Кулебяев Михаил Анатольевич
соискатель, старший преподаватель
Приволжский институт (филиал)
ФГБОУ ВО «Московский автомобильно-дорожный
государственный технический университет (МАДИ)»
г. Чебоксары, Чувашская республика

DOI 10.31483/r-156325

РЕАЛИЗАЦИЯ ПОТЕНЦИАЛА ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ТЕХНИЧЕСКОГО ВУЗА В ФОРМИРОВАНИИ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТУДЕНТОВ

Аннотация: *в статье раскрыт потенциал цифровой образовательной среды технического вуза как инструмента формирования культуры информационной безопасности студентов. Выделены технологический, информационный, аналитический и коммуникационный ресурсы, влияющие на ценностно-смысловой, когнитивный, технический и поведенческий компоненты. Экспериментально доказано, что комплексное использование ресурсов обеспечивает гармоничное развитие культуры безопасности, предотвращая дисбаланс компонентов.*

Ключевые слова: *цифровая образовательная среда, культура информационной безопасности, технический вуз, педагогический эксперимент, информационная безопасность.*

Введение. Интенсивная цифровизация высшего образования, сопровождающаяся ростом киберугроз и расширением спектра атак, эксплуатирующих человеческий фактор, выдвигает на первый план задачу формирования культуры информационной безопасности (КИБ) у студентов технических специальностей. Именно выпускники инженерных направлений в ближайшем будущем станут операторами критической информационной инфраструктуры, что придаёт проблеме стратегическую значимость. Однако, как показывают исследования [14; 15], у студентов технических вузов наблюдается дисбаланс: при

сравнительно развитом техническом компоненте ценностно-смысловой и поведенческий компоненты КИБ выражены слабо.

Цифровая образовательная среда (ЦОС) современного университета, интегрирующая технологические, информационные и коммуникационные ресурсы, способна стать не только фоном, но и действенным инструментом решения указанной проблемы. Тем не менее, в научной литературе до сих пор недостаточно полно раскрыт потенциал ЦОС именно как средства комплексного формирования всех компонентов культуры информационной безопасности. Цель настоящей статьи – раскрыть механизмы и результаты использования ЦОС технического вуза в качестве системообразующего инструмента становления культуры информационной безопасности студентов.

Обзор литературы. Понятие «культура информационной безопасности» трактуется в науке неоднозначно. Л.В. Астахова [2] рассматривает его сущность сквозь призму функциональной концепции культуры и амбивалентности информации. И.Р. Бегишев [3] акцентирует психолого-правовой аспект, включая готовность личности противостоять цифровой экспансии и опору на нормативно-правовую базу. П.Г. Былевский [4] характеризует КИБ как социально-культурный феномен, эволюционирующий от узкотехнической деятельности к общегражданской культуре. А.А. Малюк и И.Ю. Алексеева [9] связывают КИБ с целенаправленным выполнением концепции защиты информации, рассматривая её как элемент подготовки специалистов. И.Д. Рудинский и Д.Я. Околот [11] определяют КИБ как часть общей и профессиональной культуры, выделяя структурные компоненты, включающие способность к оценке достоверности данных и правомерному их использованию. В учебном пособии Б.А. Швырева и др [16] обобщены практические аспекты формирования культуры безопасности пользователей.

Применительно к студентам технических вузов наиболее развёрнутые представления даны в работах С.А. Соловьевой [14], Н.Ю. Евсюковой [13], где выделены технический, когнитивный, поведенческий и ценностно-смысловой компоненты КИБ, причём зафиксирован низкий уровень именно ценностно-смыслового и поведенческого компонентов. Дальнейшие исследования [15] позволили

разработать модель формирования КИБ, а в [7] предложен авторский диагностический инструментарий. Вопросы критического мышления как фактора КИБ рассмотрены в работах С.А. Соловьевой, Н.Ю. Евсюковой [13].

