ISSN 2949-1150 (online)
2071-8284 (print)

Научная статья
УДК 343.98

Особенности подготовки специалистов для расследования преступлений в сфере компьютерной информации

Александр Анатольевич Нечай[1], кандидат педагогических наук, доцент
Анна Владимировна Ничагина[2], кандидат педагогических наук, доцент

[1] Санкт-Петербургский университет МВД России
Санкт-Петербург (198206, ул. Летчика Пилютова, д. 1), Российская Федерация
[2] Ленинградский государственный университет имени А. С. Пушкина
Санкт-Петербург (196605, Петербургское шоссе, д. 10), Российская Федерация
[1] webexpromt@mail.ru, [2] 89315104502@mail.ru
[1] https://orcid.org/0000-0002-1202-4830, [2] https://orcid.org/0000-0001-7630-0446

Аннотация:
Введение. *В современных условиях, когда использование интернета и информационных технологий стремительно развивается, преступления в сфере компьютерной информации становятся актуальной проблемой. Сотрудники правоохранительных органов сталкиваются с трудностями в расследовании таких преступлений из-за недостатка специальных знаний и навыков. Актуальность исследования заключается в необходимости повышения готовности правоохранительных органов к борьбе с киберпреступностью и разработки эффективных методов реагирования на новые вызовы.*
Методы. *В рамках исследования был разработан инструмент в сфере информационной безопасности, известный как «Контрольный список необходимых навыков для расследователя преступлений в сфере компьютерной информации» (далее – Контрольный список). В исследовании приняли участие две группы курсантов Санкт-Петербургского университета МВД России, где одна группа обучалась по традиционной программе, а другая – с акцентом на навыки, указанные в контрольном списке. Для анализа результатов использовался критерий Пирсона χ^2.*
Результаты. *Результаты исследования показали, что в экспериментальной группе 69,57 % курсантов достигли положительных результатов в освоении необходимых навыков, в то время как в контрольной группе этот показатель составил лишь 27,27 %. Полученные результаты исследования подчеркивают важность систематического обучения сотрудников правоохранительных органов в области кибербезопасности и целесообразности внедрения Контрольного списка в практику.*

Ключевые слова:
преступления в сфере компьютерной информации, кибербезопасность, профессиональные компетенции в области расследования, контрольный список, правоохранительные органы

Для цитирования:
Нечай А. А., Ничагина А. В. Особенности подготовки специалистов для расследования преступлений в сфере компьютерной информации // Вестник Санкт-Петербургского университета МВД России. 2025. № 4 (108). С. 251–261.

Статья поступила в редакцию 06.04.2025; одобрена после рецензирования 30.09.2025; принята к публикации 25.12.2025.

Original article

Characteristic features of training specialists for investigating crimes in the field of computer information

Alexander A. Nechai[1], Cand. Sci. (Ped.), Docent
Anna V. Nichagina[2], Cand. Sci. (Ped.), Docent

[1] Saint Petersburg University of the MIA of Russia
1, Letchika Pilyutova str., Saint Petersburg, 198206, Russian Federation
[2] Saint Petersburg State University named after A. S. Pushkin
10, Petersburg hig., Saint Petersburg, 196605, Russian Federation
[1] webexpromt@mail.ru, [2] 89315104502@mail.ru
[1] https://orcid.org/0000-0002-1202-4830, [2] https://orcid.org/0000-0001-7630-0446

Abstract:
Introduction. *In today's world, with the rapid development of the Internet and information technologies, crimes in the field of computer information are becoming a pressing issue. Law enforcement officers face difficulties in investigating such crimes due to the lack of specialised knowledge and skills. The relevance of the study lies in the need to improve the readiness of law enforcement agencies to combat cybercrime and develop effective methods of responding to new challenges.*
Methods. *As part of the study, an information security tool was developed, known as the "Checklist of essential skills for investigators of crimes in the field of computer information" (hereinafter referred to as the Checklist). Two groups of cadets from St. Petersburg University of the Ministry of Internal Affairs of Russia participated in the study, with one group being trained according to the traditional academic course working program and the other one – with an emphasis on the skills specified in the checklist. Pearson's χ^2 criterion was used to analyse the results.*
Results. *The results of the study showed that in the experimental group, 69,57 % of cadets achieved positive results in mastering the necessary skills, while in the control group, this figure was only 27,27 %. The results of the study emphasise the importance of systematic training of law enforcement officers in the field of cybersecurity and the advisability of implementing the Checklist in practice.*

Keywords:
crimes in the field of computer information, cybersecurity, professional investigative competencies, checklist, law enforcement agencies

For citation:
Nechai A. A., Nichagina A. V. Characteristic features of training specialists for investigating crimes in the field of computer information // Vestnik of Saint Petersburg University of the MIA of Russia. 2025. № 4 (108). P. 251–261.

**The article was submitted April 6, 2025;
approved after reviewing September 30, 2025;
accepted for publication December 25, 2025.**

Введение

В условиях стремительного развития информационных технологий и повсеместного использования интернета проблема расследования преступлений в сфере компьютерной информации становится все более актуальной. Увеличение числа пользователей сети и рост числа киберпреступлений создают новый вызов для правоохранительных органов, которые должны адаптироваться к изменяющейся природе преступности. Преступления в этой области представляют собой сложное и динамично развивающееся явление, требующее от сотрудников полиции глубоких знаний в области компьютерных технологий и специальной подготовки для эффективного расследования таких дел [1].

