



Киберполигон CyberBY

обучение кибербезопасности на виртуальной
инфраструктуре





Актуальные проблемы и вызовы кибербезопасности

01

Дефицит квалифицированных кадров

Резкий рост киберугроз привел к нехватке специалистов, обладающих достаточным уровнем знаний и опыта для защиты организаций от сложных атак

02

Быстрое изменение ландшафта угроз

Сложность и количество атак растут, в результате чего требуются новые навыки и оперативное обновление знаний для противодействия новейшим техникам злоумышленников

03

Разрыв между теорией и практикой

Традиционные методы обучения недостаточны для формирования практических навыков — необходимы современные способы отработки реальных сценариев противодействия киберугрозам

04

Необходимость командной работы

Современные атаки требуют скоординированного подхода, но ИБ-команды часто не могут эффективно взаимодействовать между подразделениями внутри юридического лица



Задачи и решения для команд реагирования Центров кибербезопасности

Для начинающих команд

Освоение базовых навыков киберзащиты, таких как обнаружение уязвимостей, реагирование на простые инциденты и знакомство с основными инструментами защиты. Киберполигон позволяет новичкам быстро адаптироваться в безопасной и контролируемой среде

Для команд среднего уровня

Углубленная работа с более сложными сценариями атак и защитных мер, тренировки по реагированию на целевые атаки, изучение методик анализа угроз и внедрение передовых техник безопасности

Для продвинутых команд

Имитация сложных и многоступенчатых атак, которые требуют высокой координации и слаженности действий. Такие тренировки помогают командам оттачивать навыки противодействия сложным угрозам и реагирования на инциденты высокого уровня

Курсы

Тренажеры

CTF

Киберучения



Отработка и развитие навыков по кибербезопасности на Киберполигоне

Киберполигон функционирует в национальной доменной зоне **BY**

Обучающие курсы

Изучайте новые технологии и методы киберзащиты через практические курсы, подходящие для разного уровня подготовки

Самостоятельное изучение

Интерактивные тренажеры и СТФ

Запускайте виртуальные машины без длительного ожидания и оттачивайте знания на практике в любое время

Отработка на практике знаний и навыков

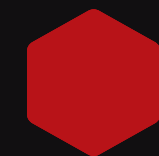
Киберучения на виртуальном городе «Neopolis»

Возможность проверить навыки как с атакующей, так и с защищающейся стороны на инфраструктуре виртуального города

Интенсивная проверка компетенций

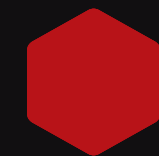


Инструментарий Киберполигона



Матрица MITRE ATT&CK

Постоянно обновляемая база знаний о техниках и методах действий киберпреступников



Dashboard

Инструмент, позволяющий осуществлять действенный контроль за процессом обучения специалистов и их прогрессом в развитии компетенций

Эти инструменты позволяют более точно настраивать процесс обучения, выявлять области для улучшения и обеспечивать постоянное развитие команды

Механика Киберполигона

Атаки



Специалисты из сообщества Киберполигона
Регулируемые атаки, покрывающие 70% матрицы MITRE ATT&CK
Red team Заказчика или его подрядчиков

Веб-портал атакующего



Веб-портал защиты

Мониторинг
Расследование
Реагирование



ИБ-команды Заказчиков (прежде всего SOC)
Возможно подключение дочерних структур и ключевых подрядчиков
Рекомендуется добавлять представителей ИТ и DevSecOps



Обучающие курсы

Здесь специалисты по информационной безопасности могут пройти практико-ориентированное обучение с подробной теоретической частью



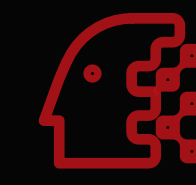
Современные и прикладные знания

Модульные курсы включают актуальные знания и практические навыки, необходимые для работы с современными киберугрозами и инструментами защиты



Обучение и доступность 24/7

Пользователи могут изучать курсы в любое удобное для них время в комфортном для них темпе

