Научная статья
УДК 004.415.25; DOI: 10.61260/2218-130X-2025-4-117-130

ОБОСНОВАНИЕ НЕОБХОДИМОСТИ РАЗРАБОТКИ СИМУЛЯТОРА КИБЕРУГРОЗ ДЛЯ РЕШЕНИЯ ОБРАЗОВАТЕЛЬНЫХ ЗАДАЧ

Акапьев Виктор Львович;
Дунаев Роман Алексеевич;
Ковалева Екатерина Геннадьевна;
✉Борисенко Александр Васильевич.
Белгородский юридический институт МВД России им. И.Д. Путилина, г. Белгород, Россия
✉borisenko02.94@mail.ru

Аннотация. Нарастающая цифровизация всех отраслей человеческой деятельности актуализирует необходимость подготовки различных категорий пользователей от простого потребителя информации до специалиста в области кибербезопасности к решению задач обеспечения информационной безопасности. Как аналитики в сфере кибербезопасности используют в своей работе различные программные инструменты, так и в процессе подготовки специалистов применяются разнообразные программные продукты. В ходе исследования необходимо выбрать из всего разнообразия наиболее подходящие, с точки зрения образовательного процесса, средства, сформулировать требования к реализации диалогового режима и пользовательскому интерфейсу, а также предложить вариант программной реализации.

Ключевые слова: киберугрозы, учебный процесс, компетентность, симулятор киберугроз, геймификация, моделирование

Для цитирования: Обоснование необходимости разработки симулятора киберугроз для решения образовательных задач / В.Л. Акапьев [и др.] // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2025. № 4. С. 117–130. DOI: 10.61260/2218-130X-2025-4-117-130.

Scientific article

JUSTIFICATION OF THE NEED TO DEVELOP A CYBER THREAT SIMULATOR TO SOLVE EDUCATIONAL PROBLEMS

Akapyev Viktor L.;
Dunaev Roman A.;
Kovaleva Ekaterina G.;
✉Borisenko Alexander V.
Belgorod Law Institute of Ministry of the Interior of the Russian Federation named after I.D. Putilin, Belgorod, Russia
✉borisenko02.94@mail.ru

Abstract. The growing digitalization of all areas of human activity makes it necessary to train various categories of users, from ordinary information consumers to cybersecurity specialists, to solve the problems of information security. Just as cybersecurity analysts use various software tools in their work, various software products are used in the training of specialists. In the course of the study, it is necessary to select the most suitable tools for the educational process, formulate requirements for the implementation of a dialogue mode and a user interface, and propose a software implementation option.

Keywords: cyberthreats, educational process, competence, cyber threat simulator, gamification, modeling

For citation: Justification of the need to develop a cyber threat simulator to solve educational problems / V.L. Akapyev [et al.] // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2025. № 4. P. 117–130. DOI: 10.61260/2218-130X-2025-4-117-130.

Введение

Независимо от того, идет ли речь о специалистах по кибербезопасности, отвечающих за интернет-безопасность крупной компании, или об обычном пользователе, который хочет обеспечить сохранность своих персональных данных и мобильных устройств, использование подходящего программного обеспечения (ПО) для реализации кибербезопасности является важнейшей частью любой стратегии [1].

Учитывая растущую важность кибербезопасности, неудивительно, что существует бесчисленное множество программных решений и инструментов для обеспечения кибербезопасности, которые обещают защитить компании и частных лиц от множества возможных онлайн-угроз.

Некоторые инструменты кибербезопасности представляют собой комплексный пакет средств защиты от целого ряда уязвимостей и угроз, в то время как другие решения направлены на конкретные области, включая сетевую безопасность, защиту конечных устройств, анализ угроз, защиту брандмауэром, системы обнаружения вторжений, защиту от вредоносного ПО, управление уязвимостями, управление поверхностью внешних атак и многое другое [2].

Аналогичная ситуация сложилась и в системе подготовки сотрудников правоохранительных органов, на которых возлагаются задачи противодействия киберпреступлениям [3]. С точки зрения авторов, необходимо на основе анализа программных средств обучения сделать выбор наиболее оптимального решения и сформулировать требования по реализации взаимодействия обучающегося с программой, определить структуру пользовательского интерфейса и разработать архитектуру системы проекта симулятора.

Анализ

Кибератака, как вариант киберугрозы, – это вовсе не отдалённая перспектива, а сегодняшняя реальность, жертвой которой в каждый момент может стать любая организация или обычный гражданин, поэтому необходимы средства противодействия.

В настоящее время лидирующие позиции в сегменте ПО для отражения киберугроз занимают такие вендоры, как AttackIQ, Cronus Cyber Technologies, CyCognito, Cymulate, GuardiCore, Pcysys, Picus Security, SafeBreach, Sophos, Verodin, WhiteHaX, XM Cyber [4]. Некоторые из популярных программных средств кибербезопасности представлены в таблице.

