DOI: https://doi.org/10.25146/1995-0861-2020-52-2-201

УДК 378:811

ОЦЕНКА УЯЗВИМОСТИ К ФИШИНГУ УЧАСТНИКОВ СЕТЕВЫХ ГЕЙМИФИЦИРОВАННЫХ ОБРАЗОВАТЕЛЬНЫХ ПРОЕКТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ[1]

К.В. Сафонов (Красноярск, Россия)
В.В. Золотарев (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. Основные угрозы, рассмотренные ниже, это реализация различных типов фишинговых атак, показаны экспериментальные данные по оценке некоторых параметров групп проекта, реализованных в социальной сети. Также приведен алгоритм действий при оценке уязвимости участников сетевых геймифицированных проектов к фишинговым атакам.

Цель исследования ориентирована на разработку подхода к оценке опасности фишинга как способа разрушения или негативного использования группового взаимодействия с точки зрения информационной безопасности, применимого для проектов в форме кейс-стади.

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

Результаты. Разработаны авторские рекомендации по оценке уязвимости участников сетевых геймифицированных образовательных проектов к фишинговым атакам, выполнен обзор связанных работ и противоречий, показаны ограничения.

Заключение. По результатам проведенного эксперимента показано, что сетевое взаимодействие может быть оценено, а итоги оценки использованы для прогнозирования развития фишинговых атак в сетевых геймифицированных образовательных 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, serious games, геймификация, фишинг, социальная сеть.*

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. Ранее авторами были рассмотрены несколько примеров игровых сред с использованием социальной сети как инструмента взаимодействия [Tang, Hanneghan, 2010; Jin et al., 2018] 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; Zani et al., 2018]. Во всех этих случаях авторы не увидели существенных усилий по обеспечению информационной безопасности, что, вероятно, может и приведет к уязвимости этих проектов к различным типам атак.

[1] Работа поддержана Российским фондом фундаментальных исследований, проект № 19-013-00711.

Ранее [Safonov et al., 2019] авторами была приведена классификация таких атак. Одной из наиболее значимых атак на игровую среду представляется реализация фишинговой атаки как с использованием механизмов самой игровой среды (от кражи аккаунтов до внутренней системы сообщений), так и с использованием внешних инструментов (таких, как социальная сеть или сеть учреждения, где работают или учатся включенные в проект студенты и преподаватели). Основные виды фишинговых атак описаны, например, в работе [Kang et al., 2018].

Известно, что при этом, несмотря на развитость и многовариантность способов воздействия на участников геймифицированного проекта, различные способы обеспечения информационной безопасности могут повлиять негативно на его успешность. Возможность применения тех или иных решений должна учитывать не только упомянутый выше основной принцип открытости образовательного процесса, но и возможности его участников, в том числе технические, социальные, психологические, а также условия его реализации.

Цель статьи – разработать подход к оценке опасности фишинга как способа разрушения или негативного использования группового взаимодействия с точки зрения информационной безопасности, применимого для проектов в форме кейс-стади или игровых решений, широко использующих информационные технологии, разрабатываемых несколькими взаимодействующими студенческими командами через социальную сеть.

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

В качестве основы для эксперимента был использован ряд проектов, завершенных или продолжаемых авторами при поддержке Фонда Потанина в 2015–2020 гг. в области обучения информационной безопасности, а также ряд исследований зарубежных и российских ученых в этой области.

Обзор научной литературы. Поставленная цель учитывает несколько базовых особенностей геймификации как средства повышения активности в сетевых проектах. В первую очередь – это уязвимость отдельных элементов игрового процесса и, как следствие, возможность их использования для нарушения безопасности информационного взаимодействия. Вместе с тем, использование игровых механик также должно быть обеспечено, поскольку оно и является основой геймификации, а защищенность отдельных компонентов и всего процесса только вторичная задача.

Ранее авторами были рассмотрены мотивационные аспекты реализации защищенности в образовательном процессе. Это важная и, безусловно, интересная составляющая управления геймификацией; здесь же предлагается сосредоточиться на тех механизмах, которые могут оказать негативное влияние как на весь проект, так и на его участников.

