Виртуальный Музей Киберинцидентов: Реальность Цифровых Артефактов

А.В. Шестаков, К.З. Билятдинов

***Аннотация* — Статья посвящена новому научно-технологическому профилю музея, порождаемому современной эпохой цифровой трансформации различных сфер деятельности человечества и их кибербезопасности, дефинициям артефакта, музейного предмета и его ценностей в метриках техногенной безопасности, в частности рисков и киберинцидентов информационной, функциональной и пожарной безопасности.**

С учетом позиций международных и отечественных повесток в области музееведения и внедрения новых цифровых технологий рассмотрены особенности формирования виртуального музея киберинцидентов в парадигме транспонирования принятых форм и способов представления артефактов через призму реальности цифровых артефактов киберинцидентов.

Сформулированы основы концепции виртуального музея киберинцидентов Санкт-Петербургского университета ГПС МЧС России как комплексной цифровой киберсреды научно-технологических исследований, образования, просвещения и пропаганды отечественных технологий и средств информационной безопасности и защиты информации различных аспектов техносферной безопасности.

***Ключевые слова* — виртуальный музей, киберинцидент, артефакт киберинцидента, информационная безопасность, функциональная безопасность, пожарная безопасность.**

I. Введение

Актуальность исследований нового технологического феномена цифровой трансформации всех видов деятельности музеев обусловлена, во-первых, внедрением новых технологий в организацию учета, изучения и публичного представления музейных предметов (коллекций) для достижения различных целей, в том числе просветительных и образовательных, а во-вторых, появлением новых сущностей явлений и предметов цифровой среды деятельности человечества, в том числе в техносфере и ее кибербезопасности, несмотря на порождение цифровых и виртуальных музеев, музейных предметов и артефактов киберсреды, которые не получили должного отражения в культурологии и музееведении.

Особая значимость исследования обусловлена появлением новых киберугроз и кибервоздействий, которые стали сопутствующими в цифровой трансформации различных видов деятельности и в развитии киберсреды.

II. Основы исследования и постановка задачи

Киберинциденты в последние годы прочно вошли в историю техносферной безопасности:

- кибератака сотрудника V. Boden на автоматизированные средства управления очистными сооружениями SCADA (Supervisory Control And Data Acquisition) с выбросом в городскую экосистему более 2,6 млн. литров канализационных вод (г. Маручи-Шир, Квинсленд, Австралия, 2000) [1];
- кибератака школьника через доработанный пульт управления телевизором на стрелки трамвайных путей со сходом 4 трамваев (г. Лодзь, Польша, 2008);
- кибератака вирусом W32.Ramnit через внешнюю корпоративную информационную сеть на внутреннюю информационную инфраструктуру АЭС (г. Гундемминген, Германия, 2016) [2];
- кибератака программой-вымогателем SNAKE с функцией принудительной остановки производственных процессов ICS на предприятии Honda (2020) [3];
- DDoS-атака (распределенная атака типа «отказ в обслуживании») на телекоммуникационную систему Маршалловых Островов (2022) [4] и ряд других.

Компании-разработчики средств защиты информации вынуждены предоставлять пользователям информацию из киберсреды в форме доступной для их восприятия, например, в форме реального мира посредством интерактивной карты киберугроз в мире.

Повестка развития и появление новых цифровых сущностей в ходе цифровой трансформации деятельности музеев и музейных предметов цифровой киберсреды, подтверждают своевременность проведения исследования по разрешению сложившихся противоречий, как в терминологии, так и в научно-технологическом представлении цифровых артефактов информационной безопасности.

Анализ тематических подборок литературы из более 1300 источников, изданных до 2014 года, размещенных на информационно-образовательном портале «Российское музееведение» [6],показывает, что:

- компьютерным технологиям и цифровым

А.В. Шестаков – д.т.н, заместитель начальника ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России» (email: alexandr.shestakov01@yandex.ru).

К.З. Билятдинов – д.т.н, профессор кафедры прикладной математики и безопасности информационных технологий ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России» (email: k74b@mail.ru).

