РАЗРАБОТКА ОБУЧАЮЩЕЙ ИГРЫ ДЛЯ ФОРМИРОВАНИЯ НАВЫКОВ ПО ЗАЩИТЕ ОТ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Клиндухов Я.А., Мажаева С.Д.

Национальный детский технопарк, г. Минск, Республика Беларусь

Бойправ О.В. – канд. тех. наук, доцент, заведующий кафедрой защиты информации

Аннотация. В статье выявлены основные проблемы разработки обучающих игр для подготовки специалистов по информационной безопасности: баланс обучения и геймплея, моделирование угроз, интеграция актуальных таксономий, оценка эффективности и техническая реализация. Предложен алгоритм создания игры, состоящий из девяти шагов. Описана реализация игры на языке программирования Python. Результаты апробации обучающей игры показали прирост среднего балла более чем на 20%, что подтверждает эффективность предложенного подхода.

Ключевые слова. обучающие игры, разработка обучающих игр, алгоритм создания обучающих игр, Cyber Kill Chain, моделирование угроз информационной безопасности, подготовка специалистов в области информационной безопасности.

В условиях стремительной цифровизации всех сфер жизни Республики Беларусь наблюдается значительный рост угроз информационной безопасности [1–3]. Согласно исследованиям Ponemon Institute, 75% инцидентов в более чем 310 компаниях по всему миру связаны именно с ошибками пользователей информационных систем. В таких условиях появляется значительный разрыв между техническими возможностями программных средств защиты информации и реальными навыками пользователей по их применению. Одним из наиболее эффективных инструментов преодоления этого разрыва выступают обучающие игры, однако их разработка сопряжена с рядом системных проблем, без решения которых обучающая игра теряет как образовательную, так и игровую ценность. Целью данной работы является выявление ключевых проблем разработки обучающих игр по информационной безопасности, предложение алгоритма их преодоления и апробация полученного решения.

Под обучающей игрой будем понимать компьютерную программу, которая разработана специально для обучения определенным предметам или навыкам [4]. Отличие обучающей игры от компьютерной заключается в получении обучающимися новых специальных знаний, наличии четкой учебной цели и педагогического результата, в то время как компьютерная игра фокусируется на развлечении, хотя и может иметь побочный образовательный эффект.

Также, обучающие игры имеют эффективное применение в области информационной безопасности, так как они позволяют моделировать реальные угрозы информационной безопасности, формируя необходимые практические и теоретические навыки. Большинство таких игр носят симуляционный характер, моделируя обучающемуся ситуацию, похожую на реальную. Особенностью таких симуляторов является возможность генерации конкретных угроз информационной безопасности, таких как внедрение вредоносного кода в процессы, использование легитимных учетных записей, почтовый фишинг и другие. Такой подход обеспечивает высокую заинтересованность обучающегося в процессе, позволяя добиться высокой эффективности обучения в короткие сроки. Кроме того, специалистам по защите информации часто требуется поиск неординарных решений, а игровые технологии способствуют развитию творческого потенциала и стратегического мышления, необходимого для решения задач проектирования и защиты информационных систем.

На основе анализа литературных данных и собственного опыта разработки обучающей игры выделены пять основных проблем, возникающих при создании обучающих игр в области информационной безопасности. Первая проблема – это баланс между обучением и геймплеем. Чрезмерное преобладание теории снижает степень заинтересованности игрой, в то время как избыточная игровая составляющая без требуемого образовательного наполнения не формирует нужных знаний и навыков.

Вторая проблема заключается в правильном моделировании реальных угроз – слишком упрощённые сценарии не дают практических навыков, что ограничивает их применение в учебном процессе. Третья проблема связана с интеграцией актуальных моделей атак: большинство существующих обучающих игр используют устаревшие или разрозненные данные об угрозах информационной безопасности и не имеют привязки к общепризнанным базам знаний, таким как MITRE ATT&CK.

Четвёртая проблема касается оценки эффективности обучения – без встроенных механизмов тестирования и сбора метрик практически невозможно измерить прирост знаний после прохождения игры. Из-за этого игрок может перейти к последующим этапам игры, не получив и не закрепив

полученные знания. Наконец, пятая проблема носит технический характер и связана с выбором языка программирования и фреймворка, которые должны обеспечивать быструю разработку, кроссплатформенность и работу на ограниченных вычислительных ресурсах. Для системного решения перечисленных проблем разработан и апробирован алгоритм создания обучающей игры по информационной безопасности, состоящий из девяти этапов, приведенный на рисунке 1.

