Статья / Article

УДК / UDC 37.016:37.011.31-051:004
DOI 10.35231/18186653_2021_2_428

Ориентированность подготовки будущих учителей информатики на формирование профессиональных компетенций по информационной безопасности

А. А. Нечай

Ленинградский государственный университет имени А.С. Пушкина, Санкт-Петербург, Российская Федерация

Введение. Информационная безопасность является глобальной проблемой из-за растущей зависимости общества от глобальной сети Интернет, а киберугрозы – один из самых серьезных вызовов для экономики и национальной безопасности. Информационная безопасность стала главным национальным приоритетом. Все организации, включая образовательные учреждения, работающие с применением цифровых компьютерных технологий, нуждаются в специалистах, обладающих компетенциями и навыками, которые включают поведенческие, управленческие и технические знания для борьбы с кибератаками в динамичной среде киберугроз. В связи с этим растет спрос не только на квалифицированных специалистов, но и на учителей, обладающих компетенциями по информационной безопасности, которые способны учить основам кибербезопасности со школьной скамьи.

Существующие противоречия между повсеместным применением цифровых технологий, уязвимых к кибератакам, и недостаточностью использования образовательного процесса для обучения информационной безопасности, а также между увеличением спроса на подготовку учителей информатики по информационной безопасности и недостаточной готовностью профессорско-педагогического состава вуза к подготовке соответствующих специалистов позволяют сформулировать актуальную проблему научного исследования, которая заключается в необходимости системного обеспечения подготовки будущих учителей информатики и формирования у них профессиональных компетенций по информационной безопасности в современных условиях развития информационного общества. Новизна исследования состоит в разработке подхода к обучению будущих учителей информатики основам кибербезопасности и формированию у них компетенций по информационной безопасности в условиях цифровизации образования.

Материалы и методы. При проведении исследования был проведен анализ зарубежных источников, из которых можно сделать вывод о том, что в европейских и азиатских странах ведется активная работа по обучению и профессиональной подготовке в области кибербезопасности; определены теоретико-методологические основы исследования и раскрыта спецификация подготовки учителей информатики по кибербезопасности.

Результаты. В ходе исследования доказано, что профессиональная подготовка учителей информатики по информационной безопасности является актуальной, а включение тем по кибербезопасности в уже существующие учебные планы – обоснованной необходимостью.

Обсуждения и выводы. Делается вывод о том, что подготовка будущих учителей информатики в системах цифрового образования включает в себя овладение современными технологиями, но программы подготовки учителей обычно рассматривают компетентность учителей информатики с точки зрения овладения информационно-коммуникационными технологиями и в незначительной мере касаются подготовки учителей в области информационной безопасности. Кибербезопасность, которая входит в состав информационной безопасности, как таковая вообще не рассматривается, так как предполагается, что кибербезопасность и информационная безопасность полностью идентичны и являются синонимами. За рубежом в европейских странах кибербезопасность уже отделилась от информационной безопасности в отдельную отрасль и постепенно внедряется в России.

Ключевые слова: учитель информатики, информационная безопасность, кибербезопасность, профессиональная подготовка, компетенция.

Для цитирования: Нечай А.А. Ориентированность подготовки будущих учителей информатики на формирование профессиональных компетенций по информационной безопасности // Вестник Ленинградского государственного университета имени А.С. Пушкина. – 2021. – № 2. – С. 428–441. DOI 10.35231/18186653_2021_2_428

Orientation of the training of future computer science teachers to the formation of professional competencies in information security

Aleksandr A. Nechai

Pushkin Leningrad State University,
Saint Petersburg, Russian Federation

Introduction. Information security is a global problem due to the growing dependence of society on the global Internet, and cyber threats are one of the most serious challenges to the economy and national security. Information security has become a top national priority. All organizations, including educational institutions, working with the use of digital computer technologies, need specialists with competencies and skills that include behavioral, managerial and technical knowledge to combat cyber attacks in a dynamic environment of cyber threats. In this regard, there is a growing demand not only for qualified specialists, but also for teachers with information security competencies who are able to teach the basics of cybersecurity from the school bench.

The existing contradictions between the widespread use of digital technologies that are vulnerable to cyber attacks, and the lack of use of the educational process for teaching information security, as well as between the increasing demand for training computer science teachers in information security and the lack of readiness of the university's teaching

staff to train relevant specialists, allow us to formulate an urgent problem of scientific research. The problem lies in the need for systematic training of future teachers of computer science and the formation of their professional competencies in information security in the modern conditions of the development of the information society. The novelty of the research is the development of an approach to teaching future computer science teachers the basics of cybersecurity and the formation of their competencies in information security in the context of digitalization of education.