В последние десятилетия развитие информационно-коммуникационных технологий (далее – ИКТ) привело к возникновению такого явления, как преступления в сфере компьютерной информации, включая взломы и использование вредоносного программного обеспечения, что стало большой социальной проблемой и серьезным вызовом для правоохранительных органов. Виртуальная среда предоставляет множество возможностей для незаконной деятельности, что негативно сказывается на экономической и социальной безопасности. Правоохранительным органам необходимо заранее планировать эффективные меры по предотвращению киберпреступлений и реагированию на них, учитывая различные технические и законодательные сложности [2].

Научная проблема заключается в недостаточной подготовленности сотрудников правоохранительных органов к ведению расследований в сфере компьютерной информации, а также в отсутствии четких критериев для определения необходимых квалификаций и технических навыков. Преступления в сфере компьютерной информации наносят значительный ущерб гражданам и обществу, подрывая основы экономической и социальной безопасности. Важно понимать, что киберпреступления – совершенно особый вид криминальной деятельности и требует пересмотра подходов к их расследованию, а также адаптации существующих методов к новым условиям.

Научная новизна исследования заключается в его направленности на преступления в сфере компьютерной информации как уникальной категории, отличающейся от традиционных правонарушений. Исследование включает анализ методов расследования и стратегий предотвращения преступлений в этой области, основанных на профессиональных навыках, необходимых сотрудникам правоохранительных органов в сфере компьютерной безопасности. В рамках исследования акцентируется внимание на ключевых вопросах, касающихся необходимых навыков, которые должны иметь полицейские для успешного расследования киберпреступлений, а также способностей, требуемых от оперативных подразделений для эффективного выполнения их задач.

Цель исследования: разработка и оценка методики подготовки специалистов для расследования преступлений в сфере компьютерной информации. Для достижения этой цели поставлены задачи: контент-анализ компетенций программы подготовки, обновление учебного материала с акцентом на ключевые навыки, включая знание современных информационных технологий и оценку угроз кибербезопасности, а также разработка инструмента оценки квалификаций для выявления и оценки знаний сотрудников правоохранительных органов.

ISSN 2949-1150 (online)
2071-8284 (print)

База исследования. Исследование проводилось с использованием методов педагогического эксперимента с участием двух параллельных групп курсантов 3-го курса Санкт-Петербургского университета МВД России, обучающихся по специальности 10.05.05 – «Безопасность информационных технологий в правоохранительной сфере», специализация – «Компьютерная экспертиза». Формирование экспериментальной (n = 23) и контрольной (n = 22) групп осуществлялось методом случайного отбора с соблюдением принципов эквивалентности по следующим параметрам: исходный уровень подготовки (результаты входного тестирования); средний балл успеваемости за предыдущий семестр; возрастно-половой состав; продолжительность обучения по программе.

Для обеспечения валидности эксперимента группы были уравнены по ключевым характеристикам с применением статистических методов проверки однородности (критерий Манна-Уитни, $p > 0{,}05$). Контрольная группа обучалась по традиционной программе, экспериментальная – с использованием разработанного авторами контрольного списка навыков и модернизированных методик.

Проблеме выявления и расследования преступлений в сфере компьютерной информации посвящено значительное количество научных исследований. В частности, рассматриваются аспекты раскрытия и расследования таких преступлений, как в Российской Федерации, так и за рубежом, включая опыт различных стран (В. О. Аманкулиева, М. В. Жижина, Д. В. Завьялова) [3; 4]. Исследуются особенности расследования компьютерных преступлений, включая методики и подходы к их проведению (Т. В. Лукьянова) [5], а также опыт различных стран в данной области (Е. А. Москалева, А. И. Раду) [6]. Дополнительно рассматриваются ключевые особенности розыскных мероприятий при расследовании преступлений, совершаемых в сфере компьютерной информации (А. С. Киселев, К. А. Горбунова) [7], и специфические моменты производства экспертиз при анализе мошенничества (А. М. Милащенко) [8]. Кроме того, исследуются вопросы становления и развития российского уголовного законодательства в данной области (И. А. Патраш) [2]. Рассматриваются современные реалии расследования уголовных дел о преступлениях, связанных с терроризмом и экстремизмом в интернет-пространстве (В. Д. Петровских) [1], цифровое доказательственное право при производстве по уголовным делам о преступлениях в сфере компьютерной информации (А. Б. Сергеев) [9] и методика проведения практических занятий по дисциплине «Расследование преступлений в сфере компьютерной информации» (М. О. Янгаева) [10].

Термин «*преступление в сфере компьютерной информации*» возник в начале 60-х гг. в американской печати, когда были зафиксированы первые случаи преступлений с использованием компьютеров [11]. В обобщенном виде это понятие охватывает преступное поведение, осуществляемое с помощью компьютеров и интернета, включая действия, в которых компьютер может выступать как инструмент для совершения преступления, объект преступного посягательства или средство для хранения и передачи информации. Однако в научной литературе до сих пор отсутствует единое и общепризнанное определение данного термина, что затрудняет его понимание [12].

