DOI: https://doi.org/10.25146/1995-0861-2019-49-3-145

**УДК 378:811**

# ОБЕСПЕЧЕНИЕ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ СТУДЕНТОВ – УЧАСТНИКОВ СЕТЕВЫХ ГЕЙМИФИЦИРОВАННЫХ ПРОЕКТОВ[1]

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

**Аннотация**

В статье рассматриваются вопросы, связанные с защищенным взаимодействием внутри геймифицированной образовательной среды, в частности в области игровых кейсов, применяемых для обучения информационной безопасности. Рассмотрены основные угрозы – воздействие на контент и кража аккаунтов, показаны экспериментальные данные по сравнению сетевого и локального взаимодействия внутри сетевого геймифицированного образовательного проекта. Также приведены мотиваторы, позволяющие организовать пользователей такого проекта, перейти к самоорганизации в области защищенного информационного взаимодействия.

*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 внедрению мотивационных установок в геймифицированный проект для повышения защищенности взаимодействия участников, показаны некоторые организационные и технические решения.

*Заключение.* По результатам проведенного эксперимента показано, что сетевое взаимодействие по активности участников может быть сравнимо с взаимодействием с реальным присутствием, и, таким образом, рассмотренные рекомендации будут действительны для обеих форм взаимодействия. 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.*

*Введение*. В области развития игровых образовательных сред существует дефицит внимания к защитным механизмам и методикам, которые позволяют обеспечить информационную безопасность взаимодействия участников геймифицированных проектов. Известно, что развитие таких проектов на основе социальных сетей [Tang et al., 2010; Jin et al., 2018] не предполагает шифрования трафика и аутентификации участников; эти задачи по умолчанию возлагаются на механизмы самой социальной сети. Ни одна из рассмотренных игровых сред [Liu et al., 2018; Beckers, Pape, 2016; Trickel et al., 2017] в области информационной безопасности не содержит защиты от социально-инженерных атак, подобных фишингу, что ставит под угрозу образовательную среду всего университета, поддерживающего такой геймифицированный проект.

Вместе с тем разработка и применение игровых кейсов в информационной безопасности – интересный способ повысить эффективность обучения в этой области. Известно, что подобный подход хорошо зарекомендовал себя

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

в повышении осведомленности о вопросах информационной безопасности, обучении защите от социальной инженерии, тестировании и защите программного кода. В публикациях [Liu et al., 2018; Beckers, Pape, 2016], как уже упоминалось ранее, представлены примеры игр, применяемых для решения упомянутых задач. Также известны примеры соревнований Capture the Flag [Trickel et al., 2017], более защищенные от технических методов нарушения безопасности, которые в игровой форме представляют решения актуальных проблем безопасности.

Упомянутые решения, несмотря на интересные концепции, заложенные в них, не реализуют решения, тезисно описанные в задаче проекта, а именно модели взаимодействия участников в них изначально небезопасны. К примеру, кража личности, достаточно распространенное явление для социальной сети, приведет к ошибочному восприятию человека по данным украденного аккаунта, что может нарушить структуру самого игрового кейса (за счет получения незапланированных привилегий, повышения уровня взаимодействия) и безопасность персональной информации. С теоретической точки зрения исследования по безопасному взаимодействию концентрируются на ограничениях при передаче или хранении информации; связи роль – информация – игровое взаимодействие с позиций исследования безопасности практически не рассматриваются.

*Цель исследования.* Представленная работа ориентирована на разработку модели и метода оценки группового взаимодействия с точки зрения информационной безопасности, применимых для проектов в форме кейс-стади или игровых решений, широко использующих информационные технологии, которые разрабатываются несколькими взаимодействующими студенческими командами через социальную сеть. Авторы ориентировались на ряд проектов, завершенных ими при поддержке Фонда Потанина в 2015–2017 гг., в области обучения информационной безопасности, а также на ряд исследований зарубежных и российских ученых в этой области.

Кибербезопасность в современном мире играет решающую роль для национальной инфраструктуры, органов федерального и местного управления, военной и гражданской промышленности, а также для персональных данных граждан.

