http://ma123.ru **ЦИТИСЭ** №3 (33) 2022 **ISSN** 2409-7616

Научная статья
УДК 378:004.7.056.53
DOI: http://doi.org/10.15350/2409-7616.2022.3.14

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Е.Ю. Воронов

Воронов Евгений Юрьевич,
специалист отдела информационной безопасности, Астраханский государственный медицинский университет, Астрахань, Россия.
ORCID iD: 0000-0003-3368-8449
foron789@yandex.ru

Аннотация. *Интернет в настоящее время становится одним из важнейших инструментов для решения различного рода задач, возникающих перед человеком, - это и возможность получения информации, онлайн услуг и образования, возможность общения и работы. Однако, с расширяющимися сферами применения интернет ресурсом, увеличивается опасность стать жертвой киберпреступников, для которых аккаунты в социальных сетях, логины и пароли от онлайн банкинга, а так же конфиденциальные данные являются достаточно привлекательными. Сегодня для киберпреступников интересны и информационные ресурсы различных компаний, организаций, в том числе и университетов, которые размещающают в своих информационных системах от личных данных сотрудников, до результатов научно-исследовательской деятельности. Поэтому вопросы обеспечения информационной безопасности университетов, а также его обучающихся и сотрудников, по мнению специалистов, является одним из актуальнейших на сегодняшний день. Несомненно, вузы предпринимают меры по защите информационных систем, создают специальные инфраструктуры по информационной безопасности. Закупаются и устанавливаются различного рода программные продукты и т.п. И все же, на наш взгляд, пользователи сети Интернет, обучающиеся и сотрудники, играют ключевую роль в обеспечении информационной безопасности как личной, так и вузовской. Поэтому, наше исследование мы ориентировали на оценку знаний в области информационной безопасности и готовности данные знания применять для обеспечения собственной безопасности. В ходе исследования мы использовали методику Ш.А. Крюгера и В.Д. Керни, позволяющую получить данные в соответствии с целью исследования. Обобщение результатов подтвердило необходимость разработки специальных образовательных программ, направленных на формирование компетенций в области информационной безопасности.*

Ключевые слова: *информационная безопасность в университете, обучение основам кибербезопасности.*

Библиографическая ссылка: *Воронов Е.Ю. Информационная безопасность образовательной организации: проблемы и перспективы // ЦИТИСЭ. 2022. № 3. С.161-169. DOI: http://doi.org/10.15350/2409-7616.2022.3.14*

Research Full Article
UDC 378:004.7.056.53

CYBER SECURITY OF AN EDUCATIONAL INSTITUTION: ISSUES AND PERSPECTIVES

E.Yu. Voronov

Evgeny Yu. Voronov,
Information Department Specialist security
of Astrakhan State Medical University,
Astrakhan, Russian Federation.
ORCID iD: 0000-0003-3368-8449
foron789@yandex.ru

Abstract. *Nowadays internet is becoming one of the most important tools for solving various challenges that arise before a person. They are the ability of receiving information, online services and education, possibility of work and communication. However, with the spreading spheres of the application of internet resources, there appears a danger of becoming a victim of cyber criminals. For them confidential data of social network accounts, online bank logins and passwords are rather attractive. Today cyber criminals are interested in the information resources of different companies, organizations as well as universities that publish in their information systems different kind of data varying from personal data of their employees to the results of scientific research activities. Thus, according to specialists, currently the issues of providing cyber security of universities as well their students and employees are the most pressing ones. Undoubtedly, universities take measures on securing information systems, special infrastructures on cyber security are created, different software is being bought and installed, etc. Still, to our mind, internet users, students and employees, play the key role in providing the personal cyber security as well as the university one. That's why we oriented our research to the assessment of the knowledge in the field of cyber security and readiness to apply this knowledge for providing self-security. As part of the study we applied the methods according to the goal of the research. Generalization of the results confirmed the necessity of developing special educational programs aimed at forming competencies in the field of cyber security.*

Keywords: *information security at the university, teaching the basics of cybersecurity.*

For citation: *Voronov E.Yu. Cyber security of an educational institution: issues and perspectives. CITISE, 2022, no. 3, pp. 161-169. DOI: http://doi.org/10.15350/2409-7616.2022.3.14*

