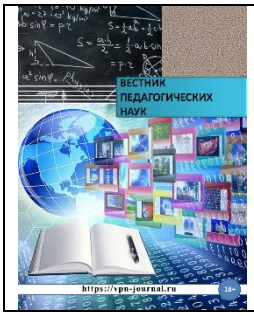

Научно-исследовательский журнал «**Вестник педагогических наук / Bulletin of Pedagogical Sciences»**
https://vpn-journal.ru
2025, № 7 / 2025, Iss. 7 https://vpn-journal.ru/archives/category/publications
Научная статья / Original article
Шифр научной специальности: 5.8.7. Методология и технология профессионального образования (педагогические науки)
УДК 37.015

[1] Болтенкова Ю.В., [2] Новохатский Д.А., [1] Навроцкая И.Н., [3] Заварзин А.В.
[1] Белгородский юридический институт Министерства внутренних дел Российской Федерации имени И.Д. Путилина
[2] Волгоградская академия Министерства внутренних дел Российской Федерации
[3] Московское высшее общевойсковое командное училище

Вопросы подготовки курсантов силовых ведомств к профессиональной деятельности в современных условиях

Аннотация: подготовка специалистов силовых ведомств, обеспечивающих защиту, безопасность и законность, что способствует развитию государства всегда была актуальной, но в современных условиях требования к подготовленности сотрудников силовых ведомств становятся все более требовательными, что подчеркивает актуальность исследования.
Проблематика исследования заключается в необходимости адаптировать процесс подготовки с учетом современных реалий и необходимости акцентировать внимание на освоение современных технологий как средства обеспечивающих эффективность служебной деятельности.
В ходе исследования решались следующие задачи: 1) анализ видов преступности и их динамика; 2) анализ подготовленности специалистов силовых ведомств с учетом современных технологий.
Полученные в ходе исследования результаты могут быть использованы при организации учебного процесса по различным видам подготовки в учебных заведениях силовых ведомств.
Ключевые слова: профессиональная подготовка, курсанты вузов силовых ведомств, цифровая криминалистика, расследование киберпреступлений, кибербезопасность

Для цитирования: Болтенкова Ю.В., Новохатский Д.А., Навроцкая И.Н., Заварзин А.В. Вопросы подготовки курсантов силовых ведомств к профессиональной деятельности в современных условиях // Вестник педагогических наук. 2025. № 7. С. 6 – 12.

Поступила в редакцию: 28 марта 2025 г.; Одобрена после рецензирования: 7 мая 2025 г.; Принята к публикации: 19 июня 2025 г.

[1] Boltenkova Yu.V., [2] Novokhatsky D.A., [1] Navrotskaya I.N., [3] Zavarzin A.V.
[1] Belgorod Law Institute of the Ministry of Internal Affairs of the Russian Federation named after I.D. Putilin
[2] Volgograd Academy of the Ministry of Internal Affairs of the Russian Federation
[3] Moscow Higher Combined Arms Command School

Issues of training cadets of law enforcement agencies for professional activity in modern conditions

Abstract: the training of specialists from law enforcement agencies to ensure security and legality, which contributed to the development of the state, has always been relevant, but in modern conditions, the requirements for the training of law enforcement officers are becoming more demanding, which underlines the relevance of the study.
The research problem lies in the need to adapt the training process to modern realities and the need to focus on the development of modern technologies as a means of ensuring the effectiveness of professional activities.
The following tasks were solved in the course of the study: 1) analysis of types of crime and their dynamics; 2) analysis of the training of specialists of law enforcement agencies taking into account modern technologies.

The results obtained in the course of the study can be used in organizing the educational process for various types of training in educational institutions of law enforcement agencies.
Keywords: professional training, university cadets of law enforcement agencies, digital forensics, investigation of cybercrimes, cybersecurity

For citation: Boltenkova Yu.V., Novokhatsky D.A., Navrotskaya I.N., Zavarzin A.V. Issues of training cadets of law enforcement agencies for professional activity in modern conditions. Bulletin of Pedagogical Sciences. 2025. 7. P. 6 – 12.

The article was submitted: March 28, 2025; Accepted after reviewing: May 7, 2025; Accepted for publication: June 19, 2025.

