ФИНАНСЫ / FINANCE

DOI: https://doi.org/10.60797/IRJ.2025.151.70

ЛИЧНАЯ КИБЕРБЕЗОПАСНОСТЬ СТУДЕНТОВ: ЭМПИРИЧЕСКОЕ ИССЛЕДОВАНИЕ ПОЛЬЗОВАТЕЛЕЙ ЦИФРОВЫХ УСТРОЙСТВ И ИНТЕРНЕТА

Научная статья

Давыденко И.Г.[1], Мисиров Д.Н.[2,] *, Акопян М.А.[3]
[1] ORCID : 0000-0003-0542-3136;
[2] ORCID : 0000-0002-2652-7228;
[3] ORCID : 0000-0002-5219-6012;
[1, 2, 3] Южный федеральный университет, Ростов-на-Дону, Российская Федерация

* Корреспондирующий автор (dmisirov[at]yandex.ru)

Аннотация

В современных условиях нарастания числа пользователей цифровых устройств и Интернета генерируются риски увеличения количества киберинцидентов, поскольку некоторые действия считаются опасными при доступе в Интернет. В указанной связи необходимы устойчивые навыки и поведенческие практики безопасной деятельности в киберсреде, позволяющие предотвращать и противостоять киберугрозам. Интенсивность использования Интернета и мультиаспектность интернет-активности студентов актуализируют проблему факторов-угроз и конфиденциальности данных в контексте достижения персональной кибербезопасности.

Целью эмпирического исследования является изучение уровня осведомленности о риск-факторах в студенческой среде, связанных с использованием Интернета с позиций обеспечения личной кибербезопасности обучающихся Академии психологии и педагогики Южного федерального университета г. Ростова-на-Дону.

Для достижения цели принята количественная методология опроса с применением 5-балльной шкалы Лайкерта. Вопросы анкеты касались легитимности веб-сайтов, использования паролей и настроек конфиденциальности персональных данных в социальных сетях. Опираясь на результаты социологического опроса студентов (N = 107, 18-22 года), установлено, что у опрошенных студентов сформированы достаточно устойчивые адаптивные поведенческие паттерны, способные оказывать противодействующий эффект факторам-угрозам личной кибербезопасности, характерных для пользователей Интернета и цифровых устройств.

Ключевые слова: личная кибербезопасность, профиль персональной кибербезопасности, киберпреступность, конфиденциальность данных, цифровая грамотность, шкала Лайкерта, цифровые «аборигены», цифровые «иммигранты».

STUDENTS' PERSONAL CYBERSECURITY: AN EMPIRICAL STUDY OF DIGITAL DEVICE AND INTERNET USERS

Research article

Davidenko I.G.[1], Misirov D.N.[2,] *, Akopyan M.A.[3]
[1] ORCID : 0000-0003-0542-3136;
[2] ORCID : 0000-0002-2652-7228;
[3] ORCID : 0000-0002-5219-6012;
[1, 2, 3] Southern Federal University, Rostov-on-Don, Russian Federation

* Corresponding author (dmisirov[at]yandex.ru)

Abstract

In today's environment of increasing numbers of users of digital devices and the Internet, risks of cyber incidents are generated, as certain activities are seen as dangerous when accessing the Internet. In this regard, sustainable skills and behavioural practices for safe cyber activities are needed to prevent and counter cyber threats. The intensity of Internet use and the multidimensional nature of students' online activities make the issue of threat factors and data privacy relevant in the context of achieving personal cybersecurity.

The aim of the empirical study is to examine the level of awareness of risk factors in the student environment related to the use of the Internet from the perspective of ensuring personal cybersecurity of students of the Academy of Psychology and Pedagogy of the Southern Federal University of Rostov-on-Don.

To achieve the objective, a quantitative survey methodology using a 5-point Likert scale was employed. The survey questions were related to the legitimacy of websites, the use of passwords and personal data privacy settings in social networks. Based on the results of a sociological survey of students (N = 107, 18–22 years old), it was found that the surveyed students have formed sufficiently stable adaptive behavioural patterns capable of counteracting threats to personal cybersecurity that are typical of Internet and digital device users.