Параллельно развиваются представления о цифровой образовательной среде технического вуза. Н.Б. Андреева [1] выделила особенности информационно-образовательной среды такого вуза. А.Г. Широколобова [17] проанализировала компонентный состав и функционал ЦОС, включив в неё, помимо программно-технического, также психолого-педагогический и социально-воспитательный блоки. Ряд авторов [5; 8; 10] акцентируют необходимость создания в образовательной организации условий для обеспечения информационной безопасности личности студента, подчёркивая комплексный характер требуемых решений.

Компоненты ЦОС и их влияние на компоненты КИБ. Опираясь на исследования представленные Н.Б. Андреевой, А.Г. Широколобовой [1; 17] и собственный опыт, мы выделяем в ЦОС четыре взаимосвязанных ресурса, каждый из которых преимущественно «ответственен» за формирование определённых составляющих КИБ (табл. 1).

Таблица 1

Влияние компонентов ЦОС на компоненты КИБ

Компонент ЦОС/ Компонент КИБ	Ценностно-смысловой	Когнитивный	Технический	Поведенческий
Технологическая инфраструктура	Косвенное	Косвенное	Прямое	Косвенное
Информационные ресурсы	Прямое	Прямое	Косвенное	Косвенное
Аналитические ресурсы	Косвенное	Прямое	Косвенное	Прямое
Коммуникационные сервисы	Прямое	Косвенное	Косвенное	Прямое

Технологическая и программная инфраструктура представлена IT-лабораториями, оснащёнными оборудованием для изучения сетевой безопасности, криптографии и средств защиты, а также LMS Moodle, обеспечивающей централизованный доступ к учебным курсам и диагностическим материалам. Именно

здесь происходит прямое формирование технического компонента КИБ – студенты осваивают инструментарий защиты информации практически.

Информационные ресурсы включают электронный модульный курс «Культура информационной безопасности», банк кейсов по ИБ, интерактивные задания «Игры разума – критическое мышление в действии», а также базы нормативно-правовых актов в сфере защиты информации, включая Концепцию формирования и развития культуры информационной безопасности граждан РФ [6]. Данный компонент служит основным источником знаний о киберугрозах и методах защиты (когнитивный компонент) и одновременно транслирует ценности ответственного отношения к информации (ценностно-смысловой компонент).

Аналитические ресурсы представлены авторским четырёхкомпонентным опросником культуры информационной безопасности (КИБ), описанным в [7]. Он позволяет проводить регулярную диагностику уровней сформированности всех компонентов КИБ, получать обратную связь и на её основе корректировать образовательный процесс. Прямое влияние аналитический ресурс оказывает на когнитивный и поведенческий компоненты: результаты диагностики стимулируют осознание студентами собственных дефицитов и мотивируют к корректировке поведения.

Коммуникационные сервисы – платформа «МАКС», Яндекс.Телемост, VK Видео, корпоративная электронная почта и мессенджеры – создают среду интерактивного взаимодействия участников образовательного процесса. Через них реализуются on-line лекции, вебинары, консультации в рамках кибер-квеста «Кибершит – путь к безопасности» и деятельности студенческого сообщества «Кибердружина МАДИ». Эти сервисы одновременно являются и каналом коммуникации, и учебным полигоном: студенты осваивают навыки безопасного общения, настройки приватности и защиты персональных данных непосредственно в процессе их использования, что формирует поведенческий и ценностно-смысловой компоненты КИБ.

Результаты педагогического эксперимента. Для проверки эффективности описанного подхода был проведён трёхлетний педагогический эксперимент

(2021–2024 гг.) на базе Приволжского института (филиала) МАДИ с участием 354 студентов пяти инженерно-технических направлений подготовки, разделённых на экспериментальную (n=174) и контрольную (n=180) группы. Исходная однородность групп была подтверждена статистически (φ-критерий Фишера, все значения $\varphi < 1{,}64$ при $p < 0{,}05$).

В экспериментальной группе последовательно задействовались все четыре компонента ЦОС, описанные выше. Контрольная группа обучалась по традиционной программе, без системного применения ресурсов ЦОС для формирования культуры информационной безопасности. Динамика уровня сформированности компонентов культуры информационной безопасности фиксировалась с помощью авторского опросника [7].