Введение

Кибербезопасность информационных систем и баз данных высших учебных заведений становится в настоящее время все более актуальной проблемой для каждого отдельного образовательного учреждения. Известно, что в среднем кибератака на информационные системы вузов происходит каждые 39 секунд [1], более 75% отрасли были заражены вредоносными программами за последний год. Это означает, что каждое устройство, подключенное к сети Интернет вуза, является потенциальной целью в любой момент времени, включая любой из компьютеров университета. Университеты всегда подвергались высокому риску киберпреступности, так как данные студентов, личная информация и чрезвычайно ценные исследования делают университеты главной мишенью для киберпреступников. После известной атаки на систему безопасности в 2018 году со стороны иранских хакеров на более чем 300 учреждений, количество атак на университеты

продолжает расти. Анализируя 2020-2021 год с точки зрения киберпреступности, можно отметить увеличение количества новых рисков, связанных с интенсивным использованием университетами различных методов дистанционных технологий обучения. Во время пандемии почти каждую неделю была зафиксирована новая атака, и как отмечается в отчетах британских образовательных учреждений, сотрудникам подразделений, отвечающих за техническую поддержку и информационную безопасность, приходилось восстанавливать IT – инфраструктуры после атак две и/или более недель. В настоящее время около трети европейских университетов признают кражу конфиденциальных данных, в том числе о национальной обороне и о медицинских исследованиях, при этом 87% пережили хотя бы одну успешную кибератаку [2, 3]. Количество фишинговых атак, с которыми вынуждены сталкиваться студенты и преподаватели вузов увеличиваться, и неудивительно, что в настоящее время университеты считают киберпреступность самым серьезным риском.

Отдельно отметим, что анализ судебной и следственной практики отмечает, что «наиболее распространенными преступлениями с применением информационно-телекоммуникационных технологий являются: создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); неправомерный доступ к компьютерной информации (ст. 272 УК РФ); мошеннические действия, совершенные с использованием электронных средств платежа (ст. 159.3 УК РФ). Следует подчеркнуть, что мошенничество с использованием платежных (банковских) карт (ст. 159.3 УК РФ) в 2020 году выросло в 8 раз по сравнению с аналогичными преступлениями, предусмотренными главой 28 УК РФ»[4]

Таким образом, высшее образование, по оценкам компании по управлению киберрисками BitSight имеет самый высокий уровень атак программ-вымогателей среди всех отраслей в периоды с 2020 по 2022 год. Это означает, что университеты должны разрабатывать и внедрять современные подходы и инструменты для укрепления своей защиты от таких серьезных потенциальных потерь. По мнению К. Милфорд, исполнительного директора Центра обмена и анализа информации по исследовательским и образовательным сетям в Университете Индианы, университеты «втянуты в дорогостоящую гонку вооружений», поскольку они изучают новые способы как борьбы с текущими атаками, так и попыток быть на шаг впереди грядущих атак [цитат. по 5]. По словам К. Милфорда, независимо от того, были ли кибератаки успешными, они представляют собой дорогостоящую и постоянную проблему, которую университеты вынуждены решать.

Хотелось бы отдельно отметить, что проблема информационной безопасности для университетов многогранна и не сводится только к киберзащите IT – инфраструктуры, она охватывает вопросы безопасности информационно-образовательной среды как информационного пространства обучающегося, а также вопросы обучения студентов и профессорско-преподавательского состава основам информационной безопасности. Поэтому целью нашего исследования являлось оценить уровень знаний обучающихся и преподавателей вузов в области информационной безопасности и готовность применять свои знания для обеспечения безопасности.

Методы исследования

Для реализации поставленных целей исследования необходимо было разработать или обоснованно выбрать диагностический инструментарий (анкеты, опросники) для оценки уровня знаний о кибербезопасности. Нами был осуществлен анализ научно-исследовательской литературы, который позволил установить, что в работах российских авторов используется авторские опросники, оценка надежности и валидности которых исследователями не осуществлялась. В зарубежных исследованиях нами отмечены три методики оценки знаний о кибербезопасности, удовлетворяющие требованиям надежности и валидности получаемых результатов и доказывающих свою эффективность в исследованиях коллег из различных стран. Так, например, метод Ш.А. Крюгера и В.Д. Керни, разработанный в 2006, позволяет оценить уровень осведомленности об информационной

