Дата поступления рукописи в редакцию: 22.01.2026 г.
Дата принятия рукописи в печать: 25.02.2026 г.
DOI: 10.24412/2224-9133-2026-1-194-201

ТАЛЬВИК Екатерина Викторовна,
Российский государственный педагогический университет имени А.И. Герцена, магистрант,
e-mail: evlasukova@yandex.ru

Научный руководитель:
ФИЛЯСОВА Юлия Анатольевна,
Российский государственный педагогический университет имени А.И. Герцена,
кандидат филологических наук, доцент,
e-mail: phill.yield@gmail.com

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ЦЕННОСТЬ ОРГАНИЗАЦИОННОЙ КУЛЬТУРЫ

Аннотация. *В современных условиях полномасштабной цифровизации операционной деятельности множества организаций и предприятий создание культуры информационной безопасности является критически важным для защиты внутренних процессов и данных от киберугроз. В первую очередь, речь идет о культуре повышения осведомленности сотрудников об информационной безопасности, регулярном обучении распознаванию и избежанию фишинговых атак, а также созданию надежных паролей. Во-вторых, необходим непрерывный мониторинг сетевой активности и сегментация сетей для ограничения потенциального ущерба от нарушений безопасности. Получение сертификатов в области информационной безопасности обеспечивает защиту организации в соответствии с лучшими отраслевыми практиками. Легитимизация информационной безопасности во внутриорганизационной среде, подразумевающая признание ее необходимости на всех иерархических уровнях, способствует формированию ответственного отношения сотрудников к данным и повышает общую устойчивость организации к киберпреступлеииям. Внедрение культуры информационной безопасности является стратегически важным шагом для достижения стабильности, устойчивого развития и защиты репутации организации.*

Ключевые слова: *управление паролями, киберпреступность, мониторинг безопасности, шифрование, конфиденциальность, цифровая гигиена, поведенческие паттерны, легитимность.*

TALVIK Ekaterina Viktorovna,
A.I. Herzen State Pedagogical University of Russia,
Master Degree Student

Scientific supervisor:
FILYASOVA Yulia Anatolyevna,
A.I. Herzen State Pedagogical University of Russia,
PhD in Philology, Associate Professor

INFORMATION SECURITY AS A VALUE OF ORGANIZATIONAL CULTURE

Annotation. *Under the current conditions of full-scale digitalization in all operational areas of many organizations and enterprises, the creation of a culture aimed at information security is critical to protecting internal processes and data from cyber threats. First, it involves a culture of raising employee awareness of information security, regular training in recognizing and avoiding phishing attacks, and creating strong passwords. Second, continuous monitoring of network activity and network segmentation are necessary for restricting the potential damage from security breaches. Obtaining information security certifications ensures*

that your organization is protected in accordance with industry best practices. Information security legitimization within an organization, which implies recognition of its necessity at all hierarchical levels, promotes the development of a responsible employee attitude towards data and increases the overall resilience of the organization to cybercrime. The implementation of an information security culture is a strategically important step to achieving stability, sustainable development, and protecting an organization's reputation.

Key words: *password management, cybercrime, security monitoring, encryption, privacy, digital hygiene, behavioral patterns, legitimacy.*

Введение

Организационная культура как совокупность общих ценностей, моделей поведения, убеждений, правил, традиций, формирующих уникальную рабочую среду, определяет стиль управления, лидерство, коммуникацию, сотрудничество и межличностное взаимодействие внутри коллектива. Организационная культура оказывает влияние на мотивацию и вовлеченность персонала, эффективность деятельности, прозрачность коммуникации, наличие коллективных практик, применение инновационных подходов [1]. В современных условиях цифровизации статичные ценности организации претерпевают значительное воздействие со стороны динамичных инноваций, включая новые цифровые технологии. Как следствие, «ценности и инновации оказываются ключевыми факторами влияния на происходящие глубокие изменения, при этом оказывая значимое взаимное влияние друг на друга» [2, с. 6]. Ценности и инновации являются факторами поддержания равновесия организационной системы на основе принципа самосохранения – за счет кадровых ресурсов и резервов, связанных с созданием и поддержанием ценностей, и принципа развития – посредством внедрения инноваций, помогающих адаптироваться к изменяющимся условиям внешней среды и достигать организационные цели. Зачастую организационные ценности и инновации вступают в открытый конфликт друг с другом: «сопротивление изменениям со стороны сотрудников организаций сектора биотехнологий в процессе цифровой трансформации связано с неопределённостью и страхом перед будущими изменениями, а также изменением формата работы» [3, с. 126-127]. В период трансформаций для снижения повышенной тревожности необходимо введение системы оценивания труда на основе критериев эффективности для повышения прозрачности управления и оценки результативности сотрудников [4]. Дополнительно, под влиянием инноваций возникает необходимость получения вспомогательных навыков и квалификаций [5]. Повышение квалификации и профессиональная переподготовка могут рассматриваться не только как возможность профессионального саморазвития (положительное отношение), но и дополнительные затраты личных временных и финансовых ресурсов (негативное отношение). Организационная среда, ориентированная на инновации, безусловно, подчеркивает важность многозадачности, непрерывного обучения во избежание эмоционального выгорания. Принцип инновационного развития в особенности актуален для организаций, обладающих большими объемами информационных ресурсов – ИТ-компании, поставщики данных и услуг связи, государственные и научные учреждения, специализированные коммерческие фирмы и отраслевые организации.