стратегиям в музеях и учреждениях музейного типа, виртуальным музеям и экспозициям, мобильным приложениям для музеев посвящено около 30% публикаций;

- техническим музеям - 1% публикаций.

Значимым также являются сравнительные показатели количества публикаций по тематикам:

- Виртуальные музеи и экспозиции - больше, чем 14 раз (787 против 54);
- Технические музеи - больше, чем в 9 раз (137 против 15);
- Краеведческие музеи - больше, чем в 94 раза (1890 против 20);
- Наука о музее, музееведение, музеология - больше, чем в 1,4 раза (126 против 85);
- Культурология (история культуры) - больше, чем в 125 раз (2006 против 16).

Сведений о музее киберинцидентов или виртуальном музее киберинцидентов и их артефактах, как показал контекстный анализ выборки, ни в одной из публикаций не приведено. Имеются несколько публикаций, в части вербального описания экспоната виртуального музея вируса-червя (I LOVE YOU), который посредством писем Microsoft Outlook заразил более 3 млн компьютеров по всему миру и обошелся мировой экономике почти в 10 млрд. долл. США (Онел де Гусман, Филиппины, 2000) [7] и онлайн музея старых компьютерных вирусов в Сан-Франциско [8, 9].

Исходя из вышеизложенного, требует исследования существующие реализации прототипов сайтов виртуального музея, его продвижение через интернет агрегаторы, платформы, социальные сети, тематические форумы и сообщества, интернет видео и фотопорталы ресурсов-музеев, возможности виртуальных гидов и специальных приложений для смартфонов, платформ онлайн-обучения и киберграмотности, геймифицированных форм популяризации киберкультуры и кибергигиены.

III. Методы исследования

Анализ исследований зарубежных и российских ученых в области музееведения в условиях их цифровой трансформации: контент-анализ публикаций и фактографический анализ данных; сравнительный анализ методов и технологий, в том числе на основе квалиметрических оценок и сверток, применяемых в виртуальных музеях естественно-технического профиля; потребности современного общества в повышении киберграмотности, кибергигиены и киберкультуры; предпочтения пользователей современной цифровой образовательной киберсреды в области информационной безопасности и защиты информации.

IV. Результаты

В настоящее время следует обратить особое внимание на появление в последние время новых специфических форм реагирования музейных институтов на киберугрозы обществу.

Рост киберугроз от кибермошенничества обусловил введение дополнительных интернет-страниц на сайтах виртуальных музеев непрофильных тематик, таких как информационные технологии и информационная безопасность.

В связи с чем для продвижения тематик виртуального музея киберинцидентов могут использоваться интернет агрегаторы и платформы, интернет видео и фотопорталы ресурсов-музеев.

При этом сегодня с целью изучения пользователей музейного информационного ресурса широко используются технологии мониторинга пользовательской активности.

Таким образом, наиболее перспективным направлением достижения социальных задач виртуального музея киберинцидентов является его присутствие в социальных сетях, тематических форумах и сообществах.

Перечень каналов и чатов в соцсетях по информационной безопасности из 177 субъектов с количеством подписчиков от 139 до 216931 человек, актуальный по состоянию на 04.01.2025, приведен Securitylab в [10].

Существующий опыт создания и использования в современных музеях платформ онлайн-обучения позволяет рассматривать их для решения задач виртуального музея киберинцидентов с целью сокращения дефицита компетенций в области информационной безопасности, защиты информации и кибергигиены, повышении киберграмотности и киберкультуры с применением таких популярных форм как геймификация контента.

Значительный объем сведений о геймификации информационной безопасности в части Security Parashoot, Phishing Phil (Wombat Security), Net Invaders (Cisco Systems, Inc.), CyberCIEGE приведен в [11].