Таблица

Программные средства отражения киберугроз

Наименование	Вид системы	Назначение
Quiz Lab ООО «Квиз Лаборатория» [5]	Симулятор отражения киберугроз (продукт был создан при финансовой поддержке Фонда содействия инновациям в рамках реализации Федерального проекта)	Комплексная платформа для развития критически важных навыков кибербезопасности предлагает уникальный опыт, который повышает уровень подготовки специалистов к реальным и постоянно меняющимся цифровым угрозам
Симулятор атак программ-вымогателей [6]	Интерактивный симулятор	В реальном времени принятие решений в отработке симмулятивных атак

Наименование	Вид системы	Назначение
Киберполигон Ampire [7]	Учебно-тренировочная платформа (комбинированная среда). Перспективный мониторинг	Иммерсивное моделирование (полное погружение), установление причин инциндента
Симулятор для реальной практики в расследовании кибератак Standoff Cyberbones [8]	Виртуализованная инфраструктура. Помогает специалистам по информационной безопасности (ИБ) практиковаться и нарабатывать опыт расследования инцидентов, используя данные реальных атак	Сценарии строятся на кейсах с кибербитв Standoff, проводимых компанией Positive Technologies
Kaspersky Interactive Protection Simulation [9]	Виртуальная платформа обучения навыкам кибербезопасности	Стратегическая бизнес-симуляция, командная игра, демонстрирующая, как кибербезопасность связана с эффективностью бизнеса
AVAREANGE [10]	Онлайн-платформа для комплексной оценки рисков и защиты от киберугроз	Программа помогает минимизировать вероятность успешных атак, обучая сотрудников распознавать угрозы и правильно реагировать на них
Cyber Range [11]	Система моделирования киберугроз	Служит эффективным инструментом для проведения тренировок, усовершенствования практических навыков и командного взаимодействия в условиях, приближенных к реальным кибератакам.
Интерактивный симулятор от «Лаборатории Касперского» [12]	Симулятор атаки программ-вымогателей, который поможет не только понять механизмы развития киберугроз, но и научиться эффективно противодействовать им с использованием современных EDR-инструментов	Ресурс предназначен для специалистов по ИБ и для всех, кто интересуется этой темой и хочет понять, как работают злоумышленники
CyberBattleSim [13]	Симулятор моделирует взлом системы с помощью искусственного интеллекта (ИИ). Программистам-защитникам нужно своевременно обнаружить проникновение, обезвредить противника или помешать его планам - напоминает соревнование Capture the Flag, только с противостоянием людей и компьютеров	Для тренировки специалистов по безопасности, чтобы они лучше понимали действия хакеров и могли быстро реагировать на любые угрозы
BreachLock [14]	Облачная платформа для тестирования на проникновение. Предлагает автоматизированное и ручное тестирование безопасности веб-приложений, сетей и API	Оценка уровня защиты. Обнаружение уязвимостей. Оценка готовности персонала. Оптимизация процессов безопасности

Наименование	Вид системы	Назначение
Foreseeti [14]	Инструмент для моделирования угроз и атак. Помогает организациям оценивать риски и совершенствовать стратегии безопасности с помощью графов атак	Моделирование угроз. Анализ путей атаки. Оценка рисков. Управление уязвимостями. Проверка средств контроля безопасности
Infection Monkey [15]	Инструмент для моделирования взломов и атак с открытым исходным кодом (BAS[1]). Проверяет устойчивость сети, имитируя боковое перемещение и методы постэксплуатации	Автоматизированное моделирование атак. Непрерывное тестирование безопасности. Виртуальная эксплуатация уязвимостей. Расстановка приоритетов на основе рисков. Мониторинг и отчётность в режиме реального времени
BAS AttackIQ [14]	Онлайн платформа. Постоянно проверяет средства контроля безопасности путем моделирования реальных киберугроз	Автоматическая проверка безопасности. Непрерывное тестирование безопасности. Моделирование сценариев угроз. Эмуляция атак
Picus [16]	Платформа для обеспечения кибербезопасности. Позволяет службам безопасности оценивать и укреплять свою защиту с помощью моделирования атак и предоставления рекомендаций по их предотвращению	Обеспечивает непрерывную проверку и тестирование безопасности. Позволяет в режиме реального времени отслеживать уязвимости в системе безопасности. Обеспечивает упреждающий поиск и обнаружение угроз
Cymulate [17]	Платформа для обеспечения кибербезопасности. Предлагает автоматизированное моделирование атак на электронную почту, конечные устройства, шлюзы и облачные среды для оценки веб эффективности мер безопасности	Оценка состояния безопасности. Непрерывное тестирование безопасности. Моделирование атак. Мониторинг в реальном времени и составление отчётов
Киберполигон MONT [18]	Виртуальная платформа, которая представляет собой типовую сетевую инфраструктуру с настроенными сервисами	Ресурс предназначен для тестирования решений в области кибербезопасности
Автоматизированный инструмент для «красной команды» и управления поверхностью атаки Randori [19]	Симулятор. Имитирует сложные атаки для выявления слабых мест	Обнаружение поверхности атаки. Непрерывная разведка. Выявление уязвимостей. Интеграция данных об угрозах
CALDERA [20]	Платформа с открытым исходным кодом для имитации атак Разработана MITRE, использует автоматизацию на основе ИИ для тестирования защитных возможностей	Автоматизированное моделирование действий противника. Создание сценариев атак. Возможности «красной команды». Интеграция данных об угрозах

[1] BAS (Breach and Attack Simulation) в контексте кибербезопасности – система для симуляции реальных кибератак в защищённой среде.

Наименование	Вид системы	Назначение
Симулятор сетевой безопасности NeSSi2 [14]	Инструмент для моделирования сетевой безопасности, предназначенный для исследований и тестирования, с упором на обнаружение сетевых вторжений и оценку реагирования на них	Поддерживает моделирование и симуляцию сложных сетевых сценариев. Позволяет оценивать меры и протоколы сетевой безопасности. Предоставляет графический пользовательский интерфейс для простой настройки и визуализации
Автоматизированный стимулятор атак XM Cyber [21]	Гибридная платформа BAS и управления путями атак, которая непрерывно моделирует пути атак для выявления уязвимостей в системе безопасности	Непрерывное тестирование безопасности. Виртуальная эксплуатация уязвимостей. Расстановка приоритетов на основе рисков
Система распознавания кибератак PRISM [22]	Иерархическая архитектура обнаружения вторжений для крупномасштабных киберсетей	Тестовая фишинговая проверка, распознание кибератак
Фишинг СберКибер [3]	Модуль сценариев	Тестовая фишинговая проверка

Как можно убедиться, инструменты для моделирования киберугроз представлены в широком ассортименте на рынке ПО, но, как правило, они предлагают пошаговые инструкции по устранению уязвимостей после их обнаружения. Эти проблемы оцениваются обучающимися с точки зрения критического риска, что позволяет обучать их способам устранения наиболее актуальных угроз.