Управление персоналом на основе ценностей предполагает эмоциональную вовлеченность сотрудников: «включение эмоциональной энергии в коммуникационные механизмы изменяет медийный фон и порождает конструктивную сопричастность в процессе преодоления кризиса» [6]. Положительный эмоциональный фон способствует повышению вовлеченности сотрудников и улучшению эффективности при выполнении текущих задач [7]. В долгосрочной перспективе организация может опираться на эмоциональный капитал как ценный нематериальный актив. К особенностям управления карьерным развитием представителей поколения Зуммеров относится возможность творческой самореализации и креативного подхода к решению организационных задач в условиях удаленного формата трудовой деятельности и снижения уровня регламентированности трудового процесса [8]. Исследователи отмечают, что «цифровые кочевники относятся к работе не как к необходимости, а как к досугу, приносящему моральное удовлетворение» [9, с. 175].

Негативный эмоциональный фон не только снижает эффективность деятельности, но и порождает социально-психологические проблемы, такие как цифровая тревожность и интернет-зависимость [10]. Актуальность изучения культуры информационной безопасности является необходимостью в контексте организации, поскольку затрагивает многие социальные аспекты, начиная от личного тайм-менеджмента, соблюдения баланса между трудовой и личной жизнью, заканчивая составлением графиком рабочего времени и формированием повседневных практик. Необходимость включения инфор-

мационной безопасности в организационную культуру обусловлена как социальной, так и цифровой средой организации.

Материал и методы

Материалом исследования послужили данные об информационной безопасности (ИБ), собранные методом сплошной выборки на сайте Elsevier [23]. Методы исследования включали семантический анализ, категоризацию и классификацию. Актуальность включения ИБ в состав организационных ценностей подтверждается многочисленными исследованиями. Проблема существенных объемов киберпреступности напрямую связана со сбоями в соблюдении политик и процедур ИБ на корпоративном уровне. Невыполнение требований ИБ, таких как слабое управление паролями (использование простых паролей, их повторное использование на разных платформах), отсутствие многофакторной аутентификации, отсутствие шифрования или несвоевременное обновление программного обеспечения усугубляют риски и тяжесть последствий для репутации компании. Игнорирование нарушений в течение длительного времени приводит к увеличению затрат на ИБ в долгосрочной перспективе. Отсутствие мониторинга безопасности, надлежащего ведения журналов и процедур реагирования на инциденты увеличивает подобные риски (*рис. 1*).

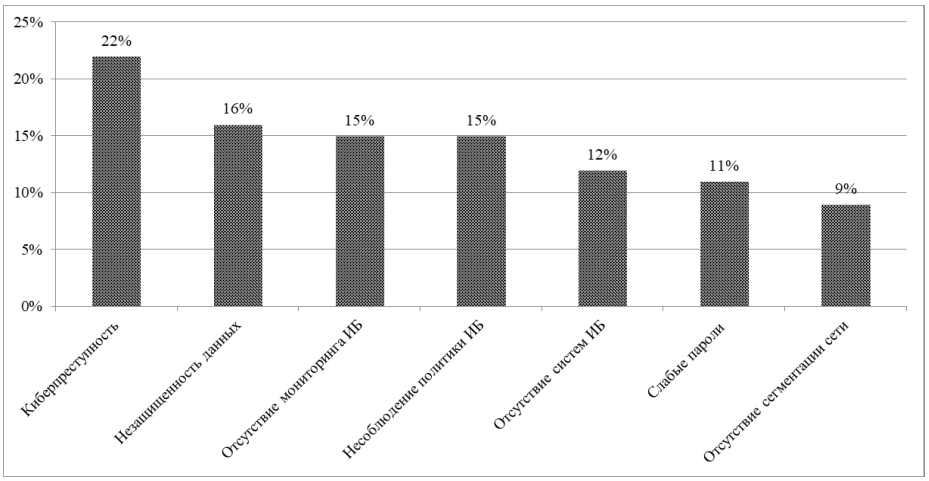

Рис. 1. Причины возникновения рисков для информационной безопасности.
Источник: составлено автором.

