К. В. Сафонов, Е. А. Ищукова, В. В. Золотарев

Применение элементов геймификации в подготовке студентов – будущих специалистов в области защиты информации

В настоящее время подготовка студентов – будущих специалистов по защите информации существенно модифицируется. В число необходимых навыков такого специалиста теперь включают «soft skills», надпрофессиональные навыки, отвечающие за эффективность участия в рабочем процессе. Сама же защита информации становится неотъемлемой частью бизнес-моделирования. В связи с этим возникает вопрос выбора наиболее эффективных технологий формирования таких навыков, выраженных в соответствующих компетенциях специалиста по защите информации.

Цель исследования – оценка использования элементов геймификации в процессе подготовке студентов – будущих специалистов по защите информации.

Исследование проводилось в Сибирском государственном университете науки и технологий, на кафедре безопасности информационных технологий, а также в рамках проекта «Разработка пакета игровых кейсов для дисциплины «Управление информационной безопасностью»». Всего в педагогической и опытно-экспериментальной работе принимало участие 182 студента 3-5 курса специалитета, 1-2 курса магистратуры направления, а также студентов 4 курса бакалавриата направления «Информационная безопасность».

В рамках исследования показано, что уменьшается время выполнения заданий для освоения компетенции (снижение времени до 30% в рамках семестра), а также отмечено, что студенты, способные освоить компетенцию, получили результаты уже в начале курса. При этом доля пассивно участвующих в прохождении элементов курса в составе малых групп снижается и составляет не более 10%, а количество не участвующих в освоении практически сведено к нулю.

Результаты исследования выборочного отклика участников сетевых коллабораций показали, что вовлеченность и изучение материала оставались на стабильно высоком уровне как в прошлые годы, так и на момент среза по итогам эксперимента. Так, например, оценка связи организаторов проекта в социальной сети ВКонтакте за 4 года действия проекта: 100% участников связаны непосредственно хотя бы через одного участника проекта; 93,75% указаны в друзьях хотя бы у одного участника проекта, доля высокоинтенсивных информационных связей составила 21,87%.

Ключевые слова: геймификация, геймифицированный элемент, образовательный процесс, менеджмент качества, вовлеченность, информационная безопасность

Ссылка для цитирования:

Сафонов К. В., Ищукова Е. А., Золотарев В. В. Применение элементов геймификации в подготовке студентов – будущих специалистов в области защиты информации // Перспективы науки и образования. 2021. № 1 (49). С. 450-463. doi: 10.32744/pse.2021.1.31

K. V. SAFONOV, E. A. ISHUKOVA, V. V. ZOLOTAREV

Application of gamification elements in the training of students – future specialists in the field of information security

Currently, the training of students-future specialists in information security is significantly modified. The necessary skills of such a specialist now include "soft skills", super-professional skills that are responsible for the effectiveness of participation in the work process. Information security itself is becoming an integral part of business modeling.

This raises the question of choosing the most effective technologies for developing such skills, expressed in the relevant competencies of an information security specialist.

The purpose of the study is to evaluate the use of gamification elements in the process of training students-future information security specialists.

The research was conducted at the Siberian State University of Science and Technology, at the Department of Information technology security, as well as in the framework of the project «Development of a package of game cases for the discipline «Information security management»». In total, 182 students of the 3rd-5th year of specialty, 1-2 year of master's degree, as well as students of the 4th year of bachelor's degree in Information security took part in pedagogical and experimental work.

The study shows that the time required to complete tasks to master the competence decreases (the time is reduced by up to 30% during the semester), and it is also noted that students who are able to master the competence received results at the beginning of the course. At the same time, the share of passively participating in the course elements in small groups is reduced to no more than 10%, and the number of non-participants in the development is practically reduced to zero.

The results of the study selective response of participants in networked collaboration showed that the involvement and study of the material remains at a consistently high level as in previous years, and the time slice at the end of the experiment. For example, the assessment of the project organizers' communication in the social network Vkontakte for 4 years of the project: 100% of participants are connected directly through at least one project participant; 93.75% are listed as friends of at least one project participant, the share of high-intensity information connections was 21.87%.

Keywords: gamification, gamified element, educational process, quality management, engagement, information security

For Reference:

Safonov, K. V., Ishukova, E. A., & Zolotarev, V. V. (2021). Application of gamification elements in the training of students – future specialists in the field of information security. *Perspektivy nauki i obrazovaniya – Perspectives of Science and Education*, 49 (1), 450-463. doi: 10.32744/pse.2021.1.31

Введение

Модификация подготовки студентов – будущих специалистов в области защиты информации – в современных условиях имеет тенденцию к включению в учебные планы дисциплины, развивающие «soft skills», надпрофессиональные навыки и умения, позволяющие встроиться в рабочий процесс, коммуницировать, работать в команде. За развитие таких навыков должны отвечать университеты (и конкретные преподаватели), тогда как ФГОС для этого предусматривает профессиональные компетенции. Примером такой компетенции является рассмотренная далее в исследовании ПК-14 у бакалавров защиты информации (способность организовывать работу малого коллектива исполнителей в профессиональной деятельности), примером формирующих такие компетенции дисциплин – «Гуманитарные аспекты информационной безопасности», «Управление информационной безопасностью».

