

Научная статья**УДК 378.147:004.056****DOI: 10.25683/VOLBI.2026.75.1590****Natalia Yurievna Evsyukova**

Candidate of Pedagogy, Associate Professor,
Director,
Volga Institute (branch)
of Moscow Automobile and Road Construction
State Technical University (MADI)
Cheboksary, Russian Federation
natalyaevsvfmadi@mail.ru

Svetlana Anatolyevna Solovyova

Candidate of Psychology,
Associate Professor of the Department of Computer Science
and Transport Process Technologies,
Volga Region Institute (branch)
of Moscow Automobile and Road Construction State
Technical University (MADI)
Cheboksary, Russian Federation
svetlanasol@yandex.ru

Anzhelika Vyacheslavovna Galyna

Candidate of Pedagogy,
Associate Professor of the Department of Computer Science
and Transport Process Technologies,
Volga Region Institute (branch)
of Moscow Automobile and Road Construction State
Technical University (MADI)
Cheboksary, Russian Federation
slavnaya0303@yandex.ru

Наталья Юрьевна Евсюкова

канд. пед. наук, доцент,
директор,
Приволжский институт (филиал)
Московского автомобильно-дорожного
государственного технического университета (МАДИ)
Чебоксары, Российская Федерация
natalyaevsvfmadi@mail.ru

Светлана Анатольевна Соловьёва

канд. психол. наук,
доцент кафедры «Информатика
и технологии транспортных процессов»,
Приволжский институт (филиал)
Московского автомобильно-дорожного
государственного технического университета (МАДИ)
Чебоксары, Российская Федерация
svetlanasol@yandex.ru

Анжелика Вячеславовна Галыня

канд. пед. наук,
доцент кафедры «Информатика
и технологии транспортных процессов»,
Приволжский институт (филиал)
Московского автомобильно-дорожного
государственного технического университета (МАДИ)
Чебоксары, Российская Федерация
slavnaya0303@yandex.ru

ДИАГНОСТИКА И РАЗВИТИЕ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ У СТУДЕНТОВ ТЕХНИЧЕСКОГО ВУЗА

5.8.7 — Методология и технология профессионального образования

Аннотация. В статье представлено исследование, посвященное проблеме диагностики и развития культуры информационной безопасности (КИБ) у студентов технического вуза. Цель работы заключается в выявлении уровня сформированности компонентов КИБ у студентов I–IV курсов и разработке на этой основе модели ее развития в условиях цифровой трансформации образования. Материалами исследования послужили теоретические положения отечественных ученых о структуре КИБ, а также эмпирические данные, полученные в ходе диагностики 186 студентов Приволжского института (филиала) Московского автомобильно-дорожного государственного технического университета. Методологической базой выступил компонентный подход М. А. Кулебяева, включающий ценностно-смысловой, когнитивный, технический и поведенческий компоненты КИБ. Для диагностики использовался авторский опросник, реализованный в рамках компьютерной системы обучения и контроля знаний (Свидетельство о государственной регистрации программы для ЭВМ № 2025618076). Методы исследования: теоретический анализ, педагогическое тестирование, анкетирование, методы математической статистики. Авторами

показано, что наиболее высокий уровень сформированности у студентов технического вуза наблюдается по когнитивно-му (73,5 %) и техническому (72 %) компонентам, тогда как ценностно-смысловой (53,25 %) и поведенческий (50,75 %) компоненты находятся на недостаточном уровне, что создает «разрыв» между знанием и действием в области информационной безопасности, достигающий 22,75 процентных пункта. На основе полученных данных авторами предложена модель формирования КИБ, включающая диагностический, содержательно-процессуальный и оценочно-рефлексивный блоки, с акцентом на аксиолого-поведенческий модуль. Выводы: для эффективного развития КИБ у студентов технического вуза необходима системная работа, направленная на аксиологизацию содержания образования и активизацию поведенческих практик в цифровой среде.

Ключевые слова: культура информационной безопасности, студенты технического вуза, диагностика, ценностно-смысловой компонент, когнитивный компонент, технический компонент, поведенческий компонент, модель формирования, цифровая образовательная среда, образовательный процесс

Для цитирования: Евсюкова Н. Ю., Соловьёва С. А., Галыня А. В. Диагностика и развитие культуры информационной безопасности у студентов технического вуза // Бизнес. Образование. Право. 2026. № 2(75). С. 410–415. DOI: 10.25683/VOLBI.2026.75.1590.