Keywords: personal cybersecurity, personal cybersecurity profile, cybercrime, data privacy, digital literacy, Likert scale, digital ‘natives’, digital ‘immigrants’.

Введение

Современные исследователи констатируют тот факт, что Интернет существенно расширился и превратился в социальное пространство. Если 15–20 лет назад онлайн- и офлайн-жизнь представлялись более различимыми, то в

настоящее время наблюдается смешение онлайн- и офлайн-опыта, совместно составляющих повседневную реальность, что делает общество сетевым, информационным. Быстрый рост и растущая популярность Интернета создали беспрецедентные возможности и перспективы для правонарушений, которые можно совершать анонимно и дистанционно, что представляет серьезную проблему для правоохранительных органов. В частности, по данным МВД РФ, «в текущем году доля киберпреступлений в России возросла до 40%; еще пять лет назад доля таких посягательств в России составляла менее 15%» [1]. С начала 2024 г. общая сумма ущерба превысила 116 млрд. руб. Кроме того, по заявлениям Генеральной прокуратуры РФ, «на протяжении последних лет раскрываемость в сфере киберпреступлений остается стабильно низкой и не превышает 27%» [2].

Исследования поведенческих практик различных возрастных групп населения, являющихся активными пользователями цифровых устройств и Интернета, приобретает все большую актуальность, в связи с необходимостью противостояния киберпреступлениям и обеспечения личной кибербезопасности. В ежегодном отчете Eurobarometer 2017 года сделан вывод о том, что возрастная группа в возрасте 15–24 лет с большей частотой, чем лица старше 55 лет, сообщала о том, что сталкивалась с различными типами киберпреступлений – онлайн-мошенничество, взлом аккаунтов, обнаружение вредоносного программного обеспечения на своих устройствах. Такой результат во многом отражает более высокий уровень использования Интернета молодой возрастной группой, а также возросшую компьютерную грамотность, что позволяет им с большей вероятностью распознавать, когда они подвергаются личной киберопасности.

В указанной связи необходимо проведение систематического мониторинга, позволяющего оценить осведомленность обучающихся вузовской среды о факторах-угрозах и определить поведенческие паттерны в киберсреде, которые способны повысить или лимитировать личную кибербезопасность студентов.

При проведении социологического исследования авторы исходили из того, информанты – студенты высшего учебного заведения имеют достаточный уровень подготовки (образования), поэтому обладают достаточным уровнем осведомленности о риск-факторах персональной кибербезопасности и способны противостоять киберпреступлениям.

Методы и принципы исследования

Методология проведенного исследования базируется на методах социологического анализа, которые конкретизируются в следующем: разработанный авторами опросник для проведения заочного, опосредованного онлайн-опроса представляет собой метод фиксации в процессе сбора первичной информации, позволивший установить уровень осведомленности информантов о факторах-угрозах личной кибербезопасности и конфиденциальности личных данных студентов Академии психологии и педагогики Южного федерального университета г. Ростова-на-Дону в определенный момент времени.

Для опроса респондентов при помощи анкетирования и обобщения фактологических данных использовалась шкала Лайкерта, позволяющая оценить опыт пользователей цифровых устройств и продуктов, веб-сайтов и т.д.

Для последующей аналитической обработки данных использовались методы описательной статистики – средних значений, стандартных отклонений и вариации.

При проведении опроса авторы следовали методологическим принципам социологического исследования: эмпиризма и учета множества факторов, детерминирующих социальное явление или процесс.

Основные результаты

Учитывая относительно новый интерес к феномену личной кибербезопасности студентов, при проведении обзора научной литературы авторы стремились обеспечить полноту поиска информации в высококлассных журналах и материалах конференций по различным дисциплинарным областям, таким как социология, психология и компьютерные науки. Научно-практический обзор по проблеме минимизации рисков студентов высших учебных заведений и повышения уровня их личной кибербезопасности посредством повышения уровня осведомленности о факторах-угрозах со стороны киберпреступности приводит к выводу о том, что эмпирические исследования носят разрозненный и разноаспектный характер.

