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-156358

НОРМАТИВНО-ПРАВОВЫЕ ОСНОВЫ ФОРМИРОВАНИЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТУДЕНТОВ ТЕХНИЧЕСКИХ ВУЗОВ

Аннотация: *в статье рассматриваются нормативно-правовые документы, регулирующие сферу информационной безопасности, и их роль в проектировании образовательных программ подготовки будущих инженеров. Проведён анализ требований законодательства к подготовке кадров, способных обеспечить защиту критической информационной инфраструктуры. Обоснована необходимость интеграции правовых модулей в учебный процесс технического вуза как условия формирования ценностно-смыслового и когнитивного компонентов культуры информационной безопасности студентов.*

Ключевые слова: *информационная безопасность, культура информационной безопасности, нормативно-правовое регулирование, технический вуз, критическая информационная инфраструктура.*

Введение. Современный этап цифровой трансформации общества характеризуется не только расширением технологических возможностей, но и нарастанием киберугроз, затрагивающих интересы личности, общества и государства. В этих условиях особую значимость приобретает подготовка кадров, обладающих не только техническими компетенциями, но и сформированной культурой информационной безопасности (КИБ). В рамках настоящего исследования культура информационной безопасности понимается как интегративное личностное образование, представляющее собой системное единство ценностно-смыслового, когнитивного, технического и поведенческого компонентов, в совокупности

обеспечивающих ответственное, правомерное и безопасное поведение в информационном пространстве. Именно правовая регламентация становится стержнем ценностно-смыслового компонента, определяя осознание будущим инженером значимости соблюдения законов и норм в области защиты информации. Отсюда вытекает актуальность интеграции нормативно-правовых аспектов в образовательный процесс профессиональной подготовки инженерных кадров.

Основные нормативно-правовые акты в сфере информационной безопасности. Фундаментальным документом, определяющим государственную политику в рассматриваемой области, является Доктрина информационной безопасности Российской Федерации, утверждённая Указом Президента РФ от 5 декабря 2016 г. № 646. Доктрина определяет информационную безопасность как состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз и закрепляет необходимость осуществления взаимоувязанных правовых, организационных и кадровых мер по её обеспечению [3]. Развитие положений Доктрины нашло отражение в Указе Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», установившем единый государственный подход к организации кибербезопасности и подготовке кадров. Как отмечает В. А. Северин, данный Указ формирует общие подходы, а решение задачи подготовки специалистов требует привлечения профессорско-преподавательского состава для проведения междисциплинарных исследований и осуществления образовательной деятельности [9].

Поворотным моментом в регулировании сферы КИБ стало принятие распоряжения Правительства РФ от 22 декабря 2022 г. № 4088-р, утвердившего Концепцию формирования и развития культуры информационной безопасности граждан Российской Федерации. Концепция впервые на нормативном уровне закрепила определение КИБ как «совокупности сформированных знаний, умений и навыков по вопросам информационной безопасности, обеспечивающей безопасное пребывание гражданина Российской Федерации в информационном пространстве», и прямо указала на отсутствие в стране системного подхода к

повышению грамотности граждан [5]. При этом Концепция акцентирует неразрывную связь КИБ как с профессиональной, так и с бытовой деятельностью граждан, что применительно к студентам технических вузов означает необходимость формирования как профессиональных, так и личностных компетенций.

Базовым законодательным актом, регулирующим отношения в сфере информации и её защиты, выступает Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», устанавливающий правовые основы обеспечения безопасности при создании и эксплуатации информационных систем [13]. Непосредственное отношение к подготовке инженерных кадров имеет Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры в целях её устойчивого функционирования при проведении компьютерных атак [12].

Как подчёркивают С.А. Соловьева и М.А. Кулебяев, «студенты технических вузов составят кадровую основу инженерной отрасли и в дальнейшем будут обеспечивать эксплуатацию и защиту технических систем, включая критическую информационную инфраструктуру» [11]. Данный вывод коррелирует с позицией законодателя: в Федеральном законе № 187-ФЗ и подзаконных актах ФСТЭК России установлены квалификационные требования к специалистам, обслуживающим объекты критической информационной инфраструктуры, что напрямую определяет содержание образовательных программ технических вузов.

Нормативно-правовое регулирование образовательной деятельности в сфере ИБ. Правовую основу интеграции вопросов ИБ в образовательный процесс составляет Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации». Часть 11 статьи 12 данного закона специально оговаривает особенности разработки примерных основных профессиональных образовательных программ в области информационной безопасности, что свидетельствует о выделении данной сферы государством в качестве приоритетной [14]. Требования к содержанию подготовки конкретизируются в федеральных

государственных образовательных стандартах высшего образования по инженерным направлениям, которые предусматривают формирование у выпускников компетенций в области информационной безопасности.