В свою очередь, перспективность и важность обучения студентов на примере вовлечения в решение игровых кейсов неоднократно отмечалась преподавателями высшей школы [Kim et al., 2017; Vanwynsberghe et al., 2013; Tang et al., 2010; Jin et al., 2018; Kaivola et al., 2012]. Одним из итогов такого использования игровых кейсов неизбежно будет развитие компетенций, связанных с принятием решений. Очевидно, что для обучающихся в магистратуре по направлению Информационная безопасность студентов это является приоритетным направлением личностного развития. Такие компетенции наиболее востребованы и на рынке труда, поскольку магистерское образование в области защиты информации воспринимается работодателями как признак наличия управленческих навыков у выпускника университета. Развитие подобных компетенций может быть использовано и в ходе обучения, в том числе как способ более успешной интеграции в научную деятельность студенческих коллективов или в крупные проекты университетского сообщества.

*Связанные работы.* Поставленная задача 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.

Известно, что итогом применения геймификации как образовательной технологии должны быть корректировка поведения обучаемого, его фокусировка на отдельных элементах материа-

ла, ускоренное усвоение отдельных разделов или развитие отдельных способностей, компетенций. Таким образом, геймификация должна выступать как инструмент преобразования или корректировки при обучении. К примеру, в работе О.В. Орловой и др. указывается, что «от других игровых практик (ролевых, деловых игр и т. д.) геймификация отличается неимитационным характером активности: сохраняя неизменным содержание образовательной деятельности, геймификация кардинально трансформирует способ организации этой деятельности и сопровождает весь образовательный цикл» [Орлова, Титова, 2015]. Кайвола и др. [Kaivola et al., 2012] рассматривают квестовую форму игрофикации как основу улучшения и совершенствования образовательного процесса, вопросы моделирования такой формы игрофикации рассмотрены в работе О.В. Ниссенбаум и др. [Nissenbaum et al., 2019]. Антоначи и коллеги [Antonaci et al., 2017] предполагают использование геймификации как инструмента улучшения массовых открытых образовательных курсов, тогда как в работе Surendeleg и др. [Surendeleg et al., 2014] перечислены различные модели, используемые как основа геймификации, из которых в настоящей работе будет использована модель Фогга. М. Ортиз [Ortiz et al., 2017] в своем обзоре выделяет два существенных для оценки геймификации параметра: эффективность обучения и вовлеченность. Следовательно, необходимо помнить, что внедрение защиты информации как части геймифицированных процессов не должно приводить к существенному, значимому снижению ни первого, ни второго параметра.

Значимые публикации, связанные с отдельными разделами, будут указаны ниже, при рассмотрении отдельных задач.

**Геймификация в сетевой форме.** Геймификация в сетевой форме рассмотрена как некоторый уровень взаимодействия, коллаборации различных групп, взаимодействующих через социальную сеть. Идея использования социальных сетей в подобных коллаборациях для повышения эффективности показана ранее другими авторами, например здесь [Vanwynsberghe et al., 2013]. Мы предлагаем взглянуть на задачу коллаборации студентов в первую очередь как на распределение ответственности. Если учесть, что в эксперименте по разработке и реализации игровых кейсов с использованием социальной сети участвовали 3 университета и 4 группы студентов, одна из которых включала студентов различных университетов, то такая постановка задачи позволяет оценить эффективность взаимодействия и, как следствие, успешность таких коллабораций. Такая работа представлена авторами в публикации [Zolotarev et al., 2018].

Там же отмечается, что при определенных условиях возможно достичь уровня эффективности взаимодействия в сетевой коллаборации, близкого к общению в группе без применения социальных сетей или иных сетевых средств коммуникации. При этом, разумеется, возникают новые риски, связанные с передачей данных в рамках социальных сетей, рассматриваются различные типы атак на сетевые ресурсы игровых задач, формулируются требования к защитным механизмам.