В работе «Конфиденциальность данных: от прозрачности к справедливости» Чао Ву определяет роль в экосистеме данных амбивалентно: владелец данных и пользователь данных. Владельцем данных может быть физическое лицо (или любая организация), данные которой генерируются и считываются. Пользователь данных – это организация, которая использует данные владельца для различных целей, таких как обработка, моделирование, агрегирование и продажа данных. Согласно этому определению, к пользователям данных относятся обработчик данных и брокер данных.

Конфиденциальность данных дает человеку права на свои данные. И далее автор статьи логически связывает конфиденциальность данных с понятием «экономика данных» как взаимосвязанного и взаимозависимого набора технологий, компаний, маркетологов и миллиардов индивидов. Будучи ценным активом, который можно монетизировать в экономике данных, данные будут занимать все большую долю доходов, создаваемых всем обществом. Поэтому, когда экономика поглотит значительную часть экономической системы, то, как справедливо распределить ее доходы, станет центральным вопросом общественного благосостояния [3].

Всесторонний обзор публикаций по проблеме конфиденциальности данных показал, что она является многовариабельной и исследовательский комплементарный интерес вызывает работа М. Вималкумар, Суджит Кумар Шарма, Джанг Бахадур Сингх, актуализирующая проблему голосовых цифровых помощников. Известно, что, несмотря на свои преимущества, цифровые помощники на основе искусственного интеллекта породили новые проблемы конфиденциальности и личной кибербезопасности. Так, цифровые помощники собирают конфиденциальные личные данные, связанные с историей местоположений пользователей и их покупок, контактами, голосовыми запросами. Как указывают авторы цитируемой научной работы, 41% опрошенных выразили недоверие

цифровым помощникам и считают, что они ставят под угрозу конфиденциальность посредством пассивного прослушивания; около 52% выразили обеспокоенность тем, что их личная информация не защищена [4].

Исследование, проведенное Эриком Рутгером Лейкфельдтом, Томасом Дж. Холтом ставит вопрос, какие факторы провоцируют киберпреступность с точки зрения «специализированного» или «универсального» преступника, который вовлечен в сети онлайн-преступников для участия в фишинге, вредоносном программном обеспечении и других экономических преступлениях. В то же время появление рынков, на которых продаются вредоносные программы, конфиденциальные данные и инструменты для взлома, значительно облегчили участие в различных формах кибератак и кибермошенничества [5].

В работе Дж. Логгена, А. Монева, Р. Лейкфельдта убедительно показано, что финансовая киберпреступность в настоящее время считается серьезной социальной угрозой, которая подрывает национальные финансовые системы, препятствует экономическому росту и приносит убытки предприятиям и частным лицам. Авторы исследования обобщили существующие знания о путях финансовой киберпреступности и противодействия ей, описали эти процессы и составили карту факторов риска, связанных с финансовой киберпреступностью. Ввиду разнородности литературы по данной проблеме авторы использовали нарративный подход для синтеза актуальных знаний в рассматриваемой проблемной области [6].

В настоящее время является актиоматичным утверждение о том, что всеобъемлющим средством получения, распространения и передачи информации признается интернет, определяющий возрастание числа пользователей цифровых устройств, которые упрощают повседневную жизнь.

В контексте проводимого исследования стоит отметить, что в последние годы образование претерпело значительные изменения в связи с появлением информационно-коммуникационных технологий. Использование современных образовательных технологий, таких как онлайн, гибридное обучение, демонстрируют тенденцию к росту. Примечательно, что в условиях COVID-19 в сфере образования произошел переход от традиционного, очного обучения к дистанционному онлайн-обучению, которое исторически считалось дополнительной модальностью образования.

В научно-практических работах российских исследователей затрагиваются вопросы, рассматривающие преимущественно проблемы методики преподавания дисциплин в содержании которых имеют место модули (разделы) цифровой грамотности обучающихся и личной кибербезопасности. Проблемы необходимости повышения уровня компьютерной и цифровой грамотности различных возрастных групп населения рассмотрены в работе Берман Н.Д., где автор демонстрирует оригинальный подход к структурированию цифровой грамотности, выделению ее наиболее значимых и существенных составляющих [7].

В работе Зуева А.В. и др. предложена авторская методика, основанная на активных формах преподавания основ обеспечения кибербезопасности в рамках факультативных занятий [8]. В научной статье Итинсон К.С., Чирковой В.М. авторы используют более широкий подход к изучению рассматриваемой проблемы: каким образом обеспечить кибербезопасность в общеобразовательных учреждениях, какие использовать правила и стратегии персональной безопасности в Интернете [9].

