Научная статья
УДК 378.147:004.056
DOI: 10.25683/VOLBI.2026.75.1586

Mikhail Anatolyevich Kulebyaev
Senior Lecturer of the Department
of Computer Science and Transport Process Technologies,
Volga Region Institute (branch)
of the Moscow Automobile and Road Construction State
Technical University (MADI)
Cheboksary, Russian Federation
kadet21rus@yandex.ru

Михаил Анатольевич Кулебяев
старший преподаватель кафедры
«Информатика и технологии транспортных процессов»,
Приволжский институт (филиал)
Московского автомобильно-дорожного
государственного технического университета (МАДИ)
Чебоксары, Российская Федерация
kadet21rus@yandex.ru

ЦЕННОСТНО-СМЫСЛОВОЕ ОТНОШЕНИЕ СТУДЕНТОВ ТЕХНИЧЕСКОГО ВУЗА К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: СТРУКТУРНО-СОДЕРЖАТЕЛЬНЫЙ АНАЛИЗ

5.8.7 — Методология и технология профессионального образования

Аннотация. *Статья посвящена описанию результатов диагностики ценностно-смыслового отношения студентов технического вуза к информационной безопасности. Представленное исследование базируется на теоретическом положении о том, что культура информационной безопасности включает не только когнитивный, технический и поведенческий, но и ценностно-смысловой компонент, который выступает внутренним регулятором безопасного поведения в цифровой среде. Диагностика сфокусирована на двух ключевых параметрах ценностно-смыслового отношения: внешней (нормативно-санкционированной) и внутренней (личностно-смысловой, рефлексивной) регуляции. В качестве инструмента автором предложен комплекс диагностических методик, включающий портретный ценностный опросник Ш. Шварца, с адаптацией к контексту информационной безопасности, семантический дифференциал для оценки субъективной значимости ключевых понятий, а также проективные вопросы открытого типа. В статье представлены результаты апробации, проводившейся с участием 186 студентов I—IV курсов Приволжского института (филиала) МАДИ. В качестве значимых результатов автор выделяет: эмпирическое подтверждение гипотезы о доминировании у студентов технического вуза внешних (инструментальных, нормативно-санкционированных) ценностных ориентаций в сфере информационной безопасности при слабой выраженности внутренних (личностно-смысловых); выявление устойчивого разрыва между вербальным принятием норм информационной безопасности и их интериоризацией на уровне личностных смыслов; разработку типологии ценностно-смыслового отношения к информационной безопасности («нормативно-конформный», «утилитарно-прагматический», «рефлексивно-ценностный» типы). Анализ проективных ответов позволил зафиксировать доминирование мотивов избегания санкций и инструментальной защиты над этическими и ценностными основаниями безопасного поведения. На основании проведенной диагностики автор приходит к выводу, что предложенный диагностический инструментарий представляет собой эффективное средство для выявления структуры и содержания ценностно-смыслового отношения студентов к информационной безопасности. Полученные данные позволяют обосновать необходимость перехода от информационно-предупредительной модели формирования культуры информационной безопасности к аксиологически ориентированной, направленной на развитие внутренних ценностно-смысловых оснований безопасного поведения в цифровой среде.*

Ключевые слова: *культура информационной безопасности, ценностно-смысловые ориентации, студенты технического вуза, диагностика, аксиологический подход, цифровая безопасность, профессиональное образование, ценностные типы, интериоризация, Приволжский институт МАДИ*

Для цитирования: Кулебяев М. А. Ценностно-смысловое отношение студентов технического вуза к информационной безопасности: структурно-содержательный анализ // Бизнес. Образование. Право. 2026. № 2(75). С. 545—553. DOI: 10.25683/VOLBI.2026.75.1586.

Original article

TECHNICAL UNIVERSITY STUDENTS' VALUE-SEMANTIC ATTITUDES TO INFORMATION SECURITY: A STRUCTURAL AND CONTENT ANALYSIS

5.8.7 — Methodology and technology of vocational education

Abstract. *This article describes the results of a diagnostic study examining the value-semantic attitudes of students at a technical university to information security. The study is based on the theoretical premise that information security culture encompasses not only cognitive, technical, and behavioral components, but also a value-semantic component that acts as an internal regulator of safe behavior in the digital environment. The analysis focuses on two key*

parameters of value-semantic attitudes: external (normative-sanctioned) and internal (personal-semantic, reflexive) regulation. The author proposes a set of diagnostic methods, including Sh. Schwartz's portrait value questionnaire, adapted to the information security context, a semantic differential for assessing the subjective significance of key concepts, and open-ended projective questions. The article presents the results of a pilot study conducted with 186 first-to fourth-year students at the Volga Region Institute (MADI branch). The author highlights the following significant results: empirical confirmation of the hypothesis regarding the dominance of external (instrumental, normative-sanctioned) value orientations in the field of information security among students of a technical university, with a weak expression of internal (personal-semantic) ones; the identification of a persistent gap between the verbal acceptance of information security norms and their internalization at the level of personal meanings; the development of a typology of value-semantic attitudes to information security ("normative-conformist", "utilitarian-pragmatic", "reflexive-value"). An analysis of projective responses made it possible to record the dominance of motives for avoiding sanctions and instrumental protection over the ethical and value-based foundations of safe behavior. Based on the conducted diagnostics, the author concludes that the proposed diagnostic tool is an effective means for identifying the structure and content of students' value-semantic attitudes to information security. The obtained data allow us to substantiate the need to move from an information-preventive model for the formation of an information security culture to an axiologically oriented one aimed at developing internal value-semantic foundations for safe behavior in the digital environment.