Указанные инструменты варьируются от платформ для моделирования BAS до фреймворков для эмуляции действий злоумышленников. Они выявляют уязвимости и противодействуют методам, которые используют злоумышленники, с распределением ролей участников и использованием элементов геймификации. По сути, это новый тип инструмента, который может решать и образовательные задачи.

Платформы для управления путями атак – это один из примеров ПО для моделирования угроз. Эти платформы непрерывно моделируют атаки на среду организации, выявляя уязвимости, которые могут быть использованы злоумышленниками, показывая, как эти уязвимости могут быть использованы, а затем помещая эти угрозы в более широкий контекст рисков. В отличие от обычных сканеров уязвимостей, которые в первую очередь ориентируются на степень серьезности уязвимостей, эти инструменты могут помещать угрозы в контекст рисков для критически важных активов [23].

Программные платформы для моделирования угроз играют решающую роль в системах симуляции, предлагая структурированный подход к выявлению и устранению потенциальных угроз, но отличаются сложностью реализации, и их применение в образовательном процессе связано с дополнительными финансовыми затратами.

Нетрудно заметить, что большинство представленных продуктов представляют собой средства моделирования кибератак или, другими словами, симуляторы.

Моделирование кибератак помогает организациям выявлять уязвимости, тестировать средства защиты и повышать уровень кибербезопасности, имитируя реальные атаки. Поэтому имитация кибератаки представляет собой не только метод тестирования компьютерной безопасности, но и эффективное средство подготовки сотрудников правоохранительных органов в безопасных условиях.

Моделирование киберугроз – один из наиболее эффективных способов решения этой задачи. С помощью ПО для моделирования угроз в процессе подготовки специалистов можно спрогнозировать возможные атаки злоумышленников и выявить слабые места в системе безопасности защищаемых объектов.

Автоматизированное моделирование угроз позволило внедрить более быстрый, менее затратный и непрерывный метод достижения той же цели. По этой причине оно может стать основным инструментом для образовательных организаций, стремящихся эффективно готовить специалистов, способных управлять угрозами и уязвимостями в условиях обычных ограничений ресурсов, с которыми сталкиваются правоохранительные органы.

В ситуации, сложившейся с уходом большинства зарубежных вендоров с российского рынка, проблемы ИБ и обслуживания инфраструктуры стали первоочередными для любого бизнеса. К наиболее критичным проявлениям стоит отнести отключение или дезактивацию ИБ-функционала оборудования и решений. Снижению уровня кибербезопасности способствует отсутствие доступа к обновлениям, комьюнити и документации, невозможность замены оборудования, разрыв сервисных контрактов на сопровождение поставленных решений и контакта с техническими специалистами. При этом аналитики отметили кратно нарастающее количество кибератак. Объективная оценка степени защищенности объектов и повышение качества профессиональной подготовки специалистов в области кибербезопасности в таких условиях становятся приоритетными [24].

На основании проведенного анализа с учетом условий специальной военной операции, резкой деградации рынка ПО и очередной декларированной необходимости перехода на отечественный soft можно сформулировать выводы о том, что наиболее оптимальным решением задачи обеспечения образовательного процесса является разработка программного симулятора с элементами геймофикации в решении учебных задач.

Геймификация в пользовательском интерфейсе симулятора

Современным курсантам и слушателям, а также специалистам в области кибербезопасности, проходящим повышение квалификации или профессиональную переподготовку, инновационные подходы к обучению, так как традиционные образовательные технологии иногда не могут привлечь и удержать внимание аудитории, поэтому объединение геймификации и симуляции открывает новые возможности в профессиональной обучении [25].

Геймификация, используя игровые механики, может значительно улучшить вовлеченность – игровые элементы стимулируют внутреннюю мотивацию, побуждая обучающихся участвовать в решении задач, которые демонстрируют их компетентность. Благодаря активному процессу обучения, геймификация способствует более глубокому пониманию концепций за счёт повторения и мгновенной обратной связи. Кроме того, геймификация создает динамичную и увлекательную среду для обучения, в которой поощряется здоровая конкуренция и сотрудничество.

Открывается возможность использования стандарта обмена данными между учебным контентом и системой обучения (xAPI) для отслеживания прогресса, а не только для оценки количества выполненных задач. Эти данные позволяют получить более глубокое представление о вовлечённости обучающихся, сохранении знаний и общей компетентности – гораздо более глубокое, чем традиционные показатели успешности/неуспешности.

Мотивационный потенциал геймификации для обучающихся можно рассмотреть на примере командных игр, когда десятки участников в ужасных погодных условиях собрались выяснить, кто из них сильнее. Такой подход доступен практически каждому благодаря своей простоте, во-вторых, в его основе лежит мощный мотиватор – желание победить. Уберите эту цель, и игра мгновенно потеряет смысл. Футбол, регби, хоккей, бейсбол и любые другие соревновательные виды спорта привлекают массу поклонников благодаря духу соперничества.

Если применить этот «мотивирующий фактор» к обучению, в результате получится геймификация, которая дает ряд преимуществ как для образовательных организации, так и для участвующих в ней обучающихся:

1. Поощряет активное обучение.