Часто термины «преступление в сфере компьютерной информации» и «киберпреступление» употребляются как синонимы, хотя на самом деле они имеют различные значения. Преступление в сфере компьютерной информации охватывает действия, непосредственно связанные с компьютером, в то время как *киберпреступление* представляет собой более широкое понятие, включающее разнообразные виды преступлений, использующих информационные технологии. Важно отметить, что «преступление в сфере компьютерной информации» – это термин, который используется в главе 28 Уголовного кодекса Российской Федерации[1] и связан с компьютером как материальным предметом, что подчеркивает его специфическую природу в контексте правоприменения [13].

С учетом природы преступлений в сфере компьютерной информации можно выделить *четыре основные категории*: преступления против личности, направленные на причинение вреда конкретным людям (взлом, кибербуллинг, мошенничество с картами); преступления против собственности, охватывающие угрозу собственности (интеллектуальная собственность, кибервандализм, передача вредоносного программного обеспечения); преступления против организаций, совершаемые против правительственных учреждений и компаний (кибертерроризм, распространение пиратского программного обеспечения); преступления против общества, включая распространение порнографии, фишинг и продажу незаконных товаров [14].

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 28.02.2025) // Собрание законодательства Российской Федерации (далее – СЗ РФ). 1996. № 25. Ст. 2954.

Методы расследования преступлений в сфере компьютерной информации включают: осмотр места происшествия для выявления виртуальных и трасологических следов; обеспечение неприкосновенности носителей следов, исключая контакт с устройствами; изъятие электронных носителей с копированием данных и использованием специализированных средств; привлечение специалистов для анализа изъятых данных; допрос подозреваемых с применением психологических приемов; производство обыска на основании предположений о наличии оборудования; проведение судебной компьютерно-технической экспертизы; создание единого криминалистического учета ключей шифрования и данных о программно-техническом обеспечении. Эти методы требуют от следователей юридических и технических знаний, основанных на профессиональных навыках, необходимых сотрудникам полиции в области компьютерной безопасности, а также постоянного обновления информации о современных технологиях [5, 15].

Стратегии предотвращения преступлений в сфере компьютерной информации включают обучение сотрудников основам кибербезопасности через регулярные тренинги, внедрение практики обновления программного обеспечения для снижения рисков уязвимостей, использование многофакторной аутентификации (MFA) для защиты учетных записей, инвестиции в современные технологии безопасности, разработку четких политики безопасности и процедур реагирования на инциденты, а также активное сотрудничество и обмен информацией между организациями и правоохранительными органами. Дополнительно важны регулярные аудиты безопасности, программы повышения осведомленности пользователей и создание систем мониторинга инцидентов для быстрого реагирования на угрозы [16].

Как показывают исследования [10; 15–18], для успешной борьбы с преступлениями в сфере компьютерной информации необходимо развивать знания и навыки сотрудников правоохранительных органов, а также обеспечивать их необходимыми ресурсами и оборудованием. Это подчеркивает актуальность нашего эксперимента, который направлен на анализ и обновление учебных программ для подготовки специалистов в данной области.

Методы

Разработанная авторская методика подготовки специалистов в области расследования компьютерных преступлений основывается на синтезе компетентностного и контекстного подходов в профессиональном образовании. Методика включает три компонента: диагностический, содержательно-методический и оценочный.

Диагностический компонент предполагает комплексный анализ профессиональных дефицитов через призму требований профессионального стандарта «Специалист по защите информации» (приказ Минтруда от 14 сентября 2022 г. № 525н[2]). На данном этапе применялись методы контент-анализа нормативных документов и анкетирования научно-педагогического состава, что позволило выявить ключевые проблемные зоны в подготовке специалистов, в частности, недостаточную практическую ориентированность курсов по компьютерной криминалистике.

Содержательно-методический компонент реализуется через систему специально разработанных практико-ориентированных заданий, моделирующих профессиональную деятельность следователя в цифровой среде. Особое внимание уделяется кейс-методу, где используются адаптированные материалы реальных уголовных дел, что соответствует принципам аутентичного обучения. Технология динамических симуляций, реализуемая на платформе *CyberLab*, обеспечивает формирование профессиональных навыков в условиях, максимально приближенных к реальной оперативной работе.

Оценочный компонент методики базируется на принципах формирующего оценивания и включает многоуровневую систему контроля, где особую роль играет разработанный авторами Контрольный список профессиональных навыков. Данный инструмент позволяет не только фиксировать достижение запланированных результатов обучения, но и осуществлять коррекцию образовательного маршрута каждого курсанта.

Реализация методики обеспечивает последовательное формирование профессиональных компетенций через систему взаимосвязанных учебных задач, что соответствует требованиям федеральных государственных образовательных стандартов высшего образования по направлению подготовки 10.05.05 «Безопасность информационных технологий в правоохранительной

[2] Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах» : приказ Министерства труда и социальной защиты Российской Федерации (далее – Минтруд России) от 14 сентября 2022 г. № 525н (зарег. в Минюсте России 14.10.2022, № 70543) // Официальный интернет-портал правовой информации (www.pravo.gov.ru) : [сетевое издание]. URL: http://publication.pravo.gov.ru/Document/View/0001202210170003 (дата обращения: 24.05.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

сфере». Особенностью методики является ее адаптивность, позволяющая оперативно вносить коррективы в содержание обучения с учетом изменений в сфере информационной безопасности и законодательной базе.

