

ИСАЕВА Елена Дмитриевна,
доцент кафедры криминалистики и уголовно-правовых дисциплин
Брянского филиала Орловского юридического института
МВД России имени В.В. Лукьянова,
e-mail: isaevaeltna1903732 @yandex.ru

ОСМАНОВ Мухамед Мартинович,
старший преподаватель кафедры
организации правоохранительной деятельности
Северо-Кавказского института повышения квалификации
сотрудников МВД (филиал) Краснодарского университета МВД России,
кандидат педагогических наук, подполковник полиции,
e-mail: muhamedosmanov8@gmail.com

К ВОПРОСУ О СОВЕРШЕНСТВОВАНИИ ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПЛЕНИЯМ

Аннотация. Статья посвящена анализу деятельности органов внутренних дел Российской Федерации в области борьбы с противоправными действиями в информационном пространстве.

Автор фокусируется на выявлении существующих трудностей в правоприменительной практике и формулирует предложения по совершенствованию профессиональной подготовки сотрудников для повышения результативности борьбы с киберпреступностью.

Ключевые слова: киберпреступность, борьба с преступностью, органы внутренних дел, информационные технологии, правоприменительная практика, совершенствование подготовки, правоохранительные органы, цифровая безопасность.

ISAEVA Elena Dmitrievna,
Associate Professor of the Department
of Criminology and Criminal Law Disciplines,
Bryansk Branch Oryol Law Institute of the Ministry
of Internal Affairs of Russia named after V.V. Lukyanov

OSMANOV Mukhamed Martinovich
Senior Lecturer at the Department of Organization
of Law Enforcement Activities of the North Caucasus Institute
for Advanced Training of Ministry of Internal Affairs Officers (branch)
of the Krasnodar University of the Ministry of Internal Affairs of Russia,
Candidate of Pedagogical Sciences, Police Lieutenant Colonel

ON THE ISSUE OF IMPROVING THE PROFESSIONAL TRAINING OF EMPLOYEES OF THE INTERNAL AFFAIRS BODIES OF THE RUSSIAN FEDERATION IN COUNTERING CYBERCRIME

Annotation. The article is devoted to the analysis of the activities of the internal affairs bodies of the Russian Federation in the field of combating illegal actions in the information space.

The author focuses on identifying existing difficulties in law enforcement practice and formulates proposals for improving the professional training of employees to increase the effectiveness of the fight against cybercrime.

Key words: cybercrime, crime control, law enforcement agencies, information technology, law enforcement practice, training improvement, law enforcement agencies, digital security.

Органы внутренних дел являются основным субъектом обеспечения охраны общественного порядка и общественной безопасности государства.

Наряду с обеспечением правопорядка и соблюдения законности гражданами в общественных местах в своей повседневной деятельности структурными подразделениями органов внутренних дел, отдельными специализированными структурными подразделениями выполняются задачи по противодействию преступлениям, совершаемым и в сети Интернет.

Вместе с тем, необходимо отметить, что для обеспечения эффективной борьбы с киберпреступлениями компетентные должностные лица правоохранительных органов должны быть не только профессионально грамотными в осуществлении своих юрисдикционных полномочий, но и обладать достаточными познаниями в сфере информационных технологий.

В виду чего, усовершенствование их способностей и знаний в данной сфере является необходимым в обеспечении противодействия киберпреступности и является безусловным приоритетом.

Это означает необходимость пересмотра учебных программ, внедрения инновационных методов обучения и предоставления возможности для практического освоения новейших программных и аппаратных средств.

Для эффективного противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, первостепенное значение имеет развитие цифровой грамотности. Эта компетенция необходима как сотрудникам правоохранительных органов, так и широкой общественности.

Не исключено, что сотрудники органов внутренних дел, используя возможности и услуги интернет-ресурсов, также могут стать целью киберпреступников и завладеть их скрытой информацией, используемой в оперативно-служебной деятельности и личными сведениями граждан или получить доступ к ведомственным сайтам.

Цифровая грамотность – это не только умение пользоваться современными технологиями и адаптироваться к новым форматам общения, но и способность действовать этично и ответственно в цифровом пространстве.

Она включает в себя комплекс практических навыков, методов защиты и мер предосторожности, обеспечивающих безопасность пользователей и их данных в онлайн-среде.

Актуальность повышения цифровой грамотности обусловлена необходимостью свободно ориентироваться в постоянно развивающихся

цифровых технологиях, приобретения навыков эффективного использования цифровой среды и критического восприятия информации, полученной из Интернет-пространства.

Важно обозначить, что в свою очередь законодатель в качестве составляющей научно-технического и кадрового обеспечения создания и функционирования государственной системы противодействия IT-преступлениям акцентирует внимание на необходимость систематического повышения квалификации, подготовку и переподготовку сотрудников, компетентных в противодействии противоправным действиям, совершаемым с использованием сети Интернет.