безопасности [6, 7]. Данный метод был апробирован в горнодобывающей компании в Южной Африке [7], политехническом университете Малазии [8] и при опросе жителей Бангладеша [9]. Структура опросника включает в себя вопросы, позволяющие оценить знания в области кибербезопасности и отношение к ней, а также предпринимаемые действия в организации информационной безопасности. Одним из преимуществ данного метода является многоуровневость оценок, что позволяет конкретизировать баллы разных категорий респондентов. Оценка надежности осуществлялась авторами методом α-Кронбаха (k относится к количеству вопросов по шкале Лайкерта):

$$\rho_T = \frac{k}{k-1}\left(1 - \frac{\sum_{i=1}^{k}\sigma_i^2}{\sigma_x^2}\right).$$

Полученные данные, α= 0,863, позволяют считать данную методику достоверной.

Второй метод, выделенный нами в научных исследованиях зарубежных авторов, основывается на оценке знаний терминологического аппарата в области информационной безопасности и тенденций его использования для решения практически значимых задач [10]. Данный метод строится на предположении о том, что незнание основных понятий информационной безопасности приводит к возрастающему риску стать жертвой киберпреступности. Недостатком данного метода, на наш взгляд, является отсутствие возможности оценки действий, предпринимаемых человеком, направленных на организацию собственной информационной безопасности и безопасности окружающих (коллег, друзей, родных).

Третий, широко используемый метод оценки уровня знаний в области информационной безопасности, основан на оценке культуры безопасности в организации, в целом. Предполагается получить в результате использования данного метода три группы данных: 1) данные об уровне организации информационной безопасности (политика компании или учреждения, наличие сравнительного анализа и анализа рисков); 2) данные об уровне управления и реализации стратегий информационной безопасности с учетом актуальных и современных угроз; 3) данные о знаниях информационной безопасности у каждого сотрудника компании или учреждения [11]. Детальное изучение данного метода позволило установить его неприменимость в условиях медицинского вуза, в связи с включением в состав вопросов глубоких знаний кибербезопасности и ее технических реализаций.

Таким образом, для оценки уровня знаний в области информационной безопасности нами использовался метод, позволяющий оценить знания, отношение и действия по защите от рисков киберугроз. Опросник включал в себя 4 группы вопросов:

1 группа позволяла собрать данные о поле, возрасте, уровни образования, частоту выхода в Интернет, оценить уровень цифровых навыков, а также выяснить какие виды устройств они регулярно используют для выхода в Интернет и с какой целью.

2 группа вопросов позволяла оценить знания респондентов о мерах, направленных на обеспечение собственной информационной безопасности;

3 группа вопросов направлена на оценку осознанности опасности киберугроз и какие действия необходимы обеспечения защиты от возможных угроз;

4 группа вопросов направлена на оценку знаний о видах киберугроз и выявления фактов киберпреступлений в отношении респондентов.

В исследовании участвовало более 3000 обучающихся и 893 преподавателя Астраханского государственного медицинского университета и Амурской государственной медицинской академии. Анкетирование осуществлялось посредством Google Forms, ссылка была направлена на все факультета вузов, участвующих в эксперименте. Для анализа результатов применялись методы описательной статистики.

Результаты

Применение указанной выше методики позволили получить, на наш взгляд, достаточно интересные результаты. Раскроем более подробно некоторые из них. Так,

например, первая группа вопросов позволила установить, что более 95% всех респондентов достаточно часто выходят в Интернет (более 2-3 раз в день), 2,1% респондентов – один или два раза в день, 2,7% -1-2 раза в неделю и лишь два человека не имели доступ к Интернету. Также выяснено, что участники опроса регулярно пользуются смартфонами (более 91%) и 9% пришлось на планшеты, ноутбуки и персональные компьютеры (рис.1).