Original article

DIAGNOSTICS AND DEVELOPMENT OF INFORMATION SECURITY CULTURE
AMONG STUDENTS OF A TECHNICAL UNIVERSITY

5.8.7 — Methodology and technology of vocational education

Abstract. *The authors of the article present a study on the problem of diagnosis and development of information security culture among students of a technical university. The purpose of the work is to identify the level of formation of information security culture components among 1st-4th year students and to develop on this basis a model of its development in the context of digital transformation of education. The research materials were the theoretical positions of Russian scientists on the structure of information security culture, as well as empirical data obtained during the diagnosis of 186 students of the Volga Institute (branch) of MADI. The methodological basis was M. A. Kulebyaev's component approach, which includes value-semantic, cognitive, technical and behavioral components of information security culture. The author's questionnaire was used for diagnostics, implemented within the framework of a computer learning and knowledge control system (Certificate of state registration of a computer program No. 2025618076). Research methods were theoretical analysis, pedagogical testing, questionnaires, and methods of mathematical statistics. The authors show*

that the highest level of education among technical university students is observed in cognitive (73.5%) and technical (72%) components, while the value-semantic (53.25%) and behavioral (50.75%) components are at an insufficient level, which creates a "gap" between knowledge and action in the field of information security, reaching 22.75%. Based on the data obtained, the authors propose a model for development of information security culture, including diagnostic, substantive-procedural and evaluative-reflexive blocks, with an emphasis on the axiological-behavioral module. It is concluded that for the effective development of information security culture among students of a technical university, systematic work is needed aimed at axiologizing the content of education and activating behavioral practices in the digital environment.

Keywords: *information security culture, technical university students, diagnostics, value-semantic component, cognitive component, technical component, behavioral component, development model, digital educational environment, educational process*

For citation: Evsyukova N. Yu., Solovyova S. A., Galyna A. V. Diagnostics and development of information security culture among students of a technical university. *Biznes. Obrazovanie. Pravo = Business. Education. Law.* 2026;2(75):410—415. DOI: 10.25683/VOLBI.2026.75.1590.

Введение

Актуальность. В эпоху цифровой трансформации всех сфер общественной жизни проблема обеспечения информационной безопасности (далее — ИБ) приобретает не только техническое, но и глубокое социально-педагогическое измерение. Особую уязвимость в киберпространстве демонстрирует студенческая молодежь, чья учебная, профессиональная и личная коммуникация практически полностью опосредована цифровыми технологиями. Т. Д. Андреева отмечает, что формирование культуры ИБ (далее — КИБ) выступает важнейшим элементом механизма обеспечения безопасности личности, общества и государства [1]. При этом, как подчеркивает И. Р. Бегишев, КИБ представляет собой сложный психолого-правовой феномен, выходящий за рамки простой совокупности технических навыков и включающий ценностные ориентации, мотивационные установки и поведенческие паттерны [2].

В условиях подготовки инженерных кадров для критически важных отраслей (транспорт, энергетика, связь) уровень КИБ выпускника технического вуза напрямую влияет на надежность и защищенность национальной инфраструктуры. П. Г. Былевский в своих работах акцентирует внимание на культурологических аспектах профессиональной КИБ [3] и показывает, что ее формирование определяется не только организационно-техническими, но и социокультурными факторами [4]. Однако, как свидетельствует практика, традиционная система высшего технического образования ориентирована преимущественно на передачу знаний и отработку алгоритмических действий, оставляя в стороне ценностно-смысловую и поведенческую составляющие. Данное противоречие и определяет актуальность настоящего исследования.

Изученность проблемы. Проблема диагностики и развития КИБ нашла отражение в работах отечественных и зарубежных авторов. Е. В. Ворopaева и А. В. Бредихина рассматривают формирование и развитие КИБ несовершеннолетних как основу профилактики девиантного поведения в цифровой среде [5]. А. К. Дубень исследует информационную культуру молодежи в контексте правового механизма обеспечения безопасности, подчеркивая нормативно-регулятивную функцию КИБ [6]. Т. А. Изосимова и М. А. Кулебяев связывают роль ИБ с обеспечением национальной безопасности, что придает теме государственную значимость [7].