Введение

В эпоху стремительного технического прогресса, эволюции криминальной тактики и изменения правового ландшафта подготовка будущих сотрудников силовых ведомств требует динамичного и адаптивного подхода. Традиционные методы подготовки, хотя и являются основополагающими, теперь должны учитывать современные вызовы, такие как киберпреступность, использование искусственного интеллекта преступными элементами и другие технологические достижения [4, 6].

Эффективность подготовки зависит от возможности обеспечить курсантов не только теоретическими знаниями, но и сформированными практическими навыками и технологической подготовленностью. Поскольку современные вызовы становится все более изощренными, включая цифровое мошенничество, транснациональную организованную преступность и юридические дилеммы, связанные с искусственным интеллектом, учебные заведения должны адаптировать учебный материал с учетом современных технологий, специалисты знали технологии с помощью, которых совершаются преступления и технологии, посредством которых данные преступления раскрываются.

В представленном материале рассматриваются важнейшие вопросы, связанные с подготовкой курсантов силовых ведомств к современным технологическим реалиям.

Решая встающие на современном этапе развития технологий задачи, учебные заведения могут обеспечить качество подготовки, что оказывает влияние насколько эффективно, будут выполнять возложенные на специалистов служебные обязанности.

Материалы и методы исследований

Для решения задач исследования были использованы теоретические и аналитические методы (анализ литературных источников и обобщения), эмпирические методы (опросы и анкетирование, наблюдения).

Результаты и обсуждения

На современном этапе получили свое развитие технологии, определяющие вид и уровень преступности, где стоит выделить бурный всплеск киберпреступности. Например, преступники используют атаки с использованием программ-вымогателей, в результате чего преступники шифруют данные и требуют оплату (часто в криптовалюте) для восстановления доступа. Так же получили свое развитие и фишинг и социальная инженерия, где у жертвы обманом добиваются раскрытия конфиденциальной информации, которую используют для достижения своих целей и для похищения финансов. Не меньшую угрозу представляют и вредоносные программы, взлом паролей, кража банковских реквизитов, материалов, мошенничество с криптовалютой, где создаются финансовые пирамиды, поддельные ICO (первичное предложение монет) и криптоджекинг (захват устройств для майнинга криптовалюты) [1, 5, 6].

Набирают «обороты» и мошенничество с глубокими подделками, созданные искусственным интеллектом, поддельные видео/аудиозаписи используются для мошенничества, шантажа и дезинформации, что может привести к непредсказуемым последствиям. И такие попытки уже предпринимались с целью дискредитации администрации областей и государства, а также распространяли дезинформацию чтобы посеять панику среди жителей Белгородской и Курской областей.

Растет число преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. На данные преступления приходится 25,8 % от всех зарегистрированных преступлений, где 72,8 % таких преступлений совершается с использованием сети «Интернет» (+1,9 %, 342,5 тыс.) [3].

Современные технологии способствовали росту финансовых преступлений и мошенничеству [7, 9, 10]. Организованная преступность уходит в интернет, где функционируют теневые веб-рынки, где продаются запрещенные к реализации товары (наркотики, оружие, украденные данные), продаваемые через зашифрованные платформы.

Происходят изменения в сфере насильственных преступлений и преступлений против собственности. Отмечается снижение числа традиционных краж, благодаря цифровым платежам количество физических ограблений сокращается. Тогда как фиксируется рост угонов транспортных средств без ключа и автомобилей класса люкс. В процессе анализа статистических данных отмечается рост числа бытового экстремизма и преступлений на почве ненависти, где политическое и социальное расслоение способствует актам насилия [2, 6, 8].

Получило свое развитие и мошенничество с использованием искусственного интеллекта, где чат-боты, имитирующие обслуживание клиентов, крадут учетные данные. Преступниками или преступными сообществами разрабатываются автоматизированные инструменты взлома, где искусственный интеллект ускоряет взлом паролей и обнаружение уязвимостей.

Киберпреступность, включая атаки программ–вымогателей, кражу личных данных, мошенничество с использованием криптовалют и кибертерроризм, становится все более изощренной, опережая традиционные методы работы полиции.