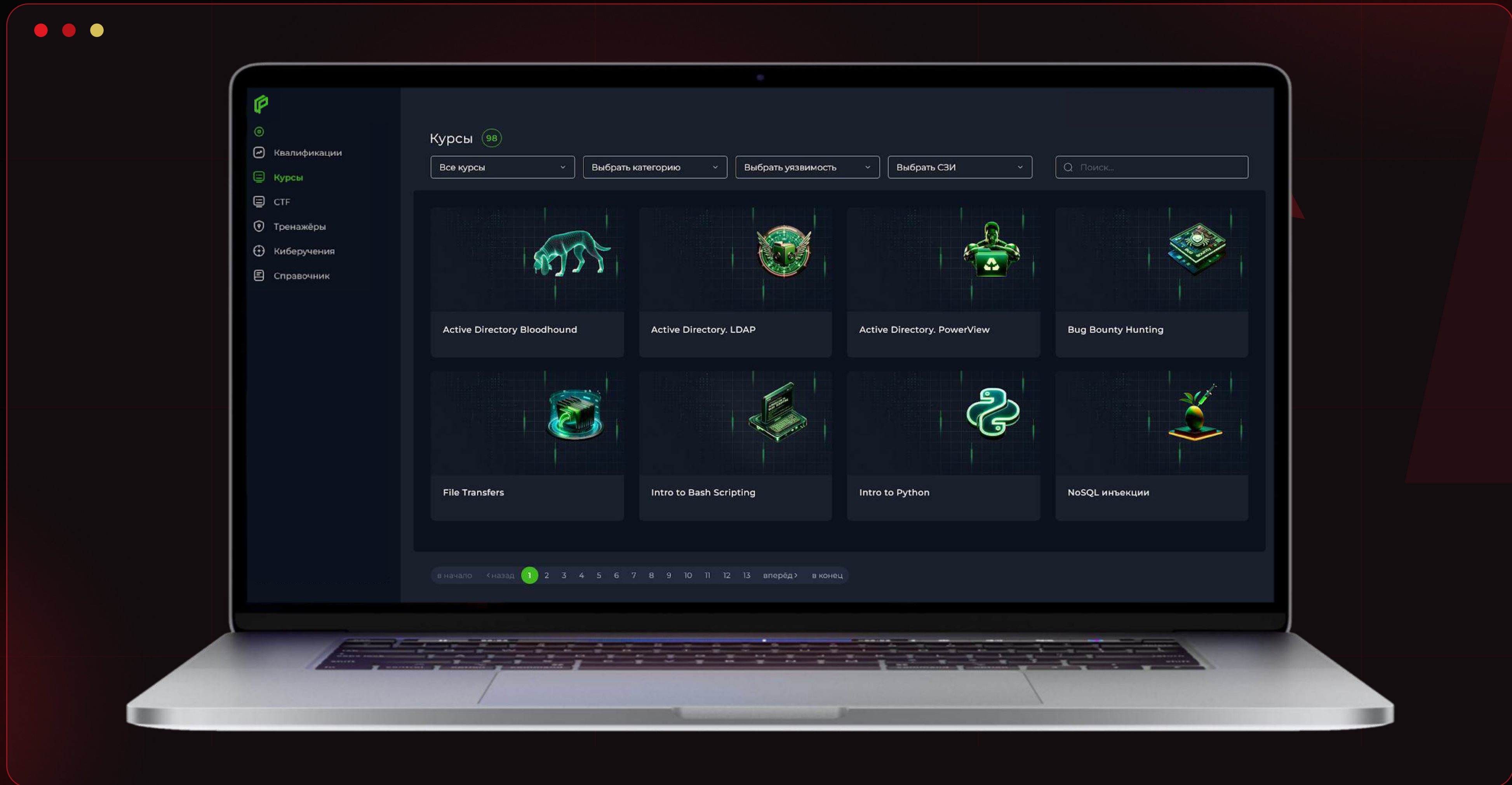


Простой доступ

Для получения доступа к курсам необходимо лишь зарегистрироваться на платформе и подключиться через VPN