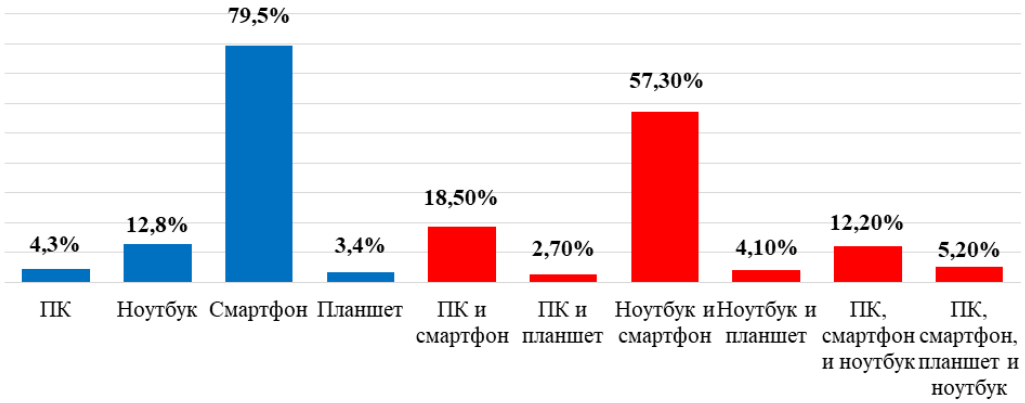

Рис.1. Устройства, используемые респондентами для выхода в Интернет

Кроме того, выявлены три группы респондентов, владеющие различным уровнем цифровых компетенций: к первой группе могут быть отнесены студенты и преподаватели с достаточно низким уровнем владения цифровыми компетенциями - посещающие только определенные веб-страницы и страницы социальных сетей (41,7%); второй и несколько приложений, таких как Microsoft Word; вторая группа участников обладает средним уровнем владения цифровых компетенций - могут загружать приложения, управлять настройками устройств и обладают знаниями как об аппаратном, так и о программном обеспечении(58,3%).

Вторая группа вопросов позволила определить какими из широко известных мер информационной безопасности, таких как антивирус, брандмауэр, аутентификация, и резервное копирование (рис.2).

Рис.2 . Наиболее часто используемые средства безопасности и приложения для устройств

Третья группа вопросов используемого нами диагностического материал позволила выяснить, осознают ли опасность киберугроз студенты и сотрудники и какие действия они предпринимают для обеспечения защиты от возможных угроз. Вопросы касались надежности посещаемых веб-сайтов, использования логинов и паролей и настройки конфиденциальности социальных сетей. Обобщение результатов представлено в таблице 1.

Таблица 1. Результаты опроса в области осознания опасность киберугроз предпринимаемых действий для обеспечения защиты от возможных угроз

Утверждения	Всегда	Часто	Иногда	Редко	Никогда
Я проверяю надежность веб-сайта, прежде чем получить доступ к нему	24,5%	46,9%	10,3%	10,1%	8,2%
Я создаю пароль, содержащий мою личную информацию (например, фамилию, дату рождения)	15,9%	18,4%	28,0%	15,5%	22,2%
Я осознаю опасность при нажатии на баннеры, рекламу или всплывающие экраны, которые появляются на экране при выходе в Интернет	30,2%	43,1%	14,0%	9,2%	3,5%
Я серьезно отношусь к настройкам конфиденциальности в моих аккаунтах в социальных сетях	8,9%	14,9%	37,3%	28,6%	10,3%
Я часто меняю пароли личных кабинетов онлайн-банкинга	5,8%	9,6%	38,2%	39,1%	7,3%
Я внимательно читаю условия соглашения, предлагаемые сайтами, прежде чем принимать решения	13,8%	17,7%	20,1%	44,3%	4,1%
Я думаю, что мои цифровые устройства (компьютер, смартфоны) не интересны хакерам	31,2%	19,0%	26,5%	10,4%	12,9%
Я внимательно отношусь к клику на ссылки в сообщении электронной почты или в социальных сетях	17,4%	38,9%	24,6%	16,0%	3,1%

Четвертая группа вопросов позволила оценить насколько участники исследования осведомлены о киберприступности и встречались ли они с ее проявлениями в отношении себя. Так, большинство преподавателей университета сформулировали определение понятия «киберпреступность» близкое к общепринятому, а именно под киберпреступностью они понимают «преступления в отношении физических лиц или организаций, осуществляемых с использованием электронных средств и методов, таких как электронные письма и текстовые сообщения [12, 13].