Сотрудники организаций становятся легкой мишенью для злоумышленников, если они не обучены распознаванию фишинговых атак, соблюдению политики безопасности и необходимости сообщения о подозрительной активности при посещении тех или иных сайтов. При отсутствии сегментации сети злоумышленники, получившие доступ к одной ее части, могут перемещаться по всей сети и получать доступ к конфиденциальным данным.

Результаты и обсуждение

Информационная безопасность как актуальная задача современных организаций

Цифровые технологии предоставляют значительные возможности для развития бизнеса с точки зрения маркетинговых коммуникаций [11], автоматизации бизнес-процессов, снижения затрат и повышения эффективности деятельности предприятий. С точки зрения управления, цифровые технологии являются основным инструментом управления и способствуют развитию управленческой деятельности в целом [12], поскольку являются фактором развития систем для учета, отчетности, анализа и планирования всех бизнес-процессов. Одновременно, они порождают социальное неравенство [13], являются причиной безработицы из-за отсутствия цифровых компетенций вследствие автоматизации ряда рабочих процедур, ранее выполняемых людьми, ограничения доступа к информации и услугам или появления новых форм контроля.

Цифровая безопасность становится ключевым фактором риска для организаций, т.к. информация является ключевым активом большинства современных компаний. От работников требуется развитие определенных мыслительных конструктов и поведенческих паттернов, позволяющих им активно использовать новые технологии и сохранять внутреннюю информацию организации [14], например, анализ преимуществ и недостатков программных средств для определения наиболее безопасного способа связи и передачи данных [15], обоснование практического значения и целе-

сообразности их использования. Ядерным элементом ИБ является цифровая гигиена [16], или комплекс мер, включающий использование сложных паролей, неразглашение личных сведений онлайн, осторожность со ссылками и незнакомыми пользователями, а также применение антивирусов. Безопасное поведение сотрудников в цифровой среде от имени компании достигается через обучение, формирование устойчивых навыков, и когнитивный подход – осознанное поведение по ограничению информации в сети и использование различных каналов связи.

Одним из наиболее ярких и сложных примеров необходимости ИБ является добыча полезных ископаемых, требующая комплексной защиты данных – конфиденциальности, целостности и доступности – от внешних и внутренних угроз [17]. Применение цифровых технологий необходимо на всех стадиях добычи полезных ископаемых для повышения эффективности производственных процессов [18], начиная от геолого-разведывательных работ и заканчивая стадией завершения, облагораживания территории и восстановления местного эко-климата. ИБ является источником производственной безопасности на подобных предприятиях. Глубокие исследования производственных процессов свидетельствуют о психологической природе безопасности [19], поскольку именно психологические модели составляют основу эффективных систем управления и повышения безопасности работников при угледобыче.

Информационная безопасность как компонент организационной культуры

Поведение сотрудников, методы принятия решений, взаимоотношения и способы выполнения задач составляют культуру организации и с течением времени формируют стереотипы о ее культуре. Общая модель ценностей, ментальных конструктов и поведенческих паттернов, типичных для сотрудников организаций, которые проявляются на протяжении длительного времени и непосредственно связаны с ИБ, определяет культуру информационной безопасности (КИБ). КИБ потенциально может быть сформирована посредством совместного обучения поведенческим навыкам в области информационных и компьютерных технологий – как менеджеров, так и сотрудников.

На практике сотрудникам необходимо в полном объеме выполнять требования менеджеров по соблюдению мер, направленных на повышение ИБ. Поведение, связанное с ИБ может быть отнесено к следующим видам: (1) поведение, направленное на обеспечение ИБ; (2) поведение, соответствующее требованиям ИБ; (3) поведение, связанное с риском для ИБ; (4) поведение, наносящее ущерб ИБ. Данные типы поведения являются индикаторами организационной культуры в отношении ИБ.