В процессе опроса о знаниях курсантов о способах похищения данных или финансов был задан вопрос, как происходит воровство данных, ответы курсантов представлены на рис. 1.

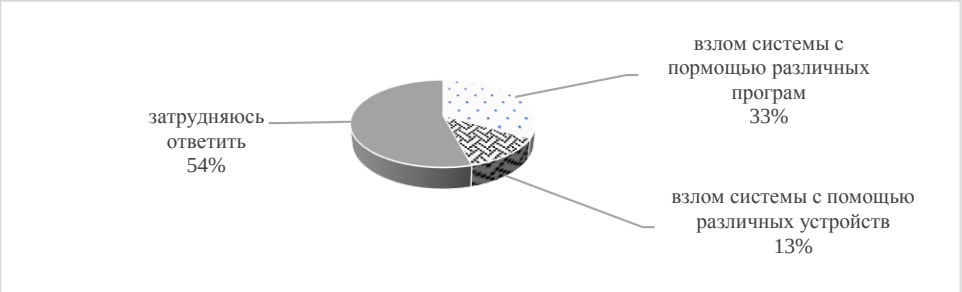

Рис. 1. Мнения курсантов о способах хищения данных.
Fig. 1. Opinions of cadets about methods of data theft.

Хотя курсантам объясняли, как получают доступ к данным и что для этого используют. Так же решили узнать, как часто они устанавливают различные программы на свои устройства (смартфоны, планшеты и компьютеры), на данный вопрос практически все указали, что по мере необходимости устанавливают. Владельцы iPhone устанавливают из медиатеки iTunes, тогда как владельцы Android используют Google Play или различные репозитории, например, Трешбокс.ру. На официальных источниках программ вопросы вирусов отсутствуют, так как каждый разработчик программ заботиться о своей репутации, то сторонние ресурсы предлагают различные программы с внедренными вирусами. Тогда как пользователи устройства уверенны, что скачанные со сторонних ресурсов программы не содержат вирусов, которые могут собрать конфиденциальные данные и отправить их злоумышленнику. На вопрос какие ресурсы вы используете для скачивания и установки программ ответы представлены на рис. 2.

В процессе опросов курсантов выяснилось, что установка программ со сторонних ресурсов может быть опасна, на что указало 78% опрошенных, так как может содержать различные вирусы и опрашиваемые это знают, но указывают, что у них установлен антивирус, который блокирует действия вирусов. Респонденты уверенны, что установленный антивирус является гарантией, что различные зловредные программы не попадут на устройство. Выявленная ситуация указывает на несформированные знания в области безопасности пользования программными продуктами и киберпреступлений, получивших свое развитие.

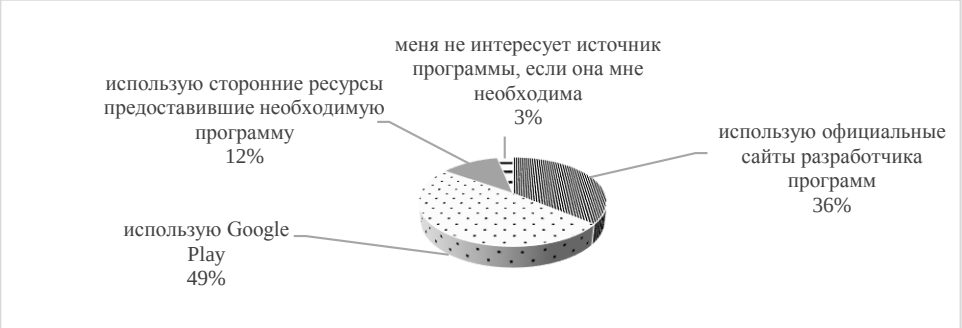

Рис. 2. Распределение ответов на вопрос какие ресурсы вы используете для скачивания и установки программ.
Fig. 2. Distribution of answers to the question what resources do you use to download and install programs.

Традиционные программы подготовки сотрудников полиции часто ориентированы на изучение места преступления, сбор вещественных доказательств и обычные следственные процедуры [2, 6, 8]. Однако современным правоохранительным органам требуется подход, который объединяет кибербезопасность, цифровую криминалистику, анализ данных и понимание новых технологий, таких как искусственный интеллект и блокчейн. Курсанты должны быть готовы не только к расследованию цифровых преступлений, но и к предвидению будущих угроз, сотрудничеству с международными агентствами и ориентированию в сложных правовых системах, регулирующих киберпространство.

