www.volsu.ru

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПНОСТИ И ДИФФЕРЕНЦИАЦИЯ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ

DOI: https://doi.org/10.15688/lc.jvolsu.2020.2.22

UDC 378
LBC 74.48

Submitted: 14.03.2020
Accepted: 05.04.2020

IMPROVING THE TRAINING OF LAW ENFORCEMENT OFFICERS IN COUNTERING CRIMES COMMITTED USING INFORMATION TECHNOLOGY

Ivan N. Arkhiptsev
Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin,
Belgorod, Russian Federation

Alexander V. Sarychev
Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I D. Putilin,
Belgorod, Russian Federation

Roman V. Krasnikov
Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin,
Belgorod, Russian Federation

Introduction: according to the official statistics, the number of acts involving information technology is increasing every year in Russia. In particular, currently, the types of crimes in the field of information technology are changing qualitatively and continue to evolve continuously, becoming highly organized and more sophisticated. Through the use of information technologies in Russia, such crimes as hacking, illegal data acquisition (information espionage), theft of other people's property from payment (settlement) cards and accounts of citizens, trafficking of drugs, arms, human beings are committed; the extremist literature is distributed, new members of terrorist groups are recruited; pornography, including children, is spread, illegal gambling and online games are conducted; fraud through the use of cellular and IP-telephony services, theft of personal data in large amount and selling them, and other crimes are committed using information technologies. The current type of computer fraud – phishing – is gaining momentum. Its essence is that cybercriminals seek to get hold of the data of ordinary people through computer technology, and using this data, get hold of their funds, including financial ones. It seems that such actions can neither contribute to the development of Russian society, nor to the development of civilized relations in society, nor to the development of information networks themselves. After all, any technology can be used for both constructive and non-constructive technologies. And when these goals are destructive, the law enforcement agencies, in our opinion, should have an effective level of training to deal with such violations. We believe that it is not enough to calculate, detect, and establish. We still need to be able to bring the culprit to criminal responsibility. In this regard, the most important thing is to ensure that anonymity not only creates the illusion of impunity, but also that the law enforcement agencies have a sufficient legal, organizational and, first of all, personnel basis to expose the criminal. In order to successfully thwart crimes in the field of information technology, the availability of

a high-quality and modern legal framework is a necessary, but not sufficient condition. The basis for the successful implementation of the adopted standards and the key to the implementation of the state policy in the field of information security is the training and education of appropriate personnel who would provide "breakthrough" results in this area. The **purpose** of the research is to study the issues of improving the training of the law enforcement officers in countering crimes committed through the use of information technologies. **Methods:** the research uses a comparative analysis and generalization of the examples of the educational methods used in the educational organizations of the Ministry of Internal Affairs in the field of information security. The authors study, in particular, the general theoretical and practical orientation of the educational process in this area, synthesizing the results obtained, whose purpose is to improve the training of highly qualified specialists for the Internal Affairs bodies capable of countering crimes in the field of information technologies. **Results:** the authors formulate the main directions for improving the training of the law enforcement officers to counter crimes committed using information technologies, in particular, on the example of the educational organizations used in the educational process of the Ministry of Internal Affairs of Russia. Thus, one of the measures proposed by the authors in this direction is the opening of a new specialty – cyber-investigator or cyber-criminalist. The entry of developed countries into the sixth technological order and the further active digitalization of the world economy predict a huge scale and replication of crimes using information technologies. This circumstance actualizes the need to popularize the profession of a cyber-investigator – a specialist with an interdisciplinary education, i.e. experience in the investigative agencies will have to be combined with the skills of a criminalist and a specialist in the field of information protection.

Key words: information technologies, cybercrime, personnel support, training of law enforcement officers, digital tehnology.