Известно, что социальная сеть как инструмент взаимодействия вносит много дополнительных проблем в любой сетевой проект. Среди них можно выделить:

– несанкционированную кооперацию участников (с любой целью, как нарушающей игровую логику, так и реализующей противоправные действия). Сюда можно отнести рассматриваемый в работе фишинг;

– подмена и удаление (уничтожение) аккаунтов участников сетевого проекта как способ внедрения в проект третьих лиц или нарушения его функционирования;

– подавление потоком внешней информации участников проекта, снижение вовлеченности, интенсивности обмена информацией;

– использование ресурсов проекта для несвязанных с его основной задачей (задачами) действий и т.д.

М.А. Басараб и др. рассматривают аспекты обнаружения противоправной деятельности в киберпространстве на основе анализа социальных сетей [Басараб и др., 2016]. Авторы работы сосре-

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

доточены на инструментальной полезности тех или иных алгоритмов, что может быть важным для реализации отдельных элементов представленного исследования. Также хороший обзор методов обнаружения угроз информационной безопасности с использованием социальных сетей представлен в работе Л. Кириченко и соавторов [Кириченко и др., 2017]. М.В. Абрамов в своих работах рассматривает в том числе такие показатели моделей пользователя и злоумышленника в ходе реализации фишинговых атак, как знание архитектуры системы, возможности и владение определенными типами атак, а в случае пользователей – и владение (возможность доступа) основными ресурсами системы [Абрамов и др., 2016].

Все указанные выше инструменты должны использоваться с учетом особенностей геймификации. Противоречие с принципом открытости проявляется здесь следующим образом: учитывая, что геймификация порождает новые угрозы безопасности, особенно при использовании социальной сети как инструмента взаимодействия, она неизбежно должна приводить к изменению образовательного процесса, дополнению его новыми функциями, ограничивающими или контролирующими, прогнозирующими и анализирующими взаимную активность участников. Такие функции могут в том числе запрещать определенные взаимодействия участников проекта как внутри коллабораций, так и с внешним миром. К примеру, использование в обучении открытых задач может привести к повышению риска негативного воздействия на участника проекта как во время поиска информации (и дополнения найденной информацией баз данных проекта), так и во время взаимодействий для решения задач.

Результаты. Итак, в согласии с предыдущими работами авторы рассматривают геймификацию в сетевой форме как некоторый уровень взаимодействия, коллаборации различных групп, взаимодействующих через социальную сеть. Если же учитывать ограничения, связанные с фишинговыми атаками, то целесообразно представлять указанные коллаборации в виде ориентированных графов, в том числе имеющих веса отдельных ребер и вершин (социальных графов) [Басараб и др, 2016]. Для формирования ограничений в таких проектах могут использоваться различные метрики, как простые, так и сложные (табл. 1).

Таблица 1

Метрики взаимодействия в сетевом геймифицированном проекте

Table 1

Interaction metrics in a network gamified project

Метрика	Способ оценки	Применение
1	2	3
Простые метрики		
Количество и сложность связей	Оценка количества и качества связей участников проекта	Выделение узлов социального графа, отвечающих за ключевые взаимодействия, обеспечение защиты выделенных ключевых узлов, работа с участниками, обеспечивающими ключевые взаимодействия
Интенсивность	Оценка интенсивности использования связей участников проекта	Простая метрика, позволяющая оценить активность участника, его вовлеченность в решение задач проекта в текущий момент времени
Метрики вершин и связей социального графа		
Усредненная степень вершины	Количество смежных вершин, нормированных на максимально возможное их количество	В статье [Басараб, 2016] отмечается, что усредненная степень вершины может определять информационное влияние в своей окрестности; для атакующего при фишинговой атаке это означает возможность повышения доверия к распространяемой информации
Промежуточность	Оценка количества кратчайших путей между узлами социального графа, проходящими через оцениваемый узел	Перехват управления или воздействие на узел с высокой промежуточностью в сетевом проекте будет означать нарушение связности; каждый обучающийся воспринимает такой узел как постоянный источник информации о проекте