Чтобы эффективно противодействовать цифровым преступлениям, будущие сотрудники силовых структур должны обладать сочетанием технических знаний, следственной работы и юридических знаний. Это требует комплексного подхода к обучению, выходящего за рамки обычной подготовки сотрудников силовых структур и включающего основы кибербезопасности, цифровую криминалистику, анализ угроз и моделирование реальных киберпреступлений. Кроме того, будущие специалисты должны понимать эволюционирующую преступную тактику, включая социальную инженерию, отмывание криптовалют и кибератаки, управляемые искусственным интеллектом [4, 6, 10].

Важнейшими компонентами для эффективной подготовки является необходимость сформировать знания основ кибербезопасности для чего требуется понимание методов похищения данных с электронных устройств, сетевых уязвимостей и стратегий защиты.

Для выявления знаний о киберпреступности был проведен опрос, где все 100% знают о возрастающей угрозе преступлений с помощью современных технологий. Многим из них звонили мошенники и пытались узнать конфиденциальные данные необходимые для получения доступа к госуслугам или приходили ссылки с просьбой поддержать кого либо, если по ней пройти, то преступник получал бы доступ к смартфону и в дальнейшем последствия для конфиденциальных данных и финансов владельца смартфона могли быть не предсказуемы.

Для выявления знаний и умений пользования компьютером и программными продуктами был проведен опрос курсантов 4 курсов, где все 100% респондентов указали, что являются уверенными пользователями компьютером. В процессе подготовки курсанты осваивали ряд программ необходимых в профессиональной деятельности, например, компьютеризированная обработка дактилоскопической информации, компьютерные системы, предназначенные для различных видов работы с изображениями людей (создание композиционных портретов, поиск по массивам фотоизображений, поиск по изображениям без вести пропавших людей и атрибуция трупов и т.д.). Но также, в процессе опроса выяснилось, что курсанты не могут отследить трафик входящий и исходящий, не знают и не умеют пользоваться необходимыми для этого программами. В процессе бесед курсанты указали, что для данной деятельности нужны специфичные знания, которые получают по другим направлениям подготовки, например, информационная безопасность и т.д. Принявшие в опросе курсанты указали, что у них другое направление подготовки и если потребуется, то будут взаимодействовать в требуемыми для раскрытия преступления специалистами.

Так же курсанты пользуются искусственным интеллектом для анализа данных или подготовки различных отчетов и т.д. Но это они осваивают самостоятельно и носит эпизодический характер, хотя искусственный интеллект все более и более входит в нашу жизнь и находит свое применение в различных сферах деятельности и примеров тому масса. Не отстают и различного рода мошенники, которые используют данный инструмент в своих, противозаконных целях.

В ходе опроса куранты указали, что если потребуется, то они выполнят задания в программе «Папилон» и других специализированных программных продуктах, но для исследований преступлений в сферах кибербезопасности необходимы не только знания, но и технические средства, позволяющие получить необходимые данные с компьютера или электронного гаджета, что не входит в систему их подготовки, у них другой профиль подготовки.

Так же для оценки знаний устройства компьютера курсантам предложили заменить оперативную память, которую разложили по выпуску DDR2, DDR3, DDR4. Только 4 курсанта из 38 принявших участие смогли выполнить задание, остальные не справились с ним, так как не знают, как их отличить друг от друга. Так же предложили заменить HDD, где с заданием справились 6 человек из тех же 38 курсантов. Данное состояние указывает на низкий уровень знаний в устройстве компьютера. Со слов, принявших участие в опросе, они пользователи, а не специалисты по ремонту компьютерной техники. Хотя особых знаний в замене HHD или оперативной памяти не требуется. А в ряде случаев данные знания необходимы для пресечения изъятия жесткого диска из компьютера, что бы злоумышленник не уничтожил улики, остающиеся на данном диске и других носителях информации.

По мере развития технологий учебные заведения правоохранительных органов должны включать в свои учебные планы обнаружение угроз на основе искусственного интеллекта, риски, связанные с квантовыми вычислениями, и безопасность Интернета вещей.

