УДК 004.056

ПРИМЕНЕНИЕ ОБУЧАЮЩИХ ИГР ДЛЯ ФОРМИРОВАНИЯ СПЕЦИАЛЬНЫХ НАВЫКОВ ПО ЗАЩИТЕ ОТ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Я.А. Клиндухов[1], С.Д. Мажаева[1], О.В. Бойправ[2],
[1]Учреждение образования «Национальный детский технопарк», г. Минск, Беларусь
[2]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Беларусь

Аннотация. В данной работе рассматривается проблема роста угроз информационной безопасности в условиях стремительной цифровизации всех сфер жизни Республики Беларусь. Обосновано применение образовательных игр как эффективного инструмента для формирования специальных навыков по защите от угроз информационной безопасности и преодоления разрыва между техническими возможностями программных средств и реальными навыками пользователей. Описана разработка обучающей игры на языке Python и фреймворке Pygame, представляющей собой симулятор практических задач специалиста отдела информационной безопасности организации. Обучающей игрой моделируются угрозы информационной безопасности согласно этапам модели Cyber Kill Chain. Приведены результаты апробации среди учащихся Национального детского технопарка, подтверждающие высокую эффективность обучения: прирост среднего арифметического отметок после прохождения игры составил более 20 %. Доказана эффективность обучающих игр в системе подготовки специалистов по информационной безопасности.

Ключевые слова: обучающие игры, цифровизация, угрозы информационной безопасности, человеческий фактор, средства защиты информации, моделирование угроз информационной безопасности, методика обучения, эффективность обучающей игры, апробация обучающей игры, подготовка специалистов по информационной безопасности.

APPLICATION OF EDUCATIONAL GAMES FOR THE FORMATION OF SPECIAL SKILLS IN PROTECTION AGAINST INFORMATION SECURITY THREATS

Y.A. Klindukhov[1], S.D. Mazhaeva[1], O.V. Boiprav[2]
[2]Educational Institution "National Children's Technopark", Minsk, Republic of Belarus
[1] Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. This paper examines the problem of the growth of information security threats in the context of the rapid digitalization of all spheres of life in the Republic of Belarus. The use of educational games as an effective tool for the formation of basic skills to protect against information security threats and to bridge the gap between the technical capabilities of software and the real skills of users is substantiated. The development of an educational game in Python and the Pygame framework is described, which is a simulator of practical tasks of a specialist in the information security department of an organization.

The educational game simulates information security threats according to the stages of the Cyber Kill Chain model. The results of the testing among students of the National Children's Technopark are presented, confirming the high effectiveness of training: the increase in the arithmetic mean of the marks after passing the game was more than 20 %. The effectiveness of educational games in the training of information security specialists has been proven.
Keywords: educational games, digitalization, information security threats, human factor, information security tools, information security threat modeling, teaching methodology, educational game effectiveness, educational game testing, information security specialist training.

Введение

В условиях стремительной цифровизации всех сфер жизни Республики Беларусь наблюдается значительный рост угроз информационной безопасности [1–3]. Несмотря на наличие современных технических средств защиты информации, ключевой проблемой остается человеческий фактор. 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. В связи с этим одной из наиболее важных задач является внедрение новых образовательных подходов, среди которых особое место занимают образовательные игры, для подготовки специалистов в области защиты информации.

Основная часть

Под образовательными играми будем понимать игры, которые разработаны специально для обучения определенным предметам или навыкам [4]. Отличие образовательной 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.

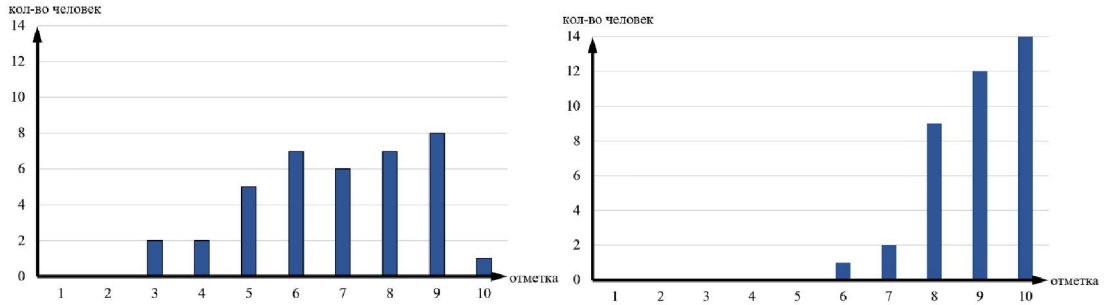
Также, обучающие игры имеют эффективное применение в области информационной безопасности, так как они позволяют моделировать реальные угрозы информационной безопасности, формируя необходимые практические и теоретические навыки. Большинство таких игр носят симуляционный характер, моделируя обучающемуся 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.

Для оценки эффективности образовательных игр в области информационной безопасности в рамках данной работы разработана обучающая игра, направленная на выбор средств защиты от угроз информационной безопасности. Для реализации игры использовался язык программирования Python 3.14.0 и фреймворк Pygame 2.5.0, что позволило создать игровой проект, не требующий больших вычислительных ресурсов. Жанр игры определен как симулятор практических задач специалиста отдела информационной безопасности организации.

