DOI: https://doi.org/10.25146/1995-0861-2021-57-3-290

УДК 378:811

АПРОБАЦИЯ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ К АТАКАМ ПРИ ВЗАИМОДЕЙСТВИИ УЧАСТНИКОВ СЕТЕВЫХ ГЕЙМИФИЦИРОВАННЫХ ОБРАЗОВАТЕЛЬНЫХ ПРОЕКТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ[1]

К.В. Сафонов (Красноярск, Россия)
В.В. Золотарев (Красноярск, Россия)
Е.А. Маро (Таганрог, Россия)
Е.А. Ищукова (Таганрог, Россия)
Е.Ю. Золотарева (Красноярск, Россия)

Аннотация

Постановка проблемы. В статье рассматриваются вопросы, связанные с защищенным взаимодействием внутри геймифицированной образовательной среды, в частности в области игровых кейсов, применяемых для обучения информационной безопасности. Приведены различные подходы к сбору цифрового следа социально-инженерных атак и способы повышения устойчивости к атакам в области социальной инженерии на основе анализа цифрового следа. Также показаны оценки и алгоритмы действий, повышающих устойчивость к указанным атакам участников сетевых геймифицированных проектов, описана их апробация. *Цель* статьи – поиск подхода к повышению безопасного взаимодействия в геймифицированных сетевых образовательных проектах.

Методологию исследования составляют анализ действующих игровых практик в рамках обучения информационной безопасности; изучение результатов междисциплинарных исследований отечественных и зарубежных ученых, посвященных использованию геймификации в различных обучающих задачах, игровых сред и решений, их оценки.

Результаты. Разработаны авторские рекомендации по повышению устойчивости участников сетевых геймифицированных образовательных проектов к социально-инженерным атакам, показаны алгоритмы и порядок действий для выполнения указанной задачи, описана их апробация.

Заключение. По результатам оценки, приведенной в статье, показана возможность использования сбора цифрового следа для повышения безопасности реализации взаимодействия участников в сетевых геймифицированных проектах. Рассматриваемые в статье авторские рекомендации могут быть применены в ходе обучения магистров по направлению подготовки 10.04.01 Информационная безопасность (очная форма обучения).

Ключевые слова: *обучение, информационная безопасность, геймификация, фишинг, социальная сеть, образовательный проект, цифровой след.*

Сафонов Константин Владимирович – доктор физико-математических наук, профессор кафедры прикладной математики, Сибирский государственный университет науки и технологий им. академика М.Ф. Решетнева; ORCID:http://orcid.org/0000-0003-0405-3065, e-mail: safonovkv@rambler.ru

Золотарев Вячеслав Владимирович – кандидат технических наук, доцент кафедры безопасности информационных технологий, Сибирский государственный университет науки и технологий им. академика М.Ф. Решетнева; ORCID: http://orcid.org/0000-0002-8054-8564; e-mail: amida.2@yandex.ru

Маро Екатерина Александровна – кандидат технических наук, доцент кафедры безопасности информационных технологий, Южный федеральный университет; ORCID: http://orcid.org/0000-0001-5136-7804; e-mail: marokat@gmail.com

Ищукова Евгения Александровна – кандидат технических наук, доцент кафедры безопасности информационных технологий, Южный федеральный университет; ORCID: http://orcid.org/0000-0002-6818-1608; e-mail: jekky82@mail.ru

Золотарева Елена Юрьевна – инженер кафедры безопасности информационных технологий, Сибирский государственный университет науки и технологий им. академика М.Ф. Решетнева; e-mail: umka.82@mail.ru

[1] Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект № 19-013-00711.

ВЕСТНИК КРАСНОЯРСКОГО ГОСУДАРСТВЕННОГО ПЕДАГОГИЧЕСКОГО УНИВЕРСИТЕТА им. В.П. АСТАФЬЕВА

Постановка проблемы. Для игровых проектов, реализованных в форме сетевых или использующих элементы сетевых проектов, существует фундаментальное противоречие между открытостью (требуемой с педагогической точки зрения для максимального охвата и вовлеченности участников в образовательный процесс, понимания и осмысления сути этого процесса, готовности к сотрудничеству, согласованности действий, особенно при широком применении геймификации) и требованиями информационной безопасности.

Методологию исследования составляют анализ действующих игровых практик в рамках обучения информационной безопасности; изучение результатов междисциплинарных исследований отечественных и зарубежных ученых, посвященных использованию геймификации в различных обучающих задачах, игровых сред и решений, их оценки. При этом основой для эксперимента в данном случае стал ряд проектов, завершенных или продолжаемых авторами при поддержке Фонда Потанина и Российского фонда фундаментальных исследований в 2015–2021 гг. в области обучения информационной безопасности, а также ряд исследований зарубежных и российских ученых в этой области. Анализ, приведенный ниже, сосредоточен на использовании цифрового следа в дообучении (повышении осведомленности) пользователей и применении некоторых защитных техник и подходов.