Окончание табл. 1

1	2	3
Собственный вектор	Определяет, насколько хорошо узел связан с другими узлами	В сетевом проекте узлы с высокой метрикой собственных векторов могут быть полезны атакующему как участники, имеющие высокий потенциальный вес в реализации решений внутри проекта
Относительная важность (PageRank)	Сравнивает составляющие (элементы) проекта, реализованные в форме групп, ссылок и ресурсов, по частоте и способу их использования участниками	В сетевом проекте ресурсы и страницы социальной сети, принадлежащие участникам и имеющие высокую относительную важность, могут быть использованы для атак как подмены, так и фальсификации; через них может распространяться информация, полезная злоумышленнику

Простые метрики могут быть использованы для оценки потенциальной пригодности аккаунта участника (или самого участника) для организатора фишинговой атаки. Примеры такой экспресс-оценки будут показаны ниже, в экспериментальной части работы.

Как можно видеть, использовать указанные в табл. 1 метрики достаточно просто в рамках любого геймифицированного процесса, реализованного через социальную сеть. В данном случае главной задачей при анализе будет являться сбор данных.

Фишинговые атаки разных типов на участников сетевых проектов, реализованных с использованием социальной сети, по-видимому являются неизбежным злом, избежать которого нельзя. При этом возможно сгенерировать такой набор действий участников проекта, который будет усложнять или максимально исключать действия, удобные атакующему.

Необходимо отметить, что при генерации таких положительных изменений может быть изменена временная или пространственная структура коллабораций в сетевом геймифицированном проекте, а также задействованы или прекращены логические связи.

Алгоритм оценки уязвимости участников при реализации фишинговой атаки в сетевых геймифицированных проектах может выглядеть следующим образом.

1. Определение модуля или подпроцесса, требующего повышения безопасности взаимодействия игроков и / или организаторов.

2. Определение задач, решаемых модулем или процессом, определенным на шаге 1.

3. Эмпирическая оценка параметров и метрик, пригодных для оценки уязвимости участников (аккаунтов участников в социальной сети) геймифицированного сетевого проекта к фишинговым атакам.

3а. Оценка «простых» метрик, таких как количество друзей и подписчиков, сформированность сильных (родственники) и слабых (проживают в одном городе и т.п.) связей, оценка интенсивности обмена информацией. В экспериментальной части показано, какие значения параметров могут свидетельствовать об уязвимости участника (или о пригодности его как цели атаки; это не всегда говорит об успешности атаки, так что уязвимость может пониматься как слабое место проекта, которым злоумышленник еще должен суметь воспользоваться).

3б (при необходимости). Оценка «сложных» метрик, работа с социальным графом, уточнение возможных путей и вторичных (третичных и т.д.) целей фишинговой атаки.

4. Оценка качественного наполнения связей участник – ресурс для выяснения дополнительной мотивации злоумышленника при реализации фишинговой атаки.

5. (при необходимости). Дополнение модели участника средствами защиты от фишинговых атак, которые реализует сам участник или социальная сеть. Необходимо понимать, что пессимистичная постановка задачи (атака возможна, несмотря на средства защиты) всегда полезнее оптимистичной.

6. Закрепление оценочных механизмов для противодействия фишингу в игровой среде, реконфигурация связей, повышение

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

эффективности образовательного процесса с учетом реализованных мер защиты.

Ограничивающими показателями в случае реализации данного алгоритма будут сложность связей, количество ресурсов и участников, динамика изменения связей и добавления (удаления) вершин социального графа. Наиболее пригоден данный алгоритм для сетевых проектов с небольшим (до 150 человек) количеством основных участников. В экспериментальной части рассматривается как раз такой проект, в среднем за год привлекавший 100–120 участников, причем рассмотрено его основное ядро – организаторы проекта.

Как уже упоминалось ранее, в качестве основы для эксперимента были использованы данные по серии сетевых проектов, которые были реализованы в Сибирском государственном университете науки и технологий им. М.Ф. Решетнева в 2015–2020 гг. В проектах, поддержанных Благотворительным фондом В. Потанина, принимало участие в среднем 100–120 человек за цикл (1–1,5 года), студенты и преподаватели 6 российских университетов (в единичных случаях еще 1–2 университета). В числе основных организаторов на настоящий момент значится 32 человека – основное управляющее ядро проекта.