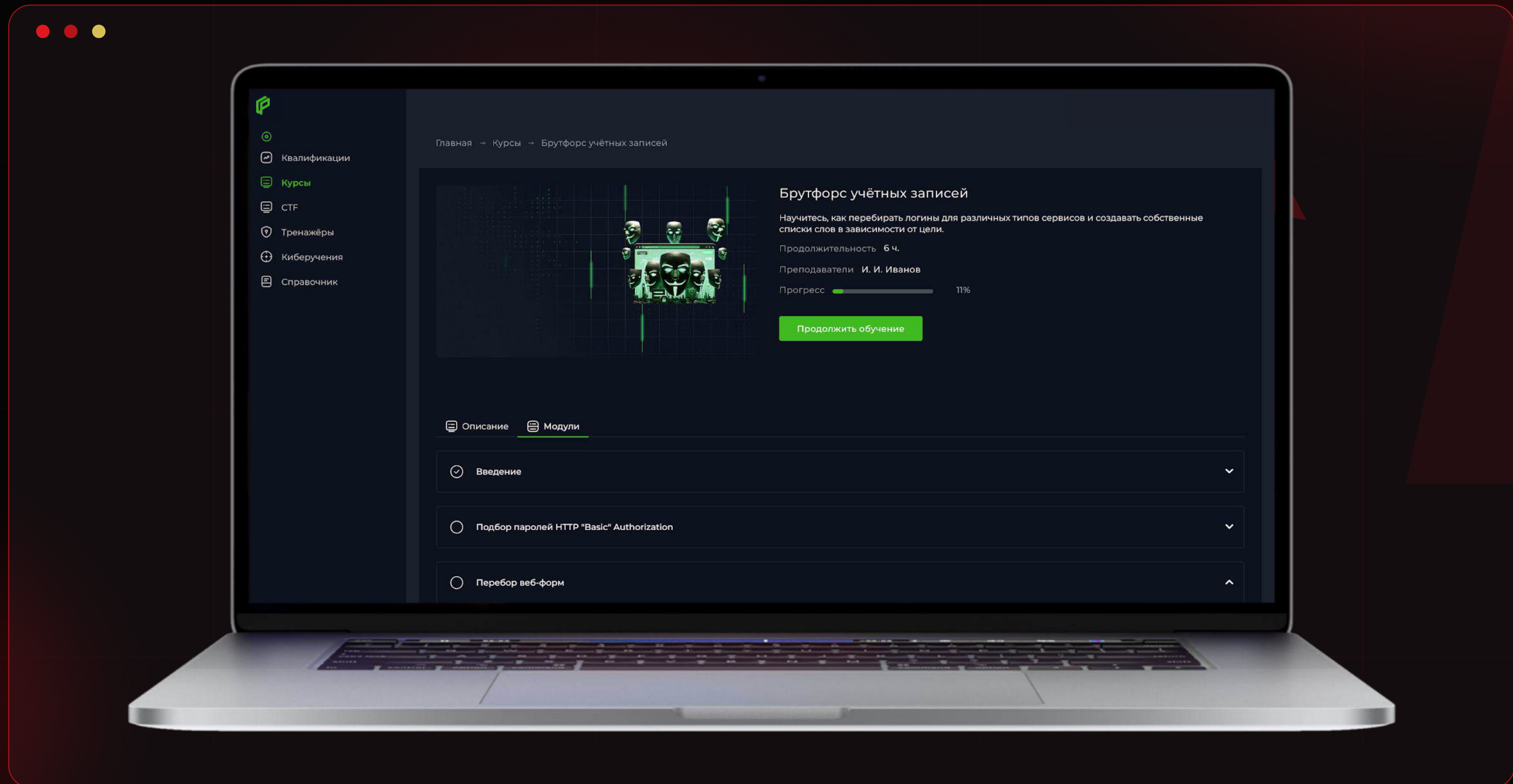


Обучающие курсы

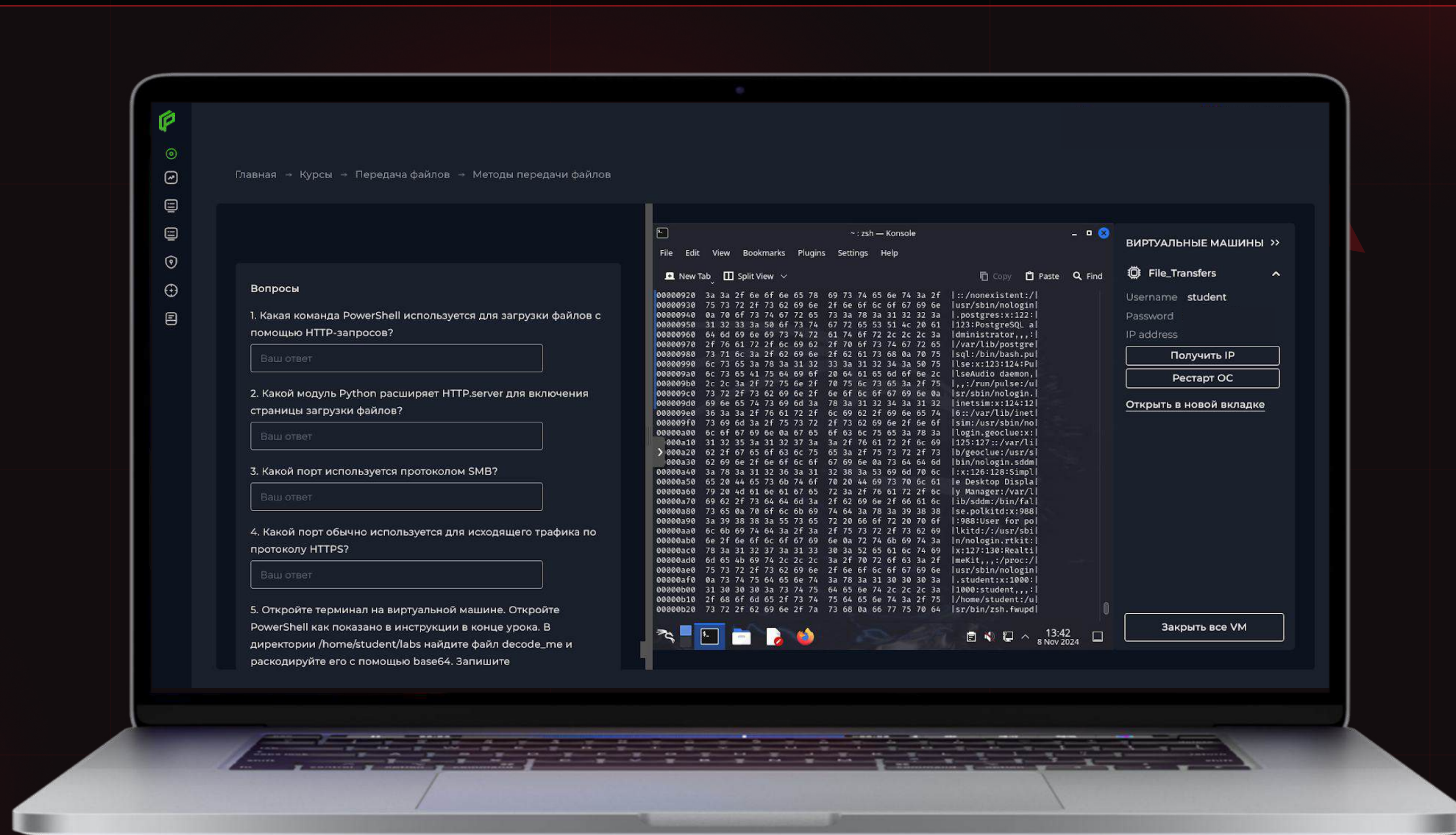




Обучающие курсы

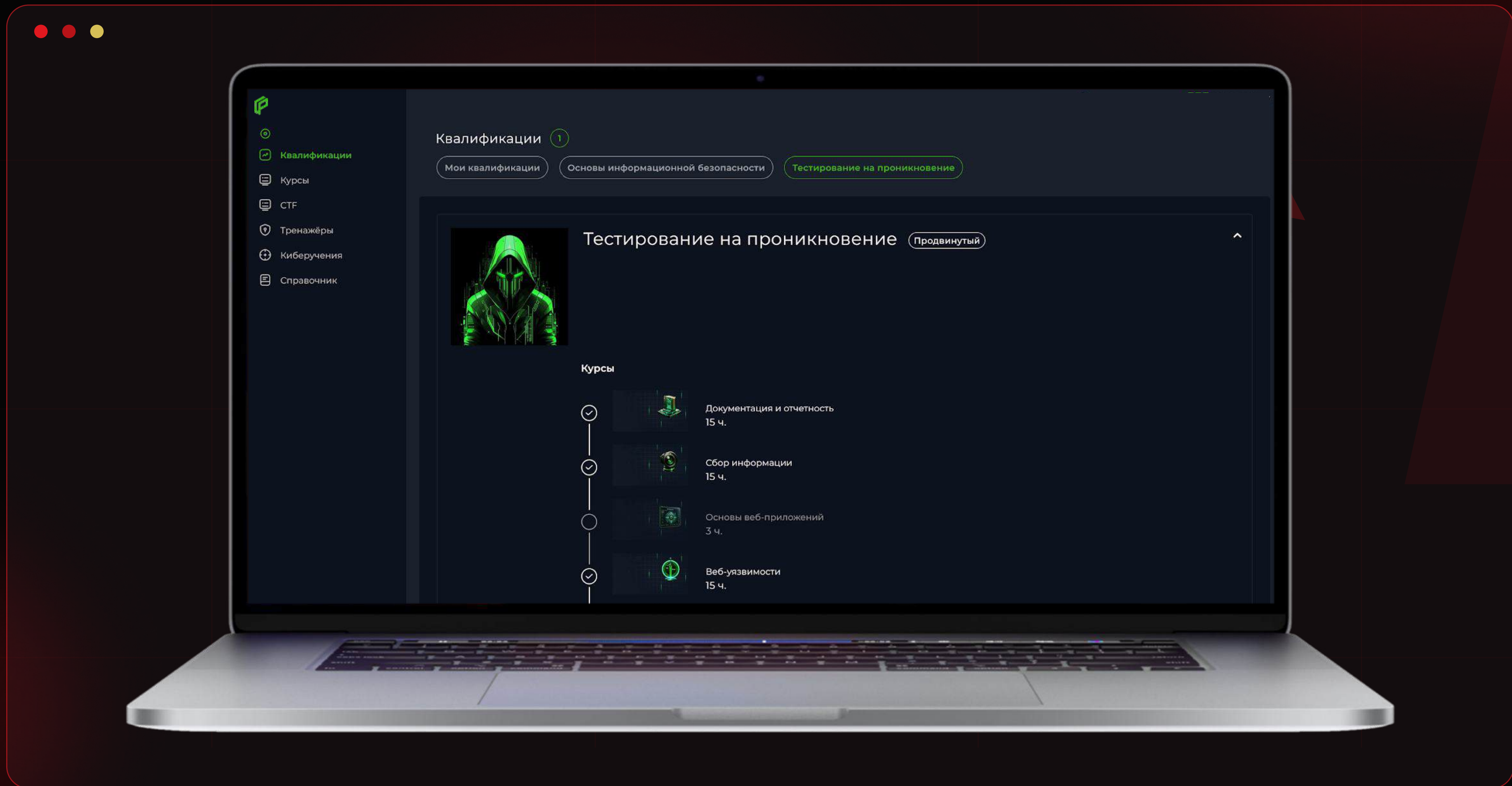


Обучающие курсы





Дорожные карты

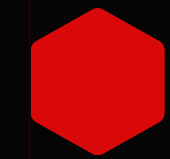




Интерактивные тренажеры и СТФ

Киберполигон предоставляет интерактивные тренажеры и СТФ-соревнования, которые позволяют отработать навыки