Педагогический эксперимент осуществлялся в рамках трех последовательных этапов, что соответствует общепринятой методологии организации научно-педагогических исследований.

На первом, констатирующем этапе, проводившемся в сентябре 2024 года, был выполнен комплекс диагностических процедур, включавший экспертизу содержания рабочей программы дисциплины, анализ учебно-методического обеспечения и входное тестирование курсантов. Результаты данного этапа позволили выявить существенный дисбаланс между теоретической и практической составляющими подготовки, а также установить недостаточный уровень владения современными методами цифровой криминалистики у обучающихся.

На данном этапе мы провели контент-анализ рабочей программы дисциплины (далее – РПД) по направлению подготовки 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», по профилю подготовки: «Технологии защиты информации в правоохранительной сфере».

В рамках данного этапа мы определили, что дисциплина «Основы информационных технологий и кибербезопасности органов внутренних дел Российской Федерации» играет важную роль в системе подготовки специалистов в области правоохранительных органов. Она имеет общую трудоемкость три зачетные единицы, что эквивалентно 108 часам, и изучается в течение второго семестра на дневном отделении. В рамках курса предусмотрены аудиторные занятия, которые составляют 60 часов, включая 14 часов лекций и 46 часов практических занятий, а также 44 часа на самостоятельную работу. Результаты освоения дисциплины требуют овладения компетенциями: ОПК-9; ОПК-11; ОПК-12.

Для эффективного выполнения задач оперативных подразделений в сфере расследования преступлений в области компьютерной информации необходим ряд ключевых навыков и способностей. Во-первых, понимание места и роли кибербезопасности в системе национальной безопасности (ОПК-9.з.1) и знание современных информационных технологий (ОПК-12.з.1) обеспечивают у обучающихся развитие профессиональных навыков быть в курсе актуальных угроз и методов защиты. Осведомленность о строении и функциях подсистем безопасности (ОПК-11.з.1) важна для оценки уязвимостей, а знание вопросов эксплуатации единой системы информационно-аналитического обеспечения МВД (ПК-8.з.1) необходимо для эффективного использования ресурсов. Понимание методов аналитической работы (ПК-8.з.2) также является важным для обеспечения комплексной защиты информации.

Кроме того, умение классифицировать и оценивать угрозы кибербезопасности (ОПК-9.у.1) позволяет выявлять потенциальные риски, а способность рационально выбирать средства и методы киберзащиты (ОПК-11.у.2) обеспечивает эффективную защиту данных. Применение нормативных правовых актов (ОПК-11.у.3) является обязательным условием соблюдения законности, а умение выбирать современные технологии (ОПК-12.у.1) гарантирует актуальность принимаемых решений. Владение профессиональной терминологией (ОПК-9.в.1) и знание методов киберзащиты (ОПК-9.в.2) позволяют эффективно реагировать на угрозы. Навыки установки и технического обслуживания операционных систем (ОПК-11.в.1) и работы в информационно-аналитических системах (ПК-8.в.1) обеспечивают необходимую подготовленность сотрудников. Все эти навыки формируют базу для успешного расследования преступлений в сфере компьютерной информации и поддерживают высокий уровень безопасности в органах внутренних дел.

Основываясь на авторской модели информационно-правового знания специалистов в сфере расследования компьютерных преступлений (Д. И. Чукова, Д. А. Медведев, М. В. Литвиненко) [18] и комплексе специальных знаний, необходимых для расследования преступлений в сфере компьютерной информации (Э. В. Лантух, В. С. Ишигеев, О. П. Грибунов) [17], а также на анализе РПД, была разработана трехуровневая структура профессиональных компетенций. Данная структура отражает поэтапное формирование компетенций: от базовых знаний через практические умения до автоматизированных навыков, обеспечивающих эффективное расследование преступлений в сфере компьютерной информации (таблица 1).

Второй, формирующий этап исследования, реализованный в период с октября 2024 по март 2025 года, характеризовался внедрением модернизированной методики подготовки, основанной на интеграции кейс-технологий и практико-ориентированного подхода. Особое внимание уделялось организации учебного процесса в условиях специализированной цифровой лаборатории, что обеспечивало формирование профессиональных умений в условиях, максимально приближенных к реальной оперативной деятельности. Регулярный мониторинг образовательных результатов подтвердил эффективность применяемых педагогических технологий.

В ходе исследования учебные материалы дисциплины были актуализированы (таблица 2). Для каждого раздела применялись классические методы активного обучения (мозговой штурм,

кейс-анализ, ролевые игры), а также адаптированы формы и средства преподавания, что повысило соответствие программы современным требованиям кибербезопасности.