Materials and methods. In the course of the study, an analysis of foreign sources was conducted, from which it can be concluded that active work is being carried out in European and Asian countries on education and training in the field of cybersecurity, the theoretical and methodological foundations of the study were determined, and the specification of the training of computer science teachers in cybersecurity was disclosed.

Results. The study proves that the professional training of computer science teachers in information security is relevant, and the inclusion of cybersecurity topics in existing curricula is a reasonable necessity.

Discussions and conclusions. It is concluded that the training of future computer science teachers in digital education systems includes the mastery of modern technologies, but teacher training programs usually consider the competence of computer science teachers and in terms of mastering information and communication technologies and to a small extent relate to the training of teachers in the field of information security. Cybersecurity, which is part of information security as such, is not considered at all, since it is assumed that cybersecurity and information security are completely identical and are synonymous. Abroad, in European countries, cybersecurity has already separated from information security into a separate industry and is gradually being introduced in Russia.

Keywords: computer science teacher, information security, cybersecurity, professional training, competence.

For citation: Nechay, A. A. (2021) Orientirovannost' podgotovki budushchikh uchitelej informatiki na formirovanie professional'nykh kompetencij po informacionnoj bezopasnosti [Orientation of the training of future computer science teachers to the formation of professional competencies in information security] // *Vestnik Leningradskogo gosudarstvennogo universiteta imeni A.S. Pushkina – Pushkin Leningrad State University Journal.* No 2. pp. 428–441. DOI 10.35231/18186653_2021_2_428 (In Russian).

Введение

Подготовка будущих учителей информатики в системах цифрового образования включает в себя овладение современными технологиями [3; 4], но программы подготовки учителей обычно рассматривают компетентность учителей информатики с точки зрения овладения информационно-коммуникационными технологиями и в незначительной мере касаются подготовки учителей в области информационной безопасности. Кибербезопасность как таковая вообще не рассматривается, так как предполагается, что кибербезопасность и информационная безопасность полностью идентичны и являются синонимами [8]. За рубежом в европей-

ских странах кибербезопасность уже отделилась от информационной безопасности [21] в отдельную отрасль и постепенно внедряется в России.

Кибербезопасность не является чем-то новым и уже почти два десятилетия является предметом серьезных дискуссий в правительстве, промышленности и научных кругах [22]. Тем не менее, существуют некоторые различия в определении и сфере применения кибербезопасности, которые были причиной разногласий между разными авторами [7; 10]. Некоторые эксперты утверждают, что эта тема чрезмерно и искусственно раздута из-за нагнетания страха, а такой термин, как «кибервойна» предназначен для того, чтобы вызвать эмоциональную, а не рациональную реакцию [11].

Опасения по поводу электронной конфиденциальности действительно могут быть обоснованными, многие киберпреступления являются прямым результатом нарушений безопасности [12; 13].

Материалы и методы

Концептуальной идеей исследования является разработка новых подходов к обучению будущих учителей информатики основам кибербезопасности [23] в рамках изучения дисциплин, формирующих профессиональные компетенции по информационной безопасности. На основе теоретико-методологических исследований [24] выделены ключевые моменты в подготовке будущих учителей информатики по информационной безопасности и раскрыта спецификация подготовки учителей информатики по кибербезопасности как подсистемы информационной безопасности [25].

Международная организация по стандартизации в настоящее время определяет кибербезопасность как сохранение конфиденциальности, целостности и доступности информации в киберпространстве [26], с сопутствующим определением киберпространства как сложной среды, возникающей в результате взаимодействия людей, программного обеспечения и услуг в Интернете с помощью технологических устройств и подключенных к нему сетей, которая не существует ни в какой физической форме [15].

Обзор литературы

Формирование профессиональных компетенций учителей информатики рассматривается в научных трудах многих авторов. Так, А.И. Блинкин рассматривает профессиональные компетенции учителя информатики двадцать первого века и делает вывод о необходимости непрерывного самообразования учителей и повышения их компетентности

в области современных информационных технологий [2].

Подготовку будущих учителей информатики в условиях цифрового образования рассматривали Е.В. Баранова и И.В. Смирнова, они предложили модель подготовки бакалавров педагогического образования, обеспечивающую формирование профессиональных компетенций учителя информатики. В своем исследовании, авторы делают вывод о том, что структура и содержание подготовки должны соответствовать личностным ожиданиям и требованиям социума к образованию и потребностям рынка труда [1].

Использование междисциплинарной методической системы при формировании профессиональных компетенций учителей информатики предлагает П.В. Никитин. Описывая проблемы формирования профессиональных компетенций в ходе обучения в педагогических вузах, указывает на необходимость усовершенствования профессиональной подготовки будущих учителей информатики [14].