Смена образовательных форматов генерирует риски персональной кибербезопасности студентов в процессе использования ими цифровых устройств и Интернета, в том числе, в процессе обучения.

Настоящее исследование является логичным продолжением ранее опубликованной работы, в которой отмечалось, что «высокий университетский ценз определяет необходимость формирования и последующего количественного измерения процедурных знаний, позволяющих, в частности, минимизировать и предотвратить финансовые риски фишинга. Для этого целесообразно провести исследование, направленное на оценку уровня личной кибербезопасности студентов на основе таких параметров как учёт информантами легитимности веб-сайтов, смена паролей персональных учётных данных, внимание к настойкам конфиденциальности учётных записей в социальных сетях и др.» [10, С. 212].

В указанной связи, целью проведения опроса выступает определение уровня личной кибербезопасности с последующим построением профиля персональной кибербезопасности студента как совокупного образа обучающегося университета, включающего поведенческие паттерны и их характеристики.

Научно-практическая проблематика исследования состоит в том, что в современных условиях цифровой трансформации высшего образования, увеличения числа киберпреступлений в виртуальной среде возникает проблема обеспечения и повышения уровня личной кибербезопасности студентов посредством их осведомленности о доминирующих факторах-угрозах и формирования адаптивных поведенческих практик при использовании Интернета.

Гипотеза исследования исходит из того, что информанты – студенты высшего учебного заведения имеют достаточный уровень подготовки (образования), поэтому обладают достаточным уровнем осведомленности о риск-факторах персональной кибербезопасности и способны противостоять киберпреступлениям, то есть существует прямая функциональная зависимость между уровнем образования и осведомленностью о факторах-угрозах при доступе в Интернет.

Для достижения цели исследования в сентябре 2024 г. посредством онлайн-приложения Google Forms были опрошены студенты Академии психологии и педагогики Южного федерального университета (далее: АПП ЮФУ) г. Ростова-на-Дону в количестве 107 человек; в опросе приняли участие обучающиеся 1 – 4 курсов бакалавриата направления подготовки 44.03.04 «Профессиональное обучение (по отраслям)»; возраст респондентов 18 – 22 года. В начале опроса авторами были соблюдены этические принципы проведения опросов в студенческой среде: указаны цели опроса и обязательность конфиденциальности и анонимности.

Выбранная в качестве научно-исследовательского инструментария «классическая» шкала Лайкерта позволяет оценить чувства, самоощущение опрошенных студентов Академии психологии и педагогики ЮФУ по отношению к проблеме личной кибербезопасности. Позиции, используемой в настоящем исследовании, шкалы Лайкерта

кодированы числами от «1» до «5» с наличием «якорных» и нейтральной позиций; шкала ответов на опросник является типичной и позволила оценить частоту, иначе говоря, как часто респонденты демонстрируют определенные поведенческие установки и практики для обеспечения персональной кибербезопасности.

Для проведения анализа цифрового поведения студентов и выявления типовых характеристик авторы сочли целесообразным структурировать опросник по личной кибербезопасности обучающихся следующим образом:

- вопросы, оценивающие уровень осведомленности о факторах-угрозах: 1 по 8 вопросы;
- вопросы, оценивающие уровень конфиденциальности личных данных: 9 и10 вопросы.

Таблица 1 - Результаты опроса по личной кибербезопасности и распределение ответов респондентов по 5-балльной шкале Лайкерта

DOI: https://doi.org/10.60797/IRJ.2025.151.70.1

№	Вопросы по осведомленности о факторах-угрозах и конфиденциальности личных данных	Всегда	Часто	Иногда	Редко	Никогда	Агрегированная оценка в численном виде
		5 баллов	4 балла	3 балла	2 балла	1 балл	
1.	Я регулярно устанавливаю обновления программного обеспечения	32	29	27	15	4	3,79
2.	Я часто меняю пароли учетных записей (например, онлайн-банкинга)	15	23	21	29	19	2,87
3.	Социальные сети защищают мою личную информацию	28	35	32	9	3	3,7

