DOI 10.37882/2223–2982.2025.12.46

АКТУАЛЬНОСТЬ ФОРМИРОВАНИЯ НАВЫКОВ РАБОТЫ С БОЛЬШИМИ ОБЪЕМАМИ ДАННЫХ И КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ У СОВРЕМЕННЫХ ОБУЧАЮЩИХСЯ – МЕТОДЫ ПРЕПОДАВАНИЯ

THE RELEVANCE OF DEVELOPING SKILLS FOR WORKING WITH LARGE AMOUNTS OF DATA AND A CYBERSECURITY CULTURE AMONG MODERN STUDENTS – TEACHING METHODS

I. Cherenkova
O. Kishkinova
I. Kutlikova

Summary: Working with large databases in modern reality is necessary for all professions whose activities are related not only to intellectual work, but also to the need to analyze and monitor information components. Moreover, most of the documents are sent and processed through electronic document management, often via the Internet, because of which, along with skills in working with Big Data, it is important to form a culture of cybersecurity behavior on online platforms. Teaching methods on these topics, in addition to theoretical and practical training parts, as well as work in specialized resources, should include the development of motivational potential, which will allow students to form information and digital competencies. According to the research results, the most productive methods of developing skills in working with large amounts of data are performing problematic tasks, visual method and project activities. It is important to make learning about cybersecurity culture not abstract, but relevant to life, closely correlating with its daily tasks, tied to specific educational, every day and potential work situations. The three main principles of effective data protection training are applicability, compatibility, as well as the vitality and visibility of the materials and skills being mastered.

Keywords: working with large amounts of data, teaching methods, information competence, digital competence, cybersecurity cultures, Big Data.

Черенкова Ирина Анатольевна
старший преподаватель, ФГБОУ ВО Московская государственная академия ветеринарной медицины и биотехнологии– МВА имени К.И. Скрябина
Кишкинова Ольга Алексеевна
старший преподаватель, ФГБОУ ВО Московская государственная академия ветеринарной медицины и биотехнологии – МВА имени К.И. Скрябина
olga.19672015@yandex.ru
Кутликова Ирина Вениаминовна
старший преподаватель, ФГБОУ ВО Московская государственная академия ветеринарной медицины и биотехнологии – МВА имени К.И. Скрябина

Аннотация: Работа с большими базами данных в современной реальности необходима для всех профессий, чья деятельность связана не только с интеллектуальным трудом, но и с необходимостью анализировать и выполнять мониторинг информационных составляющих. Более того, основная часть документов пересылается и оформляется через электронный документооборот, часто, через интернет, вследствие чего, наряду с навыками работы с *Big Data*, важно формировать культуру кибербезопасного поведения на онлайн-площадках. Методы преподавания указанной тематики, помимо теоретической и практической учебных частей, а также работы в специализированных ресурсах, должны включать в себя развитие мотивационного потенциала, что позволит сформировать у обучающихся информационные и цифровые компетенции. Согласно полученным результатам исследования, наиболее продуктивными методами формирования навыков работы с большими объемами данных являются: выполнение проблемных заданий, наглядный метод и проектная деятельность. Обучение культуре кибербезопасности важно делать не абстрактным, а релевантным для жизни, тесно коррелирующим с ее повседневными задачами, привязанным к конкретным учебным, бытовым и потенциальным рабочим ситуациям. В роли трех основных принципов эффективного обучения защите данных выступают применимость, совместимость, а также жизненность и наглядность осваиваемых материалов и навыков.

Ключевые слова: работа с большими объемами данных, методы преподавания, информационная компетенция, цифровая компетенция, культуры кибербезопасности, Big Data.

