Кузьмин Алексей Владимирович
д-р пед. наук, доцент, руководитель
Центр профессиональной подготовки им. Героя России майора милиции
В.А. Тинькова ГУ МВД России по Московской области
г. Видное, Московская область

DOI 10.31483/r-150001

АСПЕКТЫ ФОРМИРОВАНИЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОЦЕССЕ ПРОФЕССИОНАЛЬНОГО ОБУЧЕНИЯ В ЦЕНТРАХ ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ

***Аннотация**: в статье рассмотрены вопросы формирования культуры информационной безопасности в период профессионального обучения в Центре профессиональной подготовки им. Героя России майора милиции В.А. Тинькова ГУ МВД России по Московской области (далее – ЦПП). Изучены составляющие концепции становления цифрового общества. Раскрыты требования образовательных программ профессионального обучения по формированию навыков цифровой грамотности. Уделено внимание соблюдению культуры информационной безопасности при выполнении служебных обязанностей в период обучения, после окончания. Проведен мониторинг ответов слушателей по применению мер информационной безопасности и выработке предложений по развитию культуры информационной безопасности.*

***Ключевые слова**: профессиональное обучение, цифровая образовательная среда, инновационные технологии, культура информационной безопасности.*

Использование инновационных технологий обучения в период цифровизации общества предусматривает решение вопроса по формированию культуры информационной безопасности. Программа профессионального обучения в ЦПП направлена на изучение информационных технологий для формирования навыков использования информационных технологий в своей профессиональной деятельности, таких как: соблюдение мер и правил безопасности работы в сети, защищенность рабочего места, защита персональных данных, систематизации

полученных знаний использования информационных технологий, формирование цифровой репутации. Отметим, что профессиональная компетенция слушателей ЦПП обеспечивается через культуру информационной безопасности в рамках цифровой грамотности в период обучения. Именно в рамах профессионального обучения осуществляется изучение программного обеспечение компьютера, порядка и правил работы со справочными, поисковыми системами и платформами, основами информационной безопасности, применению способов защиты персональных данных, соблюдению правил техники безопасности при обращении с персональным компьютером и защищенности рабочего места.

Цель исследования – анализ формирования навыков культуры информационной безопасности. Объект исследования – культура информационной безопасности слушателей ЦПП. Предметом исследования являются педагогические условия ее формирования. При написании работы применены методы исследования: анализ источников по теме, изучение, обобщение, анкетирование, интервьюирование слушателей ЦПП.

Культура информационной безопасности – совокупность сформированных знаний, умений и навыков по вопросам информационной безопасности, обеспечивающих безопасное пребывание гражданина Российской Федерации в информационном пространстве [8]. Данное понятие включает в себя нормы поведения, правила и требования, ценностные практики, которые обеспечивают безопасную работу с информацией, применение информационных технологий во всех сферах жизнедеятельности государства. Отметим существенную роль имеет личностное осознание и риск результата поведения пользователей сети Интернет, технические средства защиты. Согласно концепции Ю.М. Вертий – отсутствие риска причинения вреда информацией, сформированное состояние защищенности физического, нравственного развития является информационной безопасностью [1, с. 189]. Естественно, такое понимание информационной безопасности должно обеспечиваться культурой информационной безопасности слушателей, овладением цифровыми навыками работы, формированием профессиональной компетенцией.

Следует согласится с мнением Т.А. Поляковой, которая рассуждает о необходимости формирования научного подхода к повышению грамотности граждан в области информационной безопасности [6, с. 310]. Такое мнение раскрывает механизм взаимодействия компонентов системы обучения в рамках культуры информационной безопасности.

Требует особого анализа мнение И.Д. Рудинского, который выделяет признаки культуры информационной безопасности, отражающиеся в способности: получать информацию, анализировать полученную информацию, определять достоверность и безопасность получаемой информации, мониторить нужный материал из общего массива данных, распространять и контролировать передачу информации с целью недопущения нарушения прав [9, с. 40]. На наш взгляд, перечень этих способностей можно дополнять в виду изменений формата работы с информацией. Е.О. Никитина выделяет показатель сформированности цифровой культуры – увеличение элементов всех уровней культуры [3, с. 71]. Уровни сформированности культуры информационной безопасности имеют отличительные черты, их можно выделить: начальный, осознанный, практический, продвинутый, экспертный. В свою очередь Б.Н. Паньшин в своей работе определяет уровни сформированности цифровой культуры: базовый, функциональный, представительский [5, с. 259]. Обязательное овладение культурой информационной безопасности, достижение ее максимального уровня необходимо для слушателей ЦПП, как представителей закона.