Citation. Arkhiptsev I.N., Sarychev A.V., Krasnikov R.V. Improving the Training of Law Enforcement Officers in Countering Crimes Committed Using Information Technology. *Legal Concept*, 2020, vol. 19, no. 2, pp. 154-163. (in Russian). DOI: https://doi.org/10.15688/lc.jvolsu.2020.2.22

УДК 378
ББК 74.48

Дата поступления статьи: 14.03.2020
Дата принятия статьи: 05.04.2020

СОВЕРШЕНСТВОВАНИЕ ПОДГОТОВКИ СОТРУДНИКОВ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Иван Николаевич Архипцев

Белгородский юридический институт МВД России им. И.Д. Путилина, г. Белгород, Российская Федерация

Александр Викторович Сарычев

Белгородский юридический институт МВД России им. И.Д. Путилина, г. Белгород, Российская Федерация

Роман Владимирович Красников

Белгородский юридический институт МВД России им. И.Д. Путилина, г. Белгород, Российская Федерация

Введение. Как свидетельствуют официальные статистические данные, с каждым годом в России увеличивается количество деяний с использованием информационных технологий. В частности, в настоящее время виды преступлений в сфере информационных технологий качественно меняются и продолжают непрерывно эволюционировать, становясь высокоорганизованными и более изощренными. Посредством использования информационных технологий в России совершаются: хакерство; незаконное получение данных (информационный шпионаж); хищения чужого имущества с платежных (расчетных) карт и счетов граждан; ведется торговля наркотиками, оружием, людьми; распространяется экстремистская литература, вербуются новые члены террористических группировок; распространяется порнография, в том числе детская; проводятся незаконные азартные игры и онлайновые игры; мошенничества с использованием сотовой связи, а также средств IP-телефонии; кражи персональных данных в больших объемах и их продажа и другие преступ-

ления, совершаемые с использованием информационных технологий. Набирает обороты актуальный на сегодняшний день вид компьютерного мошенничества – фишинг. Суть его заключается в том, что киберпреступники стремятся посредством компьютерных технологий завладеть данными обычных людей, и, используя эти данные, завладеть их средствами, в том числе и финансовыми [8, с. 99]. Как представляется, подобного рода действия не могут способствовать ни развитию российского общества, ни развитию цивилизованных отношений в обществе, ни развитию самих информационных сетей. Ведь любая технология может быть использована как для конструктивных, так и для неконструктивных технологий. И когда эти цели деструктивны, правоохранительные органы, на наш взгляд, должны иметь эффективный уровень подготовки для борьбы с такими нарушениями. Полагаем, мало вычислить, обнаружить, установить, надо еще иметь возможность привлечь виновного к уголовной ответственности. В этой связи самое главное сделать так, чтобы анонимность не только создавала иллюзию безнаказанности, но и правоохранительные органы получили достаточно емкую правовую, организационную и в первую очередь кадровую основу для того, чтобы изобличить преступника. В целях успешного противодействия преступлениям в сфере информационных технологий наличие качественной и современной правовой базы является необходимым, но не достаточным условием. Основой успешного выполнения принимаемых норм и залогом реализации государственной политики в области информационной безопасности является обучение и воспитание соответствующих кадров, которые бы обеспечили «прорывные» результаты в данной области. **Цель исследования** – изучить вопросы совершенствования подготовки сотрудников правоохранительных органов по противодействию преступлениям, совершаемым с использованием информационных технологий. **Методы исследования:** в процессе исследования используется сравнительный анализ и обобщение примеров образовательных методик, используемых в образовательных организациях системы МВД, в сфере информационной безопасности. Авторы изучают, в частности, общетеоретическую и практическую направленность образовательного процесса в данной сфере, синтезируя полученные результаты, целью которых является совершенствование подготовки высококвалифицированных специалистов для органов внутренних дел, способных противостоять преступлениям в сфере информационных технологий. **Результаты исследования:** авторами сформулированы главные направления совершенствования подготовки сотрудников правоохранительных органов по противодействию преступлениям, совершаемым с использованием информационных технологий, в частности, на примере используемых в учебном процессе образовательных организаций МВД России. Так, одной из предложенных авторами мер в данном направлении является открытие новой специальности – киберследователь или киберкриминалист. Вступление развитых стран в шестой технологический уклад, дальнейшая активная цифровизация мировой экономики прогнозируют колоссальное масштабирование и тиражирование преступлений с использованием информационных технологий. Данное обстоятельство актуализирует необходимость популяризации профессии киберследователя – специалиста с междисциплинарным образованием, то есть опыт работы в следственных органах должен будет сочетаться с навыками криминалиста и специалиста в области защиты информации.