Введение

Современные профессии тесно коррелируют с необходимостью работать с большими информационными базами, что является теперь не только важной компетенцией аналитиков данных на языке *SQL*, администраторов *Postgre SQL* или разработчиков приложений и *Big Data* на *Java* или *Oracle SQL*, но и трудиться в сферах, отдаленных от СУБД (систем управления базами данных). Например, указанные навыки необходимы, чтобы оперативно и точно составлять номенклатуру продукции, товарные или транспортные накладные, инвентаризационные описи и т.д., формировать рейтинг, собирать и анализировать статистические данные, осу-

ществлять менеджмент доступных хранилищ информации и пр. По данным *SkyPro* [6], в 2023 г. среди наиболее популярных отраслей, где требуется специалист *Big Data*, дифференцируются следующие (см. рисунок 1):

Согласно прогнозам Бюро статистики труда США *(BLS – Bureau of Labor Statistics)*, к 2028 г. число профессий, связанных с большими базами данных, увеличится на 12% – результатом станет создание более 546 000 новых рабочих мест. При этом важным требованием к соискателям, в чьи компетенции будет входить знание *Big Data*, будет навык выполнения широкого спектра задач [12].

Материалы и методы основаны на системном подходе и включают анализ, синтез и структуризацию материала, аналитику и обработку данных, междисциплинарный подход.