Активизация участия обучающихся в процессе обучения на основе геймификация электронного обучения осуществляется за счет предоставления им широких возможностей для взаимодействия с цифровыми образовательными ресурсами (ЦОР).

В самых увлекательных играх быстро проявляются последствия действий субъектов образовательного процесса: обучающийся делает ход и вскоре понимает, был ли он удачным или в следующий раз нужно действовать по-другому. Способы реализации цикла обратной связи ограничены только воображением и профессионализмом разработчика ЦОР (и тем, что нужно усвоить аудитории), но принцип вовлечения один и тот же. В этом могут помочь всесторонняя обратная связь и значки уроков Elucidat [26].

2. Способствует непрерывному обучению.

Соревновательный элемент геймификации может побуждать пользователей улучшать свои результаты или переходить на следующий уровень, что способствует непрерывному обучению. Пользователи также с большей вероятностью вернутся к модулю, если почувствуют, что могут набрать больше баллов, а значит, с большей вероятностью запомнят информацию благодаря повторению.

3. Повышает продуктивность.

Внедрение игровых элементов в ведомственное электронное обучение может помочь сотрудникам дольше сохранять вовлечённость, а значит, они будут усваивать больше контента за меньшее время. Вместо того, чтобы тратить полчаса на просмотр обучающего видео, учащиеся могут, например, пройти три десятиминутных теста. Исследование показало, что 89 % респондентов были бы более продуктивными, если бы их работа была геймифицированной, а уровень удовлетворённости работой повысился бы [27].

4. Делает процесс обучения более приятным.

Геймификация не только помогает сотрудникам сохранять вовлечённость в течение более длительного времени, но и делает процесс обучения более приятным. Благодаря этому цифровое обучение становится не рутиной, а чем-то, что пользователям нравится.

Люди любят игры, но необходимо помнить, что геймификация – это не просто развлечение. Вместо этого она мотивирует людей вовлекаться и активно участвовать в обучении, чтобы изменить их поведение.

Геймификация также открывает перед людьми мир, наполненный воображением, который игровые элементы могут привнести в процесс обучения. При правильном использовании воображение может увлечь в бесконечное путешествие открытий и возможностей внедрения игровых элементов в корпоративные программы обучения [28].

5. Поскольку геймификация повышает вовлечённость, осознанность и продуктивность учащихся, она также улучшает показатели образовательной организации.

6. Персонализация опыта.

Лучшие игры позволяют участникам делать выбор, который влияет на результат. Например, если дать учащемуся возможность управлять игровым процессом с помощью разветвлённых сценариев, это может стать эффективным способом повысить вовлечённость [27].

Авторы отмечают, что большинство рассмотренных платформ, представленных в таблице, делают упор на реалистичное моделирование инфраструктуры, при этом в одних случаях элементы геймификациии выражены явно, в других подразумеваются за счет сценария.

Обоснование разработки и схема реализации

Выбор в пользу виртуального симулятора обусловлен большей гибкостью под программу обучения в условиях отсутствия реальных стендов безопасности, их дороговизны. Использование модели позволяет усилить практическую составляющую обучения с возможностью практиковаться в любое время.

Методология разработки включает в себя анализ существующих на рынке инструментов для обучения кибербезопасности; разработка масштабируемых сценариев с элементами геймификации и последующая программная реализация симулятора с использованием технологий (HTML/CSS/JavaScript).

Общая концепция разрабатываемого виртуального симулятора киберугроз заключается в создании интерактивной среды, в которой пользователь (обучающийся) обучается распознаванию, анализу и реагированию на смоделированные киберинциденты. Разрабатываемый симулятор киберугроз будет иметь модульную веб-архитектуру «клиент-сервер» (база данных MongoDB). Уровни архитектуры представлены на рис. 1:

Рис. 1. **Схема архитектуры системы проекта симулятора**

На уровне базы данных осуществляется постоянное хранение данных и связей. База данных является основой логики разрабатываемого симулятора и учета прогресса обучения. База данных будет реализована с использованием MongoDB, которая была выбрана из-за достаточной гибкости в моделировании динамических объектов (комнаты, предметы и сценарии).

Основные сущности баз данных и их назначение.

Пользователи «users» представлены администратором, преподавателями и обучающимися. Хранят Идентификатор пользователя User_id, роли и информацию о прогрессе. Каждый пользователь будет связан с несколькими сценариями через систему отслеживания прогресса.

Таблица «Progress»:

Комнаты («rooms» – основные сцены) представляют виртуальное пространство с интерактивными элементами, такими как компьютерная и оргтехника, коммуникационное оборудование. Комнаты содержат коллекции всех объектов согласно сценарию.

Объекты («objects») представлены интерактивными компонентами. Каждый объект представляет определенный предмет и область, на которую можно нажать. Объекты будут напрямую связаны с задачами или диалогами (подсказками), которые при активации запускают действия.

Сценарии («scenarios») представлены структурированными последовательностями заданий (сюжетных линий). Каждый сценарий будет содержать задания согласно уровню сложности и указывает комнату, в которой они выполняются.

Задачи («tasks») – это отдельные задачи в процессе обучения или действия пользователя в рамках сценария. Задачи определяю инструкции, ожидаемые действия, логику проверки и баллы. Каждая задача относится к одному сценарию и может вызвать обратную связь после выполнения. Пример задачи: проанализировать файл журнала, изолирование компьютера и т.п.

Диалоги («dialog») представлены текстовыми подсказками, отображаемыми для пользователя во время взаимодействия с объектами. Могут содержать пояснения, рекомендации и информацию по развитию сюжета (при необходимости).