Ранее в статье [Safonov et al., 2019] была приведена классификация атак, связанных с игровыми ресурсами (рис. 1). Цель дальнейшей работы – используя модель Фогга для управления поведением участников, задействовать такой способ обмена информацией, который увеличивает безопасность информационного взаимодействия в сетевом геймифицированном проекте с учетом как типов атак схемы (рис.), так и требования минимализации влияния на показатели эффективности обучения и вовлеченности, приведенного ранее.

Рассматривая игровые среды, описанные в представленных ранее статьях, и ориентируясь на схему, показанную выше (рис.), можно выделить некоторый набор данных, полезных для модели Фогга. Исходно [Fogg, 2019] модель Фогга для управления поведением участников использует три элемента: мотивация (качественно оценивается от высокой к низкой), умение (от сложной задачи к простой) и триггеры, события, влияющие на определенное нужное действие.



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


*Рис. Некоторые типы атак на игровые ресурсы*

*Fig. Some types of attacks on game resources*

Если события возникают в ходе моделирования реальной ситуации в игровом кейсе, как показано в приведенном ниже эксперименте, а умение является вопросом, определяемым скорее техническими условиями игровой задачи, то мотиваторы должны быть вычленены из существующих игровых задач как некоторый обобщающий фактор. Табл. 1 рассматривает такой набор простых мотиваторов, определяющих поведение игроков.

*Таблица 1*

**Мотиваторы**

*Table 1*

**Motivators**

| Мотиватор | Умение | Возможный триггер |
|---|---|---|
| Желание защитить полученный результат, не допустить его перехвата и анализа другими пользователями, сохранить преимущество | Реализация защитных мер при передаче и обработке игровой информации | Имитация атаки на аккаунт |
| Статус игрока, сохранение преимущества, интерес к новым задачам, получаемым эксклюзивно | Реализация защитных мер при хранении информации | Несанкционированный доступ к данным игрока, моделируемый игровой ситуацией |
| Сохранение личного, приватного пространства внутри игровой среды | Сохранение приватности | Имитация атаки на аккаунт |

Простые мотиваторы, такие как любопытство игрока или стремление сократить временные затраты для организатора игры, не рассматриваются ввиду их универсальности – использование их возможно в рамках любой задачи и с любым триггером.

Как можно видеть, использовать указанные в табл. 1 мотиваторы достаточно просто в рам-

ках любого геймифицированного процесса. Далее рассмотрим вопрос безопасного взаимодействия в целевой задаче.

*Безопасное информационное взаимодействие в сетевых геймифицированных проектах.* Арабова [Арабова, 2017] и Дербень [Дербень, 2018] рассматривают необходимые факторы нарушения безопасности информационного взаимодействия, но изначально такие факторы, или триггеры, в терминологии Фогга, можно использовать и для генерации положительных изменений в области безопасности.

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 работы по указанной модели в общем случае может соответствовать следующим стадиям развития защищенного взаимодействия внутри геймифицированного процесса.

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

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

3. Привязка мотиваторов к задачам через фиксированные триггеры.

3а (при необходимости). Оценка времени, необходимого для реализации защищенного взаимодействия внутри конкретных задач, и приемлемости полученного значения для игровой среды.

4. Оценка эффективности воздействия через мотиваторы путем фиксации количественных и качественных измененений.

5. Закрепление эффективных мотиваторов в игровой среде.

В статье [Nissenbaum et al., 2019] авторами ранее приведены некоторые расчеты по квестовым задачам, реализуемым в рамках обучения информационной безопасности. Необходимо отметить, что в случае реализации защитных механизмов внутри этих задач будет изменяться, в частности, время исполнения заданий.

Также, согласно [Zolotarev et al., 2018], необходимо будет оценить сложность логических связей и, вероятнее всего, внести новые, что усложнит как саму коллаборацию и проект в целом, так и требования к его реализации.

Тем не менее можно отметить, что основой новых моделей взаимодействия будут простые технические решения, что в любом случае не вызовет критичных изменений в схеме игровых решений или организации коллаборации.