Рисунок 1 – Алгоритм создания обучающей игры в области информационной безопасности

Первым шагом идёт анализ целевой аудитории, в ходе которого определяется уровень подготовки будущих игроков – школьники, студенты или действующие сотрудники. Вторым шагом является выбор модели угроз. Третьим шагом определяется жанр игры: на основе анализа литературы, наиболее эффективным оказался жанр симулятора, поскольку он позволяет максимально приблизить игровую ситуацию к реальной работе специалиста.

Четвёртый шаг – разработка сценария, включающего детальную проработку сюжетной линии игры, роли персонажей, интерфейса пользователя и разбиение на дни или уровни сложности. Пятый шаг предполагает выбор программных средств разработки: языка программирования, конкретного фреймворка, системы управления базами данных и графических средств. Шестой шаг – реализация игровых механик, а именно разработанный геймплей должен сочетать в себе баланс графической составляющей и реализации выбранных угроз. Седьмым шагом внедряются обучающие элементы: встроенная справочная система, например в виде браузера, тесты для самопроверки и контекстные подсказки.

Восьмой шаг является рекомендуемым всем обучающим играм, в которых реализуются атаки на информационные системы, и заключается в интеграции модели нарушителя Cyber Kill Chain: каждая учебная угроза должна быть привязана к конкретному этапу цепочки атаки [5]. Девятым, заключительным шагом алгоритма выступает апробация разработанной игры и оценка её эффективности с помощью тестирования до и после прохождения.

Модель Cyber Kill Chain, предложенная компанией Lockheed Martin, описывает семь последовательных этапов кибератаки: разведка, вооружение, доставка, эксплуатация, установка, получение управления и действие нарушителя. В разработанной нами игре каждая учебная угроза сопоставляется с конкретным этапом этой цепочки. Например, фишинговая атака относится к этапу доставки, поскольку злоумышленник доставляет вредоносную ссылку или вложение. Использование легитимных учётных записей соответствует этапу эксплуатации, когда нарушитель уже получил доступ к системе и использует штатные средства. Внедрение вредоносного кода в процессы операционной системы относится к этапу установки. Такая привязка позволяет игроку не просто выбирать средство защиты, а осознанно понимать, на каком этапе развития атаки применяется то или иное программное средство – межсетевой экран, антивирус, SIEM-система или средство резервного копирования.

Для практической реализации описанного алгоритма был выбран язык программирования Python версии 3.14.0 и фреймворк Pygame версии 2.5.0, что позволило создать игровой проект, не требующий больших вычислительных ресурсов. Жанр игры определён как симулятор практических задач специалиста отдела информационной безопасности организации. Сюжет игры следующий: игрок выступает в роли нового сотрудника отдела информационной безопасности вымышленной компании «ТехноПро», и все действия происходят внутри интерфейса персонального компьютера, состоящего из различных программ, с которыми игроку предстоит взаимодействовать – SIEM-система, антивирусная программа, система анализа трафика и другие. Игра состоит из четырёх дней, причём алгоритм каждого дня един и соответствует этапам модели Cyber Kill Chain. Сначала одна из программных систем персонального компьютера уведомляет игрока об обнаружении нестандартного поведения некоторого процесса и просит выявить его среди легитимных процессов. После выявления вредоносного процесса начинается расследование угрозы, при котором игроку требуется детально изучить признаки угрозы, алгоритм её работы и методы борьбы. Важно отметить, что с каждым днём угрозы информационной безопасности меняются и их уровень возрастает, последовательно проходя этапы Cyber Kill Chain от доставки до действий нарушителя. После выполнения всех этапов обучающей игры игрок проходит тестирование по теме отражённой атаки, после чего ему выводится количество правильных ответов и, при необходимости, рекомендация повторения теоретического материала во встроенном интернет-браузере, где собраны сведения об всех угрозах из матрицы MITRE ATT&CK.

Для количественной оценки эффективности разработанной обучающей игры было проведено тестирование среди 38 учащихся Национального детского технопарка по образовательным направлениям «лазерные технологии», «электроника и связь», «информационные и компьютерные технологии» и «инженерная экология». Методика апробации включала сбор первичных знаний по теме угроз информационной безопасности в виде тестирования с выбором из четырёх вариантов ответов, всего десять вопросов, поэтому оценка осуществлялась по десятибалльной системе. Затем участникам было предложено полностью пройти игру, после чего они повторно прошли те же самые десять вопросов для выявления вторичных знаний. Результаты тестирования до прохождения игры представлены на рисунке 2, а результаты после тестирования представлены на рисунке 3.