Keywords: *information security culture, value-semantic orientations, technical university students, diagnostics, axiological approach, digital security, professional education, value types, internalization, Volga Region Institute of MADI*

For citation: Kulebyaev M. A. Technical university students' value-semantic attitudes to information security: a structural and content analysis. *Biznes. Obrazovanie. Pravo = Business. Education. Law*. 2026;2(75):545—553. DOI: 10.25683/VOLBI.2026.75.1586.

Введение

Актуальность исследования обусловлена противоречием между возрастающей требовательностью государства и общества к формированию культуры информационной безопасности граждан, с одной стороны, и недостаточной эффективностью существующих педагогических практик в технических вузах, ориентированных преимущественно на передачу нормативных знаний и алгоритмических предписаний, с другой. В Доктрине информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) и Стратегии национальной безопасности (утв. Указом РФ от 2 июля 2021 № 400) подчеркивается, что человеческий фактор остается одним из ключевых уязвимых звеньев в системе обеспечения информационной безопасности, а его преодоление возможно лишь через формирование устойчивых внутренних регуляторов поведения. Концепция формирования и развития культуры информационной безопасности граждан РФ (утв. Распоряжением Правительства РФ от 22 декабря 2022 г. № 4088-р) определяет ценностно-смысловую сферу личности в качестве базового уровня, обеспечивающего устойчивость безопасного поведения в цифровой среде. Однако, как показывает анализ образовательной практики, в технических вузах акцент традиционно смещен в сторону инструментальных компетенций, что создает риск формального усвоения требований информационной безопасности без их внутреннего присвоения.

Изученность проблемы. Проблематика культуры информационной безопасности активно разрабатывается в современной научной литературе. Р. М. Айсина и А. А. Нестерова вводят понятие «киберсоциализация», отмечая, что процессы цифровой социализации молодежи сопряжены с эффектами как позитивного, так и рискогенного характера [1]. В свою очередь, Л. В. Астахова акцентирует внимание на развитии профессиональной ответственности будущего специалиста по защите информации в вузе, подчеркивая значимость ценностно-смыслового компонента в структуре профессиональной подготовки [2]. И. Р. Бегишев в психолого-правовом аспекте обосновывает, что правовые нормы в сфере информационной безопасности эффективны лишь постольку, поскольку они присвоены личностью как личностно значимые [3]. Е. Б. Белов, М. И. Ожиганова и А. Д. Костюков рассматривают культуру информационной безопасности как междисциплинарный феномен, требующий интеграции технических и гуманитарных подходов в образовательном процессе [4].

Р. Ф. Бурнашев и Р. Г. Давронова подходят к проблеме с социально-философских позиций, рассматривая информационную безопасность личности как аксиологическую проблему [5]. П. Г. Былевский в культурологическом ключе анализирует профессиональную культуру информационной безопасности, выделяя ценностные основания профессиональной деятельности в цифровой среде [6]. О. А. Воскресенская с соавторами исследуют ценностно-мотивационные установки сотрудника в области обеспечения информационной безопасности, показывая, что доминирование внешней мотивации снижает эффективность защитных действий [7]. А. В. Галыня, в свою очередь, рассматривает культуру информационной безопасности как элемент стратегического управления рисками в киберпространстве, акцентируя необходимость формирования у будущих инженеров не только технических, но и ценностно-ориентированных компетенций [8].

Т. К. Голушко вводит понятие «информационный иммунитет», связывая его с устойчивостью личности к деструктивным информационно-психологическим воздействиям, что напрямую зависит от сформированности ценностно-смысловых ориентаций [9]. Д. Б. и Н. В. Кавецкие эмпирически подтверждают взаимосвязь информационно-психологической безопасности и ценностно-смысловой сферы личности современной молодежи [10]. А. А. и З. П. Малюки актуализируют вопросы создания системы массового обучения культуре информационной безопасности, подчеркивая необходимость перехода от информационно-предупредительной модели к ценностно-ориентированной [11].

Д. Ю. Нархов с соавторами исследуют социокультурный потенциал студенчества в аспекте информационной безопасности, фиксируя рассогласование между ценностными

установками и реальным поведением [12]. И. Д. Рудинский и Д. Я. Околот разрабатывают методику формирования культуры информационной безопасности студентов, однако их подход ориентирован преимущественно на когнитивный и деятельностный компоненты [13]. Е. Ю. Рудкевич рассматривает ценности как ресурс обеспечения национальной безопасности, что позволяет говорить о фундаментальной роли ценностно-смысловой сферы в системе защиты личности и государства [14]. С. Н. Федорова и М. А. Кулебяев предлагают модель и педагогические условия формирования культуры информационной безопасности у студентов технического вуза [15]. Е. А. Яковлева с соавторами, исследуя профессиональную идентичность студентов технических вузов, показывают, что ценностно-смысловая сфера является ядерным компонентом профессионального становления [16].

Таким образом, при значительном количестве работ, затрагивающих ценностно-смысловой аспект культуры информационной безопасности, остается недостаточно изученным вопрос о специфике структуры и содержания ценностно-смысловых ориентаций студентов именно технического вуза, а также о степени их согласованности с нормативными требованиями. Выявление реальной иерархии ценностно-смысловых ориентаций студентов позволяет определить зоны рассогласования между нормативным (декларируемым) и реальным отношением к информационной безопасности, что составляет проблемное поле настоящего исследования.

Целесообразность разработки темы определяется необходимостью эмпирического выявления реальных ценностно-смысловых доминант студентов технического вуза в сфере информационной безопасности для последующего проектирования педагогических стратегий, направленных на трансформацию внешней регуляции во внутреннюю. Без диагностики актуального состояния ценностно-смысловой сферы любые педагогические вмешательства будут носить интуитивный, а не доказательный характер.

