Леуцкий Вадим Владимирович
магистрант
ФГБОУ ВО «Кубанский государственный университет»
г. Краснодар, Краснодарский край

ИНТЕГРАЦИЯ ЦИФРОВОЙ БЕЗОПАСНОСТИ В ПРОФЕССИОНАЛЬНУЮ КУЛЬТУРУ ВЫПУСКНИКА ПЕДАГОГИЧЕСКОГО ВУЗА: ВЫЗОВЫ И ПЕРСПЕКТИВЫ

Аннотация: *статья рассматривает интеграцию цифровой безопасности в профессиональную культуру педагога в условиях нарастания информационных угроз. В статье приведены выводы о том, что формирование данной компетенции должно выходить за рамки отдельной дисциплины в вузе и приобретать метапредметный характер. Выделены ключевые направления модернизации подготовки будущих педегогов: внедрение сквозных модулей по кибергигиене в базовые дисциплины, практико-ориентированное обучение на отечественном программном обеспечении и создание в вузе экосистемы безопасного цифрового поведения. Особое внимание уделено этическому компоненту профессиональной культуры педагога как «проводника» ценностей цифровой безопасности. Сделан вывод о необходимости целостного воспитания «цифровой личности» педагога. Материалы применимы при проектировании образовательных программ и курсов повышения квалификации.*

Ключевые слова: *цифровая безопасность, профессиональная культура педагога, педагогическое образование, информационная безопасность, цифровая образовательная среда, компетентностный подход, киберсоциализация.*

В современных условиях быстрорастущего темпа развития новых технологий и внедрение их в общество, что характеризуется беспрецедентной скоростью цифровой трансформации всех социальных институтов, включая образование, повсеместное внедрение электронных образовательных платформ, дистанционных технологий и облачных сервисов, с одной стороны, расширяет дидактические горизонты, а с другой – формирует принципиально новую зону уязвимости.

Утечки конфиденциальных данных, кибербуллинг, фишинговые атаки и деструктивный контент становятся не просто техническими инцидентами, а реальными угрозами психологическому благополучию и безопасности субъектов образовательного процесса.

В таких условиях роль выпускника вуза на примере педагогического направления кардинально меняется. Он перестает быть просто пользователем информационных технологий и превращается в ключевого агента формирования культуры цифровой безопасности у подрастающего поколения. Также как и выпускник любого другого направления, так как в современном мире работа в цифровой среде обязательна почти для всех видов профессий. Однако анализ существующей практики показывает, что подготовка будущих учителей в данной области зачастую носит фрагментарный, сугубо технический или ознакомительный характер. Выпускник педагогического вуза нередко знает о существовании антивируса, но не готов методически грамотно провести классный час о защите персональных данных или выявить признаки вовлечения школьника в деструктивное интернет-сообщество.

Целью данной статьи является теоретическое осмыслении и обосновании стратегических направлений интеграции компетенции цифровой безопасности в структуру профессиональной культуры будущего педагога. И исходить нужно из гипотезы, что цифровая безопасность должна стать не ещё одним отдельным пунктом к учебному плану, а внутренним и главным компонентом профессионального сознания учителя, частью его педагогической этики и методики.

Понятие «профессиональная культура педагога» традиционно включает аксиологический (ценности), технологический (способы деятельности) и личностно-творческий компоненты. Цифровая безопасность в этом контексте долгое время ошибочно свелась лишь к технологическому аспекту – умению настроить брандмауэр или придумать сложный пароль.

Интегративный подход предполагает увеличению внимания к акценту на аксиологию. Профессиональная культура в сфере цифровой безопасности – это не столько владение инструментарием защиты, сколько сформированная

этическая позиция и *ответственное поведение*. Это понимание педагогом того, что любое его действие в цифровой среде (публикация фотографии с его урока, рассылка домашнего задания в мессенджерах, хранение списка класса в облаке) имеет правовые и воспитательные последствия. Если не начать усвоение этих ценностей на уровне профессионального мировоззрения любые инструкции останутся «мертвым грузом».

Педагогические вызовы интеграции на уровне вуза.

Проведенный в рамках диссертационного исследования анализ образовательных программ педагогических вузов позволил выделить ряд системных барьеров, препятствующих эффективной интеграции цифровой безопасности:

– *дисциплинарная изоляция.* Вопросы безопасности вынесены в специализированные курсы для будущих учителей, в то время как студенты других гуманитарных профилей (филологи, историки, учителя начальных классов) остаются практически безоружными перед лицом информационных угроз;

– *дефицит практико-ориентированности.* Традиционное обучение строится на лекционном обзоре нормативных актов (ФЗ-152, ФЗ-436) без отработки реальных кейсов. В результате студент знает о существовании статьи закона, но не может, например распознать фишинговое письмо в собственной электронной почте;

– *технологическое отставание.* Учебные классы вузов зачастую оснащены устаревшим или пиратским программным обеспечением. В то время как государственная политика импортозамещения требует подготовки специалистов, владеющих отечественными решениями (ОС Astra Linux, СЗИ Secret Net, КриптоПро CSP), выпускники покидают стены вуза, не имея опыта работы с ними.