На формирование культуры информационной безопасности в формате дистанционного обучения было направлено научное исследование А.В. Наумовой и Е.Г. Топорковой. Авторы рассмотрели дистанционное образование, а также необходимые навыки и компетенции педагога, влияющие на эффективность обучения [5].

Обеспечение информационной безопасности и защиту информации, выработку представления о значимости проблемы обеспечения безопасности личности в мировом информационном сообществе рассматривает Е.В. Чернова и делает заключение о том, что сформирование основных элементов информационной культуры позволит развить информационные и общекультурные компетенции, значимые для успешного личностного развития и профессионального роста [18].

Проблема использования интерактивных методов обучения при формировании профессиональных компетенций будущих учителей педагогов по обеспечению кибербезопасности рассмотрена в научной работе Т.В. Рихтер. Ученый выделяет составляющие кибербезопасности, группы интерактивных методов, способствующих формированию отдельных элементов профессиональной компетенции педагогов в области обеспечения кибербезопасности [17].

Формирование профессиональных компетенций у будущих учителей информатики по кибербезопасности рассмотрены в научных публикациях А.А. Нечай и С.А. Краснова, которые указывают на необходимость включения в программы подготовки будущих учителей информатики основ кибербезопасности [6; 9].

Результаты

Очевидно, что кибербезопасность является областью многочисленных дискуссий, интереса и внимания.

Также понятие «кибербезопасность» можно значительно упростить. Упрощение кибербезопасности до нескольких ключевых терминов и их отношений обеспечивает гибкую структуру. Этот уровень гибкости помогает учебным программам поддерживать относительно открытую академическую структуру, которая может способствовать решению проблем в определениях, стандартах и структурах кибербезопасности. Акцент на кибербезопасности можно ограничить в рамках трех категорий, которые следовали бы за общей предпосылкой обеспечения информационной безопасности и безопасности информации [16]: это категории «подготовка», «защита» и «действие». Первоначально кибербезопасность обозначалась категорий «реагировать», означающей реакцию на киберинцидент. Это показалось неуместным, учитывая аксиому: «лучше действовать, чем реагировать». Категория «реагировать» может вызвать в воображении, скорее, неосторожную реакцию, чем хорошо выполненный план действий. Каждая из этих категорий может быть лучше контекстуализирована с помощью следующих вопросов:

1. Какие существуют киберугрозы, как мы можем подготовиться к ним и минимизировать потенциальные атаки? (Подготовка).

2. Как проектировать и поддерживать в безопасности информационные системы? (Защита).

3. Что следует делать в случае кибератаки и как можно применять имеющиеся средства защиты? (Действие).

Подготовка к кибербезопасности означает, что риски понятны [27]. Это требует глубокого понимания угрозы и ее последствий. Важно отметить, что они не являются чисто техническими. Большая часть подготовки заключается в понимании взаимосвязи между киберпространством и реальным миром. Основными техническими темами являются тестирование на проникновение, этический взлом и продвинутые постоянные угрозы [28].

Киберзащита предполагает принятие превентивных мер по защите компьютерных систем и опять же включает в себя как технические, так и нетехнические элементы. Мы считаем, что эта категория хорошо подходит для системного администрирования. Системные администраторы отвечают за техническое обслуживание систем и сетей, а также за реализацию политик безопасности [29]. Другие соответствующие темы включают проектирование сетей и систем в контексте безопасности. Подготовка, аудит, аккредитация и обучение пользователей – все это относится к категории превентивной защиты [30].

Категория действия – это то, что нужно делать в случае кибератаки. Каковы признаки активной атаки, какие шаги следует предпринять для оценки потенциального воздействия, получения атрибуции, реагирования и восстановления сервиса? Технические темы включают цифровую судебную экспертизу (в реальном времени и в автономном режиме) и реагирование на инциденты. Другие области включают культурную и глобальную стандартизацию, правовые вопросы, контрэкспертизу, теорию компьютерной криминалистики и реагирования на инциденты, а также понимание того, как разные организации имеют разные методологии и приоритеты [19].

Кибербезопасность – это не новая тема, а скорее, метод просмотра и корреляции существующих знаний для целостного анализа, понимания, защиты от киберугроз и реагирования на них.

Начальное обучение будущих учителей информатики с последовательным подходом в обучении необходимо там, где информационная и кибербезопасность должна преподаваться как вопрос высокого приоритета в образовательной области, особенно внутри учебных программ в рамках общей системы подготовки учителей и формирования у них профессиональных компетенций в сфере кибербезопасности.