Научная новизна исследования заключается в том, что:

1) впервые осуществлена комплексная диагностика ценностно-смыслового отношения к информационной безопасности у студентов технического вуза [на примере Приволжского института (филиал) МАДИ] с использованием триангуляции методов (модифицированный опросник Шварца, семантический дифференциал, проективные вопросы);

2) выявлена и эмпирически обоснована типология ценностно-смыслового отношения к информационной безопасности («нормативно-конформный», «утилитарно-прагматический», «рефлексивно-ценностный» типы);

3) установлен количественно измеренный разрыв между вербальным принятием норм информационной безопасности и их интериоризацией на уровне личностных смыслов;

4) предложен и апробирован диагностический инструментарий, адаптированный к контексту информационной безопасности.

Цель исследования — выявить и описать ценностно-смысловые доминанты, определяющие отношение студентов к информационной безопасности, а также установить степень их согласованности с нормативными требованиями (на примере Концепции формирования и развития культуры информационной безопасности граждан РФ).

Задачи исследования:

1. Адаптировать диагностический инструментарий (портретный ценностный опросник Ш. Шварца, семантический дифференциал, проективные вопросы) для оценки ценностно-смыслового отношения студентов технического вуза к информационной безопасности.

2. Выявить структуру ценностных ориентаций студентов в сфере информационной безопасности с дифференциацией внешней (нормативно-санкционированной) и внутренней (личностно-смысловой) регуляции.

3. Определить содержательное наполнение ценностно-смыслового отношения через анализ субъективных значений ключевых понятий информационной безопасности (семантический дифференциал) и имплицитных установок (проективные вопросы).

Теоретическая значимость работы заключается в уточнении структурно-содержательных характеристик ценностно-смыслового компонента культуры информационной безопасности применительно к студентам технического вуза, обогащении понятийного аппарата педагогической науки в части различения внешней и внутренней регуляции в сфере информационной безопасности, а также в эмпирическом подтверждении взаимосвязи между типом ценностно-смыслового отношения и поведенческими паттернами в цифровой среде.

Практическая значимость исследования заключается в разработке и апробации диагностического инструментария для мониторинга сформированности культуры информационной безопасности в вузах, выделении трех типов ценностно-смыслового отношения, позволяющих осуществлять дифференцированное педагогическое сопровождение студентов, обосновании направлений совершенствования образовательного процесса (переход от информационно-предупредительной модели к аксиологически ориентированной), а также в предоставлении эмпирической базы для разработки программ формирования культуры информационной безопасности в технических вузах.

Основная часть

Методология исследования. Эмпирическое исследование проводилось в 2024/25 учебном году на базе Приволжского института (филиала) ФГБОУ ВО «Московский автомобильно-дорожный государственный технический университет (МАДИ)». Выборку составили 186 студентов I—IV курсов очной формы обучения, осваивающих технические направления подготовки: 23.03.01 «Технология транспортных процессов», 09.03.01 «Информатика и вычислительная техника», 08.03.01 «Строительство». Гендерный состав выборки: мужчины — 63,4 %, женщины — 36,6 %. Средний возраст респондентов — 19,7 года (SD = 1,8). Выборка является репрезентативной по полу, курсу обучения и направлению подготовки относительно генеральной совокупности студентов института.

1. Для диагностики ценностно-смыслового отношения студентов к информационной безопасности применялся «Портретный ценностный опросник» **(***PVQ-R***),** разработанный на основе уточненной теории базовых индивидуальных ценностей Ш. Шварца. Опросник включает 45 суждений, позволяющих измерить 19 ценностных типов, объединенных в четыре группы высшего порядка: открытость изменениям, самопреодоление, сохранение и самовозвышение.

С целью выявления специфики ценностно-смыслового отношения в контексте информационной безопасности нами был разработан дополнительный блок из 15 суждений,

сконструированных по аналогии с методикой Шварца. Данные суждения адаптируют ценностный контекст к сфере информационной безопасности и структурированы по четырем шкалам, отражающим различные типы регуляции поведения: внешняя (нормативно-санкционированная) регуляция, внутренняя (личностно-смысловая) регуляция, утилитарно-прагматические установки и рефлексивно-ценностные установки (табл. 1). Оценка каждого суждения осуществлялась по шестибалльной шкале (1 — «совсем не похоже на меня», 6 — «очень похоже на меня»).

Таблица 1

Дополнительные суждения, адаптированные к сфере информационной безопасности

Шкала	Суждение	Содержательная характеристика
Внешняя (нормативно-санкционированная) регуляция	1. Для меня важно соблюдать правила информационной безопасности, даже если это занимает дополнительное время	Ориентация на внешние требования, санкции, обязанности
	2. Я стараюсь выполнять требования по защите информации, потому что за их нарушение могут наказать (например, отчислить или оштрафовать)	
	3. Для меня важно не нарушать правила работы с персональными данными, чтобы избежать проблем с руководством или преподавателями	
	4. Я соблюдаю политику информационной безопасности своего учебного заведения, потому что это обязанность каждого студента	
Внутренняя (личностно-смысловая, рефлексивная) регуляция	5. Я чувствую внутренний дискомфорт, когда использую одинаковые пароли для разных сервисов	Внутренний дискомфорт при нарушении, осознанная ответственность
	6. Для меня важно быть ответственным за сохранность не только своих, но и чужих персональных данных	
	7. Я осознанно отношусь к тому, какие ссылки открываю и какие файлы скачиваю, потому что это моя личная ответственность	
	8. Для меня информационная безопасность — это не просто требование, а моя внутренняя потребность	
Утилитарно-прагматические установки	9. Я соблюдаю меры информационной безопасности, потому что это помогает сохранить мои аккаунты и личные данные от кражи	Рациональная выгода, инструментальная ценность информационной безопасности
	10. Для меня важно защищать свои устройства антивирусом, чтобы избежать финансовых потерь	
	11. Я использую сложные пароли, потому что не хочу терять доступ к своим социальным сетям и учебным порталам	
Рефлексивно-ценностные установки	12. Для меня важно понимать, почему те или иные правила информационной безопасности существуют, а не просто слепо их выполнять	Понимание оснований информационной безопасности, этическая позиция, интеграция в общую культуру
	13. Я задумываюсь о последствиях своих действий в цифровой среде для других людей	
	14. Для меня информационная гигиена — это проявление уважения к себе и к окружающим	
	15. Я считаю, что культура информационной безопасности – это часть общей культуры современного человека	

