СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ: КИБЕРБЕЗОПАСНОСТЬ КАК КЛЮЧЕВОЙ ФАКТОР ИЗМЕНЕНИЙ

Дильнара ЗАКИРОВА* *PhD, профессор-исследователь, университет «Туран», г. Алматы, Республика Казахстан, ulasdila@gmail.com, ORCID: 0000-0001-5161-959X, Scopus Author ID: 57205166010*

Милан Пол *PhD, профессор, Масариков университет, г. Брно, Арна Новака 1/1, 602 00, Чешская Республика, pol@phil.muni.cz, ORCID: 0000-0002-5787-8610, Scopus Author ID: 55995721000*

Дата поступления рукописи в редакцию: 12/08/2024
Доработано: 8/11/2024
Принято: 8/11/2024

DOI: 10.52123/1994-2370-2024-1310
УДК 004.056:378
МРНТИ 06.71.01

Аннотация. В условиях цифровизации образовательного процесса университеты сталкиваются с новыми вызовами, связанными с обеспечением кибербезопасности, что стало неотъемлемой частью их социальной ответственности. Увеличение объема данных и растущая зависимость от цифровых технологий делают образовательные учреждения особенно уязвимыми перед киберугрозами, такими как фишинг, программы-вымогатели и атаки, основанные на человеческом факторе. В исследовании был применен смешанный метод анализа, включающий, как качественные, так и количественные подходы. Качественный анализ был выполнен с использованием методов тематического анализа, который позволил выявить ключевые темы и тенденции, связанные с кибербезопасностью и социальной ответственностью. Количественный анализ основан на результатах анкетирования, что дало возможность статистически обработать данные и сделать выводы на основе числовых показателей. В ходе исследования выявлено, что уровень цифровой грамотности, особенно в части информационной грамотности, является критическим фактором, влияющим на кибербезопасность университетов. Недостаточные знания и осведомленность о современных киберугрозах создают дополнительные риски, которые могут привести к утечке данных и финансовым потерям. В статье обсуждаются возможные меры по повышению уровня кибербезопасности в вузах через интеграцию соответствующих практик в политику социальной ответственности. Особое внимание уделено важности повышения осведомленности и цифровой грамотности, как среди сотрудников, так и среди студентов, для снижения человеческих рисков и обеспечения устойчивости образовательных учреждений в цифровую эпоху.
Ключевые слова: социальная ответственность, кибербезопасность, цифровизация высшего образования, цифровая грамотность, информационная грамотность, киберугроза, кибератака

Аңдатпа. Білім беру процесін цифрландыру жағдайында университеттер киберқауіпсіздікті қамтамасыз етуге байланысты жаңа қиындықтарға тап болады, бұл олардың әлеуметтік жауапкершілігінің ажырамас бөлігі болды. Деректер көлемінің ұлғаюы және цифрлық технологияларға тәуелділіктің артуы білім беру мекемелерін фишинг, төлем бағдарламалары және адам факторына негізделген шабуылдар сияқты киберқауіптерге әсіресе осал етеді. Зерттеу сапалық және сандық тәсілдерді қамтитын аралас талдау әдісін қолданды. Сапалы талдау киберқауіпсіздік пен әлеуметтік жауапкершілікке байланысты негізгі тақырыптар мен тенденцияларды анықтауға мүмкіндік беретін тақырыптық талдау әдістерін қолдану арқылы жүзеге асырылды. Сандық талдау сауалнама нәтижелеріне негізделген, бұл деректерді статистикалық өңдеуге және сандық көрсеткіштер негізінде қорытынды жасауға мүмкіндік берді. Зерттеу барысында цифрлық сауаттылық деңгейі, әсіресе ақпараттық сауаттылық бөлігінде университеттердің киберқауіпсіздігіне әсер ететін маңызды фактор болып табылатыны анықталды. Қазіргі киберқауіптер туралы жеткіліксіз білім мен хабардарлық деректердің бұзылуына және қаржылық шығындарға әкелуі мүмкін қосымша тәуекелдерді тудырады. Мақалада тиісті тәжірибелерді әлеуметтік жауапкершілік саясатына интеграциялау арқылы жоғары оқу орындарында киберқауіпсіздік деңгейін арттыру бойынша ықтимал шаралар талқыланады. Қызметкерлер арасында да, студенттер арасында да хабардарлық пен цифрлық сауаттылықты арттырудың маңыздылығына, адами тәуекелдерді азайтуға және цифрлық дәуірдегі білім беру мекемелерінің тұрақтылығын қамтамасыз етуге ерекше назар аударылады.
Түйін сөздер: әлеуметтік жауапкершілік, киберқауіпсіздік, жоғары білім беруді цифрландыру, сандық сауаттылық, ақпараттық сауаттылық, киберқауіп, кибершабуыл

* *Автор для корреспонденции: Д. Закирова, ulasdila@gmail.com*

Abstract. In the context of digitalizing the educational process, universities face new challenges regarding ensuring cybersecurity, which has become an integral part of their social responsibility. The increase in data volume and growing dependence on digital technologies make educational institutions particularly vulnerable to cyber threats such as phishing, ransomware, and human-based attacks. The study used a mixed method of analysis, including both qualitative and quantitative approaches. The qualitative analysis was carried out using thematic analysis methods, which allowed us to identify key topics and trends related to cybersecurity and social responsibility. The quantitative analysis was based on the results of the questionnaire, which made it possible to statistically process the data and draw conclusions based on numerical indicators. The study revealed that the level of digital literacy, especially in terms of information literacy, is a critical factor affecting the cybersecurity of universities. Insufficient knowledge and awareness of modern cyber threats create additional risks that can lead to data leakage and financial losses. The article discusses possible measures to improve the level of cybersecurity in universities through the integration of relevant practices into social responsibility policies. Particular attention is paid to the importance of raising awareness and digital literacy among staff and students to reduce human risks and ensure the resilience of educational institutions in the digital age.
Keywords: social responsibility, cybersecurity**,** digitalization of higher education, digital literacy, information literacy, cyber threat, cyber attack

Введение

В последние десятилетия концепция социальной ответственности получила широкое распространение, как в корпоративном, так и в образовательном секторах. Согласно международным стандартам, таким как ISO 26000, социальная ответственность организации включает обязательства перед обществом и окружающей средой, которые выходят за рамки сугубо экономических интересов [1]. В образовательном контексте социальная ответственность проявляется через стремление университетов обеспечивать инклюзивность, равный доступ к образовательным ресурсам, а также через приверженность этическим и экологически устойчивым практикам [2]. Концепция социальной ответственности университетов сформировалась в результате изменений социального, политического, экономического и правового характера, обозначенных в Декларации Всемирной конференции по высшему образованию, прошедшей в Париже в 1998 году [3]. В результате был взят курс на внедрение принципов социальной ответственности в стратегическое управление университетами, что способствует формированию устойчивой и инклюзивной образовательной среды, соответствующей современным вызовам и способствующей всестороннему развитию общества [4].

Социальная ответственность организаций в условиях цифровизации претерпела значительные трансформации, стала более сложной и многоаспектной. Современные компании должны учитывать новые вызовы, такие как кибербезопасность и защита данных, а также использовать возможности цифровых технологий для продвижения социальной справедливости, экологической устойчивости и инклюзии. Цифровизация существенно изменила способы ведения бизнеса, взаимодействия с клиентами и партнерами, а также внутренние процессы в организациях, что, в свою очередь, привело к эволюции концепции социальной ответственности.

В современных условиях активного использования социальных сетей и мгновенной передачи информации общество стало более осведомленным о деятельности организаций образования. Это создает новые вызовы для вузов, которые должны быть готовы к тому, что любая их ошибка или непродуманное действие может стать достоянием общественности. В таких условиях вузы вынуждены действовать более открыто, внедрять стандарты этики и прозрачности, а также активно взаимодействовать с обществом для поддержания своей репутации.

Цифровизация также привела к появлению новых рисков, которые организации образования обязаны учитывать в рамках своей социальной ответственности. Одним из таких рисков является кибербезопасность. Учитывая рост числа кибератак, особенно в образовательном секторе, кибербезопасность становится не только технической, но и социальной проблемой, требующей осознания и участия всех заинтересованных сторон. Кибератаки могут нанести серьезный ущерб как отдельным лицам, так и обществу в целом, поэтому обеспечение кибербезопасности стало важной частью социальной ответственности.

Также важным аспектом является защита данных и конфиденциальности. В

условиях цифровизации вузы собирают и обрабатывают огромное количество личных данных, что требует от них строгого соблюдения норм конфиденциальности и защиты данных. Вузы стали нести ответственность за защиту информации своих студентов, сотрудников и партнеров, поэтому защита информации становится одной из ключевых задач [5]. Нарушение этих норм может не только подорвать доверие к организации, но и привести к юридическим последствиям. В этой связи вузы обязаны внедрять передовые практики защиты данных, информировать стейкхолдеров о том, как их данные используются, и предоставлять им контроль над их личной информацией.