Нет никаких сомнений в том, что преподаватель нуждается в знаниях в области цифровой безопасности и способам ее достижения. Ожидается, что учителя возьмут на себя ответственность за обучение цифровой безопасности и ориентируют своих учеников на правила поведения в Интернете, но учителя часто не имеют достаточной подготовки, чтобы понять риски, связанные с неэтичным поведением. Преподаватель может служить моделью, помогающей улучшить поведение студентов при использовании информационных технологий, вести беседы о рисках и ущербе и оказывать значительное влияние на студентов своими действиями.

Таким образом, первоначальное обучение кибербезопасности должно быть чутким к текущим потребностям общества, чтобы будущие учителя адаптировались к инновационным процессам и могли конкурировать на рынке труда за использование современных информационных технологий. Новая цифровая культура требует от учителей быть полезными и востребованными в цифровом обществе.

Различные исследования свидетельствуют о настоятельной необходимости для образовательных учреждений формирования центров, которые гарантируют подготовку в области кибербезопасности, чтобы повысить безопасность как приоритетные вопросы в сфере образования, особенно это касается программ подготовки будущих учителей.

На международном уровне, в европейских и азиатских странах ведется работа по повышению безопасности путем обучения и профессиональной подготовки в области кибербезопасности.

Например, в Тайване программа «Таис» определила четыре аспекта подготовки компетентных учителей:

- безопасность и защита коммуникаций;
- пригодность информации;
- безопасность в Интернете;
- собственное использование технологических устройств.

В странах ЕС такие организации, как Британское агентство образовательных коммуникаций и технологий «ВЕСТА», различные исследования в Скандинавских странах и Чешской Республике, подчеркивают важность подготовки учителей и заключают, что предшествующий опыт, знания, практика, мнения и восприятие определяют, как учителя должны преподавать, решать и заниматься проблемами кибербезопасности [20].

На глобальном уровне «ЮНИСЕФ» (Международный детский фонд организации объединенных наций) предлагает важность консолидации действий и образовательных мер для образовательных учреждений и от них – совместную ответственность родителей и учителей, а также необходимость выделения образовательных ресурсов на образовательные и профилактические программы, которые помогают избежать угроз и защищать от опасностей цифрового мира.

Обсуждения и выводы

Проведя исследования передового опыта зарубежных стран и соответствующих тематике научных публикаций, связанных с подготовкой будущих учителей по направлению кибербезопасности с целью выявления образовательных потребностей, предложен ряд тем, которые имеют решающее значение для подготовки будущего специалиста:

- правила онлайн-общения и поведения (сетевой этикет);
- меры и средства предотвращения рисков в Интернете и заботы о физическом и психическом здоровье;
- концепции, связанные с цифровой безопасностью (репутация, идентичность, цифровой разрыв и отпечаток пальца);
- защита персональных данных в сфере образования;
- безопасная защита устройств и создание паролей.

Несмотря на то что существует мало исследований, специально посвященных кибербезопасности, актуальность этой темы подтверждается регулярным ее обсуждением на повестке дня ведущих компаний и организаций, связанных с информационными технологиями. И как следствие,

это свидетельствует о необходимости углубленных исследований по обучению кибербезопасности, а также продвижении этой темы и включении ее в уже существующие учебные планы и программы на разных этапах образования.