Цель статьи ориентирована на разработку подхода к повышению безопасного взаимодействия в геймифицированных сетевых образовательных проектах, применимого для проектов в форме кейс-стади или игровых решений, широко использующих информационные технологии, разрабатываемых несколькими взаимодействующими студенческими командами через социальную сеть.

Обзор научной литературы. Ранее авторами были рассмотрены несколько примеров игровых сред как с использованием социальной сети в качестве инструмента взаимодействия [Tang, Hanneghan, 2010; Jin et al., 2018], так и с применением иных технологий вовлечения участников в игрофицированный процесс обучения [Liu et al., 2018; Yasin et al., 2018; Beckers, Pape, 2016; Trickel et al., 2017; Hart et al., 2020; Ali Zani et al., 2020]. Во всех этих случаях авторы не увидели существенных усилий по обеспечению информационной безопасности, что, вероятно, может привести к уязвимости этих проектов к различным типам атак.

Ранее авторами [Safonov, Zolotarev, Derben, 2020] была приведена классификация таких атак. Развитие исследований показало, что для различных типов атак могут быть выбраны различные типы реализации, и в некоторых случаях социально-инженерные атаки различных типов [Абрамов и др., 2016] будут иметь высокий уровень значимости. Ниже рассмотрены такие случаи, а также методы определенного противодействия подобному развитию событий.

Кроме того, интересным для авторов представлялся анализ цифрового следа атак. В рамках апробации задавались вопросы об использовании цифрового следа для дообучения участников сетевых геймифицированных проектов безопасному взаимодействию. Такие варианты и алгоритмы анализа также приведены ниже.

Возможности атак также сильно ограничивает применение усиленной аутентификации, протестированной на реальных инструментах инфраструктуры сетевых образовательных проектов.

Результаты исследования. Оценивая возможность противодействия атакам на участников геймифицированных сетевых проектов в области образования, необходимо отталкиваться от следующих их базовых особенностей:

– отказаться от взаимодействия участников внутри проекта нельзя, несмотря на проблемы безопасности, это один из основных факторов реализации такого типа проектов;

– встроенных способов защиты информации для существующих инфраструктур реализации сетевых образовательных проектов недостаточно для противодействия известным типам социально-инженерных атак, таких как фишинг или различные варианты претекстинга;

– открытость участников к воздействию из внешней среды приводит к повышению веро-

ятности реализации атак на образовательные ресурсы.

Если смотреть на задачу противодействия атакам в контексте исследования, то становится понятным, что недостаточно развернуть защитные механизмы. Должна быть обеспечена методика использования образовательной среды, обеспечивающая как уровень безопасного взаимодействия пользователей, так и итоговый эффект в области повышения такого безопасного взаимодействия. Примером среды, на которой авторы проводили апробацию ранее, можно указать Kaspersky Automated Security Awareness Platform (ASAP)[2].

С другой стороны, есть и задача обогащения обучающих задач для участников образовательной среды. Разумным путем здесь видится сбор цифрового следа; но и в этом случае наблюдается очевидное противоречие между снижением безопасности обмена данными за счет возможности атаки на места хранения собранного цифрового следа и необходимостью максимизации его сбора для повышения эффективности обучения. Конечно, можно собирать цифровой след точечно, для отдельных задач.

Схема использования цифрового следа (рис. 1) с точки зрения использования его для повышения устойчивости участников геймифицированных сетевых образовательных проектов к социально-инженерным атакам может выглядеть как набор путей, каждый из которых специализирован на своем типе цифрового следа, что и показано в соответствующем разделе на примере апробации в задаче определения точки входа атаки на определенный вид информационного ресурса проекта.

