Высшее образование в России Vysshee obrazovanie v Rossii = Higher Education in Russia

ISSN 0869-3617 (Print), ISSN 2072-0459 (Online) http://vovr.elpub.ru

Возможности сторителлинга в преподавании кибербезопасности

Научная статья
DOI: 10.31992/0869-3617-2025-34-3-113-137

Паюсова Татьяна Игоревна – доцент кафедры информационной безопасности Школы компьютерных наук, ORCID: 0000-0003-4923-1689, t.i.payusova@utmn.ru
ФГАОУ ВО «Тюменский государственный университет», Тюмень, Российская Федерация
Адрес: 625003, г. Тюмень, ул. Перекопская, 15А

Аннотация. *Современные угрозы в большей степени смещают фокус информационной безопасности с технической составляющей на социальный контекст. В процессе обучения киберзащите можно выделить ряд наиболее актуальных вызовов, предполагающих использование более эффективных методов подготовки будущих специалистов. Настоящее исследование отвечает на вопрос о возможностях сторителлинга в преподавании кибербезопасности, о способности эмоциональных историй влиять на повышение мотивационно-ценностной включённости студентов и преподавателей, формировать междисциплинарный подход и понимание сложных причинно-следственных связей в рамках различных предметных областей, помогать преодолевать нехватку у обучающихся профессиональной «насмотренности» в области уязвимостей и возможных потенциальных векторов атак. Исследование проводилось с 1 по 31 октября 2024 г. на базе Школы компьютерных наук ФГАОУ ВО «Тюменского государственного университета» в рамках элективных курсов «Основы кибербезопасности» и «Введение в пентестинг (кибербезопасность)». Результаты исследования показали, что применение сторителлинга позволяет решить задачу эмоционально-ценностного вовлечения, достичь более глубокого впечатления и понимания учебных тем, развить способность сопереживать жертвам киберпреступлений. Также необходимо отметить долгосрочное воздействие сторителлинга. Дальнейшие исследования могут быть связаны с алгоритмизацией процесса написания историй, изучением отличий между устной и письменной подачей, исследованием приёмов повышения эмоциональной вовлечённости, применением различных форматов сторителлинга, уточнением роли преподавателя при знакомстве обучающихся с историями.*

Ключевые слова: *образовательный процесс, инструменты преподавания, сторителлинг, кибербезопасность, сценарное моделирование, вирус-шифровальщик, уязвимость Heartbleed*

Для цитирования: *Паюсова Т.И.* Возможности сторителлинга в преподавании кибербезопасности // Высшее образование в России. 2025. Т. 34. № 3. С. 113–137. DOI: 10.31992/0869-3617-2025-34-3-113-137

Storytelling Opportunities in Teaching Cybersecurity

Original article
DOI: 10.31992/0869-3617-2025-34-3-113-137

Tatyana I. Payusova – Associate Professor of the Department of Information Security of the School of Computer Science, ORCID: 0000-0003-4923-1689, t.i.payusova@utmn.ru
FGAOU VO "Tyumen State University", Tyumen, Russian Federation
Address: 15A Perekopskaya str., Tyumen, 625003, Russian Federation

Abstract. Modern threats are shifting the focus of information security from the technical component to the social context to a greater extent. In the process of cyber defense training, a number of the most pressing challenges can be identified, involving the use of more effective methods of training future specialists. This study answers the question about the possibilities of storytelling in teaching cybersecurity, about the ability of emotional stories to influence the increase of motivational and value involvement of students and teachers, to form an interdisciplinary approach and understanding of complex cause-and-effect relationships within various subject areas, to help students overcome the lack of professional "awareness" in the field of vulnerabilities and possible potential attack vectors.. The study was conducted from October 1 to October 31, 2024. at the Tyumen State University School of Computer Science as part of the elective courses "Fundamentals of Cybersecurity" and "Introduction to Pentesting (Cybersecurity)". The results of the study showed that the use of storytelling makes it possible to solve the problem of emotional and value involvement, achieve a deeper impression and understanding of educational topics, and develop the ability to empathize with victims of cybercrime. The long-term effects of storytelling should also be noted. Further research may be related to the algorithmization of the story writing process, the study of the differences between oral and written presentation, the study of techniques to increase emotional engagement, the use of various storytelling formats, clarifying the role of the teacher in introducing students to stories.

Keywords: educational process, teaching tools, storytelling, cybersecurity, scenario modeling, ransomware, Heartbleed vulnerability

Cite as: Payusova, T.I. (2025). Storytelling Opportunities in Teaching Cybersecurity. *Vysshee obrazovanie v Rossii* = Higher Education in Russia. Vol. 34, no. 3, pp. 113-137, doi: 10.31992/0869-3617-2025-34-3-113-137 (In Russ., abstract in Eng.).

Введение

Современные трансформационные процессы, в том числе связанные с переходом от Индустрии 4.0 к концепции Общества 5.0, сопровождаются изменениями в области информационной безопасности (ИБ) и киберзащиты [1]. С развитием информационных и коммуникационных технологий цифровые риски проявили свою способность причинять осязаемый вред, в том числе, активировать сложные причинно-следственные цепочки на политической, экономической, социальной и культурной аренах. Вмешательство в выборы, экономические кризисы и экологические катастрофы, социальные протесты и культурные конфликты – таковы примеры некоторых событий, возникновение которых всё чаще связывают с действиями хакеров и киберпреступников. Например, компьютерный «червь» *Stuxnet* нанёс непо-

правимый урон ядерной программе Ирана[1]; хакерская атака на серверы Университета Восточной Англии стала причиной утечки данных о глобальном потеплении и последующих мировых климатических прениях 2009 года[2]; взлом хранилища радиоактивных отходов в США также подчеркнул экологические и социальные риски[3]; а действия «теневых» майнинговых ферм периодически приводят к дефициту электроэнергии и аварийным ситуациям на электросетевых комплексах[4].

На специалистов по киберзащите также ложится новая степень ответственности: любая халатность или неточность, отсутствие системного подхода и стратегического планирования при обеспечении безопасности может привести к «эффекту бабочки» и катастрофическим последствиям на локальном и глобальном уровнях [2: 3]. Можно наблюдать смещение технического фокуса информационной безопасности в сторону социальной миссии, а также исполнение системами защиты новых ролей, связанных с достижением и поддержкой общественного равновесия.

Дискуссии вокруг стратегии гуманизации и гуманитаризации инженерно-технического образования, как попытки компенсировать однобокость и исключительно прикладную составляющую образовательных программ, ведутся исследователями с начала 90-х гг. прошлого века [4]. Авторы [5] отмечают роль университета в первую очередь как института развития человека и общества, указывают на наиболее востребованные концепции современного образования, связанные с открытием новых смыслов для студентов и «сдвигом горизонта» восприятия и мировоззрения. Исследования [6; 7] также обозначают важность воспитательной задачи университетов, направленной на гражданское самоопределение и индивидуально-личностную самореализацию обучающихся. Безопасность и сэйв-отношения рассматриваются как основополагающие ценности будущих специалистов при дизайне образовательных инженерно-технических программ [8].

Несмотря на попытки внедрить стратегию гуманизации в обучающий процесс, современные эксперты по-прежнему отмечают «экзистенциальный вакуум» и прагматичное отношение к инженерно-техническому образованию [9]. При этом рынок труда технических специалистов и цифровой ландшафт указывают на запрос и востребованность универсальных, общекультурных компетенций, а также ценностно-смысловых ориентиров.

Согласно данным *Positive Technologies*, в 2024 г. дефицит кадров в РФ в области ИБ составил около 50 тыс. человек, что соответствует 45% от общего числа занятых в сфере киберзащиты[5]. Несмотря на представленное количество образовательных программ подготовки по специальностям и направлениям 10.00.00 «Информационная безопасность»[6]

[1] Шпионский ярлык: история трояна Stuxnet // Журнал Хакер.ru. URL: https://xakep.ru/2010/11/18/53950/ (дата обращения: 18.11.2024).

[2] Русские хакеры развенчали миф о глобальном потеплении // Информационный портал по безопасности SecurityLab.ru. URL: https://www.securitylab.ru/news/388013.php (дата обращения: 18.11.2024).

[3] СМИ: в США под атаку хакеров попало хранилище радиоактивных отходов // Сетевое издание РИА Новости. URL: https://ria.ru/20230616/ataka-1878632389.html (дата обращения: 18.11.2024).

[4] Битва за ресурсы: особенности нелегального криптомайнинга в облачных сервисах // Блог компании Trend Micro. URL: https://habr.com/ru/companies/trendmicro/articles/656153/ (дата обращения: 18.11.2024).

[5] Дефицит кадров в информационной безопасности в РФ составляет 50 тыс. человек // Информационное агентство ТАСС. URL: https://tass.ru/ekonomika/21018685 (дата обращения: 18.11.2024).

[6] По данным Vuzopedia.ru (каталог вузов, специальностей, профессий, материалов на тему высшего образования). URL: https://vuzopedia.ru/ (дата обращения: 18.11.2024).

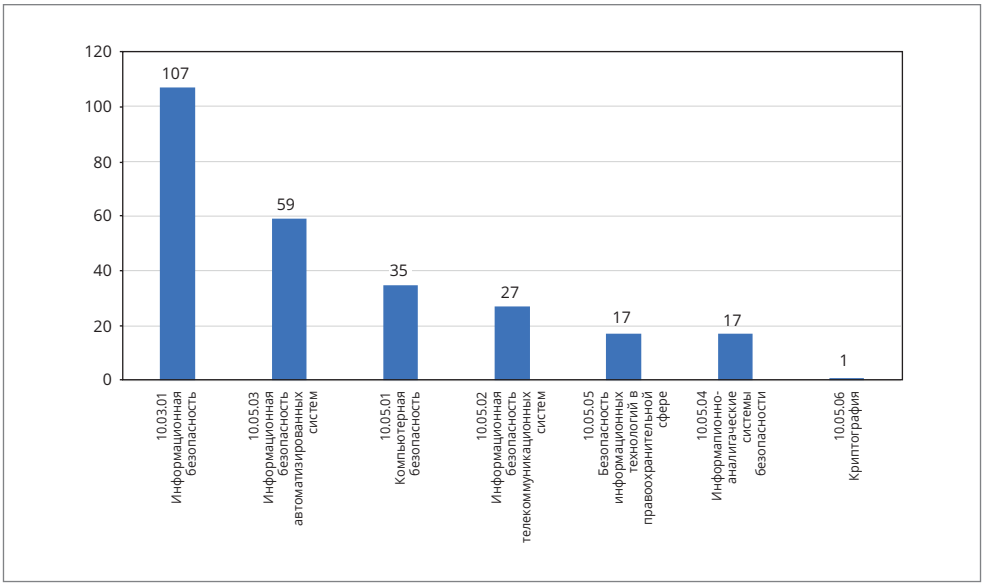

Рис. 1. Статистика по количеству вузов, осуществляющих подготовку по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» (направление 10.03.01 «Информационная безопасность» представляет бакалавриат, остальные из указанных программ подготовки представляют специалитет)

Fig. 1. Statistics on the number of universities providing training in specialties and areas of study 10.00.00 "Information Security" (the area 10.03.01 "Information Security" represents the bachelor's degree, the rest of the indicated training programs represent a specialist's degree)

(*Рис. 1*), аналитики Центра стратегических разработок «Северо-Запад» и *компании Positive Technologies* отмечают, что система профессионального образования не покрывает растущий спрос на рынке труда[7]. Эксперты прогнозируют, что к 2027 г. потребность в кадрах по информационной безопасности может вырасти до 235–261 тыс. человек, а дефицит составит от 54 до 65 тыс. специалистов[8].