Таблица 2

Динамика сформированности компонентов КИБ
в экспериментальной группе (в %)

Компонент КИБ	Конст. этап (высокий)	Контр. этап (высокий)	Конст. этап (низкий)	Контр. этап (низкий)	φ-критерий (высокий)
Интегральный уровень	13,8	37,9	25,3	10,3	5,058**
Ценностно-смысловой	12,6	31,0	40,2	18,4	4,241**
Когнитивный	25,9	46,6	31,6	13,2	4,055**
Технический	41,4	55,7	12,6	3,4	2,691**
Поведенческий	26,4	43,1	33,9	14,9	3,287**
Примечание: ** – $p < 0{,}01$ ($\varphi_{кр} = 2{,}28$)					

Как видно из таблицы 2, статистически значимая положительная динамика достигнута по всем компонентам. Наибольший прирост зафиксирован в ценностно-смысловом (φ=4,241) и когнитивном (φ=4,055) компонентах, что отражает эффективность информационных и коммуникационных ресурсов ЦОС, а также целенаправленной междисциплинарной интеграции. Рост высокого уровня поведенческого компонента с 26,4% до 43,1% (φ=3,287) подтверждает действенность системы IT-мероприятий и волонтёрской деятельности «Кибердружины

МАДИ», функционирующей, в том числе, на базе коммуникационных сервисов ЦОС.

В контрольной группе статистически значимых сдвигов не выявлено. Таким образом, именно системное применение всех компонентов ЦОС обусловило всестороннее развитие культуры информационной безопасности, устранив изначальный дисбаланс между технической подготовкой и ценностно-смысловой сферой.

Обсуждение. Полученные данные согласуются с выводами других исследователей. Так, Е.В. Иванова с соавторами [5] фиксируют устойчиво низкий уровень готовности студентов к самостоятельной защите персональных данных до проведения специальных образовательных мероприятий. Д.С. Поспелова [10] и В.В. Леуцкий [8] подтверждают необходимость интеграции кибербезопасности в учебный процесс, подчёркивая важность создания мотивационной среды. С.П. Середкин [12] уточняет современное понимание кибербезопасности, акцентируя комплексную природу этого феномена, включающую не только технические, но и поведенческие аспекты. Результаты проведённого нами эксперимента дополняют эти исследования конкретной моделью реализации потенциала ЦОС, доказывая, что при грамотно выстроенной архитектуре цифровой среды её влияние на обучающихся существенно выходит за рамки чисто технологического обеспечения.

Заключение. Проведённое исследование позволяет утверждать, что цифровая образовательная среда технического вуза обладает значимым потенциалом в формировании культуры информационной безопасности студентов. Этот потенциал раскрывается через интеграцию технологической инфраструктуры, информационных, аналитических и коммуникационных ресурсов, каждый из которых вносит специфический вклад в развитие ценностно-смыслового, когнитивного, технического и поведенческого компонентов культуры информационной безопасности. Экспериментальные данные демонстрируют статистически значимое повышение всех компонентов КИБ у студентов экспериментальной группы, причём наибольшие сдвиги достигнуты в тех аспектах, которые на констатирующем

этапе находились в зоне дефицита. Практическая значимость работы состоит в том, что апробированная модель использования ЦОС для формирования культуры информационной безопасности может быть масштабирована в других технических вузах. Перспективы дальнейших исследований связаны с дифференциацией подходов для различных инженерных профилей и адаптацией модели к новым вызовам, порождаемым стремительным развитием технологий искусственного интеллекта.

Список литературы

1. Андреева Н.Б. Особенности информационно-образовательной среды технического вуза / Н.Б. Андреева // Научное обозрение. Педагогические науки. – 2014. – №1. – С. 41.