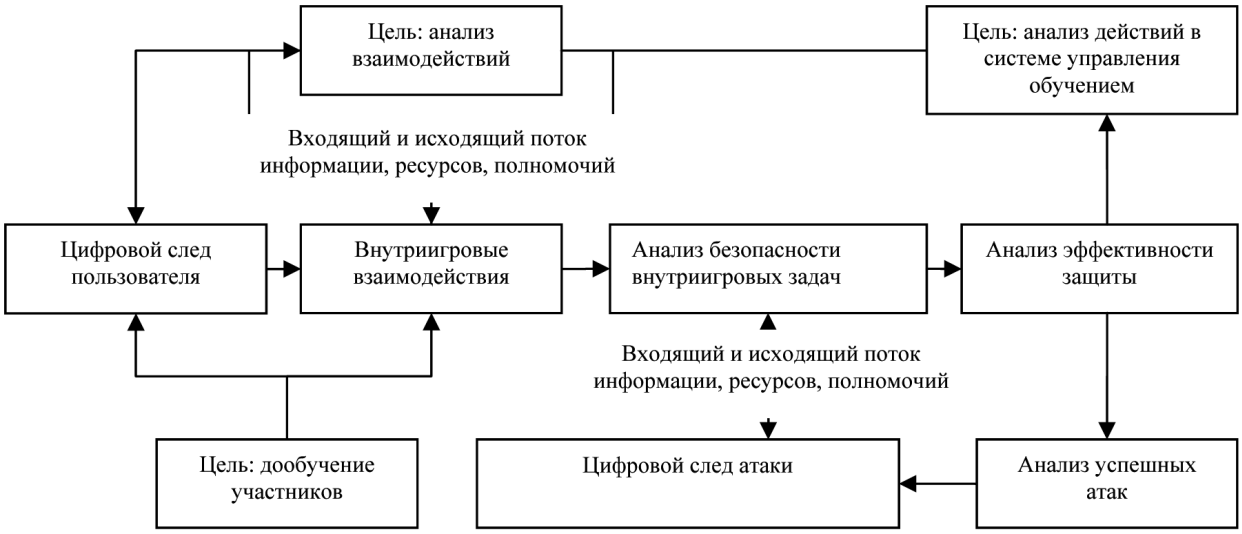

Рис. 1. Схема использования цифрового следа в задаче
Fig. 1. Digital trace collection scheme

Противоречие в использовании цифрового следа решается через разделение его видов. Алгоритм такого использования приведен в экспериментальной части исследования.

Кроме того, можно напомнить, что внутриигровые взаимодействия в геймифицированном проекте также не всегда соблюдают требования безопасности. Игроки могут сознательно или случайно идти на изменение контактов с внешней средой или внутренними ресурсами, несанкционированно кооперировать, нарушать безопасность игровых данных или информационных ресурсов проекта, а также атаковать других игроков. Все это очевидным образом диктует необходимость оценки действий участников образовательного проекта как источников угроз безопасности, а не только как объектов атак.

[2] Kaspersky Automated Security Awareness Platform. URL: https://k-asap.com/ru/ (дата обращения: 01.09. 2021).

ВЕСТНИК КРАСНОЯРСКОГО ГОСУДАРСТВЕННОГО ПЕДАГОГИЧЕСКОГО УНИВЕРСИТЕТА им. В.П. АСТАФЬЕВА

Усиленная аутентификация как способ контроля взаимодействия участников. Рассматривая участников образовательного проекта в качестве источников или объектов атак, необходимо четко различать самого участника и его аккаунт в проекте. По сути, апробация защитных технологий в рамках исследования авторами и начиналась с выделения аккаунта как первичной точки атаки и использования усиленной аутентификации как способа контроля аккаунта.