Обработка полученных данных осуществлялась в несколько этапов:

1) ***Подсчет средних баллов.*** Для каждого респондента вычислялись средние арифметические значения по каждому ценностному типу (оригинальные шкалы Шварца) и по каждой дополнительной шкале, отражающей контекст информационной безопасности.

2) ***Нормативные ориентиры.*** На основе результатов апробации (n = 186) были определены следующие интервалы для интерпретации средних баллов по 6-балльной шкале:

– *высокий уровень* (5,0—6,0) — ценность (или установка) является приоритетной для респондента;

– *средний уровень* (3,0—4,9) — ценность (или установка) умеренно значима;

– *низкий уровень* (1,0—2,9) — ценность (или установка) не значима или отвергается.

3) ***Оценка надежности.*** Для определения внутренней согласованности адаптированного блока суждений (15 пунктов) был вычислен коэффициент α Кронбаха. Полученное значение α = 0,87 свидетельствует о высокой надежности инструмента.

2. Семантический дифференциал для оценки субъективной значимости понятий, связанных с информационной безопасностью. Респондентам предлагалось оценить восемь понятий («информационная безопасность», «цифровая гигиена», «пароль», «антивирус», «персональные данные», «киберугроза», «ответственность в сети», «безопасное поведение») по трем факторам: «оценка» (опасно — безопасно, вредно — полезно), «сила» (слабое — сильное, подвластное — неподвластное), «активность» (пассивное — активное, медленное — быстрое). Шкала семибалльная.

3. Проективные вопросы открытого типа: «Что для Вас лично означает информационная безопасность?», «Почему важно соблюдать правила информационной безопасности?», «В каких ситуациях Вы готовы пренебречь правилами информационной безопасности и почему?». Ответы подвергались качественному контент-анализу с последующей квантификацией.

Результаты исследования. Обработка данных, полученных с помощью портретного ценностного опросника Ш. Шварца (*PVQ-R*), позволила выявить иерархическую структуру ценностных типов, актуализируемых у студентов технического вуза в контексте информационной безопасности. Результаты описательной статистики представлены в табл. 2.

Таблица 2

Выраженность ценностных отношений (оригинальные шкалы Шварца) у студентов технического вуза (*n* = 186)

Ценностный профиль	Средний балл (*M*)	Стандартное отклонение (*SD*)
Безопасность (личная и социальная)	5,12	0,78
Конформность (правила, межличностная)	4,89	0,92
Универсализм (забота о других, толерантность)	3,45	1,01
Самостоятельность (мысли и действия)	3,21	1,12
Достижение (личный успех, компетентность)	2,98	1,24
Гедонизм	2,76	1,31
Стимуляция	2,34	1,18
Власть (доминирование, ресурсы)	2,28	1,22
Традиция	2,15	1,09
Скромность	2,03	1,14

Наиболее высокие средние баллы зафиксированы по шкалам «Безопасность» (*M* = 5,12; *SD* = 0,78) и «Конформность» (*M* = 4,89; *SD* = 0,92). Данные ценностные типы в концепции Ш. Шварца относятся к группе высшего порядка «Сохранение» и ориентируют личность на поддержание стабильности, следование нормам и избегание угроз. Важно подчеркнуть, что высокая выраженность указанных ценностей отражает преимущественно внешнюю регуляцию поведения: студенты признают значимость соблюдения правил информационной безопасности главным образом в силу действия социальных санкций — административных (дисциплинарные взыскания), академических (снижение успеваемости) или репутационных (осуждение со стороны референтной группы).

В противоположность этому, ценности, ассоциируемые с внутренней регуляцией — «Самостоятельность» (*M* = 3,21; *SD* = 1,12) и «Универсализм» (*M* = 3,45; *SD* = 1,01) — получили лишь умеренные показатели, не достигая высокого уровня (5,0—6,0). Низкие значения по шкалам «Стимуляция» (*M* = 2,34), «Власть» (*M* = 2,28) и «Гедонизм» (*M* = 2,76) свидетельствуют о том, что ценности, связанные с риском, доминированием и получением удовольствия, не являются для студентов приоритетными в контексте информационной безопасности.

Для углубленного изучения ценностно-смыслового отношения к информационной безопасности был проанализирован блок из 15 дополнительных суждений, сгруппированных в четыре шкалы, отражающие различные типы регуляции поведения. Результаты представлены в табл. 3.

Наиболее высокие средние баллы зафиксированы по шкалам «Внешняя регуляция» (*M* = 5,21; *SD* = 0,69) и «Утилитарно-прагматические установки» (*M* = 4,85; *SD* = 0,74). Первая шкала фиксирует ориентацию студентов на внешние требования, обязанности и страх перед санкциями; вторая — инструментальное отношение к информационной безопасности как средству достижения практических выгод (сохранение аккаунтов, предотвращение финансовых потерь, защита персональных данных).