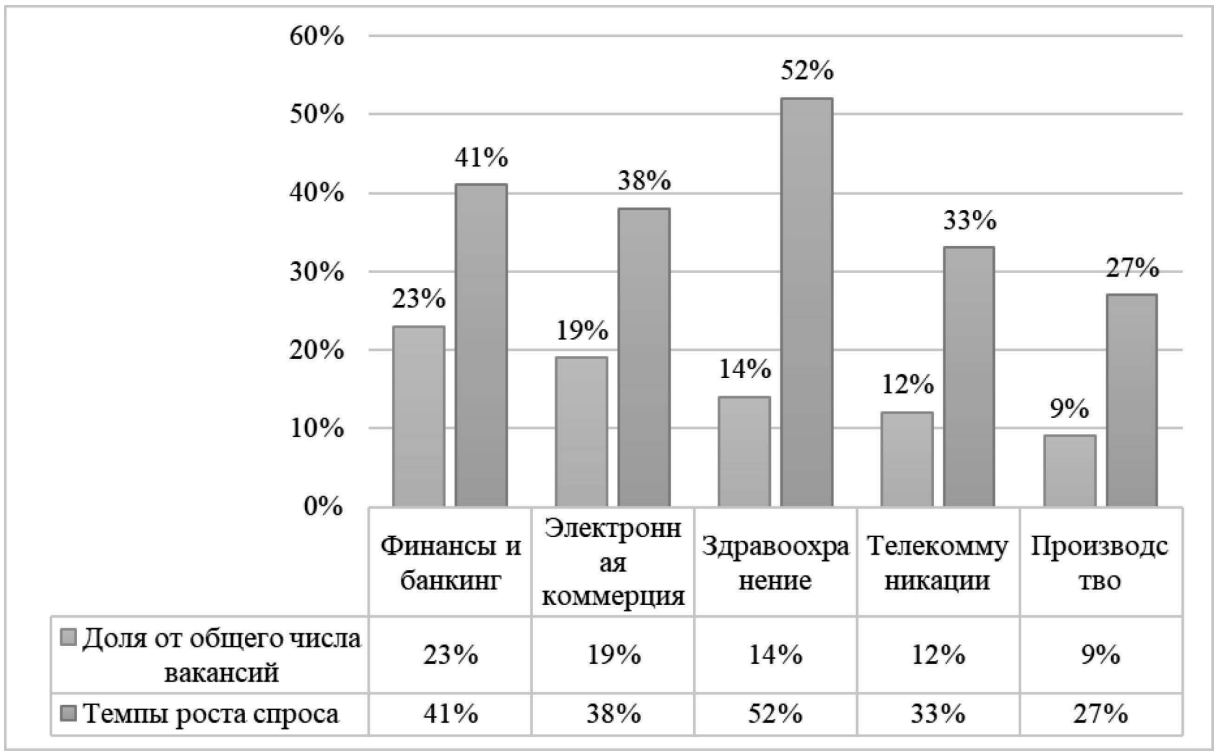
Результаты и обсуждение

Эффективное формирование навыков работы с *Big Data* и культуры кибербезопасности зависит от методов преподавания. Основной из них – **выполнение проблемных заданий** – сосредоточен на работе с реальными данными, которые постоянно фигурируют в жизни обучающихся. Сквозь призму наглядной демонстрации присутствия информационных составляющих в жизни школьников и студентов лучше осваивается целесообразность и принцип работы, а также защиты больших данных. В качестве примера можно взять за основу статистику лайков и репостов, помогающую продвигать определенный контент на лидирующие позиции; автоматический подсчет баллов и формирование рейтинга успеваемости в группе или классе, как, например, это представлено в дневниках и журналах Московских электронных школ (МЭШ); сравнение ценового диапазона стоимости всех видов кофе в разных популярных кофейнях, что можно выполнить благодаря доступу к электронным меню и сайтам данных организаций. На рисунке 2 представлен пример рейтинговой системы МЭШ:

На рисунке 2 представлен визуализированный пример больших баз данных в МЭШ, демонстрирующий, что программа позволяет анализировать прогресс в обучении, сравнивать уровень знаний обучающегося с одноклассниками и контролировать рейтинг успеваемости.

На рисунке 3 изображен пример мониторинга работы *Big Data* российского интернет-сервиса для размещения объявлений «Авито» *(Avito)* – на скриншотах видна общая картина сбора и аналитики данных, статистика показов объявления без подключения дополнительных платных услуг по его продвижению, количество просмотров объекта, число его добавлений в избранное (см. рисунок 3).

Опираясь на визуализированный материал, например, на скриншоты реально существующих данных (см. рисунок 2 и 3), необходимо не только объяснять целесообразность использования больших объемов ин-



	Финансы и банкинг	Электронная коммерция	Здравоохранение	Телекоммуникации	Производство
Доля от общего числа вакансий	23%	19%	14%	12%	9%
Темпы роста спроса	41%	38%	52%	33%	27%

Рис. 1. Наиболее востребованные отрасли с высоким спросом на специалистов, способных работать с большими базами данных (рисунок наш)