Реализация механизмов защиты в любой игровой среде может быть выполнена стандартными методами, ранее применявшимися в иных задачах подобного типа, скажем, в защите социальной сети как инфраструктуры или в защите веб-сервисов. Далее представим экспериментальные данные исследования.

**Экспериментальная часть.** Ранее при рассмотрении угроз безопасности при использовании игровых ресурсов и атак, направленных на игровые ресурсы, использовались наиболее вероятные вектора таких атак. Среди них можно отметить кражу и подмену аккаунтов, нарушение безопасности и доступности контента игровых задач. Далее рассмотрим некоторые экспериментальные варианты противодействия, предназначенного для типовых игровых сервисов.

Первичный вариант эксперимента предлагал оценить, насколько активное сетевое взаимодействие сопоставимо с реальным, происходящим в условиях личного контакта группы, участвующей в эксперименте. Некоторые данные были ранее приведены в статье [Zolotarev et al., 2018]. Основным выводом по итогам анализа полного объема данных, полученных в этом эксперименте, является сопоставимая, а иногда и большая активность, участников именно сетевой части геймифицированного проекта.

Оценивались в первую очередь информационные потоки, показатели:

p1) количество сообщений (при работе с контрольной группой обмен сообщениями учитывался в рамках встреч);

p2) количество инициаторов сообщений за сутки (за встречу);



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

*Таблица 2*

**Результаты эксперимента**

*Table 2*

**Experimental results**

| | 06.апр | 07.апр | 08.апр | 09.апр | 10.апр | 11.апр | 12.апр | 13.апр | 14.апр |
|---|---|---|---|---|---|---|---|---|---|
| p1 | 23 | 60 | 27 | 9 | 3 | 5 | 0 | 4 | 0 |
| p2 | 3 | 7 | 2 | 3 | 1 | 1 | 0 | 1 | 0 |
| p3 | 3 | 7 | 4 | 3 | 4 | 1 | 0 | 1 | 0 |
| p4 | 2 | 7 | 4 | 4 | 3 | 0 | 0 | 0 | 0 |
| (группа 1) | | | | | | | | | |
| | 09.мар | 10.мар | 14.мар | 15.мар | 16.мар | 17.мар | 18.мар | 19.мар | 20.мар |
| p1 | 66 | 24 | 49 | 35 | 253 | 20 | 0 | 29 | 85 |
| p2 | 4 | 2 | 4 | 3 | 5 | 3 | 0 | 2 | 3 |
| p3 | 5 | 3 | 6 | 5 | 8 | 3 | 0 | 3 | 7 |
| p4 | 5 | 3 | 6 | 5 | 8 | 3 | 0 | 3 | 7 |
| (группа 2) | | | | | | | | | |
| | 01.фев | | 05.фев | | 12.фев | | 15.фев | | 19.фев |
| p1 | 20 | 0 | 16 | 0 | 8 | 0 | 20 | 0 | 12 |
| p2 | 2 | 0 | 4 | 0 | 4 | 0 | 5 | 0 | 5 |
| p3 | 12 | 0 | 8 | 0 | 4 | 0 | 12 | 0 | 6 |
| p4 | 6 | 0 | 6 | 0 | 4 | 0 | 7 | 0 | 5 |
| (контроль) | | | | | | | | | |
| | 16.апр | 17.апр | 18.апр | 19.апр | 20.апр | 21.апр | 22.апр | 23.апр | 24.апр |
| p1 | 12 | 5 | 2 | 0 | 0 | 2 | 44 | 17 | 55 |
| p2 | 3 | 2 | 2 | 0 | 0 | 2 | 7 | 4 | 3 |
| p3 | 3 | 2 | 2 | 0 | 0 | 2 | 7 | 4 | 3 |
| p4 | 3 | 1 | 1 | 0 | 0 | 1 | 7 | 4 | 3 |
| (группа 1) | | | | | | | | | |
| | 22.мар | 23.мар | 24.мар | 25.мар | 26.мар | 27.мар | 28.мар | 29.мар | 30.мар |
| p1 | 0 | 9 | 0 | 0 | 92 | 0 | 15 | 0 | 53 |
| p2 | 0 | 2 | 0 | 0 | 4 | 0 | 3 | 0 | 3 |
| p3 | 0 | 3 | 0 | 0 | 6 | 0 | 3 | 0 | 3 |
| p4 | 0 | 3 | 0 | 0 | 6 | 0 | 3 | 0 | 3 |
| (группа 2) | | | | | | | | | |
| | 22.фев | | 26.фев | | 01.мар | | 05.мар | | 12.мар |
| p1 | 20 | 0 | 8 | 0 | 20 | 0 | 12 | 0 | 5 |
| p2 | 6 | 0 | 3 | 0 | 6 | 0 | 6 | 0 | 2 |
| p3 | 11 | 0 | 4 | 0 | 11 | 0 | 6 | 0 | 2 |
| p4 | 5 | 0 | 4 | 0 | 6 | 0 | 6 | 0 | 2 |
| (контроль) | | | | | | | | | |