Исследования «Лаборатории Касперского» показывают, что компании всё больше осознают необходимость обучения не только IT-кадров, но и всех работников, включая руководителей, т. к. повышение киберграмотности среди всех сотрудников становится ключевым компонентом успешного функционирования, что требует вовлечения специалистов из различных областей, включая гуманитарные и управленческие специальности[9]. Также можно отметить, что навыки, необходимые специалистам по киберзащите, меняются быстрее, чем в других направлениях передовых технологий [10]. Кроме того, стремительное увеличение атак, связанных с вредоносным программным обеспечением и

[7] Эксперты оценили дефицит кадров на рынке информационной безопасности через три года // Сетевое издание «forbes.ru». URL: https://www.forbes.ru/tekhnologii/514200-eksperty-ocenili-deficit-kadrov-na-rynke-informacionnoj-bezopasnosti-cerez-tri-goda (дата обращения: 18.11.2024).

[8] IT-кадры найдут выход. Как компании в 2024 году справляются с дефицитом IT-специалистов // Сетевое издание «Коммерсантъ». URL: https://www.kommersant.ru/doc/7230882 (дата обращения: 18.11.2024).

[9] Может рухнуть при первой атаке. Почему компаниям важно прокачивать киберграмотность // Блог компании «Лаборатория Касперского». URL: https://habr.com/ru/specials/792652/ (дата обращения: 18.11.2024).

эксплуатацией технических уязвимостей на фоне развития искусственного интеллекта и машинного обучения требует новых подходов к реагированию на инциденты, повышения технической «насмотренности» и большей способности решать практические задачи[10].

Новые вызовы цифрового ландшафта, связанные с усилением междисциплинарных связей, смещением фокуса с технических аспектов на социальные, увеличением числа вредоносного программного обеспечения и усложнением приёмов атак с использованием искусственного интеллекта и машинного обучения предполагают переосмысление методов обучения ИБ. Возникают вопросы о недостаточности традиционных форм трансляции знаний, ориентированных только на техническую составляющую исключительно в области защиты информации. Можно отметить, что классические подходы не позволяют в полной мере изучить многогранные проблемы, распространённые в реальных сценариях кибербезопасности [11]. Необходимы новые форматы и инструменты для обучения и воспитания будущих специалистов в области кибербезопасности.

Постановка проблемы исследования

Одной из актуальных проблем в преподавании ИБ выступает недостаточная мотивационно-ценностная включённость студентов и преподавателей. Студенты, не ощущающие ценности и значимости изучаемого материала, могут проявлять низкий уровень вовлечённости и интереса к предмету, что выражается в недостаточной активности на занятиях, низкой успеваемости или отсутствии желания углублённо изучать тему занятия. Без должной мотивации студенты могут воспринимать курс ИБ как формальность, что снизит их готовность к будущей профессиональной деятельности. Преподаватели, не имеющие внутренней мотивации, также могут не уделять должного внимания актуализации учебных материалов и внедрению инновационных методов обучения. Это создаёт разрыв между теорией и практикой [12]. Качественная подготовка специалистов требует значительных усилий и настойчивости, а мотивация может стать ключом к постоянному и успешному изучению материала [13; 14].

Также можно отметить отсутствие должного внимания в процессе обучения ИБ к социальной составляющей и междисциплинарному подходу, в том числе предполагающему изучение гуманитарных аспектов информационной безопасности [15; 16]. Ряд авторов указывают, что если практические навыки в современной системе кибероборазования возможно оттачивать, например, с помощью соревнований в формате *Capture The Flag (CTF)*, то гуманитарные аспекты ИБ, связанные с человеческим фактором, в большинстве случаев игнорируются [17; 18]. Преподавание ИБ часто сосредоточено исключительно на технических аспектах (программировании, сетевых технологиях, криптографии), что может привести к недостаточному пониманию социальных, культурных и психологических факторов, влияющих на безопасность информации. Например, игнорирование аспектов социальной инженерии и поведения пользователей снижает эффективность системы защиты, поскольку большинство атак направлено именно на человека, а не на технологии. Интеграция гуманитарных аспектов в учебный процесс поможет подготовить более квалифицированных специалистов, способных эффективно справляться с современными вызовами в области информационной безопасности, проявлять эмпатию и сопереживать жертвам компьютерных преступлений [19]. Инструменты обучения, способные спра-

[10] Прогноз развития киберугроз и средств защиты информации – 2025 // Николай Головко, Независимый информационно-аналитический центр по информационной безопасности Anti-Malware.ru. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Cyber-Threats-and-security-tools-development-forecast-2025 (дата обращения: 18.11.2024).

виться с обозначенным вызовом, должны предложить студентам готовый социальный контекст, раскрыть человекоцентричность задач ИБ, показать всеобщую связность, но при этом не потерять профессиональной направленности и технической составляющей образовательного материала.

Также авторы среди современных трудностей преподавания ИБ выделяют нехватку инфраструктуры и профессиональной «насмотренности» для формирования практических навыков выявления и устранения уязвимостей [20–24]. «Насмотренность» выступает ключевым элементом подготовки специалистов [25; 26], в том числе будущих профессионалов в области ИБ, и помогает развитию необходимых навыков для выявления и распознавания уязвимостей и атак. Развитие «насмотренности» может быть достигнуто через практическое обучение, анализ инцидентов и использование современных инструментов кибербезопасности. При отсутствии соответствующей инфраструктуры детальное теоретическое представление материала способно частично компенсировать отсутствие практического опыта: преподаватель выступает проводником или гидом студентов в рамках «экскурсии» в мир уязвимостей и атак, подсвечивает, обращает внимание группы на наиболее важные и ключевые моменты. Перечисленные аспекты обозначают важность и подчёркивают необходимость внедрения более эффективных методов обучения ИБ, способных дополнить традиционные формы преподнесения материала.

На основании контент-анализа источников [27–30] в *таблице 1* показаны усреднённые оценки некоторых форм представления обучающих материалов с точки зрения времени подготовки, доступности для преподавателей и обучающихся, сложности восприятия и степени эмоциональной вовлечённости. Цветовое обозначение отражает сильные стороны каждой формы работы: наиболее интенсивный оттенок синего цвета отображает наилучшие значения в рассматриваемой категории, более светлые ячейки таблицы отмечены для форм, показавших меньшую результативность по сравнению с остальными сравниваемыми элементами. Оценки могут варьироваться в зависимости от индивидуальной реализации каждой из представленных форм подачи материала. Рядом с формой изучения материала в таблице 1 в скобках указаны факторы, которые могут влиять на вариативность оценок: например, на сложность восприятия визуальных историй может влиять качество выполненной визуализации.

Результаты сравнительного анализа показали, что в отличие от большинства представленных форм преподавания, сторителлинг создаёт эмоциональную связь с аудиторией, тем самым усиливая когнитивную деятельность обучающихся [31–33]. В [34] показаны результаты опроса, в рамках которого 78% студентов отметили, что сторителлинг делает процесс обучения более привлекательным и вовлекающим, усиливает мотивационно-ценностную составляющую при изучении дисциплины. При этом сторителлинг обладает высокой степенью доступностью и низкой сложностью восприятия, но может потребовать значительного времени для подготовки учебного материала и представления его в форме эмоционального повествования. Также можно говорить о недостаточной изученности сторителлинга в рамках определённых дисциплин и предметных областей.

Применение сторителлинга при обучении экономическим дисциплинами представлено в [35; 36]. Ряд авторов обращаются к искусству рассказывать истории при изучении иностранных языков [37–40]. Обучение через истории показано в контексте образовательного процесса музыкантов, менеджеров, педагогов [41–44]. Преподавание технических дисциплин с помощью сторителлинга нашло отражение в работах [45–49]. Можно отметить, что французское Министерство обороны привлекает режиссёров, сценаристов, художников для разработки сценари-

Таблица 1

Результаты сравнительного анализа некоторых форм изучения материала

Table 1

The results of a comparative analysis of some forms of material study

Форма изучения материала (в скобках указаны факторы, влияющие на сравнительные оценки)	Время подготовки	Доступность	Сложность восприятия	Эмоциональная вовлечённость
Визуальные истории и графические новеллы (сложность сюжета и стиля, а также качество визуализации)	Среднее/ Долгое	Средняя	Низкая/ Средняя	Средняя/ Высокая
Аудиовизуальные материалы (содержание презентуемого материала, качество звука. Также можно отметить, что аудиальное восприятие материала может в большей степени, чем другие форматы, вызывать затруднения)	Среднее/ Долгое	Средняя	Средняя	Низкая/ Средняя
Интерактивные истории и ролевые игры (степень интерактивности и мастерство «ведущего»)	Среднее/ Долгое	Высокая	Низкая/ Средняя	Высокая
Кейсы (сложность и детальность описания рассматриваемых кейсов)	Среднее/ Долгое	Высокая	Низкая/ Средняя	Низкая
Дискуссии и дебаты (уровень подготовки участников и «ведущего»)	Среднее	Высокая	Средняя/ Высокая	Средняя/ Высокая
Мультимедийные презентации (содержание презентуемого материала и дизайна презентации)	Среднее/ Долгое	Высокая	Низкая/ Средняя	Низкая/ Средняя
Сторителлинг (качество подготовленной истории в формате сторителлинга и уровень мастерства рассказчика)	Среднее/ Долгое	Высокая	Низкая	Высокая
Симуляционные платформы (сложность симуляции)	Долгое	Низкая	Высокая	Высокая
Социальные роботы (степень развития и «персонализации» робота)	Долгое	Низкая	Средняя/ Высокая	Высокая
Специализированные инструменты (параметры конкретного инструмента и уровень подготовки пользователя)	Долгое	Низкая/ Средняя	Средняя/ Высокая	Низкая

ев инцидентов безопасности в рамках *Red Teaming*, или «красной команды»[11].

При этом на недостаточную изученность сторителлинга в рамках технических и инженерных дисциплин, в том числе в преподавании ИБ *(Storytelling-based Cybersecurity Education*), указывают исследования [50–53]. «Сторителлинг рассматривается как перспективный подход к повышению осведомлённости и образования обучающихся в области кибербезопасности… Однако он лишь в незначительной степени изучен профессионалами» [52].

Настоящее исследование направлено на получение ответа на вопрос о возможностях сторителлинга в преподавании ИБ, о его способности влиять на повышение мотивационно-ценностной включённости студентов и преподавателей, формировать междисциплинарный подход и понимание сложных причинно-следственных связей в рамках различных предметных областей, преодолевать нехватку у обучающихся профессиональной «насмотренности» в области уязвимостей и возможных потенциальных векторов атаки на информационную систему.

[11] Французская армия хочет сказку сделать былью. URL: https://www.kommersant.ru/doc/4615439 (дата обращения: 14.11.2024).