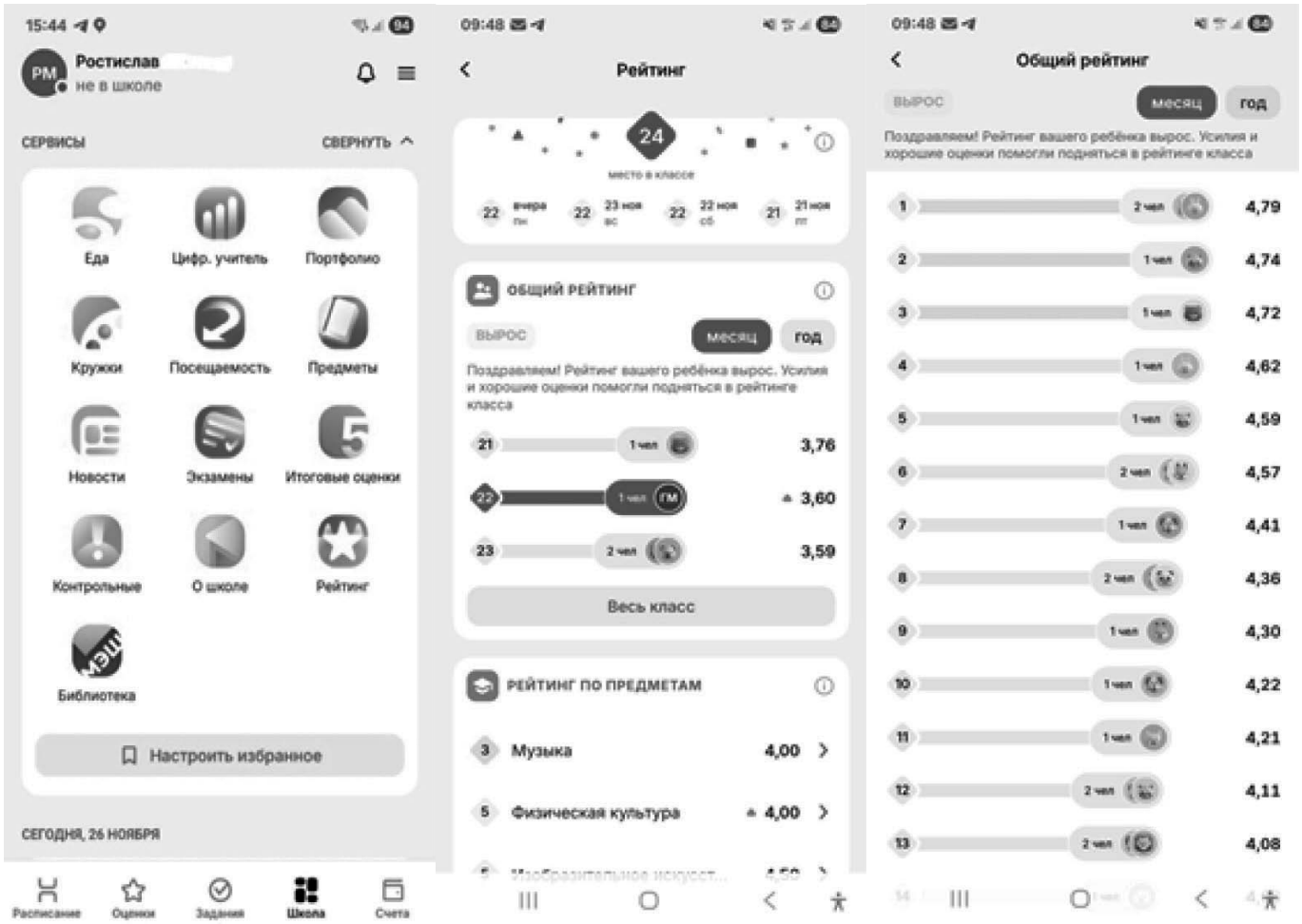


Рис. 2. Возможности работы с большими базами данных в «Московской электронной школе» (МЭШ) (скриншот наш)

Рис. 3. Работа с большими базами данных *(Big Data)* в приложении «Авито» *(Avito)* (скриншот наш)

формации, но и выполнять практические задания по указанному образцу, например: размещать объявления о чем-либо и прослеживать их динамику за установленный преподавателем срок; делать статистику популярности учебных приложений, в основе которых игровой метод; выполнять мониторинг электронных дневника / зачетной книжки / журнала (своих или обучающихся родственников), если у студентов есть к ним доступ. Тем более что с сентября 2024 г. платформа «Моя школа» доступна во всех регионах России [2], а электронные студенческие билеты и зачетные книжки интегрированы в 76-ти вузах различных регионов страны.

Второй метод – **наглядный** – заключается в подборе и демонстрации актуального видеоконтента с любопытным для конкретных возраста и специальностей материалом, обучающим работе с большими базами данных. В настоящее время на *Rutub*, в *VK* (ВКонтакте), MAX, МЭШ, Дзен и на других платформах существуют видеоуроки и презентации по обозначенной тематике, ориентированные на разные профессии и уровни цифровых и информационных компетенций аудитории. После просмотра необходимо приступать к выполнению практических заданий, которые помогут закрепить полученные навыки и знания. Например, снять свой видеоролик от 60 до 120-ти секунд, в котором обучающийся будет преподносить материал о работе с *Big Data* и культуре кибербезопасности неординарным способом (включая комедийные скетчи, иронию, мемы, забавные моменты из повседневной жизни, пародии на популярные события или личности, участие в популярных челленджах и трендах и т.д.). Позже этот ролик можно разместить в социальных сетях или на других площадках, проследив статистику его лайков, репостов и просмотров.