Угрозы для ИБ возникают в тех случаях, когда сотрудники открывают фишинговые электронные письма через почтовые сервисы организации, посещают вредоносные веб-сайты, подключают зараженные USB-накопители или загружают непроверенные документы на рабочие компьютеры. Опросы сотрудников, направленные на самоанализ поведения, как правило, не являются эффективными, поскольку сотрудники могут не замечать входа на фишинговые сайты, не способны распознавать их, заботясь исключительно о поиске информации. Утечка внутренней информации чревата серьезными последствиями вплоть до закрытия бизнеса.

Публичные сообщения об утечках данных часто приводят к кратковременной негативной реакции общественности. Однако гораздо более отрицательным является отсутствие легитимности – неспособности пройти проверки на безопасность, штрафы со стороны регулирующих органов и потеря бизнеса. Последствия подобных утечек поднимают вопросы о необходимости постоянного улучшения организационной кибербезопасности. Легитимность ИБ – это доверие к действиям компании в области безопасности со стороны заинтересованных сторон [20]. Исследования показывают, что организации с более высоким уровнем легитимизации в области ИБ подвержены значительно меньшим рискам в долгосрочной перспективе. Кроме того, незамедлительные публичные объявления об утечках снижают риски распространения негативной информации о компании. Постоянное улучшение ИБ повышает эффективность управления рисками. Положительными последствиями своевременным и проактивным управлением ИБ являются наем экспертов в области безопасности, внедрение новейших технологий и получение признанных в отрасли сертификатов безопасности. Следует отметить, что необходимость соответствия правилам безопасности требует существенных инвестиций со стороны руководства на соответствие нормам и стандартам [3].

Создание единой концепции в сфере ИБ направлено на разработку профилактических действий, которые, в совокупности с упреждающими внешними коммуникациями, такими как своевременные заявления в прессе, снижают долгосрочные финансовые риски и убытки для компании. Менеджерам необходимо разрабатывать практические рекомендации по соблюдению общеорганизационной безопасности, принимать оперативные меры быстрого реагирования, обе-

спечивать стратегическую легитимность, а также способствовать укреплению культуры кибербезопасности на всех уровнях управления.

Система управления ИБ – это систематический подход к контролю конфиденциальной информации, обеспечению ее секретности, целостности и доступности посредством минимизации рисков и принятию мер по обеспечению безопасности [21]. С точки зрения целостности и доступности информации, ИБ может гарантировать непрерывность бизнеса, принимая во внимание, что кибератаки способны нанести ущерб операционной деятельности организаций (*рис. 2*).