В настоящее время цифровая грамотность стала необходимым атрибутом социального благополучия общества и государства, в виду реализации гражданских прав на получение государственных и муниципальных услуг, онлайн образования, digital-коммуникации. При этом следует отметить возрастающие риски при работе с цифровой информацией, в частности рост преступлений с сфере мошенничества с использованием цифровых технологий.

Вопросы информационной безопасности затрагивают проблемы поиска инновационных технологий обучения, развития цифровых навыков, а также формирование культуры информационной безопасности обучающихся в центрах

профессиональной подготовки. А.В. Поникарова отмечает, что система образования перешла от традиционного образования к образовательному процессу в условиях открытой и объёмной доступности информации [7, с. 345]. Формирование культуры информационной безопасности слушателей центров профессиональной подготовки в период обучения осуществляется с целью адаптации и подготовки к выполнению служебных задач при осуществлении правоохранительных функций, согласно тематики учебных дисциплин программ профессионального обучения, требований нормативно-правовых актов. Процесс формирования культуры информационной безопасности должен охватывать не только слушателей, проходящих обучение, но и преподавателей образовательной организации. Анализ изученных материалов позволяет выделить вопрос культуры информационной безопасности в период обучения.

На коллегии МВД России от 05.03.2025 Президент РФ В.В. Путин отметил необходимость осуществления работы по защите молодых людей от криминальных угроз, в том числе киберпреступности [2]. Основные программы профессионального обучения в период цифровизации учебного процесса предусматривают активное развитие информационной безопасности. Главное значение приобретает модернизация системы безопасности, в том числе культуры информационной безопасности, системы профилактики нарушений, предупреждение преступлений, минимизация рисков от деяний, определения перечня деяний, осуществление которых запрещено [11, с.10] (рис. 1).

Рис. 1. Перечень запрещенных действий согласно требованиям Федерального закона от 27.07.2006 №149 «Об информации, информационных технологиях и о защите информации»

Таким образом, законодатель четко ограничил действия с информацией и определил направления деятельности представителей правоохранительной системы, в рамках выполнения функциональных обязанностей по вопросам профилактики правонарушений, расследованию и раскрытию преступлений. За период январь-июнь 2025 года зарегистрировано на 0,7% больше преступлений в сфере компьютерной информации, чем за аналогичный период прошлого года и составило 38484 преступления, из них по ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» 37636 преступлений, по ст. 273 УК РФ «Использование и распространение вредоносных компьютерных программ» – 253 преступлений [4] (рис. 2).

