УДК 004.056:37.091.33

TELEGRAM-БОТ ДЛЯ ОБУЧЕНИЯ ПОДРОСТКОВ ОСНОВАМ КИБЕРБЕЗОПАСНОСТИ

С.Н. Петров[1], Д.В. Ермоленко[2], А.С. Рожкова[2]

[1] *Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь*

[2] *Учреждение образования «Национальный детский технопарк», г. Минск, Республика Беларусь*

Аннотация. Разработаны специальные учебные сценарии, отражающие типовые ситуации в цифровой среде, связанные с безопасностью подростков, включающие попытки социальной инженерии и попытки втягивания в противоправную деятельность. Для прохождения сценариев реализован Telegram-бот. Для Telegram-бота графические материалы были адаптированы под формат мессенджера и использовались преимущественно в виде иллюстраций, эмодзи и встроенных медиаэлементов.

Ключевые слова: кибербезопасность; геймификация обучения; цифровая безопасность подростков; информационная безопасность; обучающие игровые сценарии; Telegram-бот.

TELEGRAM BOT FOR TEACHING TEENAGERS THE BASICS OF CYBERSECURITY

S.N. Petrov[1], D.V. Ermolenko[2], A.S. Rozhkova[2]
[1] *Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus*
[2] *Educational Institution "National Children's Technopark", Minsk, Republic of Belarus*

Abstract. Special training scenarios have been developed that reflect typical situations in the digital environment related to the safety of adolescents, including attempts at social engineering and attempts to involve them in illegal activities. A Telegram bot has been implemented to run through the scenarios. For the Telegram bot, graphic materials were adapted to the messenger format and were used primarily in the form of illustrations, emojis, and embedded media elements.
Keywords: cybersecurity; gamification of learning; digital safety of teenagers; information security; educational game scenarios; Telegram bot.

Введение

Подростки – это одно из самых активных цифровых поколений, однако при этом остаются наиболее уязвимой группой пользователей сети. Ранний доступ к интернету, высокая вовлеченность в социальные платформы и недостаточный жизненный опыт создают условия, при которых цифровые угрозы часто остаются нераспознанными. Это формирует проблему, требующую новых подходов к обучению кибербезопасности. Анализ угроз показывает, что подростки сталкиваются сразу с несколькими рисками, и их поведение в сети требует системного просвещения. Выполнен анализ образовательных приложений в области кибербезопасности, показавший, что существующие решения часто либо слишком примитивны, либо избыточно сложны [1]. Разработанный проект может занять пустующую нишу, предложив целевой аудитории (14–17 лет) контент, соответствующий их когнитивным и поведенческим условиям.

Основная часть

Реализована методика трансформации реальных угроз [2] (фишинг, вишинг, кибербуллинг, эксплуатация вредоносного ПО, AI-имперсонация, угроза деанонимизации, шантаж, вовлечение в противоправную деятельность, утечка данных, доксинг, овершеринг, сексторшен) в игровые задачи с мгновенной обратной связью, что является средством формирования навыков принятия решений в цифровой среде.

Игровая сессия проходит непосредственно в интерфейсе мессенджера. Игровой процесс построен на принципах текстового квеста и симулятора принятия решений, где каждый шаг пользователя имеет немедленное

последствие. Основным элементом взаимодействия является inline-клавиатура, прикрепленная к каждому сообщению-уровню, что обеспечивает интуитивное управление и исключает возможность ввода некорректных команд. Прогресс игрока отслеживается с помощью двух переменных: HP (Health Points) и XP (Experience Points). HP, стартующее со 100 единиц, символизирует цифровую «репутацию» или уровень защищенности. Каждая ошибка снижает HP, и при достижении нуля игра завершается, что повышает ценность каждого решения. XP, в свою очередь, начисляется за правильные ответы и служит метрикой успешности.

Сюжетная основа проходит через 75 уникальных сценариев, имитирующих реальные киберугрозы и адаптированных под формат мессенджера. Уровни сгруппированы по тематическим блокам. Игра начинается с наиболее массовых и очевидных угроз, таких как фишинг (19 сценариев) и вредоносные загрузки (5 сценариев), где от игрока требуется распознать грубые ошибки в URL или явную опасность в исполняемых файлах. По мере продвижения ситуации усложняются. Так, в блоке про мошенничество игроку предлагается оценить подлинность интернет-магазина или внезапного сбора средств от блогера.