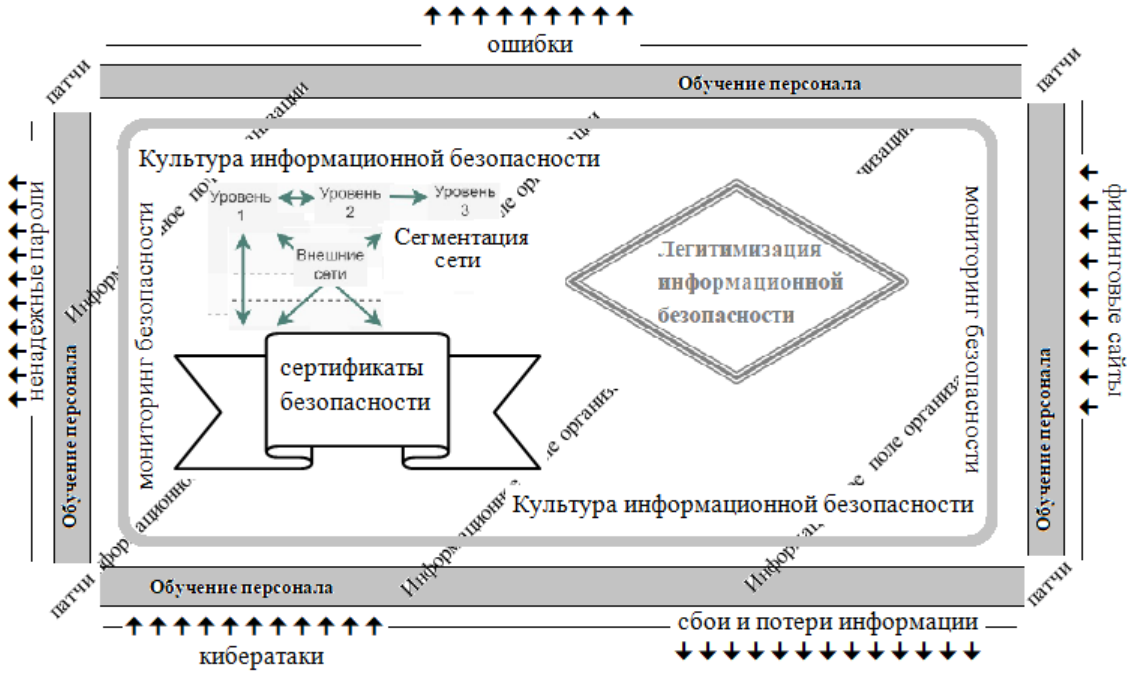

Рис. 2. Информационная безопасность как ценность организационной культуры.
Источник: составлено автором

Внедрение программ для обучения сотрудников основам ИБ, обучения менеджеров навыкам коррекции поведения сотрудников оказывает положительное влияние на профилактику киберзнарушений. Программы преследуют цели улучшения корпоративной культуры, КИБ, а также влияния на поведение сотрудников для повышения ИБ в организационной среде [22]. Подобные обучающие программы выполняют анализ поведения сотрудников и предоставляют отчеты менеджерам о рисках и негативных последствиях для организации.

Изменение поведения сотрудников при работе с информацией в интернете требует времени на распространение новых организационных ценностей и норм, формирование подходов к получению и обработке информации, внедрение новых программ и обучение сотрудников работе с соответствующими программами. Однако, прежде всего, необходимы: принятие новых инициатив на уровне руководства, имплементация стратегий работы с информацией как основополагающих принципов поведения во всех подразделениях, издание приказов и директив с назначением ответственных за контроль их исполнения во всех структурах и подразделениях.

Заключение

В современной цифровой среде ИБ перестает быть исключительно технической проблемой и переходит в разряд комплексных задач, требующих глубокой интеграции в текущую деятельность и организационную культуру учреждений и предприятий. Обеспечение конфиденциальности, целостности и доступности информации становится невозможным без активной вовлеченности персонала и формирования у сотрудников устойчивых ментальных конструктов и поведенческих паттернов, направленных на соблюдение принципов цифровой гигиены.

Непрерывное обучение распознаванию кибератак, например, фишинговых сайтов, является ключевой задачей организаций. Большинство киберпреступлений начинается с человеческой ошибки, когда сотрудник, не способный распознать приемы социальной инженерии, рас-

крывает учетные данные или запускает вредоносное программное обеспечение. Обучение, выходящее за рамки формальных инструктажей и опирающееся на интерактивные, персонализированные и регулярно проводимые занятия, способствуют аккумулированию практических навыков, противодействующих киберпреступности. Наряду с получением знаний, сотрудники организаций должны формировать критическое мышление, позволяющее им самостоятельно оценивать риски и принимать осознанные решения при возникновении киберугроз.

В дополнение к тренингам необходимы профессиональный мониторинг безопасности, установка программ, предотвращающих доступ к конфиденциальным данным и интеграция ИБ в организационную культуру предприятия:

- мониторинг безопасности – постоянный анализ лог-файлов, сетевого трафика и активности пользователей, оперативное выявление аномалий и реагирование на потенциальные угрозы;
- предотвращение доступа к конфиденциальным данным – четкое разграничение прав доступа и использование средств защиты данных;
- производственная безопасность – интеграция принципов ИБ в производственные процессы для минимизации рисков, связанных с потерей данных или несанкционированным доступом к критически важным системам.

Усилия по обеспечению ИБ должны быть легитимными и прозрачными. Сотрудники должны понимать цели и задачи политики безопасности, а также влияние их действий на общий уровень ИБ организации. Получение сертификатов безопасности служит свидетельством надежности системы управления ИБ и повышения доверия к организации со стороны клиентов и партнеров.

Эффективная система ИБ – это не только борьба с инцидентами, но и готовность к их профилактике и предупреждению. Быстрое раскрытие информации об инцидентах кибератак, грамотное управление критическими ситуациями и оперативное восстановление систем после попыток взлома позволяют минимизировать ущерб операционной деятельности организаций и предотвратить негативные реакции общественности.

Информационная безопасность – это непрерывный процесс, требующий постоянного комплексного совершенствования. Интеграция ценности ИБ в систему организационной культуры, активная вовлеченность персонала, их непрерывное обучение, использование эффективных технических средств и готовность к реагированию на инциденты являются ключевыми факторами успеха в противодействии киберпреступности и обеспечении конфиденциальности, целостности и доступности информации. Правильно выстроенная стратегия ИБ не только защищает активы организации, но и способствует повышению доверия и укреплению ее репутации.