Для решения указанных вызовов целесообразно внедрить следующие стратегические направления, апробированные в ходе экспериментальной работы на базе Кубанского государственного университета.

Цифровая безопасность должна быть тактически внедрена в содержании основных дисциплин. Например:

– в курсе *«Педагогика»* – тема «Профилактика кибербуллинга в детском коллективе: диагностика и воспитательные технологии»;

– в курсе *«Психология»* – тема «Психология влияния и социальная инженерия: как распознать манипуляцию в цифровой среде»;

– в курсе *«Методика обучения предмету»* – раздел «Безопасный поиск и критический анализ информации при подготовке к уроку».

Такой подход обеспечивает формирование целостной картины профессионального мира студента вуза, где безопасность является не отдельной операцией, а базовым условием любой профессиональной деятельности.

Исследование показало высокую эффективность элективного курса «Цифровая безопасность в образовании», построенного исключительно на базе российского программного обеспечения. Студенты, работавшие в среде Astra Linux и использовавшие криптографические средства КриптоПро, демонстрировали не только рост технических навыков (доля студентов с высоким уровнем операционально-технологического компонента выросла с 12% до 53%), но и значительный рост патриотической мотивации и понимания важности технологического суверенитета страны.

Ключевым направлением является развитие у будущих педагогов способности к решению этических дилемм цифровой эпохи. Это предполагает активное использование на семинарах кейс-метода, включающего ситуации морального выбора: допустимо ли читать личную переписку обучающихся для предотвращения трагедии?

Выработка собственной обоснованной позиции по этим вопросам превращает выпускника из исполнителя инструкций в профессионала.

Профессиональная культура не может быть сформирована в «тепличных» условиях. Вуз сам должен стать моделью безопасной цифровой среды. Если в университете студенты повсеместно используют нелицензированное или устаревшее ПО, игнорируют требования к парольной политике и публикуют скриншоты зачеток в открытых каналах, все разговоры о цифровой безопасности на лекциях будут восприниматься как лицемерие. Напротив, внедрение политики

информационной безопасности вуза, использование лицензионного ПО и регулярные тренинги для сотрудников создают ту воспитывающую среду, в которой ответственное поведение становится нормой.

Заключение.

В заключение всего вышеперечисленного важно указать, что внедрение цифровой безопасности в профессиональную культуру выпускника педагогического вуза – это не сиюминутная кампания, а долгосрочная стратегическая задача системы высшего образования. Речь идет о воспитании принципиально нового типа педагога: учителя-наставника, способного не только защитить свои персональные данные, но и подготовить подрастающее поколение инструментами критического мышления и самозащиты в цифровом пространстве.

Как показало исследование, эффективная модель такой интеграции базируется на трех основных элементах: *метапредметное содержание* (безопасность как часть всех дисциплин), *технологическая актуальность* (опора на отечественные ИТ-решения) и *этическая рефлексия* (формирование профессиональной позиции). Реализация этой модели позволит преодолеть существующий разрыв между стремительным развитием информационных угроз и статичностью педагогического образования, обеспечив готовность выпускников к вызовам цифровой реальности.

Список литературы

1. Винник Е.А. Обеспечение защиты информации в образовательных организациях / Е. А. Винник // Молодой ученый. – 2023. – №7 (454). – С. 3–6. – URL: https://moluch.ru/archive/454/100167 (дата обращения: 19.04.2026). EDN XVBDCZ

2. Зимняя И.А. Ключевые компетенции – новая парадигма результата образования / И.А. Зимняя // Эксперимент и инновации в школе. – 2009. – № 2. – URL: https://cyberleninka.ru/article/n/klyuchevye-kompetentsii-novaya-paradigma-rezultata-obrazovaniya (дата обращения: 19.04.2026).

3. 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 Международной научно-практической конференции (г. Краснодар, 14 февраля 2025 г.) / редкол.: В.М. Гребенникова [и др.]. – Чебоксары: Среда, 2025. – С. 136–137. – ISBN 978-5-907965-24-9.

4. Солдатова Г.У. Цифровая компетентность подростков и родителей / Г.У. Солдатова, Е.И. Рассказова, Т.А. Нестик. – М.: Фонд Развития Интернет, 2013. – 144 с. EDN UILWUN

5. Уваров А.Ю. Образование в мире цифровых технологий: на пути к цифровой трансформации / А.Ю. Уваров. – М.: Издательский дом ГУ-ВШЭ, 2018. – 168 с.

6. Пилецкая А.В. Искусственный интеллект и безопасность в современных возможностях / А.В. Пилецкая // Молодой ученый. – 2020. – №20 (310). – С. 50–52. – URL: https://moluch.ru/archive/310/70250/. (дата обращения: 29.03.2025). EDN SQDGCT

7. Приказ Минобрнауки РФ от 23.12.2021 №1185 «О мерах по обеспечению информационной безопасности в образовательных организациях».

8. Федеральный закон от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».