Для анализа и сопоставления данных использовались сведения группы проекта SEQuest в социальной сети ВКонтакте, данные экспериментов представлены обезличенно.

Метрики оценивались для организаторов проекта. Где это возможно и необходимо, даются пояснения, характеризующие применимость метрики и ее полезность для решения задачи исследования в данном случае. Приведены соотношения, характеризующие количество уязвимых участников.

Таблица 2

Метрики взаимодействия в сетевом геймифицированном проекте: оценка

Table 2

Interaction metrics in a network gamified project: evaluation

Метрика	Способ оценки	Применение
Простые метрики		
Количество и сложность связей	100 % участников (32) связаны непосредственно хотя бы через одного участника проекта; 93,75 % (30) указаны в друзьях хотя бы у одного участника проекта; 15 % участников имеют число друзей около 150 (что потенциально указывает на странички, используемые для социальных связей); 15 % – рабочие странички с числом друзей существенно больше 150; оставшиеся имеют среднее число друзей 300–320, что говорит о высоком числе неактивных связей этих участников	Выделение связей и характеристик узлов указывает на общую уязвимость группы для различных типов атак; для конкретного участника такая оценка тоже может быть полезной
Интенсивность	Высокоинтенсивных связей среди участников проекта 21,87 % (исключая общение вне соцсети). Неактивных связей 18,75 %	Срез активности связей показывает, насколько вовлечен участник в решение текущих задач проекта, а также, как быстро распространяется в проекте информация
Метрики вершин и связей социального графа		
Усредненная степень вершины	Вершин с высокой усредненной степенью для проекта 9,37 %	Метрика указывает точки входа для атакующего
Промежуточность	Количество вершин с высокой промежуточностью для проекта 6,25 %	Возможности развития атаки для исследуемой группы ограничены
Собственный вектор	Количество вершин с высоким значением метрики собственных векторов 18,75 %	Существует несколько альтернативных путей влияния на решения внутри проекта

На первом этапе эксперимента оценивалось, насколько влияние отдельных метрик может быть значимым для прогнозирования атаки. По ходу эксперимента было определено, что для отдельных метрик прогноз не может быть достаточно точным, а вот использование одновременно «простых» и «сложных» метрик с высокой точностью определяет точку входа атаки и уязвимые узлы.

Вычисление важности ресурсов было визуализировано (без указания персональных данных) следующим образом (рис.).