Прогресс обучения («progress») отслеживает состояние каждого пользователя, выполняющего сценарий. Тут фиксируется, какие задачи выполнены, на каком этапе находится обучающийся, накопление балов, статус – «в процессе» либо «завершено».

Сложность «difficultlavel» – дополнительная таблица, определяющая доступные уровни сложности level_id.

Логика базы данных и связи между элементами. Пользователи «Users» подключаются к «Progress» базы данных, связывая историю обучения с данными симулятора. Комнаты содержат все объекты (перечень объектов для комнат описан сценарием), которые запускают учебные задачи «Tasks». Сценарии «scenarios» ссылаются на комнаты и задания для создания пути выполнения сценария. Диалоги «dialog» привязаны к объектам «object» для реализации интерактивности. Ориентир для сценария на этапе входа – уровень сложности «difficultlavel».

Обозначен типичный для работы порядок действий – общая схема взаимодействие с базой данных (рис. 2).

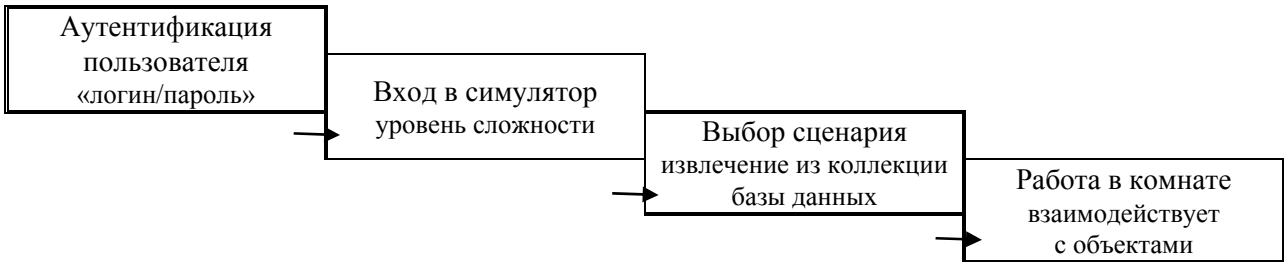

Рис. 2. **Схема порядка действия пользователя в цикле выполнения задачи**

Интерфейс симулятора состоит из нескольких интерактивных «комнат» (возможно масштабирование на перспективу), визуально и функционально напоминающих реальные офисные помещения. В каждой комнате расположены ключевые объекты (интерактивные объекты взаимодействия).

Элементы расположены в соответствии с принципами композиции и логикой учебного модуля. В проекте дизайна закладывалась концепция с учетом использования корпоративных цветов, а организация пространства подразумевала расположение обязательных внутренних объектов, среди которых – компьютерная и офисная техника, элементы коммуникаций.

На рис. 3 приведен пример композиции пространства для комнаты «Источники и каналы утечки информации» с размещенными объектами.

Концепция реализации сценария. Каждый сценарий в симуляторе представляет собой решение практических ситуаций в сфере кибербезопасности. В наборе имеются следующие комнаты: комната «Общие вопросы обеспечения кибербезопасности», комната «Принципы обеспечения компьютерной безопасности», комната «Источники и каналы утечки информации», комната «Реагирование на инциденты кибербезопасности и их обработка». Например, в комнате общих вопросов обеспечения кибербезопасности одна из ситуаций связана с обнаружением несанкционированного доступа к локальной сети, где необходимо последовательно выполнить действия – посмотреть журнал, изолировать компьютер, провести мероприятия, направленные на защиту данных. Диалоги связаны с инструктажем по порядку выполнения в случае сложностей. Прописаны критерии завершения (время, точность, итоговая оценка).

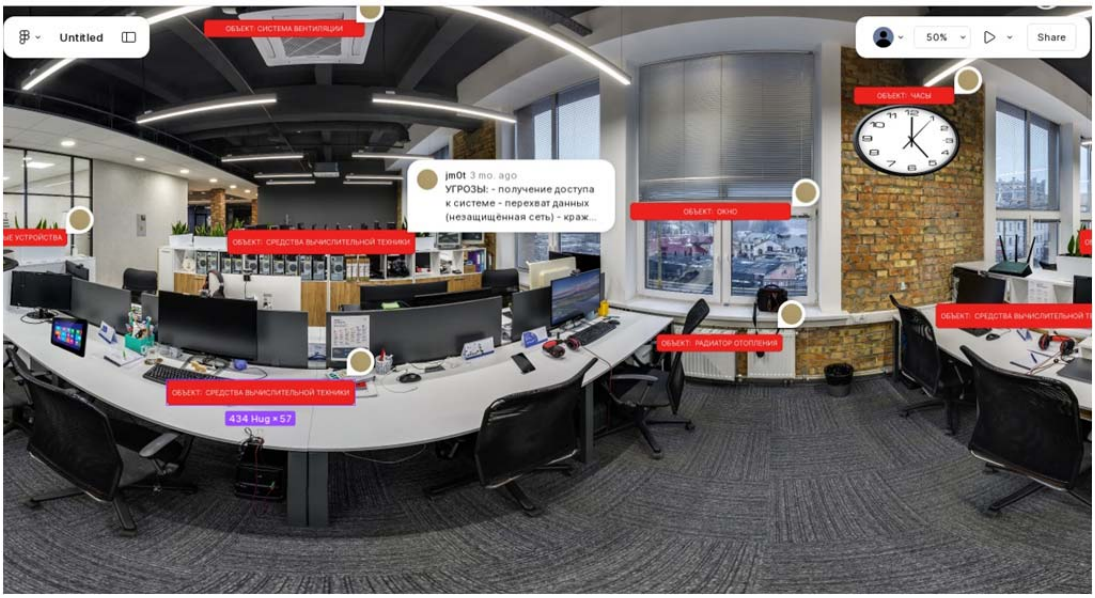

Рис. 3. **Общий вид комнаты «Каналы утечки информации»**

Далее рассмотрен подробнее дизайн и функциональность разработанного пользовательского модуля симулятора киберугроз.