Ключевые слова: информационные технологии, киберпреступления, кадровое обеспечение, подготовка сотрудников правоохранительных органов, цифровые технологии.

Цитирование. Архипцев И. Н., Сарычев А. В., Красников Р. В. Совершенствование подготовки сотрудников правоохранительных органов по противодействию преступлениям, совершаемых с использованием информационных технологий // Legal Concept = Правовая парадигма. – 2020. – Т. 19, № 2. – С. 154–163. – DOI: https://doi.org/10.15688/lc.jvolsu.2020.2.22

Обучение технологиям информационной безопасности как основа успешной борьбы с киберпреступностью

В России с целью своевременного реагирования на новые кибератаки правоохранительные органы ориентированы на ведение мониторинга ситуации, складывающейся в сети Интернет, повышение квалификации сотрудников, методическое обеспечение их деятельности [1, с. 137]. Современная картина проблем в области противодействия киберпреступлениям свидетельствует об острой необходимости «выращивания» в правоохранительных органах грамотных специалистов в сфере высоких технологий. В настоящий период приоритетным направлением реформирования МВД России является именно подготовка и обучение специалистов в области противодействия киберкриминалу. Следует отметить, что в наиболее прогрессивных образовательных организациях МВД России с инновационным техническим осна-

щением и высококомпетентным преподавательским составом уже открыты специальности киберследователей.

Ярким примером служит Московский университет МВД России, где успешно функционирует факультет подготовки специалистов в сфере информационной безопасности. Систематически организуются научно-практические конференции, посвященные технологиям информационной безопасности в деятельности органов внутренних дел, на которых освещаются результаты инновационных разработок – от электромагнитного экранирования служебных кабинетов, использования генераторов акустического шума, применения тепловизоров до космических навигационных технологий, технологий радиочастотной идентификации, использования компьютерной стеганографии, а также технологий безопасного электронного документооборота. В результате всестороннего изучения инновационных разработок повышается качество подготовки специалистов, возрастает их потенциал с целью противодействия развязыванию угрозы противоборства в информационной среде.

В Санкт-Петербургском и Краснодарском университетах МВД России открыты специальности «Организация и технология защиты информации», «Информационные системы и технологии», «Применение и эксплуатация автоматизированных систем специального назначения», а также в Воронежском институте МВД России существует специальность «Инфокоммуникационные технологии и системы специальной связи».

Одновременно с этим в региональных образовательных учреждениях системы МВД России наблюдается тотальный дефицит подобных специальностей. Обучение информационным технологиям ограничивается следующими предметами: «Информационная безопасность и применение информационных технологий в борьбе с преступностью», «Информационная безопасность и применение информационных технологий в юриспруденции», «Защита информации», «Расследование преступлений в сфере компьютерной информации и высоких технологий». При этом данные дисциплины носят исключительно теоретический и гуманитарный характер, поскольку в вузах отсутствует необходимое оснащение для практических занятий [4, с. 32].

Для примера рассмотрим рабочую программу курса повышения квалификации сотрудников органов внутренних дел МВД России «Противодействие преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий» (см. таблицу).

Как видно из вышеизложенного, рабочая программа курса повышения квалификации сотрудников органов внутренних дел МВД России «Противодействие преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий» освещает исключительно теоретические вопросы.