А. К. Иманов и Ж. А. Атыгаев анализируют цифровую культуру обучающихся в контексте ИБ личности, выделяя факторы риска и ресурсы защиты [8]. О. Ю. Кичигина поднимает вопросы формирования КИБ у обучающихся в высшей школе, констатируя недостаточную разработанность методического обеспечения этого процесса [9]. К. А. Кряжевских показывает прямое влияние информационной культуры на уровень ИБ, что подтверждает необходимость целенаправленного педагогического воздействия [10].

Ключевые теоретические и эмпирические результаты получены М. А. Кулебяевым, который не только уточнил феномен КИБ в трактовке отечественных и зарубежных авторов [11], но и предложил четырехкомпонентную структуру (ценностно-смысловой, когнитивный, технический, поведенческий) и разработал валидированный диагностический инструментарий [12]. В. М. Литвишков и Б. А. Швырев рассматривают социологические аспекты КИБ, акцентируя роль общественного мнения и групповых норм [13]. А. А. и З. П. Малоки обосновывают необходимость создания системы массового обучения КИБ,

охватывающей все уровни образования [14]. Д. А. Попов фокусируется на развитии КИБ подростков в условиях общеобразовательной школы [15].

И. Д. Рудинский и Д. Я. Околот уточняют понятие и содержание КИБ, вводя различие между обыденным и профессиональным уровнями культуры [16]. А. А. Смирнов и М. В. Румянцева выделяют системные проблемы формирования КИБ граждан Российской Федерации, включая низкую мотивацию и отсутствие обратной связи [17]. Б. А. Швырев и П. Н. Казберов описывают педагогический процесс формирования КИБ как целенаправленную, поэтапную деятельность [18]. Ю. В. Яковлева устанавливает взаимосвязь КИБ и информационной культуры, показывая, что первая является условием реализации второй [19].

Несмотря на значительный теоретический аспект, эмпирических исследований, посвященных комплексной диагностике всех компонентов КИБ у студентов технических вузов с последующим проектированием развивающих моделей, недостаточно. Особенно это касается региональных филиалов столичных вузов, где сочетаются инженерная подготовка и местные социокультурные особенности.

Целесообразность разработки темы обусловлена следующими факторами. Во-первых, выявленное в ходе нашего пилотажного исследования противоречие между относительно высоким уровнем когнитивного (73,5 %) и технического (72 %) компонентов КИБ и низким уровнем ценностно-смыслового (53,25 %) и поведенческого (50,75 %) компонентов свидетельствует о феномене «дивергенции компетенций» — разрыве между знанием и действием. Традиционные методы обучения (лекции, лабораторные работы) эффективны для первых двух компонентов, но не решают проблему интериоризации ценностей и формирования устойчивых привычек безопасного поведения. Во-вторых, специфика Приволжского филиала Московского автомобильно-дорожного государственного технического университета (МАДИ) как регионального центра подготовки кадров для транспортной отрасли требует учета профессиональных рисков: цифровые системы управления транспортом и телематика становятся объектами кибератак, поэтому КИБ выпускника выступает фактором профессиональной надежности. В-третьих, анализ литературы и практики показывает отсутствие системных, апробированных моделей формирования КИБ, ориентированных именно на студентов технического вуза и учитывающих выявленный дисбаланс компонентов. Таким образом, разработка диагностического инструментария и модели развития КИБ является своевременной и востребованной.

Научная новизна исследования заключается в выявлении специфики сформированности компонентов КИБ у студентов технического вуза (Приволжский филиал МАДИ) и в разработке структурно-функциональной модели развития КИБ, ориентированной на коррекцию дефицитарных (ценностно-смыслового и поведенческого) компонентов.

Цель исследования — на основе диагностики уровня сформированности компонентов КИБ у студентов технического вуза разработать и обосновать модель ее развития.

Задачи исследования:

1. Провести диагностику ценностно-смыслового, когнитивного, технического и поведенческого компонентов КИБ у студентов I—IV курсов.
2. Выявить компоненты с недостаточным уровнем сформированности.
3. Разработать модель формирования КИБ, направленную на развитие дефицитарных компонентов.