Проблематике геймификации, направленной на повышение компетенций в области информационной безопасности и защиты информации, посвящено ряд исследований и работ как в нашей стране, так и зарубежном, например

- особенностям геймификации обучения персонала реагирования на киберинциденты при обеспечении необходимого уровня подобия состояния компании и условий работы персонала, процессов обеспечения информационной безопасности на предприятии, как следствие действий в игре [12];
- мотивации персонала к обучению информационной безопасности посредством геймификации задач [13];
- введению геймификации в систему корпоративных тренингов [14];
- применению геймификации для снижения дефицита компетенций обучающихся в области «социальной инженерии» [15];
- разработке и внедрению пакета игровых кейсов для дисциплины «Управление информационной безопасностью» в Сибирском государственном университете науки и технологий [16];

- адаптации тестовых задач под национальные и культурные особенности обучаемых при реализации международных программ (коллабораций) в области информационной безопасности [17];
- платформенным решениям для обучаемых с любым уровнем первичной подготовки [18];
- анализу 118 различных теорий, положенных в основу геймификации с достижением различных заданных целей [19].

Результаты проведенного многофакторного анализа существующих виртуальных музеев обусловил целесообразность получения интегральной и обобщенной оценки качества системотехнических решений по построению виртуального музея киберинцидентов техносферы.

Под оценкой качества решений понимается систематическое исследование степени, с которой музейно-исторические, научно-исследовательские, образовательные и просветительские сервисы цифровой среды информационно-технических ресурсов виртуального цифрового музея способны удовлетворять установленным и подразумеваемым потребностям общества.

В практике исследований существуют работы, посвященные оценке музеев, в том числе виртуальных, как например:

- интегрированный подход с учетом реального музейного контекста и пользовательского опыта к оценке привлекательности, удобства пользования, удовлетворенности, потенциала образовательного контента, требуемой моторики пользователя [20];
- методология анализа виртуальных посещений по 6 существенным свойствам через показатели и идентификаторы [21];
- факторный анализ виртуальных экскурсий по 4 показателям (подлинность, взаимодействие, навигация, обучение) [22];
- оценка некоторых частных существенных свойств - интерфейса виртуального музея по показателям эстетики и визуальных когнитивных характеристик [23].

Таким образом, сформулированы следующие постулаты концепции виртуального музея киберинцидентов Санкт-Петербургского университета ГПС МЧС России:

1. Виртуальный музей киберинцидентов Санкт-Петербургского университета ГПС МЧС России должен быть некоммерческой постоянно действующей организационно-технической структурой, открытой, доступной и инклюзивной для любых групп посетителей-пользователей цифровых сервисов музейных информационно-телекоммуникационных ресурсов, которая служит обществу в противодействии техногенным, биогенным, социокультурным угрозам, терроризму и экстремистской идеологии, деструктивному иностранному информационно-психологическому воздействию, в том числе киберугрозам, в условиях роста гибридных угроз.
2. Виртуальный музей киберинцидентов Санкт-Петербургского университета ГПС МЧС России должен соответствовать международным и национальным принципам музееведения, закрепленных в правовых актах и документах, и выполнять следующие функции: исследовать, собирать, сохранять, интерпретировать и выставлять на обозрение материальное и нематериальное наследие по противодействию и защите от киберинцидентов в техногенной сфере.
3. Виртуальные экспозиции музея должны применять интерактивные модели, симуляции атак, а также визуализацию реальных случаев киберинцидентов. Например, посетители смогут увидеть, как кибератака на энергетические сети влияет на устойчивость мегаполисов и городов, или как взлом системы управления производствами приводит к остановке функционирования предприятий, в том числе промышленно-опасных объектов.
4. Виртуальный музей киберинцидентов Санкт-Петербургского университета ГПС МЧС России должен способствовать разнообразию и устойчивому развитию музееведения в области материального и нематериального наследия по противодействию и защите от киберинцидентов в техногенной сфере.
5. Виртуальный музей должен содержать информацию о самых известных киберинцидентах за последние десятилетия, начиная от первых вирусов и заканчивая современными сложными гибридными атаками на объекты техносферы. Это поможет проследить эволюцию угроз и методов борьбы с ними. Музей сможет предоставлять доступ к открытым базам данных о киберинцидентах, что позволит исследователям и студентам проводить собственные анализы и исследования информационной безопасности и защиты информации в техносфере.
6. Виртуальный музей киберинцидентов Санкт-Петербургского университета ГПС МЧС России должен работать и взаимодействовать с различными организациями этично, профессионально и при участии общественных организаций и профессиональных сообществ.
7. Важной частью организационной структуры виртуального музея должен стать аналитический центр, который должен заниматься исследованием текущих тенденций в области кибербезопасности и прогнозом возможных будущих киберугроз в техногенной сфере. Результаты исследований должны представляться в виде отчетов и докладов, доступных посетителям.
8. Виртуальный музей должен служить площадкой для общения и обмена опытом между специалистами по кибербезопасности в рамках форумов, вебинаров и конференций по актуальным проблемам и путям их решения.
9. Сотрудничество с крупными промышленными предприятиями позволит создавать реалистичные сценарии атак и разрабатывать эффективные меры противодействия. Компании смогут использовать музей как площадку для тестирования своих решений и обучения персонала.