Вместе с тем нельзя не отметить, что традиционный, линейный способ формирования таких дисциплин через серию последовательных практических занятий не всегда эффективен. Часто он дает результат уже в конце семестровой дисциплины, что не всегда удобно и приемлемо для преподавателя. Необходим поиск инструментов, могущих дать изменение образовательного процесса в рамках упомянутых дисциплин, повысить эффективность обучения, увеличить вовлеченность. Авторы считают, что таким инструментом может быть геймификация.

Ортиз [1] в своем обзоре выделяет два существенных для оценки геймификации параметра, эффективность обучения и вовлеченность. Оба этих параметра критичны не только для подготовки будущих специалистов по защите информации, они применимы и для подготовки «элитных специалистов о области техники и технологий», для которых также характерно развитие надпрофессиональных навыков [2]. Такая подготовка направлена в первую очередь на формирование личностных качеств обучающихся и сочетает глубокое изучение предметной области с практическими навыками выполнения творческих проектов по системе CDIO. Вместе с тем даже программа подготовки элитных специалистов в системе высшего образования должна соответствовать ФГОСам и обеспечивать компетентностный подход в образовании [3]. Кроме того, необходимо учитывать и требования к формированию электронных образовательных сервисов университета [4], которые и будут основным инструментом донесения до студентов информации и реализации возможностей обучения с учетом требований дублирования, возможности быстрого перехода на дистанционную форму обучения.

Итак, вовлеченность и повышение эффективности обучения, избранные основными параметрами оценки эффективности, затронут при внедрении геймификации творческие проекты или их элементы, развитие личностных качеств студентов – будущих специалистов по защите информации, сочетая использование дистанционных сервисов и контактной работы в рамках компетентностного подхода.

Одним из способов изменения формата образования с сохранением соответствия заданным требованиям, с одной стороны, и со стимулированием интереса учащихся, с другой стороны, является применение методов геймификации [5-7]. Эти методы в том числе могут сочетать в себе как элементы электронного обучения, так и элементы дистанционного формата. Например, для обеспечения геймификации учебного процесса можно использовать широко известную систему обучения LMS Moodle, которая

позволяет реализовать любой игровой сценарий с переходом от уровня к уровню, а также начислять баллы в зависимости от результатов прохождения уровня [8]. В задачах обучения пользователей вопросам информационной безопасности используются механизмы викторины [9], кейсов [10] и проблемно-ориентированных игр [11].

Итак, на уровне выбора инструментов имеется много форм-факторов игровых элементов, которые можно внедрить в образовательный процесс; это представляется удобным. К тому же можно учитывать, что геймификацию как прием обучения будущих специалистов по информационной безопасности рассматривают и различные организации на уровне подготовки своих сотрудников, в том числе и с вовлечением в игру действующих специалистов по кибербезопасности, что делает процесс обучения приближенным к реальным условиям работы [12]. При этом работа над геймификацией в области обучения безопасности в университете коррелирует с аналогичной работой, которую выполняют специалисты, обучающие сотрудников противодействию определенным типам атак [13]. Это способствует внедрению в университете того взгляда на проблему обучения, который, как предполагается, будет закреплён в новых стандартах ФГОС 3++ (на настоящий момент в проектах ФГОС 3++ по направлению «Информационная безопасность» уже добавлены ссылки на профессиональные стандарты в области защиты информации).

Одним из способов развития студента – будущего специалиста по защите информации с учетом надпрофессиональных навыков является непрерывный процесс, включающий в себя моделирование определенного объекта защиты (системы), выделение информации, подлежащей защите, и процесс выработки наиболее эффективных путей нейтрализации причин данного влияния. В целом такое моделирование формирует и упомянутые «soft skills», и дает представление о профессиональной деятельности, и связывает модули и различные дисциплины в рамках учебного плана.

Целесообразно задействовать общие цели бизнес-процессов, которые могут напрямую применяться при моделировании процессов управления информационной безопасностью для обучения и анализа таких процессов. К таким целям можно отнести: описание процессов, их нормирование и установление взаимосвязей. Этот подход отлично сочетается с использованием геймифицированных элементов, в частности игровых кейсов, деловых игр, тренингов.