Список литературы

1. Баранова Е.В., Симонова И.В. Развитие профессиональных компетенций бакалавров по направлению педагогического образования в области информатики в условиях цифрового образования // Известия Российского государственного педагогического университета им. А.И. Герцена. – 2018. – № 190. – С. 116–124.
2. Бликин А.И. Профессиональные компетенции учителя информатики XXI века // Инновационные технологии XXI века: материалы Междунар. науч.-практ. конф. Казанский государственный технический университет им. А.Н. Туполева. – 2015. – С. 81–82.
3. Борисов А.А., Краснов С.А., Нечай А.А. Технология блокчейн и проблемы её применения в различных информационных системах // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2018. – № 2. – С. 63–67.
4. Калиниченко С.В., Котиков, П.Е., Нечай, А.А. Решение репликационных проблем в базах данных для повышения устойчивости программного обеспечения автоматизированных систем // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2017. – № 4. – С. 18–21.
5. Наумова А.В., Топоркова Е.Г. Формирование культуры информационной безопасности в формате дистанционного обучения // Информационные проблемы и драйверы социально-экономического развития общества в условиях глобализации: сб. науч. ст. Междунар.науч.-практ. конф. Ставропольский государственный аграрный университет. – 2020. – С. 479–481.
6. Нечай А.А. Формирование профессиональной компетенции в области кибербезопасности у будущих учителей информатики // Вестник Ленинградского государственного университета им. А.С. Пушкина. – 2020. – № 4. – С. 114–124.
7. Нечай А.А. Геймификация как способ организации обучения кибербезопасности // Фундаментальные проблемы обучения математике, информатике и информатизации образования: сб. тез. докл. Междунар. науч. конф., посвящ. 180-летию педагогического образования в г. Ельце. – 2020. – С. 93–94.
8. Нечай А.А. Кибербезопасность и информационная безопасность: сущность, содержание и отличие понятий // XXIV Царскосельские чтения. 75-летие Победы в Великой Отечественной войне: материалы междунар. науч. конф. / под общ. ред. С.Г. Еремеева, 2020. – С. 229–232.
9. Нечай А.А., Краснов, С.А. Формирование компетенции учителя информатики в области кибербезопасности // Азимут научных исследований: педагогика и психология. – 2020. – Т. 9. – № 4 (33). – С. 188–190.
10. Нечай А.А. Использование инновационных методов и современных технологий для повышения квалификации в области кибербезопасности // Азимут научных исследований: педагогика и психология. – 2020. – Т. 9. – № 3 (32). – С. 193–196.
11. Нечай А.А. Формирование безопасной информационной среды // Актуальные проблемы современности: наука и общество. – 2019. – № 4 (25). – С. 43–44.
12. Нечай А.А., Краснов С.А., Свинарчук А.А. Аналитическая модель обеспечения информационной безопасности образовательных организаций системы общего и

среднего образования // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2020. – № 4. – С. 77–84.

13. Нечай А.А., Котиков П.Е. Актуальные проблемы защиты информации в современных автоматических телефонных станциях // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2015. – № 2. – С. 65–69.

14. Никитин П.В. Междисциплинарная методическая система формирования профессиональной компетентности у будущих учителей информатики // Вестник Чувашского государственного педагогического университета им. И.Я. Яковлева. – 2010. – № 3-2 (67). – С. 135–140.

15. Новиков А.Н., Нечай А.А., Малахов А.В. О подходе к обоснованию рациональной номенклатуры эталонной базы измерительных комплексов на основе нечетких моделей // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2017. – № 1. – С. 72–79.

16. Новиков А.Н., Нечай А.А., Малахов А.В. Математическая модель обоснования вариантов реконфигурации распределенной автоматизированной контрольно-измерительной системы // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2016. – № 1-2. – С. 56–59.

17. Рихтер Т.В. Использование интерактивных методов обучения при формировании профессиональных компетенций педагогов по обеспечению кибербезопасности подрастающего поколения // Активные и интерактивные методы обучения в естественно-математическом образовании. Коллективная монография. Соликамский государственный педагогический институт (филиал) ФГБОУ ВО «Пермский государственный национальный исследовательский университет». Соликамск, 2018. – С. 13–21.

18. Чернова Е.В. Информационная безопасность человека: учеб. пособие. 2-е изд., испр. и доп. Сер. 76 Высшее образование. – М., 2020. – 24 с.

19. Широбоков В.В., Нечай А.А. Алгоритм планирования энергосберегающей параллельной обработки информации с учетом информационной важности и времени поступления задач // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2017. – № 1. – С. 88–93.

20. Эсаулов К.А., Яхваров Е.К., Нечай А.А., Березин А.С. Методика интеграции системы управления киберрисками в предпринимательских структурах // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2020. – № 2. – С. 80–86.

21. Bentle M., Stephenson A., Toscas P., Zhu Z. A multivariate model to quantify and mitigate cybersecurity risk // Risks. 2020. Т. 8. № 2. P. 1-21.

22. Jeyaraj A., Zadeh A., Sethi V. Cybersecurity threats and organisational response: textual analysis and panel regression // Journal of Business Analytics. 2020.

23. Kavallieratos G., Katsikas S., Gkioulos V. Cybersecurity and safety co-engineering of cyberphysical systems – a comprehensive survey // Future Internet. 2020. Т. 12. № 4. P. 65.

24. Li Y., Xu, L. Cybersecurity investments in a two-echelon supply chain with third-party risk propagation // International Journal of Production Research. 2021. Т. 59. № 4. P. 1216–1238.

25. Panigrahi R., Borah, S. A statistical analysis of lazy classifiers using canadian institute of cybersecurity datasets // Lecture Notes on Data Engineering and Communications Technologies. 2020. Т. 37. P. 215–222.

26. Pohasii S.S., Milevskyi S.V., Milevskyi S. Cybersecurity issues in the internet of things // Black Sea Scientific Journal of Academic Research. 2019. Т. 48. № 5-1. P. 135–137.