Разработка образовательных программ должна осуществляться не только с учетом необходимости изучения основ информационной безопасности на правовом и организационном уровнях, но и с учетом специфики киберпреступлений на техническом уровне – физическом, аппаратном, программном и криптографическом. При подготовке специалистов отдельно следует рассматривать компьютерную криминалистику (форензику), уделять внимание методам сбора цифровых доказательств, изучению программного обеспечения, облегчающего разработку и объединения разных компонентов больших программных проектов (фреймворков) для криминалистического анализа и проведения оперативных исследований на удаленных конечных точках, анализу сетевого взаимодействия, средств извлечения информации с исследуемых образов операционных систем, жестких дисков и энергозависимой памяти, средств изучения машинных носителей информации, цифровых устройств и тому подобных элементов.

Теоретические аспекты раскрытия и расследования преступлений с использованием информационных технологий, безусловно, должны исследоваться. Однако теория не должна превалировать над практической деятельностью, в процессе которой и формируются необходимые для раскрытия реальных дел навыки. Каждое теоретическое занятие должно сопровождаться разбором способов совершения киберпреступлений и методик их раскрытия на конкретных примерах

Учебный план «Противодействие преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий»

Наименование разделов и тем	Лекционные занятия	Практические занятия	Самостоятельная подготовка	Форма контроля
Правовые и организационные основы деятельности органов внутренних дел по предупреждению преступлений, совершаемых с использованием современных ИКТ	2	–	–	–
Основные понятия в области информационных технологий и обеспечения информационной безопасности	2	–	2	–
Вопросы квалификации преступлений, совершенных с использованием современных ИКТ	2	2	2	–
Выявление и раскрытие преступлений в сети Интернет				
Противодействие противоправной деятельности ОПГ в сети Интернет	2	–	–	–
Противодействие противоправной деятельности ОПГ по сбыту наркотических средств в сети Интернет	2	–	–	–
Правовое регулирование осуществления оперативно-розыскной деятельности в информационно-телекоммуникационных сетях	2	–	–	–
Особенности проведения оперативно-розыскных мероприятий в сети Интернет	2	–	–	–
Особенности производства отдельных следственных действий по преступлениям, совершаемым с использованием современных ИКТ	2	–	2	–
Выходной контроль	–	–	–	2
Консультация	–	–	–	–
Итоговая аттестация	–	–	–	6
Итого	14	4	6	10

с использованием необходимых технологий. Киберпреступления являются наиболее динамичными видами преступлений, инструментарий которых систематически модернизируется, трансформируется, пополняется. Это, в свою очередь, актуализирует необходимость составления и регулярного обновления методических рекомендаций, алгоритмов раскрытия и расследования киберпреступлений. Помимо того, курсантов и слушателей образовательных учреждений системы МВД России необходимо направлять на стажировки в инновационные центры «Лаборатория Касперского», «Иннополис» и финансовые организации, обладающие соответствующим технологическим оснащением и определенными достижениями в области обеспечения собственной информационной безопасности.

Далее, в целях решения проблемы, связанной с недостаточным уровнем компетенций и навыков преподавательского состава МВД России в области информационных технологий, предлагаем привлекать к учебному процессу сотрудников подразделений «К», киберследователей, экспертов, обладающих практическим опытом в раскрытии данного рода преступлений.

Ключевым фактором совершенствования подготовки сотрудников правоохранительных органов по противодействию преступлениям, совершаемым с использованием информационных технологий, является обеспечение современной материально-технической базой, инновационным оборудованием для практических занятий, основанием полигонов-лабораторий в регионах.

Совершенствование образовательного процесса путем применения передового опыта в области обеспечения собственной информационной безопасности

Фундаментальное условие эффективной подготовки специалистов правоохранительных органов – трансформация и оптимизация парадигмы обучения с учетом специфики киберпреступлений и их расследования. Речь идет в первую очередь о необходимости активного сотрудничества образовательных учреждений системы МВД России с организациями, дос-

тигшими серьезных результатов в области обеспечения собственной информационной безопасности. Одними из ключевых субъектов в данной сфере деятельности, безусловно, являются «ПАО Сбербанк России», «Лаборатория Касперского» и некоторые другие организации. Успешным примером служит сотрудничество ПАО «Сбербанк России» и Университета МВД – банк организовал для Университета МВД полигонно-лабораторные базы, предназначенные для получения и закрепления практических навыков. Такие базы были созданы на факультете подготовки специалистов в области информационной безопасности и в Институте подготовки сотрудников для органов предварительного расследования.