При этом, хотя на уровне общих описаний присутствует множество примеров таких игр, на уровне кафедры, отдельной дисциплины, методического обеспечения есть недостаток экспериментальных исследований, который необходимо восполнить.

В связи с этим целью данной работы является оценка использования элементов геймификации в процессе подготовке студентов – будущих специалистов по защите информации.

Материалы и методы

Исследование проводилось в Сибирском государственном университете науки и технологий, на кафедре безопасности информационных технологий, а также в рамках проекта фонда Потанина «Разработка пакета игровых кейсов для дисциплины «Управление информационной безопасностью»» и в Южном федеральном университете, на кафедре безопасности информационных технологий. Всего в педагогической и опытно-экспериментальной работе принимало участие 182 студента 3-5 курса

специалитета, 1-2 курса магистратуры направления, а также студентов 4 курса бакалавриата направления «Информационная безопасность», в том числе с использованием дистанционного обучения. Исследование выполнялось на базе данных 2017/2018 учебного года, в рамках дисциплин «Управление информационной безопасностью», «Основы управления информационной безопасностью» и «Технология построения защищенных автоматизированных систем».

В работе использовались следующие методы педагогического исследования: изучение научной, научно-методической литературы, нормативно-правовой базы высшего образования Российской Федерации; эмпирические и диагностические методы: опрос, анкетирование.

При обработке результатов опытно-экспериментальной работы применялись методы математической статистики: z-тест для оценки статистической значимости и оценка ошибки выборки для принятия решений о ее размере.

Изучение внедрения инструментов геймификации отдельных элементов образовательного процесса

Работая в рамках дисциплин «Управление информационной безопасностью»/«Основы управления информационной безопасностью», выступающих объектом изучения, удалось разработать и внедрить несколько задач формата игровых кейсов. Основой рассматриваемого в исследовании кейса, к примеру, была задача сформировать и синхронизировать (связать в единую схему) процессы сбора информации, которые позволят избежать повторения проблемных ситуаций (в указанном кейсе такой проблемной ситуацией было устранение недостатков системы защиты информации в условиях внешнего воздействия), обеспечить накопление опыта и постоянный мониторинг избранного решения. Кроме того, необходимо было предложить 1-2 альтернативных предложенному варианту решения указанной практической ситуации (чтобы избежать шаблонных решений).

Кроме того, так как в рамках работы с кейсом были применены элементы геймификации, которые использовались согласно предложенной схеме управления изменениями образовательного процесса. Изменения в данном случае генерируются при появлении новых требований или рисков.

Основной задачей управления изменениями в данном случае является изменение конфигурации образовательного процесса, приводящее к повышению эффективности за счет использования геймифицированных элементов в нем.

Предложенная схема управления изменениями выглядит так:

1. Регистрация запроса на изменение элемента курса.
2. Анализ последствий изменения и принятие решения.
3. Внесение изменений в курс.
4. Анализ внесенных изменений.
5. (опционально) Улучшение системы управления изменениями.

Общими критериями анализа внесенных изменений, как указано выше, были время выполнения элементов, успешность выполнения элементов, вовлеченность.

Если время и успешность выполнения могут быть оценены эмпирически, то для измерения вовлеченности (кого) выбирались дополнительно экспертные критерии. Наиболее общими критериями вовлеченности, принятыми в настоящем исследова-

нии, можно считать средний размер коллаборации, сформированной студентами для выполнения задания, и время жизни указанной коллаборации (продолжительность ее существования), устойчивость таких коллабораций (учитывают ли студенты характер кейса при формировании таких объединений? Если да, то насколько важно наличие в коллаборациях определенных компетенций?).

Рисунок 1 Общая схема управления геймификацией образовательного процесса

Для изучения процесса управления геймификацией образовательного процесса в рамках работы над организационной и экспериментальной частью исследования были решены следующие задачи:

1. Исследование работы над задачей игрового кейса на примере малых групп, определение оптимального размера малых групп. Проведена оценка влияния работы малых групп на работу учебной группы (18-25 человек по штатному составу) в целом.
2. Определены показатели и способы их оценки для работы малых групп.
3. Оценка возможности расширения базы исследования за счет включения студентов, участвовавших в работе через сетевые коллаборации на основе социальной сети. Изучение интенсивности взаимодействия в коллаборации и в существующих малых группах (учебных группах). Сравнение их результатов.

Эти три группы задач были спроецированы на схему управления геймификацией учебного процесса (рис. 1), в которой центральная роль отведена организатору учебного процесса.