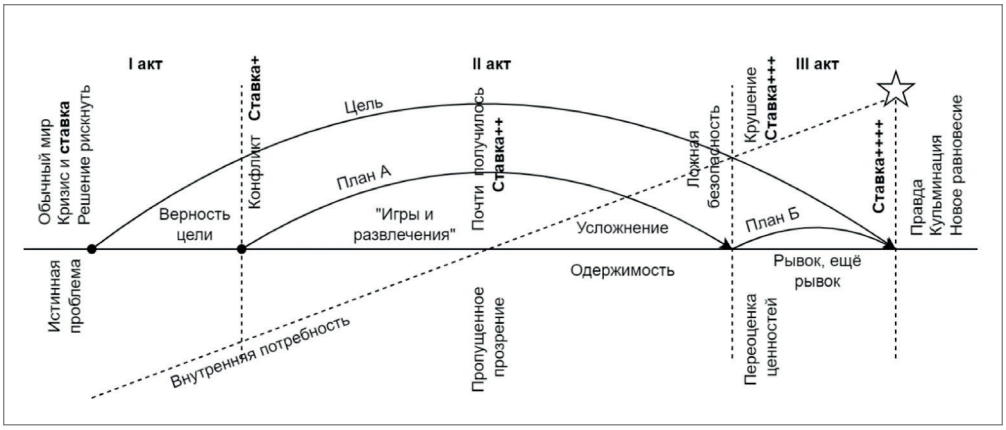

Рис. 2. Трёхактная структура драматической истории, представленная в рамках интенсива для сценаристов от SkillBox

Fig. 2. A three-act structure of a dramatic story presented as part of an intensive course for scriptwriters from SkillBox

Структура истории в формате сторителлинга

В настоящей работе построение историй основано на «Пути Героя», как наиболее традиционном формате, с которого можно начать исследование [54; 55]. «Путь Героя» включает интригующий зачин (захватывает внимание читателя/слушателя с первых строк и создаёт желание узнать, что будет дальше), развитие конфликта (ясная проблематика, которую персонаж должен разрешить), повышение ставок (конфликт нарастает по мере развития сюжета, заставляя читателя/слушателя переживать за героя) и развязку (подразумевает логичный и закрытый финал или дальнейшие возможные приключения героя).

Обязательным атрибутом, способствующим установлению эмоциональной связи и вовлечению читателя/слушателя, выступают живые персонажи. К ним предъявляются требования многогранности, реалистичности и эмоционального сопровождения: персонажи выступают сложными личностями, имеющими собственные мотивы, положительные и отрицательные качества; поведение персонажей и их реакции правдоподобны, даже если история вымышленная; читатель/слушатель должен сопереживать героям, испытывать к ним симпатию или антипатию.

Окружающий мир героя предполагает его детальное описание, чтобы в воображении читателя/слушателя появлялись яркие и запоминающиеся образы. Мир обладает уникальной атмосферой, которая создаёт определённое настроение и позволяет одной истории отличаться от другой. Требования предъявляются к языку и стилю изложения (язык доступен для читателя/слушателя, вызывает эмоции, стиль истории соответствует жанру). История может нести урок о жизни, людях, мире или содержать мораль, которая выражает определённую ценность. Возможная структура вовлекающей истории, представленная в рамках интенсива для сценаристов от *SkillBox*[12], показана на *рисунке 2*.

В течение развития сюжета герой претерпевает трансформации, оставаясь верным своей цели. По мере нарастания напряжения сюжета увеличивается ставка, ценности, которыми герой готов рискнуть для разрешения конфликта. Сюжет проходит две кульминационные точки: «почти получилось» и

[12] Евгений Казачков. Как написать сценарий? Интенсив для сценаристов от SkillBox. URL: https://www.youtube.com/watch?v=sfJZ8SI9YaI (дата обращения: 14.11.2024).

финальный рывок. В процессе путешествия героя настигает прозрение, которое он не в состоянии осознать в начале пути, и только к концу дороги, с прохождением всех метаморфоз, отрывается правда, происходит переоценка ценностей и наступает новое равновесие героя с самим собой и окружающей средой.

Приведённые структуры сосредотачивают внимание читателя/слушателя на протяжении всего повествования, обращают внимание на наиболее важные моменты, оказывающие влияние на развитие и трансформацию героя. Нарастающее напряжение и финальное разрешение конфликта создают эмоциональную вовлечённость и вызывают чувства сопереживания и сострадания. При построении сложной многоактовой истории, иллюстрирующей многогранность героя, как его положительные, так и отрицательные стороны, читатель или слушатель начинает ассоциировать себя с персонажем, проходить с ним все приключения, как бы совместно преодолевая препятствия и эмоционально проживая описанный опыт.

Трансформация технических текстов в истории

Традиционный технический текст о применении вирусов-шифровальщиков содержит описание программных аспектов эксплуатации уязвимостей, а также фактические данные, связанные с величиной и масштабом ущерба[13]. В рамках сторителлинга набор фактов может превратиться в историю о политических, экономических и социальных последствиях, связанных с остановкой рабочих процессов из-за шифрования и блокировки файлов, ростом цен на мясо на фоне дефицита поставок, недовольством сотрудников при отсутствии трудовых заданий и соответствующей оплаты труда, массовыми волнениями, объединяющими недовольных. Преобразованный текст позволяет сформировать у обучающихся объёмное восприятие опасностей, исходящих от вирусов-шифровальщиков, увидеть сложные связи между разными направлениями деятельности. Возможные элементы истории в соответствии с приведённой структурой представлены в *таблице 2*.

История может включать личные мотивации персонажей. Например, кто-то работает ради семьи, а кто-то – чтобы погасить долги. Данные элементы позволяют создать более глубокую эмоциональную привязку к событиям. Возможно указание дилемм, с которыми сталкиваются персонажи (например, стоит ли рисковать здоровьем ради спасения бизнеса). Завершение истории допустимо неожиданным поворотом событий: вирус был создан кем-то изнутри системы (инсайдером), или злоумышленник ставил совершенную иную цель. Указанный приём оставляет читателя или слушателя в напряжении после завершения истории, заставляет многократно возвращаться к ней мысленно для более детального анализа.

С учётом элементов истории, представленных в таблице 2, придуманное повествование может содержать следующие фрагменты: «Прошло несколько дней, и ситуация ухудшилась. Рабочие начали протестовать против задержки выплат. На улицах города возникали спонтанные митинги – люди требовали решения проблемы. Дефицит мяса вызвал резкий рост цен в магазинах, что только подогревало недовольство населения. Политическая обстановка накалялась: различные группы начали использовать ситуацию для своих целей. В конечном итоге руководство комбината приняло тяжёлое решение: выплатить выкуп вымогателям. Это решение стало уроком для всех – как для работников предприятия, так и для других компаний в отрасли. После инцидента началась активная работа по улучшению информационной

[13] JBS, крупнейший в мире производитель говядины, стал жертвой кибератаки // Журнал Xakep.ru. URL: https://xakep.ru/2021/06/02/jbs/ (дата обращения: 14.11.2024).

Таблица 2

Элементы истории об атаке вируса-шифровальщика

Table 2

Elements of a ransomware attack story

Структура истории			
Интригующий зачин	Развитие конфликта	Повышение ставок	Развязка
Рядовая атака вируса-шифровальщика смогла привести к политическим, экономическим волнениям, оказать влияние на социальные процессы. Преподнесённый урок позволил повысить защищённость многих других объектов	Сотрудник допустил заражение компьютеров вирусом-шифровальщиком через вредоносную ссылку из фишингового письма. Все файлы системы оказались зашифрованы и недоступны для обработки до уплаты выкупа	Атака привела к остановке производства и невозможности экспорта. Рабочие не получили зарплату, дефицит мяса привёл к росту цен. На фоне недовольства и ценового кризиса наблюдались массовые волнения	Отсутствие резервных копий вынудило выплатить выкуп вымогателям. Последствия атаки продемонстрировали роль ИБ в политических, экономических и социальных процессах
Живые персонажи			
Многогранность	Реалистичность		Эмоциональность
Сотрудник, испытывающий чувство вины, старающийся исправить положение (вызывает негодование и сочувствие). Рабочие, вынужденные приостановить работу и выйти с протестами (сострадание как к сотрудникам, так и к владельцам)	Описание элементов производственных процессов; санитарно-эпидемиологические требования; упоминание куттеров и мясорубок; аккуратность рабочих мест и использование дезинфицирующих средств. Подробное описание фишингового письма, упоминание приёмов социальной инженерии для формирования правдоподобного текста. Упоминание структуры баннера вируса-шифровальщика с сообщением о необходимости выплатить выкуп вымогателям		Наблюдаются всеобщие упаднические настроения, проявляющиеся на политической, экономической и социальной аренах. Паника из-за отсутствия понимания, чем закончится конфликт
Запоминающийся мир			
Детальность	Атмосфера		Уникальность
Зелёный стикер на экране; забытый USB-кабель; смятые бумаги; пыльные страницы; мигающая лампочка; красный баннер с сообщением от хакеров	Вместо гула работающих станков наступила звенящая тишина; ярко освещённые помещения, блестящие поверхности; ритм работы комбината; холодильные камеры, прохлада в помещениях; работники в спецодежде; запах химикатов; дождливое нерадостное утро, встречающее группу рабочих		Индустриальный антураж; контраст между слаженной и ритмичной работой комбината и хаосом, вызванным вирусом

безопасности на всех уровнях. История показала, насколько уязвимыми могут быть даже самые защищённые предприятия в условиях современного мира технологий. Информация стала важнейшим ресурсом, а безопасность – необходимым условием для успешного функционирования бизнеса».

В *таблице 3* представлены элементы возможной истории об уязвимости *Heartbleed*[14], которая затронула миллионы веб-сайтов и привела к утечке конфиденциальной информации пользователей. Уязвимость *Heartbleed (CVE-2014-0160)* представляет собой серьёзную ошибку в библиотеке *OpenSSL*, позволяющую злоумышленникам несанкционированно читать память серверов и клиентов, что может привести к утечке конфиденциальной

[14] В OpenSSL обнаружена серьёзная уязвимость // Журнал Xakep.ru. URL: https://xakep.ru/2014/04/08/62324/ (дата обращения: 14.11.2024).

Таблица 3

Элементы истории об уязвимости Heartbleed

Table 3

Elements of the Heartbleed Vulnerability Story

Структура истории			
Интригующий зачин	Развитие конфликта	Повышение ставок	Развязка
Heartbleed открыла двери к самым сокровенным данным – паролям, кредитным картам и личной переписке. Ошибка 2011 года была обнаружена лишь спустя три года, когда уже тысячи веб-сайтов стали жертвами её разрушительной силы	К моменту объявления об уязвимости около 500 тыс. веб-сайтов были подвержены риску. Ситуация усугубилась, когда выяснилось, что Агентство национальной безопасности США (АНБ) знало об уязвимости за два года до её раскрытия	Heartbleed позволяла извлекать до 64 Кбайт данных из оперативной памяти, что означало возможность доступа к даже к закрытым ключам SSL. Более 300 тыс. серверов оставались уязвимыми после публикации патча	После бурной реакции и многочисленных попыток устранить последствия, ситуация стабилизировалась. Первое обновление включало исправления, предотвращающие эксплуатацию уязвимости
Живые персонажи			
Многогранность	Реалистичность		Эмоциональность
Робин Зеггельман стремился внести вклад в улучшение безопасности. Однако недостаточная проверка его кода привела к уязвимости. Codenomicon обнаружили уязвимость и старались донести важность проблемы до аудитории	Слова Зеггельмана о том, что он «несёт ответственность за ошибку», отражают его человечность и осознание важности своей роли в проекте. Работа инженеров Codenomicon требует не только технической компетенции, но и эмоциональной стойкости. Специалисты сталкиваются с давлением времени и необходимостью быстро донести информацию. АНБ оказывается в центре этической дискуссии о том, как использовать уязвимости		Эмоциональный подъём Codenomicon от успешного просветительского проекта контрастирует со страхом не успеть охватить все слои населения и тревогой о последствиях
Запоминающийся мир			
Детальность	Атмосфера		Уникальность
Подробности о том, как работает OpenSSL и протоколы шифрования. Использование фрагментов кода или псевдокода для иллюстрации атаки	Создание атмосферы вокруг истории об уязвимости Heartbleed требует сочетания технических деталей с эмоциональными реакциями персонажей и общественной реакцией на события. Упоминание логотипа в виде кровоточащего сердца может служить ярким символом уязвимости		Рассмотрение моральных аспектов использования уязвимостей для достижения целей шпионажа

информации, включая пароли, логины и закрытые ключи шифрования. На момент обнаружения уязвимости более 17% защищённых веб-сайтов использовали уязвимые версии *OpenSSL*, что затронуло миллионы пользователей по всему миру.