№	Вопросы по осведомленности о факторах-угрозах и конфиденциальности личных данных	Всегда	Часто	Иногда	Редко	Никогда	Агрегированная оценка в численном виде
		5 баллов	4 балла	3 балла	2 балла	1 балл	
4.	Я проверяю легитимность веб-сайта перед тем, как зайти на него	35	30	18	10	14	3,58
5.	Я осознаю опасность при нажатии на баннеры, рекламу или всплывающие окна, которые появляются при работе в Интернете	66	22	10	3	6	4,3
6.	Я осторожен, нажимая на ссылки в сообщениях электронной почты или социальных сетях	64	26	9	2	6	4,3

№	Вопросы по осведомленности о факторах-угрозах и конфиденциальности личных данных	Всегда	Часто	Иногда	Редко	Никогда	Агрегированная оценка в численном виде
		5 баллов	4 балла	3 балла	2 балла	1 балл	
7.	Я чувствую себя в безопасности при использовании общедоступного Wi-Fi	16	26	22	24	19	2,96
8.	Я чувствую, что мои цифровые устройства (компьютер, смартфоны) не представляют ценности для хакеров, они не нацелены на меня	26	25	32	21	3	3,47
9.	Я создаю пароль, который содержит мою личную информацию (например, фамилию, дату рождения)	8	13	21	22	43	2,26
10.	Я уделяю должное внимание настройкам конфиденциальности в своих	60	32	12	2	1	4,37

№	Вопросы по осведомленности о факторах-угрозах и конфиденциальности личных данных	Всегда	Часто	Иногда	Редко	Никогда	Агрегированная оценка в численном виде
		5 баллов	4 балла	3 балла	2 балла	1 балл	
	учетных записях в социальных сетях						
В среднем		175	104,4	61,2	28,9	11,8	-
Стандартное отклонение		106,1	24,4	25	20,6	12,8	-
Коэффициент вариации		0,61	0,23	0,41	0,71	1,08	-

Полученные эмпирические данные шкалы Лайкерта авторы рассматривают как интервальные, т.е. для описания и интерпретации полученных количественных результатов использовались средние значения, стандартные отклонения и коэффициенты вариации (таблица 1).

Как указано ранее, «классическая» шкала Лайкерта включает 5 пунктов, однако наличие центральной точки на 5-балльной шкале несколько усложнило перевод агрегированной оценки в числовом виде в средний «словесный» результат. Эмпирические результаты показали заниженные данные по полярным утвердительным ответам: «да» как сумма ответов «всегда» и «часто» – 73%; «нет» как сумма ответов «редко» и «никогда» – 10,7%. Таким образом, наблюдается склонность к выбору положительных ответов выше, чем склонность к выбору отрицательных. Данный вывод подтверждается расчетами средних значений и стандартных отклонений: вариант ответов «всегда» имеет самое высокое среднее значение и стандартное отклонение 175 и 106,1 соответственно. Это указывает на то, что у опрошенных студентов сформированы достаточно устойчивые адаптивные поведенческие паттерны, способные оказывать противодействующий эффект факторам-угрозам личной кибербезопасности.

В ходе эмпирического исследования наши результаты показали, что коэффициент вариации как наиболее информативный и универсальный статистический показатель имеет наименьшее значение (0,23) в таком варианте ответа как «часто», что указывает на высокую степень согласованности и стабильности мнения респондентов по различным вопросам личной кибербезопасности. И наоборот, мнения студентов сильно разбросаны по отношению к среднему значению в таких вариантах ответов по шкале Лайкерта как «редко» и «никогда» – 0,71 и 1,08 соответственно.

В указанной связи, для получения валидных результатов проводимого исследования, следует дифференцировать смысловые значения таких вариантов ответов в используемой шкале как «иногда» и «редко». Авторы определяют ответ «иногда» как нейтрально-уклончивый, амбивалентный: «ни согласен, ни не согласен»; ответы респондентов «редко» тяготеют к «скорее не делаю что-то, чем делаю». Так, при ответе на вопрос «Я часто меняю пароли учетных записей» 29 респондентов ответили «редко», т.е., если и происходит смена паролей важных учетных записей, то нерегулярно, бессистемно и от случая к случаю, при этом, средний «словесный» результат (2,87) приближен к позиции «иногда».