Дополнительно была учтена теоретическая основа исследования, построенная на принципах конструктивизма, что предполагает участие обучающихся в конструировании знаний на основе предыдущего опыта. Конструктивизм, как считают основоположники применения этого подхода в электронном обучении, применим для развития метакогнитивных навыков, формирования уникального контента [14]. В частности, в рамках такого теоретического подхода в исследовании применялись игровые кейсы с открытым контентом, дополняемые участниками, без фиксированного правильного ответа; оценивалась способность формировать логику решения, способность справляться с решением за заданное время, формировать и использовать преимущества коллабораций.

Итак, схема управления геймификацией образовательного процесса в рамках исследования содержала ключевые точки, в которых и существовала возможность оценки эффективности подхода: контроль эффективности оценки, формирование малых групп и коллабораций, формирование устойчивых связей внутри коллаборации.

Итак, можно видеть, что основными измеримыми элементами в контексте исследования являются: а) работа малой группы на открытом к редактированию контентом; б) работа учебной группы в целом; в) работа сетевых коллабораций и сравнение работы в коллаборации в дистанционном формате и в рамках обычной группы.

Такие показатели были собраны в 2016-2020 году (часть по имеющимся ретроспективным данным) для отдельных групп бакалавриата направления «Информационная безопасность» в Сибирском государственном университете науки и технологий, на кафедре безопасности информационных технологий, а также в рамках проекта фонда Потанина «Разработка пакета игровых кейсов для дисциплины «Управление информационной безопасностью»». Для малой группы оценивалась вовлеченность в решение задачи, вторичный отклик по содержанию задачи на основе опроса; для учебной группы – успеваемость в рамках рейтинговой оценки по дисциплинам, указанным выше, на срезе 12 недель с начала 18-ти недель семестрового курса. Учебные группы изучались как отдельный объект, поскольку работа малых групп могла не покрывать общего количества студентов (к примеру, в случае с восстановленными студентами из академического отпуска). В качестве успешности прохождения игровых кейсов засчитывался рейтинг выше 80% по текущему уровню освоения курса. Для сетевых коллабораций был проведен (и ранее опубликован) эксперимент [15], который показал возможность расширения экспериментальной базы, и опросы по вторичному отклику, существенная для работы часть которых будет показана в экспериментальном разделе.

Работа малых групп оценивалась по следующим показателям – количество участников проекта (организаторы кейса) (1), количество участников одной малой группы (2), вовлеченность в решение задачи (устойчивость и использование ресурсов коллаборации) (3).

В рамках экспериментального внедрения геймифицированных элементов были учтены следующие особенности:

1. Возможность нарушения внутренних связей элементов. Изменение нельзя проецировать сразу на все компоненты образовательного процесса, необходимо выполнять тестовое ограниченное внедрение.

2. Централизованный учет и накопление знаний. Работа с элементами образовательного процесса должна продуцировать опыт, который может быть использован как для внешней, так и для внутренней оценки возможности повышения эффективности образовательного процесса.

Особенностью каждого игрового кейса было ограничение по времени (не более 3-4 часов), не менее 2-3 заданий внутри игрового кейса, влияющих на общую оценку, свободные (редактируемые) правила для формирования открытой части контента, с условием модерации в ходе игрового процесса.

Были выполнены и внедрены в рабочую программу дисциплины следующие экспериментальные элементы (таблица 1):

Таблица 1

Геймифицированные элементы в форме игрового кейса

№ п/п	Модули и темы дисциплины	Геймифицированные элементы	Компетенции
Раздел 1. Общие принципы и методы управления информационной безопасностью			
1.1	Принципы управления информационной безопасностью		
1.2	Сбор данных для управления информационной безопасностью	Сбор данных для управления ИБ (тренинг) (3 часа)	ПК-4, ПК-14
1.3	Методическое и документационное обеспечение управления информационной безопасностью		
Раздел 2. Подходы к управлению информационной безопасностью			
2.1	Процессный подход. Декомпозиция и особенности		
2.2	Архитектура СУИБ		
2.3	Управление рисками как элемент СУИБ	Управление рисками в нестандартной ситуации (кейс) (3 часа)	ПК-13
	Итого	2 занятия (6 часов)	

Осваиваемые в первом модуле компетенции и являлись объектом исследования, особенно показательна в плане исследования была компетенция ПК-14 (способность организовывать работу малого коллектива исполнителей в профессиональной деятельности). Исследуемый игровой кейс и содержал требования к такой работе, в частности сформировать навыки получения необходимых данных для формирования системы управления информационной безопасности и их применения в управлении информационной безопасностью, показать на примере конкретной ситуации, работая малой группой, корректность и полноту действий по управлению информационной безопасностью с использованием полученных данных, а также работы в той же ситуации с учетом внешнего воздействия.

Основные ограничения были связаны с требованиями, чтобы рабочая программа дисциплины была составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата), утвержденным приказом Министерства образования и науки Российской Федерации от 20.12.2016 № 44281.