и применить знания на практике в условиях, максимально приближенных к реальным

Тренажеры



дают возможность оттачивать различные техники защиты и атаки, чтобы затем применять полученные знания на практике

СТФ-соревнования

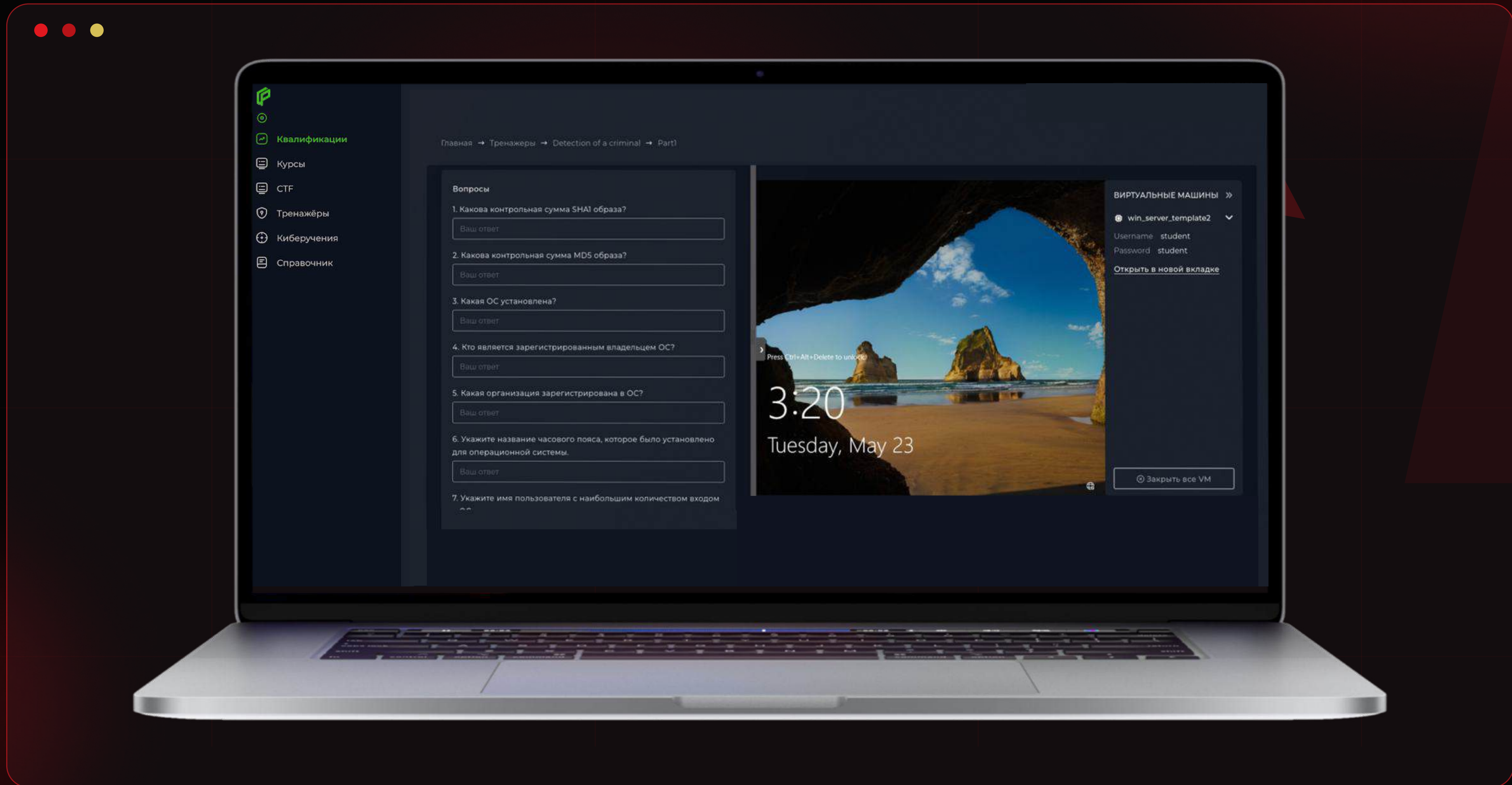


способствуют развитию навыков поиска уязвимостей, анализа данных и расследования инцидентов в конкурентной борьбе