Таблица 1

Структура профессиональных компетенций для расследования преступлений в сфере компьютерной информации

Table 1

Structure of professional competencies for investigating crimes in the field of computer information

Компонент компетенции	Описание	Рабочая программа дисциплины		Уровень значимости
		уровень освоения	индекс компетенции	
Знание сетевых технологий	Понимание модели OSI, TCP/IP, принципов работы межсетевых экранов и VPN	Знание (З)	ОПК-11.з.1	Базовый
Знание файловых систем	Понимание структур FAT, NTFS, EXT, ReFS и особенностей восстановления данных	Знание (З)	ОПК-11.з.2	Базовый
Умение работать с аппаратным обеспечением	Применение знаний о компонентах компьютерных систем при проведении экспертизы	Умение (У)	ОПК-12.у.1	Повышенный
Умение составлять технические отчеты	Документирование процессов и результатов цифровой экспертизы	Умение (У)	ОПК-12.у.2	Критический
Навык сохранения цифровых доказательств	Соблюдение процессуальных норм при изъятии, фиксации и хранении электронных доказательств	Навык (Н)	ОПК-11.н.1	Критический
Навык виртуализации	Создание и настройка изолированных сред для анализа вредоносного ПО	Навык (Н)	ОПК-11.н.2	Повышенный

Обновленная учебная программа включает разнообразные методы и приемы, которые помогли студентам не только усвоить теоретические знания, но и развить практические навыки, необходимые для работы в сфере кибербезопасности.

По итогам изучения дисциплины нами был разработан и внедрен инструмент оценки сформированности профессиональных компетенций в сфере информационной безопасности, названный «*Контрольный список необходимых навыков для расследователя преступлений в сфере компьютерной информации*» (далее – Контрольный список). При разработке данного списка мы учли:

– постановление Правительства Российской Федерации от 6 мая 2016 г. № 399[3]; приказы Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н[4] и от 14 сентября 2022 г. № 525н[5]; приказ Минобрнауки России от 17 ноября 2020 г. № 1427[6];

[3] Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса (вместе с «Правилами организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса») : постановление Правительства Российской Федерации от 6 мая 2016 г. № 399 (ред. от 11.07.2018) // СЗ РФ. 2016. № 20. Ст. 2838.

[4] Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах» : приказ Министерства труда и социальной защиты Российской Федерации (далее – Минтруд России) от 14 сентября 2022 г. № 525н (зарег. в Минюсте России 14.10.2022, № 70543) // Официальный интернет-портал правовой информации (www.pravo.gov.ru) : [сетевое издание]. URL: http://publication.pravo.gov.ru/Document/View/0001202210170003 (дата обращения: 24.05.2025).

[5] URL: http://publication.pravo.gov.ru/Document/View/0001202210170003 (дата обращения: 24.05.2025).

[6] Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность : приказ Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427 (ред. от 27.02.2023) (зарег. в Минюсте России 18.02.2021, № 62548) // Там же. URL: http://publication.pravo.gov.ru/Document/View/0001202102180040 (дата обращения: 24.05.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

– результаты работы коллег [10; 17; 18] по вопросам информационной безопасности и личный педагогический опыт [12; 19].

Таблица 2

Актуализация рабочей программы дисциплины «Основы информационных технологий и кибербезопасности органов внутренних дел Российской Федерации»

Table 2

Updating the academic course working program "Fundamentals of Information Technologies and Cybersecurity of the Internal Affairs Bodies of the Russian Federation"

Наименование разделов и тем	**Кол-во часов**	**Обновление материала (дидактические компоненты)**	**Результат с учетом компетенций**
Характер понятия информации	6	Метод мозгового штурма для свободного обмена мыслями о значении информации и ее роли в современном мире	Развитие критического мышления и осмысление понятий
Основные понятия и представления теории информации	6	Использование визуальных инструментов (инфографика, диаграммы) и обсуждения в малых группах	Улучшение усвоения теоретических аспектов и моделирование проблемных ситуаций
Модели информационных процессов передачи, обработки и хранения данных	14	Внедрение симуляционных игр для моделирования процессов передачи и обработки данных	Возможность увидеть, как работают различные модели на практике
Автоматизированные информационные системы, их задачи и функции	18	Анализ кейсов для изучения конкретных примеров автоматизированных систем в правоохранительных органах	Понимание влияния автоматизированных систем на эффективность работы
Документационные автоматизированные информационные системы	12	Работа с реальными документами и системами для практического понимания их функционирования	Осознание роли документационных систем в расследовании преступлений
Информационные технологии в правоохранительной сфере	28	Ролевые игры, где обучающиеся выступали в роли следователей и аналитиков	Понимание динамики взаимодействия между участниками процесса
Нормативно-правовое обеспечение кибербезопасности	8	Выполнение заданий на основе анализа законодательных актов и нормативных документов	Углубленное понимание правовых аспектов работы в сфере кибербезопасности
Принципы обеспечения компьютерной безопасности	12	Практические занятия семинарского типа для применения полученных знаний при разработке стратегий защиты информации	Способность применять теоретические знания на практике

Для удобства работы мы создали бланк Контрольного списка. Цель данного инструмента заключается в выявлении и оценке знаний и технических навыков, необходимых сотрудникам правоохранительных органов для эффективного расследования преступлений в области компьютерной информации.