Таким образом, в условиях цифровизации социальной ответственностью университетов становится не только предоставление равного доступа к образовательным ресурсам и поддержка академической честности, но также обеспечение кибербезопасности и защита данных стейкхолдеров. Это включает в себя создание условий для повышения цифровой грамотности, особенно в аспектах, связанных с защитой информации и соблюдением безопасности при использовании цифровых технологий.

Одним из важных факторов, способствующих эффективной киберзащите, является уровень цифровой грамотности студентов и преподавателей. Цифровая грамотность охватывает широкий спектр навыков, необходимых для эффективного использования цифровых технологий, включая информационную, компьютерную, коммуникативную грамотность, а также медиаграмотность и отношение к технологическим инновациям [6]. В контексте кибербезопасности цифровая грамотность играет важную роль, так как она позволяет пользователям не только эффективно использовать цифровые инструменты, но и защищать себя от потенциальных угроз в киберпространстве.

Однако, несмотря на важность всех компонентов цифровой грамотности, для целей кибербезопасности особое значение имеет информационная грамотность. Информационная грамотность представляет собой способность человека находить, оценивать, использовать и защищать информацию [7]. В условиях цифровой эпохи информационная грамотность становится ключевым навыком, необходимым для безопасного использования цифровых ресурсов [8]. Это объясняется тем, что информационная грамотность напрямую связана с пониманием рисков, связанных с использованием информации в цифровом пространстве, и с принятием мер по защите персональных данных и информации от кибератак [9].

В этой связи, в настоящем исследовании информационная грамотность выступает в качестве ключевого показателя для анализа уровня кибербезопасности среди студентов и преподавателей. Этот подход позволяет более точно оценить их способность защищать свои данные и взаимодействовать с информацией в цифровом пространстве, что имеет непосредственное отношение к обеспечению кибербезопасности в вузах.

Цель данного исследования - изучить трансформацию социальной ответственности университетов в условиях цифровизации, с особым акцентом на кибербезопасность, как один из ключевых аспектов современной социальной ответственности вузов.

Задачи исследования включают:

- изучение основных киберугроз, с которыми сталкиваются образовательные учреждения, и их влияния на социальную ответственность;
- оценка уровня цифровой грамотности как одного из факторов, влияющих на кибербезопасность в вузах;
- разработка рекомендаций по интеграции кибербезопасности в стратегию социальной ответственности университетов.

Актуальность исследования обусловлена тем, что в условиях стремительного роста киберугроз в мире образовательные учреждения становятся одной из основных мишеней для киберпреступников. Повышение уровня социальной ответственности через обеспечение кибербезопасности становится неотъемлемой частью устойчивого развития вузов и защиты интересов всех участников образовательного процесса.

Теоретическая значимость работы заключается в расширении понимания взаимосвязи между социальной ответственностью и кибербезопасностью в контексте цифрового образования. Исследование способствует углублению знаний о роли университетов в обеспечении информационной безопасности и защите данных.

Практическая значимость исследования связана с возможностью применения его результатов для разработки и внедрения более эффективных стратегий по повышению кибербезопасности в образовательных учреждениях. Рекомендации, предложенные в работе, могут быть использованы для улучшения политики безопасности и защиты данных, а также для повышения осведомленности сотрудников и студентов о современных киберугрозах.

Научная новизна заключается в выявлении и анализе нерешенных проблем в области социальной ответственности университетов в условиях цифровизации, а также в предложении новых подходов к интеграции кибербезопасности в стратегическое управление вузами.

Обзор литературы по теме исследования показывает, что многие работы посвящены изучению социальной ответственности организаций и кибербезопасности в целом [10, 11, 12, 13], однако вопрос интеграции кибербезопасности в контексте социальной ответственности университетов остается недостаточно изученным. Это подчеркивает необходимость дальнейших исследований в этой области, направленных на развитие комплексного подхода к управлению киберрисками в образовательных учреждениях.

Таким образом, данное исследование стремится закрыть этот пробел и предложить новые стратегии для укрепления социальной ответственности университетов через обеспечение кибербезопасности.

Материалы и методы

Для анализа текущих тенденций и подходов к кибербезопасности в вузах был проведен контент-анализ научных статей, отчетов и публикаций в области социальной ответственности и цифрового образования. Источники информации были отобраны из ведущих научных журналов и других авторитетных изданий. Полученные данные были проанализированы с использованием методов тематического анализа. Этот метод позволил выделить ключевые темы и тенденции, связанные с кибербезопасностью и социальной ответственностью в образовательных учреждениях.

В статье также использованы результаты анкетирования, проведенного авторами в рамках другого исследования, результаты которого были частично опубликованы ранее, в то время как отдельные данные представлены в данной работе впервые. В анкетировании приняли участие 226 преподавателей и 900 студентов из различных высших учебных заведений Казахстана. Анкета включала вопросы, разработанные на основе подхода, предложенного в рамках саммита G20 в 2017 году [14]. Анкетирование проводилось анонимно с использованием облачной платформы SurveyMonkey, что позволило обеспечить конфиденциальность респондентов и защитить личные данные участников, а также обеспечило удобный доступ к опросу.

Исследование проводилось с соблюдением всех этических норм и стандартов. Применяемые методы сбора, обработки и анализа данных позволили всесторонне изучить проблему, определить основные вызовы, с которыми сталкиваются университеты в области кибербезопасности, и предложить рекомендации по их преодолению.

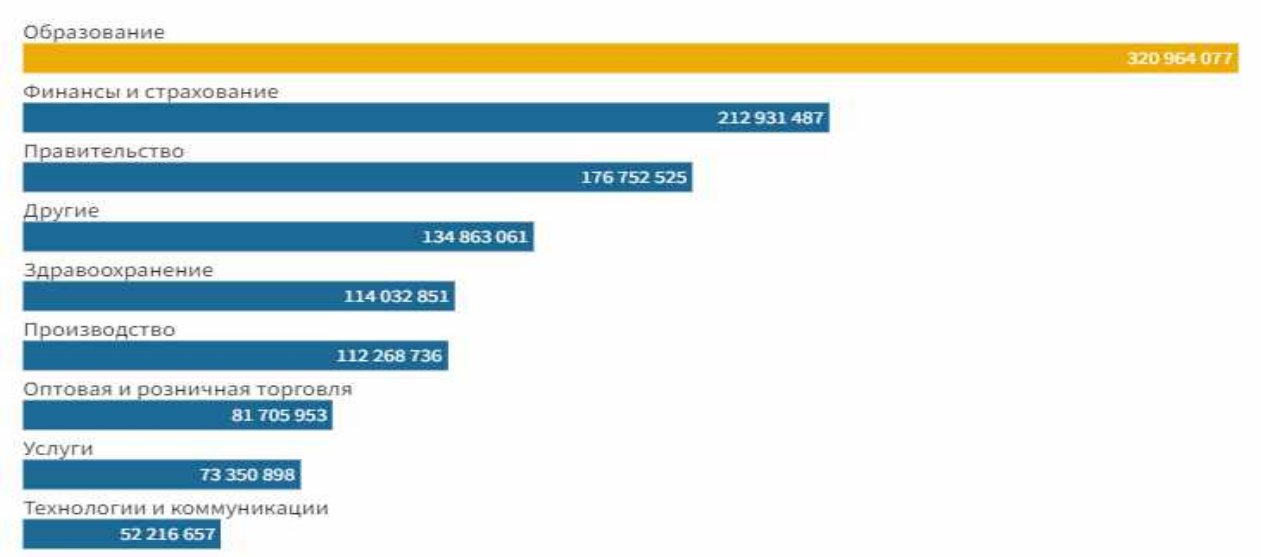
Результаты

В эпоху цифровизации социальная ответственность университетов все больше приобретает цифровой оттенок. Кибербезопасность становится одной из главных проблем социальной ответственности университетов. Кибербезопасность можно определить, как совокупность технологий, процессов и практик, направленных на защиту сетей, устройств, программ и данных от атак, повреждений или несанкционированного доступа [15]. В условиях быстрого развития

цифровых технологий и увеличения объемов данных, которыми оперируют университеты, защита этих данных и обеспечение безопасности использования цифровых инфраструктур стали критически важными задачами. Университеты обязаны защищать личные данные студентов и сотрудников, соблюдая строгие стандарты конфиденциальности и безопасности [16]. Это особенно важно в условиях роста числа кибератак и утечек данных, которые могут нанести значительный ущерб, как отдельным лицам, так и репутации образовательных учреждений.