Финальный вариант текста может образно рассказывать об уязвимости и содержать, например, следующие фрагменты: «Когда клиент отправлял запрос на “сердцебиение”, пакет данных включал длину полезной нагрузки в виде 16-битного целого числа вместе с самим содержимым», «логотип кровоточащего сердца стал мощным символом уязвимости и напоминанием о том, как легко можно потерять доверие пользователей», «в конце концов эта история стала напоминанием о том, что за каждым кодом стоят люди; что каждая строка кода может изменить судьбы миллионов; и что доверие – это самый ценный ресурс в цифровом мире», «*Heartbleed* также стал катализатором изменений в подходах к кибербезопасности по всему миру», «хотя *Heartbleed* был

Таблица 4

Примеры трансформации традиционного материала в формат сторителлинга

Table 4

Examples of transforming traditional material into a storytelling format

Пример традиционного представления	Возможные элементы истории в формате сторителлинга
Атака «водопой» позволяет хакерам внедрять вредоносное программное обеспечение в системы поставщика или провайдера	Обозначение разницы между трудоёмкой охотой за одной зеброй (отдельным клиентом) и более лёгкой организацией централизованной ловушки у водопоя (взлом поставщика услуги), к которому приходят утолить жажду сразу много животных
Бэкдор, или «чёрный вход», представляет собой программу или набор программ, обеспечивающих повторный доступ к системе без ведома пользователя	Одним из ключевых элементов, позволяющих Пожирателям Смерти получить доступ к Хогвартсу, является «исчезательный» шкаф. Шкаф можно рассматривать как бэкдор, который предоставляет возможность скрытого перемещения и обхода охраны
Диверсификация – это процесс распределения инвестиций или ресурсов между несколькими активами с целью минимизации рисков и ущерба	Кощей Бессмертный использует различные способы защиты своей жизни, но собирает их в одном месте («в сундуке сидит заяц, в зайце – утка, в утке – яйцо, а в яйце – игла»[15]). Волан-де-Морт создаёт несколько крестражей, чтобы сохранить частички своей души в разных объектах
Ботнет – это сеть заражённых устройств, управляемых злоумышленниками для выполнения различных вредоносных действий	Княгиня Ольга отомстила древлянам, отправив на Искоростень голубей и воробьёв, к которым были привязаны подожжённые кусочки трута. Птицы действуют как дистрибутивные единицы, которые одновременно поджигают разные участки
Анонимность в сети – состояние, при котором пользователь может скрывать свою личность в Интернете (может быть использована в злонамеренных целях)	Одиссей, попав в плен к Полифему, использует свою смекалку, чтобы обмануть циклопа и спастись. Он представляется как «Никто», что позволяет ему избежать прямого противостояния с Полифемом
Социальная инженерия – метод манипуляции людьми с целью получения конфиденциальной информации и несанкционированного доступа к системам	В басне «Ворона и Лисица» Лиса использует лесть как метод манипуляции, чтобы завладеть сыром Вороны. В сказке «Колобок» Лиса использует ложное представление о своей слабости, чтобы вызвать у Колобка желание приблизиться и спеть погромче
Преобладание неожиданных стратегий перед физическими мощностями подчёркивает важность креативного мышления и тактического планирования	Давид, будучи физически слабее Голиафа, использует свою ловкость и хитрость, чтобы победить гиганта. Он полагается на пращу, а не на традиционные методы боя, что позволяет ему одержать победу, несмотря на явное превосходство противника
Консолидация сил в борьбе с киберпреступниками предполагает объединение государственных, коммерческих структур и частного сектора	Герои «Гравити Фолз» понимают, что для борьбы с мощным противником, таким как Билл Шифр, им необходимо объединить силы. Когда персонажи работают вместе, они создают синергетический эффект, который позволяет им победить
Шифрование защищает данные от несанкционированного доступа, тогда как стеганография скрывает сам факт передачи информации	Геометрический шифр масонов или шифр вольных каменщиков (*Pigpen*) может быть рассмотрен через историю Пьера Безухова и его вступление в Орден масонов. В.И. Ленин использовал молоко для написания секретных сообщений с изложением своих идей
«Дымовая завеса» – тактический приём, используемый для создания временного визуального или информационного препятствия	Сюжет фильма «Такси» показывает, как полиция пытается отследить банду, использующую красные «мерседесы». Однако, когда преступники перекрашивают свои машины в серый цвет, это создаёт «дымовую завесу», затрудняющую их обнаружение

[15] Тайная хронология и психофизика русского народа // Вера Лемешко: литературный дневник. URL: https://stihi.ru/diary/veralemeshko/2015-11-02 (дата обращения: 14.11.2024).

катастрофой для многих пользователей и организаций, он также открыл новые горизонты для улучшения безопасности данных в Интернете и укрепления доверия между пользователями и сервисами».

В *таблице 4* демонстрируются различные аспекты ИБ через призму сторителлинга, что позволяет сделать темы более доступными и понятными для аудитории. Каждая из выбранных тем, от атак на поставщика услуг до социальной инженерии, проиллюстрирована через известные истории и метафоры, что помогает подчеркнуть важные принципы и механизмы, действующие в киберугрозах.

Сторителлинг позволяет представить сложные технические аспекты ИБ в формате, который легче воспринимается. Обращение к историям о кибератаках и их последствиях, вместо формального изложения фактов, помогает слушателям лучше понять риски киберугроз и важность защиты данных. Аналогии с известными литературными произведениями или историческими событиями могут помочь объяснить принципы ИБ, сформировать объёмное восприятие инцидентов и их последствий. Визуализация сценариев наглядно представляет информацию и делает её более понятной, а обучение интерактивным и увлекательным. Аудитория, сопереживая героям и осознавая последствия киберугроз, вовлекается в процесс обучения и лучше запоминает материал.

Материалы и методы

Исследование проводилось с 1 по 31 октября 2024 г. на базе Школы компьютерных наук[16] ФГАОУ ВО «Тюменского государственного университета» (ТюмГУ). В ТюмГУ внедрены индивидуальные образовательные траектории (ИОТ), в рамках которых студенты разных специальностей и направлений подготовки могут дополнять свой учебный план дисциплинами, выбранными с учётом собственных интересов и карьерных целей[17]. Настоящее исследование охватывает два элективных курса – «Основы кибербезопасности» и «Введение в пентестинг (кибербезопасность)». Материалы курса «Основы кибербезопасности» посвящены общим подходам к обеспечению информационной безопасности, начиная от защиты личности и заканчивая аспектами обороны государства. «Введение в пентестинг (кибербезопасность)» предлагает изучить технические характеристики уязвимостей в программном обеспечении и основы наступательной безопасности.

Для каждой дисциплины были подготовлены лекции с элементами сторителлинга. Студенты электива «Основы кибербезопасности» изучали междисциплинарные аспекты атаки на продовольственное предприятие *JBS Foods*, занимающееся производством мясопродуктов. Обучающиеся «Введению в пентестинг (кибербезопасность)» знакомились с техническим описанием уязвимости *Heartbleed (CVE-2014-0160)*. Истории были подготовлены в соответствии со структурами текстов, предложенными в таблицах 2 и 3.

На следующем занятии, через неделю после прослушивания материала, студентам было предложено ответить на вопросы по пройденным темам. В частности, предлагалось оценить занятия в формате сторителлинга, ответив на открытый вопрос об интересе к прослушанному материалу (вопрос позволяет оценить влияние сторителлинга на мотивационную составляющую). Также было предложено продолжить фразу: «Повышение защищённости отдельной информационной системы...» (вопрос направлен на установление понимания у обучающихся междисциплинарных связей разных предметных областей (политики, экономики,

[16] Школа компьютерных наук ФГАОУ ВО ТюмГУ. URL: https://www.utmn.ru/scs/ (дата обращения: 14.11.2024).

[17] Программа развития ТюмГУ в рамках реализации федеральной программы стратегического академического лидерства «Приоритет-2030». URL: https://www.utmn.ru/priority2030/ (дата обращения: 14.11.2024).

социума) с ИБ, а также возможных долгосрочных и масштабных последствий вследствие локальной рутинной атаки), а также ответить, какая характеристика подходит под описание уязвимости *Heartbleed* (вопрос призван выяснить, сформировалось ли у студентов знание технических характеристик уязвимости, «насмотренность» для распознавания возможных деструктивных действий). Кроме этого, обучающимся было предложено оценить ущерб от взлома электронной почты без потери конфиденциальной информации. Ответы позволили выяснить степень эмпатии к жертвам преступления в основной и контрольной группах. Анализ респондентов осуществлялся методами визуальной статистики и с помощью статистического критерия χ^2 при уровне статистической значимости *p-value*<=0,05 (допустимый уровень погрешности 5%).

Количество студентов в группе каждого электива составило 60 человек, общее число опрошенных – 120 обучающихся. Участники каждой группы (n=60) были распределены на основную и контрольную выборки (n=30). В основных группах на лекциях студенты знакомились с историями, подготовленными в формате сторителлинга. Контрольные группы проходили занятия без использования нарратива или эмоциональной вовлечённости. Среди обучающихся в обеих группах – представители 2-го года обучения (3-й семестр) специальностей и направлений подготовки 10.05.01 «Компьютерная безопасность» (26), 10.05.03 «Информационная безопасность автоматизированных систем» (22), 09.03.02 «Информационные системы и технологии» (22), 10.03.01 «Информационная безопасность» (19), 02.03.03 «Математическое обеспечение и администрирование информационных систем» (10), 09.03.03 «Прикладная информатика» (8), 01.03.01 «Математика» (3), 15.03.06 «Мехатроника и робототехника» (2), 03.03.02 «Физика» (2), 06.05.01 «Биоинженерия и биоинформатика» (1), 45.03.02 «Лингвистика» (1), 01.03.03 «Механика и математическое моделирование» (1), 37.03.01 «Психология» (1), 43.03.02 «Туризм» (1), 38.05.01 «Экономическая безопасность» (1).

Ограничения исследования

Настоящее исследование проводилось на базе двух элективных курсов «Основы кибербезопасности» и «Введение в пентестинг (кибербезопасность)» в Школе компьютерных наук ТюмГУ. Выборка обучающихся включала 120 студентов 2-го курса в возрасте до 23 лет. Элективы ориентированы на базовый уровень сложности, за пределами исследования остаются наиболее сложные технические аспекты ИБ, например, реверс-инжиниринг и вирусный анализ.