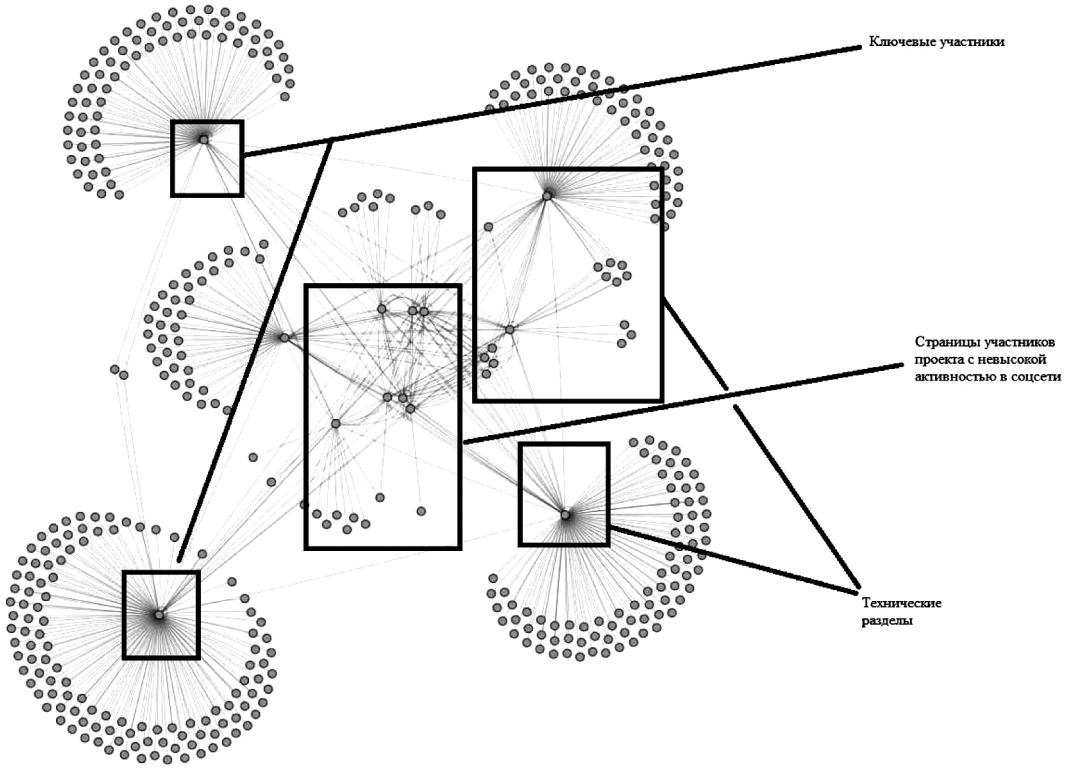

Рис. Визуализация внутреннего PageRank группы проекта
Fig. Visualization of the project group's internal PageRank

Из рисунка видно, что применение защитных мер в общем случае может быть достигнуто без радикальной переработки модели взаимодействия пользователей. Этого можно добиться за счет активизации защитных мер, направленных на несколько ключевых узлов влияния (с учетом того, что для данной группы часть узлов влияния – технические составляющие социальной сети, типа группы поддержки), а также отработки мер, направленных на внутреннее ядро группы, состоящее из малоинтенсивных связей.

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. Тем не менее даже на показанном ограниченном объеме примеров видно, что возможности для прогнозирования фишинговых атак на участников сетевых геймифицированных проектов существуют и реализуемы.

Библиографический список

1. Абрамов М.В., Азаров А.А., Тулупьева Т.В. и др. Модель профиля компетенций злоумышленника в задаче анализа защищенности персонала информационных систем от социоинженерных атак // Информационно-управляющие системы. 2016. № 4 (83). С. 77–84. DOI: 10.15217/issn1684-8853.2016.4.77

2. Басараб М.А., Иванов И.П., Колесников А.В., Матвеев В.А. Обнаружение противоправной деятельности в киберпространстве на основе анализа социальных сетей: алгоритмы, методы и средства (обзор) // Вопросы кибербезопасности. 2016. Вып. 4 (17). С. 11–19. DOI: 10.21681/2311-3456-2016-4-11-19
3. Кириченко Л., Радивилова Т., Барановский А. Обнаружение киберугроз с помощью анализа социальных сетей // Information technologies & knowledge. 2017. Vol. 11, No. 1. P. 23–48. URL: https://www.researchgate.net/publication/320233252_OBNARUZENIE_KIBERUGROZ_S_POMOSU_ANALIZA_SOCIALNYH_SETEJ (дата обращения: 01.05.2020).
4. Beckers K., Pape S. A Serious game for eliciting social engineering security requirements. In: Proceedings of the 2016 IEEE 24th International Requirements Engineering Conference (RE), 2016. DOI: 10.1109/RE.2016.39
5. 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
6. Jin G., Tu M., Kim T.-H., Heffron J., White J. Game based cybersecurity training for high school students. In: SIGCSE ‘18 Proceedings of the 49th ACM Technical Symposium on Computer Science Education. P. 68–73. DOI: 10.1145/3159450.3159591
7. Kang L., Chek K., Choon, L. A survey of phishing attacks: Their types, vectors and technical approaches // Expert Systems with Applications. 2018. No. 106. P. 1–20. DOI: 10.1016/j.eswa.2018.03.050
8. 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
9. Safonov K., Zolotarev V., Derben A. Analysis of attack strategies on game resources for technological processes training games. In: Proceedings of the IOP Conference series, 2019 [in press].
10. 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
11. Trickel E., Disperati F., Gustafson E. Shall 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).
12. 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. № 95. P. 179–200. DOI: 10.1016/j.infsof.2017.12.002
13. Zani A.A.A., Norman A.A., Ghani N. A review of security awareness approaches: Towards achieving communal awareness / Ed. by V. Benson, J. Mcalaney. In: PACIS 2018 Proceedings «Cyber influence and cognitive threats». Academic Press, 2018. P. 97–127. URL: https://aisel.aisnet.org/pacis2018/278 (дата обращения: 13.04.2020).