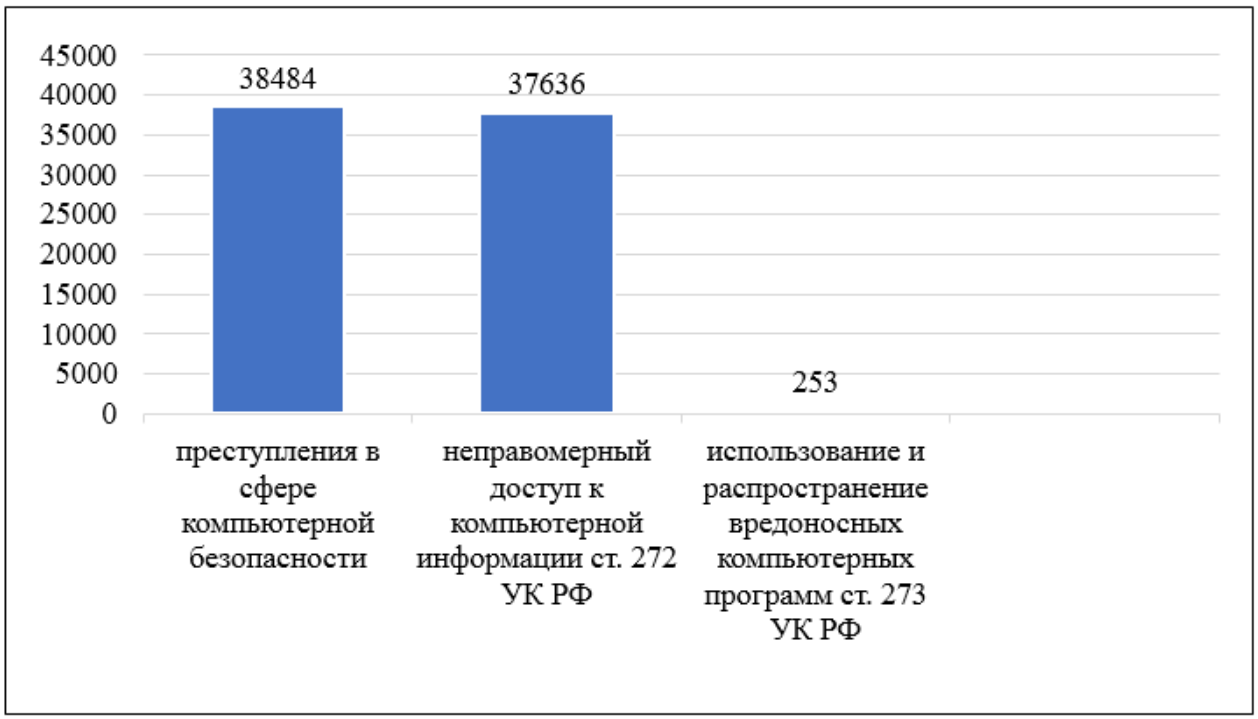

Рис. 2. Сведения о преступлениях за январь–июль 2025, совершенных в сфере компьютерной информации (глава 28 УК РФ)

При этом количество преступлений в сфере IT-информации увеличилось на 14%. Отметим, что в период глобальной цифровизации общества с помощью сети Интернет осуществляется уровень противодействия преступлениям данного вида, в том числе путем нормотворческого характера. Таким образом, защита данных и информационная безопасность становится одной из важных задач перед слушателями и преподавателями в рамках учебного процесса. Преступники, совершающие противоправные деяния в сфере информационной безопасности, с каждым годом внедряют современные способы и методы осуществления преступлений, в связи с чем сотрудникам правоохранительной сферы необходимо иметь высокий уровень знаний по защите информации и уметь реагировать на нарушение закона в полном соответствии с уровнем развития цифровизации, искать новые эффективные средства борьбы с угрозами данного типа. Слушатели ЦПП изучают дисциплины: «Основы информационных технологий и кибербезопасности в деятельности органов внутренних дел Российской Федерации», «Актуальные вопросы деятельности подразделений, специализирующихся на

предотвращении, выявлении, раскрытии и расследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий», именно на местах обучения продолжает формироваться культура информационной безопасности, азы которой должны быть сформированы с ранних лет.

С целью определения приоритетных средств и мер культуры информационной безопасности, было проведено анонимное анкетирование по вопросам информационной безопасности в период обучения в ЦПП, вне служебных рабочих мест, а затем выборочное интервьюирование слушателей, проходящих профессиональное обучение в 2025 году по программе «Профессиональная подготовка лиц среднего и старшего начальствующего состава, впервые принятых на службу в органы внутренних дел Российской Федерации по должности служащего «Полицейский». Изучены и взяты за основу диагностические инструментарии Е.В. Вострецовой, Н.В. Калининой, Н.В. Кузнецовой, В.А. Сластенина, Л.С. Подымова и других, которые адаптированы автором. Формирование культуры информационной безопасности слушателей целеориентировано на поиск методов и средств реализации учебного процесса. В анонимном тестировании приняли участие 60 человек, которые занимали должность менее 6 месяцев, возраст анкетируемых данной категории – от 21 года до 25 лет, сотрудники женского пола составили 24 человека (40%). Образование анкетируемых – высшее (100%), при этом юридическое образование – 30 сотрудников (50% от общего числа опрошенных). По критериям использования мер информационной безопасности ответы распределились следующим образом – слушателями в полном объёме были отмечены меры: размещение минимальной личной информации в сети Интернет и в социальных сетях, избежание раскрытия конфиденциальной информации. По данному вопросу все опрошенные показали положительные ответы применения в своей деятельности, что составило – 100%. При формировании паролей сложные пароли придумывают 60% опрошенных, что объясняется не субъектной ответственностью сотрудника, а проблемой делегирования ответственности внешним системам к безопасности сайта, требованиям к формулировке пароля. Качественный антивирус используют в своей деятельности 80% опрошенных, при