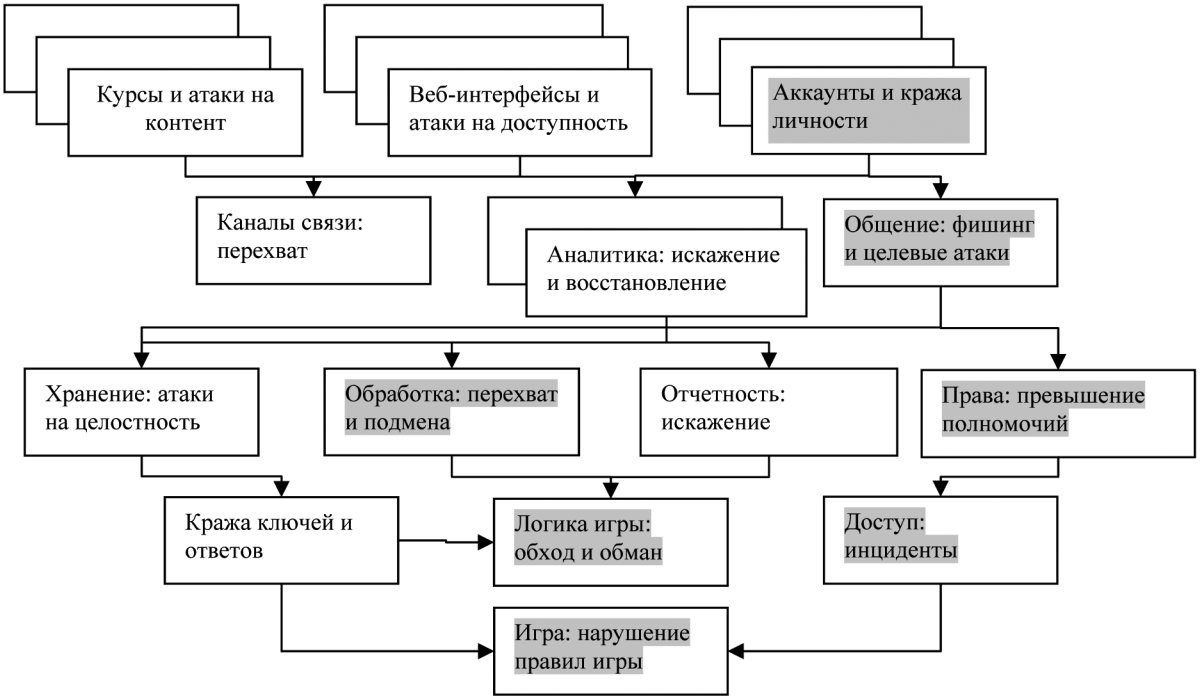

Рис. 2. Противодействие типовым атакам (выделено цветом)
Fig. 2. Resistance to typical attacks (highlighted)

В качестве предпосылок было известно, что однофакторная аутентификация (например, парольная защита) уже не может считаться надежной и применение биометрических методов аутентификации в целом является одним из перспективных направлений развития образовательных систем [Curran, Curran, 2019]. Эксперимент исследования состоял в попытке интеграции усиленных аутентификационных механизмов в систему управления обучением (LMS) Moodle.

Пример противодействия типовым атакам с помощью усиленной аутентификации показан ниже (рис. 2).

Видно, что применение усиленной аутентификации усложняет работу злоумышленника как по внедрению в систему (корень дерева атак), так и атаки внутри игрового пространства (за счет корректного учета его цифрового следа и противодействия).

В Moodle существует механизм, с помощью которого администратор может создавать роли и наделять их определенными правами доступа, следующим этапом является проверка того, действительно ли войти в аккаунт желает его владелец или же это злоумышленник, для реализации данной функции существует несколько вариантов, часть из них уже находится в системе, другая часть требует подключения плагинов. Ниже представлены основные виды аутентификации в Moodle.

1. Вход по логину и паролю (Active Directory и LDAP).
2. Двухфакторная аутентификация.
3. Вход по IP-адресу.
4. Вход с помощью технологий SSO (Single Sign On) между системами.

Технология единого входа (англ. Single Sign-On) — технология, при использовании которой пользователь переходит из одного раздела портала в другой либо из одной системы в другую,

не связанную с первой системой, без повторной аутентификации.

В рамках апробации первичных защитных механизмов была реализована следующая схема (рис. 3). Схему можно реализовать как для случая двухфакторной аутентификации (рассмотренный в исследовании вариант), так и для технологии единого входа в систему.