В современную действительность проекты в области кибербезопасности имеют решающее значение для защиты конфиденциальной информации и обеспечения устойчивости организации *(Aksoy 2024; Khasabah, Al-Hammouri, Nusairat, Fraihat 2025)* [7; 10, p. 729]. Третий метод – **проектная деятельность** – является важным звеном обучения, позволяющим гипотетически описывать необходимость создания мобильного приложения для работы с той или иной сферой деятельности и, если достаточно развиты компетенции для работы с большими данными, на практике его реализовать. Например, создать программу по компилированию, анализу и обработке данных о написании текстов искусственным интеллектом на тему о здоровье молодежи; приложение, позволяющее отслеживать количество пользователей от 18-ти до 35-ти лет, предпочитающих поступать в аспирантуру (ординатуру) или на второе высшее образование, работающее на базе *mos.ru* и т.д.; собрать базу данных о трендах популярных социальных сетей и оформить полученные результаты с помощью иконографики и т.д.

Навыки работы с *Big Data* тесно коррелируют с кибербезопасностью, которая является критически важной сферой, требующей круглосуточного мониторинга в связи с быстрым ростом числа киберугроз. Согласно исследованиям Дж. Аксой *(Aksoy 2024)*, в условиях киберрисков защита данных зависит от самого слабого звена – человеческого фактора, который можно уменьшить, если сосредоточиться на убеждениях, ценностях и установках, определяющих модель поведения обучающихся (будущих сотрудников организаций, чьи интересы они должны защищать). В данном контексте концепция культуры кибербезопасности становится ключом к повышению киберустойчивости всех участников образовательного и трудового процессов. Создание жизнеспособной культуры кибербезопасности возможно при условии, что внимание будет уделяться как техническим, так и человеческим аспектам работы с обозначенной проблематикой [7, p. 96].

В связи со стремительным развитием кибератак кибербезопасность требует комплексного подхода, который объединяет технологические решения, управление рисками, разработку политики и понимание поведения человека. Хотя кибербезопасность часто используется как синоним информационной безопасности, она имеет более широкую сферу применения, где особое внимание уделяется влиянию человеческого фактора, что делает отдельных лиц и организации более уязвимыми для атак, если не принять надлежащих мер *(Hyasat, Falahat 2025)* [9, p. 4].

Т.А. Бэш, Л. Педерсен, М.К. Борен, Л.К. Темте *(Bach, Pedersen, Borén, Temte 2025)* также отмечают, что одних технологий недостаточно для предотвращения исследуемых нарушений, поскольку киберугрозы все чаще используют поведение человека, поэтому следует создавать более устойчивые *CSC (Critical Security Controls)* для эффективного управления уязвимостями, связанными с человеческим фактором. *CSC* – рекомендации по лучшим практикам в области компьютерной безопасности фреймворком *CIS (Center for Internet Security)* – следует определять как культуру кибербезопасности организации, которая оказывает влияние на внедрение и эффективность ресурсов, политик, практик и процедур управления данной сферой, поскольку они отражают рабочую среду и лежащие в ее основе представления, отношения и привычные практики будущих сотрудников на всех уровнях [8].

Кроме того, по мере того, как организации претерпевают быструю цифровую трансформацию, ускоряемую новыми технологиями, такими как искусственный интеллект (ИИ), облачные вычисления и интернет вещей *(IoT, Internet of Things)*, возможности для атак значительно расширились. Эта эволюция привела к смене парадигмы в том, как проявляются киберугрозы и как организации должны реагировать *(Aksoy 2024; Ussher-Eke 2022)* [7; 13, p. 707]. ИИ используется как в кибератаках, так и в защите от них, а также характерен зловредным воздействием

(например, дипфейками) [5, с. 132].