Теоретическая значимость заключается в уточнении и дополнении понятия КИБ применительно к студенту технического вуза, где КИБ рассматривается как профессионально значимое качество будущего инженера, работающего с критической информационной инфраструктурой, что развивает положения П. Г. Былевского о профессиональной КИБ [3] и М. А. Кулебяева о феномене КИБ [11]. Кроме того, расширено научное представление о структуре КИБ за счет эмпирического выявления феномена дивергенции между когнитивно-техническим и ценностно-смыслово-поведенческим компонентами, что вносит вклад в педагогическую психологию и демонстрирует ограниченность сугубо когнитивистского подхода к формированию безопасного поведения в цифровой среде.

Практическая значимость исследования определяется возможностью непосредственного применения его результатов в образовательном процессе: предложенный диагностический инструментарий М. А. Кулебяева и С. Н. Федоровой («Компьютерная система обучения и контроля знаний “Культура информационной безопасности студентов технических вузов в цифровой образовательной среде”»); свидетельство о государственной регистрации программы для ЭВМ № 2025618076) может быть использован в любом техническом вузе для первичной, промежуточной и итоговой оценки уровня сформированности КИБ у студентов, что позволяет осуществлять мониторинг и своевременную коррекцию образовательных программ; разработанная модель формирования КИБ подлежит непосредственному внедрению в учебный процесс Приволжского филиала МАДИ и других транспортных вузов, причем предлагаемые формы работы (кейс-стади реальных киберинцидентов в транспортной отрасли, тренинги безопасного цифрового поведения, практикум «цифровое волонтерство», рефлексивная практика «Дневник цифровых привычек») могут быть включены в рабочие программы дисциплин («Информатика», «Безопасность жизнедеятельности», «Информационная безопасность», курсы по выбору) без существенного увеличения учебной нагрузки.

Основная часть

Методология исследования. Исследование базируется на теоретическом положении М. А. Кулебяева о том, что КИБ включает четыре взаимосвязанных компонента: ценностно-смысловой (осознание ценности информации и мотивация к ее защите), когнитивный (система знаний об угрозах и способах защиты), технический (владение программно-аппаратными средствами защиты) и поведенческий (реализация безопасных практик в цифровой среде). На основе разработанного им опросника («Компьютерная система обучения и контроля знаний “Культура информационной безопасности студентов технических вузов в цифровой образовательной среде”») были выявлены эти компоненты.

Выборка исследования составила 186 студентов I—IV курсов Приволжского института (филиал) МАДИ, обучающихся по направлениям подготовки, связанным с эксплуатацией транспортно-технологических машин и комплексов, а также информационными системами. Исследование проводилось в 2024–2025 учебном году. Методы: теоретический анализ литературы, педагогическое тестирование, анкетирование, методы описательной статистики (расчет средних значений, процентного распределения).

Результаты исследования. В ходе диагностики были получены следующие результаты (см. табл.).

Уровень сформированности компонентов КИБ у студентов (в % от максимально возможного балла по компоненту)

Компонент КИБ	I курс (n = 48)	II курс (n = 47)	III курс (n = 46)	IV курс (n = 45)	Среднее
Ценностно-смысловой	48	52	55	58	53,25
Когнитивный	62	71	78	83	73,5
Технический	58	69	76	85	72
Поведенческий	42	49	53	59	50,75

Представленные данные свидетельствуют о наличии выраженной диспропорции в формировании компонентов КИБ. Наиболее высокие показатели зафиксированы по **когнитивному** (73,5 %) и **техническому** (72 %) компонентам. Это объясняется спецификой обучения в техническом вузе: студенты получают значительный объем знаний в области информатики, программирования, технических средств защиты информации. Однако эти знания носят преимущественно формальный характер, что подтверждается более низкими показателями поведенческого компонента.

Ключевой проблемой, выявленной в ходе исследования, является недостаточная сформированность **ценностно-смыслового** (53,25 %) и **поведенческого** (50,75 %) компонентов. Разрыв между когнитивным и поведенческим компонентами составляет в среднем 22,75 процентных пункта. Это означает, что студент *знает* об угрозах и способах защиты, но не *применяет* эти знания в повседневной практике (использует слабые пароли, игнорирует двухфакторную аутентификацию, переходит по подозрительным ссылкам). Недостаточная сформированность ценностно-смыслового компонента указывает на то, что соблюдение норм ИБ не становится для студента личностно значимой ценностью.