Результаты и обсуждение

Ответы на первый открытый вопрос анкеты показали, что опрошенные студенты положительно оценивают элементы сторителлинга и отмечают повышение интереса к теме занятия и лучшее запоминание материала. Обучающиеся указывают на бóльшую динамичность и напряжённость занятий, обращают внимание на свою вовлечённость в материал и сосредоточенность в течение всего занятия, что может служить индикатором повышения мотивации к обучению при обращении к сторителлингу.

Результаты ответов обучающихся на второй вопрос, посвящённый междисциплинарным связям кибербезопасности, представлены на *рисунке 3*. Основная группа (диаграмма справа) показала более чем на 50% правильных ответов по сравнению с контрольной группой (диаграмма слева). Критерий χ^2=26,087 показал статистически достоверную разницу (p<0,001) между двумя выборками, что говорит об эффективности сторителинга для формирования у обучающихся понимания междисциплинарных связей разных предметных областей (политики, экономики, социума) с ИБ, а также способности прогнозировать возможные глобальные последствия вследствие локаль-

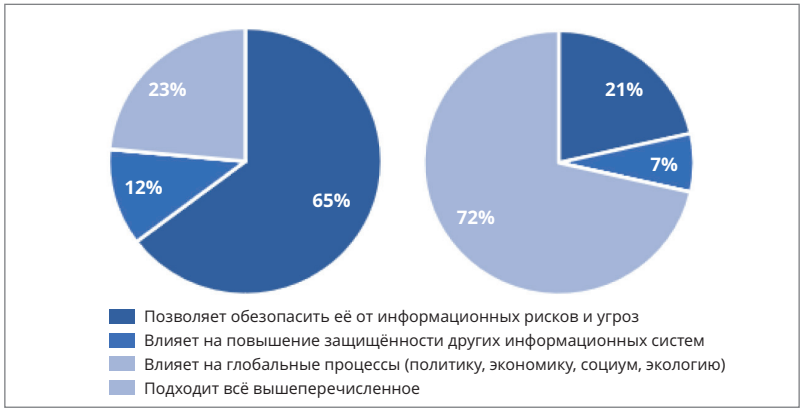

Рис. 3. Распределение ответов обучающихся на вопрос о междисциплинарных связях («Повышение защищённости отдельной информационной системы...»)
Fig. 3. Distribution of students' responses to the question about interdisciplinary connections ("Increasing the security of a separate information system...")

Рис. 4. Распределение ответов обучающихся на вопрос об уязвимости Heartbleed
Fig. 4. Distribution of student responses to the Heartbleed vulnerability question

ной атаки (нематериальные действия приводят к материальному ущербу).

Распределение ответов на вопрос «Какая характеристика подходит под описание уязвимости *Heartbleed*?» (*Рис. 4*) показало, что в основной группе (диаграмма справа), процент верных ответов оказался выше на 18% («При эксплуатации "проступают" конфиденциальные данные»). Статистически достоверная разница не установлена, тем не менее, можно отметить, что основная группа успешнее справилась с заданием. Возможно прийти к выводу, что для освоения технических аспектов недостаточно эмоциональной вовлечённости. Изучение технических аспектов дополнительно потребует работы с программным кодом и исследования архитектуры компьютеров. Тем не менее можно утверждать, что оформление технического материала в формате сторителлинга и сохранение эмоциональной вовлечённости, также может сделать изучение и запоминание более эффективным.

Также студентам было предложено ответить на вопрос о степени ущерба при взломе электронной почты, при условии, что она не

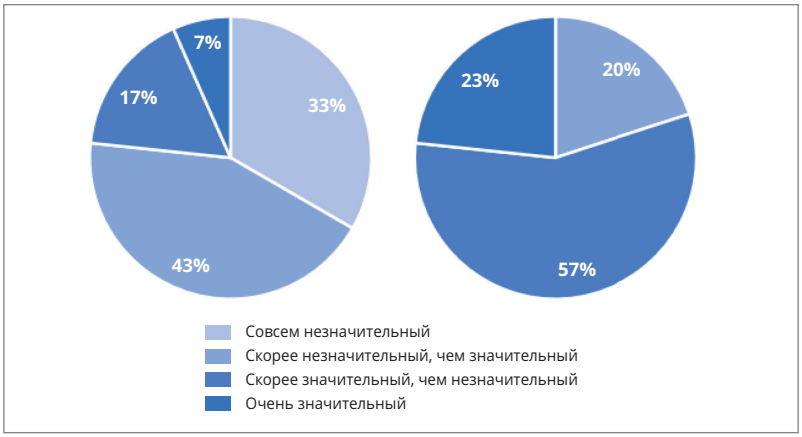

Рис. 5. Распределение ответов обучающихся на вопрос о степени ущерба при взломе электронной почты без потери конфиденциальных данных

Fig. 5. Distribution of student responses to the question of the degree of damage caused by email hacking without loss of confidential data

хранила конфиденциальной информации (*Рис.* 5). В основной группе процент студентов, оценивших ущерб как «очень значительный», оказался выше на 16%, чем в контрольной группе. Количество обучающихся в основной группе, оценивших ущерб как «скорее значительный, чем незначительный», выше на 40% по сравнению с контрольной группой.

Полученные ответы могут говорить о том, что в основной группе слушатели в гораздо большей степени сопереживают жертвам преступления и осознают, что даже отсутствие конфиденциальной информации на почте не снимает тяжесть причинённого ущерба, поскольку для человека, столкнувшегося со взломом своей, даже виртуальной, собственности, это может стать «последней каплей» или значительным нарушением личных границ. Психика человека – тонкая материя, и никогда нельзя сказать заранее, как те или иные преступные действия скажутся на ней. Сострадание, формируемое сторителлингом через сопереживание судьбам героев, позволяет воспитать профессионалов, подходящих к решению задачи со всей степенью ответственности перед пользователями информационной системы.

Стоит отметить, что опрос проходил через неделю после прослушивания подготовленных историй. Относительно высокий процент правильных ответов в основной выборке говорит о том, что материал не забывается. Эмоциональное воздействие историй на слушателей оставило более глубокое впечатление, сформированное знание и понимание междисциплинарных связей, чем последовательное изложение фактов.

Сторителлинг через образность и эмоциональную вовлечённость подчёркивает значимость проблем ИБ, демонстрируя за каждой кибератакой реальный ущерб для людей и общества. Благодаря сторителлингу выстраиваются эмоциональные связи с жертвами компьютерных преступлений, проявляются эмпатия и сопереживание, что подталкивает будущих специалистов к большей социальной ответственности, осознанию своей миссии и роли не только через призму технологий, а также смысловой наполненности и общественной пользы.

Структура истории в формате сторителлинга позволяет описывать сложные причинно-следственные цепочки: от начала кибератаки до проявления их последствий в политике, экономике, социуме, культуре. При этом сторителлинг позволяет сохранить профессиональную ориентированность, связанную со специальной терминологией,

описанием алгоритмов работы защищаемых информационных систем, техническими описаниями уязвимостей и принципов кибератак. Истории, выступающие художественными зарисовками, с одной стороны, вызывают эмоциональный отклик, с другой стороны, позволяют раскрыть технические аспекты профессиональной деятельности и их взаимосвязи с другими предметными направлениями.

Образовательным результатом применения сторителлинга могут выступить компетенции, связанные с построением более совершенной системы защиты, направленной на пресечение долгоиграющих междисциплинарных последствий, минимизацию числа преступлений и возможного ущерба. Также результатом действия сторителлинга становится усиление социальной ответственности и отдачи обществу, повышение мотивации в своей профессиональной деятельности и непрерывном развитии вследствие осознания профессиональной миссии и достижения смысловой наполненности.

Можно сделать ряд выводов о возможностях инструмента сторителлинга при преподавании информационной безопасности: эмоциональная вовлечённость слушателей через сторителлинг создаёт более глубокое впечатление и понимание тем, чем просто последовательное изложение фактов; инструмент сторителлинга полезен для формирования понимания междисциплинарных связей (основная группа продемонстрировала более чем 50% правильных ответов по сравнению с контрольной группой); эмоциональное вовлечение положительно влияет на запоминание информации (в основной группе наблюдается на 18% больше правильных ответов) и повышение эмпатии к пострадавшим от компьютерных преступлений. Относительно высокий процент правильных ответов через неделю после прослушивания говорит о том, что материал остаётся в памяти обучающихся, что может подтверждать долгосрочное воздействие сторителлинга. Наличие неправильных ответов указывает, что для полного освоения темы необходимы дополнительные технические знания, для более эффективного обучения стоит рассмотреть возможность комбинирования сторителлинга с техническими аспектами и практическими примерами, чтобы обеспечить полное понимание и усвоение материала.

Возможно выдвинуть гипотезу о получении аналогичных результатов при применении сторителлинга в других образовательных учреждениях, осуществляющих подготовку по ИБ, не только в рамках элективных курсов, но и других форматов занятий. Также допустимо предположение, что положительный опыт применения сторителлинга при преподавании ИБ может быть спроецирован на другие технические и инженерные специальности и направления подготовки, требующие в современных условиях освоения не только прикладных и инструментальных навыков, но также гуманитарных компетенций, междисциплинарного восприятия картины мира и социальной ответственности.

Заключение

Полученные результаты подчёркивают важность интеграции нарративных методов в образовательные практики при обучении информационной безопасности, открывая новые направления для дальнейших исследований в области педагогической психологии и методологии преподавания. Настоящее исследование подтверждает, что сторителлинг не только обогащает процесс обучения, но и способствует созданию более глубоких когнитивных связей между студентами и изучаемым материалом, превращая обучение в увлекательное и запоминающееся приключение. Преподаватель при этом выступает проводником или гидом, подсвечивающим наиболее важные элементы материала и связи между ними, обращая внимание студентов на неочевидные моменты, подводя обучающихся к верному решению.

Положительная оценка обучающимися материала, представленного в формате сторителлинга, свидетельствует о повыше-

нии мотивации к обучению. Статистически значимая разница между основной и контрольной выборками в понимании междисциплинарных связей кибербезопасности с различными предметными областями также указывает на эффективность сторителлинга. Повышение числа верных ответов на технический вопрос, спустя неделю после занятия, может говорить о более глубоком усвоении материала и повышении «насмотренности» с помощью инструмента сторителлинга. Также можно говорить о формировании эмпатии к жертвам компьютерных преступлений через искусство рассказывать истории.

Для достижения большей эффективности обучения возможно рассмотреть комбинирование элементов сторителлинга с описанием технических аспектов и практическими примерами. Это позволит обеспечить более глубокое понимание материала и способность применить его на практике.

Дальнейшие исследования могут быть связаны с алгоритмизацией процесса написания историй в формате сторителлинга, например, с использованием больших языковых моделей, изучением отличий между устной и письменной подачей материала, исследованием приёмов для повышения эмоциональной вовлечённости, применением других форматов, кроме «Пути Героя» («Гора», «Фальстарт», «*In medias res*», «Спарклайн», «Лепестки»), уточнением роли преподавателя при знакомстве обучающихся с историями.

Настоящая работа подчёркивает значимость инструмента сторителлинга в преподавании информационной безопасности и создаёт основу для новых исследований, которые могут быть полезны в образовательных практиках технических и инженерных специальностей и будут вдохновлять студентов на дальнейшее изучение материала.