Один из таких объектов – «Лаборатория информационной безопасности в экономической сфере» – предназначен для повышения практических навыков по защите систем, обрабатывающих финансовую информацию. Он оснащен специализированным программным обеспечением для дистанционного банковского обслуживания и другим оборудованием. На практических занятиях курсанты приобретают навыки в обнаружении «цифровых следов» в системах дистанционного банковского обслуживания, знакомятся и работают с различным банковским оборудованием. Объектами исследования выступают в основном «виртуальные следы» и электронные носители информации.

Исходя из анализа ч. 1 ст. 178 УПК РФ, участие эксперта в качестве должностного лица, как представляется, должно быть обеспечено при осмотре трупа [3, с. 92].

Другой объект, предназначенный для обучения будущих следователей, был создан в виде модели отделения Сбербанка. Там установлены банкоматы, устройства самообслуживания и персональные компьютеры. С помощью этого объекта курсанты могут обнаружить, осмотреть и описать не только внешние повреждения терминалов, полученные при классическом взломе, но и запущенное злоумышленниками вредоносное программное обеспечение. Обучаемые получают навыки по снятию образа жесткого диска с банкомата и направлению его на компьютерную экспертизу без выведения банкомата из рабочего состояния и нарушения функционирования отделения финансово-кредитного учреждения. Курсанты отрабатывают проведение таких процессуальных действий, как обыск, изъятие и упаковка электронных носителей информации, выемка, осмотр предметов и документов. Кроме того, обучаемые знакомятся с системой видеонаблюдения банкоматов и отделений банка, получают навыки по обнаружению и изъятию имеющихся фото- и видеозаписей совершенных преступлений, получают изображения преступников [2, с. 18].

В целях предотвращения и эффективной борьбы с киберкриминалом необходимо постоянно следить за последними достижениями науки и техники и прогнозировать потенциальные угрозы, которые они могут нести. Для этого необходимо беспрерывно поддерживать знания сотрудников правоохранительных органов на высоком уровне. Чтобы выполнить это условие, специалисты из разных подразделений МВД должны систематически проходить переподготовку и повышение квалификации. Так, в 2017/2018 учебном году при активной поддержке Сбербанка была проведена переподготовка действующих оперативников и следователей в новых лабораториях и полигонах на базе Университета МВД. Цель – обучение и формирование квалифицированных специалистов для органов внутренних дел, противостоящих преступлениям в сфере информационных технологий, совершаемых в финансовой сфере. Сотрудничество Сбербанка и Университета МВД по противодействию киберпреступлениям будет продолжаться. Однако для адекватного противостояния киберпреступности в этом процессе нужно задействовать все вузы МВД. Наработки Сбербанка, которые использовались в обучающем процессе при взаимодействии с Университетом МВД, могут быть переданы всем учебным заведениям, занимающимся подготовкой и переподготовкой кадров для правоохранительных органов. Было бы полезно создать еще полигоны и лаборатории по противодействию киберпреступлениям по аналогии с созданными в Университете при помощи банка. При необходимости банк готов оказать помощь в организации таких площадок. Все это позволит существенно оптимизировать механизм раскрытия и расследования многих финансово-кредитных преступлений [7, с. 200].