Полученные результаты подтверждают гипотезу о том, что традиционное обучение ИБ в техническом вузе, акцентирующее передачу знаний и технических навыков, не обеспечивает полноценного формирования КИБ. Необходимо переход к педагогическим стратегиям, направленным на аксиологизацию содержания и интериоризацию безопасных поведенческих норм.

На основе полученных результатов нами разработана структурно-функциональная модель формирования КИБ, ориентированная на устранение выявленных дефицитов. Модель включает четыре блока: целевой, диагностический, содержательно-процессуальный и оценочно-рефлексивный.

Целевой блок определяет стратегическую цель — формирование гармоничной КИБ студента как интегративного личностного качества, обеспечивающего безопасное взаимодействие в цифровой среде. Задачи: развитие ценностного отношения к ИБ, углубление знаний, совершенствование технических навыков и, что наиболее важно, формирование устойчивых безопасных поведенческих привычек.

Диагностический блок включает первоначальную, промежуточную и итоговую диагностику всех четырех компонентов КИБ с использованием валидизированного

опросника М. А. Кулебяева [11]. На этапе проектирования модели результаты первичной диагностики (см. табл.) служат отправной точкой.

Содержательно-процессуальный блок — ядро модели. Его реализация предполагает:

1) для развития *ценностно-смыслового компонента*: включение в дисциплины («Безопасность жизнедеятельности», «Информатика») кейсов реальных киберинцидентов с анализом последствий для личности, обсуждение этических дилемм ИБ, использование проектного метода (создание студентами памяток и видеороликов о ценности информации);

2) для развития *когнитивного компонента*: углубление знаний через модуль «Культура информационной безопасности» в рамках курса по выбору, лекции приглашенных специалистов-практиков, анализ нормативно-правовых документов;

3) для развития *технического компонента*: лабораторные практикумы по настройке средств защиты (антивирусы, брандмауэры), обучение методам криптографической защиты данных;

4) для развития *поведенческого компонента (ключевой акцент)*: внедрение тренингов безопасного поведения (отработка действий при фишинговой атаке, управление паролями), «цифрового волонтерства» (помощь младшим курсам и преподавателям в вопросах ИБ), ведение «Дневника цифровых привычек» с самоанализом поведения в сети. Обязательным элементом выступает создание ситуаций успешного безопасного поведения и их рефлексия.

Оценочно-рефлексивный блок предполагает не только контрольный срез уровня компонентов КИБ, но и самооценку студентом динамики своего поведения, формирование рефлексивной позиции. Критерии эффективности: положительная динамика по всем компонентам, снижение разрыва между когнитивным и поведенческим компонентами, повышение уровня мотивации к соблюдению норм ИБ.

Предложенная модель реализует принципы системности, личностно-деятельностного подхода и междисциплинарности.

Заключение и выводы

Проведенное исследование позволило получить следующие основные результаты и сформулировать выводы.

В результате диагностики студентов Приволжского филиала МАДИ установлено, что компоненты КИБ сформированы неравномерно. Наиболее высокие показатели демонстрируют когнитивный (73,5 %) и технический (72 %) компоненты, что отражает сильные стороны технического образования в области информатики.

Выявлены дефицитарные компоненты: ценностно-смысловой (53,25 %) и поведенческий (50,75 %). Установлен значительный «разрыв» между знанием и действием (в среднем 22,75 %), что указывает на формальный характер усвоения знаний и отсутствие устойчивых практик безопасного поведения.

Для преодоления выявленных недостатков разработана модель формирования КИБ, которая, в отличие от существующих, делает акцент на аксиологизации содержания образования и системной поведенческой тренировке. Ключевыми элементами модели являются: диагностический блок на основе валидизированного инструментария; содержательно-процессуальный блок с тренингами, кейсами и «цифровым волонтерством»; оценочно-рефлексивный блок, стимулирующий самоанализ.