p3) количество участников диалога за сутки (за встречу);

p4) количество участников, откликнувшихся на сообщения за сутки (за встречу) (далее – первичный отклик).

В табл. 2 показаны сопоставляющие данные для двух сетевых экспериментов, в которых участвовали три группы, географически распределенные по различным городам (Красноярск, Таганрог, Москва), и одного контрольного, где принимала участие только локализованная группа (Красноярск), функционирующая на уровне личного, не удаленного взаимодействия. Эксперимент проходил в течение 18 дней, участвовали 16 человек как организаторы игровых кейсов и 102 как игроки. Длительность общения в контрольной группе не превышала 20 минут за собрание. Группы не оповещались о проведении эксперимента, задачи выполнялись всеми одинаковые, общение между группами, помимо социальной сети, не оказывало влияние на результат.

Как видно из представленных данных, в первую очередь активность групп выравнивалась в дни активного обсуждения; но это же соображе-

ние может быть использовано для моделирования атак и противодействия им.

Работа с контентом как способ предотвращения атак, использующих один из перечисленных выше векторов, может реализовываться с использованием ролевой модели. В статье [Zukova, Zolotarev, 2019] ранее показано, что такое использование может быть существенным усилением безопасности игрового сервиса. Здесь же надо отметить, что реализация защитного механизма в игровой задаче приводит к усилению следующих защитных механизмов (табл. 3).

*Таблица 3*

**Итоги тестирования разработанного игрового сервиса**

*Table 3*

**Performance test results of the developed game service**

| Требование | Процесс тестирования | Результат и мотиваторы |
|---|---|---|
| Защищенное соединение | Просмотр параметров соединения и сертификата | Доступ осуществляется по протоколу HTTPS, данные внутри шифруются по протоколу TLS 1.2.<br>Основным мотиватором для данного механизма может выступить желание защитить полученный результат, не допустить его перехвата и анализа другими пользователями, сохранить преимущество |
| Ограничение доступа к игровым ресурсам на основе ролевой модели TBAC | Моделирование ситуаций доступа к игровым событиям различного уровня доступа | Механизм ограничения доступа к игровым ресурсам на основе ролевой модели оказывает необходимое влияние на игровой процесс.<br>Основным мотиватором для сохранения ограничения доступа могут выступать статус игрока, сохранение преимущества, интерес к новым задачам, получаемым эксклюзивно |
| Защита базы данных игрового сервиса | Определение правил доступа к базе данных | Настроенные правила доступа к базе данных позволяют защитить хранящиеся в ней игровые сведения.<br>Основным мотиватором для данного механизма может выступить желание защитить полученный результат, не допустить его перехвата и анализа другими пользователями, сохранить преимущество |

Для проведения эксперимента на платформе Google FireBase был развернут тестовый игровой сервис, реализующий основной функционал. Для сбора и анализа информации использован Google Analytics для Firebase. Он позволяет получать данные о действиях пользователей и сразу же принимать меры с помощью дополнительных функций. В качестве эксперимента рассмотрена задача группового взаимодействия, использующая в качестве основы ролевую модель управления доступом TBAC.