В 2022 году образование стало наиболее уязвимой отраслью для фишинговых атак, что подтверждается ошеломляющими данными: 320 964 077 атак по всему миру, что составило 25,1% от общего числа фишинговых атак (рисунок 1). Этот факт подчеркивает, что образовательные учреждения, студенты и сотрудники стали главной целью для киберпреступников. Особенно тревожным является рост числа атак в этой сфере на 576% за год, что свидетельствует о значительном увеличении интереса злоумышленников к образовательному сектору [17].

Рисунок 1 - Общее количество зафиксированных фишинговых атак по отраслям, 2022

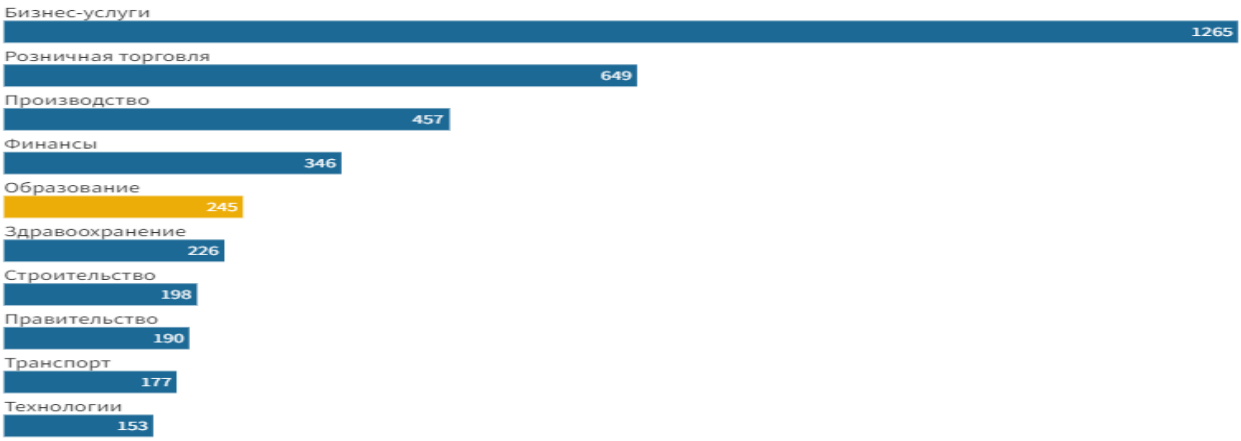


Примечание – составлено авторами на основе источника [6]

Такое резкое увеличение фишинговых атак связано с широким использованием цифровых технологий и онлайн-ресурсов в учебных заведениях, особенно в условиях пандемии и последующего перехода на дистанционное обучение [18]. Образовательные учреждения часто обладают ограниченными ресурсами для обеспечения надлежащей кибербезопасности, что и привлекает злоумышленников. К тому же, в этих учреждениях обычно обрабатывается большое количество данных, включая личные данные студентов и преподавателей, что представляет ценность для киберпреступников.

Рост атак с использованием программ-вымогателей, который наблюдался с 2022 по 2023 год, также является тревожным сигналом для всех секторов, включая образование (рисунок 2). Увеличение числа атак с 2 809 до 5 070 случаев, что составляет более 55%, свидетельствует о том, что киберугрозы становятся все более серьезными и массовыми [19]. Это подчеркивает необходимость усиления мер кибербезопасности в различных отраслях, особенно в тех, которые оказываются наиболее уязвимыми перед такими атаками.

Рисунок 2 – Общее количество зафиксированных атак с использованием программ-вымогателей по отраслям, 2023



Примечание – составлено авторами на основе источника [8]

Сфера образования, на протяжении нескольких лет входящая в пятерку секторов, наиболее подверженных атакам программ-вымогателей, находится в особой зоне риска. Атаки программ-вымогателей могут привести к блокировке доступа к важным данным, прерыванию учебного процесса и даже к утечкам конфиденциальной информации студентов и сотрудников.

Данные о кибератаках на учреждения в сфере науки и образования свидетельствуют о значительной уязвимости этих организаций перед современными киберугрозами [20]. Эти учреждения входят в топ самых часто атакуемых, причем злоумышленники в более чем половине случаев смогли украсть конфиденциальные данные, в основном персональные данные пользователей. Этот факт подчеркивает серьезность проблемы и указывает на высокую ценность информации, хранящейся в образовательных учреждениях. Особое внимание привлекает использование шифровальщиков в каждой второй атаке, где основной целью злоумышленников было получение выкупа. Это подчеркивает финансовую направленность атак и демонстрирует, насколько образовательные учреждения могут быть уязвимыми перед угрозой блокировки своих данных.

Методы социальной инженерии, применяемые в 59% случаев, показывают, что злоумышленники активно используют слабые стороны человеческого фактора. В контексте кибербезопасности социальная инженерия - это метод воздействия на человеческие слабости через манипуляцию с целью достижения вредоносных целей, таких как получение конфиденциальной информации, доступ к системам или выполнение действий в интересах злоумышленника [21]. В 25% атак злоумышленники добивались доступа к ресурсам, подбирая учетные данные или используя уже скомпрометированные пароли, что подчеркивает важность защищенности учетных записей. Также стоит отметить, что в каждой пятой атаке злоумышленники эксплуатировали уязвимости в программном обеспечении, что указывает на постоянное присутствие технических рисков в цифровой инфраструктуре образовательных учреждений. Важно упомянуть и о том, что за 2022 год значительно увеличилась доля атак на веб-ресурсы - с 11% до 20%, что отражает возрастающее внимание злоумышленников к Интернет-инфраструктуре образовательных учреждений [20].

Все эти факты демонстрируют масштаб и многогранность угроз, с которыми сталкиваются образовательные учреждения в условиях цифровой эпохи. В последние годы проблема

кибербезопасности стала одной из ключевых тем для организаций по всему миру. С развитием цифровых технологий и увеличением количества подключенных устройств, угроза кибератак стала более разнообразной и интенсивной.

Университеты, являясь хранителями огромного объема данных и использующими разнообразные информационные системы, сталкиваются с множеством киберугроз, каждая из которых может существенно повлиять на их деятельность (таблица 1).

Таблица 1 - Основные угрозы кибербезопасности для университетов

Угроза	Содержание	Влияние
Человеческие риски	Ошибки и неосмотрительные действия сотрудников и студентов, недостаточная подготовка и осведомленность о киберугрозах.	Возможные утечки конфиденциальных данных студентов и сотрудников; увеличение риска успешных кибератак из-за низкой кибербезопасной культуры.
Фишинг	Распространение мошеннических писем, пытающихся получить личные данные или доступ к учетным записям.	Компрометация личных данных студентов и сотрудников; возможные финансовые потери и ущерб репутации учебного заведения.
Программы-вымогатели	Злонамеренные программы, блокирующие доступ к данным, необходимым для функционирования университета, и требующие выкуп за их разблокирование.	Потеря важных данных и срыв учебного процесса; финансовые затраты на восстановление данных и системы.
Угрозы, основанные на ИИ	Создание сложных фишинговых писем и других атак, труднораспознаваемых для человека, автоматизации кибератак и обход традиционных мер защиты.	Усиление киберугроз и увеличение их успешности; необходимость адаптации мер защиты к новым типам атак.
Темная паутина	Продажа краденных данных, инструментов и услуг для осуществления кибератак; доступ к незаконным материалам и услугам.	Угроза утечки конфиденциальной информации; повышение рисков для безопасности и репутации университета.
Компрометация корпоративной электронной почты	Мошенничество, направленное на обман сотрудников для передачи денег или конфиденциальной информации через электронную почту. Часто атакуются руководители и сотрудники финансовых отделов.	Финансовые потери и утечка конфиденциальной информации; нарушение доверия к электронным коммуникациям внутри университета.
Удаленная работа	Увеличение числа удаленных сотрудников и студентов, использующих личные устройства и сети.	Повышенные риски утечки данных и кибератак, связанные с недостаточной защитой домашних сетей; необходимость обеспечения безопасности в распределенной ИТ-среде.
Уязвимости цепочки поставок	Атаки на поставщиков программного обеспечения и оборудования, используемых университетами; возможность внедрения вредоносного кода на этапе поставок.	Нарушение работы систем и сервисов университета; компрометация безопасности университетских данных и сетей.
Безопасность облака	Увеличение использования облачных сервисов для хранения и обработки данных.	Возможность утечки данных и нарушения конфиденциальности.
Квантовые вычисления	Потенциальные угрозы для современных методов шифрования и защиты данных.	Возможные риски для долгосрочной безопасности данных.