Список литературы:

[1] Абера, Т.Б. Влияние организационной культуры на формирование поведения персонала учреждений высшего образования (на примере университета Гондэра, Эфиопия) / Т.Б. Абера, Ж.А. Мингалева // Управление. – 2024. – Т. 12, № 4. – С. 60–69. – DOI: 10.26425/2309-3633-2024-12-4-60-69. – EDN: KBFTEY.

[2] Ворожихин, В.В. Система ценностей в инновационном развитии стран / В.В. Ворожихин, Е.И. Ларионова, А.А. Юрьева // Гуманитарные науки. Вестник Финансового университета. – 2025. – № 4(15). – С. 6–22. – DOI: 10.26794/2226-7867-2025-15-4-6-22. – EDN: NOBUUR.

[3] Штанский, А.Д. Цифровая трансформация организаций сектора биотехнологий как фактор инновационного развития / А.Д. Штанский, А.В. Желтенков // Вестник Государственного университета просвещения. Серия: Экономика. – 2025. – № 2. – С. 122–131. – DOI: 10.18384/2949-5024-2025-2-122-131. – EDN: ULKEEI.

[4] Филясова, Ю.А. Перфекционизм и рационально-эмотивное поведение как мотивационная политика управления персоналом // Управление. – 2022. – Т. 10. – № 1. – С. 16–27. – DOI: 10.26425/2309-3633-2022-10-1-16-27. – EDN: WWRVYP.

[5] Митрофанова, Е.А. Концептуальный подход к формированию и развитию человеческого капитала образовательных организаций высшего образования / Е.А. Митрофанова, О.С. Сувалов // Управление. – 2025. № 2 (13). – С. 25–41. – DOI: 10.26425/2309-3633-2025-13-2-25-41. – EDN: QAWNIO.

[6] Василенко, Л.А. Эмоции в коммуникационных механизмах управления / Л.А. Василенко, Е.А. Скачилова // Информационное общество. – 2025. – № 2. – С. 64–74. – DOI: 10.52605/16059921_2025_02_64. – EDN: GPJQAT.

[7] Filyasova, Yu.A. A semantic field of perfectionism as a social and psychological concept in academic discourse // RUDN Journal of Language Studies, Semiotics and Semantics. – 2022. – Vol. 13, No. 2. – P. 382–395. – DOI: 10.22363/2313-2299-2022-13-2-382-395. – EDN: EBBYEC.

[8] Литвинюк, А.А. Особенности мотивации карьерного развития поколения Z и их влияние на HR-менеджмент / А.А. Литвинюк, В.В. Сологуб // Лидерство и менеджмент. – 2025. № 9(12). – С. 1945–1960. – DOI: 10.18334/lim.12.9.123726. – EDN: AIDNZA.

[9] Шорникова, Н.Ю. Формирование профессиональных качеств работников в цифровой экономике // Социально-трудовые исследования. – 2025. – № 1(58). – С. 169–177. – DOI: 10.34022/2658-3712-2025-58-1-169-177. – EDN: IHRHMQ.

[10] Гасанова, З.Б. Влияние цифровой среды, интернет-зависимости и цифровой тревожности на культуру информационной безопасности у менеджеров поколения Z / З.Б. Гасанова, М.И. Гасанов // Цифровая социология. – 2025. – № 3(8). – С. 34–43. – DOI: 10.26425/2658-347X-2025-8-3-34-43. – EDN: LZQGUM.

[11] Завражных, О.В. Инструменты цифрового маркетинга на рынке автозапчастей // Наукосфера. – 2025. – No. 10-1. – P. 188–194. – DOI: 10.5281/zenodo.17358104. – EDN: FJNZRY.

[12] Мкртумова, И.В. Влияние цифровизации на международную информационную безопасность и социальные риски управленческих процессов / И.В. Мкртумова, С.С. Прокопьева // Цифровая социология. – 2025. – № 2(8). – С. 77–86. – DOI: 10.26425/2658-347X-2025-8-2-77-86. – EDN: MOTLAC.

[13] Нагайник, А.А. Цифровизация институтов потребления как ответ на социальные ограничения // Социология. – 2025. – № 8. – С. 126–132. – EDN: LHUHGF.