5-балльная шкала Лайкерта с центральной точкой «иногда» на шкале оценки смещает положительные и отрицательные ответы опрошенных к нейтральной позиции. Об этом свидетельствует полученный средний «словесный» результат по такому вопросу опросника как «Я чувствую себя в безопасности при использовании общедоступного Wi-Fi» (2,96).

В результате проведенного опроса получены ценные инсайты о пользовательском опыте и поведенческих паттернах. Студенты АПП ЮФУ на достаточном уровне осведомлены о факторах-угрозах личной кибербезопасности и конфиденциальности персональных данных.

Обсуждение

Несмотря на то, что проведенное исследование дает интересные эмпирические результаты в области описания поведенческих паттернов студентов АПП ЮФУ при работе в Интернете и с цифровыми устройствами, у него есть некоторые ограничения. Так, в шкале Лайкерта наглядно проявляется дилемма между простотой измерительных процедур и математической строгостью. «В литературе встречаются и аргументируются различные точки зрения на возможности использования шкалы Лайкерта. Эта шкала, как показал еще ее автор, является порядковой (не метрической) шкалой, однако многие исследователи считают возможным использовать ее как интервальную шкалу и применять процедуры для обработки данных, приемлемые для метрических шкал, так как, по их мнению, это не приводит к серьезным ошибкам в результатах» [11, С. 25-26].

Исходя из проблематики настоящей работы, отметим, что множество современных исследований направлено на мониторинг использования цифровых устройств и Интернета; настоящая статья фокусируется на студентах неэкономических и не IT-направлений подготовки, которые выросли в информационно-технологическую эпоху и являются «цифровыми аборигенами» [12]. Цифровой разрыв между цифровыми аборигенами (людьми, родившимися в окружении цифровых технологий) и цифровыми иммигрантами (людьми, родившимися до 1964 года в докомпьютерном мире) подчеркивает разницу между осведомленностью и знакомством с Интернетом каждого поколения [13]. Поскольку многочисленные услуги (например, коммунальные платежи, онлайн-банкинг) перемещаются в онлайн, некоторым цифровым иммигрантам сложно адаптироваться к постоянно меняющимся технологиям, особенно людям с ограниченными навыками, знаниями и опытом. Поэтому, по мнению авторов, необходимы и целесообразны дальнейшие исследования для сотрудников ЮФУ старшего возраста («цифровых иммигрантов») с последующим сравнением результатов и выявлением сходства или различий в поведенческих установках и практиках в области личной кибербезопасности, что обогатит теоретико-поведенческий каркас в области информационной безопасности.

Заключение

Поставленная цель проведения опроса студентов Академии психологии и педагогики Южного федерального университета г. Ростова-на-Дону достигнута. На основе полученных эмпирических результатов проведенного социологического исследования с использованием классической шкалы Лайкерта с 5-ю позициями, авторами дана количественная оценка уровня осведомленности информантов о факторах-угрозах личной кибербезопасности и уровне защиты конфиденциальности персональных данных.

Результатом использования интервальной шкалы Лайкерта в качестве метода исследования стало обоснование наличия адаптивных поведенческих паттернов: респонденты осознают опасность при работе в Интернете и проявляют разумную осторожность в социальных сетях и при использовании электронной почты. Поскольку вопросы

конфиденциальности учетных записей вышли на новый глобально-проблемный уровень, пересекающиеся с экономикой данных, то важно подчеркнуть, что студенты АПП ЮФУ г. Ростова-на-Дону уделяют достаточное внимание защите личной информации, включая финансовую (онлайн-банкинг).

Однако общий уровень личной кибербезопасности обучающихся снижают такие факторы, как чрезмерная уверенность в том, что социальные сети способны обеспечить защиту личной информации (агрегированный результат 3,7 приближен к позиции «часто»), а также склонность студентов недооценивать риски хакерских действий, выражающаяся в том, что, по их мнению, «цифровые устройства не представляют ценности для хакеров» (агрегированная оценка 3,47).

Практическая значимость исследования состоит в том, что контекстуализирована и подтверждена авторская гипотеза о существовании прямой детерминированной зависимости между уровень образования информантов (принадлежность к вузовской среде) и уровнем осведомленности о факторах-угрозах личной кибербезопасности и способностью противостоять киберпреступлениям.