Особая значимость в необходимости формирования профессиональной компетенции сотрудников полиции в сфере противодействия цифровым преступлениям определяется социальным заказом на подготовку специалистов, способных оперативно и профессионально грамотно выполнять профессиональные задачи с использованием новейших программных и инновационных технических средств, а также находить не типичные решения.

На данный момент в вопросах связанных с обучением сотрудников, которые могли бы оказать противодействие злоумышленникам в сети Интернет, имеются некоторые сложности и подвержена дискуссии в научной среде, причиной которого являются следующие дилеммные моменты:

- 1) Общество остро нуждается в более эффективном противодействии постоянно растущему числу информационных преступлений. Система образования, в свою очередь, демонстрирует недостаточную оперативность и гибкость в подготовке юридических специалистов, способных противостоять киберпреступности, что приводит к дефициту соответствующей компетентности.
- 2) Существует явная потребность в формировании у юристов компетенций для борьбы с преступлениями в сфере информационных технологий, однако существующая система педагогического обеспечения данного процесса оказывается неполноценной.
- 3) Для успешной деятельности по противодействию киберпреступлениям юристам необходимо повысить уровень своей информационно-технической подготовки. При этом существующий методический инструментарий для формирования у обучающихся соответствующей компетентности является недостаточным.

Главной задачей повышения эффективности кадрового потенциала в борьбе с преступле-

ниями, совершаемыми в сети Интернет, является обеспечение кадровой и методической готовности органов внутренних дел выявлять, расследовать и предотвращать подобного рода правонарушения и преступления с соблюдением правовых и этических норм и правил.

Компетентность сотрудника ОВД в сфере информационных ресурсов и технологий представлено глубокими познаниями и навыками работы в сети Интернет, способствующее в выполнении своей оперативно-служебной деятельности специализированным сотрудником на должном уровне, в соответствии с современными реалиями и помогающей в выявлении и раскрытии преступлений в информационном пространстве с использованием информационных технологий, удовлетворяющие требованиям населения и государства в целом.

Кроме того, важными аспектами компетентности в области информационной сфере являются определенные личностные качества и способности, которые позволяют сотрудникам адаптироваться к постоянно меняющимся условиям работы, быстро реагировать на новые вызовы и угрозы, а также принимать обоснованные и взвешенные решения в рамках своей профессиональной деятельности.

В этой связи особое внимание при подготовке сотрудников ОВД должно уделяться формированию у них системного мышления и навыков работы в команде для эффективного противодействия киберугрозам и обеспечения информационной безопасности.

Не менее значимой является способность к самообразованию и самосовершенствованию, ведь технологии не стоят на месте, и регулярно появляются новые инструменты и методы защиты информации.

Нельзя отрицать, что компетенции в области противодействия IT-преступлениям не могут быть выработаны исключительно на основе правовых знаний и норм. Необходимо, чтобы эти компетенции основывались на уверенном владении современными информационными технологиями, что, в свою очередь, предполагает наличие у сотрудников ОВД не только теоретических, но и практических навыков работы с ними.

В этой связи при подготовке сотрудников ОВД следует уделять внимание не только теоретической подготовке, но и практическим занятиям, в том числе проведению тренингов и симуляции кибератак, что будет способствовать не только усвоению необходимых знаний, но и оперативному применению их в реальных ситуациях.

В современных условиях традиционные образовательные подходы, такие как лекции и инструктажи, продолжают играть свою роль в передаче фундаментальных знаний, однако их

эффективность при формировании и закреплении практических навыков, как правило, ограничена.

В этой связи большой потенциал имеют интерактивные методы обучения, которые открывают перед слушателями широкие возможности для активного вовлечения в процесс обучения.

Среди методов, которые заслуживают особого внимания, можно обозначить необходимость владения богатым практическим опытом в борьбе с киберпреступлениями, совершаемые посредством применения вредоносных программных обеспечений, такими как:

- 1) Киберджекинг;
- 2) Кибершатаж;
- 3) Фишинг;
- 4) Вымогательство;
- 5) Компьютерный саботаж

Эффективная программа обучения для сотрудников органов внутренних дел Российской Федерации в выявлении и борьбы с выше обозначенными киберпреступлениями, будет способствовать эффективному расследований преступлений соответствующими должностными лицами ОВД.

Также стоит отметить, что не мало важно обеспечение необходимой качественной обратной связи и предоставление дополнительных обучающих источников, которые помогут закрепить полученные знания и навыки, что позволит не только повысить уровень понимания материала, но и обеспечить его практическое применение в реальных условиях.

Кроме того, необходимо постоянно обновлять базы данных о новых видах IT-преступлений и методах их предотвращения, что позволит оперативно реагировать на изменения в киберугрозах и поддерживать высокий уровень защиты информационных ресурсов.

Данный подход не только укрепит защиту от потенциальных атак, но и повысит общую осведомленность сотрудников ОВД о последних тенденциях в области кибербезопасности.