10. Виртуальный музей киберинцидентов Санкт-Петербургского университета ГПС МЧС России должен реализовывать и предоставлять разнообразные возможности и технологии для обучения, развлечения, размышлений и обмена знаниями в области материального и нематериального наследия по противодействию и защите от киберинцидентов в техногенной сфере.

11. Использование технологий виртуальной и дополненной реальности должно сделать посещение Музея захватывающим и познавательным. Посетители смогут погружаться в различные сценарии киберинцидентов и наблюдать за развитием событий в реальном времени.

12. Виртуальный музей киберинцидентов должен объединить современные технологии и исторический подход к изучению киберугроз и их последствий для критически важных инфраструктур. Посетители смогут попробовать себя в роли специалистов по информационной безопасности, решая задачи по защите систем от различных типов кибератак. Различные тренажеры помогут развивать навыки анализа и реагирования на киберинциденты в техносфере. Образовательная составляющая музея должна включать курсы, семинары по вопросам кибербезопасности техносферы для различных групп посетителей музея. Курсы должны охватывать темы от основ криптографии до современных методов защиты промышленных объектов. Музей должен стать ключевой современной цифровой образовательной средой, которая помогает специалистам и широкой общественности лучше понимать природу кибератак, методы защиты от них и последствия таких инцидентов, особенно в техногенной сфере. Важно усилить значимость повышения осведомленности общества о проблемах кибербезопасности техносферы. Музей может играть роль просветительского центра, объясняя простым языком сложные технические вопросы и демонстрируя важность защиты информации и инфраструктуры.

V. ЗАКЛЮЧЕНИЕ

Проведенное исследование показало, что проблематика создания виртуального музея киберинцидентов техносферы является достаточно актуальной и имеет системное развитие.

Имеющийся тренд создания и применения виртуальных музеев различного направления подтверждает возможность реализации виртуальных музеев киберинцидентов в различных сферах.

Концептуальные положения по построению и развитию системотехнических решений виртуального музея киберинцидентов Санкт-Петербургского университета ГПС МЧС России определяют проект создания виртуального музея киберинцидентов техногенной сферы.

Виртуальный музей киберинцидентов Санкт-Петербургского университета ГПС МЧС России в отличие от традиционных музеев позволит:

- обеспечить посещение экспозиций музея на основе виртуальной платформы без необходимости физического присутствия людям со всего мира;
- организовать регулярное обновление контента и введения новых механизмов, которые позволяют поддерживать актуальность тематик музея и оперативно реагировать на изменения в сфере кибербезопасности, повысить своевременность и эффективность просвещения и пропаганды отечественных технологий и средств информационной безопасности и защиты информации в различных аспектах техносферной безопасности;
- активнее совершенствовать процесс изучения с целью повышения увлеченности пользователей и эффективности применения интерактивных сред и обучающих программ;
- создать на базе аналитического центра музея постоянно действующий источник ценных знаний и идей для дальнейшего развития технологий кибербезопасности.

