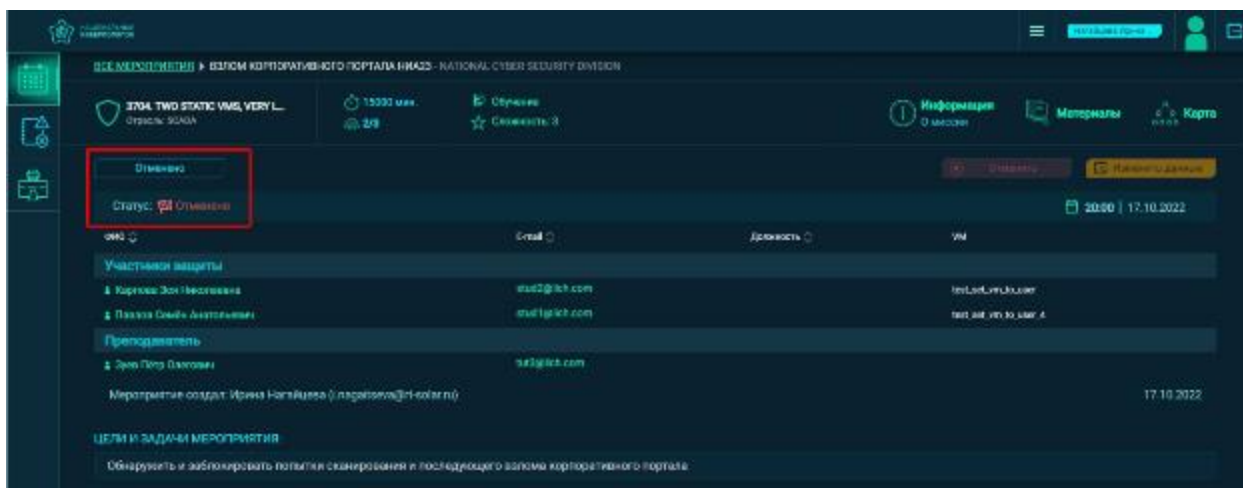


Рис. 39 – Карточка мероприятия без скоринга в статусе «Отменено»

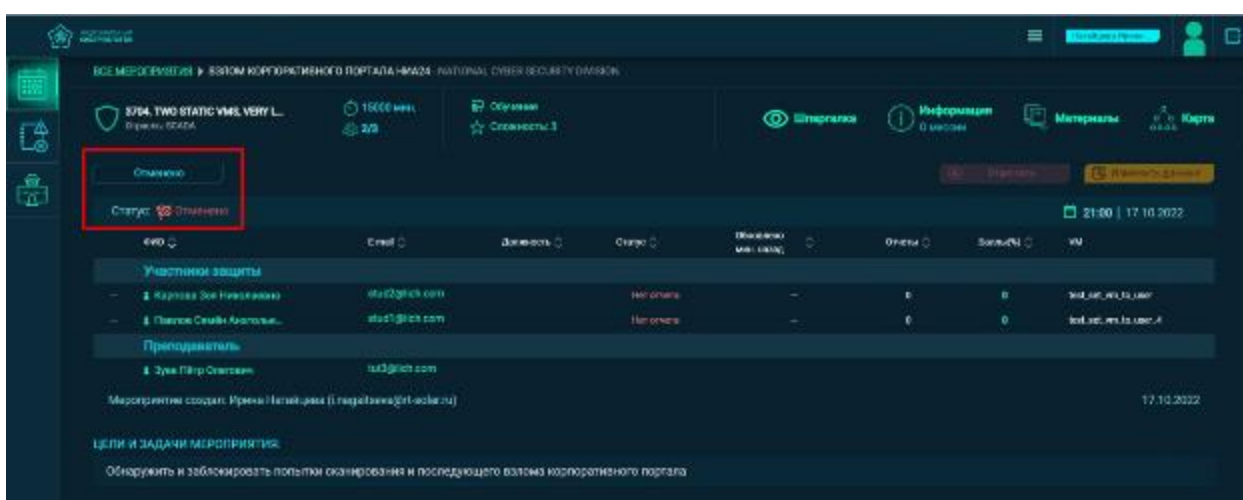


Рис. 40 – Карточка мероприятия со скорингом в статусе «Отменено»

### 3.1.3.2. Пауза мероприятия

При необходимости поставить запущенное мероприятие на паузу следует воспользоваться кнопкой «Пауза» на таймере мероприятия. При нажатии на нее платформа ждет завершения текущего раунда, во время которого появится надпись **Пауза в конце раунда**.

Когда мероприятие фактически встанет на паузу, надпись исчезнет, статус мероприятия изменится на «Пауза» и на таймере подсветится кнопка паузы **00:02:31** (Рис. 41, 42). Затем при нажатии на кнопку «Старт» продолжится выполнение запланированного сценария.

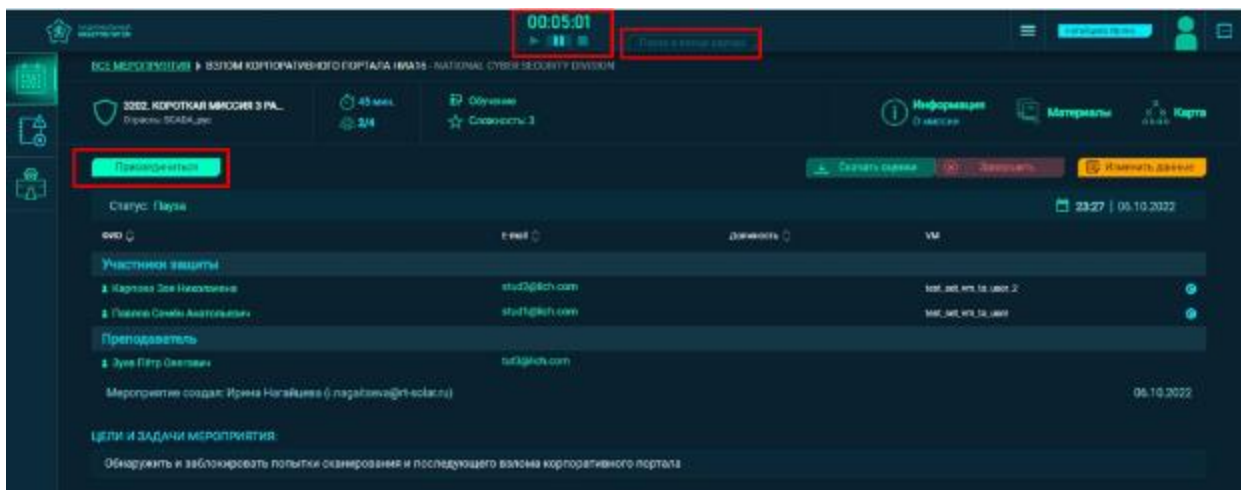


Рис. 41 – Карточка мероприятия без скоринга в статусе «Пауза»

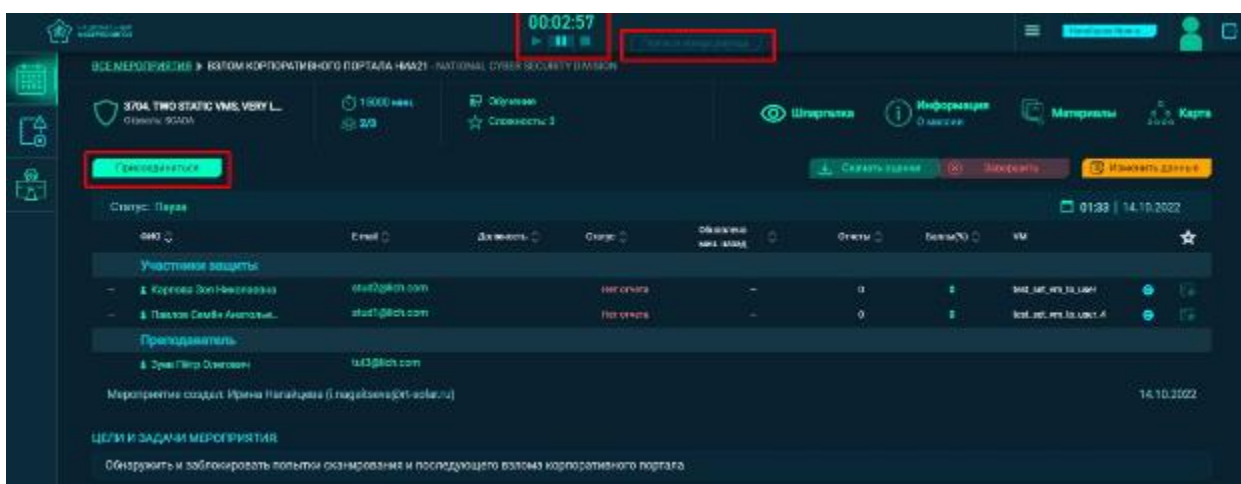


Рис. 42 – Карточка мероприятия со скорингом в статусе «Пауза»

### 3.1.3.3. Завершение мероприятия

После прохождения всех этапов сценария мероприятие перейдет в состояние **«Завершено»** и его статус изменится на **«ДД.ММ.ГГ»** – дата завершения мероприятия (Рис. 43, 44). При открытии формы проведения мероприятия по ссылке или при обновлении страницы мероприятия, которое завершилось, отображается сообщение о завершении мероприятия.

Мероприятие можно завершить вручную, нажав на кнопку **«Стоп»** на таймере мероприятия или на кнопку **«Завершить»** на карточке мероприятия.

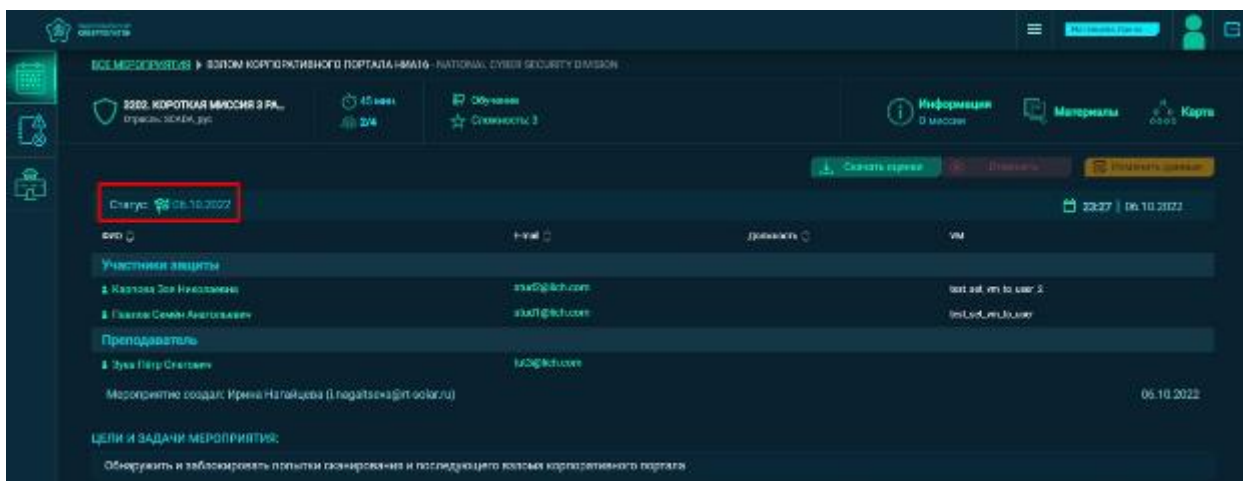


Рис. 43 – Карточка мероприятия без скоринга в статусе «Завершено»

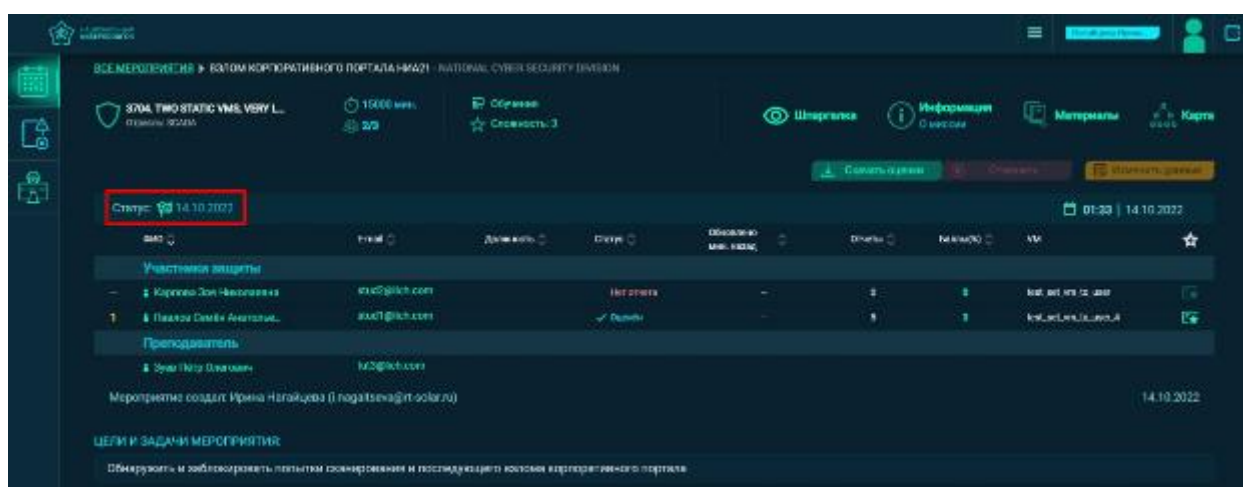


Рис. 44 – Карточка мероприятия со скорингом в статусе «Завершено»

### 3.1.3.4. Визуализация (ход) мероприятия

После присоединения к мероприятию через кнопку «Присоединиться» на карточке мероприятия открывается форма проведения мероприятия (Рис. 45).



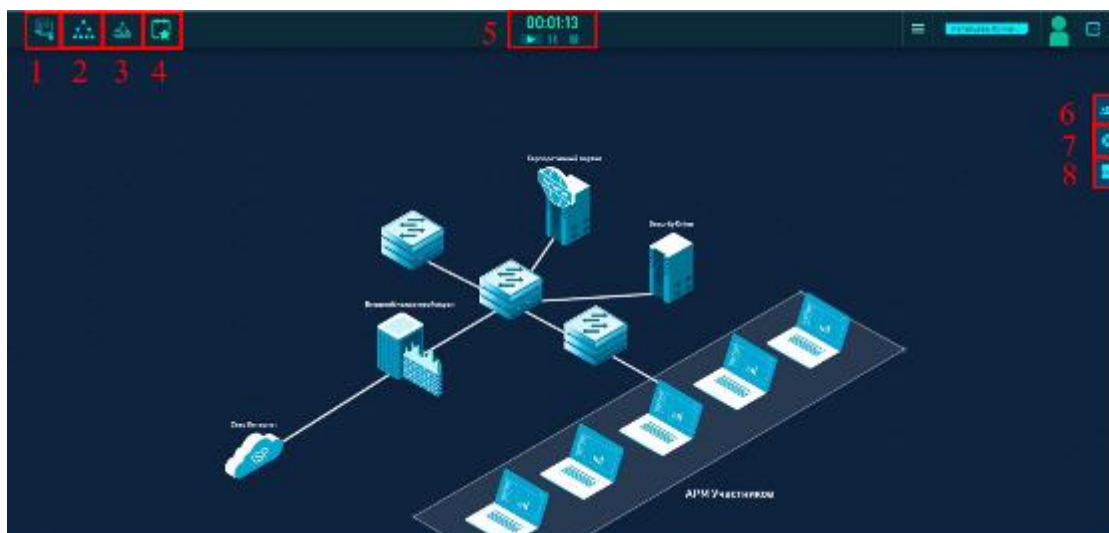





Рис. 45 – Форма проведения мероприятия

На форме доступны следующие функции:

1. Список сопроводительных материалов с информацией о мероприятии (по аналогии с карточкой мероприятия) доступен по кнопке  (Рис. 45, п. 1).

2. Карта мероприятия доступна по кнопке  (Рис. 45, п. 2).


3. Табло результатов – список текущих опубликованных результатов участников – можно посмотреть, нажав на кнопку  (при условии, что мероприятие добавлено на общее табло результатов) (Рис. 45, п. 3, 86).

4. Переход на карточку текущего мероприятия можно осуществить при нажатии на кнопку  (Рис. 45 п. 4). Если нажать на эту кнопку с зажатой клавишей Ctrl, то карточка текущего мероприятия откроется в соседней вкладке браузера.

5. Таймер мероприятия (Рис. 45, п. 5).

6. При наведении курсора мыши и удержании на кнопке (Рис. 45, п. 1–5) рядом с курсором появится всплывающая подсказка с соответствующим названием кнопки.

7. В ходе мероприятия можно посмотреть состав команды – список участников, назначенных на данное мероприятие, нажав на кнопку (Рис. 45, п. 6).

 Участники, присоединившиеся к мероприятию, подсвечиваются зеленым, не присоединившиеся – серым (Рис. 46).

При наведении курсора на иконку «ID» рядом с фото участника можно посмотреть название виртуальной машины, которая назначена этому участнику. При нажатии на название виртуальной машины оно копируется в буфер обмена. **Эта функция доступна только администратору.**

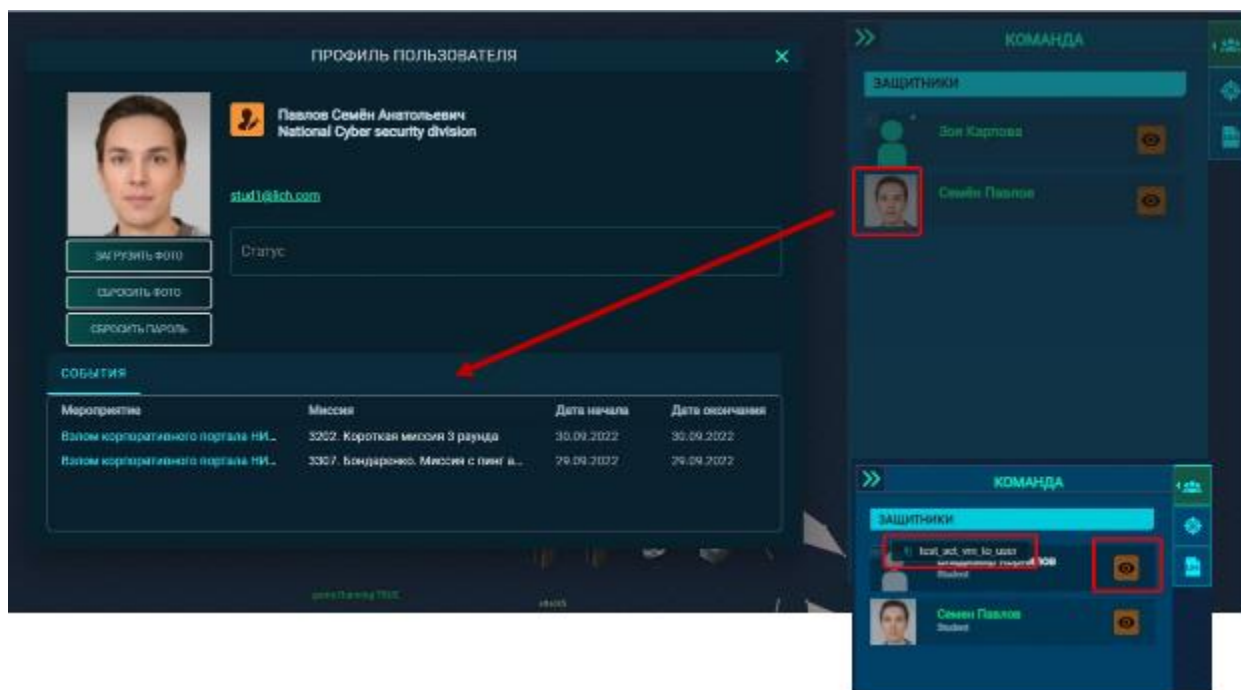


Рис. 46 – Вкладка «Команда» и профиль пользователя


Чтобы подключиться к машине участника и посмотреть, что происходит на его экране, необходимо нажать иконку  рядом с ФИО участника на вкладке «Команда» (Рис. 47, 48).



Рис. 47 – Подключение преподавателя к виртуальной машине участника

Черный экран при подключении к виртуальной машине участника может появиться в следующих случаях (Рис. 47):

- участник ни разу не подключался к мероприятию;

– участник перевел тумблер **«Полное управление»** в режим **«Выкл»** и осуществил переход в ограниченный режим управления рабочим столом (т. е. отключил протокол Guacamole и подключил протокол Spice);

– при подключении к виртуальной машине участника дано разрешение браузеру использовать буфер обмена (на всплывающем диалоговом окне браузера нажата кнопка **«Разрешить»**, (Рис. 47).

*Примечание. Для подключения к виртуальной машине участника необходимо ЗАПРЕТИТЬ доступ браузера к буферу обмена.*

Если доступ браузера к буферу обмена был разрешен, то его необходимо отозвать, выбрав пункт в настройках браузера **«Не открывать этому сайту доступ к буферу обмена»** (Рис. 48).

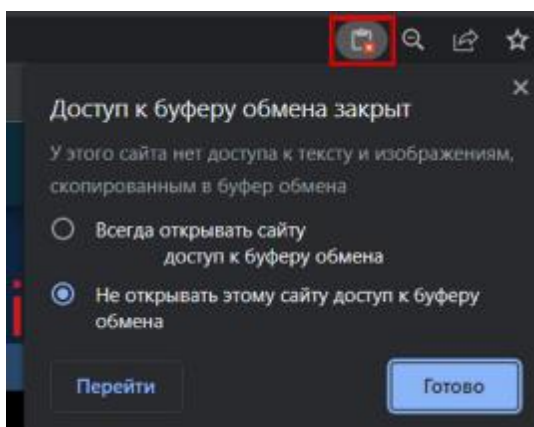


Рис. 48 – Отключение буфера обмена в настройках браузера

Вся вкладка с информацией о команде закрывается при повторном нажатии на кнопку



(Рис. 49).

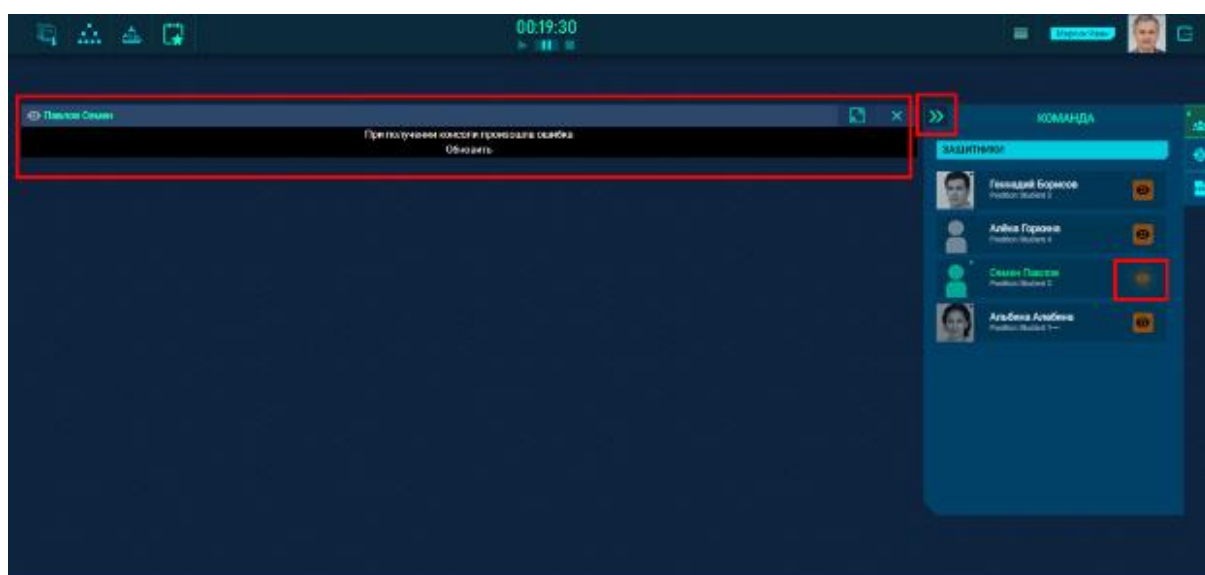



Рис. 49 – Отсутствие доступа к виртуальной машине участника

По кнопке  есть возможность посмотреть текущую задачу на этап в соответствии со сценарием (т. е. то, что происходит на данный момент; Рис. 45, п. 8), а также получить подсказку, нажав на **«Получить подсказку»** внизу окна (Рис. 50).

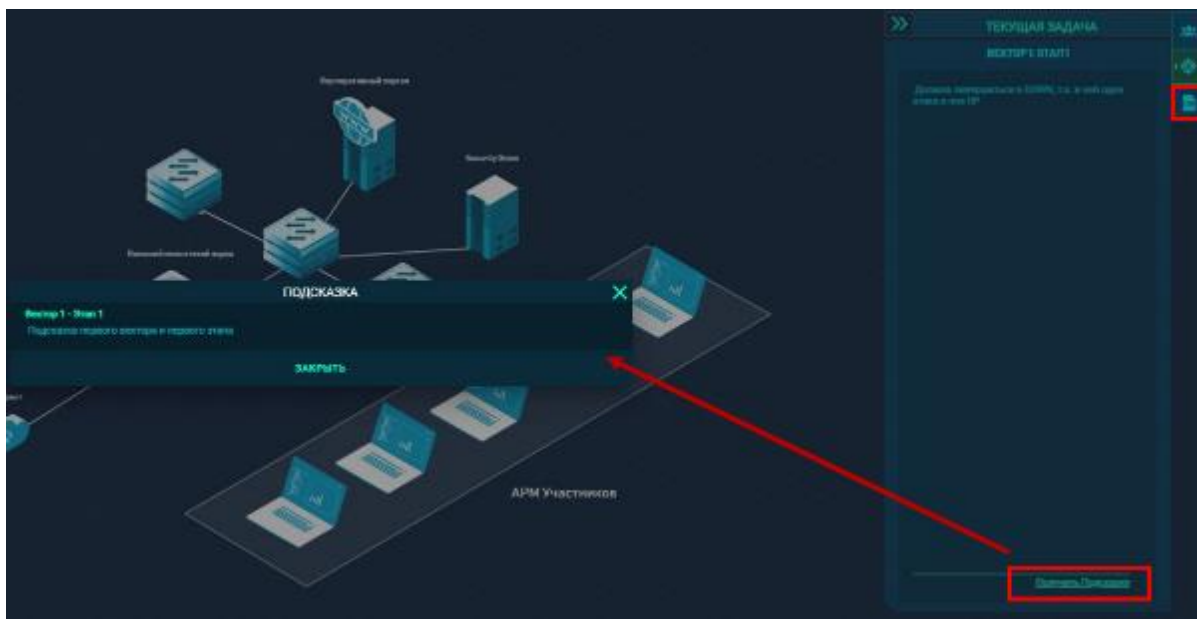






Рис. 50 – Окна с текущей задачей и подсказкой

Информация о задачах на этапы и подсказках прописана в конфигурационных файлах миссии. Соответственно, если в конфигурационных файлах не прописана информация о подсказках, то кнопка **«Получить подсказку»** в мероприятии отсутствует. Вся вкладка с информацией о текущей задаче закрывается при повторном нажатии на кнопку .

8. Историю событий с момента начала мероприятия до текущего момента можно посмотреть по кнопке  (Рис. 45, п. 7, 51). Свернуть/развернуть историю событий можно по кнопке . Вся вкладка с историей событий закрывается при повторном нажатии на кнопку .

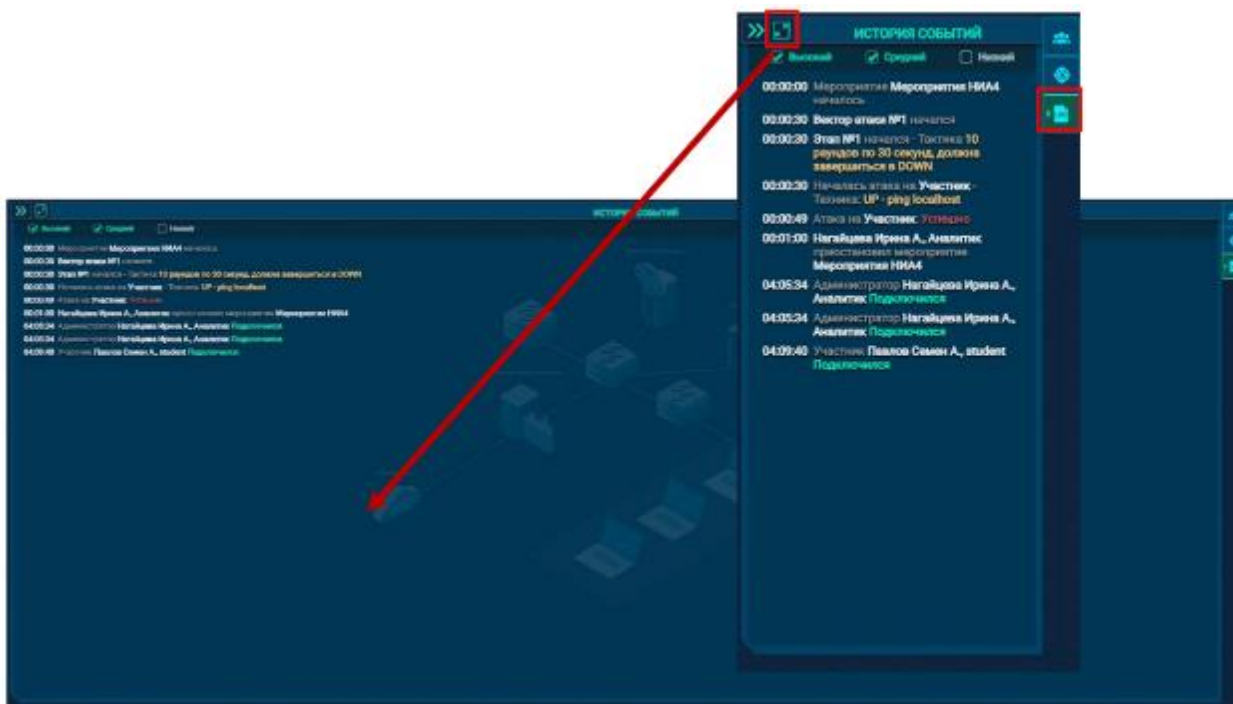


Рис. 51 – История событий мероприятия

### 3.1.4. Управление пользователями

Чтобы получить доступ к управлению всеми созданными на платформе пользователями, необходимо выбрать из главного меню раздел «Админпанель», вкладка «Пользователи» (Рис. 52).

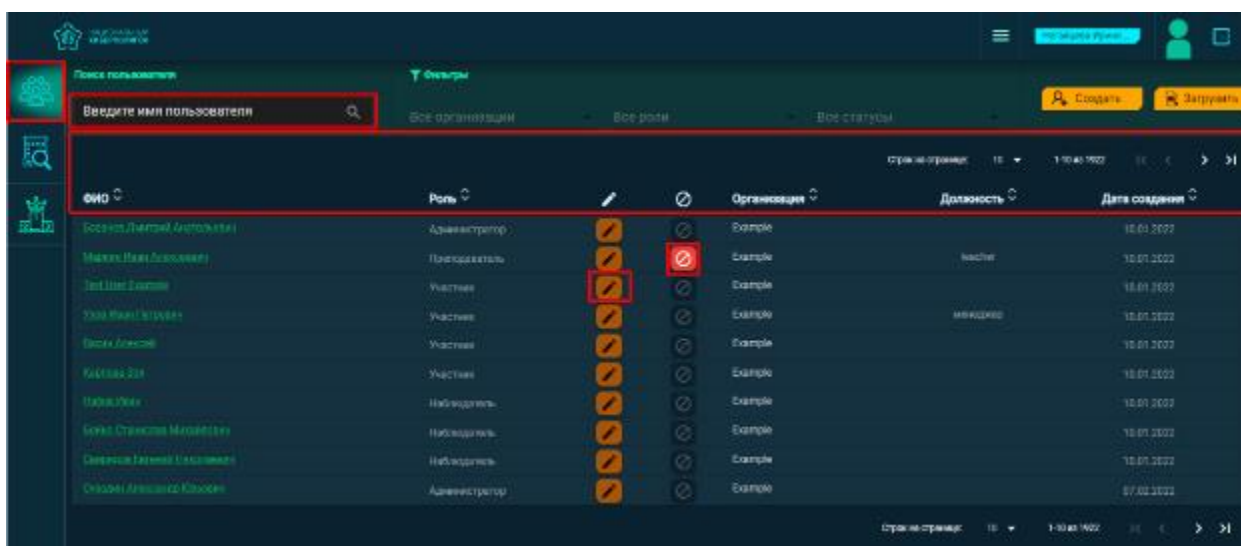



Рис. 52 – Админпанель. Вкладка «Пользователи»

Информация о пользователях представлена в виде таблицы:

1. ФИО – Фамилия, Имя и Отчество пользователя.
2. Роль пользователя.
3. Редактирование профиля пользователя по кнопке .

4. Блокировка пользователя.
5. Организация, к которой относится пользователь.
6. Должность пользователя.
7. Дата создания профиля пользователя на платформе.

На вкладке доступна функция поиска пользователя по ФИО, сортировка по столбцам, а также реализовано постраничное отображение всех созданных на платформе пользователей (Рис. 52).

Можно воспользоваться фильтром по названию организации (Рис. 53), роли (Рис. 54) и по статусу пользователя на платформе (заблокирован пользователь или нет, Рис. 55).

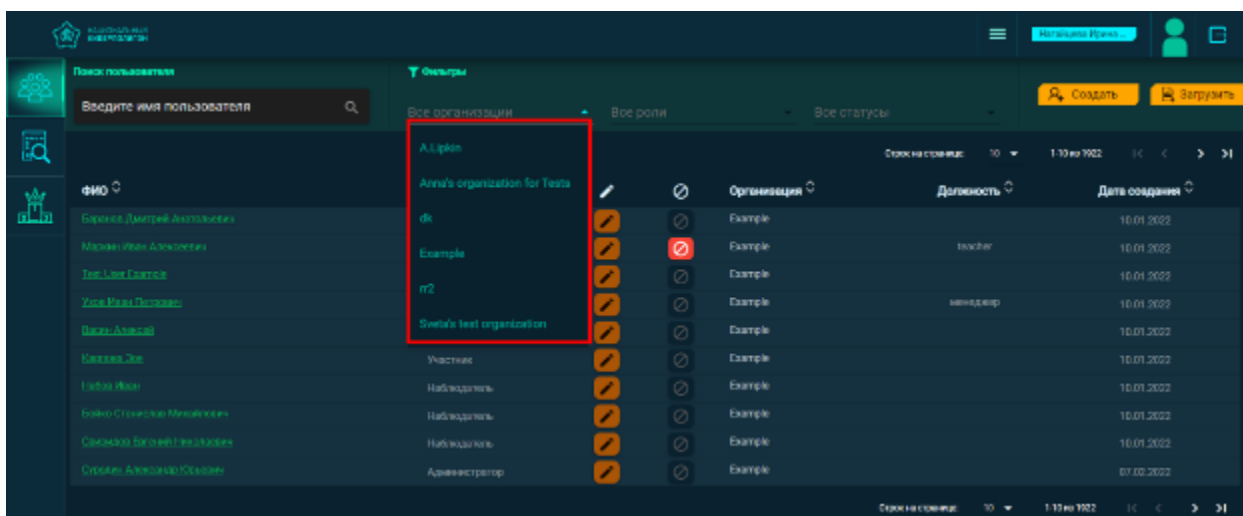


Рис. 53 – Фильтр по названию организации

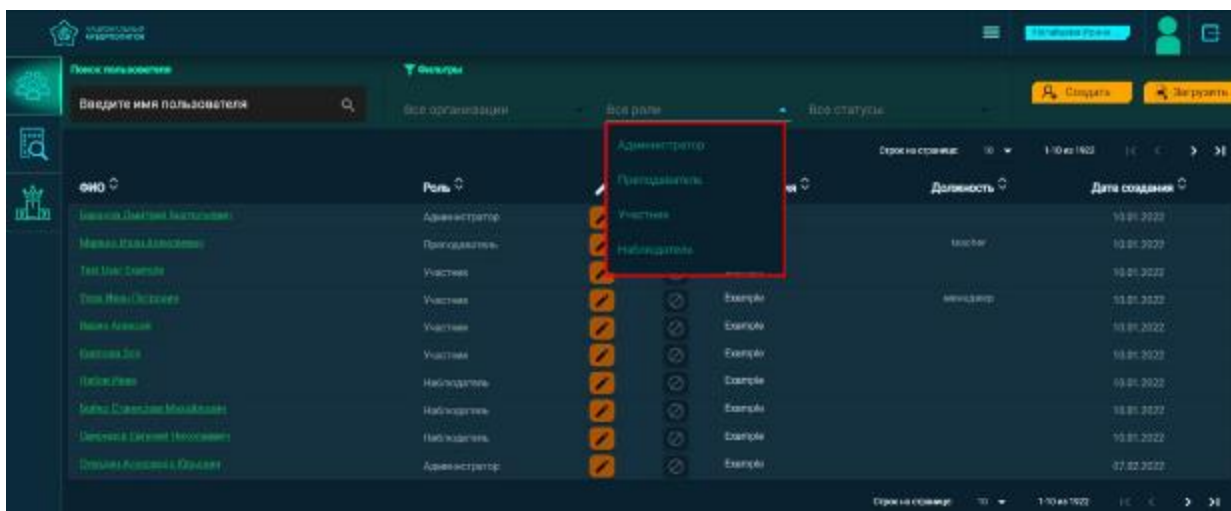


Рис. 54 – Фильтр по роли пользователя

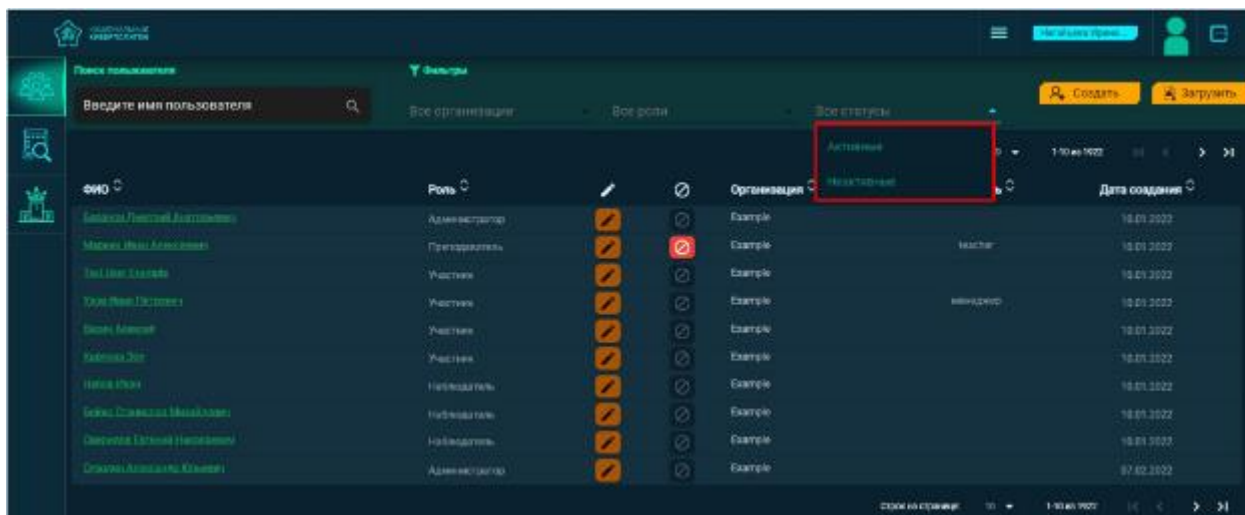


Рис. 55 – Фильтр по активности

### 3.1.4.1. Роли пользователей

На платформе существует 4 роли пользователей: администратор, преподаватель, участник и наблюдатель. При клике на ФИО пользователя в общей таблице пользователей (Рис. 52) открывается профиль пользователя.