27. Toapanta S.M.T., Jaramillo J.M.E., Gallegos L.E.M. Cybersecurity analysis to determine the impact on the social area in latin america and the caribbean // ACM International Conference Proceeding Series. 2. Cep. "ICETM 2019 – Proceedings of 2019 2nd International Conference on Education Technology Management" 2019. P. 73–78.

28. Toapanta S.M.T., Armijos M.A.A., Gallegos L.E.M. Analysis of cybersecurity models suitable to apply in an electoral process in ecuador ACM International Conference Proceeding Series. 2. Cep. "ICETM 2019 – Proceedings of 2019 2nd International Conference on Education Technology Management" 2019. P. 84-90.

29. Fernández-Caramés, T.M., Fraga-Lamas, P. Teaching and learning iot cybersecurity and vulnerability assessment with shodan through practical use cases // Sensors. 2020. T. 20. № 11. P. 30–48.

30. Xu S. Cybersecurity dynamics: a foundation for the science of cybersecurity Advances in Information Security. 2019. T. 74. P. 1–31.

Reference

1. Baranova, E.V., Simonova, I.V. (2018) Razvitie professional'nyh kompetencij bakalavrov po napravleniyu pedagogicheskogo obrazovaniya v oblasti informatiki v usloviyah cifrovogo obrazovaniya [Development of professional competencies of bachelors in the field of teacher education in the field of computer science in the context of digital education]. *Izvestiya Rossijskogo gosudarstvennogo pedagogicheskogo universiteta im. A.I. Gercena – Proceedings of the A. I. Herzen Russian State Pedagogical University.* Vol. 190. pp. 116–124. (In Russian).

2. Blikin, A.I. (2015) *Professional'nye kompetencii uchitelya informatiki XXI veka* [Professional competencies of a computer science teacher of the XXI century]. V sbornike: Innovacionnye tekhnologii XXI veka. materialy Mezhdunarodnoj nauchno-prakticheskoj konferencii. Kazanskij gosudarstvennyj tekhnicheskij universitet im. A.N. Tupoleva – In the collection: Innovative technologies of the XXI century. materials of the International Scientific and Practical Conference. Kazan State Technical University named after A. N. Tupolev. pp. 81–82. (In Russian).

3. Borisov, A.A., Krasnov, S.A., Nechaj, A.A. (2018) Tekhnologiya blokchejn i problemy eyo primeneniya v razlichnyh informacionnyh sistemah [Blockchain technology and problems of its application in various information systems]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex Systems: Models, analysis and management*. Vol. 2. pp. 63–67. (In Russian).

4. Kalinichenko, S.V., Kotikov, P.E., Nechaj, A.A. (2017) Reshenie replikacionnyh problem v bazah dannyh dlya povysheniya ustojchivosti programmnogo obespecheniya avtomatizirovannyh sistem [Solving replication problems in databases to improve the software stability of automated systems]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex Systems: Models, analysis and management.* Vol. 4. pp. 18–21. (In Russian).

5. Naumova, A.V., Toporkova, E.G. (2020) *Formirovanie kul'tury informacionnoj bezopasnosti v formate distancionnogo obucheniya* [Formation of the culture of information security in the format of distance learning]. V sbornike: Informacionnye problemy i drajvery social'no-ekonomicheskogo razvitiya obshchestva v usloviyah globalizacii. Sbornik nauchnyh statej Mezhdunarodnoj nauchno-prakticheskoj konferencii. Stavropol'skij gosudarstvennyj agrarnyj universitet – In the collection: Information problems and drivers of socio-

economic development of society in the context of globalization. Collection of scientific articles of the International Scientific and Practical Conference. Stavropol State Agrarian University. pp. 479–481. (In Russian).

6. Nechaj, A.A. (2020) Formirovanie professional'noj kompetencii v oblasti kiberbezopasnosti u budushchih uchitelej informatiki [Formation of professional competence in the field of cybersecurity for future computer science teachers]. *Vestnik Leningradskogo gosudarstvennogo universiteta im. A.S. Pushkina – Bulletin of the Leningrad State University named after A. S. Pushkin.* Vol. 4. pp. 114–124. (In Russian).

7. Nechaj, A.A. (2020) *Gejmifikaciya kak sposob organizacii obucheniya kiberbezopasnosti* [Gamification as a way to organize cybersecurity training]. V knige: Fundamental'nye problemy obucheniya matematike, informatike i informatizacii obrazovaniya. Sbornik tezisov dokladov mezhdunarodnoj nauchnoj konferencii, posvyashchennoj 180-letiyu pedagogicheskogo obrazovaniya v g. El'ce – In the book: Fundamental problems of teaching mathematics, computer science and informatization of education. Collection of abstracts of the international scientific conference dedicated to the 180th anniversary of teacher education in Yelets. pp. 93–94. (In Russian).