На рисунке 3 представлены результаты, позволяющие делать выводы о том, что % респондентов были потерпевшими со стороны вымогателей и/или хакеров (1 – «Я получал фишинговые электронные письма», 2 – «Да, у меня крали личные данные аккаунта в социальных сетях», 3 - «Мои электронные устройства подвергались вредоносными программами», 4 – «Мои аккаунты подвергались вредоносным программам вследствие чего я не мог получить доступ к онлайн-услугам», 5 – «Я сталкивался с онлайн-вымогательством».

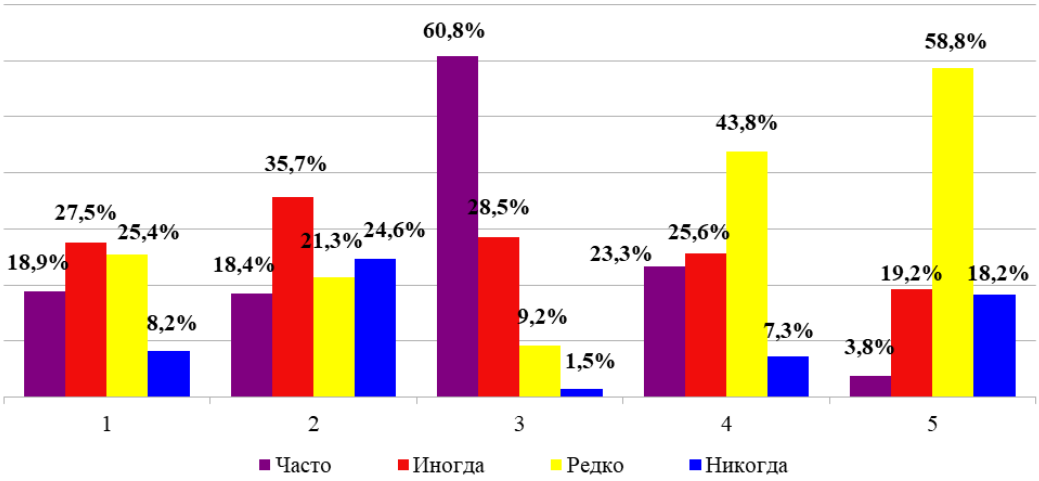

Рис. 3. Данные по потерпевшим со стороны вымогателей и/или хакеров

Таким образом обобщение полученных результатов позволило нам сформулировать ряд выводов. Во-первых, не смотря на различный уровень образования респондентов, пол и возраст, большинство из них обладают средним уровнем знаний в области информационной безопасности. Понимая значимость соблюдения мер информационной безопасности, зачастую не связывают, например, формирование логина и пароля для аккаунта с кражей личных данных и получением несанкционированного доступа сторонними лицами, злоумышленниками. Кроме того, более 63% используют личную информацию для создания логинов и паролей, а более 56% никогда или редко их меняли. Такие аккаунты, как правило, подвержены более высокому риску со стороны злоумышленников, использующих социальную инженерию или другие методы атаки.

Во-вторых, установлено, что более половины респондентов не имеют представления о фишинговых и ddos атаках (68,5%), краже личных данных (38,9%), заражении устройств (25,8%). Отдельно хотелось бы отметить, что 28,3% участников опроса являлись жертвами киберпреступлений, только 2,7% сообщили в ответственные органы, остальные не предприняли никаких действий.

Выводы

Полученные в результате нашего исследования выводы подтвердили необходимость в разработке образовательных программ, направленных на формирование знаний и навыков кибербезопасности. Несмотря на многообразие имеющихся образовательных курсов в данной предметной области, считаем важным обоснованно определить не только содержание учебного материала с учетом особенностей восприятия обучающихся различных возрастных групп и имеющегося образования, но и обоснованно выбрать теоретическую основу методики обучения основам информационной безопасности. В связи с тем, что массовые он-лайн курсы приобретают все большую популярность, предполагаем целесообразным применить известные и доказывающие при их реализации теоретические основы дистанционного обучения студентов технических и медицинских вузов, сформулированные в работах О.В. Иванчук, Е.В. Плащевая [13, 14], И.О. Цурикова [15], О.Г. Ганина [16].