1. Роль «администратор» (Рис. 56).

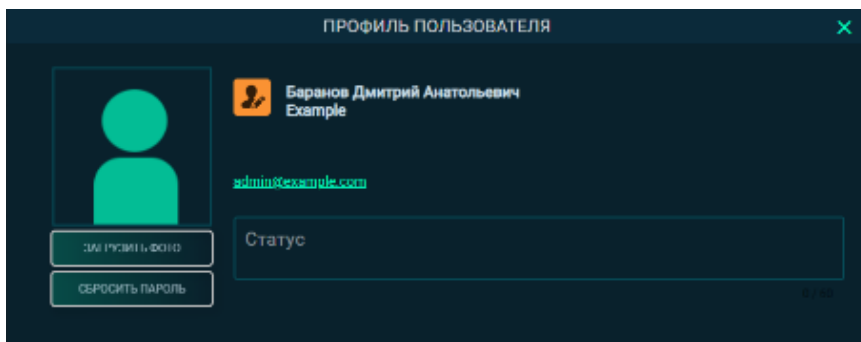


Рис. 56 – Форма «Профиль пользователя» с ролью «администратор»

2. Роль «преподаватель» (Рис. 57).

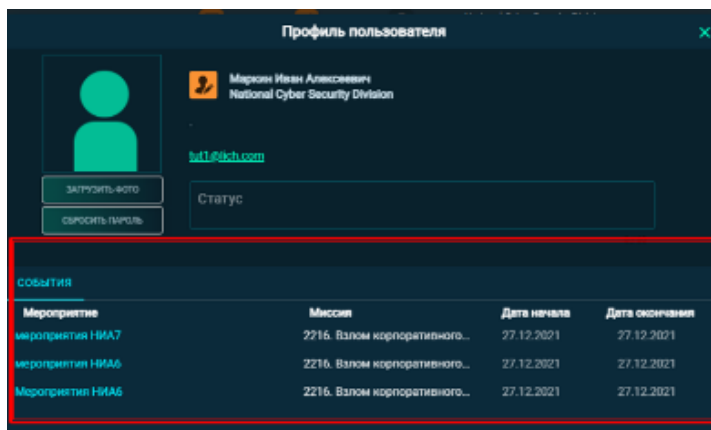


Рис. 57 – Форма «Профиль пользователя» с ролью «преподаватель»

Во вкладке «События» отображается список всех завершенных мероприятий, в которых принимал участие преподаватель.

3. Роль «участник» (Рис. 58).

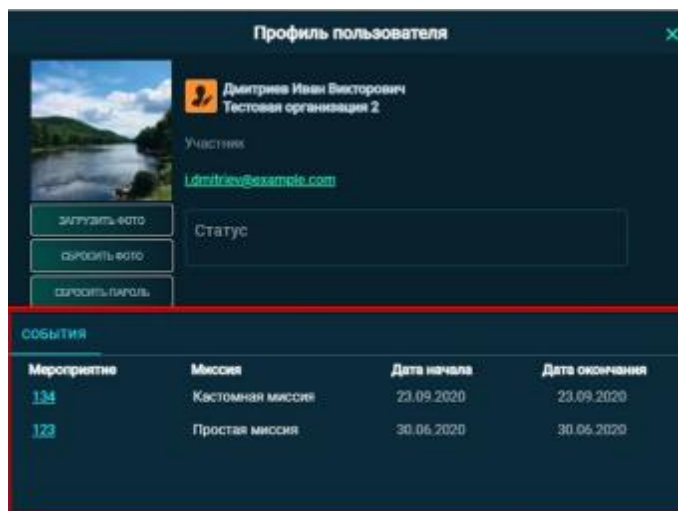


Рис. 58 – Форма «Профиль пользователя» с ролью «участник»

Во вкладке «События» отображается список всех завершенных мероприятий, в которых принимал участие участник.

4. Роль «наблюдатель» (Рис. 59).

Во вкладке «События» отображается список всех завершенных мероприятий, в которых принимал участие наблюдатель.

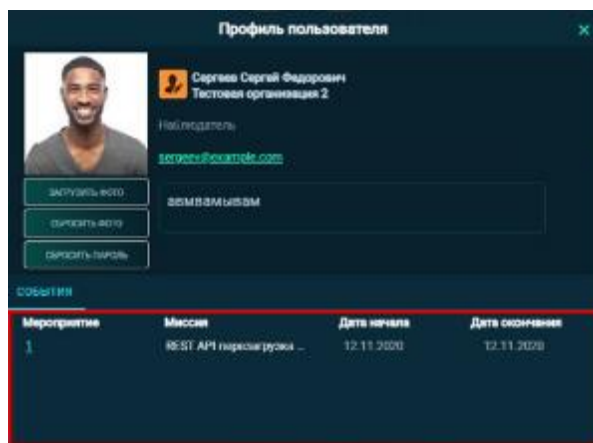


Рис. 59 – Форма «Профиль пользователя» с ролью «наблюдатель»

*Примечание. Преподавателю в общем перечне всех пользователей платформы видны только пользователи организации, к которой он прикреплен (Рис. 60).*



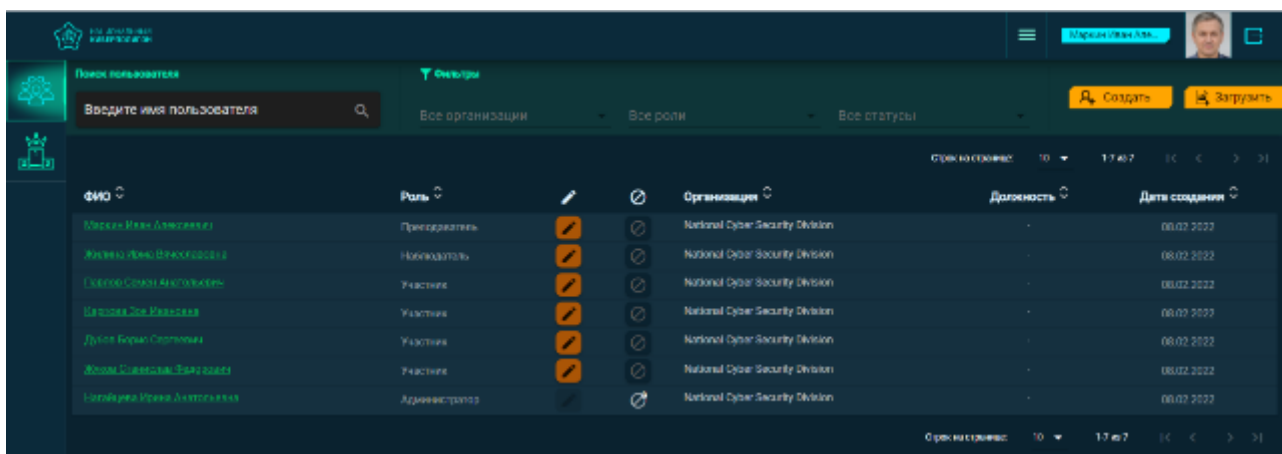


Рис. 60 – Админпанель для роли «преподаватель»

### 3.1.4.2. Регистрация и редактирование пользователей

Чтобы создать нового пользователя на платформе необходимо нажать на кнопку «Создать» на верхней панели формы «Пользователи» (Рис. 61).

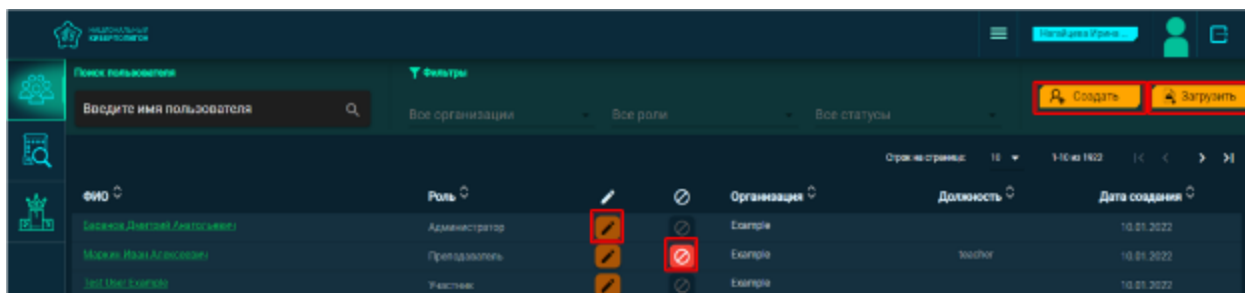


Рис. 61 – Админпанель. Вкладка «Пользователи»

В открывшейся форме «Создание пользователя» необходимо заполнить все поля: ФИО, электронная почта, организация, к которой относится пользователь, роль – и нажать на кнопку «Сохранить» (Рис. 62). После этого пользователю придет письмо с ссылкой для указания пароля.

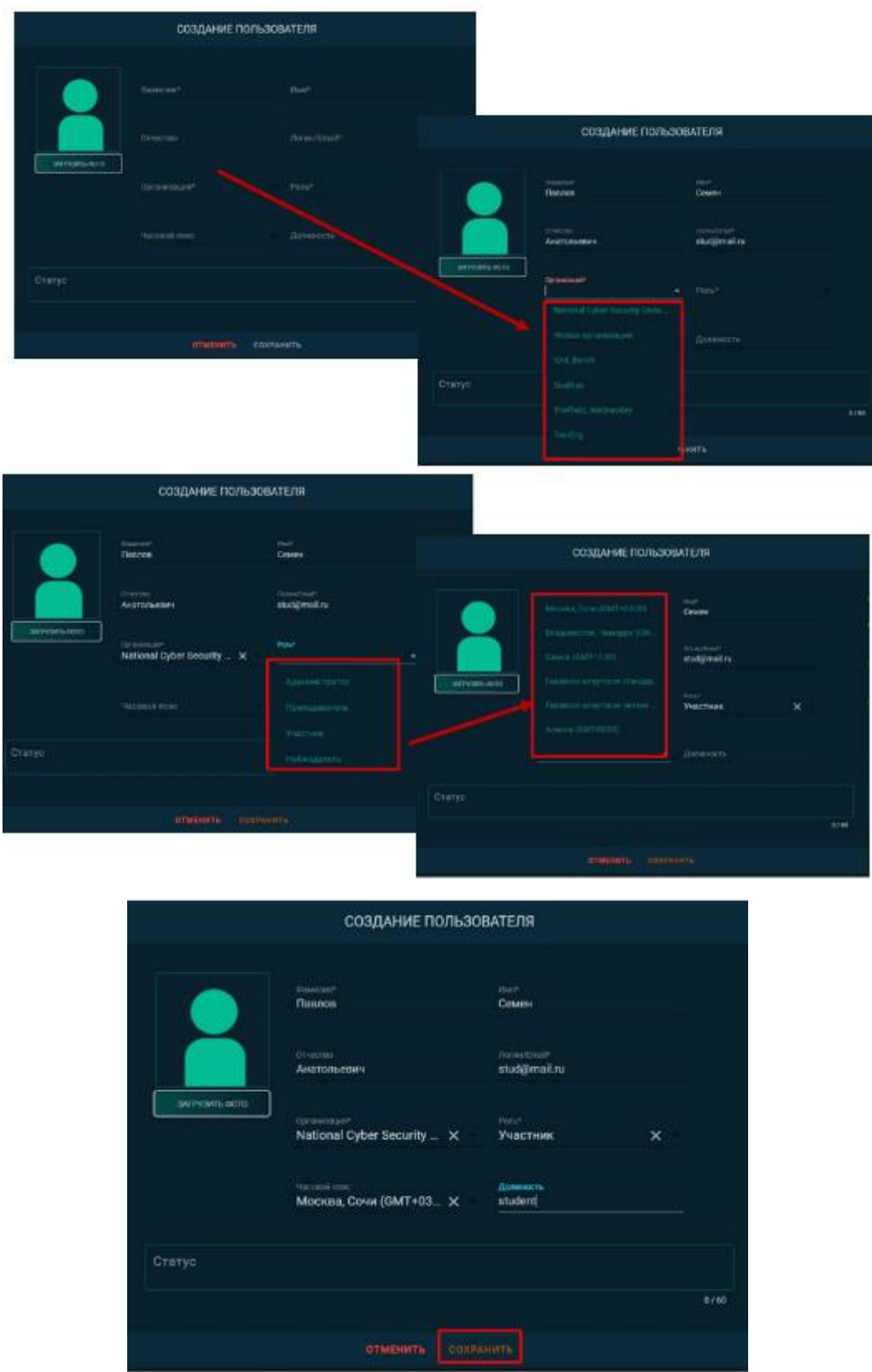


Рис. 62 – Форма «Создание пользователя»

Примечание. Преподаватель может создавать новых пользователей (участников, преподавателей и наблюдателей) только для организации, к которой прикреплен сам. Возможности создать пользователя с ролью администратора у него нет.

Чтобы одновременно загрузить на платформу несколько пользователей, необходимо нажать на кнопку «Загрузить» на верхней панели формы «Пользователи» (Рис. 61). В открывшейся форме «Загрузка пользователей» заполнить необходимые поля («Организация» и «Часовой пояс») и выбрать (или перетащить на область) файл с данными о пользователях в формате .XLSX (Рис. 63). Размер файла не должен превышать 1 Мбайт (структуру файла см. в Приложении А).

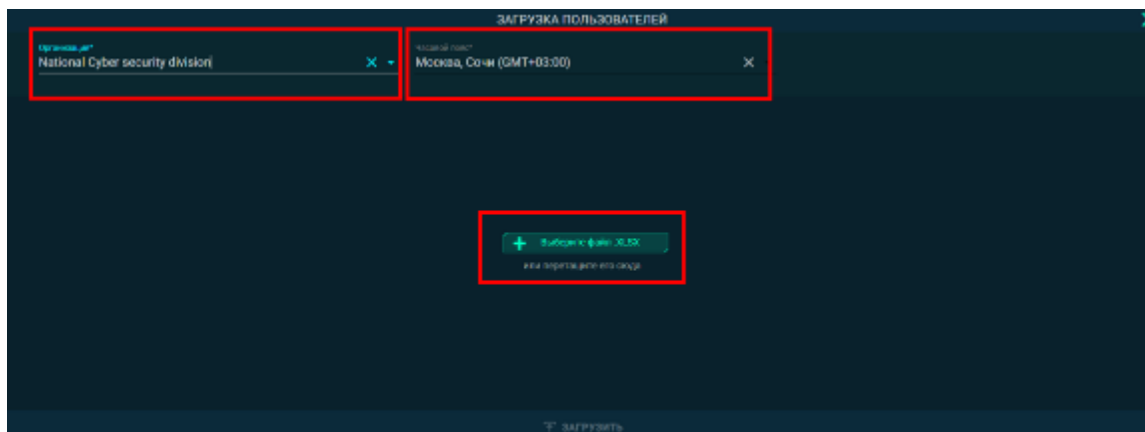


Рис. 63 – Форма «Загрузка пользователей»

Если в загружаемом файле с данными о пользователях есть ошибки (некорректный формат данных, задано неверное количество столбцов и др.), то загрузить его будет невозможно и появится окно с уведомлением об ошибке.

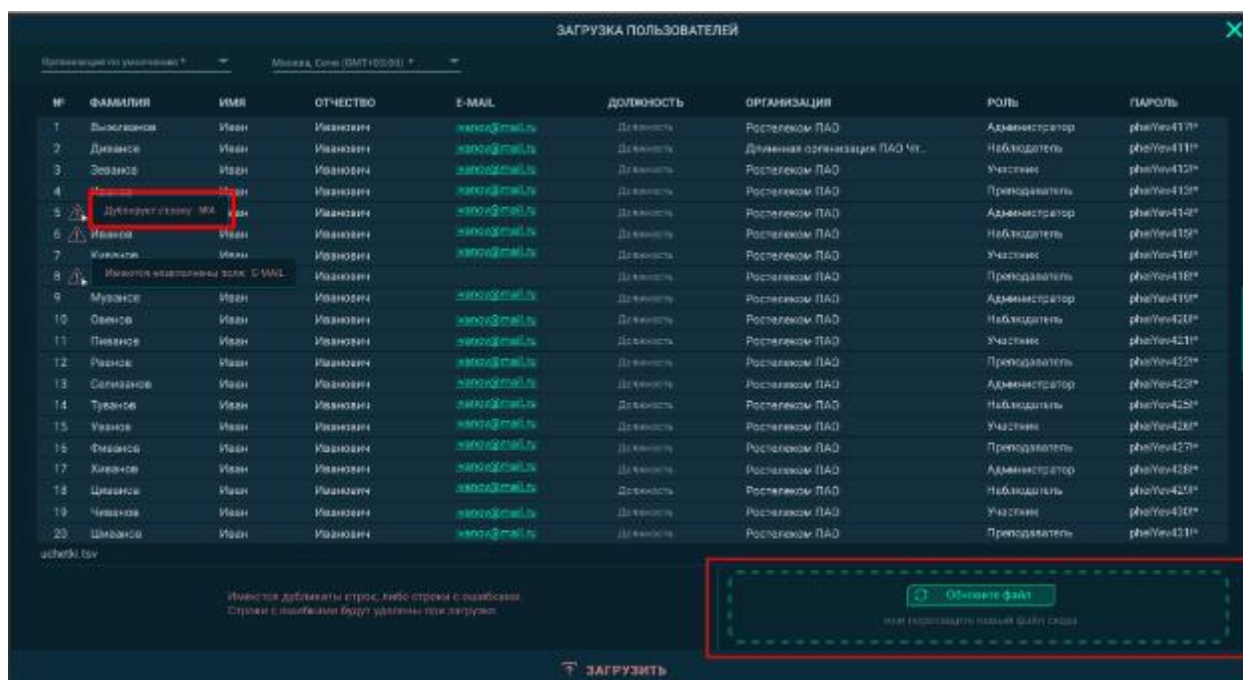



Рис. 64 – Форма «Загрузка пользователей» с ошибками в загруженных данных

Если в загружаемом файле у пользователей указаны организации, к которым их необходимо прикрепить и эти организации не заведены на платформе, то при загрузке указанные в файле организации автоматически создаются и к ним прикрепляются новые пользователи.

В случае отсутствия в загружаемом файле у пользователей указания о принадлежности к какой-либо организации при загрузке вновь созданные пользователи прикрепятся к организации, указанной в поле **«Организация»** формы «Загрузка пользователей».

**Для редактирования** профиля пользователя необходимо нажать на иконку  напротив ФИО в общей таблице пользователей (Рис. 61), после чего откроется форма для редактирования пользователя (Рис. 65).

Для изменения пароля пользователя необходимо нажать на кнопку **«Сбросить пароль»** на форме **«Редактировать пользователя»** или в профиле пользователя. После чего на почту пользователя, указанную в профиле, придет ссылка для смены пароля.

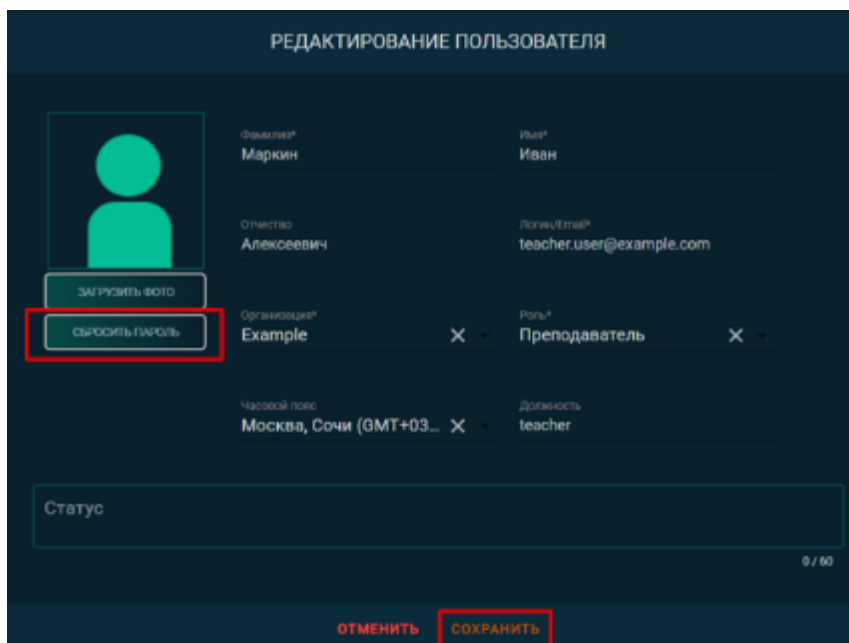



Рис. 65 – Форма «Редактирование пользователя»

### 3.1.4.3. Блокировка пользователей

Если необходимо, чтобы пользователь не имел доступа к платформе (не мог авторизоваться) и не отображался в списках при создании/редактировании мероприятий, то есть возможность его заблокировать. Для этого нужно нажать на кнопку  в строке с конкретным пользователем в общей таблице пользователей, при этом кнопка меняет свой цвет на красный (Рис. 66), что означает, что пользователь заблокирован.

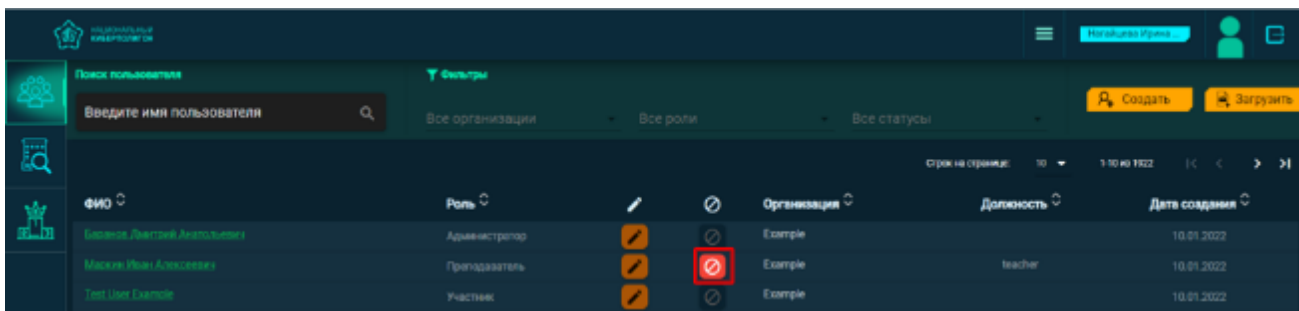


Рис. 66 – Заблокированные пользователи

Нельзя заблокировать пользователя, если на момент блокировки он участвует в мероприятии. При попытке его заблокировать появится уведомление о невозможности блокировки (Рис. 67).

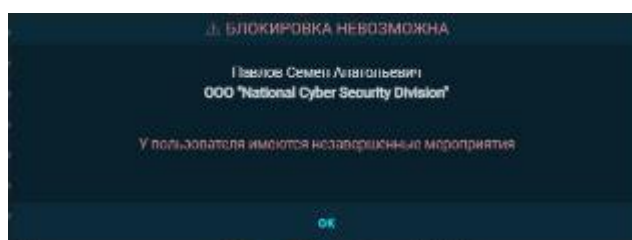


Рис. 67 – Уведомление о невозможности блокировки пользователя

Пользователя с ролью администратора нельзя заблокировать, если он является последним администратором в системе.

### 3.1.5. Управление организациями

Для управления всеми созданными на платформе организациями необходимо перейти в разделе «Админпанель» во вкладку «Организации» (Рис. 68).

*Примечание. Вкладка «Организации» доступна только администратору.*

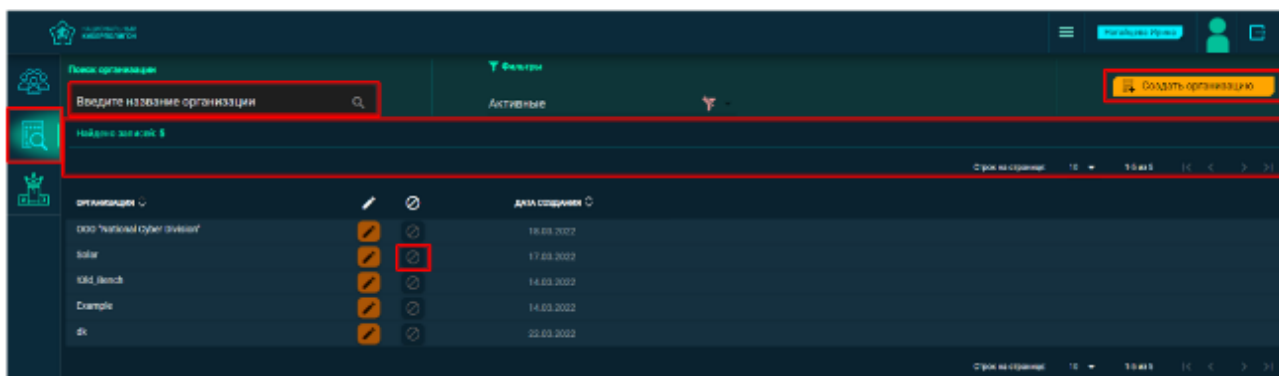




Рис. 68 – Админпанель. Вкладка «Организации»

Информация об организациях представлена в виде таблицы:

1. Название организации.
2. Редактирование организации доступно по иконке .

3. Блокировка организации возможна при нажатии на иконку .
4. Дата создания организации на платформе.

На вкладке можно воспользоваться функцией поиска организации по названию, доступен фильтр по дате создания и по активности организации на платформе (заблокирована или нет), а также доступно постраничное отображение всех созданных на платформе организаций.

### 3.1.5.1. Регистрация и редактирование организаций

Чтобы создать новую организацию, необходимо нажать на кнопку **«Создать организацию»** на верхней панели формы **«Организации»** (Рис. 68). В открывшейся форме **«Создание организации»** необходимо заполнить поле с названием организации (оно должно быть уникальным) и проставить атрибут (галочку), является ли организация внутренней или нет (Рис. 69).

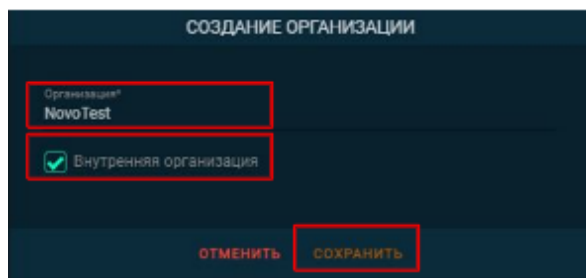



Рис. 69 – Форма «Создание организации»

Организации с атрибутом «Внутренняя организация» в списках организаций на всех формах выделяются жирным шрифтом и находятся в начале списка.

**Для редактирования организации** необходимо нажать на иконку  напротив названия организации в общей таблице всех организаций (Рис. 68), после чего откроется форма для редактирования организации (Рис. 70).

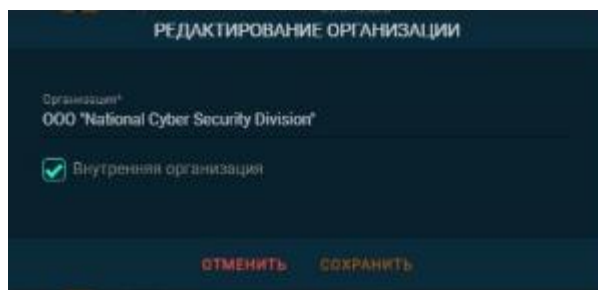



Рис. 70 – Форма «Редактирование организации»

### 3.1.5.2. Блокировка организаций

Если необходимо, чтобы организацию нельзя было использовать для создания мероприятий, а принадлежащие к ней пользователи не имели доступа к платформе (не могли авторизоваться), есть возможность ее заблокировать. Для этого необходимо нажать на кнопку  в строке с конкретной организацией в общей таблице организаций (Рис. 68), при этом кнопка изменит свой цвет на красный (Рис. 71), что означает, что организация заблокирована.

После блокировки у всех пользователей этой организации в списке пользователей иконка блокировки будет иметь бледно-красный цвет.

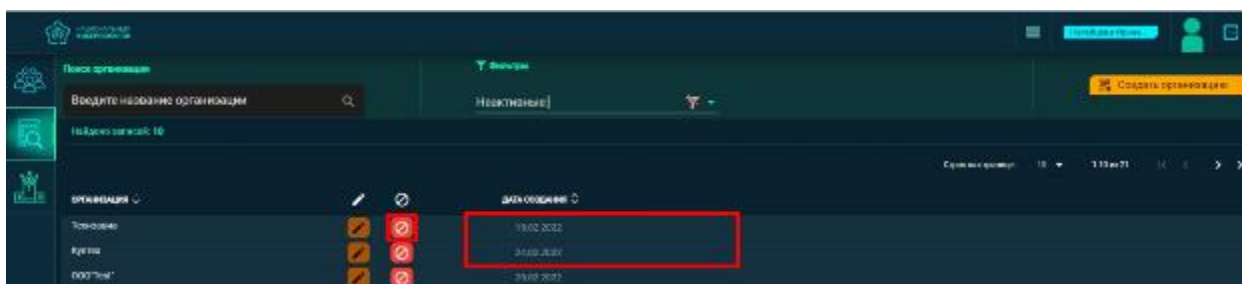


Рис. 71 – Заблокированные организации

Организацию нельзя заблокировать если:

- она имеет атрибут «Внутренняя организация»;
- если организация содержит последнего незаблокированного администратора;
- если на момент блокировки с ее участием есть незавершенные мероприятия. При попытке заблокировать такую организацию появится уведомление о невозможности блокировки (Рис. 72).

блокировки (Рис. 72).



Рис. 72 – Уведомление о невозможности блокировки организации

### 3.1.6. Перечень мероприятий

#### 3.1.6.1. Доступ к мероприятиям для администратора

Администратор может получить доступ к списку мероприятий, существующих на платформе следующими способами:

- Через главное меню, раздел **«Мероприятия»** (Рис. 73).

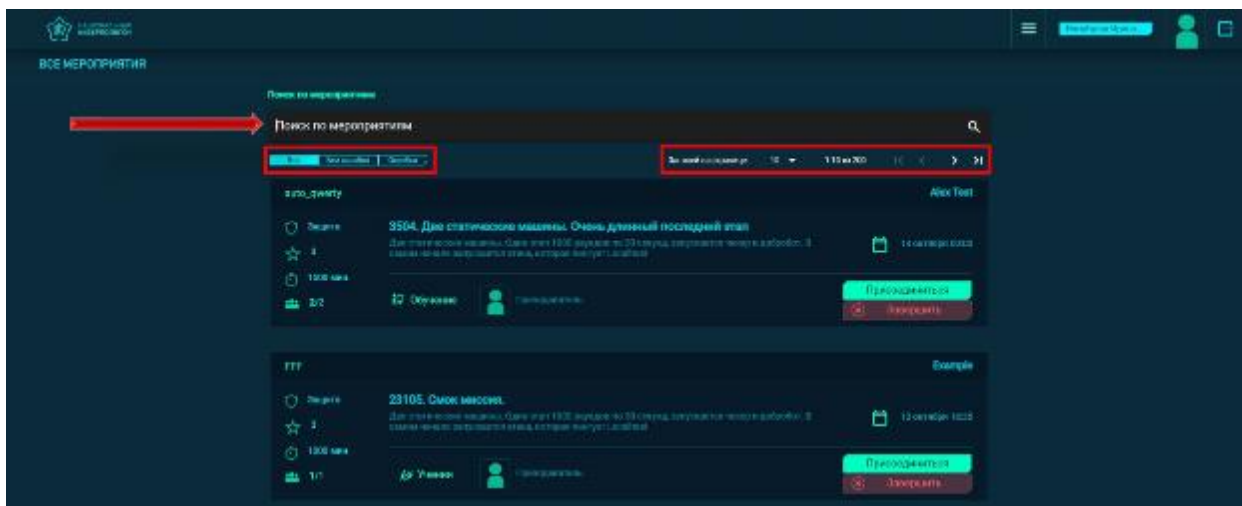


Рис. 73 – Форма «Все мероприятия» для администратора

Мероприятия представлены в виде списка карточек с кратким содержанием и возможностью присоединиться к мероприятию, подготовить, запустить или отменить его. Также доступно постраничное отображение всех карточек мероприятий, созданных на платформе (пейджинг).

- С помощью тумблера **«Все / Без ошибок / Ошибки»** есть возможность настроить отображение списка мероприятий таким образом, чтобы показывать/скрывать все мероприятия, успешно проведенные мероприятия, а также мероприятия, находящиеся в статусе **«Ошибка»** (Рис. 73). Для поиска ранее созданного мероприятия по названию можно воспользоваться функцией поиска.

При нажатии на название мероприятия осуществляется переход на карточку выбранного мероприятия.

#### 3.1.6.2. Доступ к мероприятиям для преподавателя

Для преподавателя доступ к списку мероприятий, созданных на данный момент на платформе, можно получить через главное меню, раздел **«Мероприятия»** (Рис. 74).



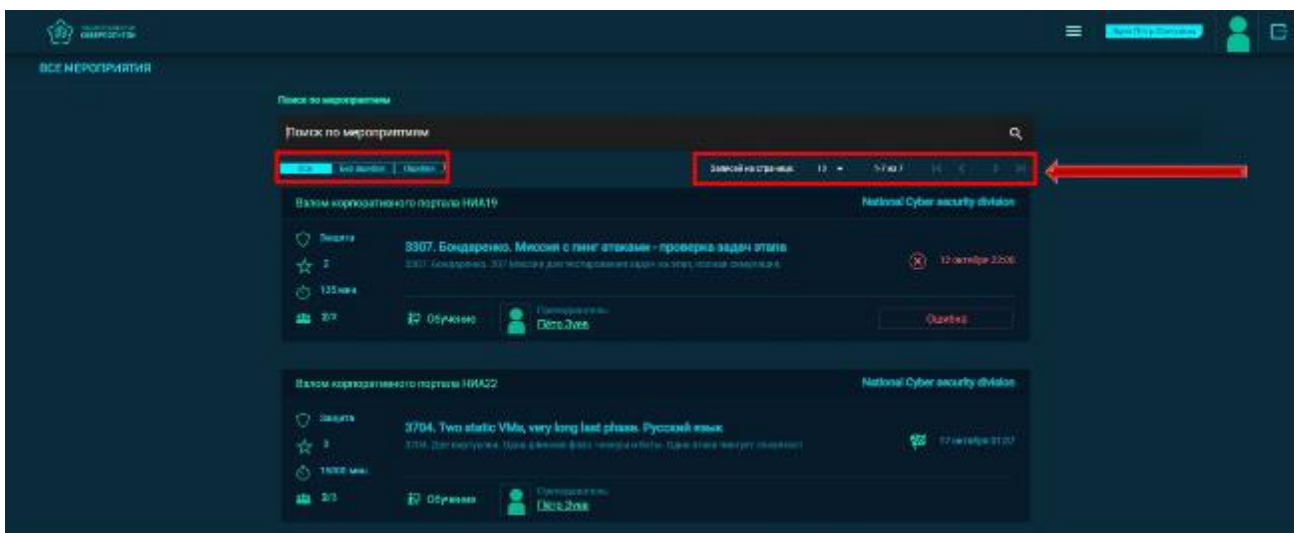


Рис. 74 – Форма «Все мероприятия» для преподавателя

Для поиска ранее созданного мероприятия по названию можно воспользоваться функцией поиска.