Литература

1. *Гунаван Б., Ратмоно Б.М., Абдулла А.Г.* Стратегическое управление кибербезопасностью // Форсайт. 2023. Т. 17. № 3. С. 88–97. DOI: 10.17323/2500-2597.2023.3.88.97
2. *Gutzwiller R.S., Ferguson-Walter K., Fugate S., Rogers A.* “Oh, Look, A Butterfly!” A Framework For Distracting Attackers To Improve Cyber Defense // Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 2018. Vol. 62. No. 1. P. 272–276. DOI: 10.1177%2F1541931218621063
3. *Hou J., Deng H., Peng J.C.H.* A Butterfly Effect: Attack-Induced Heterogeneous Equilibrium Points of High-Voltage DC Systems // IEEE Transactions on Smart Grid. 2024. Vol. 15. No. 6. P. 5992–6004. DOI: 10.1109/TSG.2024.3409704
4. *Андреев А.Л.* Гуманитарные контексты российского технического образования // Высшее образование в России. 2021. Т. 30. № 4. С. 62–72. DOI: 10.31992/0869-3617-2021-30-4-62-72
5. *Ефимов В.С., Лаптева А.В.* Концепт «студенческий опыт» с позиции философской антропологии и психологии развития // Высшее образование в России. 2024. Т. 33. № 3. С. 28–48. DOI: 10.31992/0869-3617-2024-33-3-28-48
6. *Данилаев Д.П., Маливанов Н.Н.* Функционал преподавателя технического вуза: целевые ориентиры // Высшее образование в России. 2023. Т. 32. № 3. С. 48–66. DOI: 10.31992/0869-3617-2023-32-3-48-66
7. *Полякова Т.Ю.* Преподаватель технического вуза: что ценят студенты? // Высшее образование в России. 2023. Т. 32. № 11. С. 60–76. DOI: 10.31992/0869-3617-2023-32-11-60-76
8. *Волкова О.А.* О формировании ценностно-смысловых компетенций будущих инженеров // Высшее образование в России. 2017. № 4. С. 144–150. EDN: YKOTCP.
9. *Волкова О.А., Шеболкина Е.П.* Возможности формирования, диагностики и мониторинга ценностно-смыслового компонента компетенций студентов технического вуза // Высшее образование в России. 2020. Т. 29. № 2. С. 127–140. DOI: 10.31992/0869-3617-2020-29-2-127-140
10. *Blažič B.J.* Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? // Education and information technologies. 2022. Vol. 27. No. 3. P. 3011–3036. DOI: 10.1007/s10639-021-10704-y
11. *Shivapurkar M., Bhatia S., Ahmed I.* Problem-based learning for cybersecurity education // Journal of The Colloquium for Information Systems Security Education. 2020. Vol. 7. No. 1. URL: https://cisse.info/journal/index.php/

cisse/article/view/108/108 (дата обращения: 18.11.2024).
12. *Емельянова М.В., Зайцева Е.Л., Гурьянова Т.Ю.* Ценностные ориентации обучающихся на первом и выпускном курсах в вузе // Проблемы современного педагогического образования. 2023. № 78-3. С. 88–90. EDN: SYNUTE.
13. *Kam H.J., Menard P., Ormond D., Crossler R.E.* Cultivating cybersecurity learning: An integration of self-determination and flow // Computers & Security. 2020. Vol. 96. Article no. 101875. DOI: 10.1016/j.cose.2020.101875
14. *Бурькова Е.В.* Профессиональная подготовка специалистов в области информационной безопасности // Вестник Оренбургского государственного университета. 2016. № 2 (190). С. 3–9. EDN: VXKMKN.
15. *Астахова Л.В., Земцов И.В.* Развитие готовности будущего специалиста по защите информации к ситуационному управлению информационной безопасностью // Современные проблемы науки и образования. 2020. № 1. DOI: 10.17513/spno.29541
16. *Дудина Е.В., Колыванова Л.А., Чеканушкина Е.Н.* Формирование профессиональных компетенций в области информационной безопасности как фактор успешной подготовки будущего специалиста // Известия Самарского научного центра Российской академии наук. Социальные, гуманитарные, медико-биологические науки. 2021. Т. 23. № 79-2. С. 194–201. DOI: 10.37313/2413-9645-2021-23-79(2)-194-201
17. *Ricci S., Hajny J., Piesarskas E., Parker S., Janout V.* Challenges in Cyber Security Education // International Journal of Information Security and Cybercrime. 2020. Vol. 9. No. 2. P. 7–11. DOI: 10.19107/IJISC.2020.02.01
18. *Švábenský V., Čeleda P., Vykopal J., Brišáková S.* Cybersecurity knowledge and skills taught in capture the flag challenges // Computers & Security. 2021. Vol. 102. Article no. 102154. DOI: 10.48550/arXiv.2101.01421
19. *Нархов Д.Ю., Нархова Е.Н., Ярутина С.А., Шкурин Д.В.* Социокультурный потенциал студенчества в аспекте информационной безопасности и профессиональной подготовки // Вестник Пермского национального исследовательского политехнического университета. Социально-экономические науки. 2021. № 2. С. 20–34. DOI: 10.15593/2224-9354/2021.2.2
20. *Баранов В.В., Корчагина А.П., Лобов Б.Н.* Киберполигон как площадка для подготовки специалистов в области информационной безопасности // Проблемы проектирования, применения и безопасности информационных систем в условиях цифровой экономики : Материалы XXII Международной научно-практической конференции, Ростов-на-Дону, 21–22 ноября 2022 года. Ростов-на-Дону: Ростовский государственный экономический университет «РИНХ». 2022. С. 31–39. EDN: DMLEMU.
21. *Прохоров А.И.* Киберполигон как современный инструмент обеспечения информационной безопасности // Информатизация в цифровой экономике Учредители: ООО «Первое экономическое издательство». 2023. Т. 4. № 4. С. 363–378. DOI: 10.18334/ide.4.4.119301
22. *Abdiraman A.S., Aldasheva L.S., Darmenov B., Omurzakov T.I., Zakirova A.B.* Comparative analysis of application platform for learning cybersecurity through the Capturing the Flag Competitions // Bulletin of LN Gumilyov Eurasian National University Technical Science and Technology Series. 2023. Vol. 145. No. 4. P. 49–57. DOI: 10.32523/2616-7263-2023-145-4-49-57
23. *Ciuperca E., Stanciu A., Cîrnu C.* Postmodern education and technological development. Cyber range as a tool for developing cyber security skills // 15th International Technology, Education and Development Conference. INTED2021 Proceedings. IATED. 2021. P. 8241–8246. DOI: 10.21125/inted.2021.1675
24. *Miloslavskaya N., Tolstoy A.* Cyber polygon site project in the framework of the MEPhI network security intelligence center // Brain-Inspired Cognitive Architectures for Artificial Intelligence: BICA* AI 2020: Proceedings of the 11th Annual Meeting of the BICA Society 11. Springer International Publishing. 2021. P. 295–308. DOI: 10.1007/978-3-030-65596-9_75
25. *Мазова Е.В., Гончар А.А.* Понятие «насмотренность» в профессиональном цифровом ландшафте: объём, содержание и контекст употребления // МедиаВектор. 2023. № 10. С. 76–81. EDN: GTGKUB.
26. *Сущенко С.А., Самыгин С.И., Жидяева Е.С.* Актуальные методы и технологии обучения в высшей школе в эпоху цифровизации // Наука. Образование. Современность/Science. Education. The present. 2023. № 4. С. 127–135. DOI: 10.23672/SEM.2023.96.51.012

27. *Корнеева Л.* Интерактивные методы обучения // Высшее образование в России. 2004. № 12. С. 105–108. EDN: IBMZUN.
28. *Balon T., Baggili I.* Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education // Education and Information Technologies. 2023. Vol. 28. No. 9. P. 11759–11791. DOI: 10.1007/s10639-022-11451-4
29. *Chiou Y.M., Barnes T., Mouza C., Shen, C.C.* Social robot teaches cybersecurity // Proceedings of the 2020 ACM Interaction Design and Children Conference: Extended Abstracts. 2020. P. 199–204. DOI: 10.1145/3397617.3397824
30. *Zhang-Kennedy L., Chiasson S.* A systematic review of multimedia tools for cybersecurity awareness and education // ACM Computing Surveys (CSUR). 2021. Vol. 54. No. 1. P. 1–39. DOI: 10.1145/3427920
31. *Новикова Е.Ю.* Эмоции в электронном образовательном пространстве // Высшее образование в России. 2021. № 6. С. 108–119. DOI: 10.31992/0869-3617-2021-30-6-108-119
32. *Фатуева Ю.Н.* Роль эмоций в процессе преподавания иностранного языка в вузе // Проблемы современного педагогического образования. 2023. № 78-4. С. 238–241. EDN: HQCIIE.
33. *Шиллер А.В.* Роль эмоций в когнитивно-аффективной системе как фактор развития архитектуры искусственных агентов // Вестник Московского университета. Серия 7. Философия. 2018. № 6. С. 78–90. EDN: YSQIEP.
34. *Шадрина Л.Ю.* Результаты исследования о влиянии сторителлинга на образовательный процесс / Л.Ю. Шадрина // Международный научно-исследовательский журнал [International Research Journal]. 2023. № 10 (136). DOI: 10.23670/IRJ.2023.136.42
35. *Жернов Е.Е., Кочергин Д.Г.* Сторителлинг в преподавании экономических дисциплин: антропное дополнение к цифровизации // Профессиональное образование в России и за рубежом. 2021. № 1 (41). С. 61–68. EDN: HMUQON.
36. *Lestari D., Siswandari S., Indrawati C.* The development of digital storytelling website based media for economic learning in senior high school // International Journal of Active Learning. 2019. Vol. 4. No. 1. P. 10–17. URL: https://www.learntechlib.org/p/208694/ (дата обращения: 02.02.2025).
37. *Багрецова Н.В.* Сторителлинг в обучении иностранному языку: ключевые аспекты // Педагогика и психология образования. 2020. № 2. С. 25–38. DOI: 10.31862/2500-297X-2020-2-25-38
38. *Реймер М.В., Хохлова Д.А.* Метод сторителлинга в обучении студентов университета китайскому языку // Проблемы современного педагогического образования. 2022. № 76-4. С. 279–282. EDN: DVMRLZ.
39. *Садриева Г.А.* Цифровой сторителлинг в процессе обучения иностранным языкам // Новые импульсы развития: вопросы научных исследований. 2020. № 2. С. 316–320. DOI: 10.31453/kdu.ru.978-5-7913-1143-6-2020-316-320
40. *Arvanitis P., Krystalli P.* Digital storytelling and augmented reality-based scenarios for foreign language teaching // Digital Pedagogies and the Transformation of Language Education. IGI Global. 2021. P. 1–22. DOI: 10.4018/978-1-7998-6745-6.ch001
41. *Воитлева Н.А., Лозовская Р.И.* Возможности использования дистанционной формы обучения студентов в преподавании музыкальных дисциплин // Вестник Адыгейского государственного университета. Серия 3: Педагогика и психология. 2024. № 2 (338). С. 53–59. DOI: 10.53598/2410-3004-2024-2-338-53-59
42. *Макарова В.В., Сергеева М.Г.* Техники и приёмы сторителлинга в профессиональном обучении будущих менеджеров // Концепт. 2024. № 9. С. 156–166. DOI: 10.24412/2304-120X-2024-11144
43. *Ширинкина Е.В.* Инструментарий сторителлинга при разработке обучающих решений в педагогическом проектировании // Гуманитарные науки. 2023. № 1 (61). С. 40–44. EDN: NYUCBF.
44. *Ho Weatherly K.I.C.* Using Storytelling to Enrich Expressiveness Among Young String Players // String Research Journal. 2024. Article no. 19484992241266542. DOI: 10.1177/19484992241266542
45. *Бадак Б.А.* Использование технологии «сторителлинг» в преподавании математического анализа // THEORIA: педагогика, экономика, право. 2021. № 4 (5). С. 87–93. DOI: 10.51635/27129926_2021_4_87
46. *Забелина С.Б., Середа Т.Ю.* Сторителлинг как эффективная техника дидактической коммуникации на уроках математики // Московский педагогический журнал. 2020. № 4. С. 30–37. DOI: 10.18384/2310-7219-2020-4-30-37