Таким образом, кибербезопасность охватывает широкий спектр деятельности, включая внедрение технологий защиты данных, реализацию политик и процедур безопасности, а также обучение, т.е. повышение осведомленности о кибербезопасности и внедрения лучших практик. Информируя о культуре инноваций и внедрении новые технологий в эпоху цифровых технологий, можно обеспечить глобальную конкурентоспособность и устойчивый карьерный рост будущих специалистов *(Rattanapong, Ayuthaya 2025)* [11].

Культура кибербезопасности сосредоточенна на защите информации, хранящейся на персональных компьютерах и мобильных устройствах в цифровом виде. По данным МВД (Министерств внутренних дел Российской Федерации), актуальным на ноябрь 2025 г., граждане наиболее часто страдают от следующих преступлений, связанных с несанкционированным доступом, использованием, раскрытием, видоизменением, взломом или уничтожением личных данных и данных организации [3] (см. рисунок 4):

При обучении культуре кибербезопасности (мерам и стратегиям, направленным на предотвращение мошеннических атак) необходимо систематически обновлять учебный материал по данной проблематике и рассказывать обучающимся о новых способах махинаций (которые постоянно совершенствуются и видоизменяются), в т.ч. о последних случаях из реальной жизненной практики россиян. Опирать же образовательную деятельность необходимо на три важных принципа: (1) применимость; (2) совместимость; (3) жизненность и наглядность работы с большими базами данных сквозь призму культуры кибербезопасности [4].

Применимость: каждый из пунктов культуры кибербезопасности должен быть выполним, т.е. применим на практике. Например, гипотетически идеальным является автоматически сгенерированный пароль из случайных символов, состоящий не менее чем из 18 знаков, который важно менять еженедельно, при этом запрещено его записывать на бумажных носителях. Тем не менее, данный прием не выполним, т.к. проблематично запомнить такое количество символов и постоянно их вводить при входе в систему [4]. Так, с точки зрения классической кибербезопасности менее надежным, но вполне выполнимым может быть совет сгенерировать пароль из случайных шести символов и знаков, затем

Рис. 4. Схемы мошенников и аферистов, в основе которых нарушение культуры кибербезопасности пользователями (рисунок наш)

придумать из 3-4-х символов ключевое слово, которое у обучающегося с чем-то ассоциируется. Первые 6 знаков можно записать в блокноте, а остальные 4 держать в памяти – итого получится 10-тизначный пароль для входа в систему. Данный вариант не столь идеален, как первый, однако, выполним.

Совместимость: по мнению редакции *Kaspersky Daily (2019)*, следующим важным аспектом обучения культуре кибербезопасности должна быть совместимость с обучением и, в последующем, с графиком работы и ее нагрузкой [4]. На практике чаще всего активность обучения навыкам данной культуры происходит после какого-либо инцидента, произошедшего в стране / регионе или в организации. После этого предельно активно начинается обучение в большом объеме. Материал необходимо преподносить постепенно и дозированно.

Третьим принципом является **жизненность** и **наглядность**. Работа с учебным материалом должна быть не рутинной, а релевантной и интересной, что повышает мотивацию не только осваивать материал, но и продолжать самообучение на протяжении всей жизни: базовые знания необходимы всем специальностям, а более узкое и углубленное обучение важно проводить согласно конкретной специальности. А именно, например, будущие сотрудники медицинских организаций должны больше получать знаний и навыков о работе ЕМИАС (Единой медицинской информационно-аналитической системе города Москвы, которая в будущем интегрируется по всей России), преподаватели – о МЭШ, правоохранительные органы – об Единой системе информационно-аналитического обеспечения деятельности МВД РФ (ИСОД МВД) и т.д.