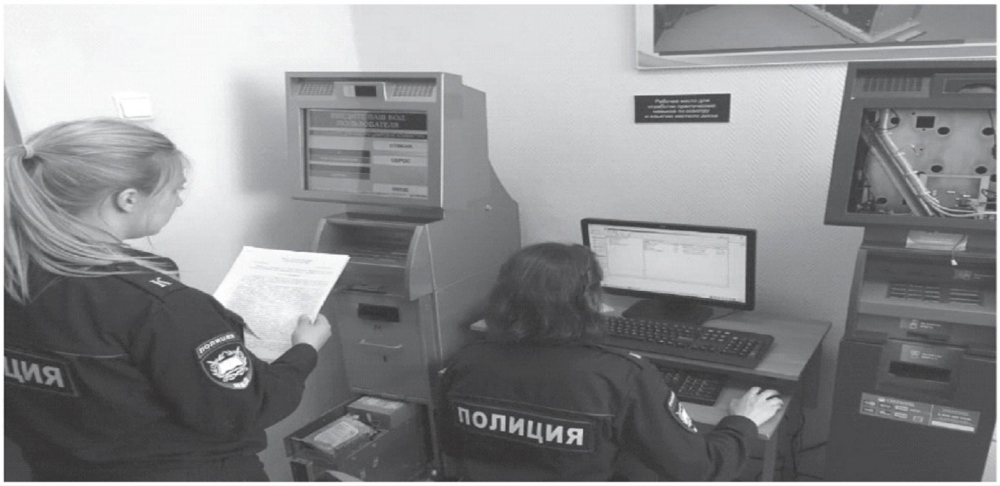

Рис. 1. Осмотр операционной системы скомпрометированного устройства самообслуживания. Исследование журнала событий с целью поиска событий, влияющих на настройки политики безопасности системы

Рис. 2. Получение и отработка умений и навыков по проведению следственного действия: осмотр предмета «Банковский терминал самообслуживания»

Все силы, задействованные для задержания (ликвидации) преступников, образуют боевой порядок. Конкретные посты, группы, подразделения являются элементами этого боевого порядка [6, с. 60].

Для обеспечения личной безопасности сотрудников ОВД необходимо специальное обучение, «педагогика личной безопасности», включающая в себя как определенную систему педагогических идей, так и комплекс практических мер учебно-воспитательного характера, направленных на повышение уровня личной безопасности сотрудников ОВД [5, с. 43].

Выводы

Исходя из вышеизложенного, можно сформулировать приоритетные направления по совершенствованию подготовки сотрудников правоохранительных органов по противодействию преступлениям, совершаемым с использованием информационных технологий:

1. Сотрудничество образовательных учреждений системы МВД России с инновационными центрами «Лаборатория Касперского», «Иннополис» и финансовыми организациями, обладающими определенными достиже-

ниями в области обеспечения собственной информационной безопасности.

2. Систематическое проведение научно-практических конференций по технологиям информационной безопасности в деятельности органов внутренних дел.

3. Привлечение в качестве преподавателей сотрудников подразделений «К», следователей, экспертов, которые имеют практический опыт в раскрытии, расследовании киберпреступлений и осуществлении компьютерных экспертиз.

4. Введение дополнительных профильных специальных дисциплин «Информационная безопасность и применение информационных технологий в борьбе с преступностью», «Информационная безопасность и применение информационных технологий в юриспруденции», «Защита информации», «Расследование преступлений в сфере компьютерной информации и высоких технологий».

5. Организация практических занятий с учетом специфики киберпреступлений на техническом уровне – физическом, аппаратном, программном и криптографическом. Изучение компьютерной криминалистики (форензики), методов сбора цифровых доказательств, фреймворков для криминалистического анализа и проведения оперативных исследований на удаленных конечных точках и т. д.

6. Формирование и подготовка актуальных методических рекомендаций, видеофильмов, раскрывающих алгоритмы раскрытия и расследования преступлений, совершаемых с использованием ИТ (кибератаки, финансовая киберпреступность, использование киберпространства для извлечения доходов от проституции, продажи порнографического контента, а также услуг, связанных с педофилией и т. д.).

7. Модернизация материально-технической базы, создание полигон-лабораторий, осуществление закупок необходимого оборудования для проведения наглядных практических занятий.