Примечание – составлено авторами на основе источника [22]

Фишинг основан на использовании социального инжиниринга для обмана пользователей с целью получения конфиденциальной информации, такой как логины, пароли, данные кредитных карт и другие чувствительные данные. Фишинговые атаки часто осуществляются через электронную почту, но могут также включать текстовые сообщения, социальные сети и другие формы цифровой коммуникации [23]. Компрометация учетных записей может привести к утечке конфиденциальных данных студентов и сотрудников, включая личную информацию, оценки, результаты исследований и финансовые данные. Кроме того, злоумышленники могут использовать украденные учетные данные для получения доступа к внутренним системам университета, что может привести к дальнейшим атакам и утечкам данных.

Программы-вымогатели (или ransomware) являются одной из самых опасных и разрушительных киберугроз для университетов [24]. Эти вредоносные программы проникают в компьютерные системы, шифруют данные и требуют выкуп за их разблокирование. Шифрование данных может затронуть студенческие и административные записи, научные исследования, учебные материалы и другие важные файлы. Это может привести к остановке учебного процесса, потере ценной исследовательской работы и нарушению административных функций. В некоторых случаях университеты могут потерять годы работы и критически важную информацию, которая не подлежит восстановлению. Репутационные потери также могут быть значительными, так как такие инциденты подрывают доверие студентов, сотрудников и партнеров.

Следующей угрозой представляется искусственный интеллект, который становится все более распространенным инструментом, как для защитников, так и для злоумышленников в киберпространстве. Если искусственный интеллект - это способность компьютерных систем выполнять задачи, требующие человеческого интеллекта, такие как визуальное восприятие, распознавание речи, принятие решений и перевод между языками [25], то угрозы, основанные на искусственном интеллекте, представляют собой новую волну кибератак, которые могут быть особенно опасными для университетов. Искусственный интеллект может анализировать огромные объемы данных из социальных сетей, корпоративных сайтов и других источников, чтобы создавать высоко целевые и правдоподобные фишинговые атаки. Такие письма могут быть трудно распознаваемыми даже для опытных пользователей, что увеличивает вероятность их успешного выполнения.

Одной из главных угроз темной паутины, или Dark Web, для университетов является утечка и продажа конфиденциальной информации. Данные, такие как личная информация студентов и сотрудников, результаты исследований, финансовые данные и другая чувствительная информация, могут быть украдены во время кибератаки и затем проданы в темной сети. Это может привести к серьезным последствиям, включая финансовые потери, нарушение репутации и юридические проблемы, связанные с несоблюдением законов о защите данных [26].

Компрометация корпоративной электронной почты (Business Email Compromise, BEC) представляет собой одну из самых изощренных и разрушительных киберугроз, направленных на учебные заведения. BEC-атаки основаны на использовании социальной инженерии для обмана пользователей с целью получения доступа к корпоративным электронным почтовым учетным записям или заставить их выполнить определенные действия, такие как перевод денег или передача конфиденциальной информации. Одним из распространенных методов BEC-атак является отправка поддельных электронных писем от имени высокопоставленных сотрудников университета. Из-за высокой правдоподобности таких писем многие сотрудники могут не распознать угрозу и выполнить требуемые действия.

Удаленная работа, ставшая повсеместной в результате пандемии COVID-19, принесла университетам

множество новых возможностей, но также и значительные киберугрозы. С переходом на удаленные форматы работы и обучения учебные заведения столкнулись с необходимостью обеспечения безопасности данных и систем в условиях распределенной ИТ-инфраструктуры [27]. Одной из основных угроз, связанных с удаленной работой, является необеспеченная домашняя инфраструктура. Домашние сети часто менее защищены, чем корпоративные, что делает их более уязвимыми для атак. Множество подключенных устройств, слабые пароли на роутерах и отсутствие шифрования делают домашние сети легкой мишенью для злоумышленников. Недостаток физической безопасности представляет еще одну серьезную угрозу. Данные и устройства, используемые вне стен университета, подвержены риску кражи или потери. Это особенно актуально для ноутбуков и мобильных устройств, которые могут содержать конфиденциальную информацию [28]. Популярные инструменты для видеоконференций, совместного использования файлов и удаленного доступа могут содержать уязвимости, что ставит под угрозу всю ИТ-инфраструктуру университета.

Уязвимости цепочки поставок возникают, когда злоумышленники получают доступ к университетским системам и данным через недостатки в безопасности у сторонних поставщиков программного и аппаратного обеспечения, сервисов и других ресурсов. Поскольку университеты часто зависят от внешних поставщиков для множества ИТ-решений, атаки на цепочку поставок могут иметь катастрофические последствия. Одной из основных угроз является возможность внедрения вредоносного кода в программное обеспечение еще на стадии разработки или распространения. В результате компрометация может оставаться незамеченной в течение длительного времени, нанося значительный ущерб и предоставляя злоумышленникам доступ к конфиденциальной информации.

С ростом использования облачных технологий в университетах, вопросы безопасности цифровых данных становятся все более актуальными. Облачные сервисы предоставляют множество преимуществ, включая гибкость, масштабируемость и доступность, но вместе с тем они также несут значительные киберриски [29]. Университеты используют облачные платформы для хранения данных, управления учебными материалами, проведения онлайн-курсов и исследований, что делает их привлекательными целями для злоумышленников. Одной из основных угроз для безопасности облака является несанкционированный доступ к данным. Уязвимости в системе аутентификации, слабые пароли и недостаточная защита учетных записей могут значительно повысить риск таких атак. Ошибки конфигурации облачных сервисов могут привести к случайной утечке данных, когда информация становится доступной для неавторизованных пользователей. Например, неправильная настройка разрешений может сделать данные доступными для всех пользователей сети, что может привести к серьезным последствиям, включая нарушение конфиденциальности и утрату интеллектуальной собственности. Доступ третьих сторон к данным также является важным аспектом безопасности облака. Университеты часто используют облачные сервисы от сторонних провайдеров, и безопасность этих данных зависит от надежности и мер защиты, применяемых провайдерами. Кроме того, облачные среды подвержены атакам, таким как распределенные атаки отказа в обслуживании (DDoS), которые могут нарушить доступность сервисов [30]. DDoS-атаки могут перегрузить облачную инфраструктуру, делая сервисы недоступными для студентов и преподавателей, что может серьезно нарушить учебный процесс и административные функции.

Квантовые вычисления представляют собой значительную киберугрозу для университетов в ближайшем будущем [31]. Эта новая технологическая парадигма обещает революционизировать вычислительные возможности, предлагая значительно более мощные способы обработки данных по сравнению с классическими компьютерами. Однако вместе с этими

возможностями квантовые вычисления также несут потенциальные риски для безопасности данных и систем, используемых университетами. Одной из основных угроз, связанных с квантовыми вычислениями, является способность квантовых компьютеров эффективно взламывать современные криптографические алгоритмы. Традиционные методы шифрования, такие как RSA и ECC, основываются на сложности математических задач, которые требуют значительных вычислительных ресурсов для их решения на классических компьютерах. Квантовые компьютеры, используя определенные алгоритмы, смогут решать эти задачи намного быстрее, что сделает текущие методы шифрования устаревшими и уязвимыми к атакам [32]. Это создает серьезные риски для конфиденциальности данных, хранящихся и передаваемых университетами. Кроме того, квантовые вычисления могут ускорить процесс взлома паролей и других методов аутентификации. Квантовые компьютеры смогут проводить перебор возможных комбинаций значительно быстрее, чем это возможно на классических компьютерах. Это увеличивает вероятность успешного взлома учетных записей и систем, особенно если используются слабые или устаревшие методы защиты.

Из всего перечня актуальных на сегодняшний день киберугроз [22], по нашему мнению, наиболее значимыми являются риски, связанные с человеческим фактором. Человеческие риски представляют собой одну из наиболее значительных угроз для кибербезопасности университетов. Эти риски связаны с поведением, ошибками и недостаточной осведомленностью сотрудников и студентов в области кибербезопасности. Люди остаются самым слабым звеном в цепочке безопасности, и даже самые современные технические средства защиты могут оказаться бессильными перед человеческим фактором.

Исследование уровня цифровой грамотности студентов и преподавателей казахстанских вузов, проведенное авторами в 2023-2024 учебном году [33, 34], продемонстрировало достаточно высокие результаты. Цифровая грамотность преподавателей сформирована на уровне 89%, студентов – 79%. Однако, из всех элементов цифровой грамотности наиболее низкие показатели оказались по информационной грамотности (рисунок 3).