В контексте совершенствования деятельности по противодействию IT-преступлениям особое внимание уделяется разработке специализированных программ обучения, которые позволяют оперативно адаптировать специалистов к постоянно меняющимся условиям и угрозам в сфере информационной безопасности.

К примеру, проводятся курсы повышения квалификации, семинары и тренинги, направленные на обмен опытом и изучение новых методик и технологий в сфере противодействия преступлениям совершаемым в сети Интернет.

Вместе с тем актуально отметить, что в практике деятельности образовательных организаций МВД России в настоящее время отсут-

ствуется единая программа, которая бы учитывала все аспекты и специфику работы в области информационной безопасности, а также обеспечивала бы высокую степень совместимости и актуальности получаемых знаний.

С учетом специфики рассматриваемых вопросов и постоянной модернизации информационных технологий содержательная составляющая программы подготовки сотрудников ОВД по противодействию IT-преступлениям должна регулярно актуализироваться, что позволит поддерживать высокий уровень готовности к возможным угрозам и обеспечит эффективное реагирование на любые инциденты в сфере информационной безопасности.

Подводя итоги исследования совершенно объективно можно отметить, что, одним из основных аспектов в деятельности образовательных организаций системы МВД России является систематическое совершенствование и увеличение образовательных программ, ориентированных на углубление знаний и развитие профессиональных умений и навыков сотрудников органов внутренних дел.

В виду вышеизложенного целесообразно выделить, что в последствие данные предложения будут способствовать повышению эффективности их деятельности в сфере противодействия противоправным деяниям, связанным с использованием современных информационных технологий.

Список литературы:

- [1] Сорокун Н.С. Особенности квалификации, выявления, устранения причин и условий совершения киберпреступлений на современном этапе / Н.С. Сорокун, О.В. Ермакова // Алтайский юридический вестник. 2023. № 3 (43). С. 134-135.
- [2] Винкерт В.В. Понятие и особенности киберпреступлений / В.В. Винкерт, А.Л. Клочкова // Междисциплинарные исследования: опыт прошлого, возможности настоящего, стратегии будущего. 2021. № 5. С. 172-173.
- [3] О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 г. № 400 // СЗ РФ. 2021. № 27 (ч. 2). Ст. 5351.
- [4] Конвенция Организации Объединенных Наций против киберпреступности, принята резолюцией 79/243 Генеральной Ассамблеей от 24.12.2024
- [5] Козырева А.А. Определение термина «кибергигиена» и возможность его применения в правовом поле // Пробелы в российском законодательстве. 2018. № 7. С. 92-94; Крюкова Е.С., Малофеев В.А., Парашук И.Б. Вопросы киберги-

гиены пользователей и операторов автоматизированной системы управления электронной библиотекой // Научные технологии в космических исследованиях Земли. 2021. Т. 13. № 2. С. 66-73.

[6] Лахтиков Д.Н. Инновационные подходы в подготовке специалистов в сфере противодействия киберпреступности // Современные цифровые технологии в деятельности образовательных организаций силовых ведомств: концепция, практика, инновации: сб. мат. II Межд. науч.-практ. конф. Уфа, 2020. С. 65.

[7] Петров К.Н. Проблемы совершенствования тактико-специальной подготовки курсантов и слушателей образовательных организаций МВД России // Вестник Московского государственного областного университета. Серия: Педагогика. 2022. № 3. С. 149.

References:

- [1] Sorokun N.S. Features of qualification, identification, elimination of the causes and conditions for committing cybercrimes at the present stage/N.S. Sorokun, O.V. Ermakova//Altai Legal Bulletin. 2023. № 3 (43). S. 134-135.
- [2] Winkert V.V. The concept and features of cybercrime/V.V. Winkert, A.L. Klochkova//Interdisciplinary research: past experience, present possibilities, future strategies. 2021. № 5. S. 172-173.
- [3] On the National Security Strategy of the Russian Federation: Decree of the President of the Russian Federation of 02.07.2021 No. 400//of the RF NW. 2021. No. 27 (part 2). Art. 5351.
- [4] United Nations Convention against Cybercrime, adopted by the General Assembly in its resolution 79/243 of 24.12.2024
- [5] Kozyreva A.A. Definition of the term "cyber hygiene" and the possibility of its application in the legal field//Gaps in Russian legislation. 2018. № 7. S. 92-94; Kryukova E.S., Malofeev V.A., Parashuk I.B. Issues of cyber hygiene of users and operators of the automated electronic library management system// High-tech technologies in space research of the Earth. 2021. T. 13. № 2. S. 66-73.
- [6] Lakhtikov D.N. Innovative approaches in training specialists in the field of countering cybercrime//Modern digital technologies in the activities of educational organizations of law enforcement agencies: concept, practice, innovation: Sat. mat. II Intl. scientific-practical. conf. Ufa, 2020. S. 65.
- [7] Petrov K.N. Problems of improving tactical and special training of cadets and students of educational organizations of the Ministry of Internal Affairs of Russia//Bulletin of the Moscow State Regional University. Series: Pedagogy. 2022. № 3. S. 149.