8. Введение специальности – киберследователь или киберкриминалист. Вступление развитых стран в шестой технологический уклад, дальнейшая активная цифровизация мировой экономики прогнозируют колоссальное масштабирование и тиражирование преступлений с использованием информационных технологий. Данное обстоятельство актуализирует необходимость популяризации профессии киберследователя – специалиста с междисциплинарным образованием, то есть опыт работы в следственных органах должен будет сочетаться с навыками криминалистики и защиты кибербезопасности.

Подводя итог исследованию, считаем необходимым отметить, что для того, чтобы успешно противодействовать преступлениям, совершаемым с использованием информационных технологий, правоохранительным органам необходимо подготавливать (переподготавливать) кадры, способные работать в современных условиях и отвечать на новые угрозы, возникающие в мире в информационной сфере. Кроме того, правоохранительным органам, в том числе подготавливающим специалистов в данной области образовательным организациям, нужно иметь технический и программный инструментарий, чтобы в дальнейшем научиться проводить цифровые расследования и задержания преступников. Все это требует, безусловно, соответствующего финансирования, причем не только со стороны государства, но и других заинтересованных участников использования информационных технологий в своей деятельности, в частности, банковского сектора и бизнес-структур, которые зачастую становятся жертвами информационных преступников.

СПИСОК ЛИТЕРАТУРЫ

1. Бородкина, Т. Н. Киберпреступления: понятие, содержание и меры противодействия / Т. Н. Бородкина, А. В. Павлюк // Социально-политические науки. – 2018. – № 1. – С. 135–137.

2. Калиниченко, И. А. Начинаем с разборки «железа» / И. А. Калиниченко // Полиция России. – 2017. – № 8. – С. 18–20.

3. Кириченко, Ю. Н. Правовая дефиниция участников уголовного процесса при производстве осмотра трупа: пути совершенствования законодательства / Ю. Н. Кириченко, Е. А. Семенов // Известия юго-западного государственного университета. Серия: История и право. – 2014. – № 3. – С. 90–93.

4. Несмеянов, А. А. Основные проблемы борьбы с преступлениями в сфере высоких технологий / А. А. Несмеянов // Вестник Восточно-Сибирского института МВД России. – 2014. – № 3. – С. 30–35.

5. Подготовка сотрудников органов внутренних дел к действиям по задержанию преступника в условиях ограниченного пространства : учеб. пособие / А. А. Тарасенко, П. Н. Войнов, Ю. Н. Кириченко. – Курск : ООО «ТОП», 2018. – 70 с.

6. Правовые и тактические особенности деятельности сотрудников органов внутренних дел Российской Федерации при задержании правонарушителей : учеб. пособие / Ю. Н. Кириченко, А. А. Устинов, М. Ю. Полушкин. – Белгород : Изд-во БелЮИ МВД РФ им. И.Д. Путилина, 2019. – 107 с.

7. Смирнов, И. В. Партнерство Сбербанка и Университета МВД в борьбе с киберпреступностью / И. В. Смирнов // Вестник экономической безопасности. – 2018. – № 3. – С. 200–203.

8. Хачатурова, С. С. Киберпреступления в информационном обществе / С. С. Хачатурова // Проблемы науки. – 2016. – № 11 (53). – С. 99–100.

REFERENCES

1. Borodkina T.N., Pavlyuk A.V. Kiberprestupleniya: ponyatiye, soderzhaniye i mery protivodeystviya [Cybercrime: Concepts, Content and Measures of Counteraction]. *Sotsialno-politicheskiye nauki* [Social and Political Sciences], 2018, no. 1, pp. 135-137.

2. Kalinichenko I.A. Nachinayem s razborki «zheleza» [Start With Disassembly of "Iron"]. *Politsiya Rossii* [The Police of Russia], 2017, no. 8, pp. 18-20.

3. Kirichenko Yu.N., Semenov E.A. Pravovaya definitsiya uchastnikov ugolovnogo protsessa pri proizvodstve osmotra trupa: puti sovershenstvovaniya zakonodatelstva [Legal Definition of Participants in Criminal Proceedings During the Examination of a Corpse: Ways to Improve Legislation]. *Izvestiya yugo-zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo* [Proceedings of Southwestern State University. Series: History and Law], 2014, no. 3, pp. 90-93.