этом 20% дополнительно сообщили об использовании антивируса в обязательном порядке, однако не считают его защиту максимальной в силу окончания бесплатного периода пользования. 80% опрошенных указали на применение двухфазной аутентификации (2FA) при регистрации на сайтах, где это не обязательно, но возможно. Ответившие на данный вопрос пояснили о выборе комбинаций: пароль, код из смс или e-mail. 90% опрошенных выделили, что в своей жизнедеятельности используют только те сайты, доступ к которым не блокирует установленная программа антивируса, остальные 10% знают о потенциальных рисках. Отсутствие личной информации в сети Интернет отметили более 90%, при этом 10% затруднились ответить. Опрошенные пояснили, что их ответы в отношении размещения личной информации в данном вопросе не касаются официальных государственных платформ, таких как «Государственные услуги», «Налоги» и другие. Выбор реальных мер культуры информационной безопасности продемонстрировал, что 80% опрошенных не сохраняют пароли на компьютере от личных кабинетов различных сайтов. 20% сохраняют, но только на тех сайтах, где уверены о недопущении взлома, минимизации причинения ущерба. 50% опрошенных указали на использование защищенного соединения Wi-Fi, остальные – 50% опрошенных не всегда знают, защищенное ли это соединение в том месте, где они прибывают (рис. 3). Полученные ответы и предложения позволяют проанализировать риск при формировании культуры информационной безопасности. При деятельностном подходе риск является мерой успешности совместной деятельности преподавателя и обучающихся. Таким образом, в дополнение к аудиторным занятиям необходимо разработать систему внеаудиторной работы, которая обладает мощным ресурсом в повышении уровня культуры информационной безопасности, а также предусматривает разработку практикума по программам профессиональной подготовки для всех категорий обучающихся по вопросам формирования культуры информационной безопасности слушателей ЦПП.

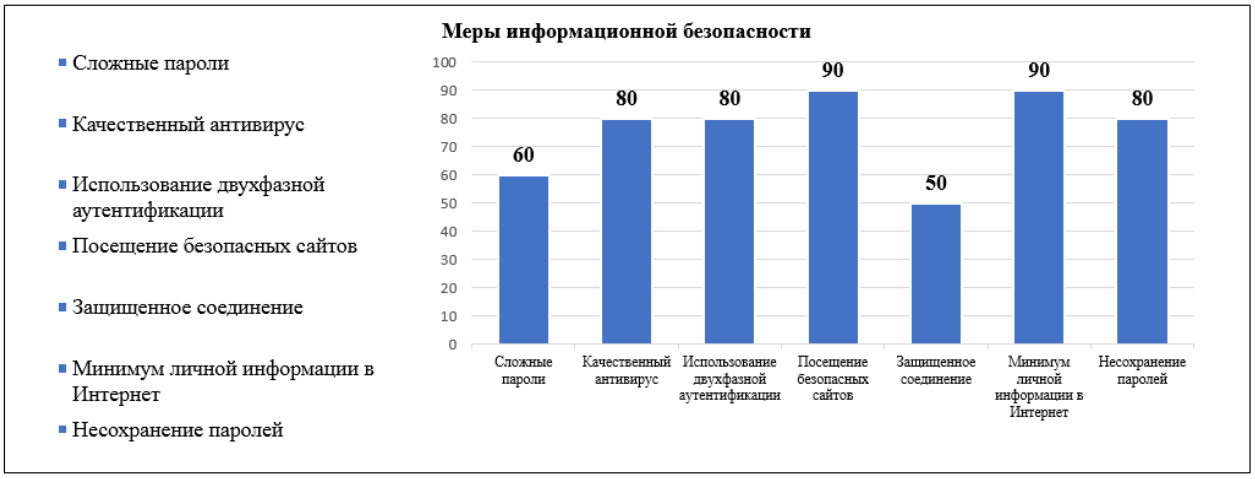

Рис. 3. Результаты ответов на вопрос о мерах информационной безопасности, которые используются ими в период служебной деятельности (n = 60)