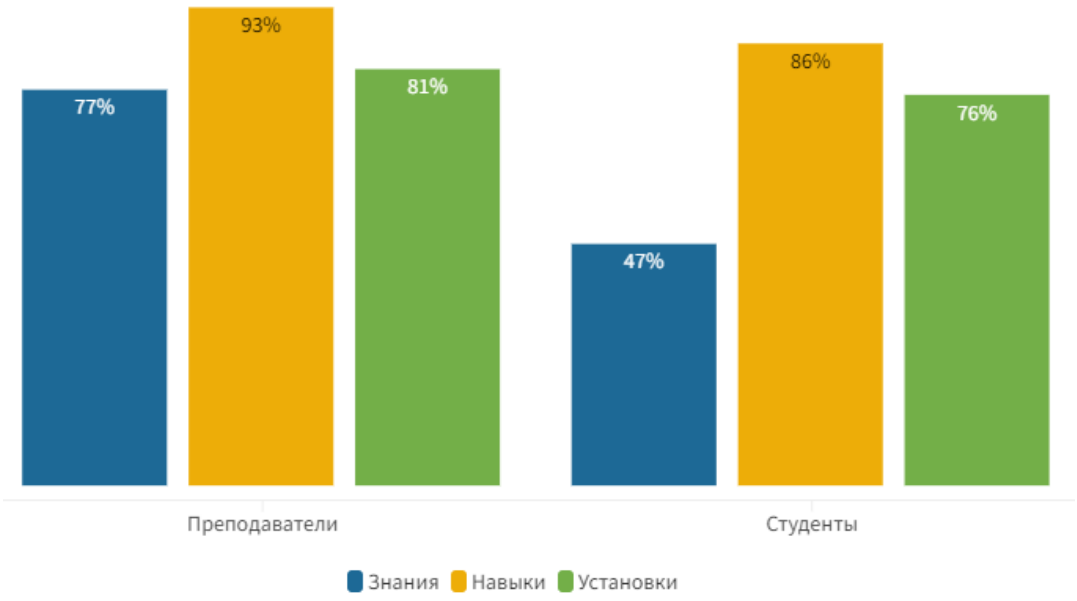
Рисунок 3 – Структура цифровой грамотности студентов и преподавателей казахстанских вузов

Примечание – составлено авторами

Информационная грамотность в контексте цифровой среды - это способность эффективно находить, оценивать, использовать и управлять информацией в цифровом пространстве [7]. Важнейшим аспектом информационной грамотности является соблюдение безопасности при использовании технологий и Интернета, которое включает понимание основных угроз, связанных с цифровой средой, и умение применять методы защиты данных и конфиденциальности.

Соблюдение безопасности при использовании технологий и Интернета начинается с осознания потенциальных рисков, таких как кибератаки, фишинговые схемы, вредоносное ПО и утечки данных. Для эффективного противостояния этим угрозам необходимо развивать навыки распознавания подозрительных действий в сети, например, идентифицировать поддельные веб-сайты или подозрительные электронные письма, а также понимать важность использования сложных паролей и двухфакторной аутентификации [35].

Результаты исследования также продемонстрировали значительный разрыв между различными компонентами информационной грамотности, особенно в области знаний, как среди преподавателей, так и среди студентов (рисунок 4).



Примечание – составлено авторами

Рисунок 4 – Компоненты информационной грамотности студентов и преподавателей казахстанских вузов

Низкие показатели знаний в области информационной грамотности имеют прямую связь с кибербезопасностью, и это вызывает серьезные опасения. Знания, составляющие лишь 77% у преподавателей и 47% у студентов, включают в себя фундаментальные теоретические аспекты, такие как понимание принципов кибербезопасности, осведомленность о современных угрозах, а также знания о методах защиты данных и конфиденциальности в цифровой среде. Недостаток этих знаний может серьезно подорвать способность преподавателей и студентов эффективно защищать себя и свои данные в цифровом пространстве.

Понимание основ кибербезопасности критически важно в условиях растущего числа кибератак, таких как программы-вымогатели, фишинговые схемы и другие виды цифровых угроз. Если знания в этой области не являются

достаточно глубокими, пользователи могут не распознавать потенциальные угрозы, что делает их уязвимыми перед кибератаками.

В то же время, навыки, то есть практическое применение знаний и умений работать с информацией, оказались лучше развиты как у преподавателей (93%), так и у студентов (86%). Это позитивный сигнал, свидетельствующий о том, что обе группы умеют эффективно использовать полученные знания на практике, хотя и испытывают дефицит в теоретической подготовке.

Установки, которые отражают отношение и мотивацию к использованию информационных технологий, также находятся на достаточно высоком уровне: 81% у преподавателей и 76% у студентов. Это означает, что в целом и преподаватели, и студенты положительно относятся к использованию технологий и осознают их важность в образовательном процессе.

Цифровая среда постоянно меняется, и новые угрозы появляются ежедневно, что подчеркивает важность постоянного обучения в области кибербезопасности. В этом контексте информационная грамотность напрямую связана с кибербезопасностью. Обучение безопасному поведению в Интернете помогает защитить не только личные данные, но и данные организаций, с которыми человек может быть связан. Это особенно важно в условиях глобализации и цифровизации, когда утечка данных может нанести ущерб репутации и финансовому состоянию не только отдельного пользователя, но и всей организации.

Развитие определенных знаний и навыков в области информационной грамотности необходимо для того, чтобы пользователи цифровых технологий могли эффективно управлять своими цифровыми активами и оставаться защищенными в сети. Эти знания включают умение распознавать и избегать фишинговых атак, использовать безопасные пароли, защищать свои устройства от вредоносных программ, а также понимать и соблюдать принципы конфиденциальности и защиты данных в социальных сетях и других онлайн-платформах.

Таким образом, информационная грамотность является ключевым элементом в обеспечении личной и организационной кибербезопасности. Она требует не только базовых знаний о работе в цифровой среде, но и глубокого понимания рисков и методов их предотвращения. В условиях постоянно растущих угроз развитие этих знаний и навыков становится не просто необходимостью, но и основой для безопасного и ответственного использования цифровых технологий в современном мире.

Обсуждение и выводы

Влияние человеческих рисков на деятельность университетов может быть многогранным. Утечка конфиденциальных данных студентов и сотрудников может привести к серьезным последствиям, включая нарушение законодательства о защите персональных данных, финансовые потери и урон репутации учебного заведения. Кроме того, успешные кибератаки могут вызвать перебои в работе университетских систем и сервисов, что негативно скажется на учебном процессе и административных функциях.

Одной из основных проблем является использование слабых паролей и отсутствие практики регулярного их обновления. Многие сотрудники и студенты по-прежнему выбирают легко угадываемые пароли или используют один и тот же пароль для множества учетных записей. Это значительно упрощает задачу злоумышленникам, пытающимся получить несанкционированный доступ к системам и данным университета.

Кроме того, ошибки при работе с электронной почтой также представляют серьезную угрозу. Открытие фишинговых писем, переход по подозрительным ссылкам или загрузка вложений от неизвестных отправителей могут привести к утечке конфиденциальной информации или заражению устройств вредоносным программным обеспечением. Несмотря на широкое распространение информации о фишинговых атаках, многие пользователи по-прежнему становятся жертвами таких мошеннических схем.

Недостаточная подготовка и осведомленность о киберугрозах среди персонала и студентов также усугубляют проблему. В условиях стремительной

цифровизации образовательных процессов многие университеты сталкиваются с необходимостью обучения своих сотрудников и студентов основам кибербезопасности [36]. Без этого знания и навыки уязвимых пользователей могут быть легко использованы злоумышленниками для проведения атак.

Для минимизации человеческих рисков университетам необходимо принимать комплексные меры. Прежде всего, важно проводить регулярные обучающие программы и тренинги по кибербезопасности, направленные на повышение осведомленности сотрудников и студентов о современных угрозах и методах их предотвращения. Такие программы должны включать информацию о важности использования сложных и уникальных паролей, распознавании фишинговых писем и безопасной работе в Интернете.

Вместе с тем необходимо внедрять строгие политики и процедуры, связанные с использованием данных и устройств. Университеты должны обеспечивать контроль доступа к критически важной информации и системам, а также устанавливать ограничения на использование личных устройств для работы с конфиденциальными данными. Регулярные проверки и аудит соблюдения этих политик помогут выявлять и устранять потенциальные уязвимости.

В целом, управление человеческими рисками в контексте кибербезопасности требует постоянного внимания и усилий со стороны университетов. Только путем создания культуры кибербезопасности, постоянного обучения и совершенствования защитных мер можно эффективно противостоять угрозам и обеспечивать безопасное образовательное пространство для всех участников учебного процесса.

Обеспечение кибербезопасности является неотъемлемой частью защиты прав на конфиденциальность, безопасность, доступ к информации и недискриминацию. Иначе говоря, обеспечение кибербезопасности является частью защиты прав человека, что в структуре компонентов социальной ответственности представляет наибольшую обеспокоенность со стороны преподавателей и обучающихся [37].

Обеспечение кибербезопасности в университетах имеет непосредственное отношение к нормам ISO 26000:2010, которые определяют ответственность организации за влияние ее решений и деятельности на общество и окружающую среду. Вузы обязаны принять этические и прозрачные меры для защиты данных и систем, способствуя устойчивому развитию, учитывая ожидания заинтересованных сторон, соблюдая действующее законодательство и соответствуя международным стандартам поведения.