Таблица 3

Выраженность ценностно-смысловых отношений (дополнительные шкалы информационной безопасности) у студентов технического вуза (*n* = 186)

Шкала	Средний балл (*M*)	Стандартное отклонение (*SD*)
Внешняя (нормативно-санкционированная) регуляция	5,21	0,69
Утилитарно-прагматические установки	4,85	0,74
Внутренняя (личностно-смысловая) регуляция	3,43	1,03
Рефлексивно-ценностные установки	3,12	1,15

Значения по шкалам «Внутренняя регуляция» (*M* = 3,43; *SD* = 1,03) и «Рефлексивно-ценностные установки» (*M* = 3,12; *SD* = 1,15) находятся в диапазоне средних значений, что свидетельствует о недостаточной сформированности личностного принятия норм информационной безопасности. Таким образом, эмпирически подтверждается преобладание внешних побудителей и инструментальных мотивов над внутренней мотивацией, основанной на осознанной ответственности и этической позиции.

Семантический дифференциал позволил оценить субъективную значимость ключевых понятий информационной безопасности по трем факторам: оценка (*E* — эмоционально-оценочное отношение: от «опасное/вредное» до «безопасное/полезное»), сила (*P* — восприятие могущества и влиятельности понятия) и активность (*A* — динамическая характеристика, скорость и интенсивность). Результаты представлены в табл. 4.

Таблица 4

Средние значения семантического дифференциала для понятий информационной безопасности (*n* = 186)

Понятие	Оценка (*E*)	Сила (*P*)	Активность (*A*)
Информационная безопасность	+2,34	+1,87	+1,12
Цифровая гигиена	+1,45	+0,98	+1,21
Пароль	+0,89	+2,01	+2,45
Антивирус	+2,56	+1,94	+2,78
Персональные данные	+2,43	+2,65	+0,87
Киберугроза	–2,12	+2,34	+1,98
Ответственность в сети	+1,78	+1,23	+1,34
Безопасное поведение	+1,34	+1,56	+1,89

Наиболее высокие значения по фактору «Оценка» зафиксированы для понятий «антивирус» (*E* = +2,56), «персональные данные» (*E* = +2,43) и «информационная безопасность» (*E* = +2,34), что свидетельствует о позитивном эмоционально-оценочном отношении студентов к данным явлениям. Напротив, понятие «киберугроза» является единственным, получившим отрицательную оценку (*E* = –2,12), что отражает его однозначное восприятие как нежелательного, угрожающего феномена.

Обращает на себя внимание сравнительно низкая оценка понятия «безопасное поведение» (*E* = +1,34) — самый низкий показатель среди всех понятий с положительной

оценкой. Данный факт указывает на недостаточную эмоциональную привлекательность активной субъектной позиции в сфере информационной безопасности для студентов технического вуза. Аналогично, понятие «цифровая гигиена» получило умеренную оценку (E = +1,45), что может свидетельствовать о восприятии его как рутинной, обременительной практики, не обладающей выраженной ценностной привлекательностью.

По фактору «Сила» максимальные значения присвоены понятиям «персональные данные» (P = +2,65) и «киберугроза» (P = +2,34), что отражает восприятие этих феноменов как обладающих высокой степенью влиятельности и могущества. Студенты осознают, что как персональные данные, так и киберугрозы являются «сильными» сущностями, способными оказывать значительное воздействие на их жизнь.

По фактору «Активность» наиболее высокие показатели демонстрируют «антивирус» (A = +2,78) и «пароль» (A = +2,45), что характеризует данные средства защиты как динамичные, оперативные инструменты. Наименее активными воспринимаются «персональные данные» (A = +0,87) и «информационная безопасность» (A = +1,12), что может указывать на их статичное, фоновое восприятие студентами.

Таким образом, семантический профиль понятий информационной безопасности у студентов технического вуза характеризуется: а) позитивной оценкой инструментальных средств защиты (антивирус, пароль); б) негативной оценкой угрозы (киберугроза); в) парадоксально низкой оценкой активной субъектной позиции (безопасное поведение, цифровая гигиена). Данное рассогласование свидетельствует о том, что студенты воспринимают информационную безопасность преимущественно через призму внешних средств защиты и угроз, а не через собственную ответственность и культуру безопасного поведения.

Контент-анализ ответов на открытые вопросы позволил выявить доминирующие смысловые категории, отражающие имплицитные представления студентов об информационной безопасности, табл. 5.

Таблица 5

Смысловые категории в ответах на открытые вопросы (n = 186, множественный выбор)

Вопрос	Варианты ответа	Значение	
		абс	%
Что для Вас лично означает информационная безопасность?	Защита персональных данных от кражи/утечки	125	67,2
	Сохранность аккаунтов и цифровых активов	109	58,6
	Отсутствие негативных последствий (штрафы, блокировки)	82	44,1
	Спокойствие и уверенность при работе в сети	59	31,7
	Профессиональное требование (для будущей работы)	52	28,0
	Ответственность перед другими	24	12,9
	Личностная ценность (принцип, убеждение)	16	8,6
	Затрудняюсь ответить / неопределенный ответ	11	5,9
Почему важно соблюдать правила информационной безопасности?	Предотвращение материального ущерба	134	72,0
	Сохранение репутации и приватности	118	63,4
	Избегание юридической ответственности	87	46,8
	Забота о своей цифровой идентичности	103	55,4
	Общественная безопасность (шире личного)	41	22,0
	Профессиональная необходимость	56	30,1
	Внутреннее убеждение / ответственность	28	15,1
В каких ситуациях Вы готовы пренебречь правилами информационной безопасности и почему?	Экономия времени	90	48,4
	Доверие к знакомому сайту/сервису	78	41,9
	Оценка риска как незначительного	66	35,5
	Социальное давление («все так делают»)	42	22,6
	Отсутствие видимых последствий в прошлом	31	16,7
	Никогда не пренебрегаю	28	15,1
	Другое / ситуативно	19	10,2

Полученные данные свидетельствуют о том, что для большинства студентов информационная безопасность ассоциируется прежде всего с защитой от внешних угроз и избеганием санкций. Этическая и ценностная составляющие встречаются значительно реже. Более 70 % респондентов допускают возможность нарушения правил информационной безопасности в ситуациях, когда это экономит время или когда риск оценивается как незначительный.