БИБЛИОГРАФИЯ

[1] Cohen, G. Throwback Attack: An insider releases 265,000 gallons of sewage on the Maroochy Shire / Industrialcybersecuritypulse, November 4, 2021 // https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-an-insider-releases-265000-gallons-of-sewage-on-the-maroochy-shire.

[2] Wall, T. Throwback Attack: German nuclear plant cyberattack is a wake-up call / Industrialcybersecuritypulse February 16, 2023 // https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-german-nuclear-plant-cyberattack-is-a-wake-up-call.

[3] Wall, T. Throwback Attack: SNAKE ransomware hits Honda plants // Industrialcybersecuritypulse, January 12, 2023 // https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-snake-ransomware-hits-honda-plants.

[4] Wall, T. Throwback attack: Lack of cyberliteracy cripples Marshall Islands' telecommunication service // Industrialcybersecuritypulse, May 6, 2022 // https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-lack-of-cyberliteracy-cripples-marshall-islands-telecommunication-service/.

[5] Федеральный закон "О Музейном фонде Российской Федерации и музеях в Российской Федерации" от 26.05.1996 №54-ФЗ.

[6] Тематические подборки литературы // Российское музееведение. Информационно-образовательный портал // https://museumstudy.ru/tematicheskie-podborki-literatury#mmanagement.

[7] Гаков В. Любовное признание червя // Системный администратор. №3 (232). 2022. - С.96.

[8] В Сан-Франциско появился онлайн музей старых компьютерных вирусов // Дилетант. 14.02.2016. /https://diletant.media/news/27833190/.

[9] O'Connor, A. Malware Museum: Visit Retro Viruses In Your Browser / 2024/ https://www.rockpapershotgun.com/malware-museum-viruses.

[10] Каналы и чаты по информационной безопасности в телеграм. Статистика подписчиков // SecurityLab.ru: https://www.securitylab.ru/blog/personal/Morning/354748.php?ysclid=m5jc0192mq594355177-.

[11] Геймификация в информационной безопасности // SecurityLab.ru 05.10.2015 https://www.securitylab.ru/blog/personal/Business_without_danger/152554.php.

[12] Сугак В.А., Мережников Д.А., Сафиуллина Л.Х., Алексеева А.А. Повышение грамотности общества в области информационной безопасности с использованием элементов геймификации // Прикаспийский журнал: управление и высокие технологии. 2024. № 1 (65). С. 45-53.

[13] Фунтикова В.А., Петрова В.Д., Поначугин А.В. Анализ влияния

элементов геймификации на мотивацию к изучению информационной безопасности // Евразийское пространство: экономика, право, общество. 2024. № 11. С. 167-171.

[14] Самсонов Н.С., Рогов Е.Д., Васюк М.Г., Коротовских Р.С. Внедрение тренингов по вопросам информационной безопасности посредством геймификации в корпоративную культуру компании // В сборнике: Безопасность информационного пространства. сборник научных трудов XXI Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. Екатеринбург, 2023. С. 21-22.

[15] Рафиков Д.М., Сажин П.А., Козлова А.В. Геймификация мошеннических действий как способ обучения информационной безопасности // В сборнике: Фундаментальные и прикладные исследования молодых учёных. сборник материалов VII Международной научно-практической конференции студентов, аспирантов и молодых учёных, приуроченной к 110-летию со дня рождения Т.В. Алексеевой. Омск, 2023. С. 611-614.

[16] 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 Международный электронный научный журнал. 2021 №1 (49). С. 450-463.

[17] Bacud, M.L., Mäses, S. Game-based learning for cybersecurity awareness training programmes in the public sector // in ECEL 2021 20th European Conference on e-Learning. Academic Conferences International limited, 2021, p. 50.

[18] Raisi, S., Ghasemshirazi, S., Shirvani, G. UltraLearn: Next-Generation CyberSecurity Learning Platform. // In 2021 12th International Conference on Information and Knowledge Technology (IKT). 2021, December.. pp. 83-88. DOI:10.1109/IKT54664.2021.9685940.