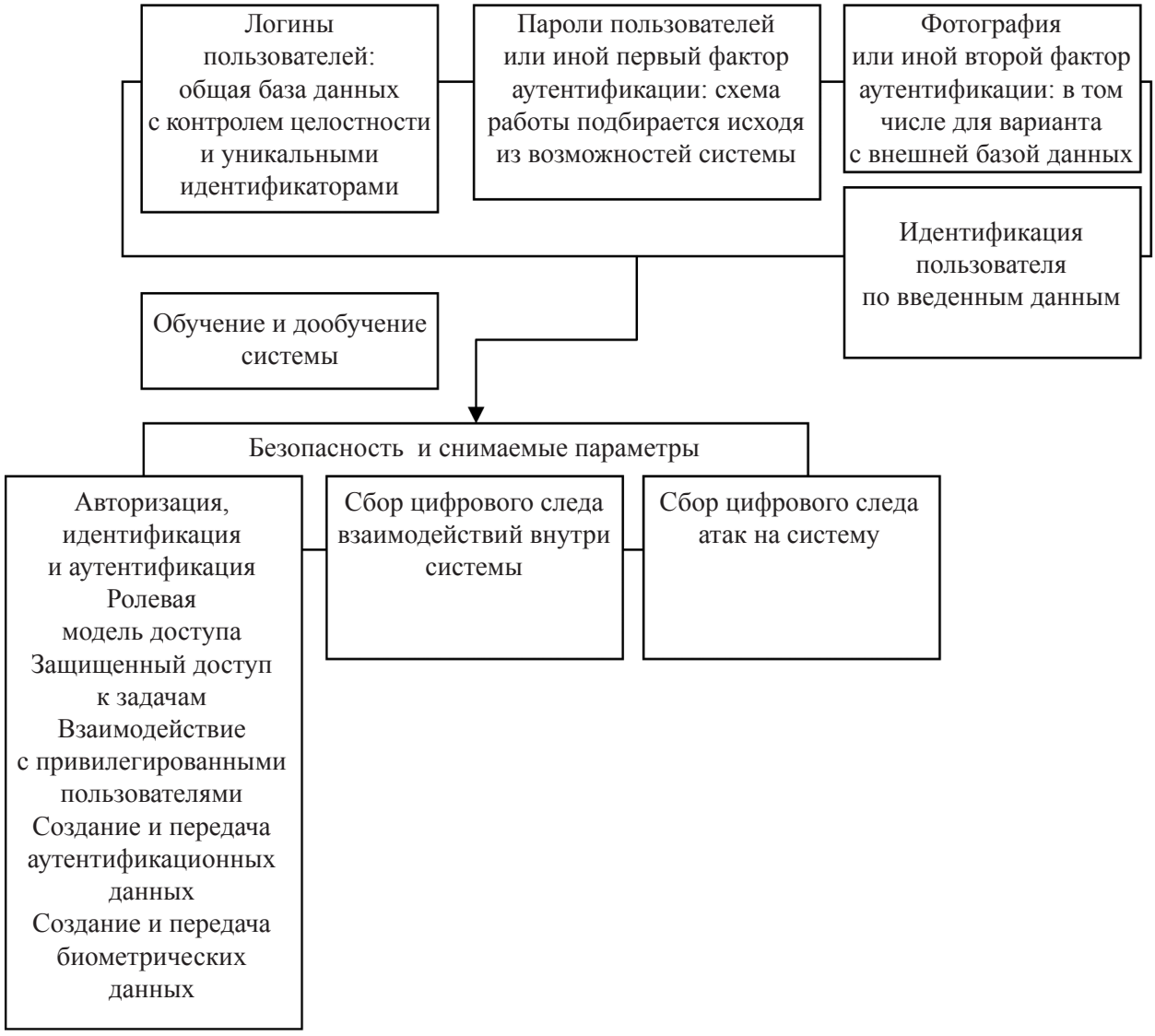

Рис. 3. Схема реализации усиленной аутентификации
Fig. 3. Enhanced authentication implementation scheme

Итогом работы по этому направлению стала возможность управлять доступом участников не опасаясь подмены или кражи аккаунтов, что в реальных сетевых проектов является серьезной опасностью.

Алгоритм работы с цифровым следом. Рассматривая варианты использования разного вида цифрового следа, исследование сосредоточивается на эффекте дообучения пользователей для противодействия возможным атакам на них. Выглядит это как набор возможностей, реализованных через различные точки контроля защитных подсистем. Формируя цифровой след для дообучения пользователей, можно сосредоточиться как на особенностях атак, так и на небезопасном взаимодействии самих пользователей.

Далее покажем пример сбора цифрового следа в задаче определения точки входа атаки при воздействии на систему управления обучением (рис. 4).