2. Астахова Л.В. Понятие культуры информационной безопасности / Л.В. Астахова // Научно-техническая информация. Серия 1. – 2014. – №2. – С. 1–8. EDN RYFSZP

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

4. Былевский П.Г. Формирование культуры информационной безопасности граждан России: эволюционная периодизация / П.Г. Былевский // Мир науки. Социология, филология, культурология. – 2023. – Т. 14. №3. EDN ISZOVL

5. Информационная безопасность личности студента в условиях цифровой образовательной среды / Е.В. Иванова, Р.Ю. Николаев, С.А. Жигалов [и др.] // Современная наука: актуальные проблемы теории и практика. Серия: Гуманитарные науки. – 2025. – №10-2. – С. 96–100.

6. Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации: утв. распоряжением Правительства РФ №4088-р от 22.12.2022.

7. Кулебяев М.А. Культура информационной безопасности студентов технического вуза: диагностический аспект / М.А. Кулебяев // Мир науки. Педагогика

и психология. – 2025. – Т. 13. №4. – URL: https://mir-nauki.com/PDF/29PDMN425.pdf (дата обращения: 11.04.2026). EDN RMYFLC

8. Леуцкий В.В. Формирование цифровой безопасности у студентов: проблемы, вызовы и перспективы интеграции в учебном процессе / В.В. Леуцкий, М.К. Басалко // Сормовские чтения-2025: научно-образовательное пространство, реалии и перспективы повышения качества образования: материалы Междунар. науч.-практ. конф. (Краснодар, 14 февр. 2025 г.). – Чебоксары: Среда, 2025. – С. 136–137. EDN FGKZIO

9. Малюк А.А. Культура информационной безопасности как элемент подготовки специалистов по защите информации / А.А. Малюк, И.Ю. Алексеева // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. – 2016. – №1(3). – С. 45–53. EDN WAIXQP

10. Поспелова Д.С. Кибербезопасность в учебном процессе: формирование культуры безопасности у студентов профессиональных образовательных организаций / Д.С. Поспелова // Молодой ученый. – 2025. – №51(602). – С. 171–173. EDN UEHXRK

11. Рудинский И.Д. Культура информационной безопасности морского специалиста и условия ее формирования / И.Д. Рудинский, Д.Я. Околот // Педагогика. Вопросы теории и практики. – 2022. – Т. 7. №1. – С. 100–107. DOI 10.30853/ped20220010. EDN EGCQQT

12. Середкин С.П. Современный взгляд на толкование понятия кибербезопасность / С.П. Середкин // Информационные технологии и математическое моделирование в управлении сложными системами. – 2023. – №2(18). – С. 17–22. DOI 10.26731/2658-3704.2023.2(18).17-22. EDN ROHMPB

13. Соловьева С.А. Роль критического мышления в развитии культуры информационной безопасности студентов технического вуза / С.А. Соловьева, Н.Ю. Евсюкова, М.А. Кулебяев // Психологически безопасная образовательная среда: проблемы проектирования и перспективы развития: сб. материалов

VI Междунар. науч.-практ. конф. (Тула, 16 окт. 2024 г.). – Чебоксары: Среда, 2024. – С. 49–51. EDN DWBEIL

14. Соловьева С.А. Специфика культуры информационной безопасности студентов технического вуза / С.А. Соловьева, М.А. Кулебяев // Развитие образования. – 2024. – Т. 7. №2. – С. 50–56. DOI 10.31483/r-110280. EDN DJMCMC

15. Федорова С.Н. Модель и педагогические условия формирования культуры информационной безопасности у студентов технического вуза / С.Н. Федорова, М.А. Кулебяев // Вестник Марийского государственного университета. – 2024. – Т. 18. №3(55). – С. 340–350. DOI 10.30914/2072-6783-2024-18-3-340-350. EDN KKZBRH

16. Швырев Б.А. Культура информационной безопасности для пользователей : учеб. пособие / Б.А. Швырев, А.В. Вилкова, А.В. Власенко. – Краснодар: Новация, 2021. – 165 с.

17. Широколобова А.Г. Цифровая образовательная среда вуза: компонентный состав и функционал / А.Г. Широколобова // Вестник Томского государственного педагогического университета. – 2024. – №5. – С. 119–128. DOI 10.23951/1609-624X-2024-5-119-128. EDN DDIKJS