8. Nechaj, A.A. (2020) *Kiberbezopasnost' i informacionnaya bezopasnost': sushchnost', soderzhanie i otlichie ponyatij* [Cybersecurity and information security: the essence, content and difference of concepts]. V sbornike: XXIV Carskosel'skie chteniya. 75-letie Pobedy v Velikoj Otechestvennoj vojne. Materialy mezhdunarodnoj nauchnoj konferencii. Pod obshchej redakciej S.G. Eremeeva – In the collection: XXIV Tsarskoye Selo readings. 75th anniversary of the Victory in the Great Patriotic War. Materials of the international scientific conference. Under the general editorship of S. G. Eremeev. pp. 229–232. (In Russian).

9. Nechaj, A.A., Krasnov, S.A. (2020) Formirovanie kompetencii uchitelya informatiki v oblasti kiberbezopasnosti [Formation of the competence of a computer science teacher in the field of cybersecurity]. *Azimut nauchnyh issledovanij: pedagogika i psihologiya – Azimuth of scientific research: pedagogy and psychology*. T.9. Vol. 4(3). pp. 188–190. (In Russian).

10. Nechaj, A.A. (2020) Ispol'zovanie innovacionnyh metodov i sovremennyh tekhnologij dlya povysheniya kvalifikacii v oblasti kiberbezopasnosti [Use of innovative methods and modern technologies for advanced training in the field of cybersecurity]. *Azimut nauchnyh issledovanij: pedagogika i psihologiya – Azimuth of scientific research: pedagogy and psychology.* T.9. Vol. 3(32). pp. 193–196. (In Russian).

11. Nechaj, A.A. (2019) Formirovanie bezopasnoj informacionnoj sredy [Creating a secure information environment]. *Aktual'nye problemy sovremennosti: nauka i obshchestvo – Actual problems of our time: science and society*. Vol. 4(25). pp. 43–44. (In Russian).

12. Nechaj, A.A., Krasnov, S.A., Svinarchuk, A.A. (2020) Analiticheskaya model' obespecheniya informacionnoj bezopasnosti obrazovatel'nyh organizacij sistemy obshchego i srednego obrazovaniya [Analytical model of ensuring information security of educational organizations of the system of general and secondary education]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex Systems: Models, analysis and management.* Vol. 4. pp. 77–84. (In Russian).

13. Nechaj, A.A., Kotikov, P.E. (2015) Aktual'nye problemy zashchity informacii v sovremennyh avtomaticheskih telefonnyh stanciyah [Actual problems of information protection in modern automatic telephone exchanges]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex Systems: Models, analysis and management*. Vol. 2. pp. 65–69. (In Russian).

14. Nikitin, P.V. (2010) Mezhdisciplinarnaya metodicheskaya sistema formirovaniya professional'noj kompetentnosti u budushchih uchitelej informatiki [Interdisciplinary methodological system for the formation of professional competence of future teachers of computer science]. *Vestnik CHuvashskogo gosudarstvennogo pedagogicheskogo universiteta im. I.YA. YAkovleva – Bulletin of the I. Ya. Yakovlev Chuvash State Pedagogical University*. Vol. 3-2(67). pp. 135–140. (In Russian).

15. Novikov, A.N., Nechaj, A.A., Malahov, A.V. (2017) O podhode k obosnovaniyu racional'noj nomenklatury etalonnoj bazy izmeritel'nyh kompleksov na osnove nechetkih modelej [On the approach to substantiating the rational nomenclature of the reference base of measurement systems based on fuzzy models]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex systems: models, analysis and management*. Vol. 1. pp. 72–79. (In Russian).

16. Novikov, A.N., Nechaj, A.A., Malahov, A.V. (2016) Matematicheskaya model' obosnovaniya variantov rekonfiguracii raspredelennoj avtomatizirovannoj kontrol'no-izmeritel'noj sistemy Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie [Mathematical model of justification of variants of reconfiguration of a distributed automated control and measurement system]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex systems: models, analysis and management*. Vol. 1-2. pp. 56–59. (In Russian).