Также было подготовлено методическое обеспечение – модифицирован лабораторный практикум, содержащий описание применения данных элементов, для их более эффективного применения.

Результаты эксперимента и рекомендации

План экспериментального исследования выглядел следующим образом:

1. Для малых групп, формируемых в ходе проекта (в том числе оцениваемых ретроспективно) за 2017-2020 гг. оценивались следующие показатели – количественные (организационное ядро, количество участников малой группы), вовлеченность в решение игровых задач. Группы формировались из числа студентов бакалавриата и магистратуры направления 10.00.00 «Информационная безопасность», 4 курс бакалавриата, 2 курс магистратуры, 3-5 курс специалитета. Формирование смешанных групп предполагало, что функции организаторов выполняют студенты магистратуры и/или специалитета, а выполняют задания студенты бакалавриата, поэтому далее при оценке успеваемости в эксперименте указана успеваемость студентов бакалавриата.

2. Для учебных групп, из состава которых формировались малые группы, оценивался срез успеваемости на уровне 80% от максимального (количество студентов, удовлетворяющих такому критерию). Число студентов, которые участвовали в исследовании – 80 человек (четыре отдельных экспериментальных группы). Ретроспективно (в том числе по данным до начала проекта) оценивалась успеваемость за 2017-2020 гг., с особым вниманием на 2018 гг. – год первичного внедрения игровых кейсов.

3. Для сетевых коллабораций, сформированных в ходе проекта фонда Потанина, изучался вторичный отклик методом анкетирования по следующим вопросам: а) оцените насыщенность обучения новой информацией (высокая, средняя, низкая), б) оцените объем изложенного материала (достаточно, недостаточно), в) насколько сложно Вам было воспринимать материал (легко, нормально, трудно)?

Результаты исследования малых групп

В ходе эксперимента были получены следующие показатели по малым группам (таблица 3):

Таблица 3

Показатели малых групп

Контрольная точка	Показатель 1	Показатель 2	Показатель 3
Ретроспективно (по архивным данным)			
01.12.2014	6/6	6	3/6
01.12.2015	8/6	4	4/4
01.06.2016	3/4 (по двум группам)	4	4/4
25.02.2017	7/7	4	4/4
Во время непосредственного проведения эксперимента			
01.12.2018	6/6	4	4/4
01.12.2019	6/4	4	3/4*
01.10.2020	4/4	4	4/4

*результат учета восстановленных в учебной группе студентов с прошлого года; академический отпуск.

Для отдельных групп был получен следующий срез активности в рамках исследования (показаны доли среди достигших успеваемости выше 4.0 по итогу эксперимента, но не позднее двенадцатинедельного среза):

Таблица 4

Соотношения количества обучающихся по оценке участия в решении игровых задач

Учебный год	Доля студентов с соответствующим уровнем освоения компетенции ПК-14 для отдельных малых групп, (% на момент среза 6 недель)/(% на момент среза 12 недель)							
	Активное участие		Работа в группе		Пассивное участие		Не участвовали	
	Очное	Сеть	Очное	Сеть	Очное	Сеть	Очное	Сеть
2016/2017	<u>4,51</u> 8,2	-	<u>0</u> 0	-	<u>18,2</u> 31,8	-	<u>77,3</u> 50,0	-
После начала эксперимента								
2017/2018	<u>27,8</u> 38,9	<u>14,7</u> 14,7	<u>38,9</u> 61,1	<u>79,4</u> 85,3	<u>33,3</u> 0	<u>11,1</u> 0	<u>0</u> 0	<u>0</u> 0
2018/2019	<u>31,6</u> 36,8	<u>13,9</u> 16,6	<u>36,8</u> 36,8	<u>72,2</u> 77,8	<u>10,5</u> 10,5	<u>13,9</u> 5,6	<u>21,1</u> 15,9	<u>0</u> 0
2019/2020	<u>25,0</u> 25,0	<u>18,8</u> 18,8	<u>50,0</u> 65,0	<u>65,6</u> 75,0	<u>25,0</u> 10,0	<u>15,6</u> 6,2	<u>0</u> 0	<u>0</u> 0

Здесь для коллабораций с использованием дистанционного обучения принято обозначение «Сеть», для коллабораций с использованием очного обучения – «Очное». В эксперименте участвовало 80 студентов очного обучения и 102 студента в коллаборациях с использованием дистанционного обучения.