Кроме того, считаем перспективным рассмотреть, используя методы математической статистики (корреляционный, многофакторный анализ), зависимость уровня знаний в области информационной безопасности и готовность к их применению от пола, возраста, национальной принадлежности. Полагаем, что полученные в результате такого анализа данные позволят разработать эффективные методы обучения основам информационной безопасности.

Список источников:

1. Das R. Cyber Security for Social Networking Sites: Issues Challenges and Solutions // International Journal for Research in Applied Science and Engineering Technolog. 2017. Vol.V(IV). P.833–838. DOI: https://doi.org/10.22214/IJRASET.2017.4153

2. Euphemia N., Odii J., Njoku D. Cyberspace Activities Awareness and Security Strategies in Tertiary Institutions in Nigeria // IRE Journals. 2019. Vol.3. P.439-445.

3. Norris D.F., Mateczun L.K., Forno R.F. Cybersecurity and Local Government. Great Britain: Wiley. 256p. ISBN: 978-1-119-78828-7

4. Никеров Д.М., Хохлова О.М. Преступления в сфере высоких технологий в современной России // Вестник восточно-сибирского института министерства внутренних дел России. 2019. № 2(89). С.82-93. DOI: https://doi.org/10.24411/2312-3184-2019-00008

5. Garba A., Siraj M., Alhaji M. A Study on Cybersecurity Awareness Among Students in Yobe: A Quantitative Approach // International Journal on Emerging Technologies. 2020. Vol. 11. P. 41-49.

6. Kruger H.A., Drevin L., Steyn T. A Vocabulary Test to Assess Information Security Awareness // Inf. Manag. Comput. Secur. 2020. Vol. 18 (5). P. 316-327. DOI: https://doi.org/10.1108/09685221011095236

7. Md. Kassim S.S., Saleh M., Zainal A. General Feelings: General User Experience and Understanding of Security in the Malaysian Polytechnic // Pattern Analysis, Smart Security and the Internet of Things. 2015. Vol. 355. P131-140. DOI: https://doi.org/10.1007/978-3-319-17398-6_12

8. Garba A., Maheyzah D.S. Cyber Security Awareness Among University Students: A Case Study // Science Proceedings Series. 2020. Vol. 2. P.82-86. DOI: https://doi.org/10.31580/sps.v2i1.1320

9. Veiga A., Martins N. Improving the information security culture through monitoring and implementation actions illustrated through a case study // Computers & Security. 2015. Vol. 49. P.49 DOI: https://doi.org/10.1016/j.cose.2014.12.006

10. Mtetwa N.S., Tarwireyi P., Sibeko C.N. Blockchain-Based Security Model for LoRaWAN Firmware Updates // Journal of Sensor and Actuator Networks. 2022. Vol.11(1). P.5. DOI: https://doi.org/10.3390/jsan11010005

11. Halder D., Jaishankar K. Cybercrime and Victimization of Women: Laws, Rights and Rules: Laws, Rights and Rules. - Igi Global, 2011. 281p. DOI: https://doi.org/10.4018/978-1-60960-830-9

12. Дерюгин Р.А. Киберпреступность в России: современное состояние и Актуальные проблемы // Вестник Уральского юридического института МВД России. 2019. № 2. С.46-49. DOI: https://doi.org/10.22394/2686-7834-2022-1-83-88

13. Плащевая Е.В., Иванчук О.В. Дистанционное обучение физике студентов медицинских вузов // Мир науки. Педагогика и психология. 2020. Т. 8, № 6. С.8 EDN: VWDRAI URL: https://www.elibrary.ru/item.asp?id=44901666

14. Плащевая Е.В., Иванчук О.В. Дистанционное медицинское образование в период пандемии COVID-19: оценка опыта // ЦИТИСЭ. 2021. № 2(28). С. 490-499. DOI: https://doi.org/10.15350/2409-7616.2021.2.45

15. Мирзабекова О.В., Цурикова И.О. Реализация принципа профессиональной направленности при дистанционном обучении физике будущих инженеров // Человек и образование. 2015. № 4(45). С. 92-95. EDN: VVYLTN URL: https://www.elibrary.ru/item.asp?id=25953516

16. Ганина О.Г., Плащевая Е.В., Иванчук О.В. Ситуационный подход: дидактические средства обучения физике студентов медицинских вузов // ЦИТИСЭ. 2020. № 2(24). С. 27-37. DOI: https://doi.org/10.15350/2409-7616.2020.2.03

References:

1. Das R. Cyber Security for Social Networking Sites: Issues. *Challenges and Solutions. International Journal for Research in Applied Science and Engineering Technology*, 2017, vol. V(IV), pp.833–838. DOI: https://doi.org/10.22214/IJRASET.2017.4153

2. Euphemia N., Odii J., Njoku D. Cyberspace Activities Awareness and Security Strategies in Tertiary Institutions in Nigeria. *IRE Journals,* 2019, vol. 3. pp. 439-445.