ВЕСТНИК КРАСНОЯРСКОГО ГОСУДАРСТВЕННОГО ПЕДАГОГИЧЕСКОГО УНИВЕРСИТЕТА им. В.П. АСТАФЬЕВА

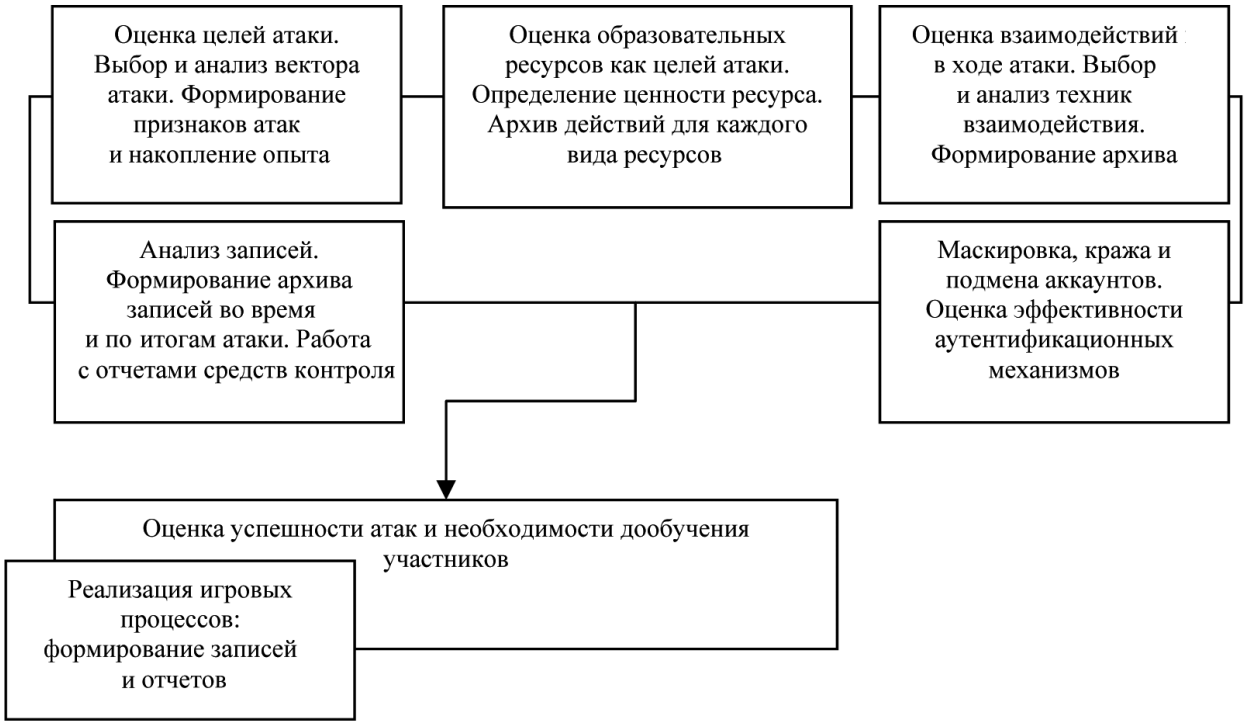

Рис. 4. Сбор цифрового следа при определении точки входа атаки
Fig. 4. Digital trace collection for attack entry point identification

Как видно в примере, сбор цифрового следа может быть не только описан, но и алгоритмизирован на техническом уровне, приемлемом для реализации в образовательной системе, что через обучение может позволить постоянно повышать осведомленность пользователей о такого типа атаках, а также совершенствовать непосредственно защиту информации образовательного ресурса.

Заключение. Основной уязвимой стороной сетевого геймифицированного проекта, как показано в статье, является взаимодействие пользователей. С точки зрения педагогической технологии опасность может представлять такая реализация принципа открытости, которая подразумевает свободное участие в жизни проекта ссылок и фрагментов информации из «внешнего мира», а также отсутствие контроля за внутренними и внешними связями. В статье показано, как реализовать определенные защитные техники, позволяющие минимизировать возможности атакующего и использовать данные атак для повышения устойчивости пользователей к их повторению.

Библиографический список

1. Абрамов М.В. и др. Модель профиля компетенций злоумышленника в задаче анализа защищенности персонала информационных систем от социоинженерных атак / Абрамов М.В., Азаров А.А., Тулупьева Т.В. и др. // Информационно-управляющие системы. 2016. № 4 (83). С. 77–84. DOI: 10.15217/issn1684-8853.2016.4.77
2. Есин Р.В., Вайнштейн Ю.В. Геймификация в электронной среде как средство вовлечения студентов в образовательный процесс // Открытое и дистанционное образование. 2017. № 2 (66). С. 26–32. URL: https://www.elibrary.ru/item.asp?id=29443397 (дата обращения: 01.09.2021).
3. Караваев Н.Л., Соболева Е.В. Совершенствование методологии геймификации учебного процесса в цифровой образовательной среде: монография. Киров: Вятский государственный университет, 2019. 105 с. URL: https://www.elibrary.ru/download/elibrary_42436675_71534097.pdf (дата обращения: 01.09.2021).