В результате можно зафиксировать следующие основные результаты: для малой группы был зафиксирован оптимальный размер – для 4 участников вовлеченность в процесс (для достижения уровня успеваемости на уровне 4.0 для 80% группы); количество организаторов игрового кейса по результатам эксперимента составило в среднем 5,5, но с тенденцией к уменьшению. Проведено 14 экспериментальных игровых кейсов с замером показателей малых групп (из 42 проведенных кейсов всего в рамках дисциплин). Видно, что количество активных студентов остается практически стабильным с начала эксперимента, тогда как количество работающих в группе студентов резко возросло и оставалось стабильным (с учетом размера учебной группы). При этом количество не участвующих в освоении компетенции в первые 12 недель обучения практически было сведено к нулю.

Результаты исследования учебных групп

В ходе эксперимента были получены следующие показатели по учебным группам (таблица 4):

Таблица 4

Результаты учебных групп

Учебный год	Количество студентов	Количество студентов, имеющих успеваемость выше 4.0 (срез 6 недель, проц.)	Количество студентов, имеющих успеваемость выше 4.0 (срез 12 недель, проц.)
Ретроспективно (до проведения эксперимента)			
2016/2017	44	22,7	36
Во время непосредственного проведения эксперимента			
2017/2018	36	66	61
2018/2019	38	31,5	36
2019/2020	40	75	75

Здесь можно зафиксировать следующий результат: несмотря на очевидный эффект от первого внедрения (статистически значимое отклонение на уровне значимости 95% по результатам z-теста), в следующем году имело место снижение общей успеваемости группы по результатам контрольных срезов; в 2019 г. успеваемость снова показала существенный рост. В целом можно сделать вывод, что если на уровне малых групп воспроизводимость организационно-педагогических условий, в том числе и на уровне вовлеченности в учебный процесс, сохраняется, то на уровне исследования успеваемости учебных групп из-за пока не выявленного дополнительного фактора имеет место выброс. Необходимо заметить, что качество группы с точки зрения общей успеваемости не считалось существенным фактором; авторы полагают, что решение игрового кейса, предполагающего формирование временных коллабораций, способно быть эффективным и в условиях общего низкого уровня группы. Также можно отметить, что результаты после внедрения кейсов в образовательный процесс достигаются уже на первом срезе и остаются стабильными; это удобно для прогнозирования общего результата работы малых групп в рамках учебной группы в целом.

Результаты исследования групп сетевых коллабораций

По результатам исследования выборочного отклика участников сетевых коллабораций, полученного в ходе опроса, можно отметить, что вовлеченность и изучение материала оставались на стабильно высоком уровне как в прошлые годы, так и на момент среза по итогам эксперимента. Сетевая коллаборация показала хороший результат в плане охвата объема предложенного материала, коммуникации, обмена опытом в ходе эксперимента.

В ходе эксперимента были получены следующие показатели по учебным группам (таблица 5):

Таблица 5

Результаты опроса (сетевая коллаборация)

Учебный год	Количество студентов	Отклик вопрос 1 (высокая или средняя насыщенность, проц.)	Отклик вопрос 2 (достаточно, проц.)	Отклик вопрос 3 (легко либо нормально, проц.)
Ретроспективно (до проведения эксперимента)				
2016/2017	-	-	-	-
Во время непосредственного проведения эксперимента				
2017/2018	34	97	76	94
2018/2019	36	91	72	88
2019/2020	32	97	84	97

Если рассматривать сетевую коллаборацию как устойчивое звено проекта, то необходимо оценить формирование активных связей между участниками эксперимента. Часть такой работы, ранее представленной авторами настоящего исследования, можно обобщить следующим образом (оценивались связи организаторов проекта, сформированные в рамках группы проекта SEQuest в социальной сети Вконтакте за 4 года действия проекта (2017-2020 гг.): 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 социаль-

ных 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. Высокоинтенсивных связей среди участников проекта 21,87% (исключая общение вне соцсети). Неактивных связей 18,75%. Видно, что стабильные связи сформировались на длительный период, что обеспечивает возобновляемость проекта и возможность его реинтеграции в образовательный процесс по мере необходимости.

Обсуждение результатов

Полученные данные свидетельствуют, что при внедрении геймифицированных элементов в подготовку студентов – будущих специалистов по защите информации возникают новые возможности, такие как быстрое погружение в дисциплину и выделение устойчивых малых групп, повышающих вовлеченность учебной группы в целом и ее активность. Сами геймифицированные элементы в этом смысле представляют собой лишь инструмент и могут быть модифицированы для лучших результатов. В частности, в этом направлении ведутся уже длительное время исследования С. Танга и соавторов [16]. Формирование или использование готовых моделей для разработки игровых задач, безусловно, повышает воспроизводимость организационно-педагогических условий при внедрении геймификации.