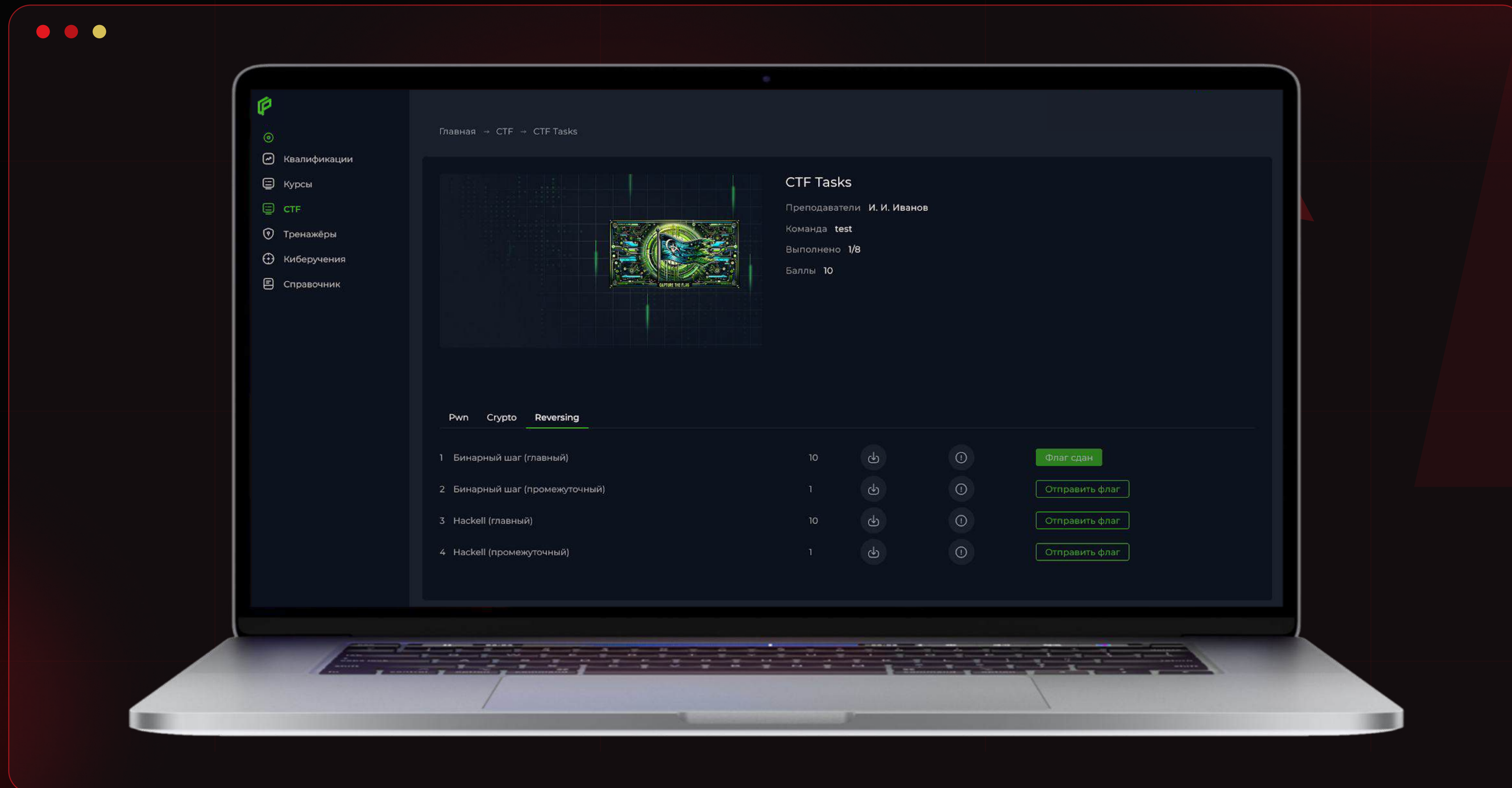
Эти инструменты доступны 24/7, что позволяет совершенствовать навыки и накапливать опыт в удобное время



Интерактивные тренажеры



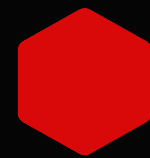
CTF





Киберучения на виртуальном городе «Neopolis»

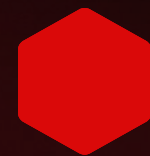
Neopolis — уникальная виртуальная среда, моделирующая инфраструктуру реального города для проведения киберучений. В этой среде специалисты могут отработать навыки как атакующих, так и защитников, участвуя в сценариях, приближённых к реальным инцидентам



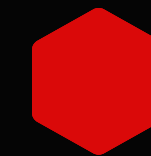
Киберучения — один из самых эффективных инструментов для проверки и подтверждения уровня подготовки ИБ-специалистов, дающий возможность оценить как теоретические, так и практические знания участников



Участники могут выбирать роль атакующих или защитников в зависимости от целей обучения, погружаясь в полноценные симуляции кибератак и реагирования



Возможность обучения навыкам тестирования на проникновение и киберзащиты на реальных виртуальных инфраструктурах организаций, где происходят инциденты различного уровня сложности, позволяя участникам изучить и отработать комплексные стратегии защиты



Neopolis помогает улучшить навыки реагирования на киберугрозы в условиях, максимально приближенных к реальной городской инфраструктуре, что позволяет подготовиться к возможным инцидентам в реальной жизни



Виртуальный 3D-город «Neopololis»

Neopololis — сердце киберучений



12 инфраструктур города Неополлис

- Нефтяная компания
- Кинотеатр
- Банк
- Энергетическая компания
- ТЭЦ
- Ж/д станция
- Спортивный стадион
- IT-консалтинг
- Маркетинговое агентство
- Аэропорт
- Медицинский центр
- Гостиница