Выводы:

Работа с большими базами данных тесно коррелирует с культурой кибербезопасности, знания о которых следует формировать через практику. Занятия, обучающие работе с указанными сферами жизни, важно проводить сквозь призму мотивирующих и активизирующих познавательную деятельность лекций и проектов, сосредоточенных на реальных жизненных ситуациях, постоянно обновляемых материалах в связи с ростом и совершенствованием киберугроз. Акцент на ситуациях, встречающихся в жизни обучающихся, является наиболее эффективным информационным ресурсом, позволяющим продуктивно работать на лекциях и семинарах.

ЛИТЕРАТУРА

1. Как оформить и предъявлять электронный студенческий билет? // 25/AIF.RU. Статья от 03.09.2024. URL: https://aif.ru/society/education/kak-oformit-i-predyavlyat-elektronnyy-studencheskiy-bilet (дата обращения: 25.11.2025).
2. Курбанова Н. Электронный дневник: как зарегистрировать и как пользоваться в 2024 году // Известия iz. Статья от 16.01.2024. URL: https://iz.ru/1635144/naina-kurbanova/elektronnyi-dnevnik-kak-zaregistrirovat-i-kak-polzovatsia-v-2024-godu (дата обращения: 25.11.2025).
3. Манькова Н. Какие схемы используют мошенники для людей разного возраста: новороссийцам на заметку // Блокнот. Статья от 23.11.2025. URL: https://bloknot-novorossiysk.ru/news/kakie-skhemy-ispolzuyut-moshenniki-dlya-lyudey-raz-1922668 (дата обращения: 26.11.2025).
4. Молчанова Е. Культура кибербезопасности вместо нудных лекций // Kaspersky Daily. Статья от 28.02.2019. URL: https://www.kaspersky.ru/blog/building-cybersecurity-culture/22334/?ysclid=mifnpabgvf185617089 (дата обращения: 26.11.2025).
5. Намиот Д.Е. О кибератаках с помощью систем Искусственного интеллекта // International Journal of Open Information Technologies. 2024. №9. С. 132–141.
6. Топ-10 профессий в сфере Big Data: карьера и высокие зарплаты // SkyPro. URL: https://sky.pro/wiki/python/ponimaem-funktsiyu-enumerate-v-python-na-primere-koda/ (дата обращения: 25.11.2025).
7. Aksoy C. (2024) Building a Cibber Security Culture for RESILIENT Organizations Against Cibber Attacks // İşletme Ekonomi ve Yönetim Araştırmaları Dergisi 7(1):96-110. https://doi.org/10.33416/baybem.13212345.
8. Bach T.A., Pedersen L., Borén M.K., Temte L.Ch. (2025) When technology is not enough: Insights from a pilot cybersecurity culture assessment in a safety-critical industrial organization // https://doi.org/10.48550/arXiv.2508.20811.
9. Hyasat O.Al, Falahat M. (2025) The role of cybersecurity in driving organizational performance: Evidence from public universities in Jordan // EDPACS. https://doi.org/10.1080/07366981.2025.2563961.
10. Khasabah M.Ali I. Al, Al-Hammouri Q., Nusairat N., Fraihat S.F.Al (2025) The impact of risk management and agile methodology on cybersecurity project success: the mediating role of team collaboration // International Journal of Data and Network Science 9(4):727-736. https://doi.org/10.5267/j.ijdns.2025.8.011.
11. Rattanapong P., Ayuthaya S.D. Na (2025) Influential factors of cybersecurity investment: A quantitative SEM analysis // Management Science Letters 15(1):31-44. https://doi.org/10.5267/j.msl.2024.3.005.
12. Top Careers in Big Data // StudentScholarships.org. URL: https://studentscholarships.org/articles/335/top-careers-in-big-data (date: 25.11.2025).
13. Ussher-Eke D. (2022) Corresponding author: Diana Ussher-Eke Building a cyber-resilient workforce through HR and IT Collaboration // World Journal of Advanced Research and Reviews 27(02):706-716. https://doi.org/10.30574/wjarr.2025.27.2.2901.

Журнал «Современная наука: актуальные проблемы теории и практики»