На основе кластерного анализа (метод k-средних) по всем диагностическим показателям (оригинальные шкалы Шварца, дополнительные шкалы контекста информационной безопасности, семантический дифференциал, контент-анализ ответов) было выделено три устойчивых типа ценностно-смыслового отношения студентов к информационной безопасности. Статистическая значимость различий между типами проверена с помощью однофакторного дисперсионного анализа $ANOVA$, $p < 0,01$ для всех ключевых шкал и подтверждает устойчивость выделенной типологии и правомерность ее использования в качестве основы для дифференцированного педагогического сопровождения студентов (табл. 6).

Таблица 6

Типология ценностно-смыслового отношения студентов к информационной безопасности (кластерный анализ, *n* = 186)

Тип	Значение		Характеристика	Средние значения по ключевым шкалам	Результаты контент-анализа (доминирующие категории)
	абс	%			
Нормативно-конформный	90	48,4	Высокие зн. по шкалам «Безопасность» (M = 5,12) и «Конформность» (*M* = 4,89), максимальные баллы по внешней регуляции (*M* = 5,52)	Внешняя регуляция: 5,52; Внутренняя регуляция: 2,98; Рефлексивно-ценностные установки: 2,67	Защита персональных данных (71,1 %); избегание санкций (54,4 %); пренебрежение правилами при экономии времени (61,1 %)
Утилитарно-прагматический	61	32,8	Средние значения по шкале «Безопасность», высокие по шкале «Достижение» (*M* = 4,12), максимальные баллы по утилитарно-прагматическим установкам (*M* = 5,34)	Утилитарно-прагматические установки: 5,34; Внешняя регуляция: 4,87; Внутренняя регуляция: 3,21	Сохранность аккаунтов (65,6 %); предотвращение финансовых потерь (60,7 %); пренебрежение правилами при доверии к знакомым ресурсам (50,8 %)
Рефлексивно-ценностный	35	18,8	Наиболее высокие показатели по шкалам «Самостоятельность» (*M* = 4,56) и «Универсализм» (*M* = 4,23), максимальные баллы по внутренней регуляции (*M* = 4,98) и рефлексивно-ценностным установкам (*M* = 4,85)	Внутренняя регуляция: 4,98; Рефлексивно-ценностные установки: 4,85; Внешняя регуляция: 3,12	Личностная ценность **и**нформационной безопасности (48,6 %); ответственность перед другими (42,9 %); никогда не пренебрегают правилами (57,1 %)

Представленная типология демонстрирует качественное своеобразие ценностно-смыслового отношения студентов к информационной безопасности.

Нормативно-конформный тип, охватывающий почти половину выборки студентов технического вуза (48,4 %), ориентирован на внешние регуляторы поведения, где они признают важность соблюдения правил информационной безопасности, однако их мотивация носит внешний характер, поскольку они следуют нормативам из страха перед наказанием или под давлением социальных ожиданий, что подтверждается результатами контент-анализа — доминирующими категориями ответов являются «защита персональных данных» (71,1 %) и «избегание санкций» (54,4 %), а 61,1 % респондентов этого типа допускают пренебрежение правилами в ситуациях, требующих временных затрат.

Утилитарно-прагматический тип (32,8 %) руководствуется рациональным расчетом, при котором соблюдение мер информационной безопасности ценится постольку, поскольку оно приносит практическую пользу — сохраняет аккаунты, предотвращает финансовые потери и защищает цифровые активы; контент-анализ показал, что для данной группы наиболее значимы категории «сохранность аккаунтов» (65,6 %) и «предотвращение финансовых потерь» (60,7 %), при этом 50,8 % студентов этого типа готовы пренебречь правилами, если ресурс кажется им знакомым и надежным, что указывает на действие эвристики доверия, снижающей бдительность.

Рефлексивно-ценностный тип, являющийся наименьшей группой (18,8 %), демонстрирует сформированную внутреннюю регуляцию, где студенты осознанно и ответственно подходят к вопросам информационной безопасности, воспринимая ее не как внешнее требование, а как личностную ценность и компонент общей культуры; контент-анализ зафиксировал, что 48,6 % респондентов этого типа связывают информационную безопасность с личностной ценностью, 42,9 % — с ответственностью перед другими, а 57,1 % заявляют, что никогда не пренебрегают правилами, в связи с чем данный тип может рассматриваться как целевой ориентир при проектировании педагогических стратегий формирования культуры информационной безопасности.

Заключение и выводы

Проведенное исследование позволило достичь поставленной цели и решить сформулированные задачи, а именно:

1. Выявлена структура ценностно-смысловых ориентаций студентов технического вуза в области информационной безопасности. Установлено, что доминирующими являются ценности нормативно-санкционированной безопасности и конформности, тогда как рефлексивно-ценностные и этические компоненты выражены слабо. Это подтверждает гипотезу о преобладании внешней регуляции.