В используемом в проекте контенте сделан упор на соответствие дидактических единиц учебной программы дисциплины с объектами взаимодействия и учетом принципов эффективного удаленного обучения, а именно: доступность, персонализация, практика и обратная связь. Каждый сценарий построен на основе конкретных учебных целей и соответствует профессиональному стандарту.

Обучающийся перемещается по комнатам, областям помещений, взаимодействуя с внутренними объектами. Для каждой «комнаты» разработан отдельный сценарий, включающий диалоги, расположение необходимых объектов, в том числе и мебели. В определенной комнате решается определенная практическая задача. Выполняя задания, участник симулятора направляется по различным путям решения практических задач (возможный вариант, когда решение определенного количество задач открывает дополнительную ветку сценария, таким образом добавляя уровень сложности). В помещениях выбор объекта осуществляется при помощи кликабельных точек – областей изображения.

Сценарий построен на модели линейного квеста с взаимосвязанными задачами, то есть некоторые задания практикума связаны между собой, часть из которых необходимо выполнить по строгому алгоритму для перехода к следующему. Например, в одном случае необходимо идентифицировать сами угрозы (выявление признаков заражения системы, обозначение канала утечки информации и пр.), в другом – выполнить последовательность действий на компьютере: (без пароля/ с паролем) осуществить вход в систему и получить доступ к папке жесткого диска; провести настройку брандмауэра операционной системы; взаимодействие с дисками хранения информации (анализ); отработка электронного фишингового сообщения и пр.

При проектировании закладываются следующие приоритеты:

– масштабируемость, которая позволяет добавлять «комнаты» в проект;

– гибкость, обозначающая возможность повторного использования объектов в различных сценариях по сложности;

– производительность (распределение ресурсов и данных);

– возможность интеграции с LMS.

Заключение

Инструменты для моделирования киберугроз представлены в широком ассортименте на рынке ПО, но, как правило, они предлагают пошаговые инструкции по устранению уязвимостей после их обнаружения. Эти проблемы оцениваются обучающимися с точки зрения критического риска, что позволяет обучать их способам устранения наиболее актуальных угроз. Выбор в пользу собственной разработки виртуального симулятора обусловлен большей гибкостью под программу обучения в условиях отсутствия реальных стендов безопасности, их дороговизны.

Результатом исследования является полностью сформированная логическая структура, готовая к программной реализации. Использование данной модели позволяет усилить практическую составляющую подготовки, а интеграция геймификации – элементы игрового дизайна (очки, таблица лидеров, значки) в неигровых контекстах с целью повышения вовлеченности и мотивации – превращают выполнение заданий в соревнование (игру), привычную для данной категории обучающихся.

Список источников

1. Cybersecurity Tools. URL: https://brainstation.io/career-guides/what-tools-do-cybersecurity-analysts-use (дата обращения: 06.10.2025).

2. MONT открыла киберполигон для тестирования решений по информационной безопасности. URL: https://www.mont.ru/ru-ru/news/6312 (дата обращения: 05.10.2025).

3. Фишинг – тебе пишут мошенники. URL: https://www.sberbank.ru/promo/scs-school/courseid-2.html (дата обращения: 15.10.2025).

4. Обзор мирового и российского рынков средств симуляции кибератак (Breach and Attack Simulation, BAS). URL: https://www.anti-malware.ru/analytics/Market_Analysis/Breach-and-Attack-Simulation-Market-Overview (дата обращения: 01.10.2025).

5. Вовлекающее обучение для суперкоманд. URL: https://quizlab.pro/ (дата обращения: 05.10.2025).

6. Интерактивный симулятор атаки программ-вымогателей TADVISER. URL: https://www.tadviser.ru/index.php (дата обращения: 03.10.2025).

7. Киберполигон Ampire. URL: https://softline.ru/solutions/security/kiberpoligon-ampire (дата обращения: 23.08.2025).

8. Standoff Cyberbones: симулятор для реальной практики в расследовании кибератак. URL: https://www.securitylab.ru/analytics/557408.php (дата обращения: 29.08.2025).

9. Kaspersky Interactive Protection Simulation (KIPS). URL: https://www.robotx.ru/programmnoe-obespechenie/informatsionnaya--bezopasnost/platforma-obuchenie-kiberbezopasnosti/Kaspersky-Interactive-Protection-Simulation-KIPS/ (дата обращения: 17.10.2025).

10. Как сделать из ваших сотрудников первую линию киберзащиты всего за 2 недели? URL: https://avareange.ru/ (дата обращения: 11.10.2025).

11. Validate Your Cybersecurity Posture and Resilience. URL: https://cyberranges.com/ (дата обращения: 01.10.2025).

12. Интерактивный симулятор от «Лаборатории Касперского» – новый подход к обучению защите от киберугроз. URL: https://gk-ur.ru/info/news/interaktivnyy-simulyator-ot-laboratorii-kasperskogo-novyy-podkhod-k-obucheniyu-zashchite-ot-kiberugr/ (дата обращения: 05.10.2025).

13. Microsoft представила симулятор кибератак с машинным обучением. URL: https://habr.com/ru/news/551558/ (дата обращения: 09.10.2025).

14. Top 10 Best Cyber Attack Simulation Tools – 2025. URL: https://cybersecuritynews.com/cyber-attack-simulation-tools/ (дата обращения: 02.10.2025).