С помощью тумблера **«Все / Без ошибок / Ошибки»** есть возможность настроить отображение списка мероприятий таким образом, чтобы показывать/скрывать все мероприятия, успешно проведенные мероприятия, а также мероприятия, находящиеся в статусе **«Ошибка»** (Рис. 74). Также доступно постраничное отображение всех карточек мероприятий, созданных на платформе.

*Примечание. Преподавателю видны только те мероприятия, на которые он назначен в роли преподавателя. На карточках мероприятий управляющие кнопки («Отменить», «Подготовить», «Запустить») доступны только для администратора.*

### 3.1.7. Скоринг отчетов участников

#### 3.1.7.1. Заполнение отчетов участниками

Для оценки результатов участников мероприятия используется скоринг (оценка результатов), основные настройки которого производятся при создании мероприятия (Рис. 10, п. 14).

Обнаруженную в ходе мероприятия информацию об атаках участники вносят в форму **«Отчет участника»** и отправляют на оценку преподавателю до того, как мероприятие перешло в статус **«Подведение итогов»** или **«Завершено»** (Рис. 75).

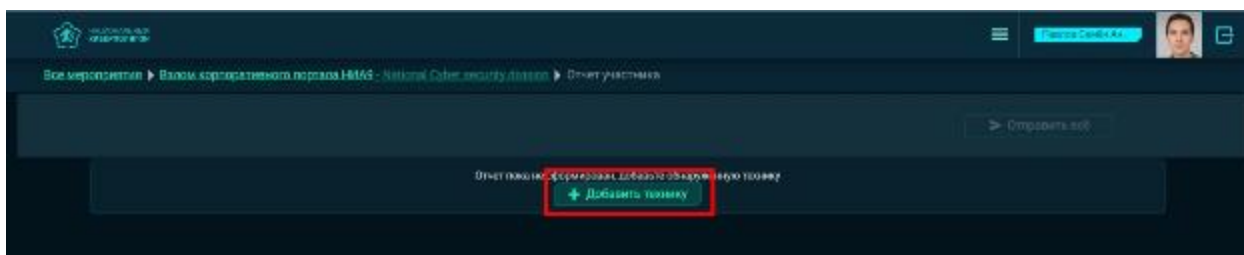


Рис. 75 – Добавление техник на форме отчета участника

### 3.1.7.2. Оценка результатов участников

После отправки отчета участником на карточке мероприятия напротив фамилии участника изменятся данные в столбцах (статус отчета, время последнего обновления отчета, количество отправленных отчетов, начисленные баллы), а также станет доступна кнопка для перехода на форму оценки отчета (Рис. 76).

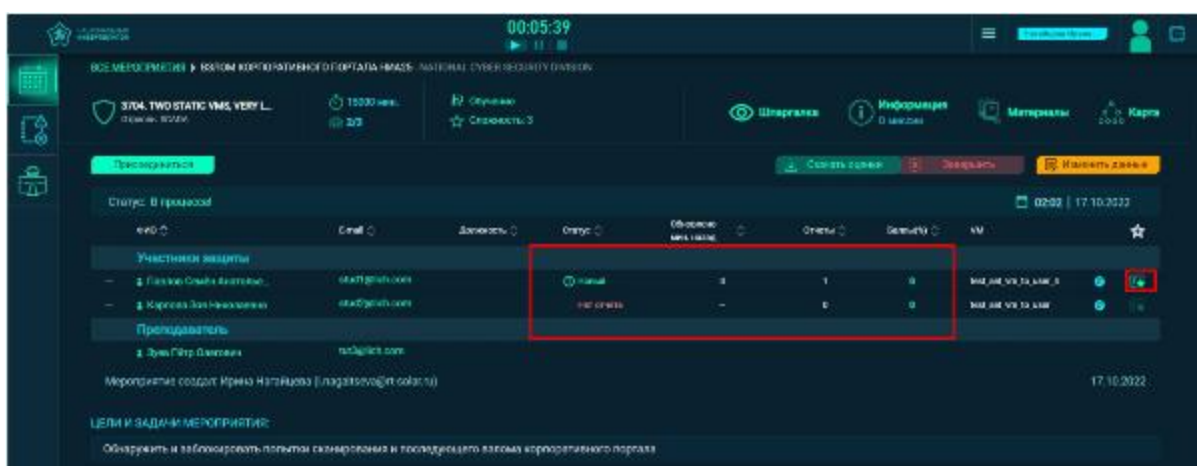


Рис. 76 – Карточка мероприятия с новым отчетом участника

*Примечание.* На платформу загружается справочник (конфигурационный файл `scoring_references.yaml`), в котором содержатся названия атак и техник, применяемых к этим атакам. При загрузке платформы справочник попадает в базу данных.

На стенде в папку с ID миссии, на основании которой создается мероприятие, загружается:

- справочник (конфигурационный файл `scoring_references.yaml`), в котором содержатся названия атак и техник, применяемых к этим атакам;
- конфигурационный файл `scoring_report.yaml` (эталонный отчет миссии), который служит для автоматической/автоматизированной оценки результатов и навыков участников методом сопоставления их отчета с эталонным отчетом с начислением очков.

Для формирования эталонного отчета из файла `scoring_references.yaml` берутся коды техник и атрибуты и указывается их фактическое значение, необходимое для конкретного сценария, разрабатываемое сценаристом.

Для проверки и публикации результатов отчета участника преподавателю необходимо перейти на форму оценки и проверить все заполненные участником техники, которые автоматически оценила система, сопоставляя их с эталонным отчетом (Рис. 76).

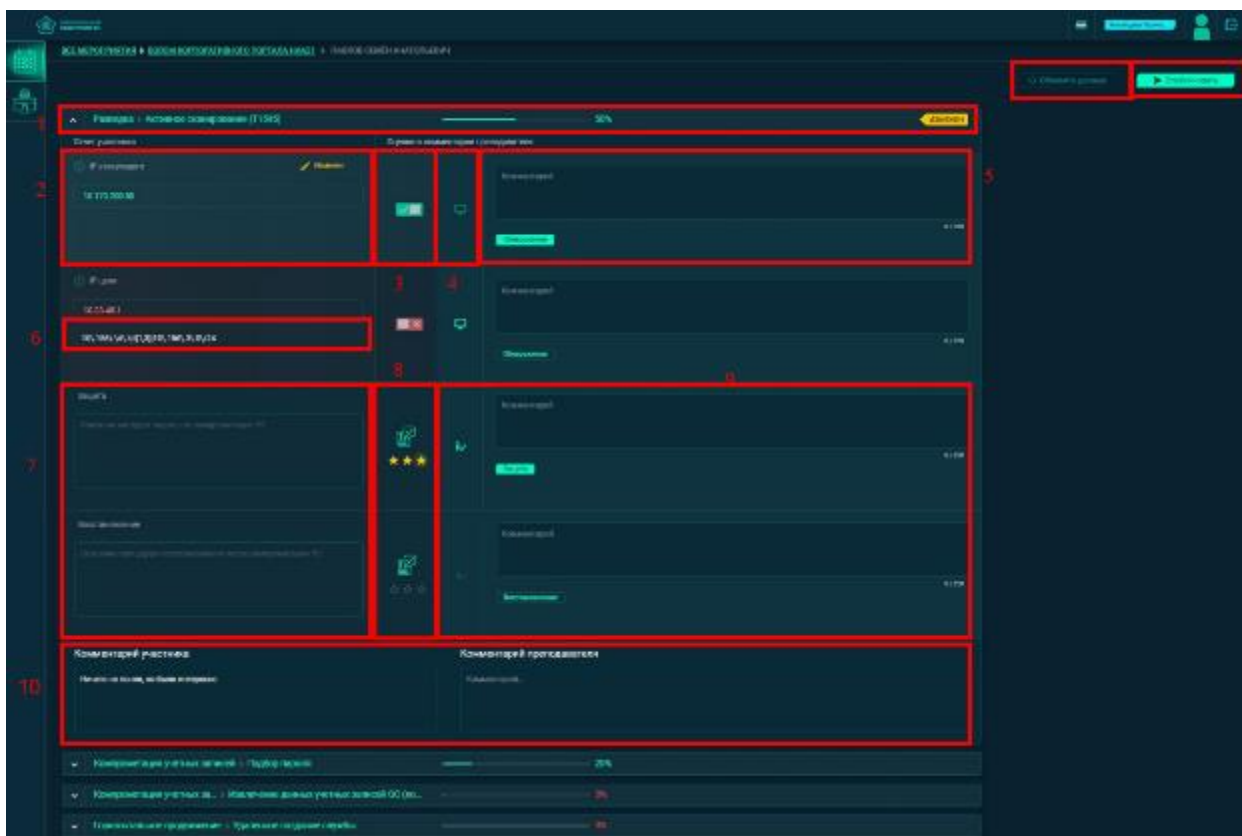




Рис. 77 – Форма оценки отчета участника

На форме оценки отчета участника есть доступ к следующей информации:

1. Название атакующей техники и процент правильности заполнения всей техники по 100-процентной шкале, а также тег, показывающий текущее состояние техники (Новый, Изменен; Рис. 77, п.1). Тег определяется исходя из сравнения отчета из последней опубликованной оценки и отчета, открытого на оценке у администратора/преподавателя.

Первый раз заполненные и отправленные участником техники в отчете будут иметь тег **«НОВЫЙ»**. Также иконка  **Новый** появляется рядом с IoC'ом в случае, если участник заполнил его после последней публикации оценки (ранее он был не заполнен).

Если участник внес изменения в ранее отправленную технику, то у техники появится тег **«ИЗМЕНЕН»** (Рис. 77), а рядом с измененным IoC'ом в технике появится иконка  **Изменен** – в случае изменения IoC'a участником с момента последней публикации оценки (Рис. 77, п. 2).

Зеленая подсветка названия свернутой техники означает, что она прошла сравнение с техникой из эталонного отчета, красная подсветка – что техника для сравнения в эталонном отчете не найдена.



Рис. 78 – Форма оценки отчета участника со свернутыми техниками и тегами

Если участник создает аналогичную технику, которая уже есть в его отчете, но вносит в нее больше правильных ответов, чем в предыдущей, то на форме оценки преподавателя после обновления (публикации) появятся техники одного типа, но последняя (более правильная) сравнится с эталонным отчетом и будет подсвечиваться зеленым, а первая станет подсвечиваться красным (Рис. 79).

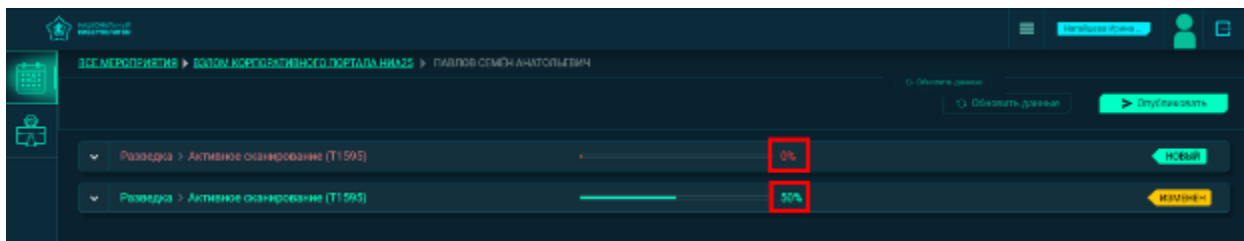







Рис. 79 – Форма оценки отчета участника с двумя аналогичными техниками


2. Правильно заполненный IoC (Рис. 77, п. 2).
3. Переключатель, позволяющий зачесть/не зачесть IoC (Рис. 77, п. 3).
4. Иконка, показывающая каким образом произведена оценка (Рис. 77, п. 4):
  - иконка –  автоматически оценено системой;
  - иконка –  автоматически оценено системой как ошибка;
  - иконка –  преподаватель изменил оценку системы;
  - иконка –  оценено преподавателем как правильный ответ (применяется для оценки полей «Защита» и «Восстановление»).
  - иконка  – не оценено преподавателем (применяется для оценки полей «Защита» и «Восстановление»).
5. Комментарии (обоснование) преподавателя по применению навыка для каждого IoC'a и список навыков (тегов), которые могут быть применены для выявления данного IoC'a (Рис. 77, п. 5). Закладываются сценаристом при составлении эталонного отчета и проставляются преподавателем к конкретному IoC'у при желании.
6. Если IoC заполнен неправильно, то появится подсказка из эталонного отчета (Рис.

77, п. 6).

Преподаватель при оценке присланного отчета имеет возможность изменить результат оценки каждого IoC'a, который автоматически произвела система (Рис. 77, п. 3), вручную применить навык к IoC'у и обосновать его комментарием (Рис. 77, п. 5, 9).

7. Заполненные участником в свободной форме поля **«Защита»** и **«Восстановление»** (Рис. 77, п. 7).

8. Блок иконок полей **«Защита»** и **«Восстановление»** состоит из:

- кнопки  при нажатии на которую появляется всплывающее окно с эталонным описанием, на которое преподаватель может ориентироваться при оценке данных полей (Рис. 80);

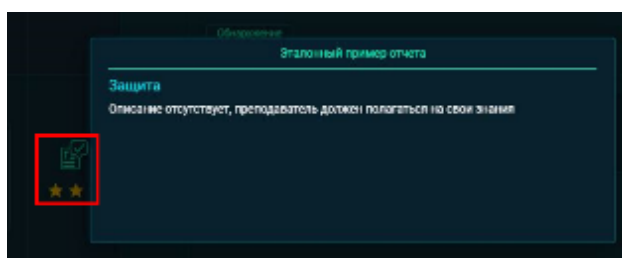



Рис. 80 – Подсказка для заполнения полей **«Защита»** и **«Восстановление»**

- иконок-звезд , которые проставляются преподавателем за заполнение участником полей **«Защита»** и **«Восстановление»** (Рис. 77, п. 8). Количество звезд будет влиять на общий результат по технике, если в эталонном отчете прописаны баллы за защиту и восстановление (т. е. одна звезда – это 1/3 от максимальной оценки, прописанной в эталонном отчете).

9. Комментарии преподавателя по описанию защиты, восстановления и список навыков (тегов) (Рис. 77, п. 9).

10. Комментарий участника и комментарий преподавателя на всю технику (Рис. 77, п. 10).

При наведении курсора на поля **«Защита»**, **«Восстановление»**, комментарии участника и преподавателя отображается всплывающее окно с полным описанием того, что указано в данных полях (Рис. 77, п. 7, 10).

В некоторых мероприятиях при оценке отчета участника в техниках отображаются несовпавшие IoC'и.

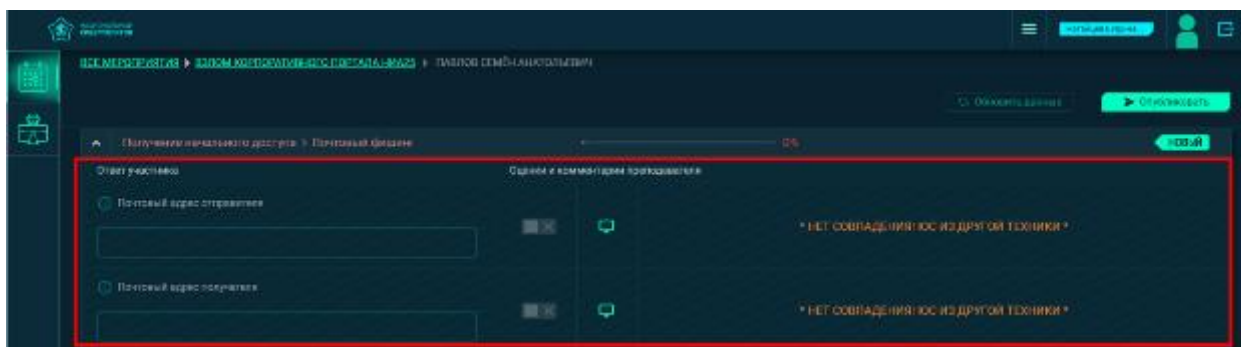


Рис. 81 – Отображение несовпавших IoC'ов при оценке отчета участника

При добавлении техники в отчет участника происходит объединение IoC'ов из справочника и IoC'ов из эталонного отчета для данной техники в одно множество. А также в эталонном отчете может быть несколько техник одинакового типа (например, «Активное сканирование») с разным набором IoC'ов.

При оценке подбирается техника из эталонного отчета для данного мероприятия, которая наиболее подходит под объединенное множество IoC'ов, и сравнивается с техникой из отчета участника один к одному. После сравнения в техниках отчета участника могут появиться IoC'и, которые не используются в эталонном отчете для данной техники. Такие IoC'и называются несовпавшими IoC'ами и на форме оценки будут отображаться в виде недоступных полей с надписью: «**НЕТ СОВПАДЕНИЙ ИОС'ОВ ИЗ ДРУГОЙ ТЕХНИКИ**» (Рис. 81).

Если участник при заполнении отчета внесет информацию в поля с несовпавшими IoC'ами, то такие IoC'и не будут засчитаны (IoC'и заблокированы).

Если в мероприятии настроен автоматизированный скоринг, то во время оценки преподавателем отчета участника на карточке мероприятия появляется статус отчета «**На оценке**» (Рис. 82).

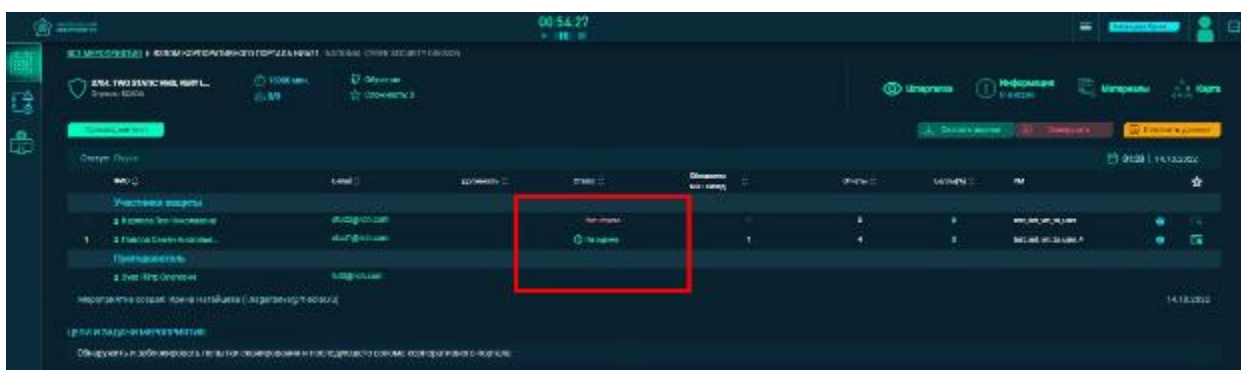


Рис. 82 – Карточка мероприятия с отчетом участника в процессе оценки

После оценки правильности заполнения всех IoC'ов и полей в отчете преподаватель нажимает кнопку «**Опубликовать**» (Рис. 77), что приводит к сохранению отчета и всех

внесенных правок и пересчету баллов. На карточке мероприятия статус отчета изменится на «Оценен» (Рис. 83).

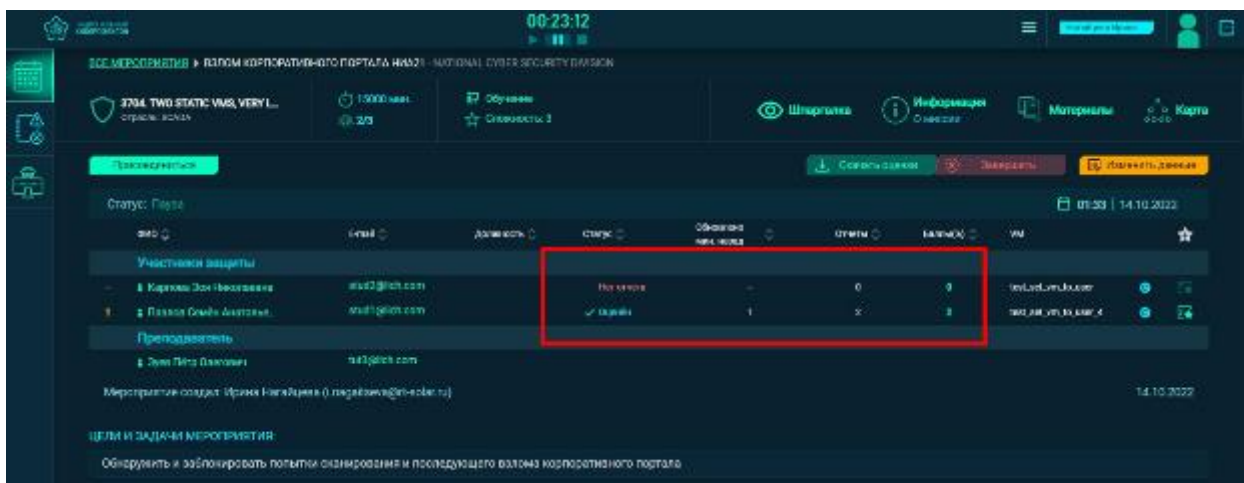


Рис. 83 – Карточка мероприятия с оцененным отчетом участника

Если во время мероприятия участник несколько раз обновляет отчет, то при каждом сохранении отчета запускается процедура полного пересчета баллов по данному участнику.

В случае, если участник обновил отчет в момент проверки преподавателем его предыдущего отчета, то у преподавателя на верхней панели появится уведомление «**Имеются обновления по отчету**» и, чтобы перейти к проверке обновленного отчета, ему необходимо обновить данные, нажав на кнопку «**Обновить данные**» (произойдет слияние обработанного преподавателем отчета участника с новыми правками, внесенными участником в отчет) (Рис. 84).

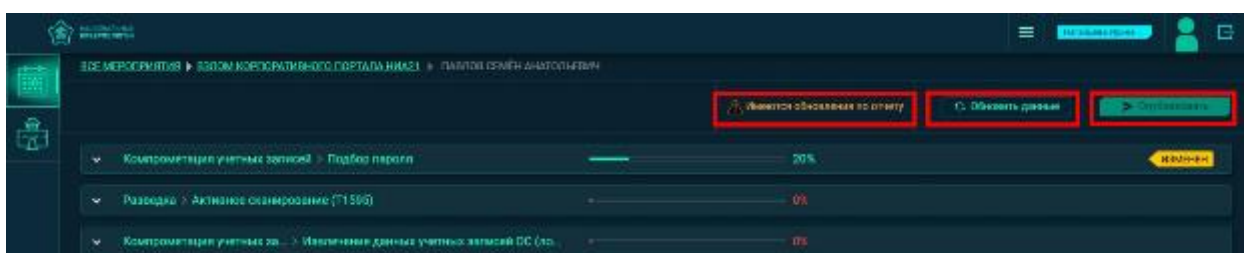


Рис. 84 – Форма оценки устаревшего отчета участника

Если в мероприятии настроен автоматический скоринг (без тренера), то сразу после отправки отчета участника система автоматически проведет оценку и опубликует результаты.

### 3.1.7.3. Просмотр результатов участников на табло результатов

Для отображения опубликованных результатов участников мероприятия используется форма «**Табло результатов**» (единая для всей платформы). Попасть на нее можно из главного

меню, выбрав раздел **«Табло результатов»** (Рис. 85), или с формы проведения мероприятия, нажав на соответствующую кнопку (Рис. 45 п. 3).

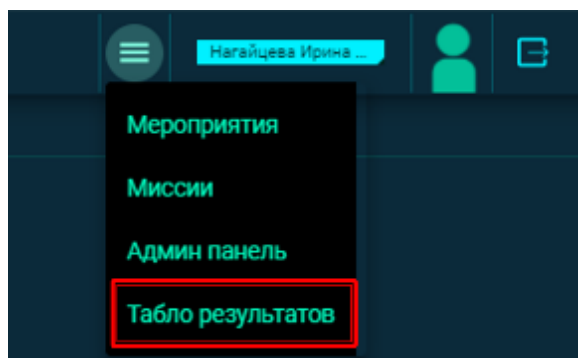


Рис. 85 – Главное меню «Табло результатов» с одним мероприятием

Информация о результатах участников представлена в виде таблицы (Рис. 86):

- отображение места участника в общей таблице;
- ФИО участников (либо названия мероприятий, если добавлено несколько мероприятий);
- набранные баллы;
- организация, к которой прикреплен участник.




Рис. 86 – Форма «Табло результатов» с одним мероприятием

На форме можно воспользоваться сортировкой по столбцам. Сортировка является индивидуальной в рамках открытой вкладки (сессии) браузера пользователя несмотря на то, что форма «Табло результатов» единая для всей платформы.

*Примечание. Табло результатов доступно к просмотру пользователям с другими ролями, если мероприятие, в котором они участвуют, было добавлено на табло результатов администратором.*

#### 3.1.7.4. Настройка табло результатов

*Примечание. Администратор имеет возможность настраивать табло результатов (добавлять мероприятия).*

Для того чтобы мероприятие отображалось на общем табло, необходимо его добавить, нажав на кнопку  и выбрав из списка активных мероприятий (Рис. 87).



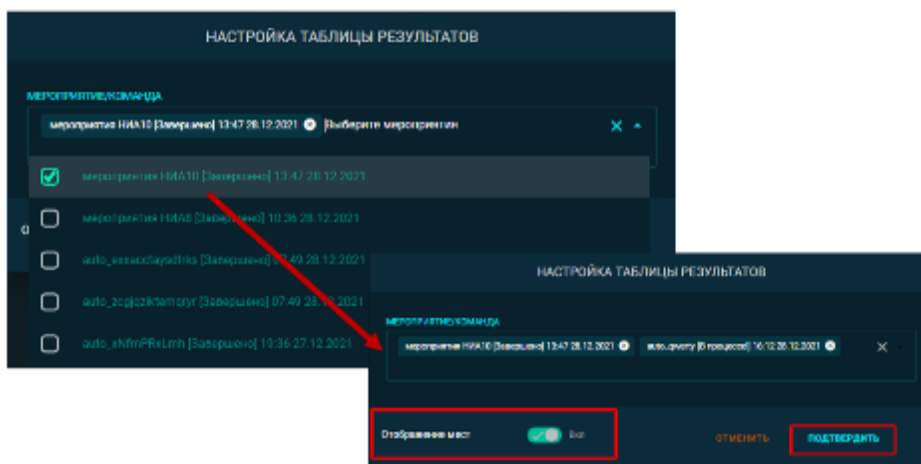


Рис. 87 – Настройка таблицы результатов

Если на форме «**Настройка таблицы результатов**» переключатель «**Отображение мест**» перевести в режим «Выкл», то в таблице результатов будет скрыт первый столбец с отображением мест участников.

Если на табло добавлено одно мероприятие, то в списке участников отображаются все участники этого мероприятия и их баллы (Рис. 86). Если на табло добавлено несколько мероприятий, то в списке отобразится по одному результату участника с максимальным количеством баллов из каждого мероприятия (Рис. 88).

Если в одном мероприятии несколько участников набрали одинаковое максимальное количество баллов, то на табло результатов будет показан один из них (выбранный случайным образом).

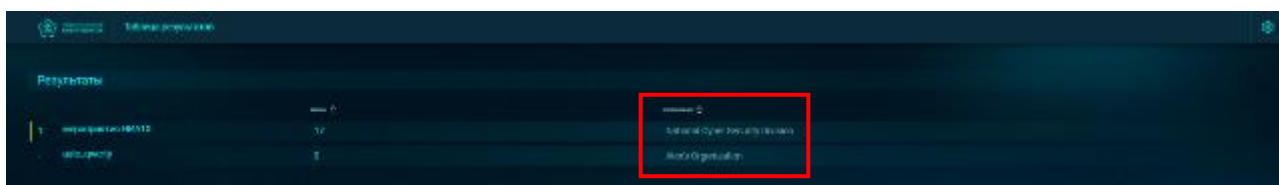


Рис. 88 – Форма «Табло результатов» с несколькими мероприятиями

### 3.1.8. Настройка скорборда платформы

Чтобы получить доступ к скорборду платформы, пользователю необходимо выбрать из главного меню раздел «**Админпанель**», вкладка «**Настройка скорборда**» (Рис. 89, 90).

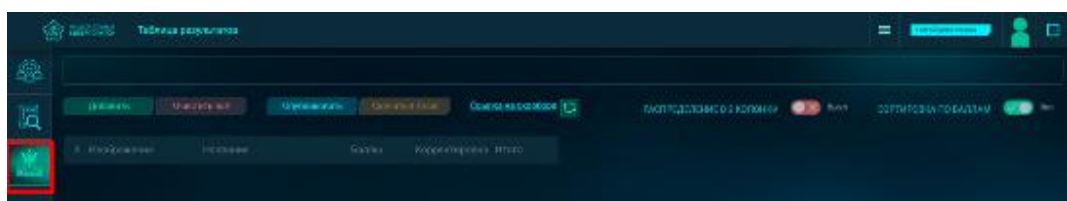


Рис. 89 – Админпанель. Вкладка «Настройка скорборда» по умолчанию

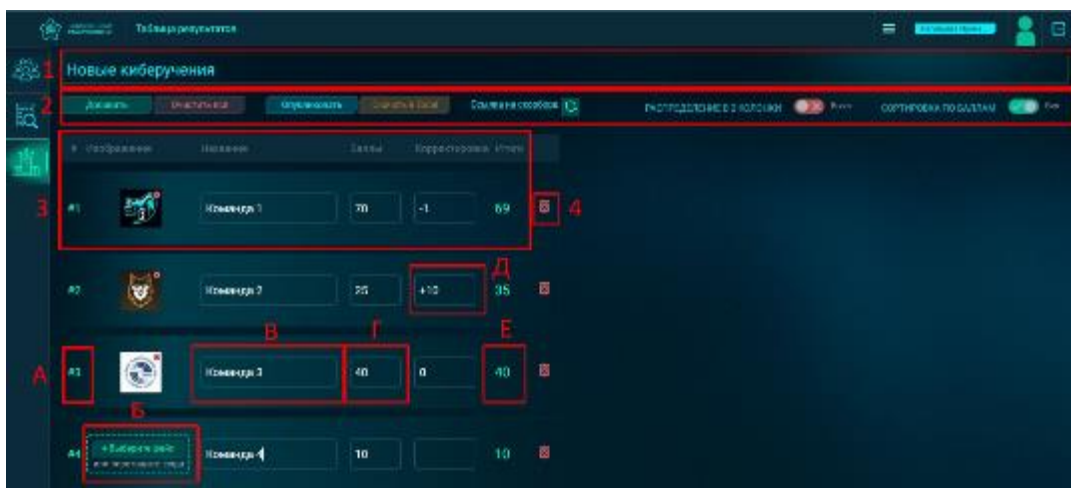


Рис. 90 – Форма настройки скорборда

На вкладке доступна следующая информация:

1. Название мероприятия (Рис. 90, п. 1). В данное поле необходимо вписать название мероприятия. Максимальная длина названия – 200 символов.
2. Блок с кнопками и тумблерами, используемыми для настройки скорборда (Рис. 90, п. 2);
3. Блок с информацией о команде (Рис. 90, п. 3). Добавляется при нажатии на кнопку **«Добавить»**, расположенную в верхнем блоке кнопок. Количество добавляемых команд неограниченно.

По умолчанию блок с информацией о команде добавляется пустой, и его атрибуты необходимо заполнить:

А Порядковый номер команды (Рис. 90, п. А). Присваивается автоматически при добавлении команды и не отображается на панели с результатами.

Б Поле «Изображение» позволяет загрузить изображение с логотипом команды (Рис. 90, п. Б). Для этого необходимо нажать на кнопку и выбрать необходимый файл с логотипом команды или перетащить его курсором мыши на данное поле.

Файл должен быть в формате PNG, а изображение должно вписываться в форму квадрата. Если выбран некорректный формат изображения, то система не загрузит логотип и выведет рядом с полем сообщение об ошибке: **«Некорректный формат (выберите .png)»**.

Если файл не загружен, то на панели с результатами на месте логотипа команды отобразится пустое место.


В Поле **«Название»** (Рис. 90, п. В). В данное поле необходимо вписать название команды. Максимальная длина названия – 30 символов;

Г Поле **«Баллы»** (Рис. 90, п. Г). В данное поле необходимо вписать общее

количество баллов, присвоенное команде. Ввести можно только положительные числа от 1 до 9999 или 0, остальные будут игнорироваться и не отображаться в поле ввода.

Д Поле **«Корректировка»** (Рис. 90, п. Д). Введенные в данное поле баллы откорректируют общие баллы команды. Если будет введено число со знаком плюс (или без него), то дополнительные баллы команде прибавятся, если со знаком минус – убавятся. Также можно ввести дробное число с сотыми долями, отделяющимися друг от друга точкой, либо при желании можно оставить данное поле пустым.

Е Поле **«Итого»** (Рис. 90, п. Е). Отображает итоговое количество баллов команды, учитывая баллы введенные в поля **«Баллы»** и **«Корректировка»**. Итоговые баллы округляются до целой части числа. Отрицательные значения отображаются со знаком «-», положительные значения отображаются без знака. Поле не доступно для редактирования. Данные из поля отображаются на панели с результатами.

4. Для удаления команды из списка команд необходимо нажать на иконку  (Рис. 90, п. 4). При попытке удаления команды появится уведомление о подтверждении удаления (Рис. 91).

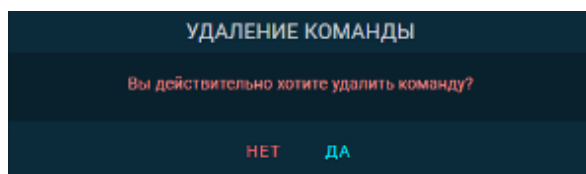


Рис. 91 – Уведомление о подтверждении удаления команды

Для того чтобы участники мероприятия могли видеть свои текущие результаты, необходимо вывести на панель с результатами информацию о командах и их баллах, введенную на форме с настройками скорборда админпанели. Для этого необходимо нажать кнопку **«Опубликовать»**, расположенную в верхней части формы с настройками скорборда (Рис. 90). При этом появится уведомление о подтверждении публикации результатов (Рис. 92).

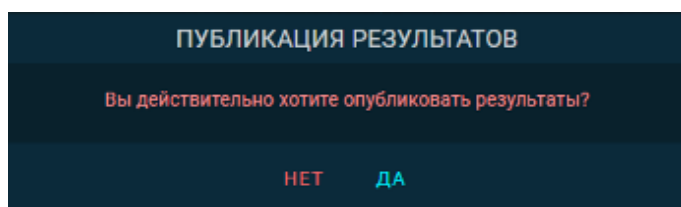

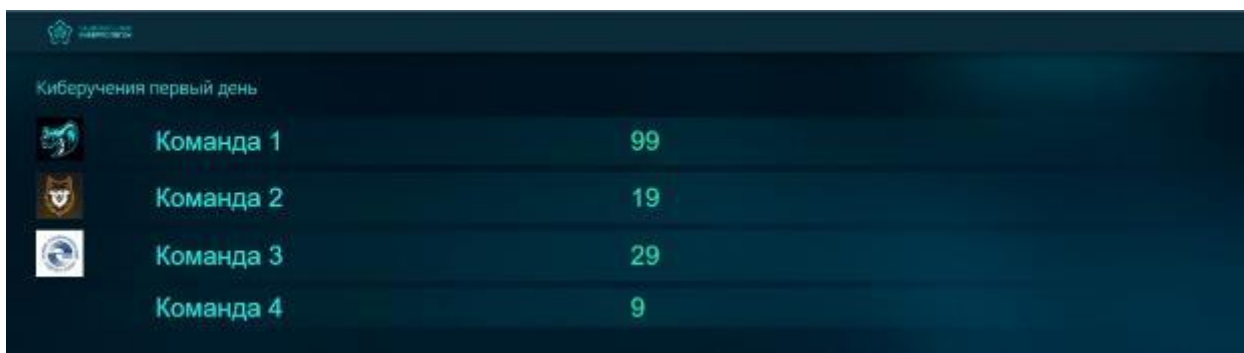


Рис. 92 – Уведомление о подтверждении публикации результатов

После публикации формируется ссылка на панель с результатами команд (токен). Перейти на панель можно, нажав на ссылку , расположенную в верхней части формы с настройками скорборда (Рис. 90, 93).