Поскольку в результате социологического исследования выявлены факторы, лимитирующие общий уровень кибербезопасности студентов АПП ЮФУ, авторами предложен комплекс организационно-методических рекомендаций, направленных на минимизацию киберугроз обучающихся. Во-первых, в рамках Модуля управляемой академической мобильности студентам ЮФУ предложена к изучению вариативная дисциплина «Финансовая грамотность», которую целесообразно дополнить структурным разделом «Основы цифровой грамотности и кибербезопасности» с соответствующим тематическим контентом: общие вопросы, законодательное обеспечение кибербезопасности, основы информационной безопасности и др. В ходе освоения дисциплины важна реализация активных методов обучения, обеспечивающих высокую степень вовлеченности студентов в образовательный процесс, например, кейс-технологии и нарративный подход. Во-вторых, с 2014 г. на базе Южного федерального университета функционирует пилотная образовательная площадка – Центр финансовой грамотности населения (ЦФГ) при ПАО КБ «Центр-инвест». На базе ЦФГ организовано обучение по различным аспектам деятельности банковского и финансового секторов экономики. Однако, в условиях нарастания киберугроз, переход на новый концептуальный уровень: от финансовой грамотности к финансово-информационной безопасности, усиление институционально-образовательного взаимодействия ЮФУ с партнёрами банковского бизнес-сообщества обеспечит получение профилактического эффекта в области личной кибербезопасности студентов.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Колокольцев заявил о росте доли киберпреступлений в России // РИА Новости. — 2024 — URL: https://ria.ru/20241014/prestupleniya-1978033005.html (дата обращения: 15.10.2024)

2. Генпрокурор заявил о тысячах дел, где «между двумя корочками ничего нет» // Гру́ппа компа́ний «РБК». — 2024 — URL: https://www.rbc.ru/society/10/10/2024/6707e5b09a794718b633f9e3 (дата обращения: 10.10.2024)

3. Wu C. Data privacy: From transparency to fairness / C. Wu // Technology in Society. — 2024. — № 76.

4. Vimal K.M. Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants / K.M. Vimal, K.S. Sujeet, B.S. Jang [et al.] // Computers in Human Behavior. — 2021. — № 120 (3). — DOI: 10.1016/j.chb.2021.106763.

5. Leukfeldt E.R. Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals / E.R. Leukfeldt, T.J. Holt // Computers in Human Behavior. — 2022. — № 126.

6. Берман Н.Д. К вопросу о цифровой грамотности / Н.Д. Берман // Russian Journal of Education and Psychology. — 2017. — № 6-2. — С. 35–38.

7. Loggen J. A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime / J. Loggen, A. Moneva, R. Leukfeldt // Computer Law & Security Review. — 2024. — № 52.

8. Зуев А.В Методологические аспекты обучения студентов в области обеспечения кибербезопасности на факультативных занятиях / А.В Зуев, А.В. Платонов, В.А. Беседина [и др.] // Ученые записки университета имени П.С. Легафта. — 2023. — № 7 (221). — С. 145–148. — DOI: 10.34835/issn.2308-1961.2023.07.p145-148.

9. Итинсон К.С. Обеспечение кибербезопасности в образовательных учреждениях: осведомленность, правила, стратегия / К.С. Итинсон, В.М. Чиркова // Балтийский гуманитарный журнал. — 2021. — Т. 10. — №4 (37). — С. 99–101.

10. Давыденко И.Г. Измерение уровня осведомленности студентов о кибермошенничестве в кредитно-финансовой сфере / И.Г. Давыденко, Д.Н. Мисиров, Н.Г. Александрова // Экономика устойчивого развития. — 2024. — № 3 (59). — С. 208–213.

11. Дубина И.Н. Математические основы эмпирических социально-экономических исследований / И.Н. Дубина — Барнаул: Издательство АлтГУ, 2006. — 263 с.

12. Руденкин Д.В. Эвристический потенциал теории «цифровых аборигенов» М. Пренски при исследовании современной российской молодежи / Д.В. Руденкин // Социодинамика. — 2019. — № 9. — С. 9–20. — DOI: 10.25136/2409-7144.2019.9.30365.