4. Перевозчикова М.С., Ренжина А.А. Проектирование и создание персонально ориентированной образовательной среды с элементами геймификации // Личность в культуре и образовании: психологическое сопровождение, развитие, социализация: матер. Всерос. научн.-практ. конф. 2019. № 7. С. 506–513. URL: https://www.elibrary.ru/download/elibrary_42461263_70631844.pdf (дата обращения: 01.09.2021).
5. Полякова В.А., Козлов О.А. Воздействие геймификации на информационно-образовательную среду школы // Современные проблемы науки и образования. 2015. № 5. С. 513. URL: https://www.elibrary.ru/download/elibrary_32664400_59116799.pdf (дата обращения: 01.09.2021).
6. Ali Zani A., Norman A., Ghani N. A review of security awareness approaches: Towards achieving communal awareness. In: A. Ali Zani, A. Norman, N. Ghani “Cyber Influence and Cognitive Threats”. Academic Press, 2020. P. 97–127. URL: https://aisel.aisnet.org/pacis2018/278 (дата обращения: 13.04.2020).
7. Beckers K., Pape S. A Serious game for eliciting social engineering security requirements. In: Proceedings of 24th International Requirements Engineering Conference (RE) “2016 IEEE”. 2016. DOI: 10.1109/RE.2016.39
8. Curran J., Curran K. Biometric authentication techniques in online learning environments. In: Biometric Authentication in Online Learning Environments / ed. by A.V. Senthil Kumar. IGI Global, 2019. P. 266–278. DOI: http://doi:10.4018/978-1-5225-7724-9.ch011
9. Hart S., Margheri A., Paci F., Sassone V. Riskio: A serious game for cyber security awareness and education // Computers & Security. 2020. Vol. 95. P. 101827. DOI: 10.1016/j.cose.2020.101827
10. Jin G., Tu M., Kim T.-H., Heffron J., White J. Game based cybersecurity training for high school students. In: Proceedings of the 49th ACM Technical Symposium on Computer Science Education “SIGCSE’18”. 2018. P. 68–73. DOI: 10.1145/3159450.3159591
11. Liu L., Yasin A., Li T., Fatima R., Wang J.Improving software security awareness using a serious game. In: IET Software, 2018. DOI: 10.1049/iet-sen.2018.5095
12. Safonov K., Zolotarev V., Derben A. Analysis of attack strategies on game resources for technological processes training games // IOP Conference Series: Materials Science and Engineering. 2020. Is. 822 (1). P. 012027.
13. Tang S., Hanneghan M. A Model-driven framework to support development of serious games for game based learning. In: Proceedings of the 3rd International Conference on Developments in e-Systems Engineering. London, UK. 2010. DOI: 10.1109/DeSE.2010.23
14. Trickel E., Disperati F., Gustafson E. et al. Shell we play a game? CTF-as-a-service for Security Education. In: Proceedings of the USENIX Workshop on Advances in Security Education (ASE), 2017. URL: https://www.researchgate.net/publication/319141725_Shell_We_Play_A_Game_CTF-as-a-service_for_Security_Education (дата обращения: 10.04.2020).
15. Yasin A., Liu L., Li T., Wang J., Zowghi D. Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG) // Information and Software Technology. 2018. Is. 95. P. 179–200. DOI: 10.1016/j.infsof.2017.12.002

DOI: https://doi.org/10.25146/1995-0861-2021-57-3-290

TESTING OF INCREASING RESISTANCE TO ATTACKS WHEN INTERACTING WITH PARTICIPANTS OF NETWORK GAMIFIED EDUCATIONAL PROJECTS ON INFORMATION SECURITY

K.V. Safonov (Krasnoyarsk, Russia)
V.V. Zolotarev (Krasnoyarsk, Russia)
E.A. Maro (Taganrog, Russia)
E.A. Ishchukova (Taganrog, Russia)
E.Yu. Zolotareva (Krasnoyarsk, Russia)

Abstract

Statement of the problem. The article deals with issues related to secure interaction within a gamified educational environment, in particular in the field of game cases used for information security training. Various approaches to collecting the digital footprint of social engineering attacks and ways to increase resistance to attacks in the field of social engineering based on the analysis of the digital footprint are presented. Estimates and algorithms of actions that increase the resistance to these attacks of participants in network gamified projects are also shown, and their approbation is described.

The purpose of the article is to search for an approach to improving secure interaction in gamified network educational projects.

The research methodology consists of the analysis of current gaming practices in the framework of information security training; the study of the results of interdisciplinary research by Russian and foreign scientists on the use of gamification in various training tasks, game environments and solutions, and their evaluation.

Research results. Author's recommendations for increasing the resistance of participants in network gamified educational projects to social engineering attacks are developed, algorithms and procedures for performing this task are shown, and their approbation is described.

Conclusion. According to the results of the assessment given in the article, the possibility of using the digital footprint collection to improve the security of the implementation of the interaction of participants in network gamified projects is shown. The author's recommendations considered in the article can be applied during the training of masters in the field of specialization: 10.04.01 Information security (full-time education).

Keywords: *training, information security, serious games, gamification, phishing, social network, digital trace*.