Интеграция кибербезопасности должна быть всесторонней и охватывать все аспекты деятельности университета. Принятие мер по защите от кибератак также способствует поддержанию академической честности и прозрачности, что является важным аспектом социальной ответственности. Необходимость обеспечения безопасных условий для удаленной работы, защиты от фишинга и программ-вымогателей, а также повышение осведомленности сотрудников и студентов о киберугрозах - все это ключевые элементы, которые должны быть включены в политику социальной ответственности университетов.

Внедрение и соблюдение принципов кибербезопасности помогут университетам не только соответствовать нормам ISO 26000, но и укрепить доверие со стороны общества, студентов и сотрудников. Это потребует пересмотра текущих принципов социальной ответственности, интеграции новых технологий и методов защиты, а также постоянного обучения и повышения квалификации всех участников образовательного процесса. Таким образом, университеты смогут создать безопасную и устойчивую образовательную среду, способствующую развитию общества и соблюдению высоких стандартов социальной ответственности.

Для дальнейшего углубленного изучения кибербезопасности и социальной ответственности в образовательных учреждениях предлагается несколько направлений исследований. Одним из ключевых направлений является проведение международных сравнительных исследований для выявления общих тенденций и специфических особенностей в

обеспечении кибербезопасности и социальной ответственности в университетах разных стран. Это позволит определить лучшие практики, которые могут быть адаптированы к различным культурным и законодательным контекстам.

Другим важным направлением является разработка и внедрение образовательных программ по кибербезопасности. Исследования в этой области могут быть направлены на оценку эффективности различных программ и курсов, ориентированных на повышение уровня информационной грамотности и осведомленности о киберугрозах среди студентов и преподавателей. Необходимо определить, какие методы обучения наиболее эффективны для различных групп пользователей и как они могут способствовать укреплению кибербезопасности в университетах.

Кроме того, важным направлением является изучение влияния киберугроз на академическую честность и прозрачность в образовательных учреждениях. Это может включать исследования, направленные на понимание того, как такие кибератаки, как фишинг и программы-вымогатели, могут подрывать доверие между преподавателями и студентами, а также как они влияют на академическую честность.

Еще одно перспективное направление связано с оценкой влияния уровня цифровой грамотности на киберустойчивость университетов. Такие исследования помогут определить, в какой степени цифровая грамотность преподавателей и студентов способствует защите от киберугроз, и выявить области, требующие дополнительного внимания и улучшения.

В совокупности эти направления исследований могут способствовать более глубокому пониманию проблемы и разработке эффективных стратегий для обеспечения кибербезопасности и социальной ответственности в образовательных учреждениях, что, в свою очередь, будет способствовать созданию безопасной и устойчивой образовательной среды.

Ограничения

Исследование имеет несколько ограничений, которые следует учитывать при интерпретации полученных результатов. Во-первых, анкетирование проводилось среди студентов и преподавателей только казахстанских вузов, что ограничивает возможность обобщения выводов на другие страны и образовательные системы. Результаты могут отражать специфические особенности цифровой грамотности и кибербезопасности в конкретном национальном контексте. Другое ограничение связано с характером используемых методов. Контент-анализ и анализ нормативных документов предоставляют ценную информацию, но они не всегда позволяют выявить все возможные аспекты и нюансы практического применения мер кибербезопасности. Кроме того, в исследовании не использовались сложные статистические методы анализа, что ограничивает глубину и точность полученных выводов. Учитывая эти ограничения, результаты исследования следует рассматривать как основу для дальнейших более широких и детализированных исследований, направленных на изучение кибербезопасности и социальной ответственности в образовательных учреждениях на международном уровне.

Финансирование

Исследование выполнено в рамках грантового финансирования Комитета науки Министерства науки и высшего образования Республики Казахстан (№AP13268867)

Список литературы

1 ISO 26000. ISO 26000 Adopted as European Standard [Офиц. сайт]. - URL: https://iso26000.info/iso/iso-standards/iso-26000/european-standard-iso-26000/. (Date of access: 20.07.2024)

2 Godonoga, A. The conceptualisation of socially responsible universities in higher education research: a systematic literature review [Text] / Godonoga, A., Sporn, B. // Studies in Higher Education. - Vol. 48(3). – pp. 445-459. https://doi.org/10.1080/03075079.2022.2145462

3 World Conference on Higher Education for the Twenty-first Century: Vision and Action // UNESCO General Conference 30th Session. – 1999. - URL: https://unesdoc.unesco.org/ark:/48223/pf0000117022_rus. (Date of access: 20.07.2024)

4 Zhao, W. Application of ISO 26000 in digital education during COVID-19 [Text] / Zhao, W., Zhang, J., Liu, X., Jiang, Zh. // Ain Shams Engineering Journal. – 2022. – Vol. 13(3). https://doi.org/10.1016/j.asej.2021.10.025

5 Bongiovanni, I. The least secure places in the universe? A systematic literature review on information security management in higher education [Text] / Bongiovanni, I. // Computers & Security. – 2019. - Vol. 86. – 350-357. https://doi.org/10.1016/j.cose.2019.07.003

6 Аймалетдинов Т.А. Цифровая грамотность российских педагогов. Готовность к использованию цифровых технологий в учебном процессе [Текст] / Аймалетдинов, Т.А., Баймуратова, Л.Р., Зайцева, О.А., Имаева, Г.Р., Спиридонова, Л.В. // Аналитический центр НАФИ. – М.: Издательство НАФИ. - 2019. – 84 с.

7 Overview of Information Literacy Resources Worldwide // UNESCO. – 2013. - URL: https://unesdoc.unesco.org/ark:/48223/pf0000219667. (Date of access: 20.07.2024)

8 Rodrigues, A.F. Cybersecurity risks: A behavioural approach through the influence of media and information literacy [Text] / Rodrigues, A.F., Monteiro, B.M., Pedrosa, I. // Iberian Conference on Information Systems and Technologies, CISTI. – 2021. https://doi.org/10.23919/CISTI52073.2021.9476383

9 Denchev, S. Information Literacy, Information Transparency and Information Accessibility – Distinctive Features of Cyber Security [Text] / Denchev, S., Peteva, I., Yordanova, S. // Proceedings IMCIC - International Multi-Conference on Complexity, Informatics and Cybernetics. – 2024. - pp. 145-147. https://doi.org/10.54808/IMCIC2024.01.145

10 Fauzi, M.A. University social responsibility: the present and future trends based on bibliometric analysis [Text] / Fauzi, M.A., Abdul Wahab, N., Ahmad, M.H. and Abidin, I. // Journal of Applied Research in Higher Education. – 2024. - Vol. 16(3). - pp. 948-965. https://doi.org/10.1108/JARHE-03-2023-0110

11 del Consuelo Gallardo Aguilar, M. University social responsibility: Evaluation and impact on student satisfaction as an opportunity for knowledge management and sustainability [Text] / del Consuelo Gallardo Aguilar, M., de la Garza Carranza, M.T., Ibarra, S.T.C., Cervantes, M.S. // Ecocentrism for Knowledge Management and Sustainability: Theoretical and Practical Studies in the Post-industrial Era. – 2024. – pp. 176-188.

12 Ricci, S. Understanding Cybersecurity Education Gaps in Europe [Text] / Ricci, S., Parker, S., Jerabek, J., Danidou, Y., Chatzopoulou, A., Badonnel, R., Lendak, I., Janout, V. // IEEE Transactions on Education. - April 2024. - Vol. 67(2). - pp. 190-201. https://doi.org/10.1109/TE.2023.3340868

13 Simon, N. Reimaging Cybersecurity in Educational Practices: An International Case Study [Text] / Simon, N., Jiménez, J.L., Strocchia, D. // Handbook of Research on Current Trends in Cybersecurity and Educational Technology. - IGI Global. – 2023. - pp. 1-18. https://doi.org/10.4018/978-1-6684-6092-4.ch001

14 Баймуратова, Л.Р. Цифровая грамотность для экономики будущего [Текст] / Баймуратова, Л.Р., Долгова, О.А., Имаева, Г.Р., Гриценко, В.И., Смирнов, К.В., Аймалетдинов, Т.А. // Аналитический центр НАФИ. – М.: Издательство НАФИ. - 2018. – 86 с.

15 Craigen, D. Defining cybersecurity [Text] / Craigen, D., Diakun-Thibault, N., Purse, R. // Technology Innovation Management Review. – 2014. – Vol. 4. – pp. 13-21.

16 Zhang-Kennedy, L. The role of cybersecurity in information technology education [Text] / Zhang-Kennedy, L., Chiasson, S. [Text] // Proceedings of the 2011 Conference on Information Technology Education. - 2021. – pp. 113-122.