[19] Krath, J., Schürmann, L., Harald F.O. von Korflesch. Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learnin // Computers in Human Behavior 125:106963 August 2021. 33 p. DOI:10.1016/j.chb.2021.106963.

[20] Pagano, A., Pietroni, E., Poli, C. An Integrated Methodological Approach To Evaluate Virtual Museums In Real Museum Contexts // Conference: International Technology, Education and Development Conference. November 2016. DOI:10.21125/iceri.2016.1077.

[21] Cabrera, M., Teruel, L. The Virtual Truth Versus the Real Image of the Museums. Method to Analyse Virtual Visits to Museums // In: Katsoni, V., Şerban, A.C. (eds) Transcending Borders in Tourism Through Innovation and Cultural Heritage. Springer Proceedings in Business and Economics. Springer, Cham. 28 April 2022. pp 475–494. https://doi.org/10.1007/978-3-030-92491-1_29.

[22] Li J., Nie J-W., Ye, J. Evaluation of virtual tour in an online museum: Exhibition of Architecture of the Forbidden City // PLOS One. January 2022/ 17(1):e0261607/ DOI:10.1371/journal.pone.0261607.

[23] Wang W., Wen Z., Chen J., Gu Y., Peng Q. Evaluation Method for Virtual Museum Interface Integrating Layout Aesthetics and Visual Cognitive Characteristics Based on Improved Gray H-Convex Correlation Model // Applied Sciences. August 2024. 14(16):7006. DOI:10.3390/app14167006.

Virtual museum of cyber incidents: the reality of digital artifacts

A.V. Shestakov, K.Z. Biliatdinov

Annotation — The article is devoted to the new scientific and technological profile of the museum, generated by the modern era of digital transformation of various spheres of human activity and their cybersecurity, definitions of artefacts, museum objects and their values in terms of technogenic security, in particular risks and cyber incidents of information, functional, and fire safety.

Taking into account the positions of international and domestic agendas in the field of museology and the introduction of new digital technologies, the features of the formation of a virtual museum of cyber incidents in the paradigm of transposing accepted forms and methods of presenting artifacts through the prism of the reality of digital artifacts of cyber incidents are considered.

The basics of the concept of the virtual museum of cyber incidents of St. Petersburg University of the Ministry of Emergency Situations of Russia as a comprehensive digital cyber environment for scientific and technological research, education, enlightenment and promotion of domestic technologies and information security tools and information protection of various aspects of technosphere security are presented.

Key words — virtual museum, cyber incident, cyber incident artifact, information security, functional security, fire safety.

REFERENCES

[1] Cohen, G. Throwback Attack: An insider releases 265,000 gallons of sewage on the Maroochy Shire / Industrialcybersecuritypulse, November 4, 2021 // https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-an-insider-releases-265000-gallons-of-sewage-on-the-maroochy-shire.

[2] Wall, T. Throwback Attack: German nuclear plant cyberattack is a wake-up call / Industrialcybersecuritypulse February 16, 2023 // https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-german-nuclear-plant-cyberattack-is-a-wake-up-call.

[3] Wall, T. Throwback Attack: SNAKE ransomware hits Honda plants // Industrialcybersecuritypulse, January 12, 2023 // https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-snake-ransomware-hits-honda-plants.

[4] Wall, T. Throwback attack: Lack of cyberliteracy cripples Marshall Islands' telecommunication service // Industrialcybersecuritypulse, May 6, 2022 // https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-lack-of-cyberliteracy-cripples-marshall-islands-telecommunication-service/.

[5] Federal Law "On the Museum Fund of the Russian Federation and Museums in the Russian Federation" dated 26.05.1996 No. 54-FZ.

[6] Thematic selections of literature // Russian Museology. Information and educational portal // https://museumstudy.ru/tematicheskie-podborki-literatury#mmanagement.

[7] Gakov V. Love confession of a worm // System administrator. No. 3 (232). 2022. - P. 96.

[8] An online museum of old computer viruses has appeared in San Francisco // Dilettante. 14.02.2016. /https://diletant.media/news/27833190/.