Сюжет игры следующий. Игрок выступает в роли нового сотрудника отдела информационной безопасности вымышленной компании «ТехноПро». Действие разворачивается внутри интерфейса персонального компьютера сотрудника, состоящего из различных программ, с которыми игроку предстоит взаимодействовать (SIEM–система, антивирусная программа, система анализа трафика и другие). Далее в игре моделируется угроза информационной безопасности, которую игрок должен выявить, идентифицировать, проанализировать и устранить. Важно отметить, что деятельность нарушителя в игре представлена в виде последовательных этапов, согласно этапам модели нарушителя Cyber Kill Chain [5].

Для количественной оценки эффективности разработанной обучающей игры было предложено собрать первичные знания по теме угроз информационной безопасности, которые реализованы в игре, в виде тестирования с выбором из 4 вариантов ответов. Всего вопросов 10, поэтому оценка осуществлялась по 10-балльной системе. Далее было предложено полностью пройти игру. После прохождения игры было предложено снова пройти те же 10 вопросов для выявления вторичных знаний. Результаты тестирования до прохождения игры представлены на части *а* рисунка, а результаты после тестирования – на части *б* рисунка. Выборка составила 38 человек, учащихся Национального детского технопарка образовательных направлений (лазерные технологии, электроника и связь, информационные и компьютерные технологии, инженерная экология и другие).



Распределение отметок до прохождения обучающей игры (*a*) и после (*b*)
Distribution of marks before completing the educational game (*a*) and after (*b*)

Как видно из результатов, до тестирования средний балл составил 6.87 балла, а после игры данное значение составило 8.95 балла. Прирост среднего балла до и после игры составил 2.08 балла, что говорит о приросте значений более чем в 20%. Данные результаты свидетельствуют о высокой эффективности обучающей игры. Также отзывы участников исследования говорят о высоком уровне заинтересованности обучающей игрой, что выделяет игру среди других видов обучающих материалов.

Заключение

В ходе исследования было обосновано применение обучающей игры как эффективного инструмента для формирования специальных навыков по защите от угроз информационной безопасности. Разработанный симулятор практических задач специалиста отдела информационной безопасности позволил реализовать интерактивный подход к обучению. Моделирование реальных сценариев атак (в соответствии с моделью Cyber Kill Chain) в безопасной среде дало возможность обучающимся не только ознакомиться с интерфейсом программного обеспечения, но и выявить, идентифицировать, проанализировать и устранить угрозы информационной безопасности.

Результаты экспериментальной апробации, проведенной среди учащихся Национального детского технопарка, подтвердили высокую эффективность разработанной обучающей игры. Сравнительный анализ данных первичного и вторичного контроля показал прирост среднего балла успеваемости с 6.87 до 8.95, что составляет более 20%.

Таким образом, обучающие игры могут быть эффективным средством для подготовки специалистов в области защиты информации. Использование образовательных игр способствует повышению уровня знаний в области информационной безопасности. Помимо улучшения количественных показателей успеваемости, данный подход обеспечивает высокую вовлеченность обучающихся, развивает аналитическое и стратегическое мышление, что делает внедрение обучающих

перспективным направлением в системе подготовки специалистов по информационной безопасности.

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 информации.* 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»

References

1. Barilo K. S., Nesterenkov S. N., Beglyak E. V. (2025) Cryptographic Methods of Information Protection in the Field of Electronic Document Management. *Technical Information Security Tools*. 66–69 (in Russian).

2. Myradov P. S., Myradov P. S. (2025) Technical Information Security Tools: Modern Technologies, Methods and Prospects. *Technical Information Security Tools*. 260–263 (in Russian).

3. Drozdov M. M., Prudnik A. M. (2017) State Analysis and Methodology for Ensuring the Security of Information Systems. *Technical Information Security Tools*. 15–16 (in Russian).

4. Ryabinin N. S. (2025) Multifunctional Web Service for Testing and Interactive Games Using Artificial Intelligence. *Radio Engineering and Electronics*. 171–175 (in Russian).

5. Borbotko T. V., Boiprav O. V., Timofeev A. M. (2025) *Fundamentals of Information Security*. Minsk, BSUIR Publishing House (in Russian).

Сведения об авторах

Клиндухов Я.А., учащийся по направлению «Информационная безопасность», учреждение образования «Национальный детский технопарк», klinduhov.science@gmail.com.

Мажаева С.Д., учащаяся по направлению «Информационная безопасность», учреждение образования «Национальный детский технопарк», sd.mazhaeva2009@gmail.com.

Бойправ О.В., канд. техн. наук, доц., зав. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», smu@bsuir.by.

Information about the authors

Klindukhov Y.A., Student of the direction "Information Security", Educational Institution "National Children's Technopark", klinduhov.science@gmail.com.

Mazhaeva S.D., Student of the direction "Information Security", Educational Institution "National Children's Technopark", sd.mazhaeva2009@gmail.com.

Boiprav O.V., Cand. Sci. (Tech.), Associate Professor, Head of the Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", smu@bsuir.by.