СПИСОК ИСТОЧНИКОВ

1. Андреева Т. Д. Формирование культуры информационной безопасности как важнейшего элемента механизма обеспечения безопасности личности, общества и государства // Алтайский юридический вестник. 2025. № 4(52). С. 58—64.
2. Бегишев И. Р. Культура информационной безопасности: психолого-правовой аспект // Психология и право. 2021. Т. 11. № 4. С. 207—220. DOI: 10.17759/psylaw.2021110415.
3. Былевский П. Г. Культурологические аспекты профессиональной культуры информационной безопасности // Культура и искусство. 2023. № 8. С. 39—49. DOI: 10.7256/2454-0625.2023.8.43846.
4. Былевский П. Г. Эволюция культуры информационной безопасности: организационно-технические и социокультурные факторы // Вестник современных цифровых технологий. 2025. № 24. С. 22—29.
5. Воропаева Е. В., Бредихина А. В. Формирование и развитие культуры информационной безопасности несовершеннолетних в Российской Федерации // Universum: психология и образование. 2025. № 11(137). С. 20—22. DOI: 10.32743/UniPsy.2025.137.11.20961.
6. Дубень А. К. Информационная культура молодежи как правовой механизм обеспечения безопасности // Аграрное и земельное право. 2024. № 5(233). С. 119—121.
7. Изосимова Т. А., Кулебяев М. А. Роль информационной безопасности в обеспечении национальной безопасности // Развитие экономики (на микро- и макроуровнях) на основе обеспечения безопасности в сфере ПОД/ФТ/ФРОМУ : сб. науч. ст. по материалам Междунар. конф. преподавателей и студентов : в 2 т. М. : МФЮА, 2024. Т. 1. С. 453—457.
8. Иманов А. К., Атыгаев Ж. А. Цифровая культура обучающихся в контексте информационной безопасности личности // Научные инновации. 2025. № 1(1). С. 44—50.
9. Кичигина О. Ю. Вопросы формирования культуры информационной безопасности у обучающихся в высшей школе // Теория и практика социогуманитарных наук. 2023. № 4(24). С. 14—22.
10. Кряжевских К. А. Влияние информационной культуры на уровень информационной безопасности // Вопросы российской юстиции. 2023. № 24. С. 568—573.
11. Кулебяев М. А. Феномен культуры информационной безопасности в трактовке отечественных и зарубежных авторов // Казанская наука. 2024. № 7. С. 71—76.
12. Кулебяев М. А. Культура информационной безопасности студентов технического вуза: диагностический аспект // Мир науки. Педагогика и психология. 2025. Т. 13. № 4. URL: <https://mir-nauki.com/PDF/29PDMN425.pdf>.
13. Литвишков В. М., Швырев Б. А. Социологические аспекты культуры информационной безопасности // Уголовно-исполнительная система: право, экономика, управление. 2020. № 2. С. 38—40.
14. Малюк А. А., Малюк З. П. Актуальные вопросы создания системы массового обучения культуре информационной безопасности // Безопасность информационных технологий. 2021. Т. 28. № 4. С. 6—21.
15. Попов Д. А. Развитие культуры информационной безопасности подростков // Наука. Управление. Образование. РФ. 2024. № 2(14). С. 83—87.
16. Рудинский И. Д., Околот Д. Я. Культура информационной безопасности. Понятие и содержание // Информатизация образования и науки. 2020. № 3(47). С. 39—44.
17. Смирнов А. А., Румянцева М. В. Проблемы формирования культуры информационной безопасности граждан Российской Федерации // Правовая информатика. 2025. № 3. С. 154—163. DOI: 10.24412/1994-1404-2025-3-00-16.
18. Швырев Б. А., Казберов П. Н. Педагогический процесс формирования культуры информационной безопасности // Антропология. 2025. № 4(20). С. 76—83.
19. Яковлева Ю. В. Взаимосвязь информационной безопасности и информационной культуры // Вестник науки. 2022. № 1(46). Т. 1. С. 77—81.