Работа с аккаунтами предполагала усиление процедур аутентификации и идентификации при входе в систему. На тестовом уровне были реализованы следующие процедуры (табл. 4).

Видно, что применение защитных мер в общем случае может быть достигнуто без радикальной переработки модели взаимодействия пользователей, за счет активного сетевого обмена и применения дополнительной мотивации, согласно модели Фогга, может быть получен эффект, заключающийся как в повышении безопасности, так и в активизации сетевых взаимодействий, причем одновременно.

*Выводы*. Основной уязвимой стороной сетевого геймифицированного проекта, как показано в статье, является взаимодействие пользователей. Несмотря на сложность этой задачи, с точки зрения педагогической технологии может быть разработана и представлена пользователям игрового сервиса система мотивации, которая позволит повысить уровень информационной безопасности игровых задач за счет самоорганизации пользователей и некоторых дополнительных технических решений. Управление таким проектом, как показано выше, потребует определенных дополнительных усилий, но за счет самоорганизации пользователей эти усилия могут быть минимизированы.



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

*Таблица 4*

**Итоги тестирования разработанного игрового сервиса**

*Table 4*

**Performance test results of the developed game service**

| Требование | Процесс тестирования | Результат |
|---|---|---|
| Двухфакторная система аутентификации | Попытки доступа к веб-страницам в обход системы аутентификации; попытки ввода неверных аутентификационных данных; попытки подмены ассоциированного мобильного телефона | Доступ к веб-страницам в обход системы аутентификации запрещен; ввод неверных аутентификационных данных не позволяет обойти систему аутентификации; подмена мобильного телефона не позволяет обойти систему аутентификации.<br>Основной мотиватор – сохранение личного, приватного пространства внутри игровой среды |
| Ограничения взаимодействия пользователей | Моделирование ситуаций взаимодействия игроков с разными уровнями | Взаимодействие игроков возможно только если они объединены игровым решением; взаимодействие игроков с разным уровнем ограничено.<br>Основной мотиватор – сохранение преимущества |
| Liveness detection как метод усиленной идентификации | Анализ возможности кражи аккаунта через хищение или подмену биометрических данных | Добавлен второй фактор для усиления процедуры идентификации – активное взаимодействие с пользователем путем считывания движений рта при проговаривании слова-ключа [Золотарев, 2019].<br>Основной мотиватор – сохранение личного, приватного пространства внутри игровой среды |
| Распределенная аутентификация | Анализ возможности решения игровых задач в режиме группового взаимодействия при сохранении заданного уровня безопасности | Предложен вариант распределенной аутентификации с использованием носимых устройств [Левкина, 2019].<br>Основной мотиватор – получение эксклюзивного доступа к игровым задачам, интерес, любопытство |

## Библиографический список


1. Арабова Т.И. Анализ тональности отзывов на событие для выявления предрасположенности к атакам на персонал // Инжиниринг предприятий и управление знаниями: матер. XX юбилейной Российской науч. конф. 2017. С. 18–23.
2. Дербень А.М. Анализ рисков в условиях распределенных кибератак // Студенческая наука для развития информационного общества: матер. VII Всерос. науч.-техн. конф. 2018. С. 280–284.
3. Орлова О.В., Титова В.Н. Геймификация как способ организации обучения // Вестник Томского государственного педагогического университета. 2015. Вып. 9 (162). С. 60–64.
4. Antonaci A., Klemke R., Stracke C., Spatafora M., Stefanova K., Specht M. Gamification to empower information security education // Proceedings of GamiFIN conference. 2017. P. 32–38.
5. Beckers K., Pape S. A serious game for eliciting social engineering security requirements // Proceedings of 2016 IEEE 24th International Requirements Engineering Conference (RE). 2016.
6. Fogg B.J. Fogg behavior model. URL: https://www.behaviormodel.org/
7. Jin G., Tu M., Kim T.-H., Heffron J., White J. Game based cybersecurity training for high school students: SIGCSE ‘18 Proceedings of the 49th ACM Technical Symposium on Computer Science Education. P. 68–73.
8. Kaivola T., Salomaki T., Taina J. In quest for better understanding of student learning experiences // Procedia-Social and Behavioral Sciences. 2012. № 46. P. 8–12.
9. Kim B.-H., Kim K.-C., Hong S.-E., Oh S.-Y., Development of cyber information security education and training system // Multimedia Tools and Applications. 2017. 76(4). P. 6051–6064.
10. Liu L., Yasin A., Li T. Improving software security awareness using a serious game / L. Liu, A. Yasin, T. Li, R. Fatima, J. Wang. IET Software, 2018.
11. Nissenbaum O., Maro E., Ishchukova E., Zolotarev V. Markov and semi-Markov. Models of