47. *Afkar M., Jebreilzadeh M., Gavagsaz-Ghoachani R., Phattanasak M.* A teaching method based on storytelling of a student social activity in renewable energy education // 2019 6th International Conference on Technical Education (ICTechEd6). 2019. P. 1–6. DOI: 10.1109/ICTechEd6.2019.8790890
48. *Caratozzolo P., Alvarez-Delgado A., Hosseini S.* Perspectives on the use of Serious-Storytelling for Creative Thinking Awareness in Engineering // 2020 IEEE Frontiers in Education Conference (FIE). IEEE. 2020. P. 1–9. DOI: 10.1109/FIE44824.2020.9273994
49. *Gholami A., Gavagsaz-Ghoachani R., Phattanasak M.* Storytelling-Based Teaching and Evaluation Method Through Visualization in Engineering Topics // 2022 Research, Invention, and Innovation Congress: Innovative Electricals and Electronics (RI2C). IEEE. 2022. P. 310–313. DOI: 10.1109/RI2C56397.2022.9910333
50. *Afkar M., Gholami A., Gavagsaz-Ghoachani R., Phattanasak M., Pierfederici S.* Sustainable Education for Sustainable Future: Art of storytelling for Enhancing Creativity, Knowledge Retention on the acme of successful education // IEEE Access. 2024. Vol. 12. P. 101782–101796. DOI: 10.1109/access.2024.3432030
51. *Chiou Y.M., Barnes T., Jelenewicz S.M., Mouza C., Shen C.C.* Teacher views on storytelling-based cybersecurity education with Social Robots // Proceedings of the 20th Annual ACM Interaction Design and Children Conference. 2021. P. 508–512. DOI: 10.1145/3459990.3465199
52. *Citro T., Palmieri G., Pellegrino M.A.* Digital Tools, Approaches and Assessment for Cybersecurity Education via Storytelling: a Systematic Literature Review // 2nd International Workshop on Cyber Security Education for Industry and Academia (CSE4IA), Genoa, Italy. 2024. Vol. 3700. DOI: 10.5281/zenodo.11126096
53. *Rodrãguez C.L., Garcãa-Jimã M., Cruz-Gonzã C.* Digital storytelling in education: A systematic review of the literature // Review of European Studies. 2021. Vol. 13. No. 2. P. 13–25. DOI: 10.5539/res.v13n2p13
54. *Gentile J.S.* The Hero's Journey: Creating a Theatre/Storytelling Performance Inspired by the Work of Joseph Campbell // Research Methods in Performance Studies. Routledge. 2023. P. 173–180. DOI: 10.4324/9781351044790
55. *Gouvêa M.T.A., Santoro F.M., Cappelli C., Motta C.L., Borges M.R.* Epos: The Hero's Journey in organizations through Group Storytelling // 2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD). IEEE. 2019. P. 123–128. DOI: 10.1109/CSCWD.2019.8791860

Статья поступила в редакцию 21.11.2024
Принята к публикации 06.03.2025

References

1. Gunawan, B., Ratmono, B.M., Abdullah, A.G. (2023). Cybersecurity and Strategic Management. *Foresight and STI Governance*. Vol. 17, no. 3, pp. 88-97, doi: 10.17323/2500-2597.2023.3.88.97
2. Gutzwiller, R.S., Ferguson-Walter, K., Fugate, S., Rogers, A. (2018). "Oh, Look, A Butterfly!" A Framework For Distracting Attackers To Improve Cyber Defense. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. Vol. 62, no. 1, pp. 272-276, doi: 10.1177%2F1541931218621063
3. Hou, J., Deng, H., Peng, J.C.H. (2024). A Butterfly Effect: Attack-Induced Heterogeneous Equilibrium Points of High-Voltage DC Systems. *IEEE Transactions on Smart Grid*. Vol. 15, no. 6, pp. 5992-6004, doi: 10.1109/TSG.2024.3409704
4. Andreev, A.L. (2021). Humanitarian Contexts of Technical Education in Russia. *Vysshee obrazovanie v Rossii = Higher Education in Russia*. Vol. 30, no. 4, pp. 62-72, doi: 10.31992/0869-3617-2021-30-4-62-72 (In Russ., abstract in Eng.).
5. Efimov, V.S., Lapteva, A.V. (2024). The Concept "Student Experience" from the Point of View of Philosophical Anthropology and Developmental Psychology. *Vysshee obrazovanie v Rossii = Higher Education in Russia*. Vol. 33, no. 3, pp. 28-48, doi: 10.31992/0869-3617-2024-33-3-28-48 (In Russ., abstract in Eng.).

6. Danilaev, D.P., Malivanov, N.N. (2023). The Labor Intensity of the "Ideal" Teachers' Work: Targets. *Vysshee obrazovanie v Rossii = Higher Education in Russia.* Vol. 32, no. 3, pp. 48-66, doi: 10.31992/0869-3617-2023-32-3-48-66 (In Russ., abstract in Eng.).
7. Polyakova, T.Yu. (2023). The Technical University Teacher: What Do Students Value? *Vysshee obrazovanie v Rossii = Higher Education in Russia.* Vol. 32, no. 11, pp. 60-76, doi: 10.31992/0869-3617-2023-32-11-60-76 (In Russ., abstract in Eng.).
8. Volkova, O.A. (2017). Formation of Axiological Competencies of Future Engineers. *Vysshee obrazovanie v Rossii = Higher Education in Russia.* No. 4 (211), pp. 144-150. Available at: https://www.elibrary.ru/download/elibrary_28998176_40797097.pdf (accessed: 18.11.2024). (In Russ., abstract in Eng.).
9. Volkova, O.A., Shebolkina, E.P. (2020). Possibilities of Formation, Diagnostics and Monitoring of Axiological Competences of Technical University Students. *Vysshee obrazovanie v Rossii = Higher Education in Russia.* Vol. 29, no. 2, pp. 127-140, doi: 10.31992/0869-3617-2020-29-2-127-140 (In Russ., abstract in Eng.).
10. Blažič, B.J. (2022). Changing the Landscape of Cybersecurity Education in the EU: Will the New Approach Produce the Required Cybersecurity Skills? *Education and Information Technologies.* Vol. 27, no. 3, pp. 3011-3036, doi: 10.1007/s10639-021-10704-y
11. Shivapurkar, M., Bhatia, S., Ahmed, I. (2020). Problem-Based Learning for Cybersecurity Education. *Journal of The Colloquium for Information Systems Security Education.* Vol. 7, no. 1. Available at: https://cisse.info/journal/index.php/cisse/article/view/108/108 (accessed: 18.11.2024).
12. Emelyanova, M.V., Zaitseva, E.L., Guryanova, T.Yu. (2023). Value Orientations of First- and Final-Year Students at a University. *Problemy sovremennogo pedagogicheskogo obrazovaniya = Problems of Modern Pedagogical Education.* No. 78-3, pp. 88-90. Available at: https://www.elibrary.ru/download/elibrary_53825799_10282571.pdf (accessed: 18.11.2024). (In Russ., abstract in Eng.).
13. Kam, H.J., Menard, P., Ormond, D., Crossler, R.E. (2020). Cultivating Cybersecurity Learning: An Integration of Self-Determination and Flow. *Computers & Security.* Vol. 96, article no. 101875, doi: 10.1016/j.cose.2020.101875
14. Burkova, E.V. (2016). Professional Training of Specialists in the Field of Information Security. *Vestnik Orenburgskogo gosudarstvennogo universiteta = Bulletin of the Orenburg State University.* No. 2 (190), pp. 3-9. Available at: http://vestnik.osu.ru/2016_2/1.pdf (accessed: 18.11.2024). (In Russ.).
15. Astakhova, L.V., Zemtsov, I.V. (2020). Developing the Readiness of Future Information Security Specialists for Situational Information Security Management. *Sovremennye problemy nauki i obrazovaniya = Modern Problems of Science and Education.* No. 1, doi: 10.17513/spno.29541 (In Russ.).
16. Dudina, E.V., Kolyvanova, L.A., Chekanushkina, E.N. (2021). Formation of Professional Competencies in the Field of Information Security as a Factor in the Successful Training of a Future Specialist. *Izvestiya Samarskogo nauchnogo tsentra Rossiiskoi akademii nauk. Sotsial'nye, gumanitarnye, mediko-biologicheskie nauki = Bulletin of the Samara Scientific Center of the Russian Academy of Sciences. Social, Humanitarian, Medical and Biological Sciences.* Vol. 23, no. 79-2, pp. 194-201, doi: 10.37313/2413-9645-2021-23-79(2)-194-201 (In Russ.).
17. Ricci, S., Hajny, J., Piesarskas, E., Parker, S., Janout, V. (2020). Challenges in Cyber Security Education. *International Journal of Information Security and Cybercrime.* Vol. 9, no. 2. pp. 7-11, doi: 10.19107/IJISC.2020.02.01
18. Švábenský, V., Čeleda, P., Vykopal, J., Brišáková, S. (2021). Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges. *Computers & Security.* Vol. 102, article no. 102154, doi: 10.48550/arXiv.2101.01421