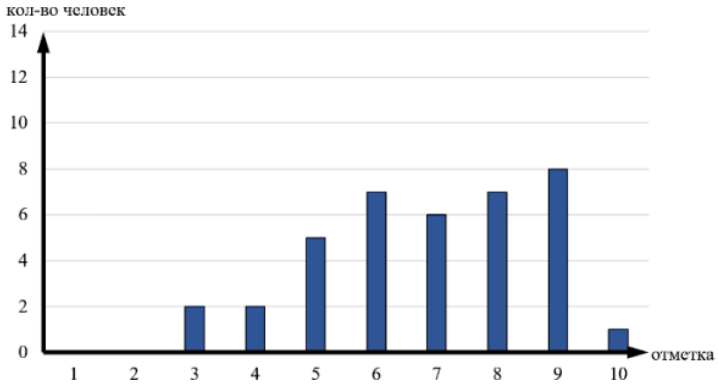

Рисунок 2 – Распределение отметок до прохождения обучающей игры

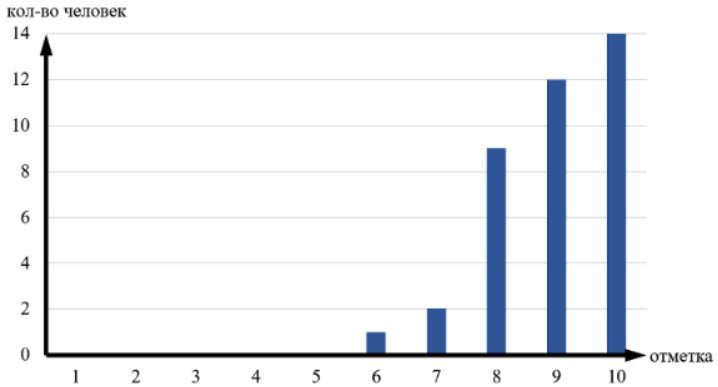

Рисунок 3 – Распределение отметок после прохождения обучающей игры

Результаты тестирования показали, что до прохождения игры средний балл составил 6,87, тогда как после прохождения игры средний балл повысился до 8,95. Таким образом, прирост среднего балла составил 2,08, что говорит об увеличении среднего балла более чем на 20%. Полученные результаты свидетельствуют о высокой эффективности разработанной обучающей игры.

Кроме того, отзывы участников исследования говорят о высоком уровне заинтересованности обучающей игрой, что выгодно отличает её среди других видов обучающих материалов.

В ходе проведённого исследования были выявлены пять ключевых проблем разработки обучающих игр в области информационной безопасности: баланс между обучением и геймплеем, адекватное моделирование реальных угроз, интеграция актуальных моделей атак, оценка эффективности обучения и техническая реализация. Для преодоления этих проблем предложен и апробирован формализованный девятишаговый алгоритм создания обучающей игры, обязательным элементом которого выступает интеграция модели Cyber Kill Chain. Разработанный на основе этого алгоритма симулятор практических задач специалиста отдела информационной безопасности позволил реализовать интерактивный подход к обучению, где каждая угроза привязана к конкретному этапу цепочки атак. Результаты экспериментальной апробации, проведённой среди учащихся Национального детского технопарка, подтвердили высокую эффективность разработанной обучающей игры: прирост среднего балла успеваемости составил более 20%. Таким образом, обучающие игры, созданные по предложенному алгоритму, могут быть эффективным средством для подготовки специалистов в области защиты информации, обеспечивая высокую вовлечённость обучающихся и развивая аналитическое и стратегическое мышление.

Список использованных источников:

1. Барило К. С., Нестеренков С. Н., Бегляк Е. В. (2025) Криптографические методы защиты информации в сфере электронного документооборота. Технические средства защиты информации. 66–69.

2. Мырадов П. С., Мырадов П. С. (2025) Технические средства защиты информации: современные технологии, методы и перспективы. Технические средства защиты информа-ции. 260–263.

3. Дроздов М. М., Прудник А. М. (2017) Анализ состояния и методология обеспечения безопасности информационных систем. Технические средства защиты информации. 15–16.

4. Рябинин Н. С. (2025) Многофункциональный веб-сервис для тестирования и интерактивных игр с использованием искусственного интеллекта. Радиотехника и электроника. 171–175.

5. Борботько Т. В., Бойправ О. В., Тимофеев А. М. (2025) Основы информационной безопасности. Минск, Издательство «БГУИР».