Так же необходимо участие в семинарах по новым угрозам, например: борьба с киберпреступлениями, связанными с искусственным интеллектом, глубокими подделками и рисками, связанными с квантовыми вычислениями.

Успешное расследование цифровых преступлений требует междисциплинарного подхода, сочетающего криминалистические технологии, правовую базу и упреждающий сбор необходимой информации.

Приведем список наиболее острых проблем, с которыми сталкиваются сегодня учебные заведения в подготовке специалистов:

– отставание учебных программ от современных тенденций, в учебных планах по-прежнему преобладают модели преступности 1990-х годов;
– ограниченное количество часов для изучения киберпреступлений, цифровых улик, алгоритмической предвзятости;
– нехватка специализированных специалистов в области искусственного интеллекта, крипто активов, криминалистики беспилотников;

Приведенные проблемы требуют своего разрешения, так как современные технологии очень быстро совершенствуются, что требует адекватного ответа со стороны учебных заведений, для качественной подготовки специалистов.

Выводы

Разрабатывая стандарты физической подготовки в соответствии с требованиями реального мира, учебные заведения могут обеспечить все виды подготовки сотрудников силовых ведомств для эффективной защиты населения от различных видов преступлений.

Но без учета современных тенденций в преступности, невозможно обеспечить качественную подготовку специалистов силовых ведомств. И это прежде всего должно касаться самих специалистов, которые должны знать способы получения различных данных преступниками и перекрывать данные каналы.

Процесс подготовки курсантов силовых структур нуждается в модернизации в соответствии с развитием технологий. Одни только занятия, разработанные без учета современных тенденций в технологиях и науке, не могут обеспечить качество подготовки будущих специалистов к работе в условиях, когда доминируют зашифрованные сообщения, беспилотники и видеоконтент, вызывающий общественный резонанс.

Разрабатывая рабочие программы учебных дисциплин, уделяя особое внимание формированию знаний в сфере предотвращения, выявления и судебного преследования киберпреступлений, учебные заведения могут подготовить будущих специалистов к защите общества в условиях цифрового мира.

Выстраивание подготовки с учетом развития технологий, будет способствовать сформированности навыков, знаний и ценностей, необходимых для эффективной служебной деятельности.

Список источников

1. Бессонов А.А. Использование алгоритмов искусственного интеллекта в криминалистическом изучении преступной деятельности (на примере серийных преступлений) // Вестник Университета им. О.Е. Кутафина. 2021. № 2. С. 45 – 53.
2. Дуюнов Е.А., Иванов Е.В., Белоглазов М.В., Борисова К.О. Вопросы подготовки специалистов силовых ведомств к служебной деятельности // Успехи гуманитарных наук. 2024. № 6. С. 110 – 115. DOI: 10.58224/2618-7175-2024-6-110-115.
3. Генеральная прокуратура Российской Федерации. Портал правовой статистики. http://crimestat.ru/analytics (дата обращения: 08.05.2025).
4. Жуков А.З. Совершенствование инструментов противодействия киберртерроризму в современных условиях // Пробелы в российском законодательстве. 2021. Т. 14. № 5. С. 123 – 128.
5. Бахтеев Д.В., Буглаева Е.А., Зазулин А.И. [и др.].Использование искусственного интеллекта при выявлении, раскрытии, расследовании преступлений и рассмотрении уголовных дел в суде. Москва: Издательство "Юрлитинформ", 2022. 216 с.
6. Лукина А.А. Методы криминалистики будущего // Правосудие современности: материалы III Всероссийской научно-практической конференции студентов и молодых ученых. Екатеринбург, 29 марта 2024 года. Екатеринбург: Уральский государственный юридический университет им. В.Ф. Яковлева, 2025. С. 424 – 429.
7. Пекарева В.В., Фроловская Ю.И. Цифровая модель криминалистических средств при расследовании преступных посягательств на безопасность информационного и физического пространства // Аграрное и земельное право. 2024. № 5 (233). С. 237 – 239. DOI: 10.47643/1815-1329_2024_5_237.
8. Совершенствование профессиональной и физической подготовки курсантов, слушателей образовательных организаций и сотрудников силовых ведомств: сборник материалов XIX международной научно-практической конференции. В 2-х томах. Иркутск, 15–16 июня 2017 года. Том II. Иркутск: Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2017. 328 с.
9. Тюнис И.О., Анисимова А.М. Искусственный интеллект и цифровые технологии в криминалистике // Закон и право. 2025. № 3. С. 246 – 251. DOI: 10.24412/2073-3313-2025-3-246-251.
10. Чупахин В.Е., Долгов Н.В., Иванов Д.А. Сеть интернет и киберпреступность // Российская наука в современном мире: сборник статей LIII международной научно-практической конференции. Москва, 15 апреля 2023 года. Москва: Общество с ограниченной ответственностью "Актуальность.РФ", 2023. С. 245 – 247.