Состав киберучений



12 инфраструктур виртуального города «Neopolis»



Сопровождение участников тренером киберучений



Набор встроенных СЗИ различных классов



Эмулируются инфраструктуры банка, предприятий нефтяной и энергетической промышленности, аэропорта, ТЭЦ и других предприятий



Анимация после каждой успешно реализованной атаки или успешно расследованного киберинцидента — геймификация киберучений



Обучение и практика на реальных сценариях, позволяющих специалистам улучшить свои навыки и получить опыт реагирования на актуальные угрозы



Моделирование конкретных кибератак и обучение их противодействию в составе команд — атакующих и защищающихся



58 различных сценариев недопустимых событий: от вывода денежных средств со счета компании до отключения блока управления ветрогенераторами



Предоставление отчетов и анализ результатов киберучений через удобный специализированный интерфейс



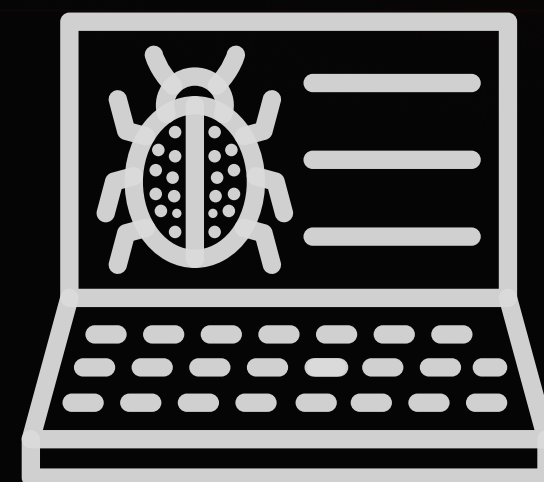
Пример атаки

Показана упрощенная последовательность шагов для совершения атаки в рамках киберучений