17 Desai, D., Hegde, R., Laufer, E., Wang, J. Phishing Report Reveals 47.2% Surge in Phishing Attacks Last Year [Text] April 18, 2023. https://www.zscaler.com/blogs/security-research/2023-phishing-report-reveals-47-2-surge-phishing-attacks-last-year (Date of access: 20.07.2024)

18 Pranggono, B. COVID-19 pandemic cybersecurity issues [Text] / Pranggono, B., Arabo, A. // Internet Technology Letters. – 2021. – Vol. 4(2). – p. 247

19 Ransomware Trends 2023 Report [Text] April 7, 2024. https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report/ (Date of access: 20.07.2024)

20 Кибербезопасность в 2022-2023. Тренды и прогнозы [Текст] 13 января 2023. https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/#id14 (Дата обращения: 20.07.2024)

21 Aldawood, H. Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review [Text] / Aldawood, H., Skinner, G. // Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering. – 2018. – pp. 62-68. https://doi.org/10.1109/TALE.2018.8615162

22 Top 10 cybersecurity threats in 2024 [Text] https://blog.usecure.io/top-10-cybersecurity-threats#Human-risks (Date of access: 20.07.2024)

23 Greco, F. Supporting the Design of Phishing Education, Training and Awareness interventions: an LLM-based approach [Text] / Greco, F., Desolda, G., Viganò, L. // CEUR Workshop Proceedings. - 2024

24 Amaka, R.O. Cybersecurity Crisis Management in Higher Education Institutions: A Case of How the University of Sunderland in London Managed a Ransomware Threat [Text] / Amaka, R.O., Cantafio, G.U. // Promoting Crisis Management and Creative Problem-Solving Skills in Educational Leadership. – pp. 26-48 https://doi.org/10.4018/978-1-6684-8332-9.ch002

25 Russell, S. Artificial Intelligence: A Modern Approach [Text] / Russell, S., Norvig, P. // Prentice Hall, 3 edition, 2010.

26 Dalvi, A. Dark web content classification using quantum encoding [Text] / Dalvi, A., Bhoir, S., Kazi, F., Bhirud, S.G. // Quantum Computing in Cybersecurity. – 2023. – pp. 57-79. https://doi.org/10.1002/9781394167401.ch4

27 Whitty, M.T. Cybersecurity when working from home during COVID-19: considering the human factors [Text] / Whitty, M.T., Nour, M., Grobler, M. // Journal of Cybersecurity. – 2024. – Vol. 10(1). https://doi.org/10.1093/cybsec/tyae001

28 Ferdousi, B. Cyber security risks of bring your own device (BYOD) practice in workplace and strategies to address the risks [Text] / Ferdousi, B. // International Journal of Science Academic Research. – 2022. – Vol. 3(10). - pp. 4554-4558.

29 Akinrolabu, O. Cyber risk assessment in cloud provider environments: Current models and future needs [Text] / Akinrolabu, O., Nurse, J.R.C., Martin, A., New, S. // Computers and Security. – 2019. – Vol. 87. https://doi.org/10.1016/j.cose.2019.101600

30 Sharma, K. Cyber risk assessment and mitigation using logit and probit models for DDoS attacks [Text] / Sharma, K., Mukhopadhyay, A. // 26th Americas Conference on Information Systems, AMCIS. – 2020.

31 Serrano, M.A. Towards a quantum world in cybersecurity land [Text] / Serrano, M.A., Sanchez, L.E., Santos-Olmo, A., ... Blanco, C., Fernandez-Medina, E. // CEUR Workshop Proceedings. – 2023.

32 Singh, J. Contemporary Quantum Computing Use Cases: Taxonomy, Review and Challenges [Text] / Singh, J., Bhangu, K.S. // Archives of Computational Methods in Engineering. – 2023. – Vol. 30(1). – pp. 615-638. https://doi.org/10.1007/s11831-022-09809-5

33 Закирова, Д.И. Контуры современного образования: оценка цифровых навыков студентов [Текст] / Закирова, Д.И., Пол, М. // Научный журнал «Вестник университета «Туран». – 2024. - № 1(101). - с. 355-373. https://doi.org/10.46914/1562-2959-2024-1-1-355-373

34 Закирова, Д.И. Анализ уровня цифровой грамотности преподавателей вуза: многокомпонентный подход [Текст] / Закирова, Д.И. // Proceedings of the 6th International Scientific Conference «Research Retrieval and Academic Letters». - July 4-5, 2024. – pp. 5-15

35 Guillén-Gámez, D. Digital Competences in Cybersecurity of Teachers in Training [Text] / Guillén-Gámez, D. F., Martínez-García, I., Alastor, E., Tomczyk, Ł. // Computers in the Schools. – 2024. – Vol. 1. - p. 26. https://doi.org/10.1080/07380569.2024.2361614

36 Allison, J. Cybersecurity Risk Management Scenarios for Teaching Information Security Management [Text] / Allison, J. // Journal of Applied Security Research. – 2024. – Vol. 1. – p. 22. https://doi.org/10.1080/19361610.2024.2358272

37 Rodrigues de Sousa J.C. University social responsibility: Perceptions and advances [Text] / Rodrigues de Sousa, J.C., Stradiotto Siqueira, E., Binotto, E., Holanda Nepomuceno Nobre, L. // Social Responsibility Journal. – 2021. – Vol. 17. – pp. 263-281. https://doi.org/10.1108/SRJ-10-2017-0199

References

1 ISO 26000. ISO 26000 Adopted as European Standard [Ofic. sajt]. - URL: https://iso26000.info/iso/iso-standards/iso-26000/european-standard-iso-26000/. (Date of access: 20.07.2024)

2 Godonoga, A. The conceptualisation of socially responsible universities in higher education research: a systematic literature review [Text] / Godonoga, A., Sporn, B. // Studies in Higher Education. - Vol. 48(3). – pp. 445-459. https://doi.org/10.1080/03075079.2022.2145462

3 World Conference on Higher Education for the Twenty-first Century: Vision and Action // UNESCO General Conference 30th Session. – 1999. - URL: https://unesdoc.unesco.org/ark:/48223/pf0000117022_rus. (Date of access: 20.07.2024)

4 Zhao, W. Application of ISO 26000 in digital education during COVID-19 [Text] / Zhao, W., Zhang, J., Liu, X., Jiang, Zh. // Ain Shams Engineering Journal. – 2022. – Vol. 13(3). https://doi.org/10.1016/j.asej.2021.10.025

5 Bongiovanni, I. The least secure places in the universe? A systematic literature review on information security management in higher education [Text] / Bongiovanni, I. // Computers & Security. – 2019. - Vol. 86. – 350-357. https://doi.org/10.1016/j.cose.2019.07.003

6 Ajmaletdinov T.A. Cifrovaja gramotnost' rossijskih pedagogov. Gotovnost' k ispol'zovaniju cifrovyh tehnologij v uchebnom processe [Text] / Ajmaletdinov, T.A., Bajmuratova, L.R., Zajceva, O.A., Imaeva, G.R., Spiridonova, L.V. // Analiticheskij centr NAFI. – M.: Izdatel'stvo NAFI. - 2019. – 84 p.

7 Overview of Information Literacy Resources Worldwide // UNESCO. – 2013. - URL: https://unesdoc.unesco.org/ark:/48223/pf0000219667. (Date of access: 20.07.2024)

8 Rodrigues, A.F. Cybersecurity risks: A behavioural approach through the influence of media and information literacy [Text] / Rodrigues, A.F., Monteiro, B.M., Pedrosa, I. // Iberian Conference on Information Systems and Technologies, CISTI. – 2021. https://doi.org/10.23919/CISTI52073.2021.9476383

9 Denchev, S. Information Literacy, Information Transparency and Information Accessibility – Distinctive Features of Cyber Security [Text] / Denchev, S., Peteva, I., Yordanova, S. // Proceedings IMCIC - International Multi-Conference on Complexity, Informatics and Cybernetics. – 2024. - pp. 145-147. https://doi.org/10.54808/IMCIC2024.01.145

10 Fauzi, M.A. University social responsibility: the present and future trends based on bibliometric analysis [Text] / Fauzi, M.A., Abdul Wahab, N., Ahmad, M.H. and Abidin, I. // Journal of Applied Research in Higher Education. – 2024. - Vol. 16(3). - pp. 948-965. https://doi.org/10.1108/JARHE-03-2023-0110

11 del Consuelo Gallardo Aguilar, M. University social responsibility: Evaluation and impact on student satisfaction as an opportunity for knowledge management and sustainability [Text] / del Consuelo Gallardo Aguilar, M., de la Garza Carranza, M.T., Ibarra, S.T.C., Cervantes, M.S. // Ecocentrism for Knowledge Management and Sustainability: Theoretical and Practical Studies in the Post-industrial Era. – 2024. – pp. 176-188.