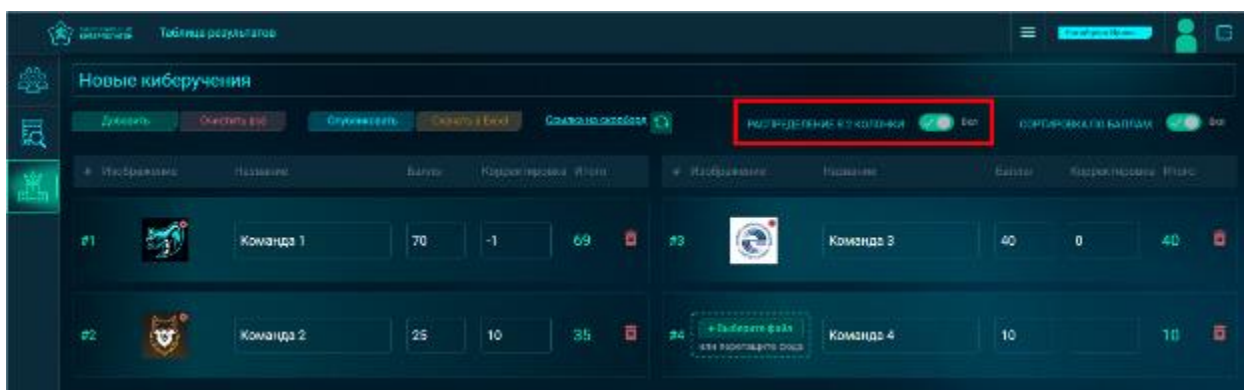


Команда	Баллы
Команда 1	99
Команда 2	19
Команда 3	29
Команда 4	9

Рис. 93 – Панель с результатами команд

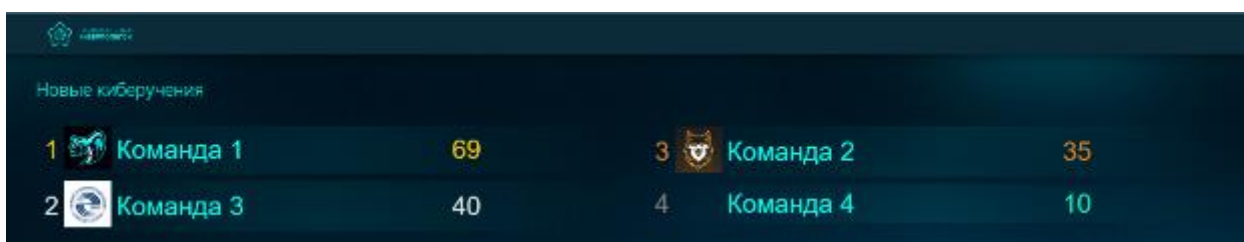
Также ссылку на панель с результатами можно разослать участникам мероприятия, чтобы они имели возможность посмотреть текущие баллы и рейтинг команд.

Для компактного размещения списка команд в области видимости экрана необходимо перевести тумблер **РАСПРЕДЕЛЕНИЕ В 2 КОЛОНКИ**  Вкл, расположенный в верхней части формы с настройками скорборда, в положение «Вкл», после чего команды распределятся в 2 колонки (Рис. 94, 95).



Иконка	Название	Баллы	Корректировка	Итого
#1	Команда 1	70	-1	69
#2	Команда 2	25	10	35
#3	Команда 3	40	0	40
#4	Команда 4	10		10

Рис. 94 – Расположение команд в 2 колонки



Рейтинг	Иконка	Название	Баллы
1	Команда 1	69	
2	Команда 3	40	
3	Команда 2	35	
4	Команда 4	10	

Рис. 95 – Расположение команд в 2 колонки на панели с результатами

Чтобы отобразить рейтинг команд и расположить их в порядке убывания набранных баллов в таблице на панели с результатами, необходимо применить сортировку по баллам. Для этого тумблер **«Сортировка по баллам»** на форме с настройками скорборда необходимо перевести в положение «Вкл» (Рис. 96, 97).

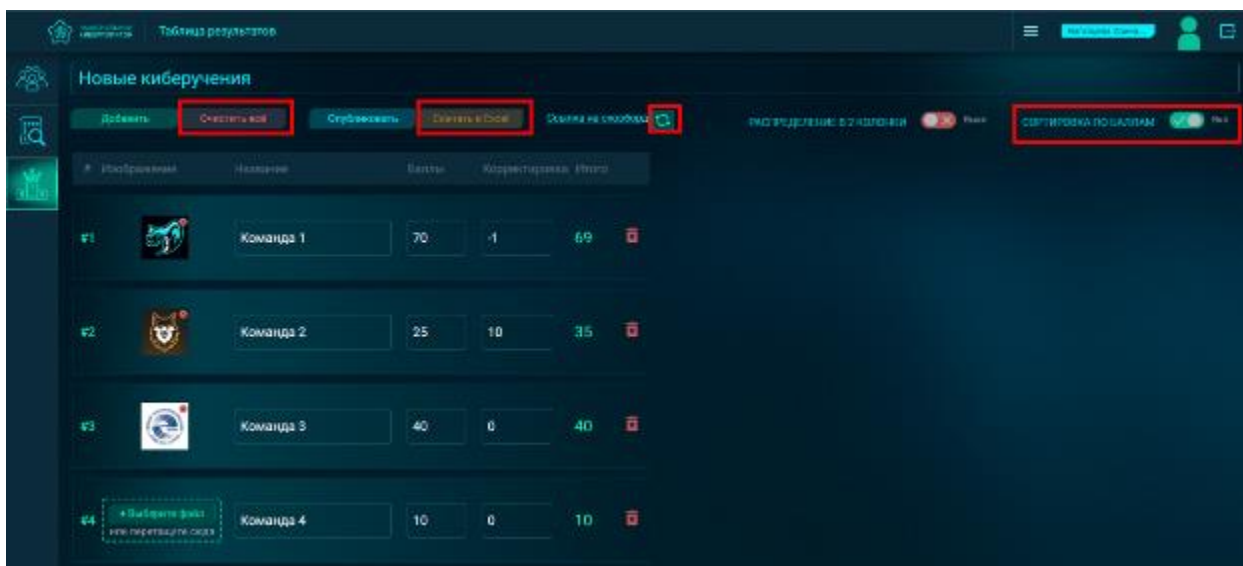


Рис. 96 – Настройка сортировки команд по баллам

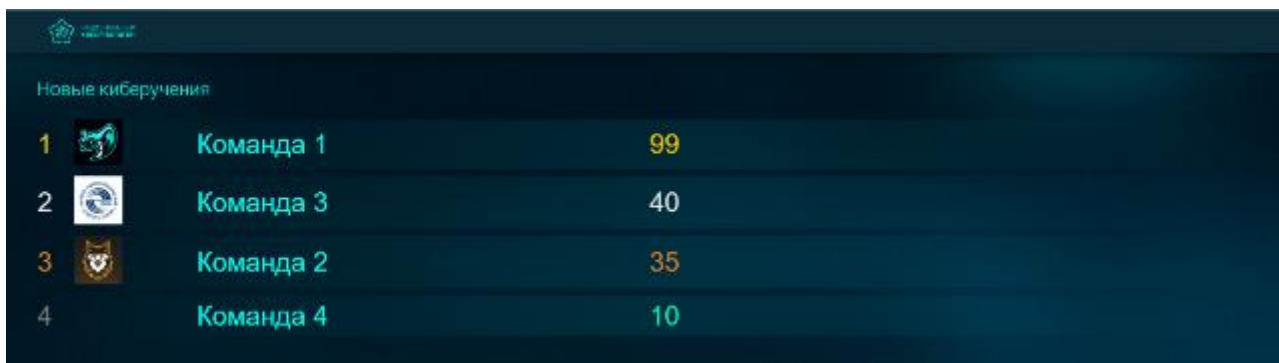


Рис. 97 – Панель с результатами и сортировкой команд по баллам

Для очистки всех данных о командах, внесенных в форму с настройками скорборда необходимо воспользоваться кнопкой **«Очистить все»**, расположенной на верхней панели скорборда (Рис. 96). После нажатия на кнопку появится уведомление о подтверждении очистки всех введенных данных (Рис. 98).

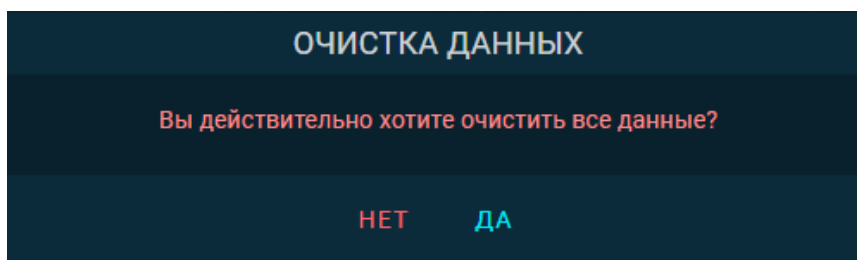



Рис. 98 – Уведомление об очистке данных

Если возникла необходимость отменить доступ к табло результатов для участников (чтобы текущая ссылка стала невалидной), то можно обновить ссылку на табло (сменить токен), нажав на кнопку , расположенную в верхней части формы с настройками скорборда (Рис.

98). После нажатия на кнопку появится уведомление о подтверждении обновления ссылки на табло результатов (Рис. 99).

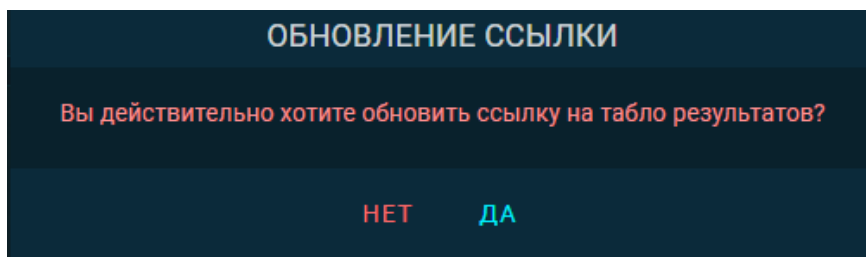


Рис. 99 – Уведомление об обновлении ссылки на табло результатов

Данные о командах, размещенные на скорборде, можно скачать в excel-файл, нажав на кнопку «Скачать в Excel», расположенную в верхней части формы (Рис. 96).

### 3.1.9. Редактор визуализации

#### 3.1.9.1. Назначение, область применения и вход в редактор визуализации

Конструктор визуализации платформы необходим для конфигурирования отображения объектов топологии в зависимости от событий мероприятия и представляет собой утилиту, которая является частью программного комплекса кибертренировок «Солар Кибермир».

Для доступа к редактору визуализации необходимо выполнить следующие действия:

- авторизоваться на платформе, используя логин и пароль;
- в адресной строке браузера добавить к адресу платформы «/tools» и перейти по ссылке.

#### 3.1.9.2. Интерфейс редактора визуализации

После входа в редактор визуализации открывается основное окно с пустой сценой и панелями, расположенными по краям рабочей области, которые можно показывать и скрывать по мере необходимости при наведении на них курсора (Рис. 100):

- панель с объектами топологии (Рис. 100, п. 1);
- сцена редактора, на которой размещена топология сети (Рис. 100, п. 2);
- панель инструментов (Рис. 100, п. 3);
- панель свойств объекта (Рис. 100, п. 4).

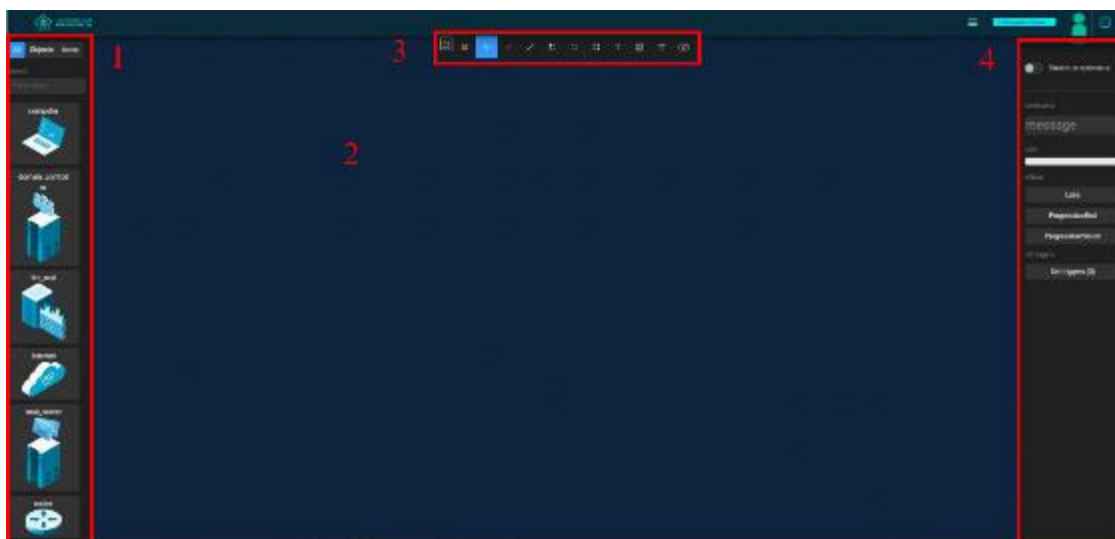


Рис. 100 – Интерфейс редактора визуализации

*Примечание. Если в редакторе ранее создавалась топология сети, то при повторном входе откроется топология, с которой в последний раз проводилась работа.*

### 3.1.9.3. Панель с объектами топологии

В редакторе визуализации представлены следующие типы графических объектов:

- объект топологии;
- сцена;
- линия;
- текст;
- подложка.

На левой боковой всплывающей панели доступен перечень объектов и иконок, которые можно создать на сцене (Рис. 101).

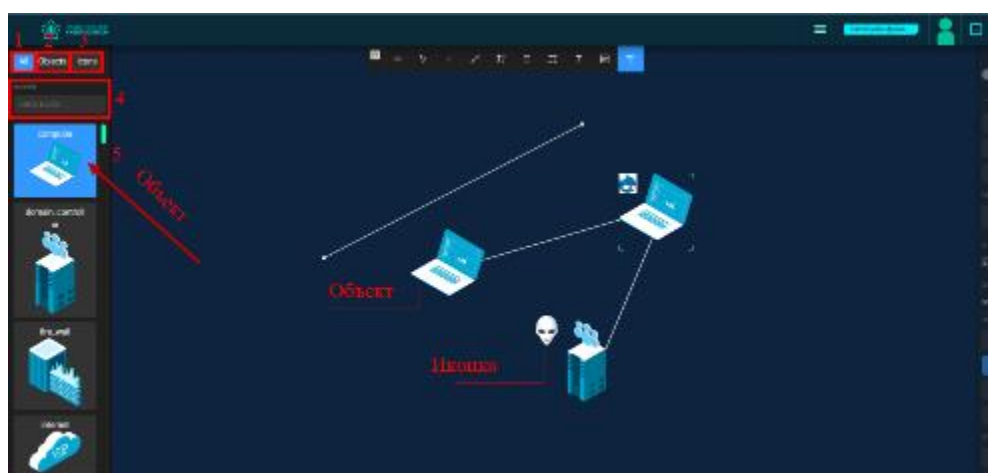


Рис. 101 – Сцена и панель с объектами

На панели объекты распределяются следующим образом:

- Во вкладке **«All»** располагается список всех доступных объектов топологии (объекты и иконки). Вкладка активна по умолчанию (Рис. 101, п. 1).
- Во вкладке **«Objects»** располагается список доступных объектов из общего списка объектов топологии (Рис. 101, п. 2).
- Во вкладке **«Icons»** располагается список доступных иконок из общего списка объектов топологии. Иконки показывают, что происходит с объектом в процессе прохождения мероприятия. После добавления иконки к объекту на сцене она привязывается к объекту и становится его частью. Расположена иконка по умолчанию в левом верхнем углу рядом с объектом (Рис. 101, Рис. 102 п. 3).

Для поиска конкретного объекта или иконки по названию можно воспользоваться функцией поиска (Рис. 101, п. 4).

При нажатии на объект или иконку левой клавишей мыши он добавляется на сцену редактора (Рис. 101, п. 5).

*Примечание. Иконки относятся (привязаны) к объекту топологии и отдельно существовать не могут.*

#### **3.1.9.4. Сцена редактора визуализации**

В центре основного окна редактора расположена сцена на которой подготавливается вся топология сети (Рис. 100, п. 2).

На сцене можно производить следующие действия:

- масштабировать (отдалять или приближать) все расположенные на ней объекты топологии, вращая среднее колесо мыши;
- перемещать в разные стороны сцену с расположенными на ней объектами, удерживая среднее колесо мыши;
- выделить один объект топологии, кликая по нему левой клавишей мыши. Появившиеся вокруг объекта уголки рамки зеленого цвета укажут на то, что объект выделен;
- выделить прямоугольной областью несколько объектов топологии, удерживая клавишу Shift, левую клавишу мыши и перемещая указатель, захватывая необходимые объекты;
- перемещать по сцене выделенные один или несколько объектов;
- продублировать существующий на сцене объект или группу объектов. Для этого необходимо выделить объект (объекты), нажать сочетание клавиш «Ctrl+C»,



установить курсор в место, куда планируется продублировать объект (объекты), и нажать сочетание клавиш «Ctrl+V». При этом новый объект (объекты) содержит все свойства дублируемого объекта;

– удалить один или несколько выделенных объектов, нажав кнопку «Delete» на клавиатуре или кликнув правой клавишей мыши и вызвав контекстное меню, после чего выбрать пункт «Delete».

### 3.1.9.5. Панель инструментов

При работе в редакторе визуализации используются различные инструменты. Некоторые из них ответственны за создание объектов, другие – за работу с существующими объектами. Все инструменты представлены на верхней центральной всплывающей панели (Рис. 102):

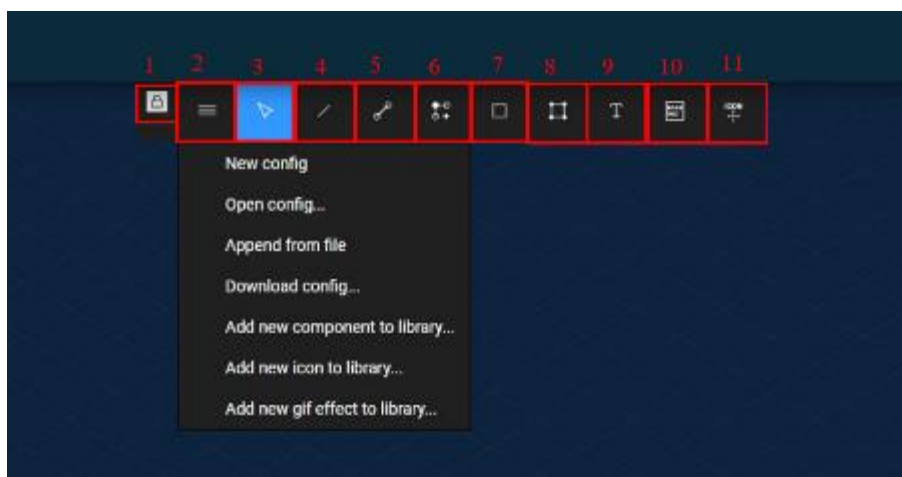


Рис. 102 – Панель инструментов

1. Иконка, позволяющая закрепить/открепить панель в открытом положении (Рис. 102, п. 1).
2. Кнопка «Меню» открывает панель с перечнем действий, которые можно совершить в редакторе (Рис. 102, п. 2).
3. Инструмент «Стрелка» позволяет выделять и перемещать объекты на топологии (Рис. 102, п. 3). Выбор этого инструмента соответствует основному режиму работы в редакторе.
4. Инструмент «Линия» позволяет нарисовать линию на сцене (Рис. 102, п. 4). Для этого необходимо кликнуть левой клавишей мыши в желаемом месте сцены и, удерживая ее, перемещать курсор по сцене на необходимое расстояние, затем отпустить левую клавишу мыши (Рис. 103). На сцене создастся линия с выделенными начальной и конечной точками.

Созданную линию можно трансформировать. Для этого необходимо выделить инструментом «Стрелка» одну из точек линии и, удерживая ее, изменить координату точки.

Для перемещения всей линии по сцене необходимо инструментом «Стрелка» кликнуть по телу линии и, удерживая нажатой левую клавишу мыши, переместить всю линию по сцене в нужное место.

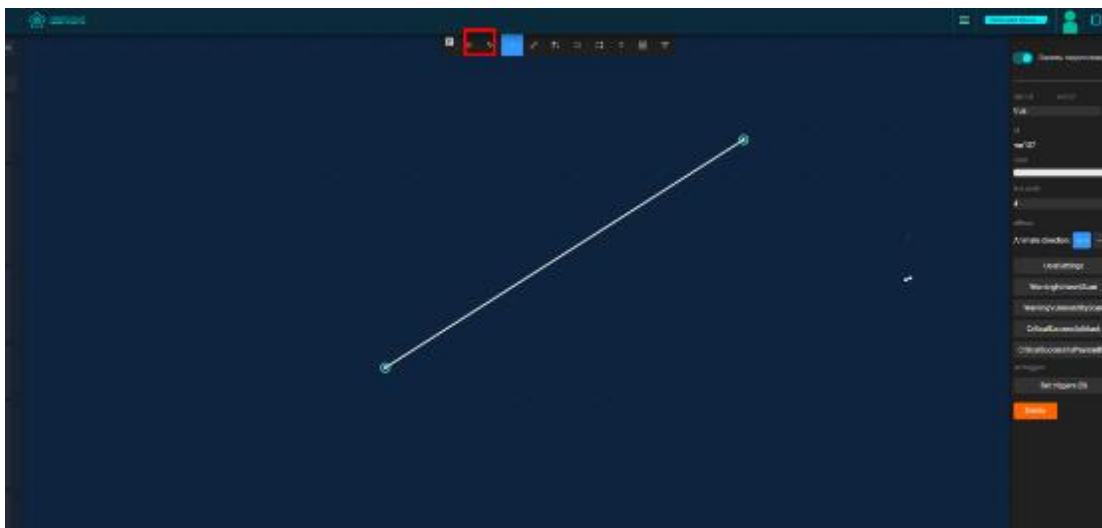


Рис. 103 – Создание линии

Линию можно удалить, выделив ее инструментом «Стрелка» и нажав на клавиатуре клавишу «Delete» либо по кнопке «Delete» на панели свойств линии.

Также удалить линию можно через контекстное меню. Для этого после выделения линии необходимо кликнуть правой клавишей мыши и далее в диалоговом окне выбрать пункт «Delete» (Рис. 104).

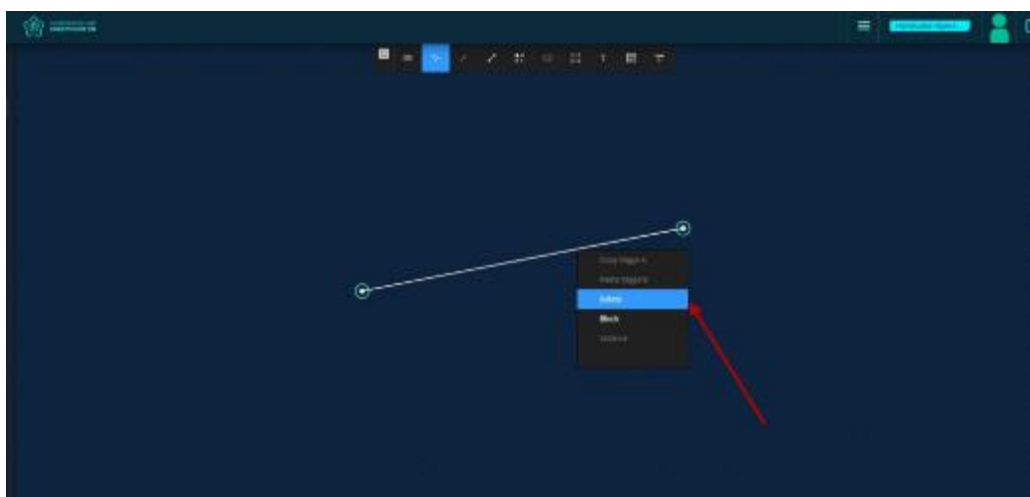


Рис. 104 – Удаление линии

Линию на сцене можно заблокировать, ограничив ей перемещение и возможность удаления. Для этого нужно выделить линию инструментом «Стрелка», кликнуть правой клавишей

мыши и далее в диалоговом окне выбрать пункт «Block» (Рис. 105). Точки на заблокированной линии будут подсвечиваться желтым, ее перемещение по сцене и удаление будет невозможно. Также невозможным станет копирование и вставка триггеров. Аналогичным образом через пункт «Unblock» в контекстном меню можно разблокировать линию и вернуть ей весь функционал.

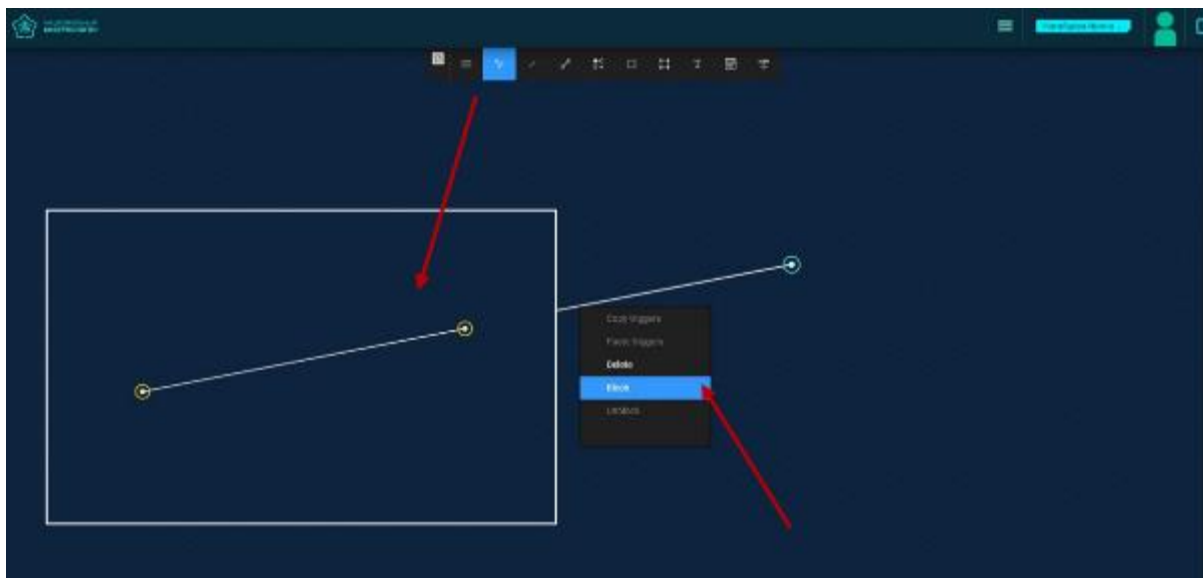


Рис. 105 – Блокировка линии

5. Инструмент «Связующая линия» позволяет протянуть связующую линию между двумя объектами топологии (Рис. 102 п. 5). Для соединения двух объектов необходимо сначала кликнуть на одном объекте топологии и, удерживая нажатой левую клавишу мыши, протянуть линию до второго объекта (Рис. 106). При перемещении объектов линия меняет свою длину и положение, оставаясь связанной с объектами. Изменить положение центра соединения связующей линии (коннектора) и объекта можно в свойствах соединяемого объекта.

При удалении двух связанных объектов связующая линия становится обычной линией, сохраняя все свои свойства и триггеры, при этом получает функции обычной линии (возможность задавать точки на линии).

Связующую линию на сцене можно заблокировать, ограничив ей перемещение и возможность удаления. Для этого нужно выделить связующую линию инструментом «Стрелка», кликнуть правой клавишей мыши и далее в диалоговом окне выбрать пункт «Block». Аналогичным образом через пункт «Unblock» в контекстном меню можно разблокировать линию и вернуть ей весь функционал.

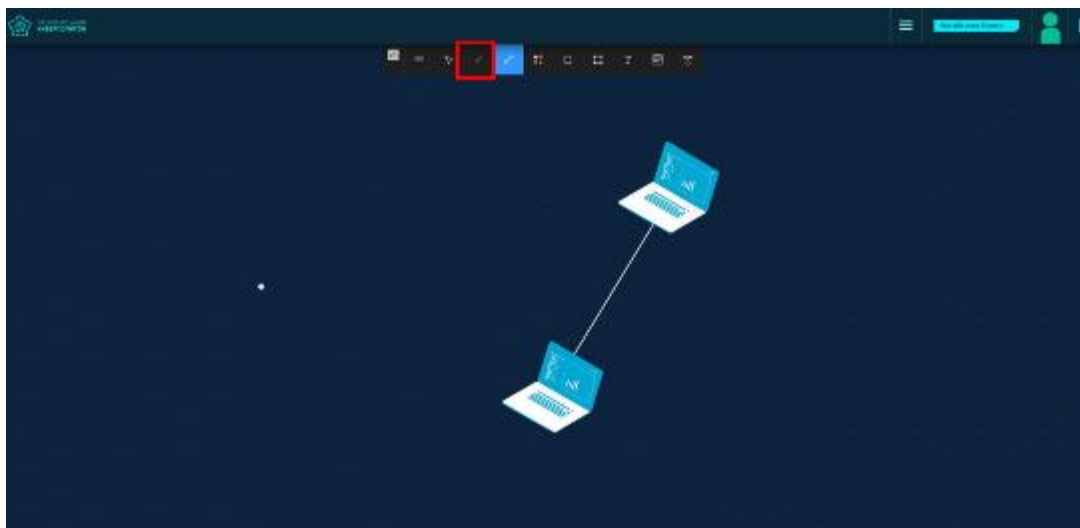


Рис. 106 – Создание коннектора между объектами

Простую линию можно преобразовать в коннектор, соединяющий расположенные рядом объекты, если на панели свойств линии в полях «start id» и «end id» прописать идентификаторы объектов (Рис. 107).



Рис. 107 – Преобразование линии в коннектор

Блок «effects» содержит 5 эффектов, которые можно применить к связующей линии, а с помощью кнопок «Animate direction» есть возможность указать направление распространения эффекта вдоль линии коннектора. Блок «set triggers» дает возможность задать триггеры для коннектора (Рис. 107).

Нажав на кнопку «Delete» на панели свойств коннектора, можно удалить весь объект (Рис. 107).

6. Инструмент «Точка на линии» позволяет добавить точку на ранее созданную линию (Рис. 102, п. 6). Для этого необходимо сначала выделить линию, на которой будет добавлена точка, а затем уже выбрать действие по добавлению точки (Рис. 108).

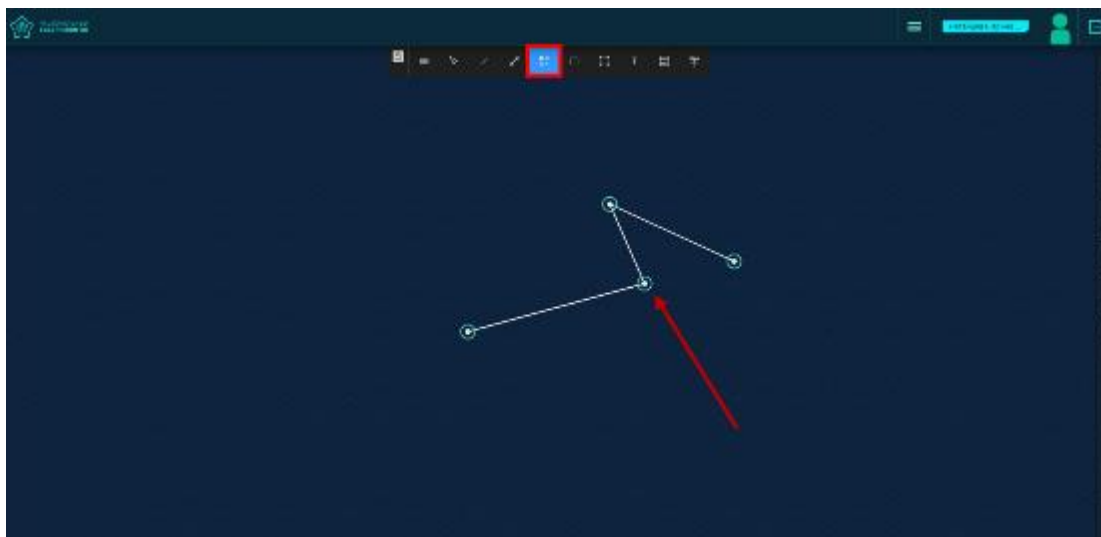


Рис. 108 – Добавление точки на линию

Точку на линии можно удалить, выделив ее инструментом «Стрелка» и нажав на клавиатуре клавишу «Delete», а также через контекстное меню. Для этого после выделения точки необходимо кликнуть правой клавишей мыши и далее в диалоговом окне выбрать пункт «Delete point» (Рис. 109).

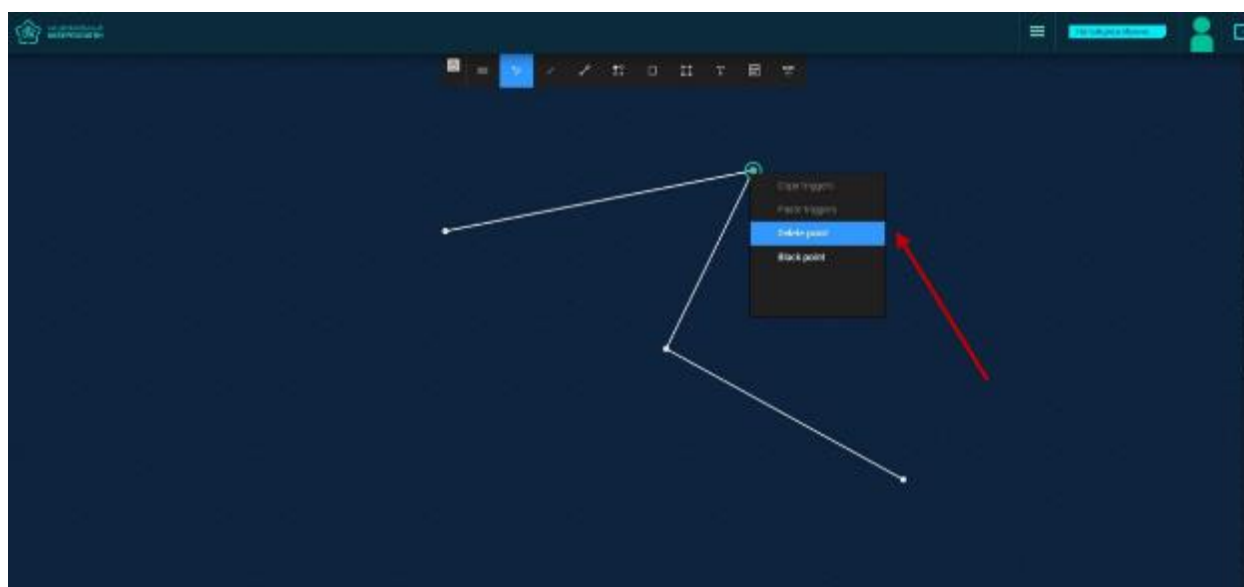


Рис. 109 – Удаление точки

Одну или несколько точек на линии можно заблокировать, ограничив им перемещение по сцене и возможность удаления. Для этого нужно выделить блокируемую точку инструментом «Стрелка», кликнуть правой клавишей мыши и далее в диалоговом окне выбрать пункт «Block point» (Рис. 110).

Заблокированная точка будет подсвечиваться желтым, и ее перемещение по сцене и удаление будет невозможно.

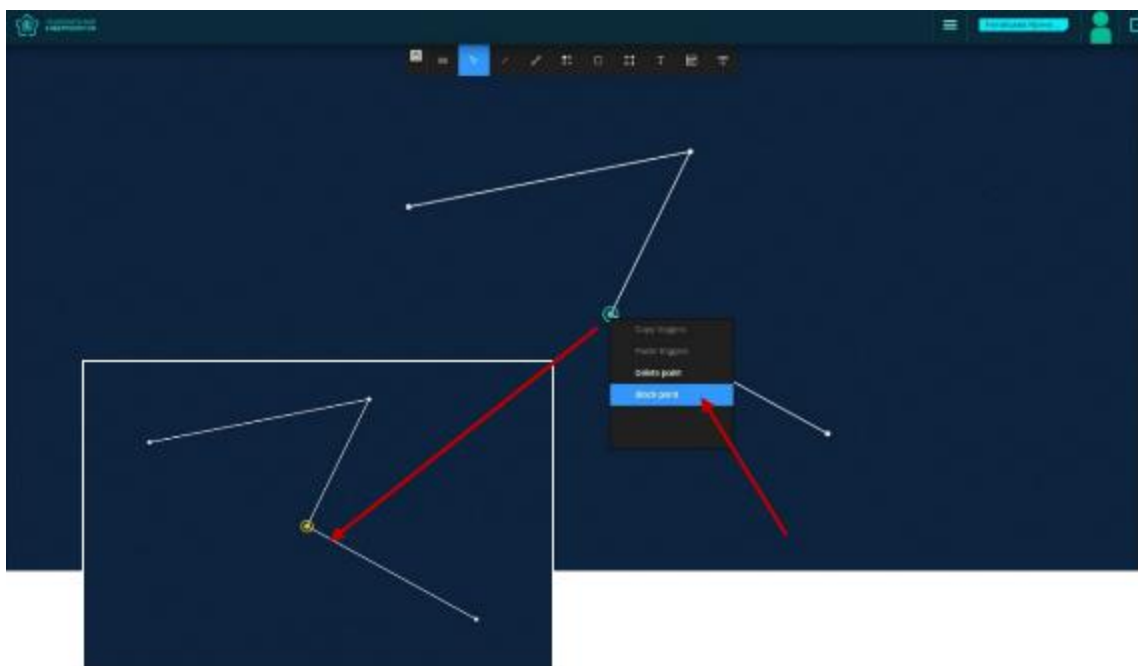


Рис. 110 – Блокировка точки

7. Инструмент «Создание подложки» позволяет визуальнo объединить несколько объектов на сцене (Рис. 102, п. 7). Подложка может использоваться, чтобы визуальнo подчеркнуть, что объекты на топологии относятся к одной подсети. Подложка создается в форме прямоугольника в фиксированном размере (Рис. 111).