17. Rihter, T.V. (2018) *Ispol'zovanie interaktivnyh metodov obucheniya pri formirovanii professional'nyh kompetencij pedagogov po obespecheniyu kiberbezopasnosti podrastayushchego pokoleniya* [The use of interactive teaching methods in the formation of professional competencies of teachers to ensure the cybersecurity of the younger generation]. V knige: Aktivnye i interaktivnye metody obucheniya v estestvenno-matematicheskom obrazovanii. Kollektivnaya monografiya. Solikamskij gosudarstvennyj pedagogicheskij institut (filial) FGBOU VO «Permskij gosudarstvennyj nacional'nyj issledovatel'skij universitet». Solikamsk – In the book: Active and interactive teaching methods in natural-mathematical education. Collective monograph. Solikamsk State Pedagogical Institute (branch) of the Perm State National Research University. Solikamsk. pp. 13–21. (In Russian).

18. CHernova, E.V. (2020) *Informacionnaya bezopasnost' cheloveka* [Human information security]. Uchebnoe posobie / Moskva. Vysshee obrazovanie (2-e izd., ispr. i dop). – Textbook / Moscow, 2020. Ser. 76 Higher education (2nd ed., ispr. and dop.). Vol. 76. p. 24. (In Russian).

19. SHirobokov, V.V., Nechaj, A.A. (2017) Algoritm planirovaniya energosberegayushchej parallel'noj obrabotki informacii s uchetom informacionnoj vazhnosti i vremeni postupleniya zadach [An algorithm for planning energy-saving parallel processing of information, taking into account the information importance and the time of receipt of tasks]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex Systems: Models, analysis and management.* Vol. 1. pp. 88–93. (In Russian).

20. Esaulov, K.A., YAhvarov, E.K., Nechaj, A.A., Berezin, A.S. (2020) // Metodika integracii sistemy upravleniya kiberriskami v predprinimatel'skih strukturah [Methodology of integration of the cyber risk management system in business structures]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex Systems: Models, analysis and management.* Vol. 2. pp. 80–86. (In Russian).

21. Bentle M., Stephenson A., Toscas P., Zhu Z. (2020) A multivariate model to quantify and mitigate cybersecurity risk // Risks. Т. 8. № 2. P. 1-21.

22. Jeyaraj A., Zadeh A., Sethi V. (2020) Cybersecurity threats and organisational response: textual analysis and panel regression // Journal of Business Analytics.

23. Kavallieratos G., Katsikas S., Gkioulos V. (2020) Cybersecurity and safety co-engineering of cyberphysical systems – a comprehensive survey // Future Internet. Т. 12. № 4. P. 65.

24. Li, Y., Xu, L. (2021) Cybersecurity investments in a two-echelon supply chain with third-party risk propagation // International Journal of Production Research. Т. 59. № 4. P. 1216–1238.

25. Panigrahi, R., Borah, S. (2020) A statistical analysis of lazy classifiers using canadian institute of cybersecurity datasets // Lecture Notes on Data Engineering and Communications Technologies. Т. 37. P. 215–222.

26. Pohasii, S.S., Milevskyi, S.V., Milevskyi, S. (2019) Cybersecurity issues in the internet of things // Black Sea Scientific Journal of Academic Research. Т. 48. № 5-1. P. 135–137.

27. Toapanta, S.M.T., Jaramillo, J.M.E., Gallegos, L.E.M. (2019) Cybersecurity analysis to determine the impact on the social area in latin america and the caribbean // ACM International Conference Proceeding Series. 2. Сер. "ICETM 2019 – Proceedings of 2019 2nd International Conference on Education Technology Management" 2019. P. 73–78.

28. Toapanta, S.M.T., Armijos, M.A.A., Gallegos, L.E.M. (2019) Analysis of cybersecurity models suitable to apply in an electoral process in ecuador ACM International Conference Proceeding Series. 2. Сер. "ICETM 2019 – Proceedings of 2019 2nd International Conference on Education Technology Management". P. 84–90.

29. Fernández-Caramés, T.M., Fraga-Lamas, P. (2020) Teaching and learning iot cybersecurity and vulnerability assessment with shodan through practical use cases // Sensors. Т. 20. № 11. P. 30–48.

30. Xu S. (2019) Cybersecurity dynamics: a foundation for the science of cybersecurity Advances in Information Security. Т. 74. P. 1–31.

Об авторе

Нечай Александр Анатольевич, аспирант, преподаватель, Ленинградский государственный университет имени А.С. Пушкина, Санкт-Петербург, Российская Федерация, ORCID ID: 0000-0002-1202-4830, e-mail: webexpromt@mail.ru

About the author

Aleksandr A. Nechai, post-graduate student, teacher, Pushkin Leningrad State University, Saint Petersburg, Russian Federation, ORCID ID: 0000-0002-1202-4830, e-mail: webexpromt@mail.ru

Поступила в редакцию: 27.04.2021 Received: 27 Apr. 2021

Принята к публикации: 12.05.2021 Accepted: 12 May 2021

Опубликована: 30.06.2021 Published: 30 June 2021