Результаты тестирования позволяют сформулировать представление о применении базовых правил культуры информационной безопасности. Отметим, что вопросы культуры иинформационной безопасности необходимо изучать в рамках наставничества в подраздлениях. Развитие культуры информационной безопасности является непрерывным процессом. Необходимо постоянное развитие профессиональной зрелости слушателей, направление должного внимания на самовоспитание и саморазвитие как специалиста в области информационной безопасности [10, с. 213]. Проведённый мониторинг проблемы исследования позволяет сформулировать педагогические условия по формированию культуры информационной безопасности в период обучения: развитие уровня культуры безопасности обучающихся путем повышения квалификации информационной безопасности преподавательского состава в рамках цифровой грамотности; самообразования по направлению овладения цифровыми навыками; реализации основных программ профессионального обучения на высоком методическом уровне путем предоставления доступа к информационно-коммуникационным системам, справочно-правовым и специализированных профессиональным системам; формирования навыков использования электронных образовательных ресурсов по учебным дисциплинам и учебно-методических материалов с учетом требований культуры информационной безопасности. Обладание навыками по приобретению,

пополнению и систематизации полученных знаний по основам использования информационных технологий в профессиональной деятельности является задачей профессионального обучения.

Список литературы

1. Вертий Ю.М. Цифровая культура населения как основа конституционно-правового механизма обеспечения информационной безопасности России / Ю.М. Вертий // Экономика, политика, право: актуальные вопросы, тенденции и перспективы развития: материалы XXII Международной научно-практической конференции. – Ростов н/Д., 2024. – С. 189. – EDN VOCPAO

2. Выступление Президента Российской Федерации на коллегии МВД России 05.03.2025. Информационные ресурсы Президента Российской Федерации [Электронный ресурс]. – Режим доступа: http://kremlin.ru/events/president/news/76408. (дата обращения: 10.08.2025).

3. Никитина Е.О. Педагогические условия развития информационной культуры курсантов образовательных организаций МВД России: монография / Е.О. Никитина. – М.: Московский университет МВД России им. В.Я. Кикотя, 2017. – С. 71. – EDN XRDEJF

4. Официальный сайт МВД России. Сведения о состоянии преступности [Электронный ресурс]. – Режим доступа: https://xn--b1aew.xn--p1ai/reports/item/67755056/ (дата обращения: 02.08.2025).

5. Паньшин Б.Н. Роль цифровой культуры в развитии современного города / Б.Н. Паньшин // Urbis et Orbis. Микроистория и семиотика города. – 2023. – Т. 3. №2. – С. 259. – DOI 10.34680/urbis-2023-3(2)-259-270. – EDN OACSMK

6. Полякова Т.А. Образование и культура информационной безопасности граждан Российской Федерации: научно-правовые аспекты / Т.А. Полякова, Н.А. Троян // Образование и право. – 2023. – №3. – С. 310. – DOI 10.24412/2076-1503-2023-3-310-317. – EDN ROFGQT

7. Поникарова А.В. К вопросу формирования культуры информационной безопасности школьников / А.В. Поникарова, Ю.И. Богатырева // Личностное и

профессиональное развитие будущего специалиста. – Тамбов: Державинский, 2019. – С. 345. – EDN GLIMPQ

8. Распоряжение Правительства РФ от 22.12.2022 №4088-р «О Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации» (с изм. и доп.). // СПС «КонсультантПлюс».

9. Рудинский И.Д. Формирование культуры информационной безопасности студентов колледжа / И.Д. Рудинский, Д.Я. Околот // Информатика и образование. – 2019. – №9 (308). – С. 40.

10. Самедова Ю.А. Педагогические аспекты формирования критического мышления как средства информационной безопасности будущих офицеров в условиях военного вуза / Ю.А. Самедова, А.Н. Дорохов, С.Ю. Григоров // Современные наукоемкие технологии. – 2021. – №2. – С. 213. – DOI 10.17513/snt.38520. – EDN JPKTGD

11. Федеральный закон от 27.07.2006 №149 «Об информации, информационных технологиях и о защите информации» (с изм. и доп.). // СПС «КонсультантПлюс».