12 Ricci, S. Understanding Cybersecurity Education Gaps in Europe [Text] / Ricci, S., Parker, S., Jerabek, J., Danidou, Y., Chatzopoulou, A., Badonnel, R., Lendak, I., Janout, V. //

IEEE Transactions on Education. - April 2024. - Vol. 67(2). - pp. 190-201. https://doi.org/10.1109/TE.2023.3340868

13 Simon, N. Reimaging Cybersecurity in Educational Practices: An International Case Study [Text] / Simon, N., Jiménez, J.L., Strocchia, D. // Handbook of Research on Current Trends in Cybersecurity and Educational Technology. - IGI Global. – 2023. - pp. 1-18. https://doi.org/10.4018/978-1-6684-6092-4.ch001

14 Bajmuratova, L.R. Cifrovaja gramotnost' dlja jekonomiki budushhego [Text] / Bajmuratova, L.R., Dolgova, O.A., Imaeva, G.R., Gricenko, V.I., Smirnov, K.V., Ajmaletdinov, T.A. // Analiticheskij centr NAFI. – M.: Izdatel'stvo NAFI. - 2018. – 86 p.

15 Craigen, D. Defining cybersecurity [Text] / Craigen, D., Diakun-Thibault, N., Purse, R. // Technology Innovation Management Review. – 2014. – Vol. 4. – pp. 13-21.

16 Zhang-Kennedy, L. The role of cybersecurity in information technology education [Text] / Zhang-Kennedy, L., Chiasson, S. [Text] // Proceedings of the 2011 Conference on Information Technology Education. - 2021. – pp. 113-122.

17 Desai, D., Hegde, R., Laufer, E., Wang, J. Phishing Report Reveals 47.2% Surge in Phishing Attacks Last Year [Text] April 18, 2023. https://www.zscaler.com/blogs/security-research/2023-phishing-report-reveals-47-2-surge-phishing-attacks-last-year (Date of access: 20.07.2024)

18 Pranggono, B. COVID-19 pandemic cybersecurity issues [Text] / Pranggono, B., Arabo, A. // Internet Technology Letters. – 2021. – Vol. 4(2). – p. 247

19 Ransomware Trends 2023 Report [Text] April 7, 2024. https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report/ (Date of access: 20.07.2024)

20 Kiberbezopasnost' v 2022-2023. Trendy i prognozy [Text] 13 janvarja 2023. https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/#id14 (Date of access: 20.07.2024)

21 Aldawood, H. Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review [Text] / Aldawood, H., Skinner, G. // Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering. – 2018. – pp. 62-68. https://doi.org/10.1109/TALE.2018.8615162

22 Top 10 cybersecurity threats in 2024 [Text] https://blog.usecure.io/top-10-cybersecurity-threats#Human-risks (Date of access: 20.07.2024)

23 Greco, F. Supporting the Design of Phishing Education, Training and Awareness interventions: an LLM-based approach [Text] / Greco, F., Desolda, G., Viganò, L. // CEUR Workshop Proceedings. - 2024

24 Amaka, R.O. Cybersecurity Crisis Management in Higher Education Institutions: A Case of How the University of Sunderland in London Managed a Ransomware Threat [Text] / Amaka, R.O., Cantafio, G.U. // Promoting Crisis Management and Creative Problem-Solving Skills in Educational Leadership. – pp. 26-48 https://doi.org/10.4018/978-1-6684-8332-9.ch002

25 Russell, S. Artificial Intelligence: A Modern Approach [Text] / Russell, S., Norvig, P. // Prentice Hall, 3 edition, 2010.

26 Dalvi, A. Dark web content classification using quantum encoding [Text] / Dalvi, A., Bhoir, S., Kazi, F., Bhirud, S.G. // Quantum Computing in Cybersecurity. – 2023. – pp. 57-79. https://doi.org/10.1002/9781394167401.ch4

27 Whitty, M.T. Cybersecurity when working from home during COVID-19: considering the human factors [Text] / Whitty, M.T., Nour, M., Grobler, M. // Journal of Cybersecurity. – 2024. – Vol. 10(1). https://doi.org/10.1093/cybsec/tyae001

28 Ferdousi, B. Cyber security risks of bring your own device (BYOD) practice in workplace and strategies to address the risks [Text] / Ferdousi, B. // International Journal of Science Academic Research. – 2022. – Vol. 3(10). - pp. 4554-4558.

29 Akinrolabu, O. Cyber risk assessment in cloud provider environments: Current models and future needs [Text] / Akinrolabu, O., Nurse, J.R.C., Martin, A., New, S. // Computers and Security. – 2019. – Vol. 87. https://doi.org/10.1016/j.cose.2019.101600

30 Sharma, K. Cyber risk assessment and mitigation using logit and probit models for DDoS attacks [Text] / Sharma, K., Mukhopadhyay, A. // 26th Americas Conference on Information Systems, AMCIS. – 2020.

31 Serrano, M.A. Towards a quantum world in cybersecurity land [Text] / Serrano, M.A., Sanchez, L.E., Santos-Olmo, A., ... Blanco, C., Fernandez-Medina, E. // CEUR Workshop Proceedings. – 2023.

32 Singh, J. Contemporary Quantum Computing Use Cases: Taxonomy, Review and Challenges [Text] / Singh, J., Bhangu, K.S. // Archives of Computational Methods in Engineering. – 2023. – Vol. 30(1). – pp. 615-638. https://doi.org/10.1007/s11831-022-09809-5

33 Zakirova, D.I. Kontury sovremennogo obrazovanija: ocenka cifrovyh navykov studentov [Tekst] / Zakirova, D.I., Pol, M. // Nauchnyj zhurnal «Vestnik universiteta «Turan». – 2024. - № 1(101). - s. 355-373. https://doi.org/10.46914/1562-2959-2024-1-1-355-373

34 Zakirova, D.I. Analiz urovnja cifrovoj gramotnosti prepodavatelej vuza: mnogokomponentnyj podhod [Tekst] / Zakirova, D.I. // Proceedings of the 6th International Scientific Conference «Research Retrieval and Academic Letters». - July 4-5, 2024. – pp. 5-15

35 Guillén-Gámez, D. Digital Competences in Cybersecurity of Teachers in Training [Text] / Guillén-Gámez, D. F., Martínez-García, I., Alastor, E., Tomczyk, Ł. // Computers in the Schools. – 2024. – Vol. 1. - p. 26. https://doi.org/10.1080/07380569.2024.2361614

36 Allison, J. Cybersecurity Risk Management Scenarios for Teaching Information Security Management [Text] / Allison, J. // Journal of Applied Security Research. – 2024. – Vol. 1. – p. 22. https://doi.org/10.1080/19361610.2024.2358272

37 Rodrigues de Sousa J.C. University social responsibility: Perceptions and advances [Text] / Rodrigues de Sousa, J.C., Stradiotto Siqueira, E., Binotto, E., Holanda Nepomuceno Nobre, L. // Social Responsibility Journal. – 2021. – Vol. 17. – pp. 263-281. https://doi.org/10.1108/SRJ-10-2017-0199

ЖОҒАРЫ БІЛІМ БЕРУДІ ЦИФРЛАНДЫРУ ЖАҒДАЙЫНДАҒЫ ӘЛЕУМЕТТІК ЖАУАПКЕРШІЛІК: ӨЗГЕРІСТЕРДІҢ НЕГІЗГІ ФАКТОРЫ РЕТІНДЕ КИБЕРҚАУІПСІЗДІК

Дильнара ЗАКИРОВА*, *PhD, зерттеуші профессор, «Тұран» университеті, Алматы қ., Қазақстан Республикасы, ulasdila@gmail.com, ORCID: 0000-0001-5161-959X, Scopus Author ID: 57205166010*

***Милан ПОЛ**, PhD, профессор, Масариков университеті, Брно қ., Чехия, pol@phil.muni.cz, ORCID: 0000-0002-5787-8610, Scopus Author ID: 559957210*

SOCIAL RESPONSIBILITY IN THE CONTEXT OF DIGITALIZATION OF HIGHER EDUCATION: CYBERSECURITY AS A KEY FACTOR OF CHANGE

Dilnara ZAKIROVA*, *PhD, research professor, Turan University, Almaty, Republic of Kazakhstan, ulasdila@gmail.com, ORCID: 0000-0001-5161-959X, Scopus Author ID: 57205166010*

***Milan POL**, PhD, professor, Masaryk University, Brno, Arna Novaka 1/1, 602 00, Czech Republic, pol@phil.muni.cz, ORCID: 0000-0002-5787-8610, Scopus Author ID: 55995721000*