2. Описано содержательное наполнение ценностно-смыслового отношения через анализ ответов на проективные вопросы. Показано, что для большинства студентов информационная безопасность означает прежде всего защиту от конкретных угроз и избегание санкций; личностно-смысловое принятие норм информационной безопасности встречается лишь у 8,6 % респондентов.

3. Разработана типология ценностно-смыслового отношения к информационной безопасности («нормативно-конформный», «утилитарно-прагматический», «рефлексивно-ценностный» типы), которая может служить основой для дифференцированного педагогического сопровождения.

Полученные результаты свидетельствуют о том, что существующая в технических вузах информационно-предупредительная модель формирования культуры информационной безопасности, ориентированная на передачу нормативных знаний и алгоритмических предписаний, достигает своих целей лишь на уровне внешней регуляции. Студенты знают правила, но не присваивают их как личностно значимые; они осознают риски, но не развивают устойчивую внутреннюю мотивацию к безопасному поведению.

В связи с этим обосновывается необходимость перехода к аксиологически ориентированной модели формирования культуры информационной безопасности, которая предполагает:

• Смещение фокуса с трансляции норм на рефлексию ценностей. В содержание дисциплин, связанных с информационной безопасностью, необходимо включать модули,

направленные на осмысление студентами ценностных оснований безопасного поведения (этические дилеммы, анализ кейсов, дискуссии о личной и профессиональной ответственности).

• Развитие внутренней регуляции через опыт проживания ситуаций выбора. Использование активных и интерактивных методов обучения (деловые игры, проектные задачи, симуляции) позволяет студентам не только узнавать правила, но и «проживать» ситуации, в которых требуется сделать выбор между безопасностью и удобством, риском и выгодой.

• Формирование рефлексивно-ценностных установок. Необходимо целенаправленно развивать у студентов способность рефлексировать последствия своих действий в цифровой среде не только для себя, но и для других людей, формируя понимание информационной безопасности как компонента общей культуры и профессиональной этики.

• Интеграцию ценностного компонента в профессиональную подготовку. Ценности информационной безопасности должны быть встроены в содержание профессиональных дисциплин и практик, а не оставаться изолированным блоком в рамках курсов по информационной безопасности.

• Мониторинг ценностно-смысловой динамики. Регулярное использование разработанного диагностического инструментария позволит отслеживать изменения ценностно-смыслового отношения студентов и корректировать педагогические воздействия.

• Переход от информационно-предупредительной модели формирования культуры информационной безопасности к аксиологически ориентированной представляет собой не просто методическое уточнение, а смену образовательной парадигмы, в центре которой находится не трансляция знаний о безопасности, а развитие личности, способной к рефлексивному, ответственному и ценностно-обоснованному поведению в цифровой среде.

СПИСОК ИСТОЧНИКОВ

1. Айсина Р. М., Нестерова А. А. Киберсоциализация молодежи в информационно-коммуникационном пространстве современного мира: эффекты и риски // Социальная психология и общество. 2019. Т. 10. № 4. С. 42—57. DOI: 10.17759/sps.2019100404.

2. Астахова Л. В. Развитие профессиональной ответственности будущего специалиста по защите информации в вузе // Вестник Южно-Уральского государственного университета. Серия: Образование. Педагогические науки. 2022. Т. 14. № 2. С. 21—29. DOI: 10.14529/ped220202.

3. Бегишев И. Р. Культура информационной безопасности: психолого-правовой аспект // Психология и право. 2021. Т. 11. № 4. С. 207—220. DOI: 10.17759/psylaw.2021110415.

4. Белов Е. Б., Ожиганова М. И., Костюков А. Д. К вопросу о культуре информационной безопасности // Социотехнические и гуманитарные аспекты информационной безопасности : материалы Всерос. науч.-практ. конф. Пятигорск : Пятигор. гос. ун-т, 2019. С. 43—48.

5. Бурнашев Р. Ф., Давронова Р. Г. Информационная безопасность личности как аксиологическая проблема: социально-философский анализ // Universum: общественные науки. 2024. № 12(115). DOI: 10.32743/UniSoc.2024.115.12.18844.

6. 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.

7. Воскресенская О. А., Сладкова Н. М., Горковенко Ю. Л. Оценка ценностно-мотивационных установок сотрудника в области обеспечения информационной безопасности // Социально-трудовые исследования. 2022. № 1(46). С. 142—153.

8. Галыня А. В. Культура информационной безопасности как элемент стратегического управления рисками в киберпространстве // Дорожно-транспортный комплекс: состояние, проблемы и перспективы развития : сб. науч. тр. XXIV Междунар. техн. науч.-практ. конф. Чебоксары : Волж. фил. Моск. автомоб.-дорож. гос. техн. ун-та (МАДИ), 2025. С. 506—510.

9. Голушко Т. К. Информационный иммунитет как ключевое понятие информационно-психологической безопасности личности // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2022. Т. 27. № 6. С. 1483—1495. DOI: 10.20310/1810-0201-2022-27-6-1483-1495.

10. Кавецкий Д. Б., Кавецкая Н. В. Взаимосвязь информационно-психологической безопасности и ценностно-смысловой сферы личности современной молодежи // Вестник педагогических наук. 2022. № 7. С. 26—33.

11. 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.

12. Нархов Д. Ю., Нархова Е. Н., Ярутина С. А., Шкурин Д. В. Социокультурный потенциал студенчества в аспекте информационной безопасности и профессиональной подготовки // Вестник Пермского национального исследовательского политехнического университета. Социально-экономические науки. 2021. № 2. С. 20—34. DOI: 10.15593/2224-9354/2021.2.2.

13. Рудинский И. Д., Околот Д. Я. Формирование культуры информационной безопасности студентов колледжа // Информатика и образование. 2019. № 9(308). С. 29—36. DOI: 10.32517/0234-0453-2019-34-9-29-36.