Следует отметить, что, как указывают Серёдкин С.П. и Кулага И.В., «нормативно-правовая база, определяющая общие принципы работы с информацией, требует дальнейшего развития применительно к образовательной среде», и особое внимание должно уделяться «роли образовательных учреждений в формировании культуры кибербезопасности» [10]. Аналогичной позиции придерживается Бокова Л.Н., которая, анализируя правовой режим создания безопасной цифровой образовательной среды, обосновывает необходимость введения в научный оборот правоведения понятия «безопасность образовательной среды» и предлагает направления совершенствования законодательства в данной сфере [1].

Важным этапом развития нормативной базы стало принятие Приказа Министерства науки и высшего образования РФ от 4 сентября 2024 г. № 579, который внёс изменения в порядок разработки дополнительных профессиональных программ в области информационной безопасности [8]. Данный акт создаёт правовые основания для организации повышения квалификации профессорско-преподавательского состава технических вузов в сфере ИБ.

В контексте интеграции правовых аспектов в подготовку инженеров значимым является исследование Е.Е. Ковалева, обобщившего опыт интеграции правовых компетенций и аспектов информационной безопасности в образовательные программы института математики и информатики МПГУ [4]. Автор показывает, что включение правовых модулей в технические дисциплины способствует формированию у студентов целостного представления о правовых последствиях нарушений в сфере ИБ.

Подготовка кадров для защиты критической информационной инфраструктуры. Как отмечалось выше, Указ Президента РФ №250 сформировал единый государственный подход к организации кибербезопасности и подготовки кадров. В.А. Северин, анализируя данный Указ, подчёркивает, что «он устанавливает единый подход к организации кибербезопасности государственных и

коммерческих структур, относящихся к субъектам критической информационной инфраструктуры, а также подготовки кадров с учётом единых квалификационных требований» [9]. Данная позиция усиливается выводами Т.А. Поляковой и А.А. Стрельцова, в учебнике которых систематизированы организационные и правовые аспекты обеспечения информационной безопасности, включая требования к компетенциям специалистов [7].

По мнению Былевского П.Г., принятие Правительством России Концепции формирования и развития КИБ «подтверждает актуальность указанной темы», а существующие подходы демонстрируют «ограниченность узкой специализации (технической, нормативно-правовой, организационной, психологической, педагогической)», что обусловливает востребованность профильного системного подхода к формированию профессиональной культуры ИБ в разных отраслях [2].

Интеграция правовых модулей в учебный процесс технических вузов. В разработанной нами совместно с С.А. Соловьевой [11] и С.Н. Федоровой [15] структурно-функциональной модели формирования культуры информационной безопасности студентов технических вузов одно из четырёх организационно-педагогических условий непосредственно направлено на становление ценностно-смыслового компонента. Это условие сформулировано как «интеграция этических и правовых аспектов информационной безопасности в учебные программы» и рассматривается не как факультативное дополнение, а как обязательный элемент профессиональной подготовки будущего инженера. Выделение данного условия продиктовано установленным в ходе констатирующего эксперимента парадоксом: при сравнительно развитой технической грамотности и наличии базовых когнитивных представлений об угрозах ценностно-смысловой и поведенческий компоненты КИБ демонстрируют выраженный дефицит [6; 11]. Иными словами, знания о том, *как* устроены системы защиты, не конвертируются автоматически в понимание того, *почему* их нарушение недопустимо с правовой и этической точек зрения.

Устранение этого разрыва требует системного включения правовых модулей в содержание как профильных, так и гуманитарных и социально-

экономических дисциплин на протяжении всего периода обучения. Так, в рамках курса «Правоведение», изучаемого на первом-втором курсах, студенты знакомятся с ключевыми нормативными актами: Федеральным законом «Об информации, информационных технологиях и о защите информации» [13], Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» [12], а также с положениями Кодекса об административных правонарушениях и Уголовного кодекса, устанавливающими ответственность за киберпреступления. Особый акцент делается на рассмотрении реальных судебных дел, связанных с неправомерным доступом к компьютерной информации, распространением вредоносных программ и нарушением правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации. Такой подход не только формирует когнитивный компонент КИБ (знание правовых норм), но и непосредственно воздействует на ценностно-смысловую сферу, демонстрируя неотвратимость и серьёзность юридических последствий.

Дальнейшее углубление правовых аспектов происходит на старших курсах в рамках дисциплины «Информатика», где студенты изучают правовые основы защиты данных, принципы лицензирования программного обеспечения, нормы, регулирующие использование криптографических средств и обработку персональных данных в информационных системах. Параллельно в курсе «Социология и политология» анализируются социальные последствия информационных войн и правовые механизмы противодействия дезинформации, что усиливает гражданскую составляющую ценностно-смыслового компонента. В курсе «Философия» рассматриваются этические дилеммы цифровой эпохи, а в курсе «Культурология» – культура информационной безопасности как часть общей культуры личности в контексте глобальных вызовов техногенной цивилизации.