[9] O'Connor, A. Malware Museum: Visit Retro Viruses In Your Browser / 2024/ https://www.rockpapershotgun.com/malware-museum-viruses.

[10] Telegram channels and chats on information security. Subscriber statistics // SecurityLab.ru: https://www.securitylab.ru/blog/personal/Morning/354748.php?ysclid=m5jc0192mq594355177-.

[11] Gamification in Information Security // SecurityLab.ru 05.10.2015 https://www.securitylab.ru/blog/personal/Business_without_danger/152554.php.

[12] Sugak V.A., Merezhnikov D.A., Safiullina L.Kh., Alekseeva A.A. Improving the literacy of society in the field of information security using elements of gamification // Caspian Journal: Management and High Technologies. 2024. No. 1 (65). P. 45-53.

[13] Funtikova V.A., Petrova V.D., Ponachugin A.V. Analysis of the influence of gamification elements on motivation to study information security // Eurasian space: economics, law, society. 2024. No. 11. P. 167-171.

[14] Samsonov N.S., Rogov E.D., Vasyuk M.G., Korotovskikh R.S. Implementation of trainings on information security issues through gamification in the corporate culture of the company // In the collection: Security of information space. collection of scientific papers of the XXI All-Russian scientific and practical conference of students, graduate students and young scientists. Ekaterinburg, 2023. Pp. 21-22.

[15] Rafikov D.M., Sazhin P.A., Kozlova A.V. Gamification of fraudulent actions as a method of teaching information security // In the collection: Fundamental and applied research of young scientists. collection of materials of the VII International scientific and practical conference of students, graduate students and young scientists, dedicated to the 110th anniversary of the birth of T.V. Alekseeva. Omsk, 2023. Pp. 611-614.

[16] Safonov K.V., Ishchukova E.A., Zolotarev V.V. Application of gamification elements in the training of students - future specialists in the field of information security // Prospects of Science and Education International electronic scientific journal. 2021 No. 1 (49). P. 450-463.

[17] Bacud, M.L., Mäses, S. Game-based learning for cybersecurity awareness training programmes in the public sector // in ECEL 2021 20th European Conference on e-Learning. Academic Conferences International limited, 2021, p. 50.

[18] Raisi, S., Ghasemshirazi, S., Shirvani, G. UltraLearn: Next-Generation CyberSecurity Learning Platform. // In 2021 12th International Conference on Information and Knowledge Technology (IKT). 2021, December.. pp. 83-88. DOI:10.1109/IKT54664.2021.9685940.

[19] Krath, J., Schürmann, L., Harald F.O. von Korflesch. Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learnin // Computers in Human Behavior 125:106963 August 2021. 33 p. DOI:10.1016/j.chb.2021.106963.

[20] Pagano, A., Pietroni, E., Poli, C. An Integrated Methodological Approach To Evaluate Virtual Museums In Real Museum Contexts // Conference: International Technology, Education and Development Conference. November 2016. DOI:10.21125/iceri.2016.1077.

[21] Cabrera, M., Teruel, L. The Virtual Truth Versus the Real Image of the Museums. Method to Analyse Virtual Visits to Museums // In: Katsoni, V., Şerban, A.C. (eds) Transcending Borders in Tourism Through Innovation and Cultural Heritage. Springer Proceedings in Business and Economics. Springer, Cham. 28 April 2022. pp 475–494. https://doi.org/10.1007/978-3-030-92491-1_29.

[22] Li J., Nie J-W., Ye, J. Evaluation of virtual tour in an online museum: Exhibition of Architecture of the Forbidden City // PLOS One. January 2022/ 17(1):e0261607/ DOI:10.1371/journal.pone.0261607.

[23] Wang W., Wen Z., Chen J., Gu Y., Peng Q. Evaluation Method for Virtual Museum Interface Integrating Layout Aesthetics and Visual

Cognitive Characteristics Based on Improved Gray H-Convex Correlation Model // Applied Sciences. August 2024. 14(16):7006. DOI:10.3390/app14167006.