Для поддержания вовлеченности и развития критического мышления в игру интегрировано 15 сценариев, где нет никакой угрозы. Это заставляет игрока постоянно анализировать контекст, а не действовать по заученному шаблону «все ссылки опасны». Правильное распознавание безопасной ситуации является таким же важным навыком, как и идентификация угрозы.

Кнопки выбора действий были сделаны динамическими, чтобы их названия соответствовали контексту ситуации. Вместо абстрактных «Доверять», «Проверить», «В бан», которые не всегда логичны, используются конкретные формулировки, такие как «Перейти по ссылке», «Спросить отправителя», «Заблокировать» или «Удалить». Это значительно повышает реализм и интуитивность интерфейса. Например, в сценарии с телефонным мошенничеством правильным действием будет «Сбросить», а в ситуации с угрозами в комментариях (кибербуллинг) – «Пожаловаться». Уровни про сваттинг и вовлечение в преступную деятельность демонстрируют не только цифровые, но и реальные юридические последствия неосторожных действий в сети.

В структуру бота встроена вспомогательная команда /theory, которая открывает отдельное Mini App (веб-приложение внутри Telegram) с базой знаний по вопросам кибербезопасности. Эта энциклопедия позволит игроку в любой момент изучить теорию по конкретной угрозе. Это превращает бота из простого квеста в комплексный обучающий инструмент с гибридной механикой.

Серверной часть реализована на языке Python 3.10 с использованием специализированных библиотек. Ядром системы выступает библиотека pyTelegramBotAPI (Telebot), обеспечивающая полное покрытие методов Telegram Bot API, включая работу с InlineKeyboardMarkup для реализации динамического интерфейса и WebAppInfo для интеграции мини-приложений. Для реализации веб-сервера, обслуживающего контент Mini App и обрабатывающего API-запросы, интегрирован микрофреймворк Flask.

Заключение

Разработаны специальные учебные сценарии, отражающие типовые ситуации в цифровой среде, включающие примеры фишинговых атак, попыток социальной инженерии, кибербуллинга и попытки выманить персональные данные. Для прохождения разработанных сценариев выполнили реализацию Telegram-бота, который доступен по ссылке @csgame1203bot.

Список использованных источников

1. Петров С. Н. Использование обучающих игр для формирования навыков кибербезопасности у подростков / С. Н. Петров, Д. В. Ермоленко, А. С. Рожкова // Мир студенческой науки: сборник статей X Международного научно-исследовательского конкурса. – Пенза: МЦНС «Наука и Просвещение». – 2025. – С. 7–11.

2. Солдатова, Г. У. Цифровое поколение России: компетентность и безопасность / Г. У. Солдатова, Е. И. Рассказова, Т. А. Нестик. – М. : Смысл, 2017. – 375 с.

References

1. Petrov S. N. Using educational games to develop cybersecurity skills in teenagers / S. N. Petrov, D. V. Ermolenko, A. S. Rozhkova // The World of student Science: a collection of articles from the X International Scientific Research Competition. – Penza: ICSC «Nauka i Prosveshchenie». – 2025. – P. 7–11. (in Russian).

2. Soldatova G. U. Russia's Digital Generation: competence and security / G. U. Soldatova, E. I. Rasskazova, T. A. Nestik. – M. : Smysl, 2017. – 375 p. (in Russian).

Сведения об авторах

Петров С.Н., канд. техн. наук, доц., доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», petrov@bsuir.by.

Ермоленко Д. В., учащийся, учреждение образования «Национальный детский технопарк», chenazesm@gmail.com.

Рожкова А. С., учащийся, учреждение образования «Национальный детский технопарк», alinarazhkova@gmail.com.

Information about the authors

Petrov S.N., Cand. of Sci., Associate Professor, Associate Professor of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", petrov@bsuir.by.

Ermolenko D. V., student, Educational Institution "National Children's Technopark", chenazesm@gmail.com.

Rozhkova A. S., student, Educational Institution "National Children's Technopark", alinarazhkova@gmail.com.