15. Infection Monkey: Test and validate your defenses with Infection Monkey, our free open-source malware vaccine. URL: https://www.akamai.com/infectionmonkey (дата обращения: 11.10.2025).

16. Attack Surfaces Expanding Faster Than Teams Can Manage. URL: https://www.picussecurity.com/ (дата обращения: 01.10.2025).

17. Cymulate – Exposure Management Platform Built for Real Risk. URL: https://cymulate.com/ (дата обращения: 01.08.2025).

18. MONT открыла киберполигон. URL: https://www.mont.ru/ru-ru/news/6312 (дата обращения: 13.10.2025).

19. 10 инструментов моделирования кибератак для повышения безопасности. URL: https://dzen.ru/a/ZG89c5dzB3yyeIzP (дата обращения: 19.10.2025).

20. Get Involved https. URL: //caldera.mitre.org/ (дата обращения: 18.10.2025).

21. High-Risk Exposures Faster. URL: https://xmcyber.com/ (дата обращения: 01.10.2025).

22. PRISM: A Hierarchical Intrusion Detection Architecture for Large-Scale Cyber Networks. URL: https://deepai.org/publication/prism-a-hierarchical-intrusion-detection-architecture-for-large-scale-cyber-networks (дата обращения: 11.09.2025).

23. What is Threat Simulation? URL: https://xmcyber.com/glossary/what-is-threat-simulation/ (дата общения: 04.10.2025).

24. Реальная атака защищает. Симуляция кибератак с помощью BAS-решений. URL: https://www.cti.ru/media/publications/realnaya-ataka-zashchishchaet-simulyatsiya-kiberatak-s-pomoshchyu-bas-resheniy/ (дата обращения: 01.10.2025).

25. Gamification And Simulations: Powering Up Training And Productivity. URL: https://elearningindustry.com/gamification-and-simulations-powering-up-training-and-productivity (дата обращения 18.10.2025).

26. Kirstie Greany Why gamification in elearning is important. URL: https://www.elucidat.com/blog/why-gamification-in-elearning-is-important/ (дата обращения: 19.10.2025).

27. Акапьев В.Л., Савотченко С.Е. Геймификация в электронном образовании // Вестник Воронежского государственного университета. Сер.: Проблемы высшего образования. 2025. № 3. С. 19–23.

28. The Top 5 Benefits of Gamification in Learning. URL: https://www.learnlight.com/en/articles/5-benefits-of-gamification-in-learning/ (дата обращения: 01.10.2025).

References

1. Cybersecurity Tools. URL: https://brainstation.io/career-guides/what-tools-do-cybersecurity-analysts-use (data obrashcheniya: 06.10.2025).

2. MONT otkryla kiberpoligon dlya testirovaniya reshenij po informacionnoj bezopasnosti. URL: https://www.mont.ru/ru-ru/news/6312 (data obrashcheniya: 05.10.2025).

3. Fishing – tebe pishut moshenniki. URL: https://www.sberbank.ru/promo/scs-school/courseid-2.html (data obrashcheniya: 15.10.2025).

4. Obzor mirovogo i rossijskogo rynkov sredstv simulyacii kiberatak (Breach and Attack Simulation, BAS). URL: https://www.anti-malware.ru/analytics/Market_Analysis/Breach-and-Attack-Simulation-Market-Overview (data obrashcheniya: 01.10.2025).

5. Vovlekayushchee obuchenie dlya superkomand. URL: https://quizlab.pro/ (data obrashcheniya: 05.10.2025).

6. Interaktivnyj simulyator ataki programm-vymogatelej TADVISER. URL: https://www.tadviser.ru/index.php (data obrashcheniya: 03.10.2025).

7. Kiberpoligon Ampire. URL: https://softline.ru/solutions/security/kiberpoligon-ampire (data obrashcheniya: 23.08.2025).

8. Standoff Cyberbones: simulyator dlya real'noj praktiki v rassledovanii kiberatak. URL: https://www.securitylab.ru/analytics/557408.php (data obrashcheniya: 29.08.2025).

9. Kaspersky Interactive Protection Simulation (KIPS). URL: https://www.robotx.ru/programmnoe-obespechenie/informatsionnaya--bezopasnost/platforma-obuchenie-kiberbezopasnosti/Kaspersky-Interactive-Protection-Simulation-KIPS/ (data obrashcheniya: 17.10.2025).

10. Kak sdelat' iz vashih sotrudnikov pervuyu liniyu kiberzashchity vsego za 2 nedeli? URL: https://avareange.ru/ (data obrashcheniya: 11.10.2025).

11. Validate Your Cybersecurity Posture and Resilience. URL: https://cyberranges.com/ (data obrashcheniya: 01.10.2025).

12. Interaktivnyj simulyator ot «Laboratorii Kasperskogo» – novyj podhod k obucheniyu zashchite ot kiberugroz. URL: https://gk-ur.ru/info/news/interaktivnyy-simulyator-ot-laboratorii-kasperskogo-novyy-podkhod-k-obucheniyu-zashchite-ot-kiberugr/ (data obrashcheniya: 05.10.2025).

13. Microsoft predstavila simulyator kiberatak s mashinnym obucheniem. URL: https://habr.com/ru/news/551558/ (data obrashcheniya: 09.10.2025).

14. Top 10 Best Cyber Attack Simulation Tools – 2025. URL: https://cybersecuritynews.com/cyber-attack-simulation-tools/ (data obrashcheniya: 02.10.2025).

15. Infection Monkey: Test and validate your defenses with Infection Monkey, our free open-source malware vaccine. URL: https://www.akamai.com/infectionmonkey (data obrashcheniya: 11.10.2025).