REFERENCES

1. Andreeva T. D. Formation of an information security culture as an essential element of the mechanism for ensuring the security of individuals, society and the state. *Altaiiskii yuridicheskii vestnik = Altai law journal*. 2025;4(52):58—64. (In Russ.)
2. Begishev I. R. Cyber-Security Culture: Psychological and Legal Aspects. *Psikhologiya i pravo = Psychology and Law*. 2021;11(4):207—220. (In Russ.) DOI: 10.17759/psylaw.2021110415.
3. Bylevskiy P. G. Culturology of professional culture of information security. *Kul'tura i iskusstvo*. 2023;8:39—49. (In Russ.) DOI: 10.7256/2454-0625.2023.8.43846.
4. Bylevskiy P. G. The evolution of information security culture: organizational, technical, and socio-cultural factors. *Vestnik sovremennykh tsifrovyykh tekhnologii*. 2025;24:22—29. (In Russ.)
5. Voropaeva E. V., Bredikhina A. V. Formation and development of a culture of information security for minors in the Russian Federation. *Universum: psikhologiya i obrazovanie*. 2025;11(137):20—22. (In Russ.) DOI: 10.32743/UniPsy.2025.137.11.20961.
6. Duben A. K. Youth information culture as a legal mechanism for ensuring security. *Agrarnoe i zemel'noe pravo = Agrarian and land law*. 2024;5(233):119—121. (In Russ.)
7. Izosimova T. A., Kulebyaev M. A. The role of information security in ensuring national security. *Razvitie ekonomiki (na mikro- i makrourovnyakh) na osnove obespecheniya bezopasnosti v sfere pod/FT/FROMU = Economic development (at micro and macro levels) based on AML/CFT/FML security. Collection of scientific articles based on the materials of the International Conference of Teachers and Students*. Moscow, Moscow Academy of Finance and Law publ., 2024;1:453—457. (In Russ.)
8. Imanov A. K., Atygaev Zh. A. Digital culture of students in the context of personal information security. *Nauchnye innovatsii = Scientific Innovations*. 2025;1(1):44—50. (In Russ.)
9. Kichigina O. Yu. Issues of information security culture formation among students in higher school. *Teoriya i praktika sotsiologicheskikh nauk = Theory and practice of socio-humanitarian studies*. 2023;4(24):14—22. (In Russ.)

10. Kryazhevskikh K. A. Impact of information culture on the level of information security. *Voprosy rossiiskoi yustitsii = Issues of Russian Justice*. 2023;24:568—573. (In Russ.)
11. Kulebyaev M. A. The phenomenon of information security culture in the interpretation of domestic and foreign authors. *Kazanskaya nauka = Kazan Science*. 2024;7:71—76. (In Russ.)
12. Kulebyaev M. A. Information security culture of students at technical universities: diagnostic aspect. *Mir nauki. Pedagogika i psikhologiya = World of Science. Pedagogy and psychology*. 2025;13(4). (In Russ.) URL: <https://mir-nauki.com/PDF/29PDMN425.pdf>.
13. Litvishkov V. M., Shvyrev B. A. Sociological aspects of the information security culture. *Ugolovno-isspolnitel'naya sistema: pravo, ekonomika, upravlenie = Criminal-executory system: law, economics, management*. 2020;2:38—40. (In Russ.)
14. Malyuk A. A., Malyuk Z. P. Topical issues of creating a mass education system for information security culture. *Bezopasnost' informatsionnykh tekhnologii = IT Security*. 2021;28(4):6—21. (In Russ.)
15. Popov D. A. Development of a culture of information security for adolescents. *Nauka. Upravlenie. Obrazovanie. RF*. 2024;2(14):83—87. (In Russ.)
16. Rudinskij I. D., Okolot D. Y. The culture of information security. the concept and content. *Informatizatsiya obrazovaniya i nauki*. 2020;3(47):39—44. (In Russ.)
17. Smirnov A. A., Rumyantseva M. V. Problems of forming a culture of information security for citizens of the Russian Federation. *Pravovaya informatika = Legal informatics*. 2025;3:154—163. (In Russ.) DOI: 10.24412/1994-1404-2025-3-00-16.
18. Shvyrev B. A., Kazberov P. N. Pedagogical process of formation of information security culture. *Antropogogika*. 2025;4(20):76—83. (In Russ.)
19. Yakovleva Yu. V. The relationship of information security and information culture. *Vestnik nauki*. 2022;1(46)-1:77—81. (In Russ.)

Статья поступила в редакцию 27.02.2026; одобрена после рецензирования 01.04.2026; принята к публикации 06.04.2026.
The article was submitted 27.02.2026; approved after reviewing 01.04.2026; accepted for publication 06.04.2026.