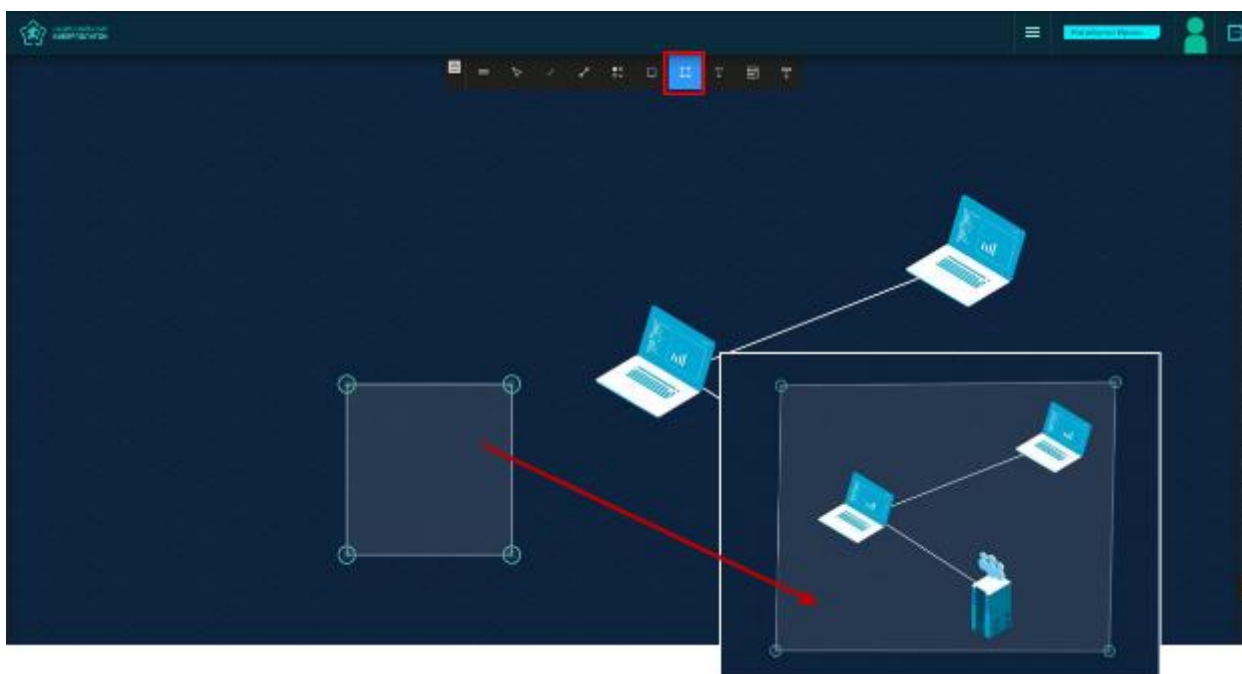


Рис. 111 – Создание и трансформация подложки

Сразу после создания подложки система осуществляет переход на элемент «Редактирование подложки».

8. Инструмент «Редактирование подложки» (Рис. 102, п. 8) позволяет менять форму

подложки, перетаскивая ее курсором за угловые точки или меняя координаты угловых точек на панели свойств подложки (Рис. 112). Дополнительные точки на подложку добавить нельзя.

На панели свойств подложки можно задать ее цвет, выбрав его из всплывающей палитры, прозрачность, а также цвет контура подложки (Рис. 112).

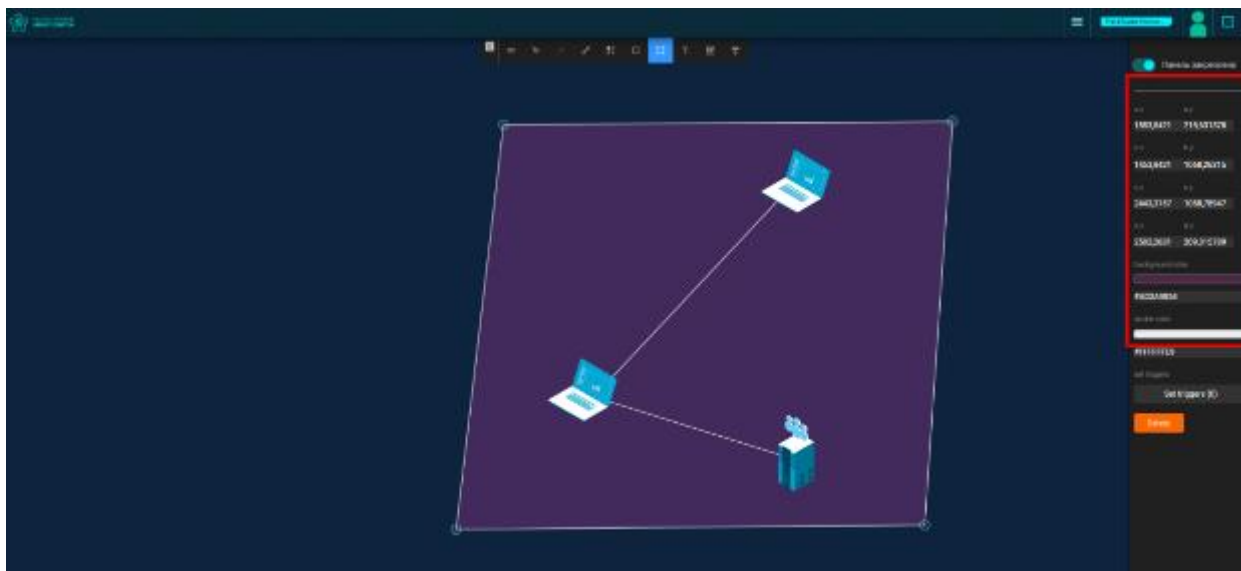


Рис. 112 – Свойства подложки

9. Инструмент «Добавление текста» позволяет добавить текстовое сообщение на топологию (Рис. 102, п. 9, 14).

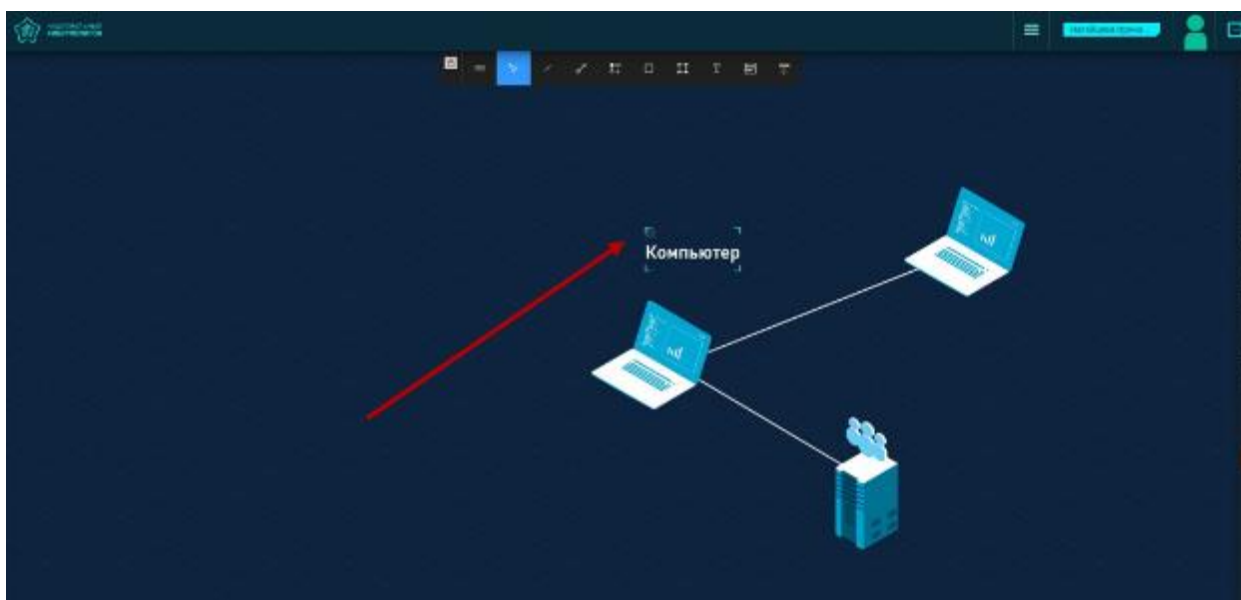


Рис. 113 – Добавление текста на сцену

10. Инструмент «Тестирование анимации» позволяет проверить заданные триггеры объектов (Рис. 102, п. 10, 15). При выборе данного инструмента появляется левая боковая панель «Изменения объекта», на которой с помощью тумблера можно выбрать режим ввода

информации о триггере.

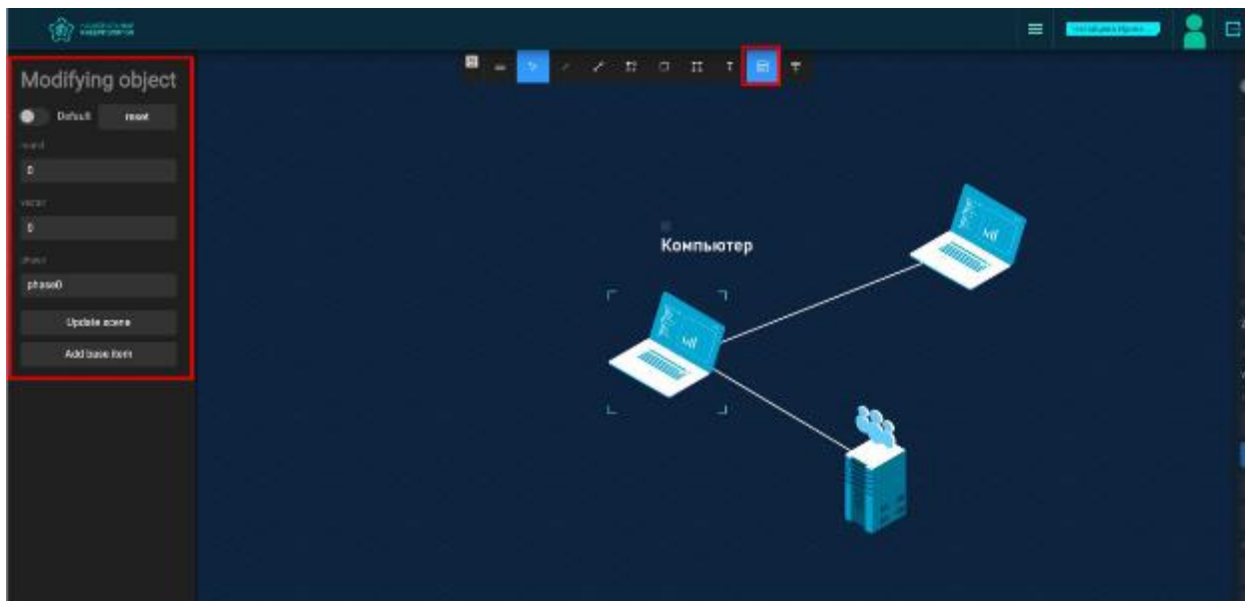


Рис. 114 – Инструмент «Тестирование анимации»

11. Инструмент «Подвинуть иконку» позволяет подвинуть иконку относительно объекта (Рис. 102, п. 11). Для этого необходимо курсором выделить объект, иконку которого планируется переместить, далее выбрать инструмент «Подвинуть иконку». Кликнув левой клавишей мыши по иконке и удерживая ее, перемещать иконку по сцене на необходимое расстояние (Рис. 115).

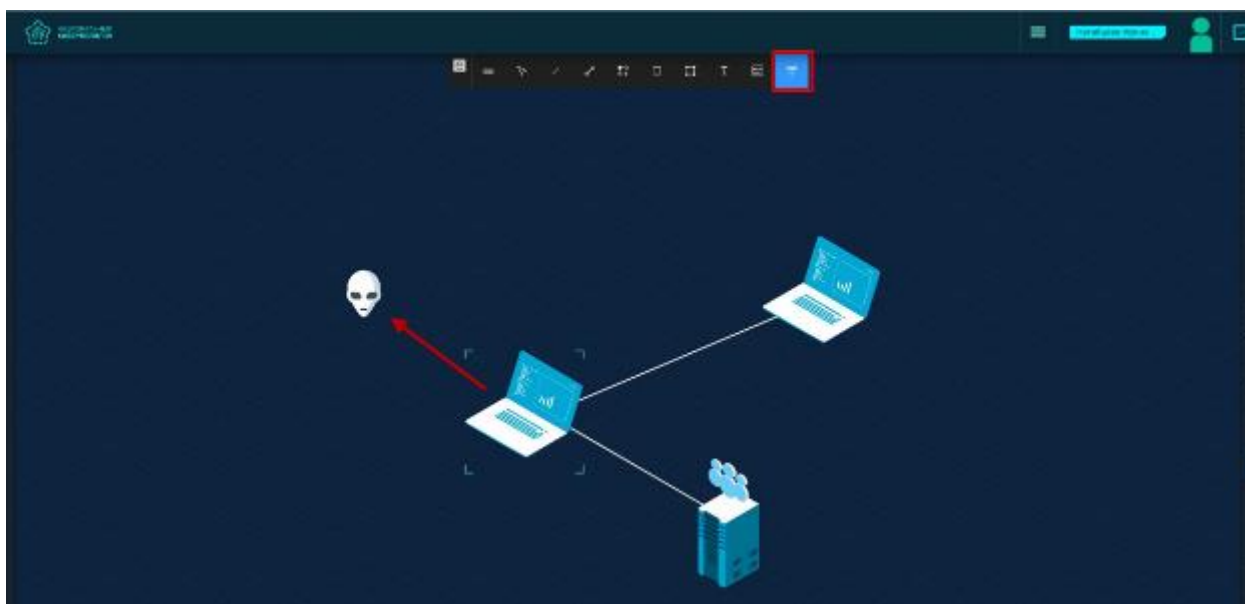


Рис. 115 – Инструмент «Подвинуть иконку»



### 3.1.9.6. Меню с основными действиями

Первая кнопка «Меню» на панели инструментов открывает доступ к перечню действий, которые можно совершить в редакторе (Рис. 116Рис. 117):

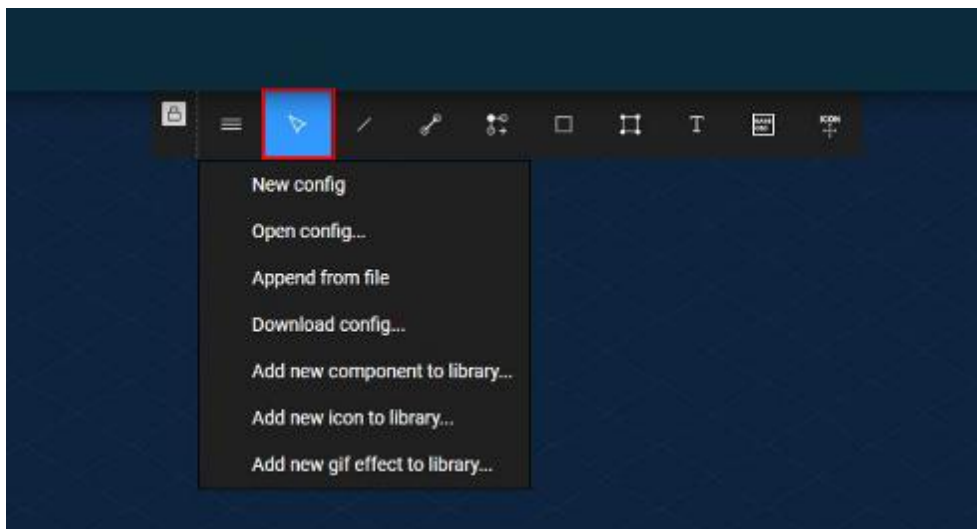


Рис. 116 – Кнопка «Меню» на панели инструментов

- действие **«New config»** – создает новую топологию (новый конфигурационный файл), очищая при этом текущую;
- действие **«Open config»** – загружает ранее созданную топологию (конфигурационный файл), заменяя при этом текущую топологию;
- действие **«Append from file»** – дополнительно загружает все объекты из существующей топологии, не затирая того, что уже расположено на сцене;
- действие **«Download config»** – скачивает конфигурационный файл из редактора в формате json с созданной топологией (объекты, триггеры и т. д.). Скаченный файл необходимо переименовать в «network-map.json» и поместить в папку с конфигурационными файлами миссии;
- действие **«Add new component to library...»** – добавляет новый компонент в библиотеку с объектами, расположенную в левой всплывающей панели. При выборе этого пункта меню открывается форма (Рис. 117), в которой необходимо заполнить название компонента и добавить 4 изображения, соответствующие состояниям нового компонента. При нажатии на кнопку «Add component» новый компонент добавляется в библиотеку;

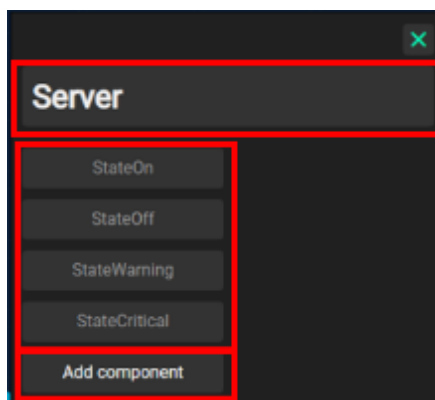


Рис. 117 – Форма для добавления нового объекта в библиотеку

- действие **«Add new icon to library...»** – добавляет новый компонент в библиотеку с иконками, расположенную в левой всплывающей панели. При выборе этого пункта меню открывается форма (Рис. 118), в которой необходимо заполнить название иконки и по кнопке «Выбрать» добавить графическое изображение иконки. При нажатии на кнопку «Сохранить» новая иконка добавляется в библиотеку;

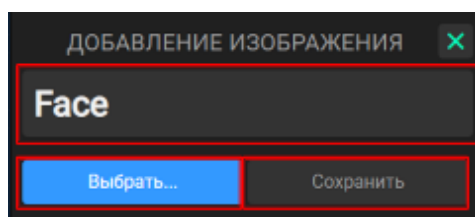


Рис. 118 – Форма для добавления новой иконки в библиотеку

- действие **«Add new gif effects to library...»** – добавляет gif-эффект для выбранного объекта. При выборе этого пункта меню открывается форма для добавления gif-эффекта (Рис. 119).

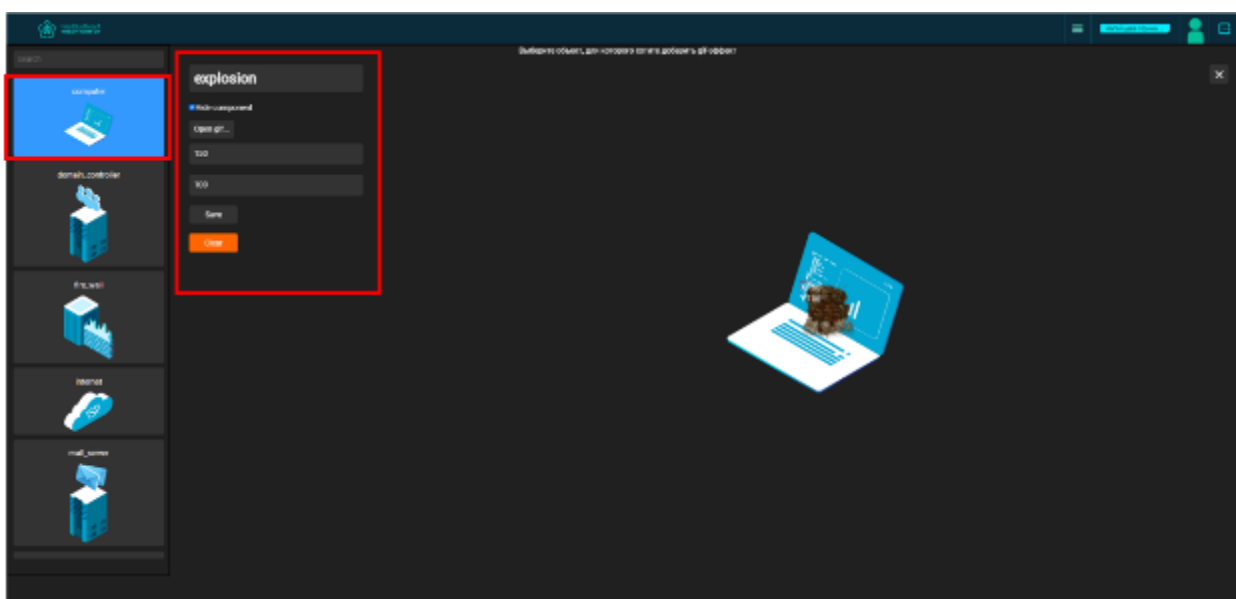


Рис. 119 – Форма для добавления gif-эффекта

Для добавления gif-эффекта необходимо выполнить следующие действия:

- выбрать из библиотеки объект, к которому планируется добавить gif-эффект;
- заполнить поле с названием gif-эффекта;
- проставить галочку, если изображение gif-эффекта будет заменять текущее изображение объекта;
- загрузить файл с gif-анимацией;
- установить координаты gif-эффекта по осям X и Y;
- сохранить gif-эффект в библиотеку, нажав на кнопку «Save».
- Кнопка «Clear» очищает всю введенную в вышеописанные поля информацию.

### 3.1.9.7. Панель свойств графических объектов

Для конфигурирования отображения объектов топологии используются свойства объектов, которые доступны на правой боковой всплывающей панели.

### 3.1.9.8. Свойства сцены

При клике левой клавишей мыши по сцене на правой боковой панели отображаются следующие свойства (Рис. 120):

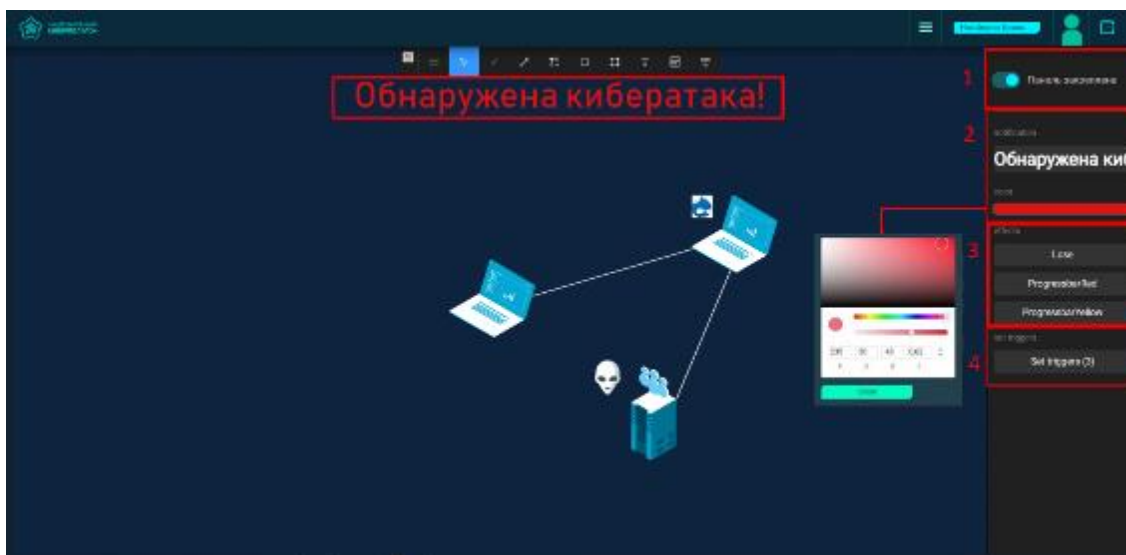


Рис. 120 – Панель свойств сцены

1. Тумблер, позволяющий закрепить/открепить панель в открытом положении (Рис. 120, п. 1).
2. Поле для ввода текста уведомления, который расположен в центральной части сцены (Рис. 120, п. 2). Чтобы задать цвет текста, необходимо нажать на цветовую полосу, после чего появится всплывающая цветовая палитра, позволяющая выбрать любой цветовой оттенок

как с помощью ползунка цвета, так и используя буквенно-цифровое обозначение цвета в цветовых моделях RGBA (HEX) и HSLA (переключение между цветовыми моделями осуществляется при нажатии на стрелочки). Вторым ползунком можно отрегулировать уровень прозрачности цвета текста.

3. **Блок «effects»** содержит 3 эффекта, которые можно добавить к сцене (Рис. 120, п. 3):

- эффект «lose» – добавляет по краям сцены красное свечение (Рис. 121);

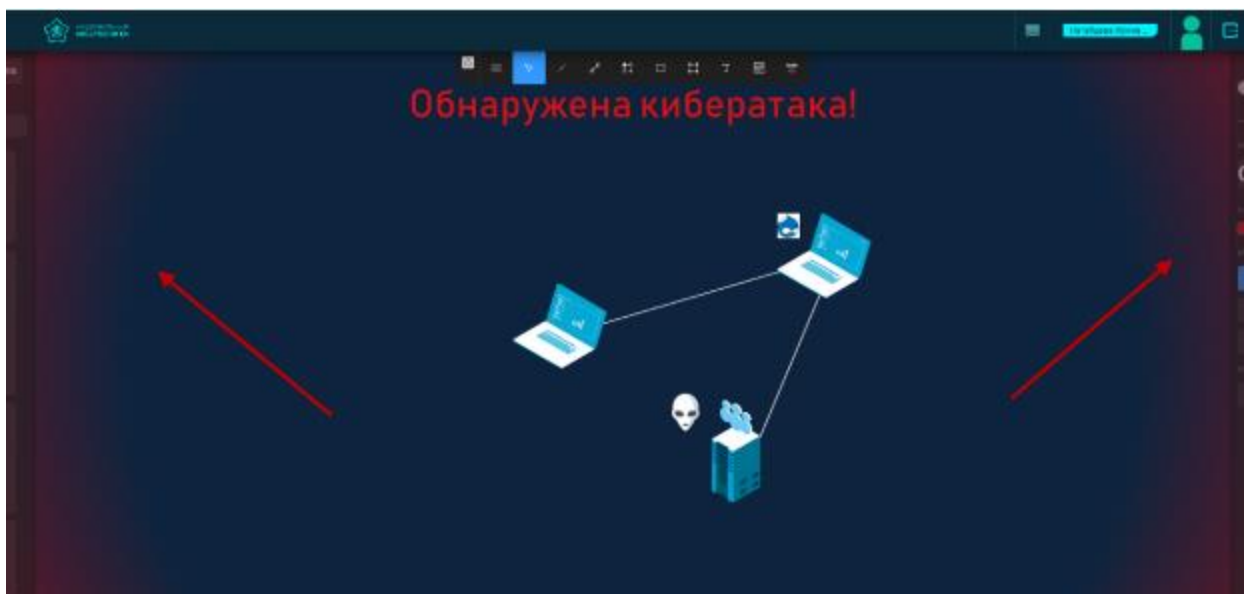


Рис. 121 – Эффект «lose» на сцене

- эффект «ProgressbarRed» – добавляет на сцену индикатор процесса красного цвета, свидетельствующий об атаке (Рис. 122);

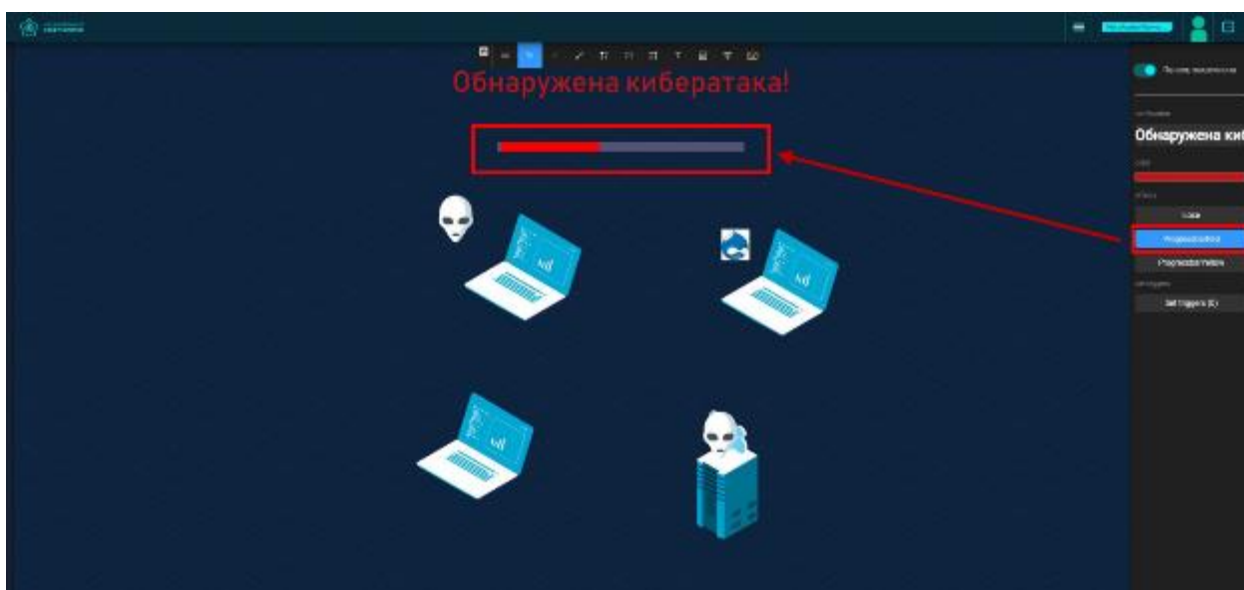


Рис. 122 – Применение эффекта «ProgressbarRed» на сцене

- эффект «ProgressbarYellow» – добавляет на сцену индикатор процесса желтого цвета, свидетельствующий об атаке (Рис. 123).

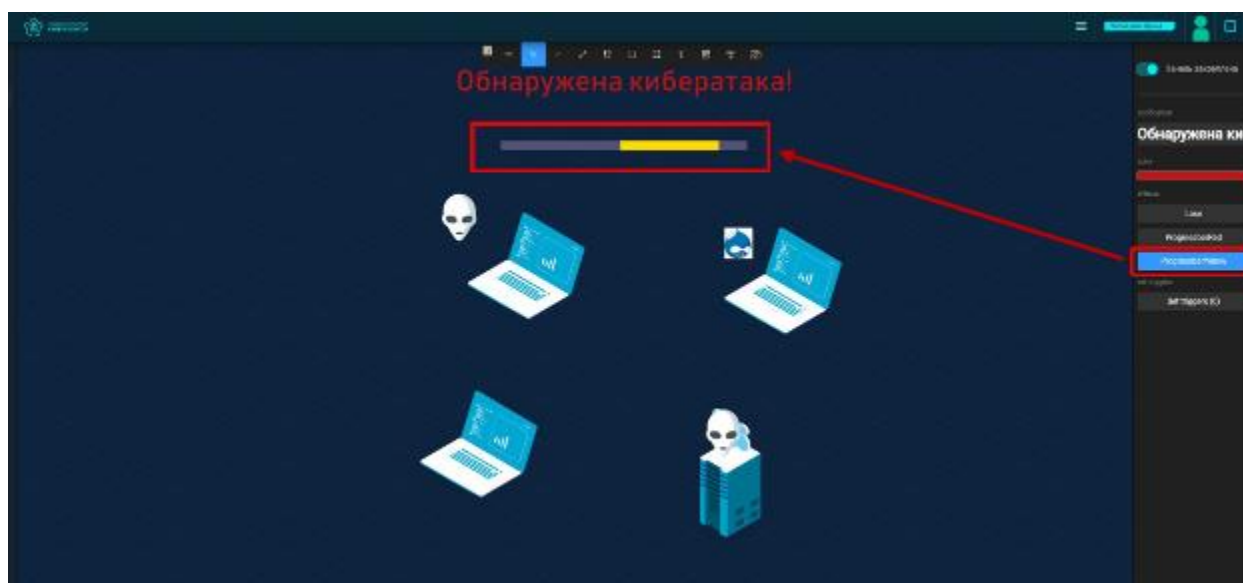


Рис. 123 – Применение эффекта «ProgressbarYellow» на сцене

Эффекты для сцены могут применяться по отдельности, в разных комбинациях или все одновременно. Однако при их одновременном применении эффекты визуально будут накладываться друг на друга и на сцене будет виден только примененный ранее всех эффект.

*Примечание. При одновременном применении эффектов «ProgressbarRed» и «ProgressbarYellow» на сцене будет виден эффект «ProgressbarYellow» вне зависимости от очередности их добавления.*

4. Блок «set triggers» дает возможность задать триггеры для сцены.

#### 3.1.9.9. Свойства объектов топологии

При выделении объекта топологии на сцене на правой боковой панели отображаются следующие свойства (Рис. 124):

1. **Блокировка/Разблокировка объекта** осуществляется нажатием на кнопку «Blocked». При этом вокруг блокируемого объекта появятся уголки рамки желтого цвета и перемещение объекта по сцене станет невозможным (Рис. 124).

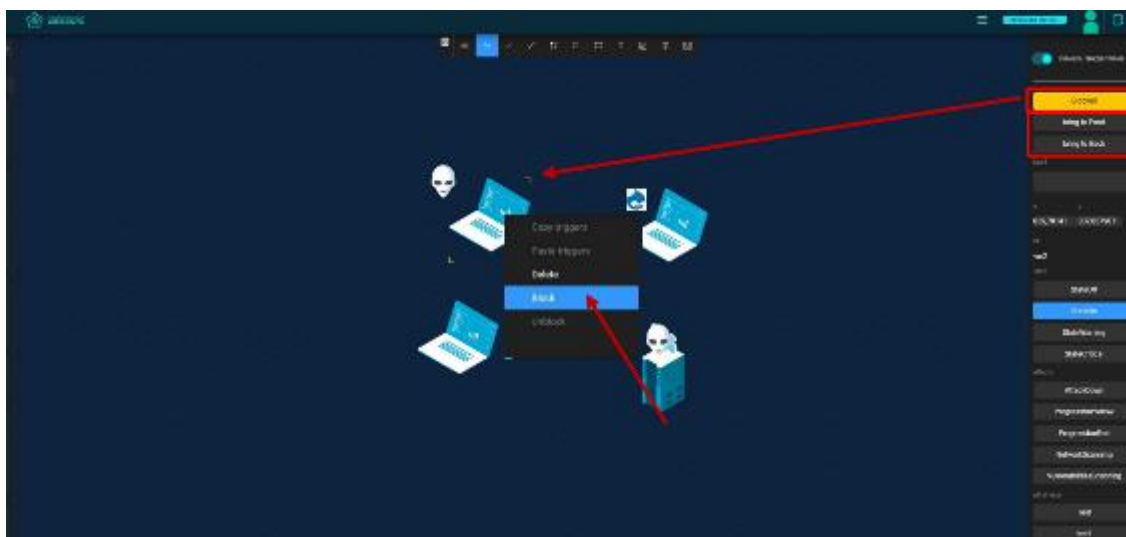


Рис. 124 – Свойства объекта

Заблокировать перемещение объекта по сцене можно из контекстного меню. Для этого необходимо кликнуть правой клавишей мыши по объекту и далее в диалоговом окне в меню выбрать пункт «Block» (Рис. 124). Для разблокирования – выбрать пункт «Unblock».

2. При наложении двух объектов их можно перемещать на передний или задний план друг относительно друга с помощью кнопок «Bring to front» и «Bring to back» (Рис. 124).

3. Название для объекта можно прописать в поле «label». В полях «x», «y» и «id» отображаются координаты объекта по оси X и Y и его идентификатор. При необходимости разместить объект в конкретной точке сцены в поля «x» и «y» нужно ввести координаты точки (Рис. 125).