Взлом сайта компании



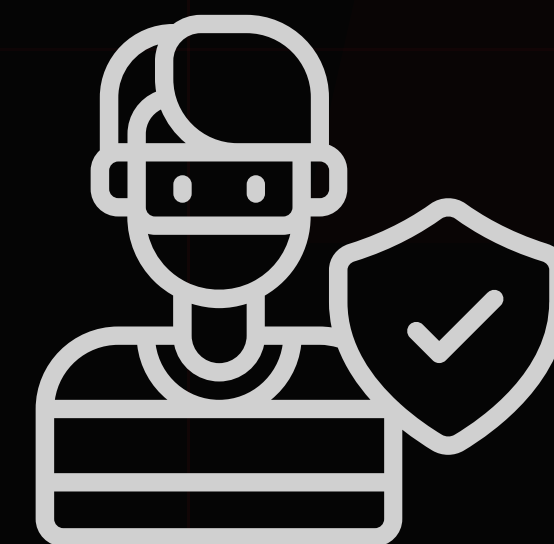
Внедрение сборщика паролей на сайт



Подключение к сетевой папке компании

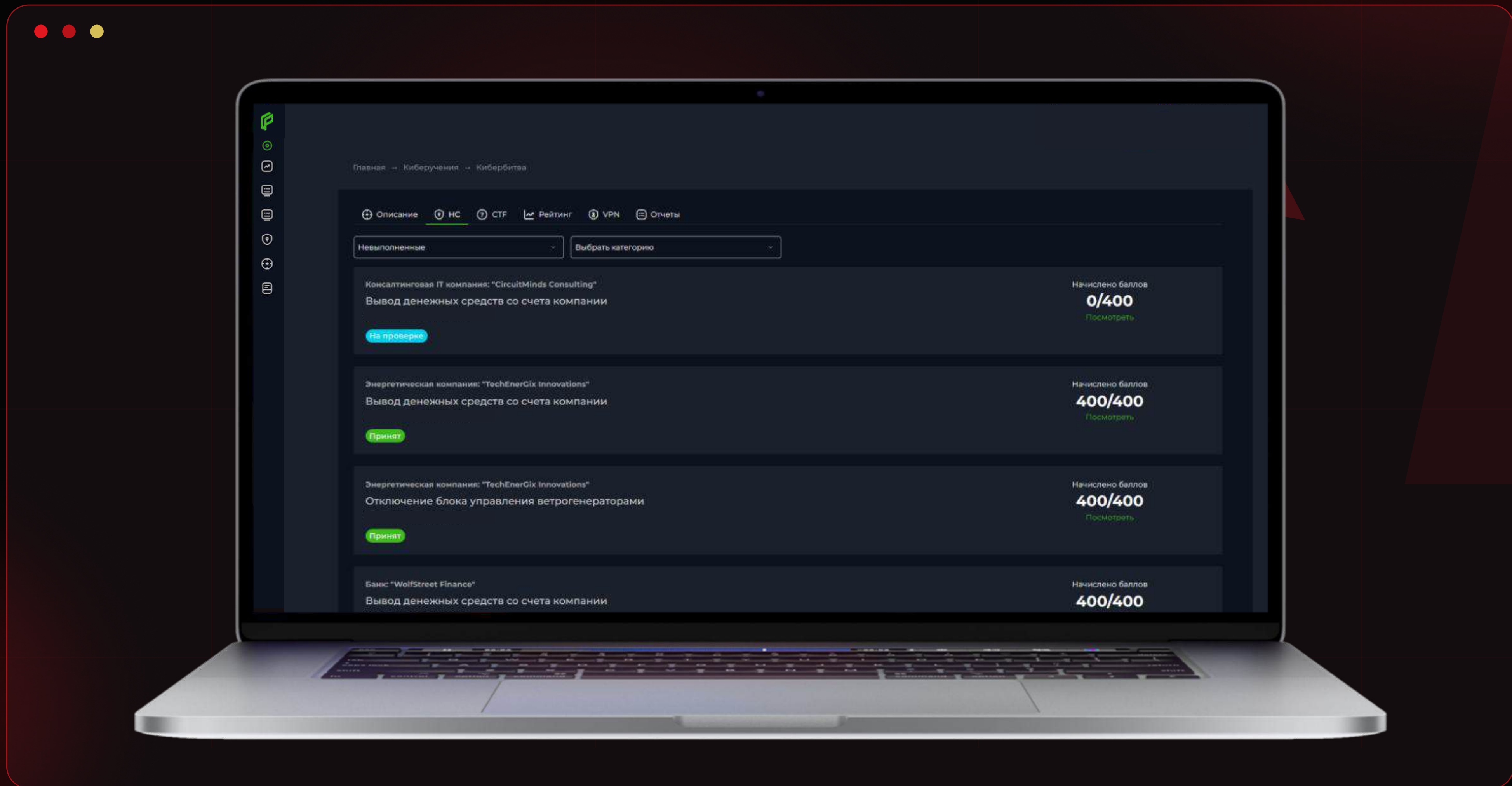


Кража конфиденциальных документов



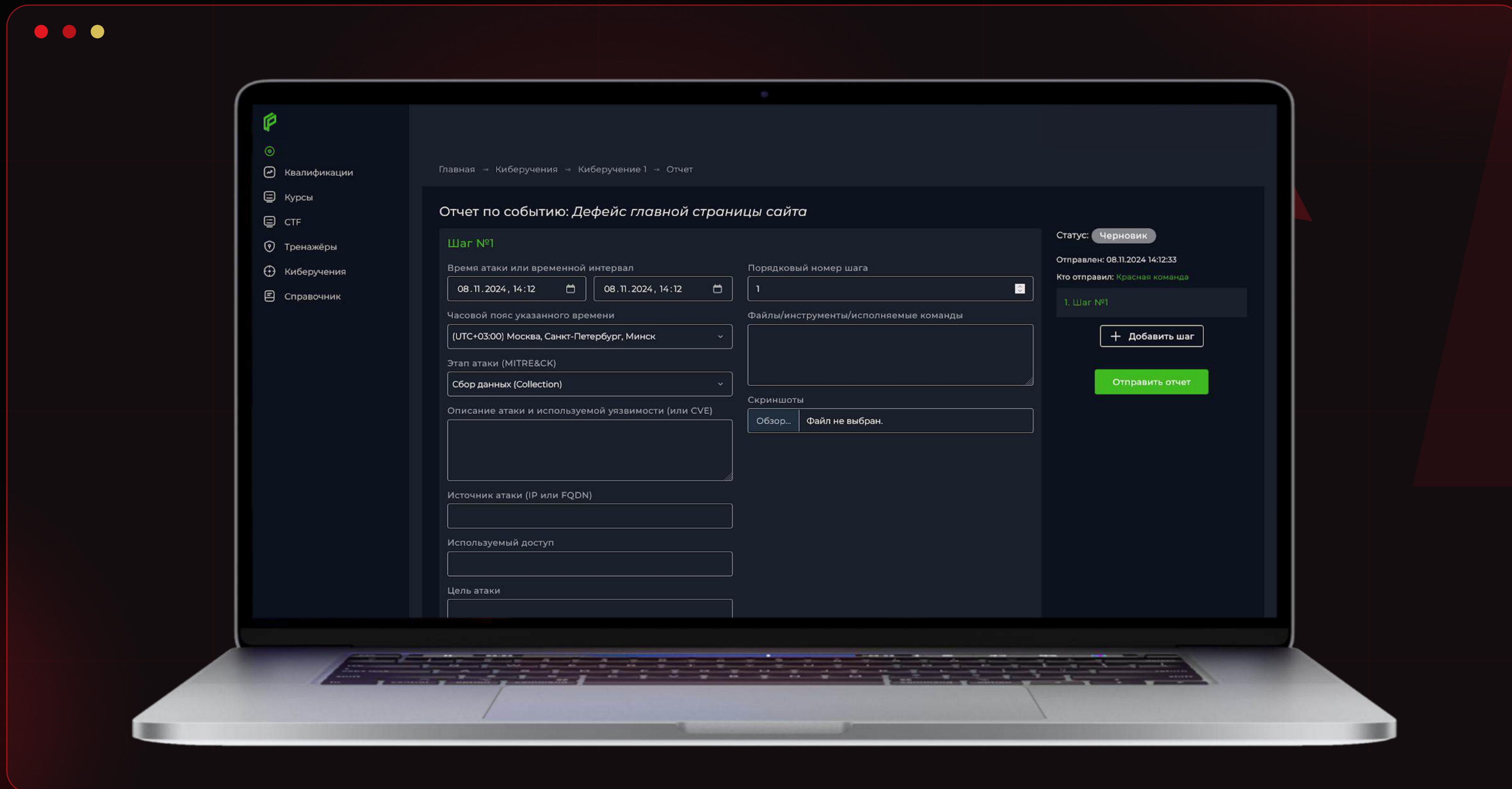


Киберучения на виртуальном городе «Neopolis»