DOI: https://doi.org/10.25146/1995-0861-2020-52-2-201

ASSESSMENT OF PARTICIPANTS VULNERABILITY TO PHISHING WITHIN NETWORK GAMIFIED PROJECTS IN THE FIELD OF INFORMATION SECURITY

K.V. Safonov (Krasnoyarsk, Russia),
V.V. Zolotarev (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. The main threats discussed below are the implementation of various types of phishing attacks. Experimental data are shown on the evaluation of some parameters of project groups implemented in the social network. An algorithm for evaluating the vulnerability of participants in network gamified projects to phishing attacks is also provided.

The purpose of the article is focused on developing an approach to assessing the danger of phishing as a way to destroy or negatively use group interaction from the point of view of information security applicable to case study projects.

The research methodology consists of an 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 assessing the vulnerability of participants in network gamified educational projects to phishing attacks were developed, a review of related works and contradictions was performed, and restrictions were shown.

Conclusion. Based on the results of the experiment, it is shown that network interaction can be evaluated, and the results of the evaluation can be used to predict the development of phishing attacks in network gamified educational projects. The author's recommendations considered in the article can be applied during the training of masters in the field of training: 10.04.01 Information security (full-time training).

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

References

1. Abramov M.V., Azarov A.A., Tulupeva T.V. et al. The model of the attacker's competence profile in the task of analyzing the security of information systems personnel from socioengineering attacks // Informatsionno-upravlyayushchie sistemy (Information management systems). 2016. No. 4 (83). P. 77–84.
2. Basarab M.A., Ivanov I.P., Kolesnikov A.V., Matveev V.A. Detection of illegal activity in cyberspace based on the analysis of social networks: algorithms, methods and tools (review) // Voprosy kiberbezopasnosti (Questions of cybersecurity). 2016. No. 4(17). P. 11–19.
3. Kirichenko L., Radivilova T., Baranovsky A. Detection of cyber threats using social network analysis // Information technologies & knowledge. 2017. Vol. 11, No. 1. P. 23–48.
4. Beckers K., Pape S. A Serious game for eliciting social engineering security requirements. In: Proceedings of the 2016 IEEE 24th International Requirements Engineering Conference (RE), 2016. DOI: 10.1109/RE.2016.39
5. 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
6. Jin G., Tu M., Kim T.-H., Heffron J., White J. Game based cybersecurity training for high school students. In: SIGCSE '18 Proceedings of the 49th ACM Technical Symposium on Computer Science Education. P. 68–73. DOI: 10.1145/3159450.3159591
7. Kang L., Chek K., Choon, L. A survey of phishing attacks: Their types, vectors and technical approaches // Expert Systems with Applications. 2018. No. 106. P. 1–20. DOI: 10.1016/j.eswa.2018.03.050
8. Liu L., Yasin A., Li T., Fatima R., Wang J. Improving software security awareness using

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

a serious game. In: IET Software, 2018. DOI: 10.1049/iet-sen.2018.5095

9. Safonov K., Zolotarev V., Derben A. Analysis of attack strategies on game resources for technological processes training games. In: Proceedings of the IOP Conference series, 2019 [in press].
10. 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
11. Trickel E., Disperati F., Gustafson E. Shall 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).
12. 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. No. 95. P. 179–200. DOI: 10.1016/j.infsof.2017.12.002
13. Zani A.A.A., Norman A.A., Ghani N. A review of security awareness approaches: Towards achieving communal awareness / Ed. by V. Benson, J. Mcalaney. In: PACIS 2018 Proceedings “Cyber influence and cognitive threats”. Academic Press, 2018. P. 97–127. URL: https://aisel.aisnet.org/pacis2018/278 (access date: 13.04.2020).