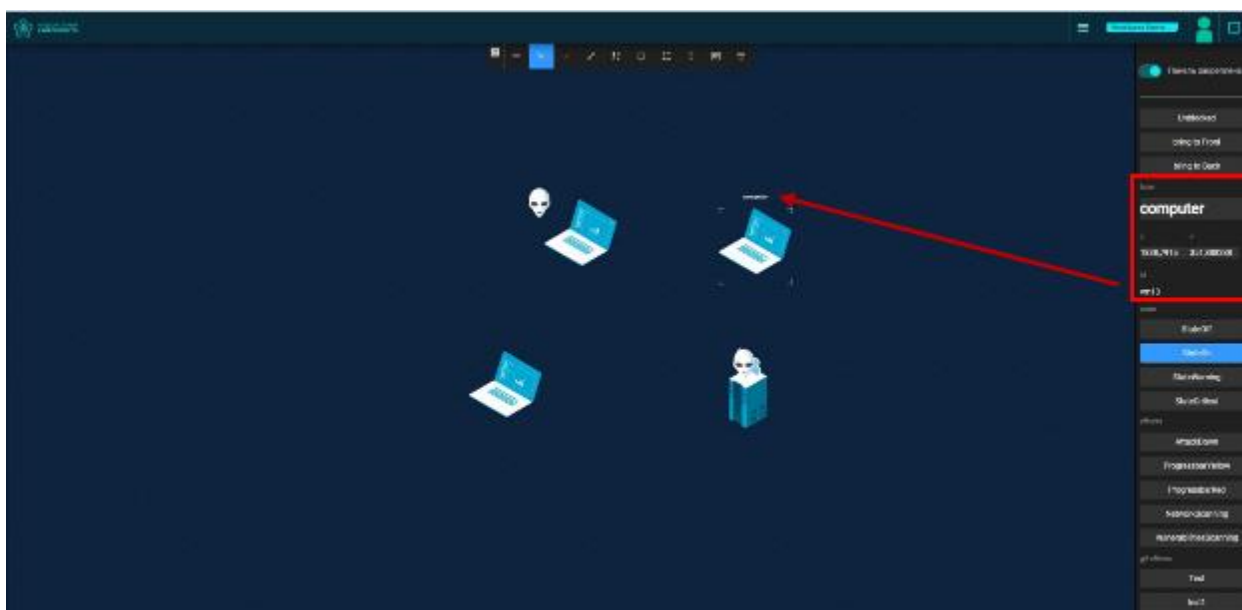


Рис. 125 – Свойства объекта

4. **Блок «state»** содержит состояния, которые можно задать объекту. Объект может

находиться только в одном определенном состоянии в каждый момент времени. На панели свойств доступны 4 состояния (Рис. 126):

- StateOff – объект не активен;
- StateOn – объект активен;
- StateWarning – опасное состояние объекта;
- StateCritical – критическое состояние объекта.

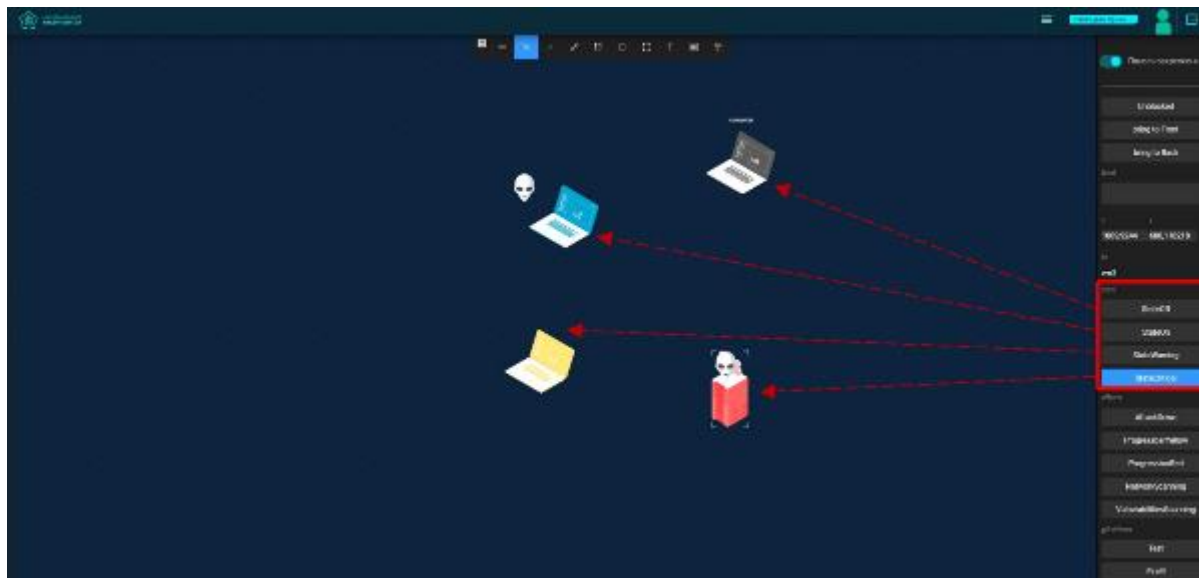


Рис. 126 – Состояния объекта

5. **Блок «effects»** содержит 5 эффектов, которые можно применить к любому объекту (Рис. 128):

- AttackDown – создает силовое поле (купол) над объектом (атака отражена);
- ProgressbarRed – добавляет к объекту индикатор процесса красного цвета, показывающий, что на этот объект производится атака;
- ProgressbarYellow – добавляет к объекту индикатор процесса желтого цвета, показывающий что на этот объект производится атака;
- NetworkScanning – добавляет индикатор сетевого сканирования хоста;
- VulnerabilitiesScanning – добавляет индикатор сканирования на уязвимости.
- К одному объекту одновременно можно применить несколько эффектов.

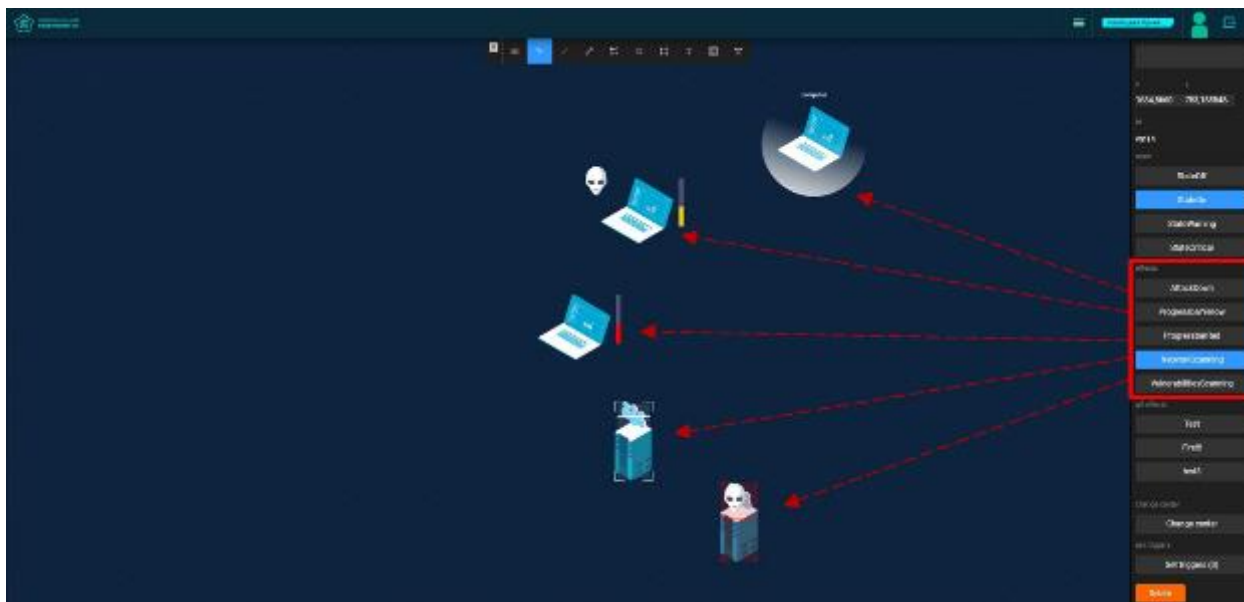


Рис. 127 – Эффекты объекта

6. Блок «gif effects» содержит перечень gif-эффектов, которые применены к конкретному объекту. Эти эффекты задаются для каждого объекта в отдельном окне через верхнее меню с инструментами «Add new gif effects to library...». Нажав на панели свойств объекта кнопку с названием, примененного к нему gif-эффекта, на сцене у объекта запустится анимированная визуализация эффекта (Рис. 128). Одновременно могут показываться все gif-эффекты, примененные объекту.

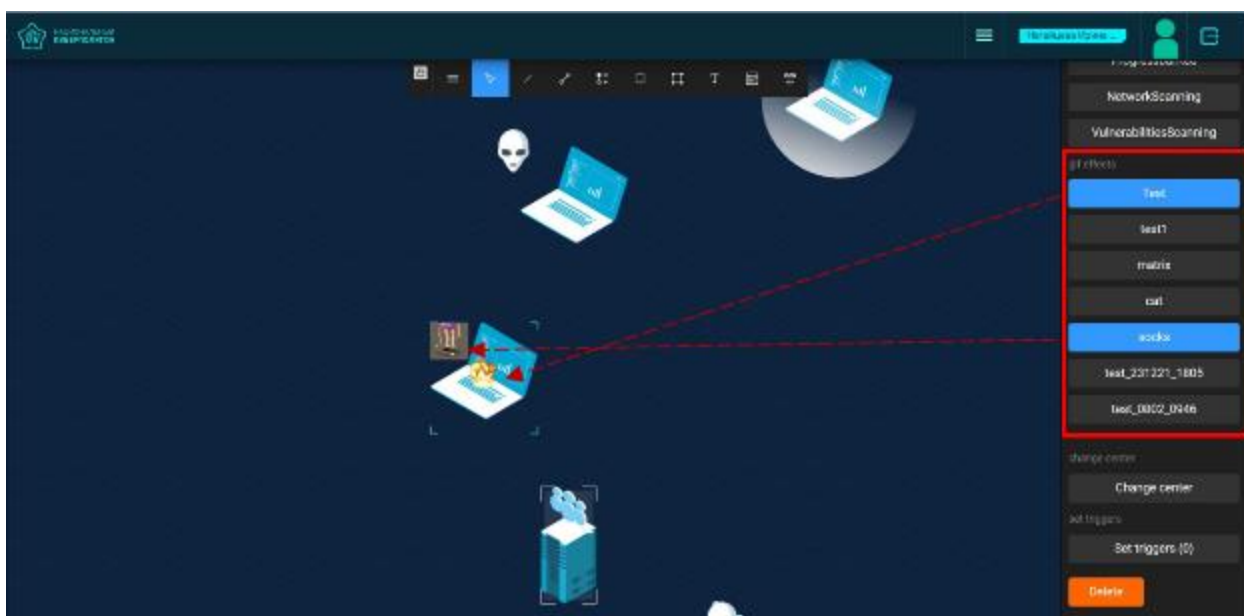


Рис. 128 – Gif-эффекты объекта

7. Изменения центра соединения объектов «Change center». Два объекта, соединенные связующей линией, имеют точки привязки линии к каждому из объектов (по умолчанию это левый верхний угол объекта). Положение этой точки можно изменить, выбрав



объект и нажав кнопку «Change center» на панели его свойств (Рис. 129). В появившемся на боковой панели окне с изображением объекта точку привязки (красную точку) необходимо переместить в место желаемого центра соединения объекта.

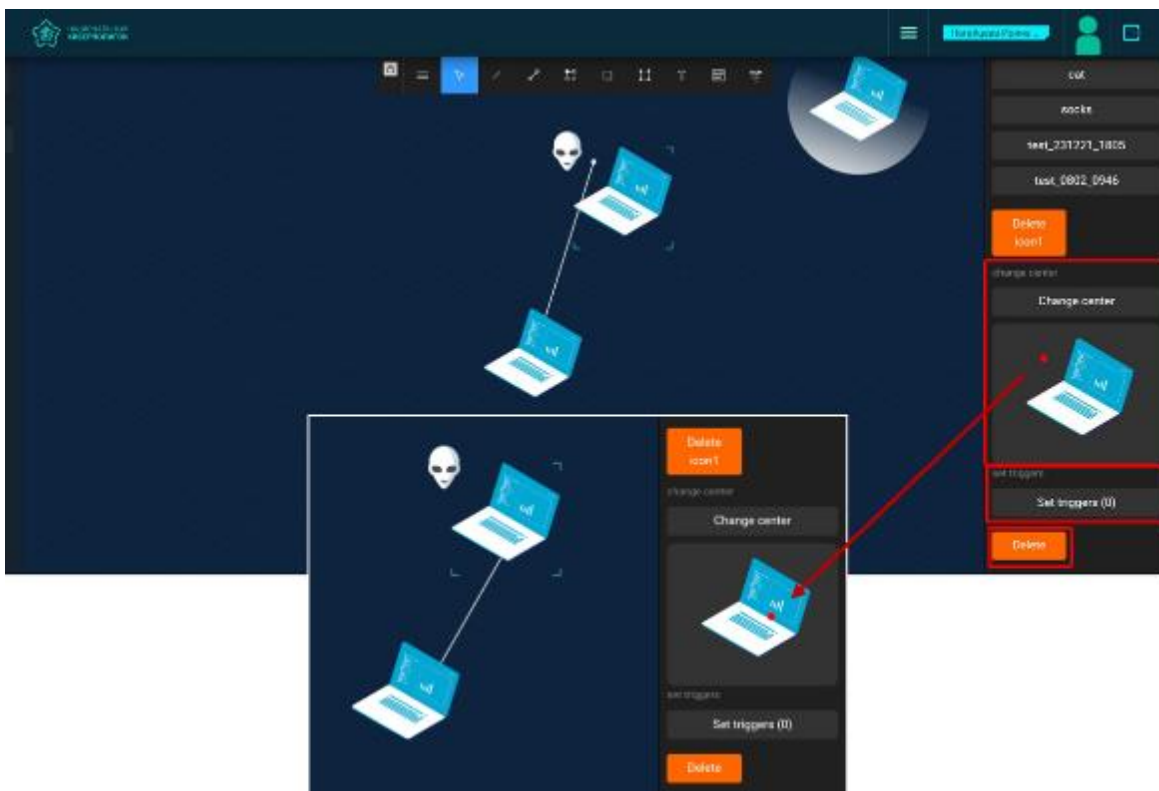


Рис. 129 – Изменение центра объекта

8. Блок «set triggers» дает возможность задать триггеры для объекта топологии.
9. Нажав на кнопку «Delete» на панели свойств объекта, можно удалить объект (Рис. 129).

### 3.1.9.10. Свойства линии

При выделении линии на сцене на правой боковой панели отображаются следующие свойства (Рис. 130):

1. В полях «start id», «end id» и «id» отображаются идентификаторы начала, конца линии и идентификатор самой линии (Рис. 130). По умолчанию заполняются поля «start id» значением «true» и в поле «id» проставляется идентификатор линии.

Если необходимо преобразовать линию в связующую линию (коннектор), то в полях «start id» и «end id» необходимо прописать идентификаторы объектов, которые планируется соединить.

2. С помощью всплывающей цветовой палитры можно задать цвет линии и ее прозрачность.

3. В поле «line width» можно указать толщину линии (Рис. 130).

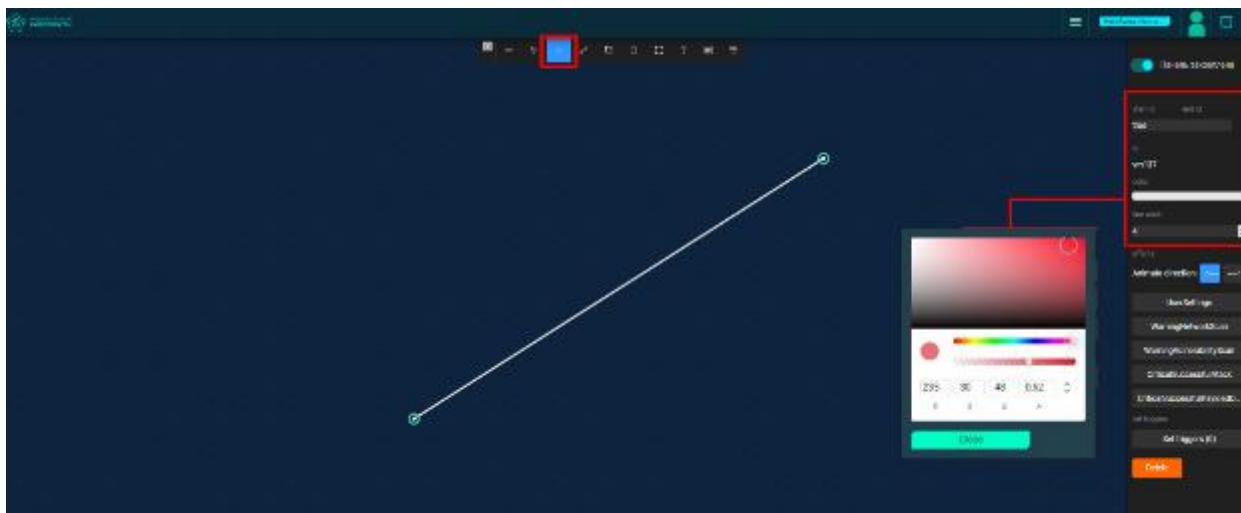


Рис. 130 – Создание линии

4. Блок «effects» на панели свойств содержит 5 эффектов, которые можно применить к линии, а с помощью кнопок «Animate direction» есть возможность указать направление распространения эффекта вдоль линии (Рис. 131).

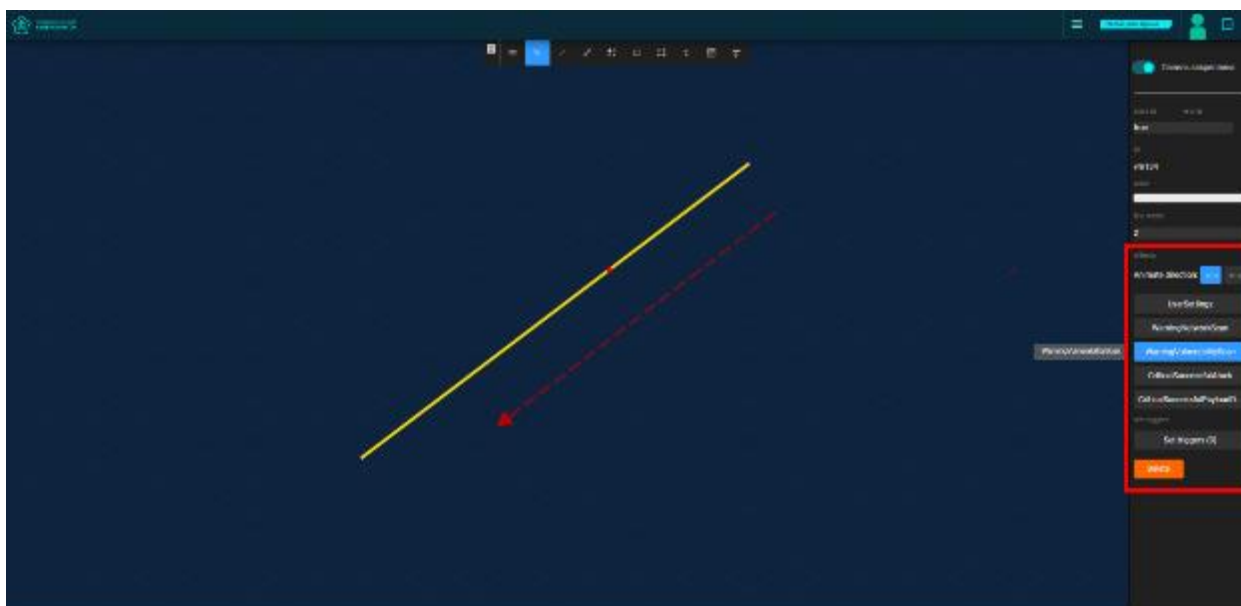


Рис. 131 – Направление анимации линии

5. Блок «set triggers» дает возможность задать триггеры для линии.  
6. Нажав на кнопку «Delete» на панели свойств линии, можно удалить всю линию.

### 3.1.9.11. Свойства текста

При выделении расположенного на сцене текста на правой боковой панели отображаются следующие свойства (Рис. 132):

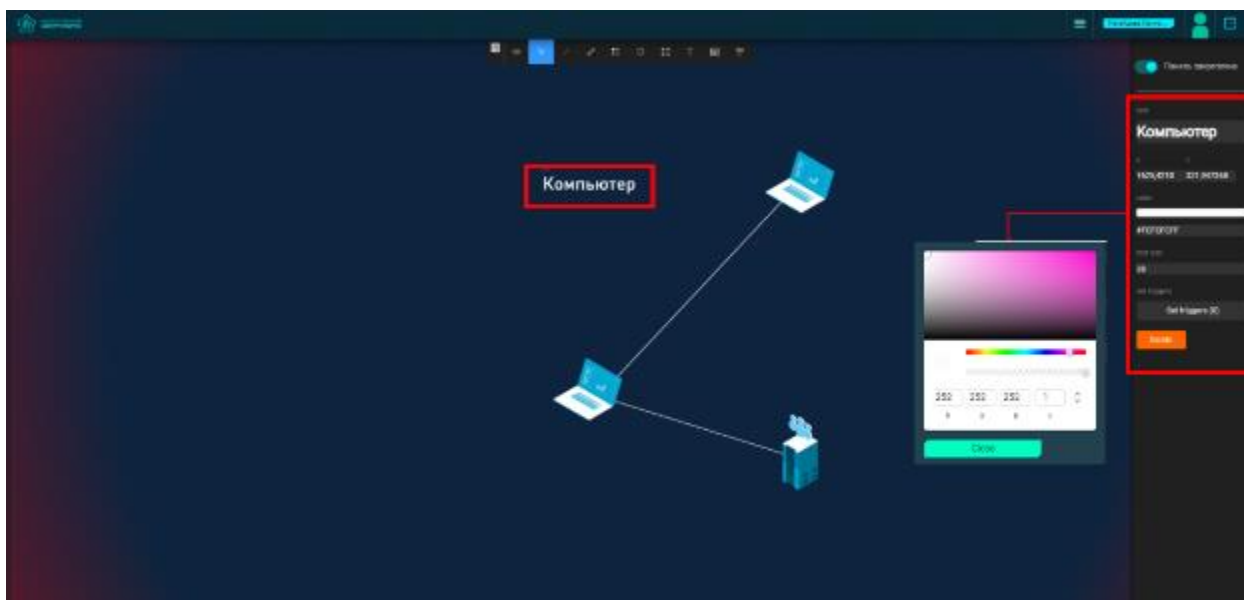


Рис. 132 – Свойства объекта

1. В поле «text» можно внести текст, который необходимо разместить на сцене.
2. Координаты расположения текста на сцене отображаются в полях «x» и «y».

Значение координат автоматически изменяется при перемещении текста по сцене. При необходимости разместить текст в конкретной точке сцены в поля «x» и «y» нужно ввести координаты точки.

3. Цвет текста и его прозрачность можно выбрать из всплывающей цветовой палитры либо ввести данные формата цвета в поле после «#».

4. В поле «font size» задается размер шрифта (Рис. 132). По умолчанию устанавливается размер 16.

5. Блок «set triggers» дает возможность задать триггеры для текста.
6. Нажав на кнопку «Delete» на панели свойств текста, можно удалить весь текст.

### 3.1.9.12. Свойства подложки

При выделении расположенной на сцене подложки на правой боковой панели отображаются следующие свойства (Рис. 133):

1. Координаты расположения 4 угловых точек подложки на сцене отображаются в полях «x» и «y». Значение координат автоматически изменяется при перемещении подложки по сцене.
2. Цвет подложки и ее контур, а также их прозрачность можно выбрать из всплывающей цветовой палитры либо ввести данные формата цвета в поле после «#»
3. Блок «set triggers» дает возможность задать триггеры для подложки.

4. Нажав на кнопку «Delete» на панели свойств подложки, можно удалить всю подложку.

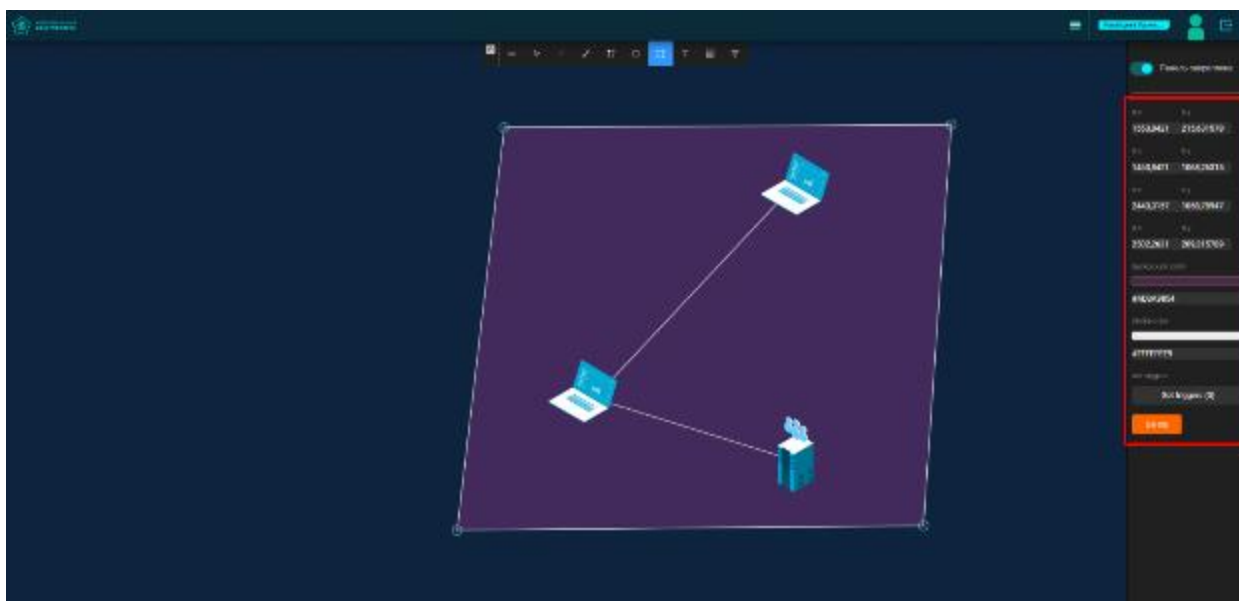


Рис. 133 – Свойства подложки

### 3.1.9.13. Триггеры редактора визуализации

На панели свойств различных типов графических объектов в блоках «set triggers» есть возможность установить условия, при которых будет запущен тот или иной эффект.

### 3.1.9.14. Триггеры объектов

При нажатии на кнопку «Set triggers» на панели свойств объекта откроется окно с настройками триггера (Рис. 134):

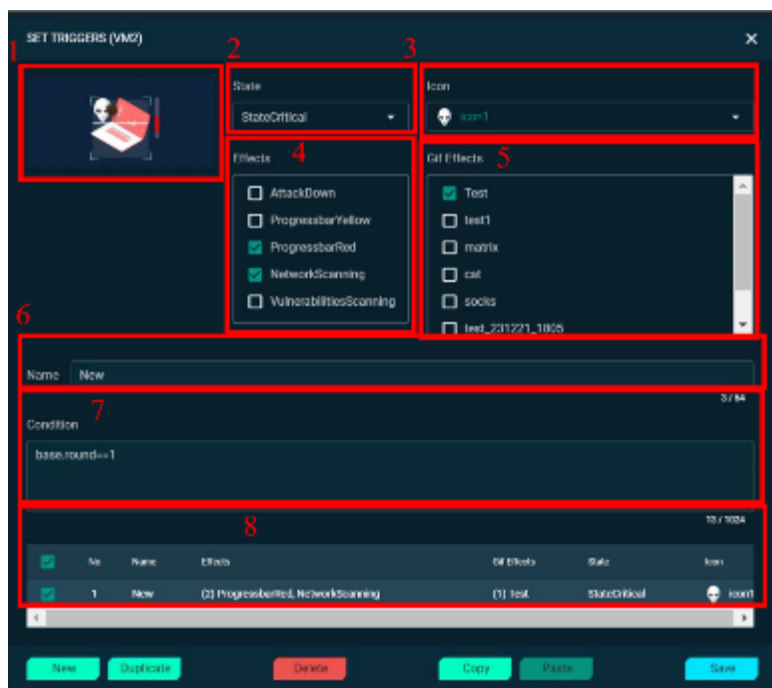


Рис. 134 – Создание триггера объекта

1. Изображение объекта, к которому применяется триггер (Рис. 134, п. 1).
2. В блоке «State» выбирается состояние объекта (Рис. 134, п. 2). В выпадающем списке доступны 4 состояния: StateOff, StateOn, StateWarning и StateCritical.
3. В блоке «Icon» в выпадающем списке выбирается иконка, отображаемая рядом с объектом (Рис. 134, п. 3).
4. В блоке «Effects» выбирается эффект (или несколько эффектов), которые будут применены к объекту (Рис. 134, п. 4).
5. В блоке «Gif Effects» выбирается динамический эффект (или несколько динамических эффектов), которые будут применены к объекту (Рис. 134, п. 5).
6. В поле «Name» необходимо задать название триггера (Рис. 134, п. 6).
7. В поле «Condition» прописывается условие, при котором срабатывает триггер (Рис. 134, п. 7).

Примеры:

Триггер, срабатывающий на определенном раунде:

```
base.round == 1
```

Триггер, срабатывающий в фазе phase1:

```
base.phase == 'phase1'
```

Триггер, срабатывающий при успешности атаки attack1:

```
base.attackStates.attack1&&base.attackStates.attack1=='UP'
```

В платформе есть объект «base» с набором атрибутов, значения которых меняются в ходе проведения мероприятия. Объект «base» – это обычный JS-объект, который инициализируется каждый раз при выполнении триггера. Объект «base» содержит в себе поля, представляющие состояние игры на текущий момент.

### Состав объекта «base»

Название	Описание
round	Целое число, текущий раунд мероприятия, сквозное значение для всех этапов, начинается с 0
phaseRound	Целое число, текущий раунд этапа, для каждого этапа счетчик инициализируется заново, начинается с 1
vector	Строка, строковой идентификатор текущего вектора из scenario.yaml
phase	Строка, строковой идентификатор текущего этапа из scenario.yaml
attack	Строка, строковой идентификатор текущей атаки из scenario.yaml
attackStates	Объект, содержит в себе пары «ключ-значение» для всех атак, которые идут или уже произошли, ключом является идентификатор атаки из scenario.yaml, а значением – одна из строк UP, DOWN, MUMBLE, RUNNING
checkerStates	Объект, содержит в себе пары «ключ-значение» для всех чекеров, которые запущены в данный момент или вернули какой-то результат, ключом является идентификатор чекера из scenario.yaml, а значением – одна из четырех строк UP, DOWN, MUMBLE, RUNNING
noiseAttackStates	Объект, содержит в себе пары «ключ-значение» для всех шумовых атак, которые идут или уже произошли, ключом является идентификатор шумовой атаки из scenario.yaml, а значением – одна из четырех строк UP, DOWN, MUMBLE, RUNNING
botStates	Объект, содержит в себе пары «ключ-значение» для всех ботов, которые запущены в данный момент или вернули какой-то результат, ключом является идентификатор бота из

scenario.yaml, а значением – одна из четырех строк UP, DOWN, MUMBLE, RUNNING

gameRunning Булево значение, отображающее текущее состояние игры: запущена или не запущена

8. Список добавленных триггеров для объекта (Рис. 134, п. 8). В таблице для каждого триггера отображаются его порядковый номер, название, состояние, эффект, динамический эффект, иконка. В списке доступна сортировка таблицы по номеру триггера.

Для создания нового триггера необходимо нажать кнопку **«New»** в окне создания триггера. В список триггеров объекта добавится новый объект с перечнем вышеперечисленных полей (см. Рис. 134, п. 2–7), которые необходимо заполнить. После заполнения всех полей окна для сохранения триггера необходимо нажать кнопку **«Save»**. Выделенный галочкой в общем списке триггер возможно продублировать, скопировать и вставить с помощью кнопок **«Duplicate»**, **«Copy»**, **«Paste»**, а также удалить с помощью кнопки **«Delete»** (Рис. 135).

### 3.1.9.15. Триггеры сцены

При нажатии на кнопку «Set triggers» на панели свойств сцены откроется окно с настройками триггера (Рис. 135):

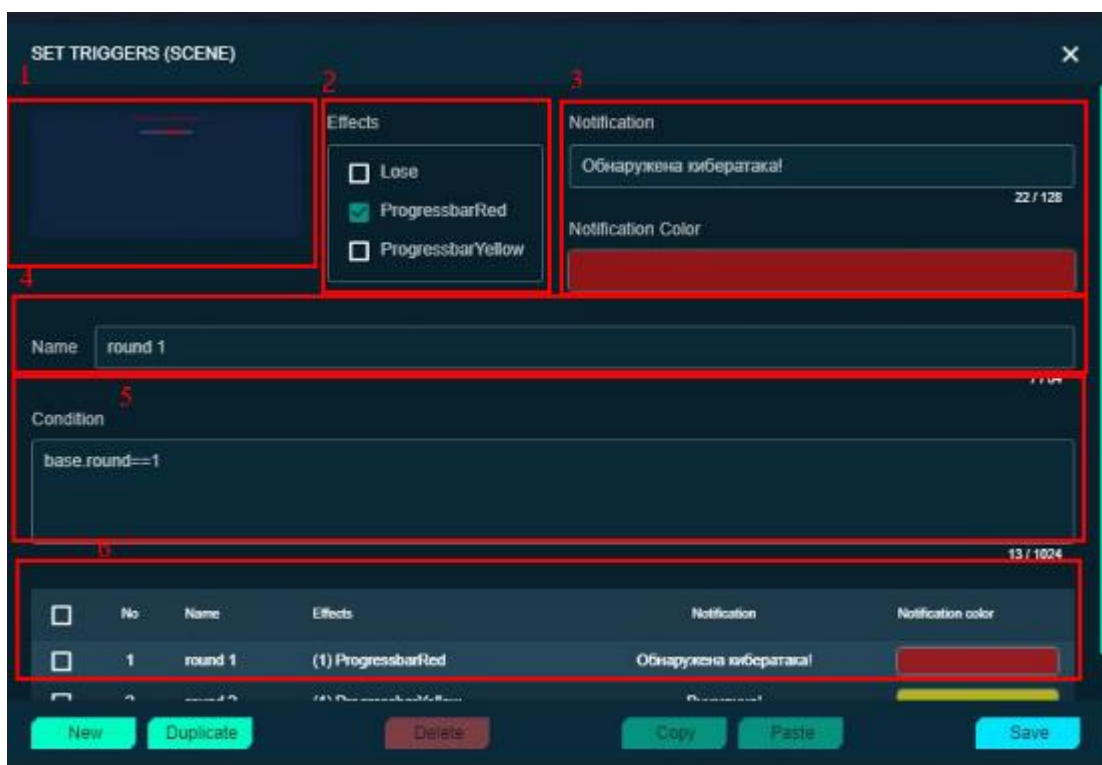


Рис. 135 – Окно с настройками триггера сцены

- внешний вид сцены при срабатывании выбранного триггера (Рис. 135, п. 1);
- в блоке «Effects» есть возможность выбрать эффект (или несколько эффектов), которые будут применены к сцене (Рис. 135, п. 2);
- в блоке «Notification» есть возможность прописать текст уведомления, который будет расположен в центральной части сцены, а также настроить его цвет и прозрачность с помощью всплывающей цветовой панели (Рис. 135, п. 3);
- в поле «Name» задается название триггера (Рис. 135, п. 4);
- в поле «Condition» прописывается условие, при котором срабатывает триггер (Рис. 135, п. 5);
- список триггеров для сцены (Рис. 135, п. 6). В таблице для каждого триггера отображаются его порядковый номер, название, эффект, текст уведомления и его цвет. В списке доступна сортировка по номеру триггера.

Для создания нового триггера необходимо нажать кнопку **«New»** в окне настроек.

В список триггеров объекта добавится новый объект с перечнем вышеперечисленных полей (Рис. 135, п. 2–5), которые необходимо заполнить. После заполнения всех полей окна для сохранения триггера необходимо нажать кнопку **«Save»**. Выделенный в общем списке триггер возможно продублировать, скопировать и вставить с помощью кнопок **«Duplicate»**, **«Copy»**, **«Paste»**, а также удалить с помощью кнопки **«Delete»**.

### 3.1.9.16. Триггер линий, текста и подложки

Триггеры для линий, текста и подложки создаются аналогичным образом через кнопку «Set triggers» на соответствующих панелях свойств. После заполнения всех настроек для сохранения триггера необходимо нажать кнопку **«Save»**.

Между равнозначными объектами триггеры можно копировать. Для этого нужно выделить объект, триггер которого необходимо скопировать, кликнуть правой клавишей мыши и далее в диалоговом окне выбрать пункт «Copy triggers» (Рис. 136).