References

1. Bessonov A.A. Use of artificial intelligence algorithms in the forensic study of criminal activity (on the example of serial crimes). Bulletin of the O.E. Kutafin University. 2021. No. 2. P. 45 – 53.
2. Duyunov E.A., Ivanov E.V., Beloglazov M.V., Borisova K.O. Issues of training specialists of law enforcement agencies for official activities. Successes in the Humanities. 2024. No. 6. P. 110 – 115. DOI: 10.58224/2618-7175-2024-6-110-115.
3. Prosecutor General's Office of the Russian Federation. Legal Statistics Portal. http://crimestat.ru/analytics (accessed: 08.05.2025).
4. Zhukov A.Z. Improving tools for countering cyberterrorism in modern conditions. Gaps in Russian legislation. 2021. Vol. 14. No. 5. P. 123 – 128.
5. Bakhteyev D.V., Buglaeva E.A., Zazulin A.I. [et al.]. Using artificial intelligence in identifying, solving, investigating crimes and considering criminal cases in court. Moscow: Yurlitinform Publishing House, 2022. 216 p.
6. Lukina A.A. Forensic science methods of the future. Justice of our time: materials of the III All-Russian scientific and practical conference of students and young scientists. Ekaterinburg, March 29, 2024. Ekaterinburg: Ural State Law University named after V.F. Yakovleva, 2025. P. 424 – 429.
7. Pekareva V.V., Frolovskaya Yu.I. Digital model of forensic tools in the investigation of criminal attacks on the security of information and physical space. Agrarian and land law. 2024. No. 5 (233). P. 237 – 239. DOI: 10.47643/1815-1329_2024_5_237.
8. Improving the professional and physical training of cadets, students of educational organizations and employees of law enforcement agencies: collection of materials from the XIX international scientific and practical conference. In 2 volumes. Irkutsk, June 15–16, 2017. Volume II. Irkutsk: East Siberian Institute of the Ministry of Internal Affairs of the Russian Federation, 2017. 328 p.

9. Tyunis I.O., Anisimov A.M. Artificial Intelligence and Digital Technologies in Forensic Science. Law and Right. 2025. No. 3. P. 246 – 251. DOI: 10.24412/2073-3313-2025-3-246-251.

10. Chupakhin V.E., Dolgov N.V., Ivanov D.A. The Internet and Cybercrime. Russian Science in the Modern World: Collection of Articles from the LIII International Scientific and Practical Conference. Moscow, April 15, 2023. Moscow: Limited Liability Company "Aktualnost.RF", 2023. P. 245 – 247.

Информация об авторах

Болтенкова Ю.В., кандидат социологических наук, доцент, Федеральное государственное казенное образовательное учреждение высшего образования «Белгородский юридический институт Министерства внутренних дел Российской Федерации имени И.Д. Путилина»

Новохатский Д.А., кандидат юридических наук, Федеральное государственное казенное образовательное учреждение высшего образования «Волгоградская академия Министерства внутренних дел Российской Федерации», datoys92@mail.ru

Навроцкая И.Н., Федеральное государственное казенное образовательное учреждение высшего образования «Белгородский юридический институт Министерства внутренних дел Российской Федерации имени И.Д. Путилина»

Заварзин А.В., Федеральное государственное казенное военное образовательное учреждение высшего образования «Московское высшее общевойсковое командное орденов Ленина и Октябрьской Революции Краснознаменное училище» Министерства обороны Российской Федерации