4. Nesmeyanov A.A. Osnovnyye problemy borby s prestupleniyami v sfere vysokikh tekhnologiy [Main Problems of Fighting Crimes in the Sphere of High Technologies]. *Vestnik Vostochno-Sibirskogo instituta MVD Rossii* [Bulletin of the East Siberian Institute of the Ministry of internal Affairs of Russia], 2014, no. 3, pp. 30-35.

5. Tarasenko A.A., Voynov P.N., Kirichenko Yu.N. *Podgotovka sotrudnikov organov vnutrennikh del k deystviyam po zaderzhaniyu prestupnika v usloviyakh ogranichennogo prostranstva: ucheb. posobiye* [Preparation of Employees of Internal Affairs Bodies for Actions on Detention of the Criminal in the Conditions of Limited Space. Tutorial]. Kursk, OOO «TOP», 2018. 70 p.

6. Kirichenko Yu.N., Ustinov A.A., Polushkin M.Yu. *Pravovyye i takticheskiye osobennosti deyatelnosti sotrudnikov organov vnutrennikh del Rossiyskoy Federatsii pri zaderzhanii pravonarushiteley: ucheb. posobiye* [Legal and Tactical Features of Activity of Employees of Internal Affairs Bodies of the Russian Federation in the Apprehension of Offenders.Tutorial]. Belgorod, BelIuI MVD RF im. I.D. Putilina, 2019. 107 p.

7. Smirnov I.V. Partnerstvo Sberbanka i Universiteta MVD v borbe s kiberprestupnostyu [Partnership of Sberbank and the University of the Ministry of Internal Affairs in the Fight Against Cybercrime]. *Vestnik ekonomicheskoy bezopasnosti* [Bulletin of Economic Security], 2018, no. 3, pp. 200-203.

8. Khachaturova S.S. Kiberprestupleniya v informatsionnom obshchestve [Cybercrime in the Information Society]. *Problemy nauki* [Problems of Science], 2016, no. 11 (53), pp. 99-100.

Information About the Authors

Ivan N. Arkhiptsev, Candidate of Sciences (Jurisprudence), Associate Professor, Department of Criminal Law Disciplines, Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin, Gorkogo St., 71, 308024 Belgorod, Russian Federation, ArhiptsevIN@yandex.ru, https://orcid.org/0000-0003-2307-2712

Alexander V. Sarychev, Lecturer, Department of Tactical and Special Training, Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin, Gorkogo St., 71, 308024 Belgorod, Russian Federation, w0773@yandex.ru, https://orcid.org/0000-0002-2115-3191

Roman V. Krasnikov, Lecturer, Department of Tactical and Special Training, Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin, Gorkogo St., 71, 308024 Belgorod, Russian Federation, rvk.doc@mai.ru, https://orcid.org/0000-0002-2161-6678

Информация об авторах

Иван Николаевич Архипцев, кандидат юридических наук, доцент кафедры уголовно-правовых дисциплин, Белгородский юридический институт МВД России им. И.Д. Путилина, ул. Горького, 71, 308024 г. Белгород, Российская Федерация, ArhiptsevIN@yandex.ru, https://orcid.org/0000-0003-2307-2712

Александр Викторович Сарычев, преподаватель кафедры тактико-специальной подготовки, Белгородский юридический институт МВД России им. И.Д. Путилина, ул. Горького, 71, 308024 г. Белгород, Российская Федерация, w0773@yandex.ru, https://orcid.org/0000-0002-2115-3191

Роман Владимирович Красников, преподаватель кафедры тактико-специальной подготовки, Белгородский юридический институт МВД России им. И.Д. Путилина, ул. Горького, 71, 308024 г. Белгород, Российская Федерация, rvk.doc@mai.ru, https://orcid.org/0000-0002-2161-6678