13. Karagiannopoulos V. Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study / V. Karagiannopoulos, A. Kirby, S. Oftadeh-Moghadam [et al.] // Computer Law & Security Review. — 2021. — № 43. — DOI: 10.1016/j.clsr.2021.105615.

Список литературы на английском языке / References in English

1. Kolokol'tsev zajavil o roste doli kiberprestuplenij v Rossii [Kolokoltsev announced an increase in the share of cybercrimes in Russia] // RIA News. — 2024 — URL: https://ria.ru/20241014/prestupleniya-1978033005.html (accessed: 15.10.2024) [in Russian]

2. Genprokuror zajavil o tysjachah del, gde «mezhdu dvumja korochkami nichego net» [The Prosecutor General announced thousands of cases where "there is nothing between two crusts"] // RBC Group. — 2024 — URL: https://www.rbc.ru/society/10/10/2024/6707e5b09a794718b633f9e3 (accessed: 10.10.2024) [in Russian]

3. Wu C. Data privacy: From transparency to fairness / C. Wu // Technology in Society. — 2024. — № 76.

4. Vimal K.M. Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants / K.M. Vimal, K.S. Sujeet, B.S. Jang [et al.] // Computers in Human Behavior. — 2021. — № 120 (3). — DOI: 10.1016/j.chb.2021.106763.

5. Leukfeldt E.R. Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals / E.R. Leukfeldt, T.J. Holt // Computers in Human Behavior. — 2022. — № 126.

6. Berman N.D. K voprosu o tsifrovoj gramotnosti [On the issue of digital literacy] / N.D. Berman // Russian Journal of Education and Psychology. — 2017. — № 6-2. — P. 35–38. [in Russian]

7. Loggen J. A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime / J. Loggen, A. Moneva, R. Leukfeldt // Computer Law & Security Review. — 2024. — № 52.

8. Zuev A.V Metodologicheskie aspekty obuchenija studentov v oblasti obespechenija kiberbezopasnosti na fakul'tativnyh zanjatijah [Methodological aspects of teaching students in the field of cybersecurity in elective classes] / A.V Zuev, A.V. Platonov, V.A. Besedina [et al.] // Scientific notes of the P.S. Lesgaft University. — 2023. — № 7 (221). — P. 145–148. — DOI: 10.34835/issn.2308-1961.2023.07.p145-148. [in Russian]

9. Itinson K.S. Obespechenie kiberbezopasnosti v obrazovatel'nyh uchrezhdenijah: osvedomlennost', pravila, strategija [Ensuring cybersecurity in educational institutions: awareness, rules, strategy] / K.S. Itinson, V.M. Chirkova // The Baltic Humanitarian Journal. — 2021. — Vol. 10. — №4 (37). — P. 99–101. [in Russian]

10. Davydenko I.G. Izmerenie urovnja osvedomlennosti studentov o kibermoshennichestve v kreditno-finansovoj sfere [Measuring students' awareness of cyber fraud in the financial and credit sector] / I.G. Davydenko, D.N. Misirov, N.G. Aleksandrova // The Economics of Sustainable Development. — 2024. — № 3 (59). — P. 208–213. [in Russian]

11. Dubina I.N. Matematicheskie osnovy empiricheskih sotsial'no-ekonomicheskih issledovanij [Mathematical foundations of empirical socio-economic research] / I.N. Dubina — Barnaul: AltSU Publishing House, 2006. — 263 p. [in Russian]

12. Rudenkin D.V. Evristicheskij potentsial teorii «tsifrovyh aborigenov» M. Prenski pri issledovanii sovremennoj rossijskoj molodezhi [The heuristic potential of the theory of "digital aborigines" by M. Prensky in the study of modern Russian youth] / D.V. Rudenkin // Sociodynamics. — 2019. — № 9. — P. 9–20. — DOI: 10.25136/2409-7144.2019.9.30365. [in Russian]

13. Karagiannopoulos V. Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study / V. Karagiannopoulos, A. Kirby, S. Oftadeh-Moghadam [et al.] // Computer Law & Security Review. — 2021. — № 43. — DOI: 10.1016/j.clsr.2021.105615.