[14] Золин, И.Е. Цифровизация как фактор динамики рынка труда / И.Е. Золин, М.К. Кобыляцкий // Социальные и гуманитарные знания. – 2024. – № 3(10). – С. 314–325. – DOI: 10.18255/2412-6519-2024-3-314-325. – EDN: KVFCNG.

[15] Matrokhina, K.V. Ensuring information security in corporate communication systems / K.V. Matrokhina, A.B. Makhovikov, E.N. Trofimets // E3S Web of Conferences. 2021. Vol. 266. – P. 09001. – DOI: 10.1051/e3sconf/202126609001. – EDN: NYFDTT.

[16] Милушев, Э.Х. Методы и технологии цифровой гигиены для защиты персональных данных пользователей / Э.Х. Милушев, В.С. Киселева, С.С. Багиева // Гуманитарный научный вестник. – 2025. – № 10. – С. 104–109. – DOI: 10.5281/zenodo.17647946. – EDN: MQWTNN.

[17] Маховиков, А.Б. Цифровые технологии при добыче твёрдых полезных ископаемых в Арктике / А.Б. Маховиков, Ю.А. Филясова // Устойчивое развитие горных территорий. – 2024. – Т. 16, № 3(61). – С. 1110–1117. – DOI: 10.21177/1998-4502-2024-16-3-1110-1117. – EDN: JGVYBO.

[18] Filyasova, Yu.A. Effectiveness vs. efficiency: an analysis of valency and collocability in a technical context // RUDN Journal of Language Studies, Semiotics and Semantics. – 2019. – Vol. 10, No. 1. – P. 187–196. – DOI: 10.22363/2313-2299-2019-10-1-187-196. – EDN: FOKJKB.

[19] Невская, Е.Е. Информационные технологии для систематизации способов повышения безопасности в угольных шахтах / Е.Е. Невская, Д.А. Медведев, А.Б. Маховиков, Ю.А. Филясова // Устойчивое развитие горных территорий. – 2025. – Т. 17. № 2(64). – С. 627–635. – DOI 10.21177/1998-4502-2025-17-2-627-635. – EDN IDIBIZ.

[20] Shaikh, F.A. Reassessing information security perceptions following a data breach announcement: The role of post-breach management in firm-specific risk / F.A. Shaikh, D. Joseph, E. Kang // Computers & Security. – 2026. – №161. – 104752. – DOI: 10.1016/j.cose.2025.104752.

[21] Mirtsch, M. Certification as a compensation mechanism for weak regulation? Exploring the diffusion of the international standard ISO/IEC 27001 for information security management / J. Pohlisch, K. Blind // Computers & Security. – 2026. – №162. – 104774. – DOI: 10.1016/j.cose.2025.104774.

[22] Grill, M. Training for improved information security culture: a longitudinal randomized controlled trial / M. Grill, T. Sommestad, H. Karlzén, A. Pousette // Information and Computer Security. – 2025. – №5(33). – P. 690–718. – DOI: 10.1108/ICS-08-2024-0189.

[23] Information security [Electronic resource]. URL: sciencedirect.com (дата обращения: 12.09.2025)

References:

[1] Abera T.B., Mingaleva Zh.A. Impact of organisational culture on the formation of behaviour of personnel in higher education institutions (case study of the university of Gondar, Ethiopia) // Upravlenie. 2024. no. 4(12). pp. 60–69. DOI: 10.26425/2309-3633-2024-12-4-60-69.

[2] Vorozhikhin V.V., Larionova E., Yuryeva A.A. The system of values in the innovative development of countries // Humanities and Social Sciences. Bulletin of the Financial University. 2025. no. 4(15). pp. 6–22. DOI: 10.26794/2226-7867-2025-15-4-6-22.

[3] Shtansky A.D., Zheltenkov A.V. Digital transformation of biotechnology sector organizations as a factor of innovative development // Bulletin of State University of Education. Series: Economics. 2025. no. 2. pp. 122–131. DOI: 10.18384/2949-5024-2025-2-122-131.

[4] Filyasova Yu.A. Perfectionism and rational-emotive behaviour as a motivational policy for human resource management // Upravlenie. 2022. no. 1(10). pp. 16–27. DOI: 10.26425/2309-3633-2022-10-1-16-27.

[5] Mitrofanova E.A., Suvalov O.S. A Conceptual Approach To Forming And Developing Human Capital In Higher Education Institutions // Upravlenie. 2025. no. 2 (13). pp. 25–41. DOI: 10.26425/2309-3633-2025-13-2-25-41.