16. Attack Surfaces Expanding Faster Than Teams Can Manage. URL: https://www.picussecurity.com/ (data obrashcheniya: 01.10.2025).

17. Cymulate – Exposure Management Platform Built for Real Risk. URL: https://cymulate.com/ (data obrashcheniya: 01.08.2025).

18. MONT otkryla kiberpoligon. URL: https://www.mont.ru/ru-ru/news/6312 (data obrashcheniya: 13.10.2025).

19. 10 instrumentov modelirovaniya kiberatak dlya povysheniya bezopasnosti. URL: https://dzen.ru/a/ZG89c5dzB3yyeIzP (data obrashcheniya: 19.10.2025).

20. Get Involved https. URL: //caldera.mitre.org/ (data obrashcheniya: 18.10.2025).

21. High-Risk Exposures Faster. URL: https://xmcyber.com/ (data obrashcheniya: 01.10.2025).

22. PRISM: A Hierarchical Intrusion Detection Architecture for Large-Scale Cyber Networks. URL: https://deepai.org/publication/prism-a-hierarchical-intrusion-detection-architecture-for-large-scale-cyber-networks (data obrashcheniya: 11.09.2025).

23. What is Threat Simulation? URL: https://xmcyber.com/glossary/what-is-threat-simulation/ (data obshcheniya: 04.10.2025).

24. Real'naya ataka zashchishchaet. Simulyaciya kiberatak s pomoshch'yu BAS-reshenij. URL: https://www.cti.ru/media/publications/realnaya-ataka-zashchishchaet-simulyatsiya-kiberatak-s-pomoshchyu-bas-resheniy/ (data obrashcheniya: 01.10.2025).

25. Gamification And Simulations: Powering Up Training And Productivity. URL: https://elearningindustry.com/gamification-and-simulations-powering-up-training-and-productivity (data obrashcheniya 18.10.2025).

26. Kirstie Greany Why gamification in elearning is important. URL: https://www.elucidat.com/blog/why-gamification-in-elearning-is-important/ (data obrashcheniya: 19.10.2025).

27. Akap'ev V.L., Savotchenko S.E. Gejmifikaciya v elektronnom obrazovanii // Vestnik Voronezhskogo gosudarstvennogo universiteta. Ser.: Problemy vysshego obrazovaniya. 2025. № 3. S. 19–23.

28. The Top 5 Benefits of Gamification in Learning. URL: https://www.learnlight.com/en/articles/5-benefits-of-gamification-in-learning/ (data obrashcheniya: 01.10.2025).

Информация о статье:
Статья поступила в редакцию: 31.10.2025; одобрена после рецензирования: 24.11.2025;
принята к публикации: 25.11.2025

Information about the article:
The article was submitted to the editorial office: 31.10.2025; approved after review: 24.11.2025;
accepted for publication: 25.11.2025

Информация об авторах:
Акапьев Виктор Львович, доцент кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России им. И.Д. Путилина (308024, г. Белгород, ул. Горького, д. 71), кандидат педагогических наук, e-mail: akapevv@yandex.ru, https://orcid.org/0009-0001-0560-8117, SPIN-код: 6275-6804.
Дунаев Роман Алексеевич, доцент кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России им. И.Д. Путилина (308024, г. Белгород, ул. Горького, д. 71), кандидат философских наук, e-mail: r_dunaev@bk.ru, https://orcid.org/ 0009-0003-0144-5976, SPIN-код: 7718-7350
Ковалева Екатерина Геннадьевна, доцент кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России им. И.Д. Путилина (308024, г. Белгород, ул. Горького, д. 71), кандидат технических наук, e-mail: kovalevazchs@yandex.ru, https://orcid.org/ 0000-0001-7502-5163, SPIN-код: 2280-5610
Борисенко Александр Васильевич, преподаватель кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России им. И.Д. Путилина (308024, г. Белгород, ул. Горького, д. 71), кандидат физико-математических наук, e-mail: borisenko02.94@mail.ru, https://orcid.org/0000-0002-2539-3096, SPIN-код: 4684-8218

Information about authors:
Akapyev Viktor L., associate professor of the department of information and computer technologies in the activities of the department of internal affairs Belgorod Law Institute of Ministry of the Interior of the Russian Federation named after I.D. Putilin (308024, Belgorod, Gorky street, 71), candidate of pedagogical sciences, e-mail: akapevv@yandex.ru, https://orcid.org/0009-0001-0560-8117, SPIN: 6275-6804
Dunaev Roman A., associate professor of the department of information and computer technologies in the activities of the department of internal affairs Belgorod Law Institute of Ministry of the Interior of the Russian Federation named after I.D. Putilin (308024, Belgorod, Gorky street, 71), candidate of philosophical sciences, e-mail: r_dunaev@bk.ru, https://orcid.org/ 0009-0003-0144-5976, SPIN: 7718-7350
Kovaleva Ekaterina G., associate professor of the department of information and computer technologies in the activities of the department of internal affairs Belgorod Law Institute of Ministry of the Interior of the Russian Federation named after I.D. Putilin (308024, Belgorod, Gorky street, 71), candidate of technical sciences, e-mail: kovalevazchs@yandex.ru, https://orcid.org/ 0000-0001-7502-5163, SPIN: 2280-5610
Borisenko Alexander V., lecturer at the department of information and computer technologies in the activities of the department of internal affairs Belgorod Law Institute of Ministry of the Interior of the Russian Federation named after I.D. Putilin (308024, Belgorod, Gorky street, 71), candidate of physico-mathematical sciences, e-mail: borisenko02.94@mail.ru, https://orcid.org/0000-0002-2539-3096, SPIN: 4684-8218