Если рассматривать другую сторону описанных в работе результатов, то на уровне профессиональных и надпрофессиональных навыков студентов формируется как умение взаимодействовать в рамках игры, представлять оценку в виде процесса, концепции, имитирующей реальные задачи – так называемой «серьезной игры», при этом для преподавателя можно предоставлять средства оценки того или иного игрового решения [17], так и возможность в дальнейшем решать сугубо профессиональные задачи, такие как уязвимость конкретного сотрудника к социально-инженерным атакам [18] на примере действий или задач игроков.

Представляется, что такой подход в подготовке является перспективным. Стоит отметить и то, что применение в рамках подхода стандартизированных платформ, таких как LMS Moodle, позволило бы автоматизировать требования к кейсам и другим геймифицированным элементам, что в сочетании с формальными моделями привело бы к быстрому масштабированию и развертыванию в различных образовательных организациях результатов исследования; такие исследования, учитывающие опыт, к примеру, авторов статьи [19], запланированы в дальнейшем. Также интересным направлением развития исследования представляется авторам и оценка влияния геймификации на индивидуальные образовательные траектории, что может потребовать отдельного изучения предпочтений пользователей при решении геймифицированных задач в области защиты информации. Широкое поле для действий в этом направлении может предоставить опыт участия студентов университета в соревнованиях в области компьютерной безопасности Capture the Flag [21].

Стоит отметить и возможность обмена опытом в области сетевых коллабораций, что в рамках подхода гарантирует инвариантность подготовки студентов – будущих специалистов в области защиты информации за счет академической мобильности (в том числе и с использованием дистанционных технологий).

Заключение

В ходе проведенного исследования была выполнена оценка и анализ внедрения геймифицированных элементов определенного типа (игровой кейс) в рамках дисциплины «Управление информационной безопасностью» для направления 10.00.00 «Информационная безопасность» (уровни бакалавриата, специалитета, магистратуры). Основой исследования было прохождение игровых кейсов, формирующих определенную компетенцию, студентами старшего курса бакалавриата 10.03.01.

По результатам исследования можно отметить, что для исследуемого объекта характерно формирование устойчивых малых групп, работа в которых повышает вовлеченность студентов в процесс изучения дисциплины и формирования компетенции (вовлеченность до 100% в малых группах), до 30% уменьшается время выполнения заданий для освоения компетенции для активных студентов и студентов, работающих в малых группах, формируются устойчивые коллаборации для решения заданий и при дистанционном обучении, в том числе среди разработчиков и организаторов проведения игровых кейсов (до 21,9% стабильных активных связей).

В целом можно отметить, что проведенное исследование показывает повышение эффективности формирования определенной компетенции бакалавров информационной безопасности за счет большей вовлеченности и сокращения времени выполнения необходимых заданий, а также за счет формирования стабильных связей и коллабораций внутри учебной группы. При этом результаты учебной группы в целом могут зависеть и от других факторов.

Вместе с тем показанные результаты апробации говорят о возможном положительном эффекте внедрения геймифицированных элементов от обучения отдельной дисциплине до развития методики геймификации.

Если же говорить о конкретных положительных эффектах от внедрения подхода, то можно отметить формирование и актуализацию целей обучения при геймификации; актуализацию и мониторинг задач обучения; актуализацию методических указаний к геймифицированным задачам; их комплексирование и оценка на периодической основе.

Финансирование

Работа поддержана Российским фондом фундаментальных исследований, проект № 19-013-00711

REFERENCES

1. Ortiz M., Chiluita K., Valcke M. Gamification and learning performance: A systematic review of the literature. *Proceedings of the 11th European Conference on Games Based Learning*, 2017.
2. Chubik P., Chuchalin A., Soloviev M., Zamyatina O. Training of elite specialists in the field of engineering and technology. *Education Studies Moscow*, 2013, no. 2, pp. 188-208.
3. Solodovnikova O., Zamyatina O., Mozgaleva P., Lycheva M. Formation of competencies of an elite technical specialist. *Professional education in Russia and abroad*, 2013, no. 3 (11), pp. 65-71.
4. Tikhomirov V., Dneprovskaya N. and Yankovskaya E. Development of University's Web-Services Smart Education and Smart e-Learning. *Smart Innovation, Systems and Technologies*, 2015, no. 41, pp. 265-271.
5. 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.