real-time quests in information security education // Proceedings of 2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 2019.

12. Ortiz M., Chiluiza K., Valcke M. Gamification and learning performance: A systematic review of the literature // Proceedings of the 11th European Conference on Games Based Learning, 2017.
13. Safonov K., Zolotarev V., Derben A. Analysis of attack strategies on game resources for technological processes training games // Proceedings of the IOP Conference series. 2019 [in press].
14. Surendeleg G., Murwa V., Yun H., Kim Y.S. The role of gamification in education – a literature review // Contemporary Engineering Sciences. 2014. Vol. 7. P. 1609–1616.
15. Tang S., Hanneghan M. A Model-driven framework to support development of serious games for game based learning // Proceedings of the 3rd International Conference on Developments in e-Systems Engineering. London, UK. 2010.
16. Trickel E., Disperati F., Gustafson E. et al. Shall we play a game? CTF-as-a-service for security education // Proceedings of the USENIX Workshop on Advances in Security Education (ASE). 2017.
17. Vanwynsberghe H., Verdegem P. Integrating social media in education // CLCWeb: Comparative Literature and Culture. 2013. 15.3.
18. Yasin A., Liu L., Li T. Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG) / L. Liu, A. Yasin, T. Li, J. Wang, D. Zowghi // Information and Software Technology. 2018. 95. P. 179–200.
19. Zhukova M., Zolotarev V. Role model features in educational serious games // Proceedings of the 2019 International conference «Quality management, transport and information security, information technologies» (IT&QM&IS–2019). Sochi. 2019 [ in press].
20. Zolotarev V., Povazhnyuk A., Maro E. Liveness detection methods implementation to face identification reinforcement in gaming services // Proceedings of the 12th International Conference on Security of Information and Networks (SIN 2019) [in press].
21. Zolotarev V., Maro E. and Kulikova S. New approach to activity evaluation for social network based student collaboration // Proceedings of the 12th IEEE International Conference on Application of Information and Communication Technologies (AICT 2018). P. 374–380.

DOI: https://doi.org/10.25146/1995-0861-2019-49-3-145

# PROVIDING SECURE INFORMATION INTERACTION OF PARTICIPANTS IN NETWORK GAMIFIED PROJECTS

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

**Abstract**

*Statement of the problem and purpose of the article*. The article deals with the issues related to the protected interaction within the gamified educational environment, in particular in the field of game cases used for teaching information security. The main threats discussed below are impact on content and account theft. Experimental data comparing network and local interaction within a network gamified educational project are shown. Also the motivators are given allowing to organize users of such project, to pass to self-organization in the field of the protected information interaction.

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

*Results.* The author's recommendations on the implementation of motivational attitudes in a gamified project to improve the security of interaction between participants are developed, some organizational and technical solutions are shown.

*Conclusion.* According to the results of the experiment, it is shown that the network interaction on the activity of the participants can be compared with the interaction with the real presence, and thus the recommendations considered will be valid for both forms of interaction. The author's recommendations considered in the article can be applied in the master-degree course of training for students specializing in 10.04.01 Information security (full-time education).