Вводная часть Контрольного списка представляет собой анкету, предназначенную для сбора личных данных сотрудников правоохранительных органов, участвующих в расследовании преступлений в сфере компьютерной информации. Этот раздел включает в себя вопросы о возрасте, поле, семейном положении, уровне образования, полицейском ранге, стаже службы и опыте работы с киберпреступлениями. Сбор этих данных позволит оценить квалификацию и опыт участников, а также выявить их готовность к расследованию преступлений в области компьютерной безопасности.

Основная часть состоит из четырех осей:

Первая ось Контрольного списка посвящена уровню знакомства участников с инструментами и методами, используемыми для совершения киберпреступлений. Вопросы в этой оси охватывают такие темы, как компьютерные вирусы, трояны, программы для взлома паролей и социальная инженерия. Оценка знаний в этой области позволит определить, насколько хорошо сотрудники понимают механизмы, используемые преступниками, и как это знание может помочь в их расследованиях.

Вторая ось фокусируется на уровне осведомленности о некоторых аспектах киберпреступности, включая известные случаи преступлений, текущую реальность, категории преступников и законодательство, касающееся этих преступлений. Этот раздел помогает понять, насколько сотрудники правоохранительных органов осведомлены о современных тенденциях в области киберпреступности и как это знание может быть применено в их работе.

Третья ось Контрольного списка касается уровня знаний о различных типах киберпреступлений и их характеристиках. Вопросы этой оси позволяют оценить, насколько хорошо участники понимают такие преступления, как кража данных, кибертерроризм и мошенничество.

Четвертая ось направлена на уровень знакомства с программами и инструментами, используемыми в расследовании киберпреступлений, что важно для эффективного выполнения служебных обязанностей.

Для оценки ответов участников исследования на утверждения основных переменных использовалась пятибалльная шкала Лайкерта [20], где значения соответствуют следующим категориям: «отлично» (5), «очень хорошо» (4), «хорошо» (3), «плохо» (2) и «очень плохо» (1).

Разработанный инструмент был апробирован на экспериментальной группе (далее – ЭГ) курсантов, обучавшихся с упором на Контрольный список необходимых навыков, в то время как контрольная группа (далее – КГ) использовала традиционные программы без акцента на направления информационной безопасности, указанные в этом списке.

Третий, заключительный контрольный этап, проведенный в апреле 2025 года, включал комплексную оценку достигнутых результатов с использованием разработанного авторами контрольно-измерительного инструментария. Статистический анализ полученных данных продемонстрировал существенный прогресс в формировании профессиональных компетенций у курсантов экспериментальной группы. Применение непараметрического критерия Пирсона χ^2 подтвердило достоверность выявленных различий между экспериментальной и контрольной группами.

Результаты

Для анализа результатов использовался критерий Пирсона χ^2 (хи-квадрат), который широко применяется в педагогических исследованиях для проверки гипотез о зависимости между категориальными переменными. В рамках исследования были сформулированы гипотезы: нулевая (*H0*) – между экспериментальной и контрольной группами нет значительных различий в успеваемости; альтернативная (*H1*) – такие различия существуют благодаря применению Контрольного списка необходимых навыков для расследователя преступлений в сфере компьютерной информации.

Результаты, достигнутые курсантами в ключевых направлениях, распределяются следующим образом: в ЭГ 16 человек достигли положительных результатов (69,57 %), а семь – не достигли положительного результата (30,43 %). В КГ положительные результаты показали шесть курсантов (27,27 %), в то время как 16 человек не достигли успеха (72,73 %).

Для расчета критерии хи-квадрат (χ^2) Пирсона необходимо выполнить следующее:

Шаг 1: Составляется таблица сопряженности (таблица 3), после чего применяется формула χ^2.

Таблица 3

Результаты педагогического эксперимента (первый контрольный срез)

Table 3

Results of the pedagogical experiment (first control section)

Группа	Положительный результат	Не достигли положительного результата	Общее количество человек в группе
Экспериментальная	16 чел. (69,57 %)	7 чел. (30,43 %)	23
Контрольная	6 чел. (27,27 %)	16 чел. (72,73 %)	22
Итого	22 чел.	23 чел.	45

ISSN 2949-1150 (online)
2071-8284 (print)

Шаг 2: Производится расчет ожидаемых частот. Расчет критерия Пирсона χ^2 осуществляется по формуле:

$$\chi^2 = \frac{\sum (O_i - E_i)^2}{E_i}, \quad (1)$$

где: O_i – наблюдаемые значения;
E_i – ожидаемые значения, которые определяются по формуле:

$$E_{ij} = \frac{(\text{Сумма строки}_i) \times (\text{Сумма столбца}_j)}{(\text{Общая сумма})}, \quad (2)$$