Safonov Konstantin V. – DSc (Physics and Mathematics), Professor, Head of the Department of Applied Mathematics, Reshetnev Siberian State University of Science and Technology (Krasnoyarsk); ORCID: http://orcid.org/0000-0003-0405-3065; e-mail: safonovkv@rambler.ru
Zolotarev Vyacheslav V. – PhD (Technology), Associate Professor, Head of the Department of IT Security, Reshetnev Siberian State University of Science and Technology (Krasnoyarsk); ORCID: http://orcid.org/0000-0002-8054-8564; e-mail: amida.2@yandex.ru
Maro Ekaterina A. – PhD (Technology), Associate Professor, Department of IT Security, South Federal University (Taganrog, Russia); ORCID: http://orcid.org/0000-0001-5136-7804; e-mail: marokat@gmail.com
Ischukova Evgenia A. – PhD (Technology), Associate Professor, Department of IT Security, South Federal University (Taganrog, Russia); ORCID: http://orcid.org/0000-0002-6818-1608; e-mail: jekky82@mail.ru
Zolotareva Elena Yu. – Engineer, Department of IT Security, Reshetnev Siberian State University of Science and Technology (Krasnoyarsk); e-mail: umka.82@mail.ru

References

1. Abramov M.V., Azarov A.A., Tulupyeva T.V. et al. Model of the attacker's competence profile in the task of analyzing the security of information systems personnel from socio-engineering attacks // Informatsionno-upravlyayushchie sistemy (Information Management Systems). 2016. No. 4 (83). P. 77–84. DOI: 10.15217/issn1684-8853.2016.4.77

2. Esin R.V., Weinstein Yu.V. Gamification in the electronic environment as a means of involving students in the educational process // Otkrytoe i distantsionnoe obrazovanie (Open and Distance Education). 2017. No. 2 (66). P. 26–32.
3. Karavaev N.L., Soboleva E.V. Improving methodology of gamification of an educational process in digital educational environment: monograph. Kirov: Vyatka State University, 2019. 105 p.
4. Perevozchikova M.S., Renzhina A.A. Designing and creating a person-oriented educational environment with elements of gamification. In: Proceedings of the All-Russian Scientific and practical conference “Personality in culture and education: psychological support, development, socialization”. 2019. No. 7. P. 506–513.
5. Polyakova V.A., Kozlov O.A. The impact of gamification on the information and educational environment of a secondary school // Sovremennye problemy nauki i obrazovaniya (Modern Problems of Science and Education). 2015. No. 5. P. 513.
6. Ali Zani A., Norman A., Ghani N. A review of security awareness approaches: Towards achieving communal awareness. In: A. Ali Zani, A. Norman, N. Ghani “Cyber Influence and Cognitive Threats”. Academic Press, 2020. P. 97–127. URL: https://aisel.aisnet.org/pacis2018/278 (access date: 13.04.2020).
7. Beckers K., Pape S. A Serious game for eliciting social engineering security requirements. In: Proceedings of 24th International Requirements Engineering Conference (RE) “2016 IEEE”. 2016. DOI: 10.1109/RE.2016.39
8. Curran J., Curran K. Biometric authentication techniques in online learning environments. In: Biometric Authentication in Online Learning Environments / ed. by A.V. Senthil Kumar. IGI Global, 2019. P. 266–278. DOI: http://doi:10.4018/978-1-5225-7724-9.ch011
9. Hart S., Margheri A., Paci F., Sassone V. Riskio: A serious game for cyber security awareness and education // Computers & Security. 2020. Vol. 95. P. 101827. DOI: 10.1016/j.cose.2020.101827
10. Jin G., Tu M., Kim T.-H., Heffron J., White J. Game based cybersecurity training for high school students. In: Proceedings of the 49th ACM Technical Symposium on Computer Science Education “SIGCSE’18”. 2018. P. 68–73. DOI: 10.1145/3159450.3159591
11. Liu L., Yasin A., Li T., Fatima R., Wang J. Improving software security awareness using a serious game. In: IET Software, 2018. DOI: 10.1049/iet-sen.2018.5095
12. Safonov K., Zolotarev V., Derben A. Analysis of attack strategies on game resources for technological processes training games // IOP Conference Series: Materials Science and Engineering. 2020. Is. 822 (1). P. 012027.
13. Tang S., Hanneghan M. A Model-driven framework to support development of serious games for game based learning. In: Proceedings of the 3rd International Conference on Developments in e-Systems Engineering. London, UK. 2010. DOI: 10.1109/DeSE.2010.23
14. Trickel E., Disperati F., Gustafson E.et al. Shell we play a game? CTF-as-a-service for Security Education. In: Proceedings of the USENIX Workshop on Advances in Security Education (ASE), 2017. URL: https://www.researchgate.net/publication/319141725_Shell_We_Play_A_Game_CTF-as-a-service_for_Security_Education (access date: 10.04.2020).
15. Yasin A., Liu L., Li T., Wang J., Zowghi D.Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG) // Information and Software Technology. 2018. Is. 95. P. 179–200. DOI: 10.1016/j.infsof.2017.12.002