3. Norris D.F., Mateczun L.K., Forno R.F. *Cybersecurity and Local Government.* Great Britain: Wiley. 256p. ISBN: 978-1-119-78828-7

4. Nikerov D.M., Khokhlova O.M. Crimes in the sphere of high technologies in modern Russia. *Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia*, 2019, no. 2(89), pp.82-93. (In Russian) DOI: https://doi.org/10.24411/2312-3184-2019-00008

5. Garba A., Siraj M., Alhaji M. A Study on Cybersecurity Awareness Among Students in Yobe: A Quantitative Approach. *International Journal on Emerging Technologies*, 2020, vol. 11, pp. 41-49.

6. Kruger H.A., Drevin L., Steyn T. A Vocabulary Test to Assess Information Security Awareness. *Inf. Manag. Comput. Secur*, 2020, vol. 18, pp.316-327. DOI: https://doi.org/10.1108/09685221011095236

7. Md. Kassim S.S., Saleh M., Zainal A. General Feelings: General User Experience and Understanding of Security in the Malaysian Polytechnic. *Pattern Analysis, Smart Security and the Internet of Things*, 2015, vol. 355, pp131-140p. DOI: https://doi.org/10.1007/978-3-319-17398-6_12

8. Garba A., Maheyzah D.S. Cyber Security Awareness Among University Students: A Case Study. *Science Proceedings Series.* 2020, vol. 2, pp. 82-86. DOI: https://doi.org/10.31580/sps.v2i1.1320

9. Veiga A., Martins N. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 2015, vol. 49, pp. 49. DOI: https://doi.org/10.1016/j.cose.2014.12.006

10. Mtetwa N.S., Tarwireyi P., Sibeko C.N. Blockchain-Based Security Model for LoRaWAN Firmware Updates. *Journal of Sensor and Actuator Networks*, 2022, vol. 11(1), pp.5. DOI: https://doi.org/10.3390/jsan11010005

11. Halder D., Jaishankar K. *Cybercrime and Victimization of Women: Laws, Rights and Rules:* Laws, Rights and Rules. - Igi Global, 2011. 281p. DOI: https://doi.org/10.4018/978-1-60960-830-9

12. Deryugin R. A. Cybercrime in Russia: current state and current problems. *Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia.* 2019, no. 2, pp. 46-49. (In Russian) DOI: https://doi.org/10.22394/2686-7834-2022-1-83-88

13. Plashchevaya E.V., Ivanchuk O.V. Distance learning in physics of students of medical universities. *The world of science. Pedagogy and psychology*, 2020. vol. 8, no 6, pp.8 (In Russian) EDN: VWDRAI URL: https://www.elibrary.ru/item.asp?id=44901666

14. Plashchevaya E.V., Ivanchuk O.V. Distance medical education during the COVID-19 pandemic: assessment of experience. *CITISE*, 2021, no. 2(28), pp. 490-499. (In Russian) DOI: https://doi.org/10.15350/2409-7616.2021.2.45

15. Mirzabekova O.V., Tsurikova I.O. Implementation of the principle of professional orientation in distance learning in physics of future engineers. *Man and education*, 2015, no. 4(45), pp. 92-95. (In Russian) EDN: VVYLTN URL: https://www.elibrary.ru/item.asp?id=25953516

16. Ganina O.G., Plashchevaya E.V., Ivanchuk O.V. Situational approach: didactic means of teaching physics to students of medical universities. *CITISE*, 2020, no 2(24), pp. 27-37. (In Russian) DOI: https://doi.org/10.15350/2409-7616.2020.2.03

Submitted: 23 July 2022 Accepted: 24 August 2022 Published: 25 August 2022