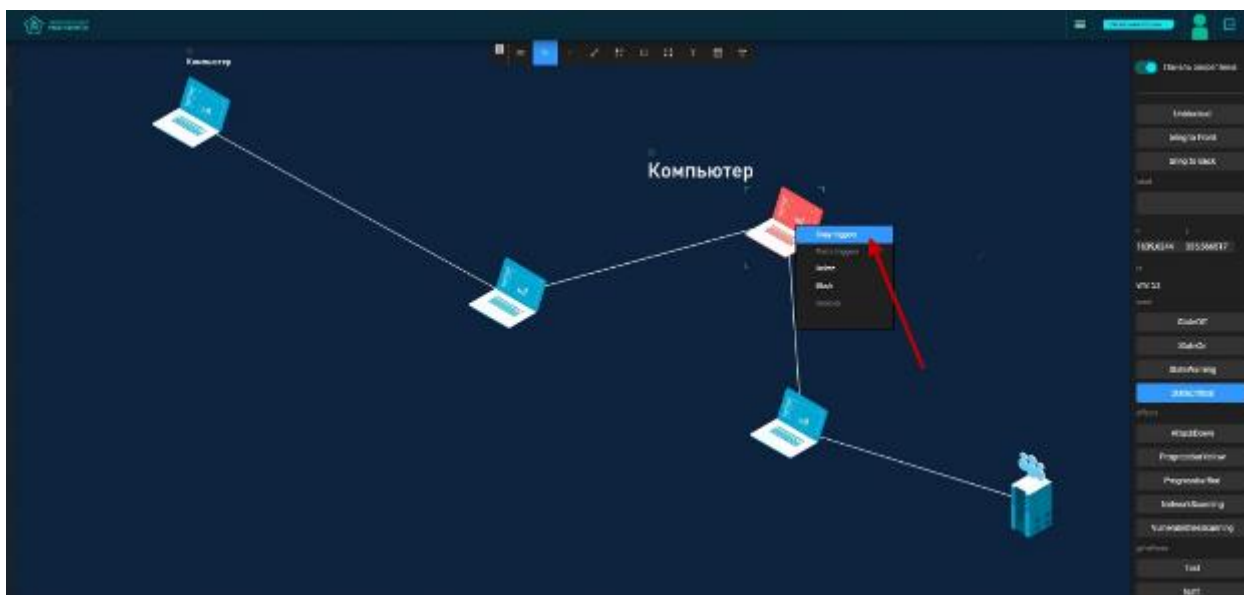


Рис. 136 – Копирование триггера объекта

Далее необходимо выделить объект, в который необходимо вставить скопированный триггер, кликнуть правой клавишей мыши и далее в диалоговом окне выбрать пункт «Paste triggers» (Рис. 137).

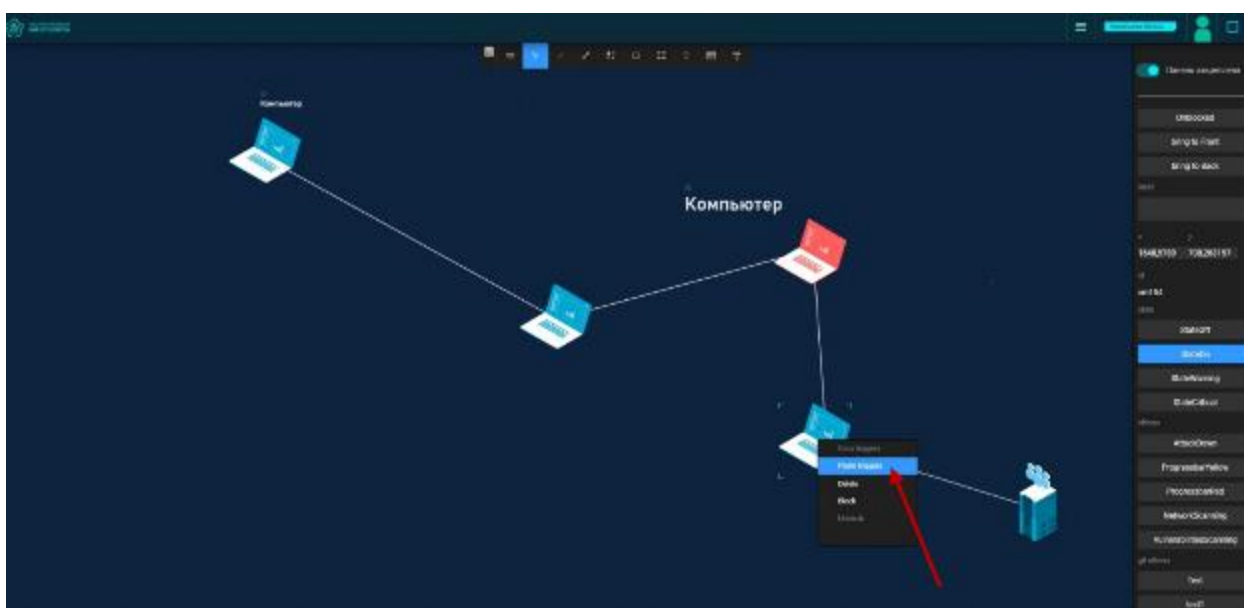


Рис. 137 – Вставка триггера объекта

### 3.1.9.17. Тестирование анимации

Чтобы проверить работу заданных триггеров графических объектов необходимо использовать инструмент «Тестирование анимации», который расположен на верхней панели инструментов (Рис. 138).

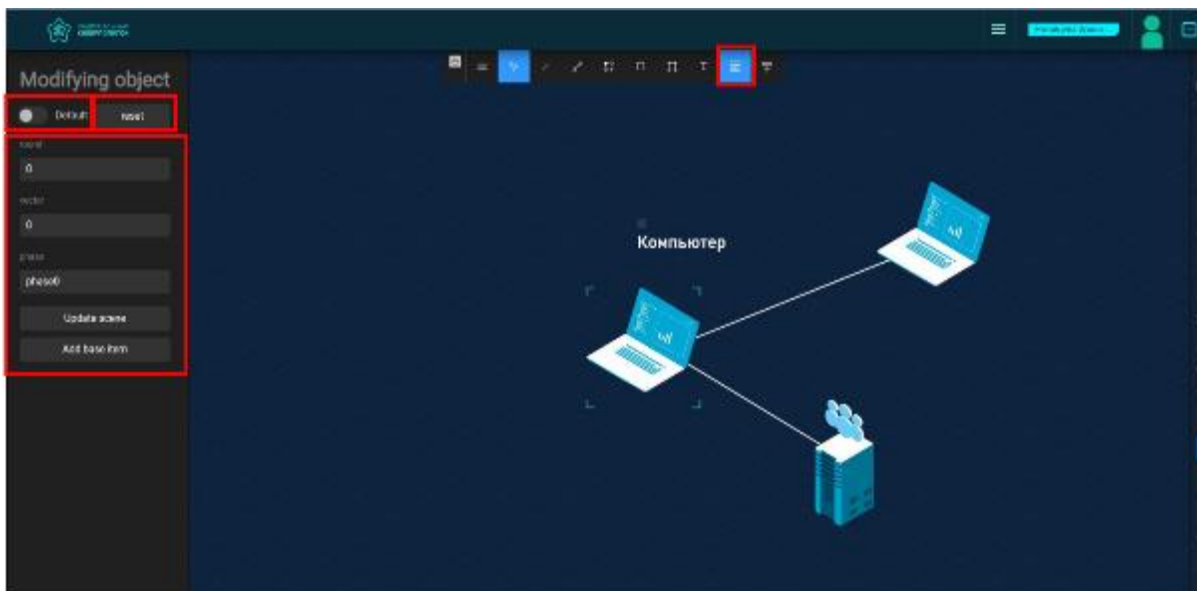


Рис. 138 – Режим «Default» инструмента «Тестирование анимации»

При выборе данного инструмента появляется левая боковая панель «Изменения объекта», на которой с помощью тумблера можно выбрать режим ввода информации о триггере:

- Режим «Default» – режим по умолчанию (Рис. 138). При этом режиме доступны для заполнения поля: «ground», «vector», «phase». Нажатие кнопки «Update scene» позволяет применить изменения и отобразить эффекты, примененные ко всем объектам сетевой инфраструктуры, в соответствии с заданными параметрами объекта «base». Кнопка «Reset» сбрасывает отображение сетевой инфраструктуры к исходному состоянию.
- Режим «JSON». В данном режиме описание объекта «base» представлено в формате json и доступно больше параметров для внесения изменений (Рис. 139). Кнопка «Add base item» позволяет добавлять состояния объекта «base» с разными раундами, и тогда, нажимая на кнопки «base1», «base2» и т. д., можно наблюдать, как будут меняться эффекты сетевой инфраструктуры в зависимости от раунда.

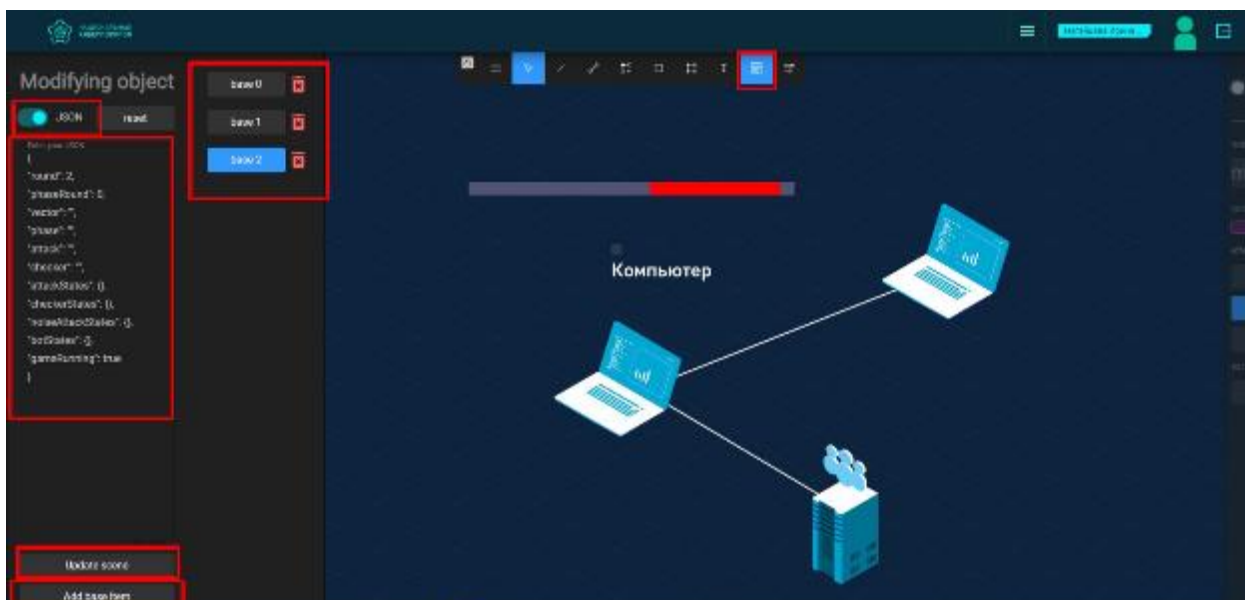


Рис. 139 – Режим «JSON» инструмента «Тестирование анимации»

Оба режима равнозначны.

## 3.2. Работа участника на платформе

### 3.2.1. Вход в платформу (авторизация)

Для доступа к платформе необходимо выполнить следующие действия:

- получить Логин и Пароль у организатора мероприятия;
- в адресной строке браузера указать адрес платформы и перейти по ссылке (предоставляется организатором);
- на форме входа в верхнем поле выбрать язык отображения интерфейса платформы, заполнить поля **«Логин»** и **«Пароль»**, проставить галочку напротив «Я принимаю условия пользовательского соглашения» и нажать кнопку **«Войти»** (Рис. 140);
- ознакомиться с соглашением об условиях использования можно, кликнув по фразе

**пользовательского соглашения**

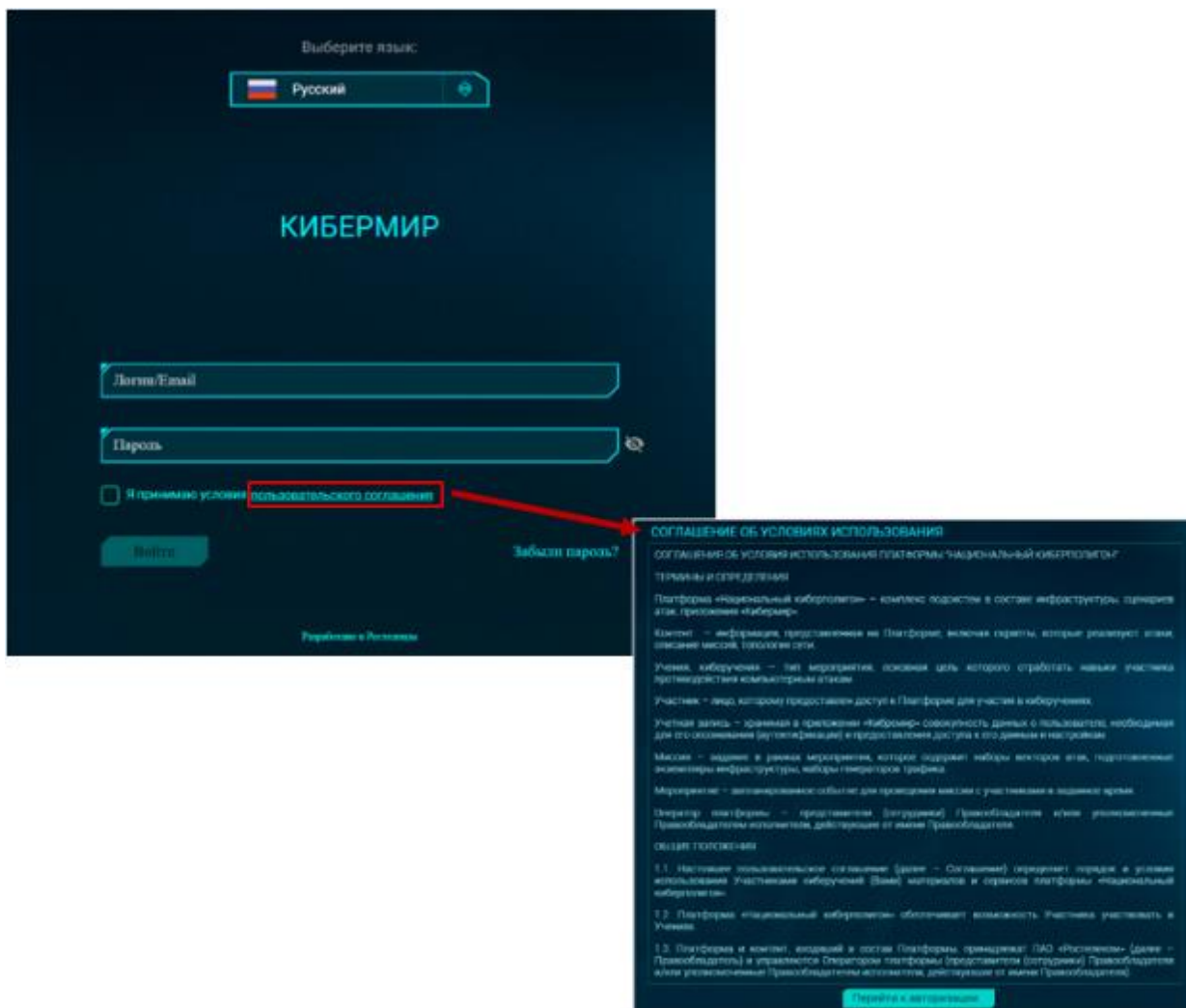


Рис. 140 – Форма входа в платформу

*Примечание. Чтобы изменить язык отображения интерфейса, необходимо выйти из платформы, выбрать другой язык и снова авторизоваться (ввести Логин и Пароль).*

Если возникли проблемы:

- проверить правильность ввода символов (нажатие клавиши CapsLock, RU/ENG-раскладка);
- обратиться к организатору мероприятия, если предыдущий шаг не помог.

### 3.2.2. Подключение к мероприятию

После успешной авторизации откроется форма **«Все мероприятия»**, содержащая список мероприятий, доступных на данный момент.

1. Если в списке не появилось ни одного мероприятия или нет необходимого, значит, оно еще не подготовлено организаторами (Рис. 141). Необходимо дождаться его появления или обратиться к организатору мероприятия для уточнения.

Для поиска мероприятия по названию можно воспользоваться функцией поиска.

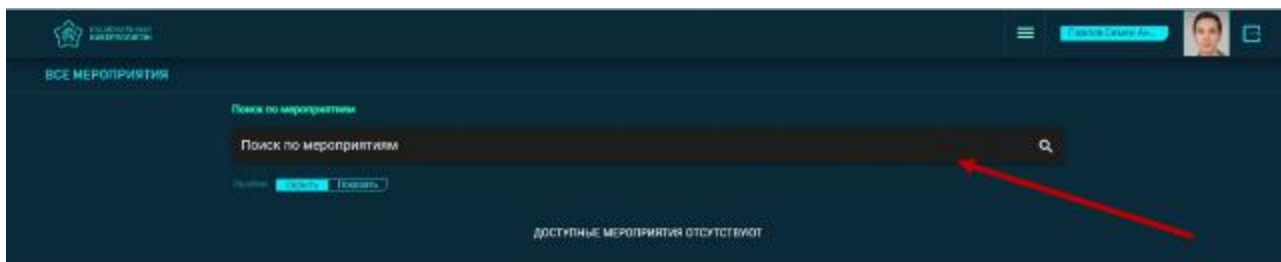


Рис. 141 – Форма со списком мероприятий

2. Если мероприятие отображается в списке, но еще находится в процессе подготовки организаторами и не началось, то у него будет статус «Ожидание», «Подготовка» или «Скоро начнется» (Рис. 142).

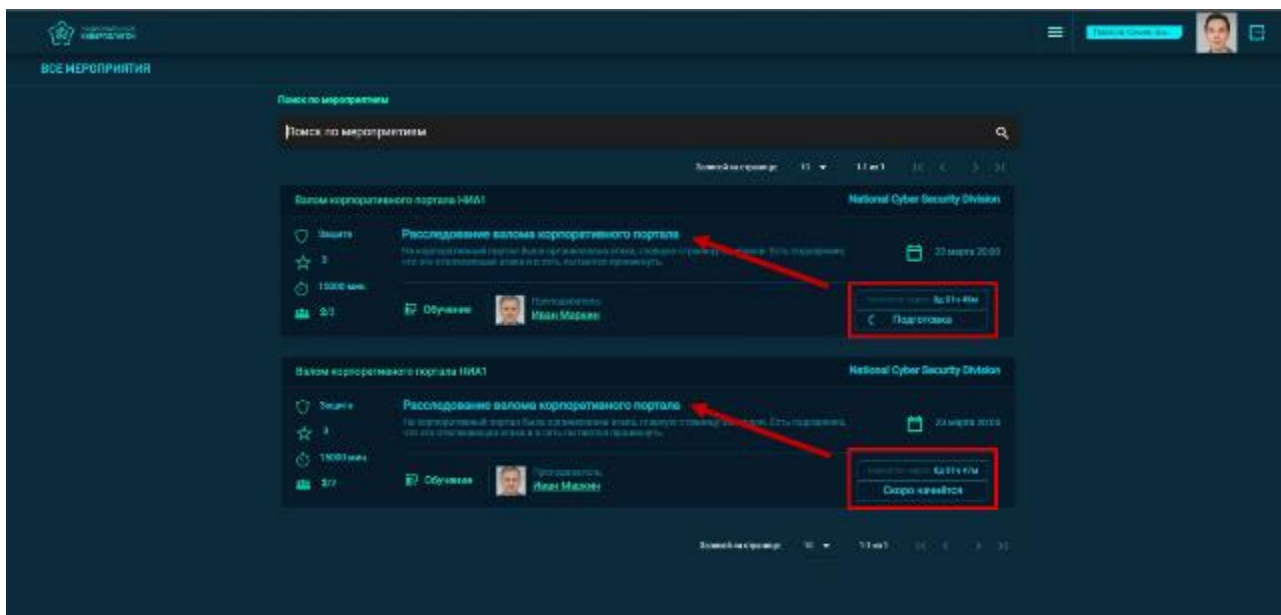


Рис. 142 – Мероприятия в списке мероприятий в статусах «Скоро начнется» и «Подготовка»

При нажатии на название мероприятия откроется карточка мероприятия (Рис. 143, 145).



Рис. 143 – Карточка мероприятия в статусе «Подготовка»

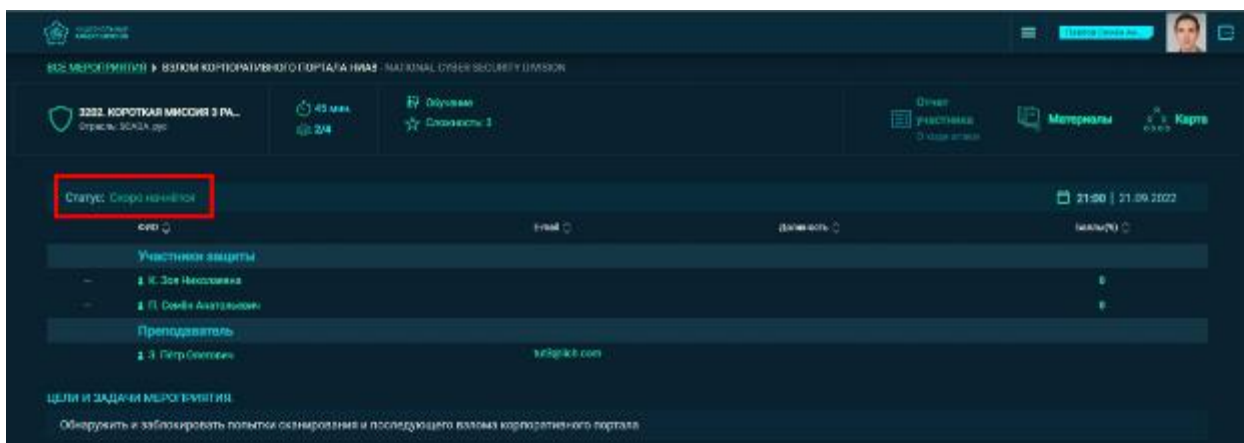


Рис. 144 – Карточка мероприятия в статусе «Скоро начнется»

3. Если мероприятие уже началось, то статус его изменится на **«В процессе!»** и появится кнопка **«Присоединиться»** (Рис. 145).

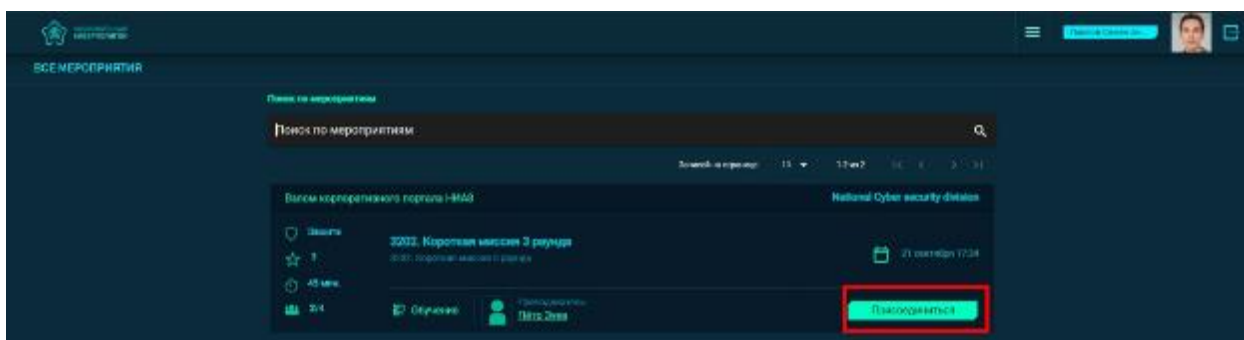


Рис. 145 – Список доступных мероприятий с кнопкой «Присоединиться»

4. Если мероприятие не единственное в списке, то необходимое можно найти по информации в карточке мероприятия (название, ФИО преподавателя, ФИО участников, дата и время проведения и т. д.).

Для подключения к необходимому мероприятию (для перехода на форму проведения мероприятия) необходимо нажать на кнопку **«Присоединиться»** в списке мероприятий (Рис. 145) либо в карточке мероприятия (Рис. 146).

### 3.2.3. Карточка мероприятия

На карточке мероприятия (Рис. 146) в течение всего времени прохождения мероприятия есть доступ к следующей информации:

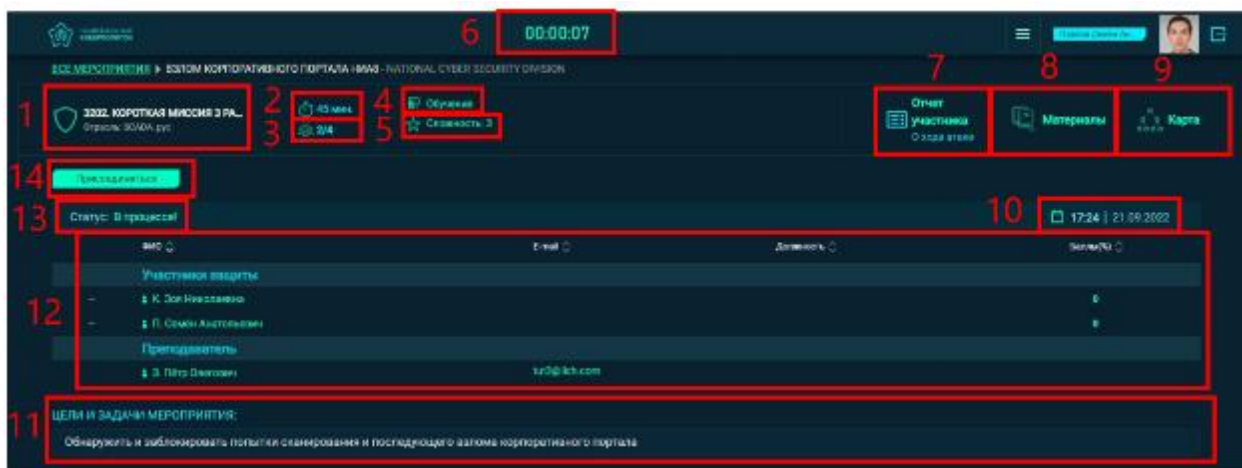


Рис. 146 – Карточка мероприятия

1. Название мероприятия и организации (Рис. 146, п. 1).
2. Длительность мероприятия (Рис. 146 п. 2).
3. Количество участников (Рис. 146, п. 3).
4. Тип мероприятия (Рис. 146, п. 4).
5. Сложность мероприятия (Рис. 146, п. 5).
6. Таймер текущего мероприятия (Рис. 146, п. 6).
7. Кнопка перехода на форму для заполнения отчета участника (Рис. 146, п. 7).
8. Кнопка перехода на форму, где можно скачать комплект сопроводительных материалов с информацией о мероприятии (Рис. 146, п. 8).
9. Кнопка, при нажатии на которую можно посмотреть топологию сети текущего мероприятия (Рис. 146, п. 9).
10. Время и дата начала мероприятия (Рис. 146, п. 10).
11. Цели и задачи мероприятия (Рис. 146, п. 11).
12. Список участников мероприятия с информацией о набранных баллах и информация о преподавателе (Рис. 146, п. 12).
13. Статус мероприятия (Рис. 146, п. 13).
14. Кнопка для перехода в виртуальное рабочее место, описанное в п. 1.4 (Рис. 146, п. 14).

Скачивание доступных материалов. Чтобы скачать комплект сопроводительных материалов с информацией о мероприятии необходимо нажать на кнопку «Материалы» (Рис. 146, п. 8) и в всплывающем окне появится перечень материалов, доступных для данного мероприятия (Рис. 147).

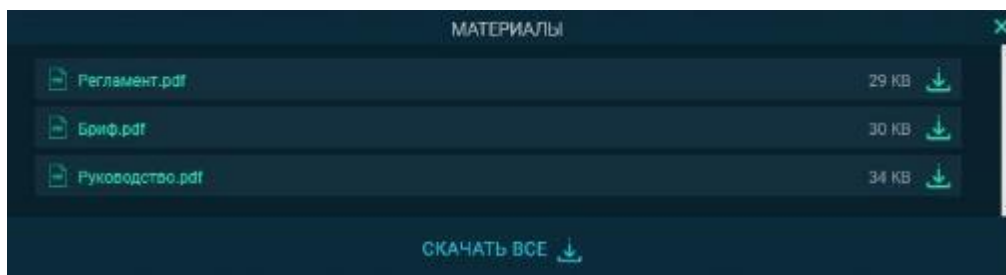





Рис. 147 – Комплект материалов для скачивания

Каждый документ можно скачать отдельно, нажав на  иконку.

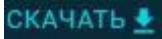

Весь комплект материалов скачивается по  кнопке в виде единого zip-архива.

При нажатии на название файла или на иконку  документ откроется в отдельной вкладке браузера.

Карта текущего мероприятия для просмотра и скачивания доступна по кнопке «Карта» (Рис. 146, п. 9).



Рис. 148 – Карта мероприятия

- карту можно скачать отдельно, нажав на  кнопку
- при нажатии на  кнопку карта откроется в отдельной вкладке браузера.

*Примечание.* Если кнопки «Карта» и «Материалы» отсутствуют на карточке мероприятия, значит, доступ к этой информации не предусмотрен для данного мероприятия.

### 3.2.4. Подключение к виртуальному рабочему месту

После присоединения к мероприятию откроется форма проведения мероприятия с виртуальным рабочим местом участника (Рис. 149).



В случае появления консоли виртуальной машины необходимо заполнить поля «Логин» и «Пароль» (Рис. 149) и начать работу. Логин и пароль можно получить у организатора мероприятия.

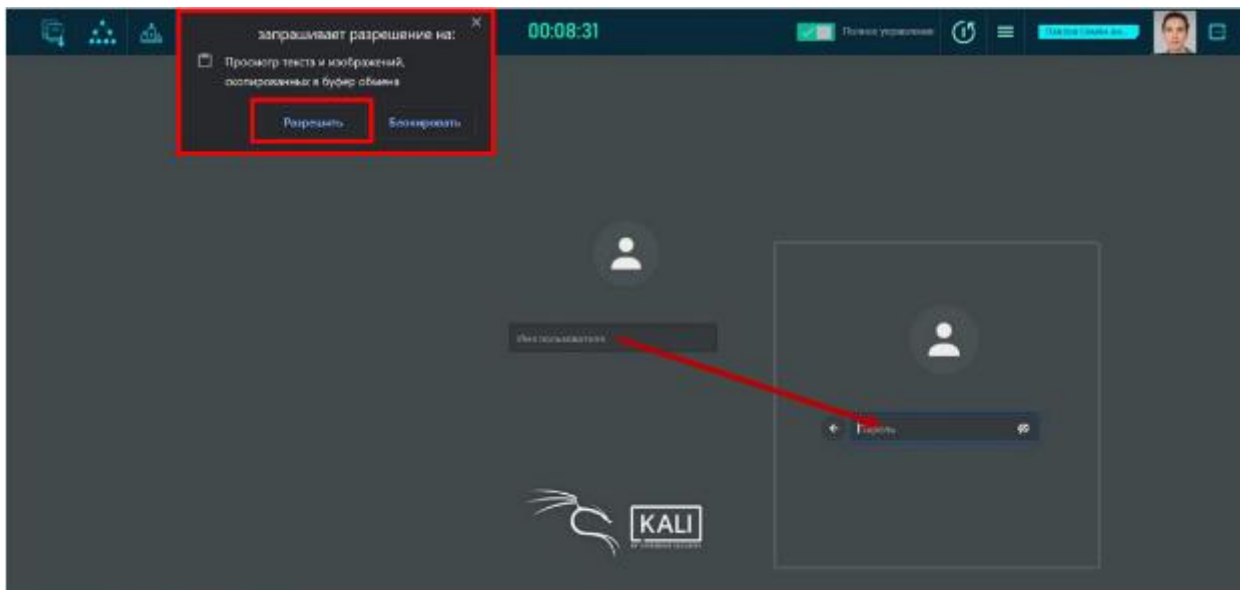


Рис. 149 – Форма входа в виртуальное рабочее место

Если вместо консоли виртуальной машины отображается черный экран, то необходимо:

- обновить консоль с помощью кнопки «Обновить» на экране по центру или обновить вкладку браузера (F5 ↻ или ) (Рис. 150);
- обратиться к организатору мероприятия, если предыдущие шаги не помогли.

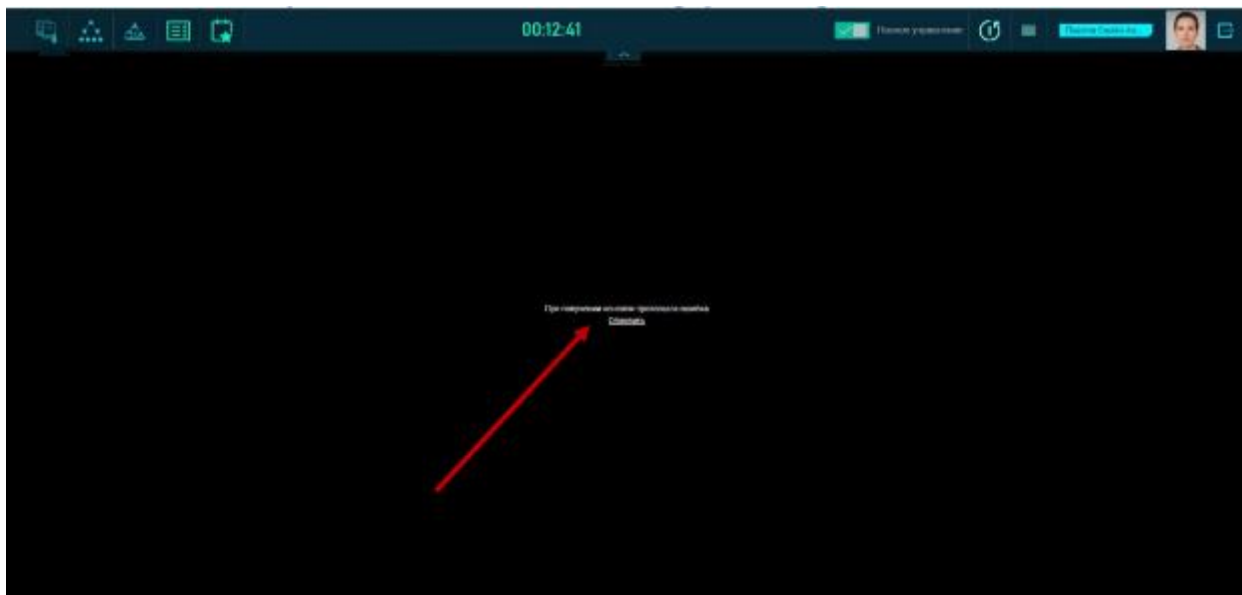


Рис. 150 – Ошибка входа в виртуальное рабочее место

При подключении к виртуальной машине необходимо разрешить браузеру использовать буфер обмена, для этого на всплывающем диалоговом окне браузера необходимо нажать на кнопку **«Разрешить»** (Рис. 149).

Если доступ браузера к буферу обмена был запрещен, то необходимо в настройках браузера выбрать пункт **«Оставить этому сайту доступ к буферу обмена»** (Рис. 151).

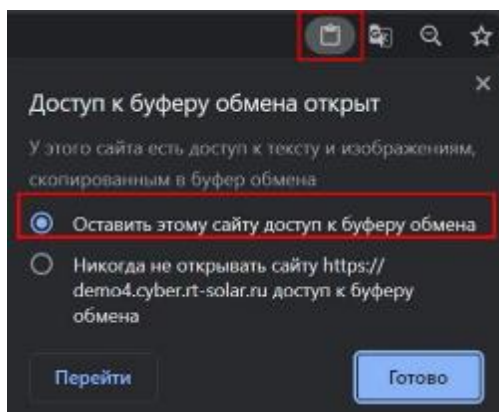


Рис. 151 – Изменение настроек браузера

Основная работа ведется на форме проведения мероприятия (Рис. 152). Панели, расположенные по верхнему и правому краю рабочей области, можно показывать и скрывать по мере необходимости. Для того чтобы появилась верхняя панель, необходимо кликнуть на ярлычок, расположенный посередине верхней панели (Рис. 152). При наведении курсора на правую границу экрана появится правая панель.