[6] Vasilenko L.A., Scachilova E.A. Emotions in communication mechanisms of management // Information Society. 2025. no. 2. pp. 64–74. DOI: 10.52605/16059921_2025_02_64.

[7] Filyasova Yu.A. A semantic field of perfectionism as a social and psychological concept in academic discourse // RUDN Journal of Language Studies, Semiotics and Semantics. 2022. no. 2(13). pp. 382–395. – DOI: 10.22363/2313-2299-2022-13-2-382-395.

[8] Litvinyuk A.A., Sologub V.V. Particularities of career development motivation of generation Z and their impact on HR management // Leadership and Management. 2025. no. 9(12). pp. 1945–1960. DOI: 10.18334/lim.12.9.123726.

[9] Shornikova N.Yu. Formation of professional qualities of employees in the digital economy // Social & Labor Research. 2025. no. 1(58). pp. 169–177. DOI: 10.34022/2658-3712-2025-58-1-169-177.

[10] Gasanova Z.B., Gasanov M.I. The impact of digital environment, internet addiction, and digital anxiety on information security culture among generation Z managers // Digital Sociology. 2025. no. 3(8). pp. 34–43. DOI: 10.26425/2658-347X-2025-8-3-34-43.

[11] Zavrazhnykh O. V. Digital marketing techniques for the autoparts market // Naukosfera. 2025. no. 10-1. pp. 188–194. DOI: 10.5281/zenodo.17358104.

[12] Mkrtumova I.V., Prokopyeva S.S. Impact of digitalisation on international information security and social risks of management processes // Digital Sociology. 2025. no. 2(8). pp. 77–86. DOI: 10.26425/2658-347X-2025-8-2-77-86.

[13] Nagaynik A.A. Digitalization of consumer institutions as a response to social restrictions // Sociology. 2025. no. 8. pp. 126–132.

[14] Zolin I.E., Kobylyatskiy M.K. Digitalization as a factor of labor market dynamics // Social'nye I Gumanitarnye Znania. 2024. no. 3(10). pp. 314–325. DOI: 10.18255/2412-6519-2024-3-314-325.

[15] Matrokhina K.V., Makhovikov A.B., Trofimets E.N. Ensuring information security in corporate communication systems // E3S Web of Conferences. 2021. Vol. 266. P. 09001. DOI: 10.1051/e3sconf/202126609001.

[16] Milushev E.Kh., Kiseleva V.S., Bagieva S.S. Digital Hygiene methods and technologies to protect users' personal data // Humanitarian Scientific Bulletin. 2025. no. 10. pp. 104–109. DOI: 10.5281/zenodo.17647946.

[17] Makhovikov A.B., Filyasova Yu.A. Information technologies for solid mineral extraction in the arctic // Sustainable Development of Mountain Territories. 2024. vol. 16. no. 3(61). pp. 1110–1117. DOI: 10.21177/1998-4502-2024-16-3-1110-1117.

[18] Filyasova Yu.A. Effectiveness vs. efficiency: an analysis of valency and collocability in a technical context // RUDN Journal of Language Studies, Semiotics and Semantics. 2019. no. 1(10). pp. 187–196. DOI: 10.22363/2313-2299-2019-10-1-187-196.

[19] Nevskaia E.E., Medvedev D.A., Makhovikov A.B., Filyasova Yu.A. Information technologies for systematization of methods improving safety in coal mines // Sustainable Development of Mountain Territories. 2025. vol. 17. no. 2(64). pp. 627–635. DOI: 10.21177/1998-4502-2025-17-2-627-635.

[20] Shaikh F.A., Joseph D., Kang E. Reassessing information security perceptions following a data breach announcement: The role of post-breach management in firm-specific risk // Computers & Security. 2026. no. 161. 104752. DOI: 10.1016/j.cose.2025.104752.

[21] Mirtsch M., Pohlisch J., Blind K. Certification as a compensation mechanism for weak regulation? Exploring the diffusion of the international standard ISO/IEC 27001 for information security management // Computers & Security. 2026. no. 162. 104774. DOI: 10.1016/j.cose.2025.104774.

[22] Grill M., Sommestad T., Karlzén H., Pousette A. Training for improved information security culture: a longitudinal randomized controlled trial // Information and Computer Security. 2025. no. 5(33). pp. 690–718. DOI: 10.1108/ICS-08-2024-0189.

[23] Information security [Electronic resource]. URL: sciencedirect.com (дата обращения: 12.09.2025)