После подстановки значений получим ожидаемые частоты для каждой ячейки:
ЭГ (положительный результат):

$$E_{11} = \frac{23 \times 22}{45} \approx 11{,}24$$

ЭГ (отрицательный результат):

$$E_{12} = \frac{23 \times 23}{45} \approx 11{,}75$$

КГ (положительный результат):

$$E_{21} = \frac{22 \times 22}{45} \approx 1{,}75$$

КГ (отрицательный результат):

$$E_{21} = \frac{22 \times 23}{45} \approx 11{,}24$$

Шаг 3: Выполняется расчет χ^2. Теперь мы можем использовать формулу для расчета критерия Пирсона χ^2:

$$\chi^2 = \frac{\sum (O_{ij} - E_{ij})^2}{E_{ij}}, \quad (3)$$

где: O_{ij} – наблюдаемые частоты;
E_{ij} – ожидаемые частоты.
Подсчитаем χ^2 для каждой ячейки:
ЭГ (положительный результат): $\frac{(16 - 11{,}24)^2}{11{,}24} \approx 2{,}01$

ЭГ (отрицательный результат): $\frac{(7 - 11{,}75)^2}{11{,}75} \approx 1{,}92$

КГ (положительный результат): $\frac{(6 - 10{,}75)^2}{10{,}75} \approx 2{,}09$

КГ (отрицательный результат): $\frac{(16 - 11{,}24)^2}{11{,}24} \approx 2{,}01$

Теперь сложим все значения:

$$\chi^2 = 2{,}01 + 1{,}92 + 2{,}09 + 2{,}01 = 8{,}03$$

Шаг 4: Интерпретация результата. Чтобы интерпретировать полученное значение χ^2, необходимо сравнить его с критическим значением из таблицы распределения χ^2 для заданного уровня значимости (обычно 0,05) и числа степеней свободы (df = 1), которое составляет примерно 3,841.

Поскольку полученное расчетное значение критерия Пирсона χ^2 = 8,03 больше, чем критическое значение 3,841 из таблицы распределений, можно отвергнуть нулевую гипотезу и сделать вывод, что существует статистически значимая разница в результатах между экспериментальной и контрольной группами.

Обсуждение

Полученные результаты исследования подтверждают гипотезу о том, что разработанная методика подготовки специалистов в области расследования преступлений в сфере компьютерной информации, основанная на использовании Контрольного списка необходимых навыков, положительно влияет на уровень подготовки курсантов. В ЭГ 69,57 % курсантов достигли положительных результатов, в то время как в КГ этот показатель составил лишь 27,27 %. Это свидетельствует о том, что целенаправленная подготовка, акцентирующая внимание на актуальных знаниях и навыках, значительно улучшает готовность сотрудников правоохранительных органов к расследованию преступлений в сфере компьютерной информации.

В ходе подготовки был проведен контент-анализ компетенций программы, что позволило выявить ключевые навыки, необходимые для эффективного расследования компьютерных преступлений. Обновление учебного материала с акцентом на знания современных информационных технологий и оценку угроз кибербезопасности также способствовало улучшению усвоения материала курсантами. Однако следует отметить некоторые недостатки исследования. Во-первых, выборка курсантов состояла всего из двух учебных взводов, что может снижать обобщаемость результатов на более широкую аудиторию сотрудников правоохранительных органов. Во-вторых, исследование проводилось в рамках одного учебного заведения, что может повлиять на репрезентативность результатов и ограничивает возможность их прямого переноса, поскольку методики и технологии подготовки могут различаться в других образовательных организациях.

Несмотря на эти ограничения, результаты исследования доказывают важность систематической подготовки сотрудников правоохранительных органов в области компьютерных преступлений. Разработанный инструмент оценки квалификаций для выявления и оценки знаний сотрудников является важным шагом к повышению эффективности расследования киберпреступлений. В дальнейшем рекомендуется проводить дополнительные исследования, направленные на оценку долгосрочной эффективности предложенных методов подготовки и их влияние на профессиональную деятельность сотрудников правоохранительных органов, а также на возможность внедрения этих методов в учебные программы других учебных заведений.

Заключение

Данное исследование подтвердило значимость специализированной подготовки сотрудников правоохранительных органов в области расследования преступлений в сфере компьютерной информации. Результаты показали, что применение разработанной методики подготовки, включая Контрольный список необходимых навыков, существенно повышает уровень знаний и готовности курсантов к эффективному реагированию на преступления в сфере компьютерной информации.

Перспективным направлением дальнейших исследований является совершенствование методики обучения с внедрением актуальных образовательных подходов и анализом их результативности в реальной работе правоохранительных структур. Рекомендуется также исследовать влияние этих обновлений на профессиональную подготовку сотрудников правоохранительных органов, проводить межведомственные тренинги и симуляции, направленные на улучшение взаимодействия между различными структурами в борьбе с преступлениями в сфере компьютерной информации. Учитывая динамичное развитие технологий и угроз, необходимо регулярно обновлять содержание учебных программ и методы подготовки сотрудников правоохранительных органов в данной области.

Список источников

1. *Петровских В. Д.* Современные реалии расследования уголовных дел о преступлениях, связанных с терроризмом и экстремизмом, противодействие преступности в Интернет-пространстве / Проблемы борьбы с терроризмом и экстремизмом с учетом современных реалий : сборник научных статей межведомственной конференции, г. Саратов, 21 сентября 2022 г. Саратов : Саратовский военный ордена Жукова Краснознаменный институт войск национальной гвардии Российской Федерации, 2022. С. 64–72.

2. *Патраш И. А.* К вопросу о становлении и развитии российского Уголовного законодательства в сфере компьютерной информации // NovaUm.Ru. 2022. № 36. С. 16–19.