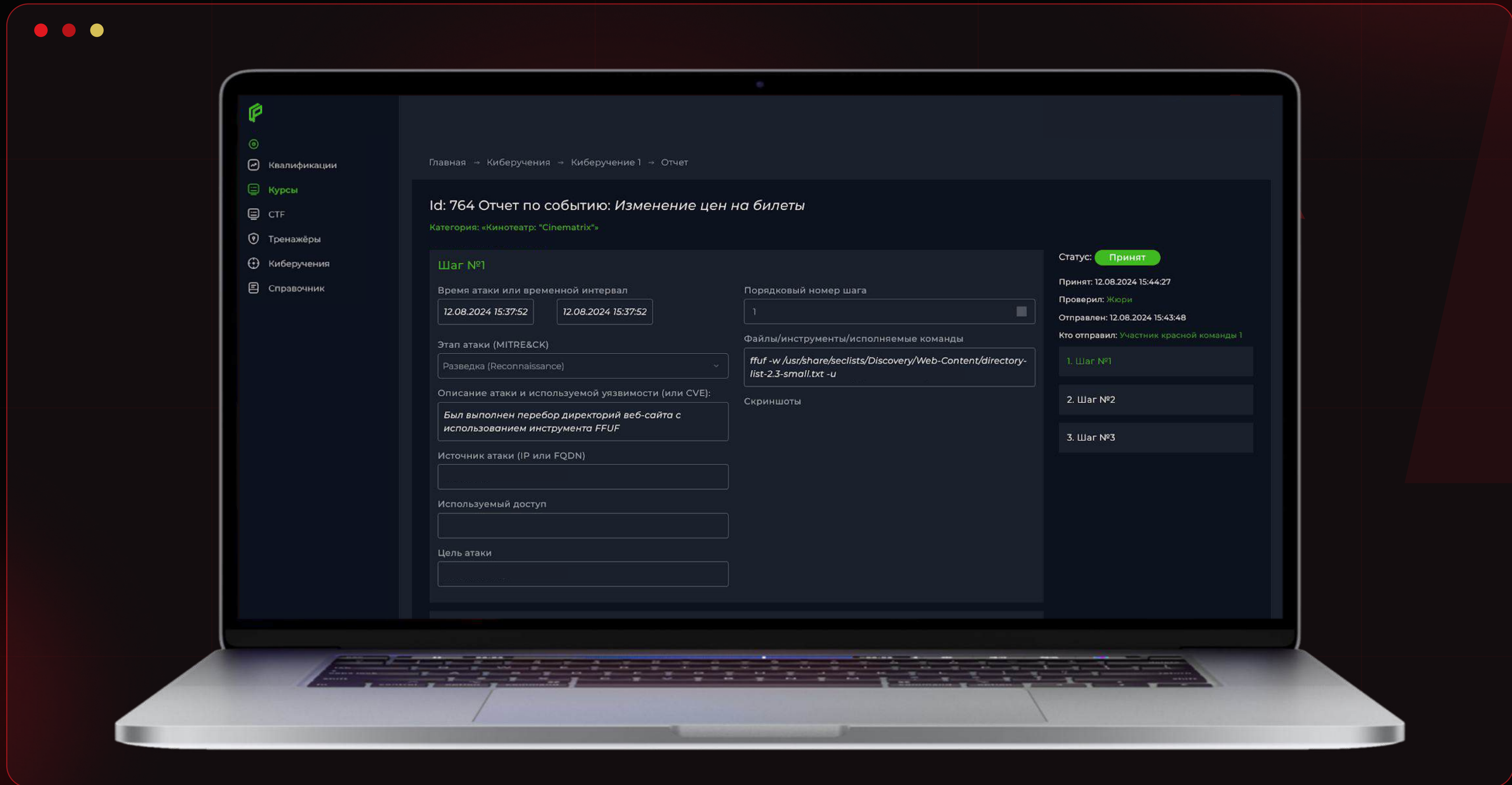


Киберучения на виртуальном городе «Neopolis»





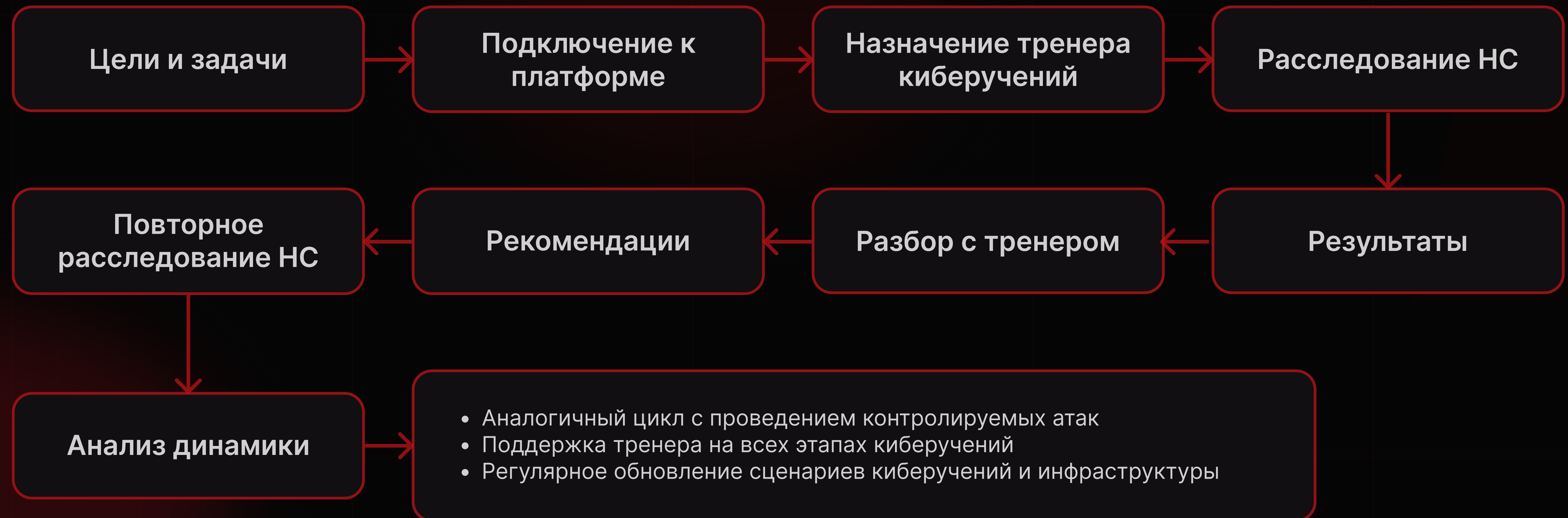
Киберучения на виртуальном городе «Neopololis»





Киберучения на виртуальном городе «Neopolis»

Погружение в виртуальные инфраструктуры, моделирующие реальные компании, позволяет участникам изучать и отрабатывать навыки тестирования на проникновение и защитные стратегии





Спасибо!

surte.by

vz@surte.by

+375 (29) 114 81 69