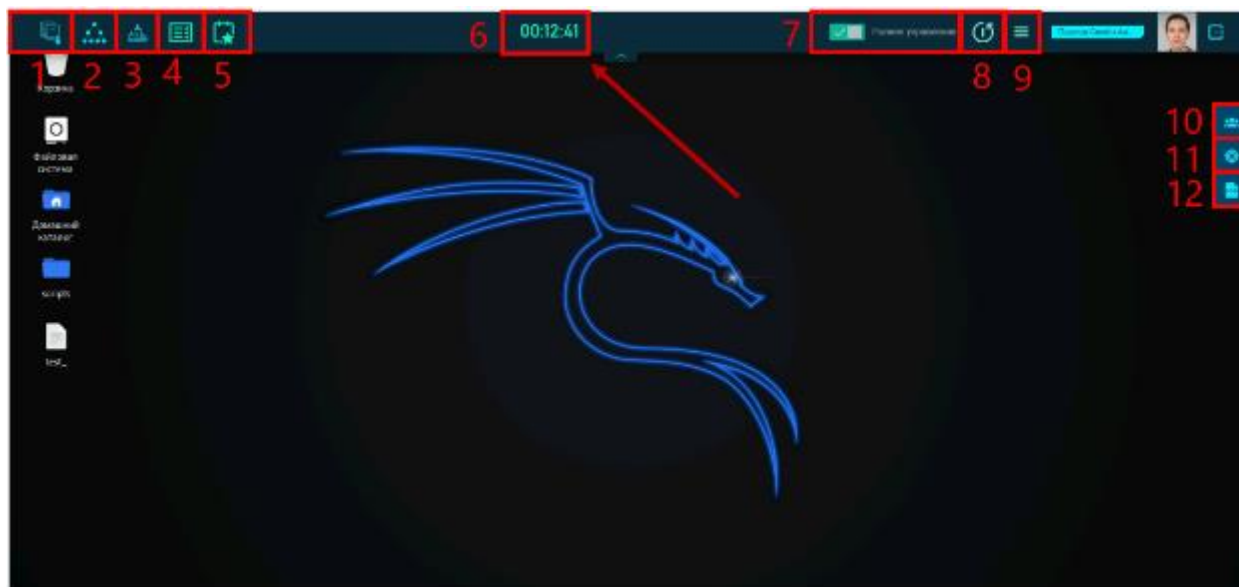






Рис. 152 – Форма проведения мероприятия

На форме доступны следующие функции:

1. Материалы мероприятия (аналогичные тем, что в карточке мероприятия) можно скачать, нажав на кнопку (Рис. 152,  п. 1).
2. Карта мероприятия доступна по кнопке  (Рис. 152, п. 2).
3. Список текущих опубликованных результатов участников можно посмотреть, нажав на кнопку (при  условии, что ваше мероприятие добавлено администратором на общее табло результатов) (Рис. 152, п. 3).
4. Форма для заполнения отчета доступна по кнопке (Рис. 152, п. 4).
5. Переход в карточку текущего мероприятия доступен по кнопке  (Рис. 152, п. 5). Если нажать на эту кнопку, удерживая клавишу Ctrl, то карточка текущего мероприятия откроется в соседней вкладке браузера.
6. Таймер мероприятия (Рис. 152, п. 6).
7. С помощью переключателя «Полное управление» осуществляется переключение между полнофункциональным и ограниченным режимом управления рабочим столом (Рис. 152, п. 7).

По умолчанию при первом переходе на форму проведения мероприятия переключатель находится в режиме **«Вкл»** (означает, что используется полнофункциональный режим управления). В этом режиме доступен буфер обмена данными между рабочим столом и браузером.

При возникновении технических проблем с подключением к удаленному рабочему столу есть возможность переключения в ограниченный режим управления. Для этого переключатель **«Полное управление»** необходимо перевести в режим **«Выкл»**, после чего появится уведомление о подтверждении переключения в ограниченный режим (Рис. 153).

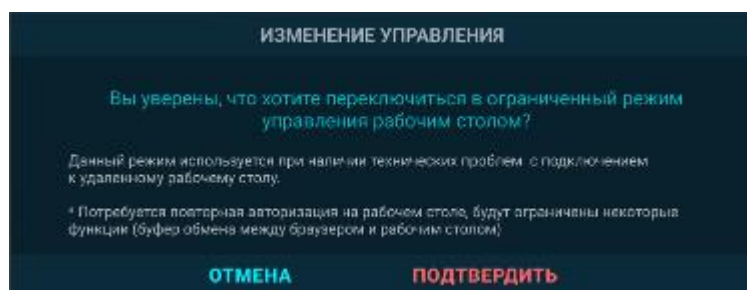



Рис. 153 Уведомление о подтверждении переключения в ограниченный режим управления рабочим столом

*Примечание. Если возникла необходимость переключиться в ограниченный режим управления рабочим столом, необходимо перезагрузить виртуальную машину во избежание сбоев в работе.*

Для осуществления перезагрузки необходимо нажать на  кнопку на верхней панели формы проведения мероприятия.

После переключения в ограниченный режим управления рабочим столом будет доступна консоль виртуальной машины (виртуальное рабочее место участника). Необходимо заполнить поля «Логин» и «Пароль» (Рис. 149) и начать работу. Логин и пароль можно получить у организатора мероприятия.

Для возврата в полнофункциональный режим управления рабочим столом необходимо перевести переключатель «**Полное управление**» в режим «**Вкл**», после чего появится уведомление о подтверждении переключения в полнофункциональный режим (Рис. 154).

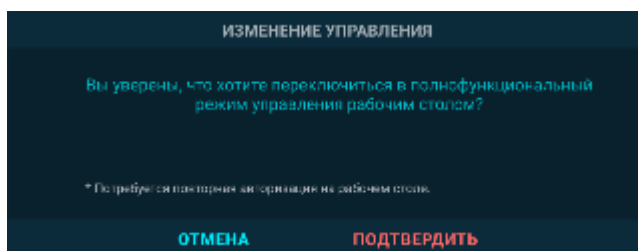



Рис. 154 – Уведомление о подтверждении переключения в полнофункциональный режим управления рабочим столом

8. Перезагрузить виртуальную машину, если возникла такая необходимость, можно, нажав на кнопку  (Рис. 152, п. 8), после чего появится уведомление о подтверждении перезагрузки машины (Рис. 155) и виртуальная машина перезагружается.

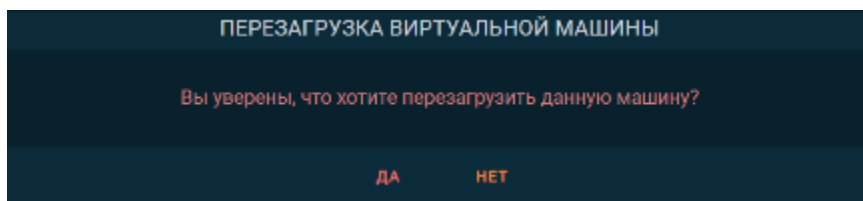


Рис. 155 – Уведомление о подтверждении перезагрузки виртуальной машины

На время перезагрузки виртуальной машины форма проведения мероприятия примет вид как на рисунке 156.

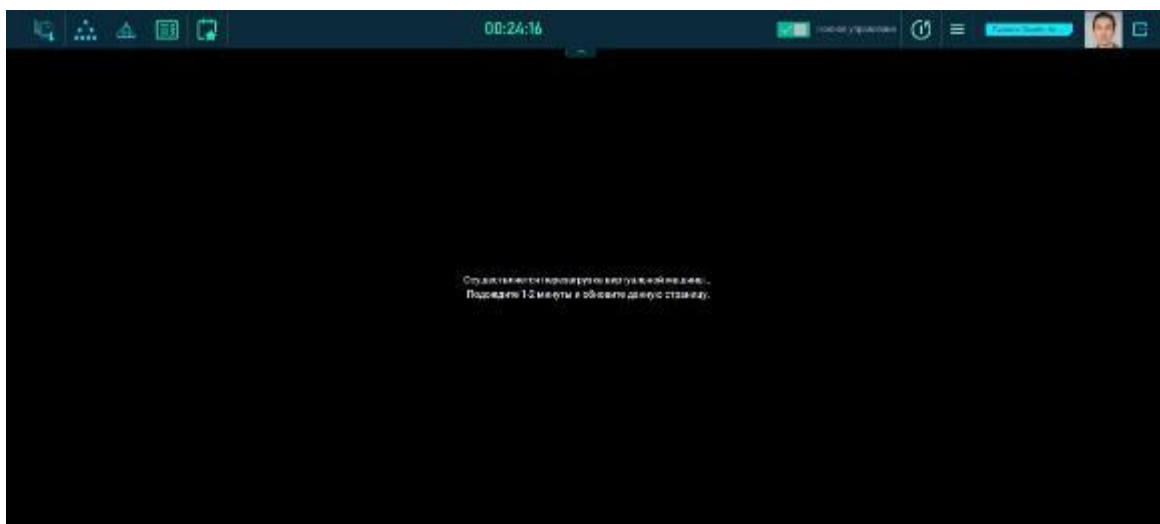



Рис. 156 – Форма проведения мероприятия при перезагрузке виртуальной машины

Данная кнопка отображается только на форме проведения мероприятия и только для участников с назначенной виртуальной машиной.

9. Нажав на кнопку  и выбрав в выпадающем списке пункт **«Мероприятия»**, можно перейти к списку доступных мероприятий (Рис. 152, п. 9).

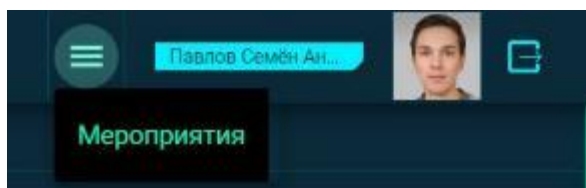



Рис. 157 – Переход к списку мероприятий

10. В ходе мероприятия можно посмотреть состав команды – список участников, назначенных на данное мероприятие, нажав на кнопку  (Рис. 152, п. 10).

Участники, присоединившиеся к мероприятию, подсвечиваются зеленым, не присоединившиеся – серым (Рис. 158).

Кликнув на фото участника, можно посмотреть его профиль.

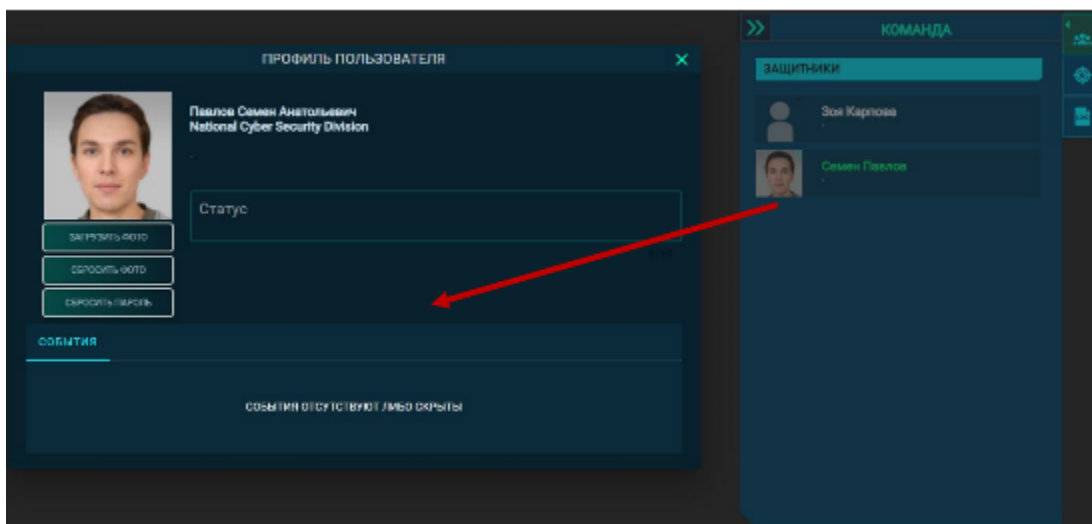



Рис. 158 – Список участников мероприятия и профиль участника

11. По кнопке  можно посмотреть текущую задачу на этап в соответствии со сценарием (т. е. то, что происходит на данный момент) (Рис. 152, п. 11), а также получить подсказку, нажав на **«Получить подсказку»** внизу окна (Рис. 159).

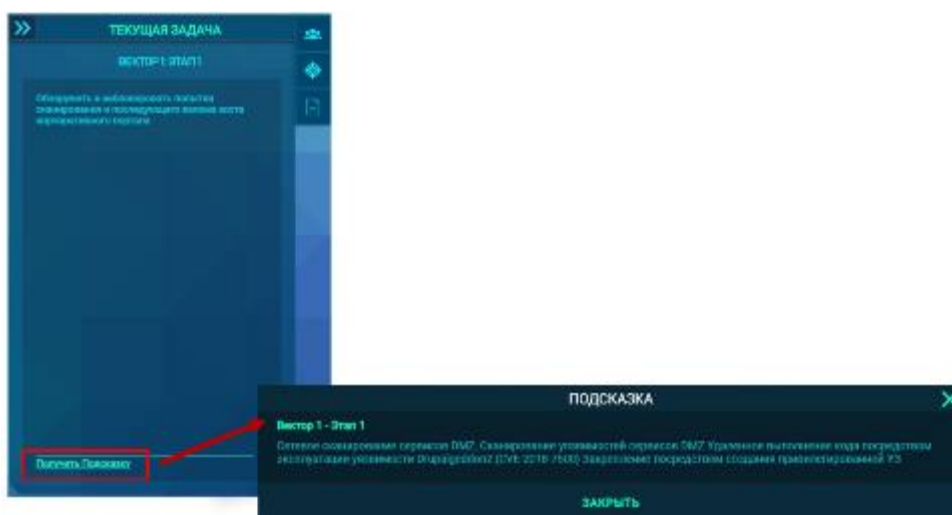



Рис. 159 – Окна с текущей задачей и с подсказкой

На некоторых мероприятиях кнопка **«Получить подсказку»** может отсутствовать.

12. История событий мероприятия – историю событий с момента начала мероприятия до текущего момента можно посмотреть по кнопке (Рис. 152, п.  12, 21).

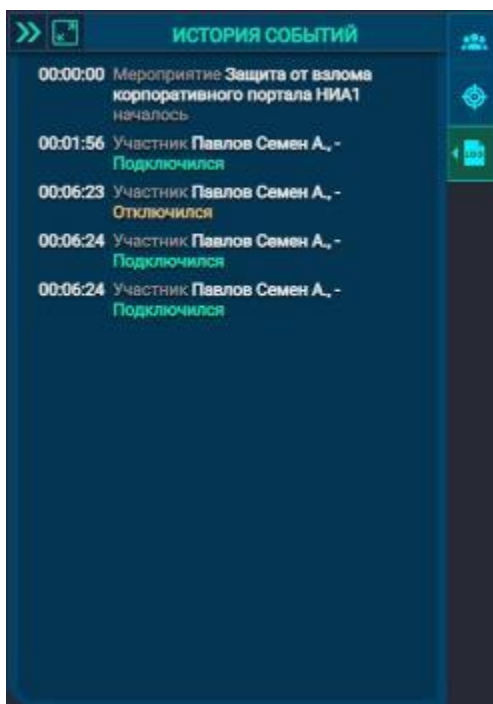


Рис. 160 – История событий мероприятия

### 3.2.5. Заполнение отчета об обнаруженных атаках



При нажатии на  кнопку на карточке мероприятия либо на кнопку  на форме проведения мероприятия (Рис. 152) откроется форма для заполнения отчета (Рис. 161).



Рис. 161 – Форма отчета. Вид по умолчанию

На данной форме необходимо добавить и заполнить все атаки, которые были обнаружены в ходе мероприятия.

*Примечание. При работе в ограниченном режиме управления рабочим столом, чтобы не вводить данные в отчет вручную, можно, открыв интерфейс платформы через браузер рабочего стола, воспользоваться буфером обмена внутри виртуальной машины.*

### 3.2.6. Добавление техник

Для добавления новой атаки в отчет нужно определить, к какой технике/тактике относится эта атака. Далее для создания новой техники необходимо нажать на кнопку «Добавить технику», расположенную в середине верхней панели отчета (Рис. 161).

Откроется форма «Карта техник», где необходимо выбрать подходящую технику (Рис. 162).



Рис. 162 – Форма «Карта техник»


На форме представлена следующая информация:

1. Фильтр техник по ключевым словам. Для его использования необходимо в поле фильтра ввести, разделяя пробелами, ключевые слова (корни слов), связанные с техниками. Например: скан SYN (Рис. 162, п. 1).

2. Колонки с названием тактик (Рис. 162, п. 2).

Заголовки колонок состоят из 2 строк:

- название тактики;
- название тактики в MITRE ATT@CK на английском языке.

При наведении курсора мыши на иконку , расположенную перед названием колонки, появляется всплывающая подсказка с общим описанием тактики (Рис. 163).

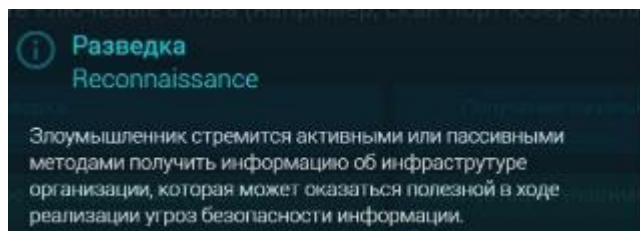


Рис. 163 – Всплывающая подсказка с описанием техники

3. Карточки техник, расположенные в соответствующих колонках тактик (Рис. 162, п. 3).

Карточка техники содержит название техники и краткое описание данной техники.

4. Всплывающая подсказка с описанием техники доступна при наведении курсора мыши на карточку техники (Рис. 162, п. 4).



5. При нажатии левой клавишей мыши на карточку техники она становится выбранной и подсвечивается (Рис. 162, п. 5).

При нажатии на кнопку **«Подтвердить»** в отчет добавляется техника с перечнем полей (индикаторов компрометации и описаний процедур защиты и восстановления) для заполнения, соответствующих заданному типу техники.

Двойное нажатие на левую клавишу мыши на карточке техники сразу добавляет карточку в отчет и закрывает карту техник (или форму выбора техник).

Чтобы закрыть форму «Карта техник», необходимо нажать на кнопку **«Отмена»**, при этом новая техника в отчет не добавляется (Рис. 162).

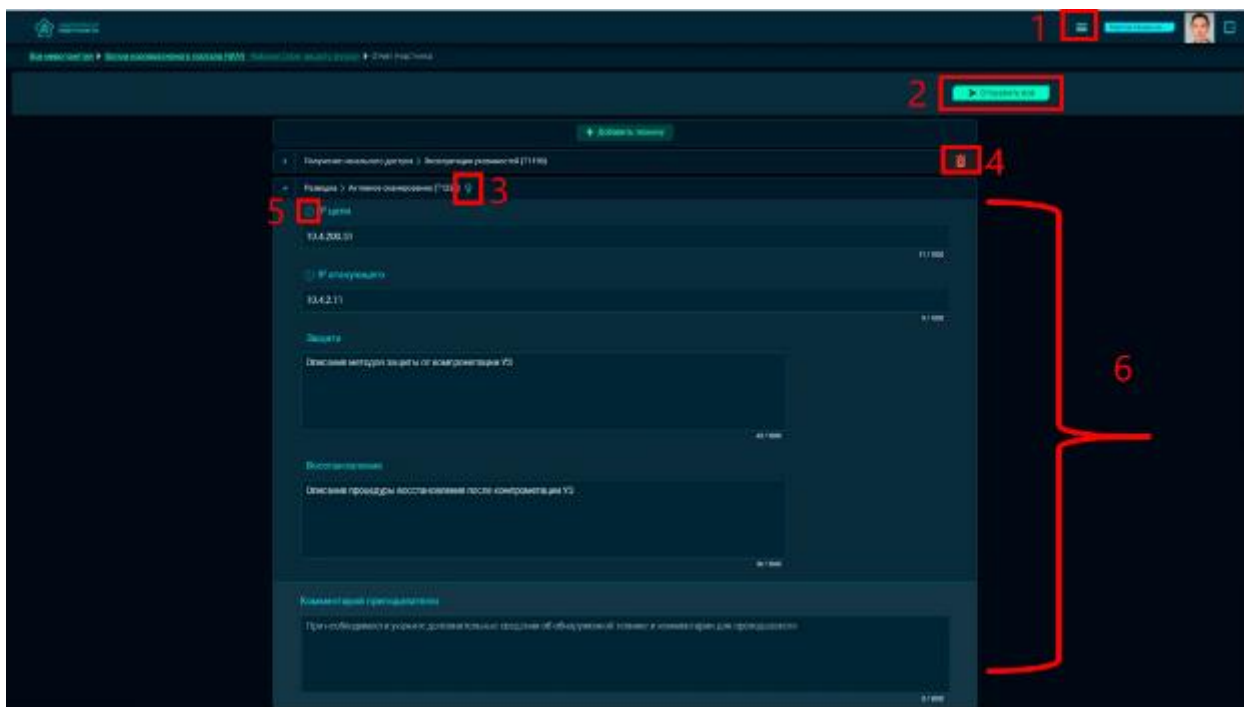



Рис. 164 – Форма отчета

На форме отчета доступны следующие функции:

1. Нажав на кнопку  и выбрав в выпадающем списке **«Табло результатов»**, можно перейти к списку текущих опубликованных результатов участников (при условии, что ваше мероприятие добавлено администратором на общее табло результатов) (Рис. 164 п. 1, 166, 167).

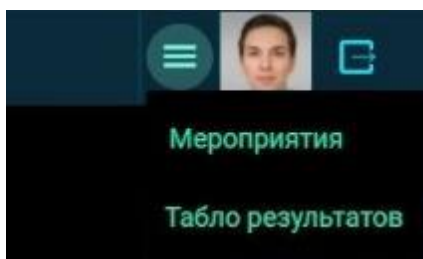


Рис. 165 – Переход к табло результатов

Имя	Баллы	Организация
П. Савин Александрович	100	National Cyber security division
К. Зоя Николаевна	0	National Cyber security division

Рис. 166 – Таблица результатов

Посмотреть рейтинг и количество баллов, полученных за заполнение отчета, можно также в карточке мероприятия в столбце «Баллы» (Рис. 146).

2. При нажатии на кнопку **«Отправить всё»** (Рис. 164, п. 2) весь отчет будет отправлен на автоматизированную оценку и кнопка станет недоступной (Рис. 167).

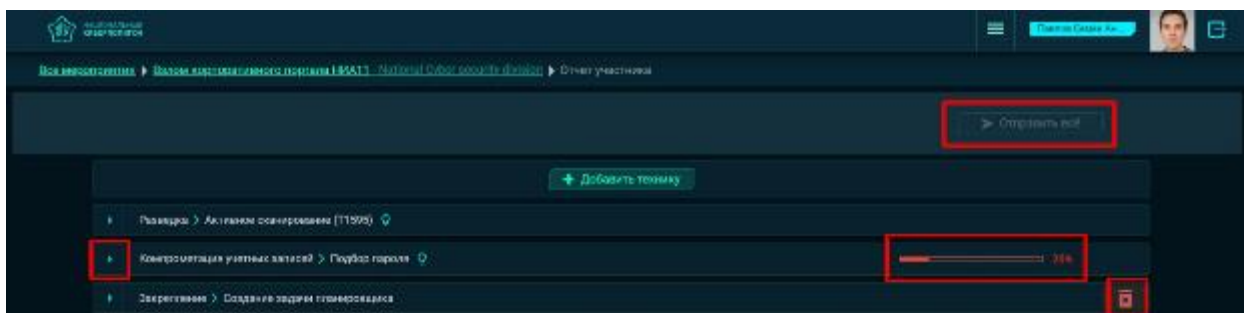



Рис. 167 – Форма отчета после отправки

3. При открытии отчета могут быть автоматически добавлены одна или несколько техник, предусмотренных для данного мероприятия. Эти техники в отчете помечены иконкой рядом с названием техники (Рис. 164, п. 3).

Если автоматически предоставленных техник недостаточно для полного описания обнаруженных в ходе мероприятий атак, то дополнительные техники можно добавить, нажав на кнопку **«Добавить технику»**.

4. Технику из отчета можно удалить, нажав на иконку в  правом углу панели каждой техники (Рис. 164, п. 4, 168). При этом появится всплывающее диалоговое окно для подтверждения или отмены удаления (Рис. 168).

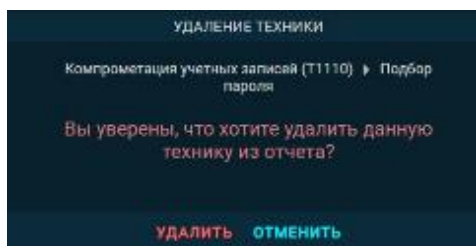




Рис. 168 – Диалоговое окно при удалении техники

При переходе мероприятия в статус «Подведение итогов» или «Завершено» иконка для удаления техники из отчета станет недоступна.

Для автоматически добавленных техник, предусмотренных для данного мероприятия, возможность удаления отсутствует и иконка не отображается. 

5. В каждой технике необходимо заполнить появившиеся поля – индикаторы компрометации (IoC) – на основании данных, полученных в ходе мероприятия (обнаружения и расследования кибератак) (Рис. 164, п. 5).

Каждая техника внутри общего отчета может быть свернута или развернута кликом по панели техники. Выше всех в списке располагается техника, которая добавлена в общий отчет позднее остальных (Рис. 167). Одновременно может быть развернуто не более одной техники.

6. При наведении курсора на иконку  расположенную рядом с названием поля, появляется подсказка с примером заполнения данного поля (Рис. 164, п. 6).

Добавленные в отчет техники отсортированы по времени их добавления в отчет, то есть первой становится техника, добавленная последней.

Техники в отчете можно перемещать между другими техниками с помощью переноса левой кнопки мыши за заголовок. При перемещении все техники должны быть свернуты.

Правильность заполнения техники отображается в виде линейного индикатора с процентами. Если заполнено 50% техники и более, то цвет линейного индикатора – зеленый (Рис. 169). Если заполнено менее 50%, то цвет линейного индикатора – красный (Рис. 168).

Если по мере продвижения в расследовании атак необходимо изменить или дополнить уже отправленный отчет, то после внесения изменений (дополнений) в поля отчета кнопка для его отправки примет вид «Отправить всё» и ее необходимо будет нажать снова (Рис. 169).

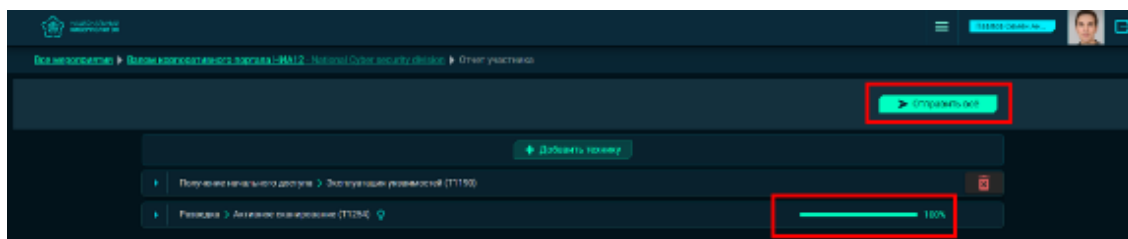


Рис. 169 – Форма отчета после внесения правок

Отчет необходимо заполнить и отправить до завершения мероприятия. При переходе мероприятия в статус «Подведение итогов» или «Завершено» кнопка для отправки отчета станет недоступна и примет вид **«Отправка недоступна»**, а также при наведении курсором над ней появится предупредительное уведомление **«Идет подведение итогов или мероприятие завершено»** (Рис. 170).

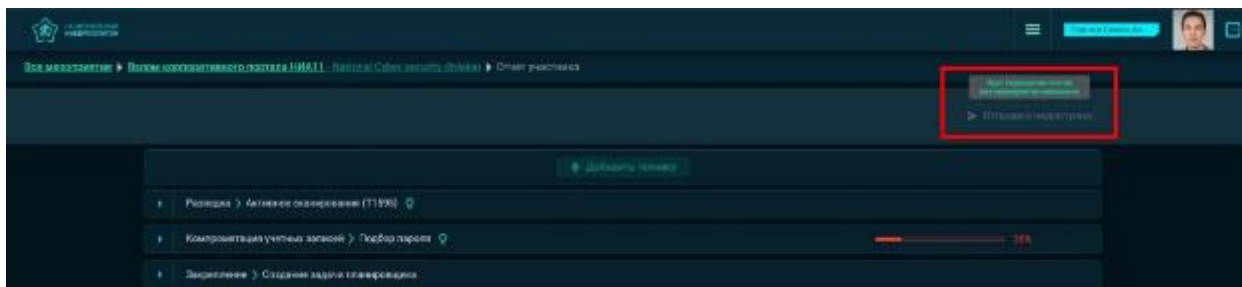


Рис. 170 – Форма отчета в режиме подведения итогов

*Важно! На протяжении всего мероприятия работа ведется с единым отчетом. Дополнять, редактировать и отправлять отчет можно неограниченное число раз, пока идет мероприятие.*

### 3.2.7. Копирование данных об обнаруженных техниках в отчет с использованием буфера обмена внутри виртуальной машины при работе в ограниченном режиме управления рабочим столом

Если при работе в ограниченном режиме управления рабочим столом для заполнения отчета необходимо скопировать данные из виртуальной машины в форму отчета (буфер обмена между виртуальной машиной и браузером недоступен), нужно выполнить следующие действия:

- после подключения к виртуальной машине необходимо открыть браузер внутри нее;
- в адресной строке браузера указать адрес платформы и перейти по ссылке;
- осуществить вход в платформу используя тот же логин и пароль;

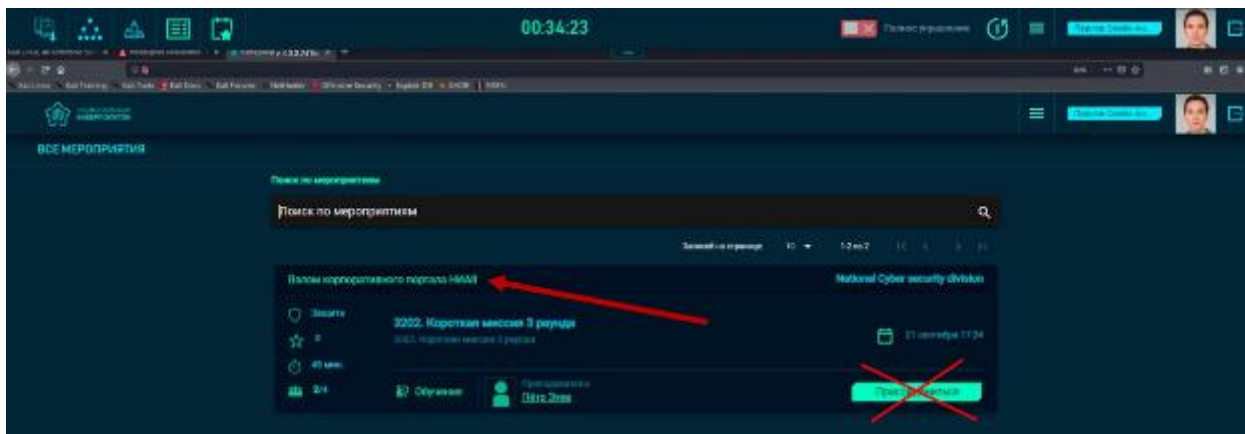
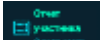


Рис. 171 – Форма «Все мероприятия» внутри виртуальной машины

- на форме «Все мероприятия» зайти в карточку необходимого мероприятия и открыть форму отчета,  используя кнопку (Рис. 172);

**ВАЖНО!**

1. Присоединяться к мероприятию **НЕ НУЖНО!**
2. Работа одновременно в двух формах отчета (внутри виртуальной машины и на платформе в основном браузере) может привести к **перезаписи и потере данных**.

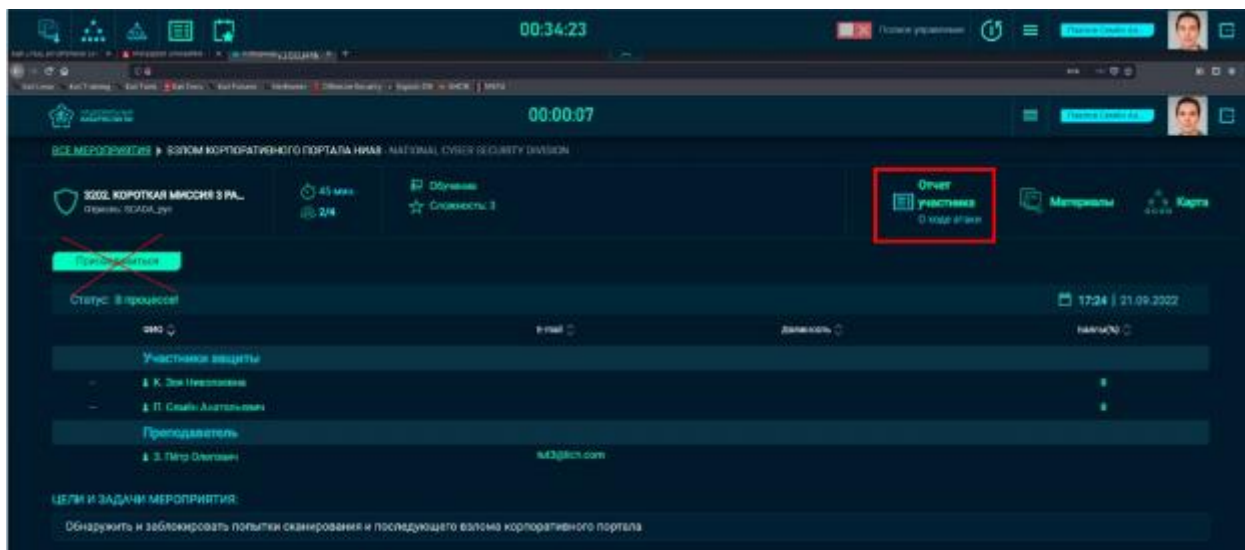


Рис. 172 – Карточка мероприятия внутри виртуальной машины

- заполнить форму отчета техниками, обнаруженными в ходе мероприятия, используя буфер обмена виртуальной машины, и отправить отчет (Рис. 173).

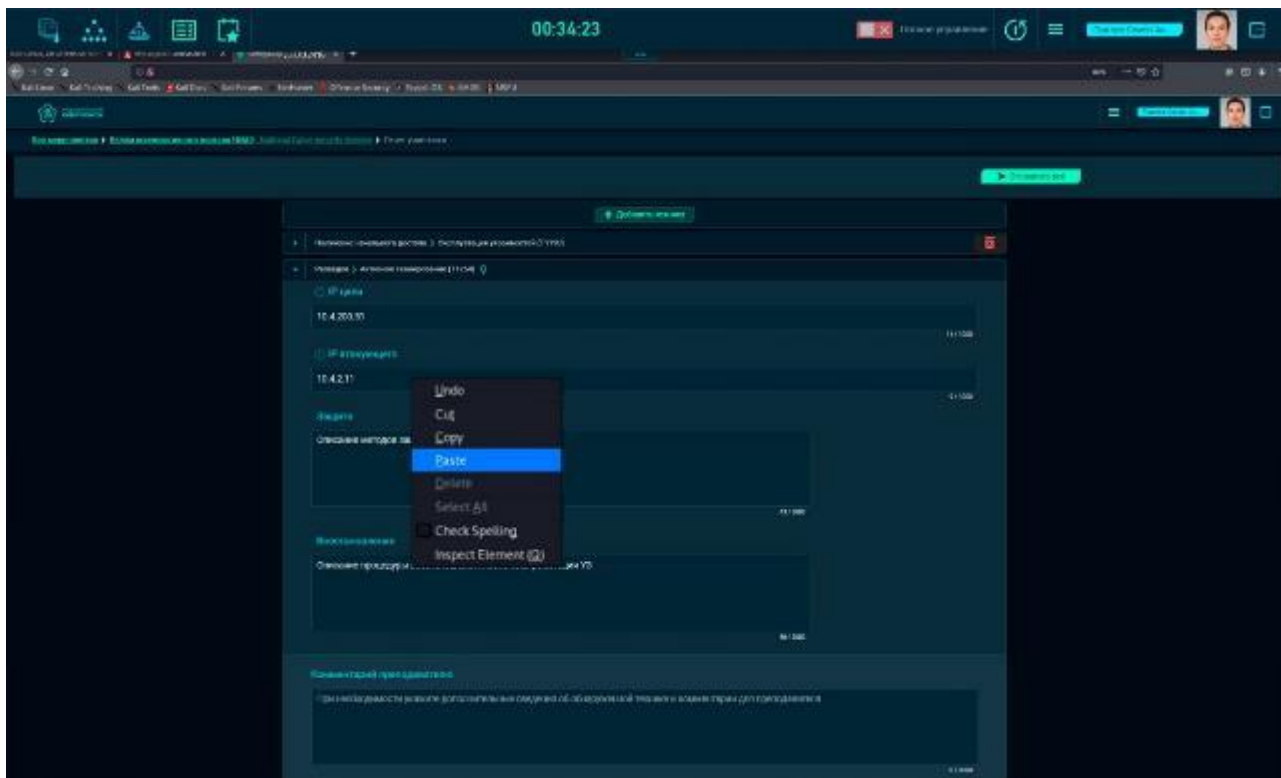


Рис. 173 – Форма отчета внутри виртуальной машины

Если возникла проблема, не описанная в данном методическом пособии, то для ее решения нужно обратиться к организаторам.

## Приложение А. Файл с данными о пользователях .xlsx

Название колонки	Формат данных	Обязательное значение
Фамилия	Строка	Да
Имя	Строка	Да
Отчество	Строка	Нет
Е-mail	Е-mail	Да
Должность	Строка	Нет
Организация	Строка	Нет
Роль	Строка	Нет
Пароль	Строка	Нет

Пример содержимого файла:

```
Белов Василий Петрович vp_belov17@mail.ru Специалист по ИБ АО "Сбербанк" Participant $56TyUm67_"
```