3. *Аманкулиева В. О.* Раскрытие и расследование преступлений в сфере компьютерной информации // Научное образование. 2024. № 1 (22). С. 154–157.

4. *Жижина М. В., Завьялова Д. В.* Расследование преступлений в сфере компьютерной информации в Российской Федерации и зарубежных странах : монография. Москва : Проспект, 2023. 136 с.

ISSN 2949-1150 (online)
2071-8284 (print)

5. *Лукьянова Т. В.* Особенности расследования компьютерных преступлений // Научный аспект. 2024. Т. 38, № 5. С. 5204–5210.

6. *Москалева Е. А., Раду А. И.* Расследование преступлений в сфере компьютерной информации: российский и зарубежный опыт / Актуальные вопросы расследования преступлений в сфере компьютерной информации или с применением компьютерных технологий в условиях цифровизации экономики и государственного управления : материалы Межвузовского круглого стола, Москва, 23 ноября 2023 г. Москва : Русайнс, 2024. С. 160–166.

7. *Киселев А. С., Горбунова К. А.* Особенности розыскных мероприятий при расследовании преступлений, совершаемых в сфере компьютерной информации // Правопорядок: история, теория, практика. 2023. № 4 (39). С. 147–154. https://doi.org/10.47475/2311-696X-2023-39-4-147-154

8. *Милащенко А. М.* Особенности производства экспертиз при расследовании мошенничества в сфере компьютерной информации / Миссия права 2024 : сборник материалов Всероссийской научно-практической конференции, г. Великий Новгород, 17 апреля 2024 г. Великий Новгород : Новгородский государственный университет имени Ярослава Мудрого, 2024. С. 92–98.

9. *Сергеев А. Б.* Цифровое доказательственное право при производстве по уголовным делам о преступлениях в сфере компьютерной информации: вопросы целесообразности // Юридическая наука и правоохранительная практика. 2022. № 3 (61). С. 66–72.

10. *Янгаева М. О.* О методике проведения практического занятия по дисциплине «Расследование преступлений в сфере компьютерной информации» // Вестник Барнаульского юридического института МВД России. 2024. № 2 (47). С. 35–38.

11. *Петрова И. А., Лобачев И. А.* Преступления в сфере компьютерной информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств // Журнал прикладных исследований. 2020. № 1. С. 52–62.

12. *Нечай А. А.* Использование инновационных методов и современных технологий для повышения квалификации в области кибербезопасности // Азимут научных исследований: педагогика и психология. 2020. Т. 9, № 3 (32). С. 193–196. https://doi.org/10.26140/anip-2020-0903-0043

13. *Сабирзянова Э. Р.* К вопросу о понятии и классификации киберпреступлений как угрозы экономической безопасности Российской Федерации / Цифровые технологии и право : сборник научных трудов II Международной научно-практической конференции : в 6 т., г. Казань, 22 сентября 2023 г. / ред.:: И. Р. Бегишев [и др.]. Казань : Познание, 2023. Т. 3. С. 319–322.

14. *Гринев В. А., Захаров С. В.* Уголовно-процессуальные и криминалистические аспекты борьбы с преступностью в России в условиях «цифровизации» современного общества / Актуальные проблемы борьбы с преступностью : материалы межвузовской научно-практической конференции, Тула, 25 марта 2021 г. Тула : Тульский институт (филиал) ВГУЮ (РПА Минюста России), 2022. С. 103–114.

15. *Зеленкина О. Ю.* Особенности расследования преступлений в сфере компьютерной информации // Сибирские уголовно-процессуальные и криминалистические чтения. 2019. № 2 (24). С. 92–100.

16. *Ерастов Е. Д.* Современные проблемы кибербезопасности: вызовы и решения // Вестник науки. 2024. Т. 4, № 10 (79). С. 745–749.

17. *Лантух Э. В., Ишигеев В. С., Грибунов О. П.* Использование специальных знаний при расследовании преступлений в сфере компьютерной информации // Всероссийский криминологический журнал. 2020. Т. 14, № 6. С. 882–890. https://doi.org/10.17150/2500-4255.2020.14(6).882-890

18. *Чукова Д. И., Медведев Д. А., Литвиненко М. В.* Модель формирования компетенций специалиста в сфере расследования компьютерных преступлений // Вопросы кибербезопасности. 2019. № 3 (31). С. 57–62.

19. *Нечай А. А., Ничагина А. В.* Анализ использования информационных систем для мониторинга образовательной деятельности в вузе // Азимут научных исследований: педагогика и психология. 2023. Т. 12, № 4 (45). С. 112–116. https://doi.org/10.57145/27128474_2023_12_04_23

20. *Квон Г. М., Вакс В. Б., Поздеева О. Г.* Использование шкалы Лайкерта при исследовании мотивационных факторов, обучающихся // Концепт : [электронный журнал]. 2018. № 11. С. 84–96. https://doi.org/10.24411/2304-120X-2018-11086

Авторами внесен равный вклад в написание статьи.
Авторы заявляют об отсутствии конфликта интересов.

The authors have made an equal contribution to the writing of the article.
The authors declare no conflicts of interests.