Принципиально важным методическим инструментом интеграции правовых аспектов выступает кейс-метод «Этика в Цифровом пространстве», разработанный и апробированный в ходе эксперимента. Студентам предлагаются для анализа смоделированные или реальные ситуации, воспроизводящие правовые

коллизии, с которыми инженер может столкнуться в профессиональной деятельности: обнаружение уязвимости в корпоративной системе и дилемма о её разглашении; просьба руководства «обойти» протоколы безопасности для срочного выполнения задачи; использование служебной информации в личных целях. Обсуждение и аргументация позиций в таких кейсах способствуют интернализации правовых ценностей, превращая формальное знание закона в личностно принятый регулятор поведения.

Эффективность предложенной интеграции подтверждается данными трёхлетнего педагогического эксперимента на базе Приволжского института (филиала) МАДИ. Констатирующий этап, результаты которого подробно освещены в диагностическом исследовании [6], зафиксировал низкий уровень ценностно-смыслового компонента более чем у 40% респондентов в экспериментальной и контрольной группах при отсутствии статистически значимых различий между ними. После реализации комплекса педагогических условий, включающего описанную интеграцию правовых модулей, доля студентов с высоким уровнем ценностно-смыслового компонента в экспериментальной группе возросла с 12,6% до 31,0%, а с низким – сократилась с 40,2% до 18,4% (φ-критерий Фишера = 4,549, $p < 0,01$). В контрольной группе, где интеграция не проводилась, значимых сдвигов не выявлено. Эти данные убедительно доказывают, что целенаправленное формирование правосознания является действенным механизмом становления ценностно-смысловой составляющей культуры информационной безопасности.

Таким образом, интеграция правовых модулей в учебный процесс технических вузов решает двуединую задачу: с одной стороны, вооружает будущих инженеров знанием нормативной базы, необходимой для правомерной эксплуатации и защиты информационных систем, а с другой – способствует интериоризации правовых и этических норм, формируя устойчивую внутреннюю мотивацию к безопасному поведению в цифровой среде. С учётом того, что, как справедливо замечают С.П. Серёдкин и И.В. Кулага, «нормативно-правовая база, определяющая общие принципы работы с информацией, требует дальнейшего развития

применительно к образовательной среде» [10], предлагаемая модель может служить практическим ориентиром для такого развития, обеспечивая соответствие подготовки инженеров актуальным законодательным требованиям и вызовам кибербезопасности.

Список литературы

1. Бокова Л.Н. Правовой режим создания безопасной цифровой образовательной среды / Л.Н. Бокова // Вестник РУДН. Серия: Юридические науки. – 2020. – №2. – URL: https://cyberleninka.ru/article/n/pravovoy-rezhim-sozdaniya-bezopasnoy-tsifrovoy-obrazovatelnoy-sredy (дата обращения: 30.04.2026). DOI 10.22363/2313-2337-2020-24-2-274-292. EDN PFSRHB

2. Былевский П.Г. Формирование культуры информационной безопасности граждан России: эволюционная периодизация / П.Г. Былевский // Мир науки. Социология, филология, культурология. – 2023. – Т. 14. № 3. – DOI 10.15862/28KLSK323. EDN ISZOVL

3. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 №646.

4. Ковалев Е.Е. Опыт интеграции правовых компетенций и аспектов информационной безопасности в образовательных программах института математики и информатики МПГУ / Е.Е. Ковалев // Право и цифровые технологии: электрон. сб. ст. Междунар. науч.-практ. конф. – Новополоцк: Полоц. гос. ун-т, 2024. – С. 119–121. EDN EBLYRX

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

6. 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: 30.04.2026). EDN RMYFLC

7. Полякова Т.А. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под ред. Т.А. Поляковой, А.А. Стрельцова. – М.: Юрайт, 2023. – 325 с.

8. Приказ Министерства науки и высшего образования РФ от 04.09.2024 № 579 «О внесении изменений в Порядок разработки дополнительных профессиональных программ... в области информационной безопасности».

9. Северин В.А. Комплексный подход подготовки кадров для обеспечения кибербезопасности: вызовы и проблемы / В.А. Северин // Лоббирование в законодательстве. – 2023. – Т. 2. №2. – С. 16–20. – DOI 10.33693/2782-7372-2023-2-2–16–20. EDN COZFBT

10. Серёдкин С.П. Современные подходы к обеспечению информационной безопасности студентов / С.П. Серёдкин, И.В. Кулага // Информационные технологии и математическое моделирование в управлении сложными системами: электрон. науч. журн. – 2025. – №4. – С. 16–23. EDN SZYVMD

11. 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

12. Федеральный закон от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (ред. от 07.04.2025).

13. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

14. Федеральный закон от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации».

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