**Keywords:** *education, information security, serious games, gamification*.

## References

1. Arabova T.I. Sentiment analysis of event reviews to identify predisposition to attacks on personnel // Proceedings of the XX anniversary Russian scientific conference "Enterprise engineering and knowledge management". 2017. P. 18–23.
2. Derben A.M. Risk analysis in distributed cyber-attacks // Proceedings of the VII all-Russian scientific and technical conference "Student science for the development of information society". 2018. P. 280–284.
3. Orlova O.V., Titova V.N. Gamification as a way of teaching // Bulletin of Tomsk State Pedagogical University. 2015. Vol. 9 (162). P. 60–64.
4. Antonaci A., Klemke R., Stracke C., Spatafora M., Stefanova K., Specht M. Gamification to empower information security education // Proceedings of GamiFIN conference. 2017. P. 32–38.
5. Beckers K., Pape S. A serious game for eliciting social engineering security requirements // Proceedings of 2016 IEEE 24th International Requirements Engineering Conference (RE). 2016.
6. Fogg B.J. Fogg behavior model. URL: https://www.behaviormodel.org/
7. Jin G., Tu M., Kim T.-H., Heffron J., White J. Game based cybersecurity training for high school students: SIGCSE '18 Proceedings of the 49th ACM Technical Symposium on Computer Science Education. P. 68–73.
8. Kaivola T., Salomaki T., Taina J. In quest for better understanding of student learning experiences // Procedia-Social and Behavioral Sciences. 2012. No. 46. P. 8–12.
9. Kim B.-H., Kim K.-C., Hong S.-E., Oh S.-Y., Development of cyber information security education and training system // Multimedia Tools and Applications. 2017. 76(4). P. 6051–6064.

10. Liu L., Yasin A., Li T. Improving software security awareness using a serious game / L. Liu, A. Yasin, T. Li, R. Fatima, J. Wang. IET Software, 2018.
11. Nissenbaum O., Maro E., Ishchukova E., Zolotarev V. Markov and semi-Markov models of real-time quests in information security education // Proceedings of 2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 2019.
12. Ortiz M., Chiluiza K., Valcke M. Gamification and learning performance: A systematic review of the literature // Proceedings of the 11th European Conference on Games Based Learning, 2017.
13. Safonov K., Zolotarev V., Derben A. Analysis of attack strategies on game resources for technological processes training games // Proceedings of the IOP Conference series. 2019 [in press].
14. Surendeleg G., Murwa V., Yun H., Kim Y.S. The role of gamification in education – a literature review // Contemporary Engineering Sciences. 2014. Vol. 7. P. 1609–1616.
15. Tang S., Hanneghan M. A Model-driven framework to support development of serious games for game based learning // Proceedings of the 3rd International Conference on Developments in e-Systems Engineering. London, UK. 2010.
16. Trickel E., Disperati F., Gustafson E. et al. Shall we play a game? CTF-as-a-service for security education // Proceedings of the USENIX Workshop on Advances in Security Education (ASE). 2017.
17. Vanwynsberghe H., Verdegem P. Integrating social media in education // CLCWeb: Comparative Literature and Culture. 2013. 15.3.
18. Yasin A., Liu L., Li T. Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG) / L. Liu, A. Yasin, T. Li, J. Wang, D. Zowghi // Information and Software Technology. 2018. 95. P. 179–200.
19. Zhukova M., Zolotarev V. Role model features in educational serious games // Proceedings of the 2019 International conference «Quality management, transport and information security, information technologies» (IT&QM&IS–2019). Sochi, 2019 [in press].
20. Zolotarev V., Povazhnyuk A., Maro E. Liveness detection methods implementation to face identification reinforcement in gaming services // Proceedings of the 12th International Conference on Security of Information and Networks (SIN 2019) [in press].
21. Zolotarev V., Maro E. and Kulikova S. New approach to activity evaluation for social network based student collaboration // Proceedings of the 12th IEEE International Conference on Application of Information and Communication Technologies (AICT 2018). P. 374–380.