14. Рудкевич Е. Ю. Ценности: ресурс обеспечения национальной безопасности // Вестник Поволжского института управления. 2024. Т. 24. № 2. С. 62—70.

15. Федорова С. Н., Кулебяев М. А. Модель и педагогические условия формирования культуры информационной безопасности у студентов технического вуза // Вестник Марийского государственного университета. 2024. Т. 18. № 3. С. 340—350. DOI: 10.30914/2072-6783-2024-18-3-340-350.

16. Яковлева Е. А., Евсюкова Н. Ю., Соловьева С. А. Профессиональная идентичность студентов технических вузов в контексте образовательной среды // Мир науки. Педагогика и психология. 2025. Т. 13. № 5. URL: https://mir-nauki.com/PDF/14PSMN525.pdf.

REFERENCES

1. Aysina R. M., Nesterova A. A. Cyber socialization of youth in the information and communication space of the modern world: effects and risks. *Sotsial`naya psikhologiya i obshchestvo = Social Psychology and Society*. 2019;10(4):42—57. (In Russ.) DOI: 10.17759/sps.2019100404.

2. Astakhova L. V. Development of professional responsibility of a future specialist in information security at the university. *Vestnik Yuzhno-Ural`skogo gosudarstvennogo universiteta. Seriya: Obrazovanie. Pedagogicheskie nauki = Bulletin of the South Ural State University. Series: Education. Pedagogy*. 2022;14(2):21—29. (In Russ.) DOI: 10.14529/ped220202.

3. 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.

4. Belov E. B., Ozhiganova M. I., Kostyukov A. D. On the issue of information security culture. *Sotsiotekhnicheskie i gumanitarnye aspekty informatsionnoi bezopasnosti = Sociotechnical and humanitarian aspects of information security. Proceedings of the All-Russian scientific and practical conference*. Pyatigorsk, Pyatigorsk State University publ., 2019:43—48. (In Russ.)

5. Burnashev R., Davronova R. Personal information security as an axiological problem: socio-philosophical analysis. *Universum: obshchestvennye nauki*. 2024;12(115). (In Russ.) DOI: 10.32743/UniSoc.2024.115.12.18844.

6. 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.

7. Voskresenskaya O. A., Sladkova N. M., Gorkovenko Yu. L. Assessment of the value and motivational attitudes of the employee in the area of information security. *Sotsial`no-trudovye issledovaniya = Social & labour research*. 2022;1(46): 142—153. (In Russ.)

8. Galynya A. V. Information security culture as an element of strategic risk management in cyberspace. *Dorozhno-transportnyi kompleks: sostoyanie, problemy i perspektivy razvitiya = Road transport complex: current state, challenges, and development prospects. Collection of scientific papers of the XXIV International technical and scientific and practical conference*. Cheboksary, Volga branch of the Moscow Automobile and Road Construction State Technical University (MADI) publ., 2025:506—510. (In Russ.)

9. Golushko T. K. Information immunity as a key concept of information and psychological security of the individual. *Vestnik Tambovskogo universiteta. Seriya: Gumanitarnye nauki = Tambov University Review. Series: Humanities*. 2022;27(6): 1483—1495. (In Russ.) DOI: 10.20310/1810-0201-2022-27-6-1483-1495.

10. Kavetsky D. B., Kavetskaya N. V. The relationship of information and psychological security and the value-semantic sphere of the personality of modern youth. *Vestnik pedagogicheskikh nauk*. 2022;7:26—33. (In Russ.)

11. Malyuk A. A., Malyuk Z. P. Topical issues of creating a mass education system for information security culture. *Bezopasnost` informatsionnykh tekhnologii = IT Security (Russia)*. 2021;28(4):6—21. (In Russ.)

12. Narkhov D. Yu., Narkhova E. N., Yarutina S. A., Shkurin D. V. Sociocultural potential of students in reflecting of information safety and professional education. *Vestnik Permskogo natsional`nogo issledovatel`skogo politekhnicheskogo universiteta. Sotsial`no-ekonomicheskie nauki = PNRPU sociology and economics bulletin*. 2021;2:20—34. (In Russ.) DOI: 10.15593/2224-9354/2021.2.2.

13. Rudinskiy I. D., Okolot D. Ya. The formation of information security culture of college students. *Informatika i obrazovanie = Informatics and education*. 2019;9:29—36. (In Russ.) DOI: 10.32517/0234-0453-2019-34-9-29-36.

14. Rudkevich E. Yu. Values: national security resource. *Vestnik Povolzhskogo instituta upravleniya = Bulletin of the Volga Region Institute of Administration*. 2024;24(2):62—70. (In Russ.)

15. Fedorova S. N., Kulebyaev M. A. The model and pedagogical conditions for the formation of an information security culture among students of a technical university. *Vestnik Mariiskogo gosudarstvennogo universiteta = Vestnik of the Mari State University*. 2024;18(3):340—350. (In Russ.) DOI: 10.30914/2072-6783-2024-18-3-340-350.

16. Yakovleva E. A., Evsyukova N. Yu., Solovyova S. A. Professional identity of students of technical universities in the context of the educational environment. *Mir nauki. Pedagogika i psikhologiya = World of Science. Pedagogy and psychology*. 2025;13(5). (In Russ.) URL: https://mir-nauki.com/PDF/14PSMN525.pdf.

Статья поступила в редакцию 10.02.2026; одобрена после рецензирования 27.03.2026; принята к публикации 30.03.2026.
The article was submitted 10.02.2026; approved after reviewing 27.03.2026; accepted for publication 30.03.2026.