19. Narkhov, D.Yu., Narkhova, E.N., Yarutina, S.A., Shkurin, D.V. (2021). Sociocultural Potential of Students in the Aspect of Information Security and Professional Training. Vestnik *Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Sotsial'no-ekonomicheskie nauki = Bulletin of Perm National Research Polytechnic University. Social and Economic Sciences*. No. 2, pp. 20-34, doi: 10.15593/2224-9354/2021.2.2 (In Russ.).
20. Baranov, V.V., Korchagina, A.P., Lobov, B.N. (2022). Cyber Range as a Platform for Training Specialists in the Field of Information Security. *Problems of Design, Application and Security of Information Systems in the Digital Economy. Proceedings of the XXII International Scientific and Practical Conference, Rostov-on-Don, November 21–22, 2022. Rostov-on-Don: Rostov State University of Economics "RINH"*. Pp. 31-39. Available at: https://www.elibrary.ru/download/elibrary_54019915_69445321.pdf (accessed: 18.11.2024). (In Russ.).
21. Prokhorov, A.I. (2023). Cyber Range as a Modern Tool for Ensuring Information Security. *Informatization in the Digital Economy Founders: First Economic Publishing House, LLC*. Vol. 4, no. 4, pp. 363-378, doi: 10.18334/ide.4.4.119301 (In Russ., abstract in Eng.).
22. Abdiraman, A.S., Aldasheva, L.S., Darmenov, B., Omurzakov, T.I., Zakirova, A.B. (2023). Comparative Analysis of Application Platform for Learning Cybersecurity Through the Capturing the Flag Competitions. *Bulletin of LN Gumilyov Eurasian National University Technical Science and Technology Series*. Vol. 145, no. 4, pp. 49-57, doi: 10.32523/2616-7263-2023-145-4-49-57
23. Ciuperca, E., Stanciu, A., Cîrnu, C. (2021). Postmodern Education and Technological Development. Cyber Range as a Tool for Developing Cyber Security Skills. *15th International Technology, Education and Development Conference. INTED2021 Proceedings. IATED*. Pp. 8241-8246, doi: 10.21125/inted.2021.1675
24. Miloslavskaya, N., Tolstoy, A. (2021). Cyber Polygon Site Project in the Framework of the Mephi Network Security Intelligence Center. *Brain-Inspired Cognitive Architectures for Artificial Intelligence: BICA* AI 2020: Proceedings of the 11th Annual Meeting of the BICA Society 11. Springer International Publishing*. Pp. 295-308, doi: 10.1007/978-3-030-65596-9_75
25. Mazova, E.V., Gonchar, A.A. (2023). *The Concept of "Watchfulness" in the Professional Digital Landscape: Volume, Content and Context of Use*. MediaVector. No. 10, pp. 76-81. Available at: https://www.elibrary.ru/download/elibrary_59888973_62028176.pdf (accessed: 18.11.2024). (In Russ., abstract in Eng.).
26. Sushchenko, S.A., Samygin, S.I., Zhidyaeva, E.S. (2023). Current Methods and Technologies of Teaching in Higher Education in the Era of Digitalization. *Nauka. Obrazovanie. Sovremennost' = Science. Education. The Present*. No. 4, pp. 127-135, doi: 10.23672/SEM.2023.96.51.012 (In Russ.).
27. Korneeva, L. (2004). Interactive Teaching Methods. *Vysshee obrazovanie v Rossii = Higher Education in Russia*. No. 12, pp. 105-108. Available at: https://www.elibrary.ru/download/elibrary_9573633_59230782.pdf (accessed: 18.11.2024). (In Russ.).
28. Balon, T., Baggili, I. (2023). Cybercompetitions: A Survey of Competitions, Tools, and Systems to Support Cybersecurity Education. *Education and Information Technologies*. Vol. 28, no. 9, pp. 11759-11791, doi: 10.1007/s10639-022-11451-4
29. Chiou, Y.M., Barnes, T., Mouza, C., Shen, C.C. (2020). Social Robot Teaches Cybersecurity. *Proceedings of the 2020 ACM Interaction Design and Children Conference: Extended Abstracts*. Pp. 199-204, doi: 10.1145/3397617.3397824
30. Zhang-Kennedy, L., Chiasson, S. (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys (CSUR)*. Vol. 54, no. 1, pp. 1-39, doi: 10.1145/3427920

31. Novikova, E.Yu. (2021). Emotions in the Electronic Educational Space. *Vysshee obrazovanie v Rossii = Higher Education in Russia.* No. 6, pp. 108-119, doi: 10.31992/0869-3617-2021-30-6-108-119 (In Russ., abstract in Eng.).
32. Fatueva, Yu.N. (2023). The Role of Emotions in the Process of Teaching a Foreign Language At A University. *Problemy sovremennogo pedagogicheskogo obrazovaniya = Problems of Modern Pedagogical Education.* No. 78-4, pp. 238-241. Available at: https://www.elibrary.ru/download/elibrary_53985457_14924294.pdf (accessed: 18.11.2024). (In Russ., abstract in Eng.).
33. Schiller, A.V. (2018). The Role of Emotions in the Cognitive-Affective System as a Factor in the Development of the Architecture of Artificial Agents. *Vestnik Moskovskogo universiteta. Seriya 7. Filosofiya. = Bulletin of Moscow University. Series 7. Philosophy.* No. 6, pp. 78-90. Available at: https://www.elibrary.ru/download/elibrary_36708167_97207772.pdf (accessed: 18.11.2024). (In Russ., abstract in Eng.).
34. Shadrina, L.Y. (2023). Results of a Study on the Impact of Storytelling on the Educational Process. *Mezhdunarodnyi nauchno-issledovatel'skii zhurnal = International Research Journal*. No. 10 (136), doi: 10.23670/IRJ.2023.136.42 (In Russ., abstract in Eng.).
35. Zhernov, E.E., Kochergin, D.G. (2021). Storytelling in Teaching Economic Disciplines: An Anthropic Supplement to Digitalization. *Professional'noe obrazovanie v Rossii i za rubezhom = Professional Education in Russia and Abroad*. No. 1 (41), pp. 61-68. Available at: https://www.elibrary.ru/download/elibrary_45688390_95904519.pdf (accessed: 18.11.2024). (In Russ., abstract in Eng.).
36. Lestari, D., Siswandari, S., Indrawati, C. (2019). The Development of Digital Storytelling Website Based Media for Economic Learning in Senior High School. *International Journal of Active Learning*. Vol. 4, no. 1, pp. 10-17. Available at: https://www.learntechlib.org/p/208694/ (accessed: 18.11.2024).
37. Bagretsova, N.V. (2020). Storytelling in Teaching a Foreign Language: Key Aspects. *Pedagogika i psikhologiya obrazovaniya = Pedagogy and Psychology of Education.* No. 2, pp. 25-38, doi: 10.31862/2500-297X-2020-2-25-38 (In Russ., abstract in Eng.).
38. Reimer, M.V., Khokhlova, D.A. (2022). Storytelling Method in Teaching University Students the Chinese Language. *Problemy sovremennogo pedagogicheskogo obrazovaniya = Problems of Modern Pedagogical Education.* No. 76-4, pp. 279-282. Available at: https://www.elibrary.ru/download/elibrary_50010353_25690896.pdf (accessed: 18.11.2024). (In Russ., abstract in Eng.).
39. Sadrieva, G.A. (2020). Digital Storytelling in Teaching Foreign Languages. *Novye impul'sy razvitiya: voprosy nauchnykh issledovanii = New Impulse of Development: Research Issues.* No. 2, pp. 316-320, doi: 10.31453/kdu.ru.978-5-7913-1143-6-2020-316-320 (In Russ., abstract in Eng.).
40. Arvanitis, P., Krystalli, P. (2021). Digital Storytelling and Augmented Reality-Based Scenarios for Foreign Language Teaching. *Digital Pedagogies and the Transformation of Language Education. IGI Global*. Pp. 1-22, doi: 10.4018/978-1-7998-6745-6.ch001
41. Voitleva, N.A., Lozovskaya, R.I. (2024). Possibilities of Using Distance Learning for Students in Teaching Musical Disciplines. *Vestnik Adygeiskogo gosudarstvennogo universiteta. Seriya 3: Pedagogika i psikhologiya = Bulletin of Adyghe State University. Series 3: Pedagogy and Psychology*. No. 2 (338), pp. 53-59, doi: 10.53598/2410-3004-2024-2-338-53-59 (In Russ., abstract in Eng.).
42. Makarova, V.V., Sergeeva, M.G. (2024). Storytelling Techniques and Methods in Professional Training of Future Managers. *Kontsept = Concept*. No. 9, pp. 156-166, doi: 10.24412/2304-120X-2024-11144 (In Russ., abstract in Eng.).
43. Shirinkina, E.V. (2023). Storytelling Tools in Developing Educational Solutions in Pedagogical Design. *Gumanitarnye nauki = Humanities*. No. 1 (61), pp. 40-44. Available at: https://www.elibrary.ru/download/elibrary_52285208_64615456.pdf (accessed: 18.11.2024). (In Russ.).

44. Ho Weatherly, K.I.C. (2024). Using Storytelling to Enrich Expressiveness Among Young String Players. *String Research Journal*. Article no. 19484992241266542, doi: 10.1177/19484992241266542
45. Badak, B.A. (2021). Using Storytelling Technology in Teaching Mathematical Analysis. *THEORIA: pedagogika, ekonomika, pravo = THEORIA: Pedagogy, Economics, Law*. No. 4 (5), pp. 87-93, doi: 10.51635/27129926_2021_4_87 (In Russ.).
46. Zabelina S.B., Sereda T.Yu. (2020). Storytelling as an Effective Technique of Didactic Communication in Mathematics Lessons. *Moskovskii pedagogicheskii zhurnal = Moscow Pedagogical Journal*. No. 4, pp. 30-37, doi: 10.18384/2310-7219-2020-4-30-37 (In Russ., abstract in Eng.).
47. Afkar, M., Jebreilzadeh, M., Gavagsaz-Ghoachani, R., Phattanasak, M. (2019). A Teaching Method Based on Storytelling of a Student Social Activity in Renewable Energy Education. *2019 6th International Conference on Technical Education (ICTechEd6)*. Pp. 1-6, doi: 10.1109/ICTechEd6.2019.8790890
48. Caratozzolo, P., Alvarez-Delgado, A., Hosseini, S. (2020). Perspectives on the Use of Serious-Storytelling for Creative Thinking Awareness in Engineering. *2020 IEEE Frontiers in Education Conference (FIE). IEEE*. Pp. 1-9, doi: 10.1109/FIE44824.2020.9273994
49. Gholami, A., Gavagsaz-Ghoachani, R., Phattanasak, M. (2022). Storytelling-Based Teaching and Evaluation Method Through Visualization in Engineering Topics. *2022 Research, Invention, and Innovation Congress: Innovative Electricals and Electronics (RI2C). IEEE*. Pp. 310-313, doi: 10.1109/RI2C56397.2022.9910333
50. Afkar, M., Gholami, A., Gavagsaz-Ghoachani, R., Phattanasak, M., Pierfederici, S. (2024). Sustainable Education for Sustainable Future: Art of storytelling for Enhancing Creativity, Knowledge Retention on the acme of successful education. *IEEE Access*. Vol. 12, pp. 101782-101796, doi: 10.1109/access.2024.3432030
51. Chiou, Y.M., Barnes, T., Jelenewicz, S.M., Mouza, C., Shen, C.C. (2021). Teacher Views on Storytelling-Based Cybersecurity Education with Social Robots. *Proceedings of the 20th Annual ACM Interaction Design and Children Conference*. Pp. 508-512, doi: 10.1145/3459990.3465199
52. Citro, T., Palmieri, G., Pellegrino, M.A. (2024). Digital Tools, Approaches and Assessment for Cybersecurity Education via Storytelling: a Systematic Literature Review. *2nd International Workshop on Cyber Security Education for Industry and Academia (CSE4IA), Genoa, Italy*. Vol. 3700, doi: 10.5281/zenodo.11126096
53. Rodrãguez, C.L., Garcãa-Jimã, M., Cruz-Gonzã, C.(2021). Digital Storytelling in Education: A Systematic Review of the Literature. Review of European Studies. Vol. 13, no. 2, pp. 13-25, doi: 10.5539/res.v13n2p13
54. Gentile, J.S. (2023). The Hero's Journey: Creating a Theatre/Storytelling Performance Inspired by the Work of Joseph Campbell. *Research Methods in Performance Studies. Routledge*. Pp. 173-180, doi: 10.4324/9781351044790
55. Gouvêa, M.T.A., Santoro, F.M., Cappelli, C., Motta, C.L., Borges, M.R. (2019). Epos: The Hero's Journey in organizations through Group Storytelling. *2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD). IEEE*. Pp. 123-128, doi: 10.1109/CSCWD.2019.8791860

The paper was submitted 21.11.2024
Accepted for publication 06.03.2025