6. 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, vol. 76(4), pp. 6051–6064.
7. Surendele G., Murwa V., Yun H., Kim Y.S. The role of gamification in education – a literature review. *Contemporary Engineering Sciences*, 2014, vol. 7, pp. 1609–1616.
8. Toda A., Toledo Palomino P., Oliveira W., Rodrigues L., Klock A., Gasparini I., Cristea A. and Isotani, S. How to Gamify Learning Systems? An Experience Report using the Design Sprint Method and a Taxonomy for Gamification Elements in Education. *Educational Technology & Society*, 2020, vol. 22, pp. 47-60.
9. Pape S., Goeke L., Quintanar A., Beckers K. Conceptualization of a CyberSecurity Awareness Quiz. In proc. *ESORICS 2020 International Workshops MSTEC*, 2020.
10. Sillanpää M., Hautamäki J. Social Engineering Intrusion: A Case Study. in proc. *IAIT2020: The 11th International Conference on Advances in Information Technology*, 2020, p. 1-5.
11. Hart S., Margheri A., Paci F., Sassone V. Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security*, 2020, vol. 95, 101827.
12. Ali Zani A., Norman A., Ghani N. A review of security awareness approaches: Towards achieving communal awareness / Editor(s): Vladlena Benson, John Mcalaney / A. Ali Zani, A. Norman, N. Ghani. In *Cyber Influence and Cognitive Threats*, Academic Press, 2020, pp. 97-127.
13. Aldawood H., Skinner G. Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering. In proc. *2019 Cybersecurity and Cyberforensics Conference*, 2019, pp. 111-117.
14. Janelli, M. E-Learning in Theory, Practice, and Research. *Education Studies Moscow*. 2018, no. 4, pp. 81-98.
15. Zolotarev V., Maro E., Kulikova S. New approach to activity evaluation for social network based student collaboration. In proc. *12th IEEE International Conference on Application of Information and Communication Technologies (AICT 2018)*, 2018, pp. 374-380
16. Tang S. and Hanneghan M. Game Content Model: An Ontology for Documenting Serious Game Design. In proc. *2011 Developments in E-systems Engineering*, 2011, Dubai, pp. 431-436.
17. Emmerich K., Bockholt M. Serious Games Evaluation: Processes, Models, and Concepts. In: Dörner R., Göbel S., Kickmeier-Rust M., Masuch M., Zweig K. (eds) *Entertainment Computing and Serious Games. Lecture Notes in Computer Science*, vol. 9970, pp 265-283.
18. Mouton, F. Social Engineering Attack Detection Model. Thesis for PhD Computer Science, advisor: Venter H.S. University of Pretoria, 2018.
19. Dicheva D., Irwin K., Dichev C., Talasila S. A course gamification platform supporting student motivation and engagement. In proc. *International Conference on Web and Open Access to Learning (ICWOAL)*, Dubai, 2014, pp. 1-4.
20. Tondello Gustavo F., Nacke Lennart E. Validation of User Preferences and Effects of Personalized Gamification on Task Performance. *Frontiers in Computer Science*, 2020, vol. 2, no. 29.
21. Trickle E., Disperati F., Gustafson E. Shell We Play A Game? CTF-as-a-service for Security Education. In proc. *USENIX Workshop on Advances in Security Education (ASE)*, 2017.

Информация об авторах
Сафонов Константин Владимирович
(Россия, г. Красноярск)

Профессор, доктор физико-математических наук, заведующий кафедрой прикладной математики Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева
E-mail: safonovkv@rambler.ru
ORCID ID: 0000-0003-0405-3065
Scopus ID: 6602800656

Ищукова Евгения Александровна
(Россия, г. Таганрог)

Доцент, кандидат технических наук, доцент кафедры безопасности информационных технологий Южный федеральный университет
E-mail: jekky82@mail.ru
ORCID ID: 0000-0002-6818-1608
Scopus ID: 36561670100
ResearcherID L-4489-2016

Золотарев Вячеслав Владимирович
(Россия, г. Красноярск)

Доцент, кандидат технических наук, заведующий кафедрой безопасности информационных технологий Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева
E-mail: amida.2@yandex.ru
ORCID ID: 0000-0002-8054-8564
Scopus ID: 57200777760
ResearcherID: B-5438-2017

Information about the authors

Konstantin V. Safonov
(Russia, Krasnoyarsk)
Professor, Doctor of Physical and Mathematical Sciences, Head of the Department of Applied Mathematics Reshetnev Siberian State University of Science and Technology
E-mail: safonovkv@rambler.ru
ORCID ID: 0000-0003-0405-3065
Scopus ID: 6602800656

Evgeniya A. Ischukova
(Russia, Taganrog)

Associate Professor, PhD in Technical Sciences, Associate Professor of the Department of Information Technology Security South Federal University
E-mail: jekky82@mail.ru
ORCID ID: 0000-0002-6818-1608
Scopus ID: 36561670100
ResearcherID L-4489-2016

Vyacheslav V. Zolotarev
(Russia, Krasnoyarsk)

Associate Professor, PhD in Technical Sciences, Head of the Department of Information Technology Security Reshetnev Siberian State University of Science and Technology
E-mail: amida.2@yandex.ru
ORCID ID: 0000-0002-8054-8564
Scopus ID: 57200777760
ResearcherID: B-5438-2017