5. Постановление Правительства Российской Федерации от 27 ноября 2017 г. № 1428 «Об особенностях осуществления закупки для нужд страны и безопасности государства» // СЗ РФ. 2017. № 49. ст. 7465.
6. Постановление Правительства Российской Федерации от 08.02.2017 № 145 «Об утверждении Правил формирования и ведения в единой информационной системе в сфере закупок каталога товаров, работ, услуг для обеспечения государственных и муниципальных нужд и Правил использования каталога товаров, работ, услуг для обеспечения государственных и муниципальных нужд» // СЗ РФ. 2017. № 7 ст. 1084
7. Приказ МВД России от 21 июля 2018 № 460 «Об определении требований к закупаемым подразделениями и организациями МВД России отдельным видам товаров, работ, услуг (в том числе предельных цен товаров, работ, услуг)» // https://base.garant//73426211/
8. Елисеев О. В. Повышение эффективности выполнения государственного оборонного заказа на основе развития контрактного механизма: Дисс. … канд. экон. наук. М., 2014.
9. Малыхина Е. А. Контрактная система в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд: особенности финансово-правового регулирования: Дисс. … канд. юрид. наук. Саратов, 2015.

УДК 004.9

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ПОДГОТОВКИ СОТРУДНИКОВ, СПЕЦИАЛИЗИРУЮЩИХСЯ НА ПРОТИВОДЕЙСТВИИ ИТ-ПРЕСТУПЛЕНИЯМ

***П. Б. Скрипко**, начальник кафедры информационного и технического обеспечения ОВД Дальневосточного юридического института МВД России, кандидат технических наук, доцент*

С учетом требований руководящих документов МВД России рассматриваются вопросы содержания программ подготовки сотрудников, специализирующихся на противодействии ИТ-преступлениям, и предлагается расширить их тематику за счет формирования специализированных компетенций поиска и сбора информации в интернет, компьютерной криминалистики и этичного хакинга.

Ключевые слова: противодействие ИТ-преступлениям, повышение квалификации, методы поиска и сбора информации, компьютерная криминалистика, этичный хакинг.

FEATURES OF IMPLEMENTATION OF EDUCATIONAL TRAINING PROGRAMS FOR EMPLOYEES SPECIALIZING IN COUNTERING IT CRIMES

P. B. Skripko, *Head of the Department of Information and Technical Support of the Internal Affairs Directorate of the Far Eastern Law Institute of the Ministry of Internal Affairs of Russia, kandidat nauk, degree in Technical Sciences, Associate Professor*

Taking into account the requirements of the guidance documents of the Ministry of Internal Affairs of Russia, the content of training programs for employees specializing in combating IT crimes is considered, and it is proposed to expand their topics by developing specialized competencies for searching and collecting information on the Internet, computer forensics and ethical hacking.

Keywords: combating IT crimes, professional development, methods of searching and collecting information, computer forensics, ethical hacking.

Значительное увеличение числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (далее – ИТ-преступления), прирост которых в 2020 году составил более 75 % при их раскрываемости, не превышающей 25 % [4], требует от правоохранительных органов принятия незамедлительных мер по предотвращению, выявлению, раскрытию и расследованию данного вида преступлений. Ключевым условием для повышения эффективности противодействия ИТ-преступлениям является повышение профессионального уровня сотрудников органов внутренних дел в сфере информационных и телекоммуникационных технологий, особенно в части идентификации преступников, отслеживания и документирования их действий.

Высокие темпы развития информационных и телекоммуникационных технологий, внедрение систем искусственного интеллекта и технологий больших данных отражается и на характере криминальной активности в киберпространстве. Это не только новые виды и способы совершения ИТ-преступлений и сокрытия следов преступной деятельности, но и новые объекты преступных посягательств, новые компетенции злоумышленников. МВД России со своей стороны принимает ряд мер, направленных на повышение уровня знаний сотрудников в сфере информационных и телекоммуникационных технологий. В частности, это утвержденные Министром внутренних дел Российской Федерации генералом полиции Российской Федерации В. А. Колокольцевым комплексы мероприятий [1, 2].

В этой связи наиболее оптимальным решением задачи повышения профессионального уровня сотрудников ОВД, специализирующихся на противодействии ИТ-преступлениям, является реализация дополнительных профессиональных программ повышения квалификации данной категории сотрудников. Краткие сроки реализации, актуальность и практическая направленность содержания таких образовательных программ, возможность ежегодного обучения, а при необходимости и каждые полгода, позволяет обеспечить требуемый уровень подготовки сотрудников в области противодействия ИТ-преступлениям.

В настоящее время в Дальневосточном юридическом институте реализуется ряд программ направленности противодействия ИТ-преступлениям. Это дополнительные программы повышения квалификации следующих категорий сотрудников:

– занимающихся вопросами выявления и расследования преступлений, связанных с использованием криптовалют и других виртуальных активов;

– задействованных в раскрытии и расследовании преступлений, совершаемых с использованием современных информационно-коммуникационных технологий;

– специализирующихся на выявлении и пресечении преступлений в сфере незаконного оборота наркотических средств, совершаемых с использованием современных информационно-коммуникационных технологий и электронных платежных систем;

– участвующих в расследовании преступлений, связанных с заведомо ложными сообщениями об акте терроризма и совершенных с использованием современных информационных технологий.

Не смотря на востребованность подготовки сотрудников по указанным программам со стороны территориальных подразделений МВД России, актуальность их структуры и содержания, остается ряд вопросов, рассмотрение которых требует включения в состав данных программ дополнительной тематики. Предполагается, что ключевыми составляющими данной тематики должны стать вопросы идентификации личности и местоположения злоумышленника, выявление и документирование следов совершения и сокрытия преступлений. Изучение данных вопросов в рамках программ повышения квалификации позволит сформировать ряд необходимых компетенций, которые условно можно разделить на следующие три группы.

I группа – *компетенции поиска информации*. Группа включает соответствующие знания и умения применять методы и приемы поиска и сбора сведений о людях, компаниях, событиях; представления о принципах работы поисковиков, языках поисковых запросов; знания архитектуры, особенностей функционирования, а также «недокументированные» возможности популярных поисковых ресурсов (google, yandex). При этом следует также знать

о методах поиска и сбора информации в «теневом» или «сером интернет» (darknet'е) и мессенеджерах. В эту же группу необходимо включить умения по применению методов и инструментов OSINT – технологии разведки на основе открытых источников [5].

Формирование компетенций этой группы позволит сотрудникам без привлечения специального инструментария, специалистов и подразделений эффективно осуществить сбор информации (сведений) на начальном этапе расследования ИТ-преступлений. К такой информации можно отнести, например, такие находящиеся в открытом доступе сведения, как сведения об организациях, расчетных банковских счетах, руководителях, юридических адресах и т. д. В свою очередь знания и умения применять методы поиска информации в darknet и мессенджерах даст возможность собрать дополнительные сведения негативного характера.

Что касается инструментов OSINT, то эта относительно новая технология сбора информации уже обладает достаточно развитым и разнообразным инструментарием, а предлагаемые в рамках данной технологии методики интернет-разведки найдут применение в противодействии ИТ-преступлениям. Также, в составе первой группы компетенций следует отметить знания и умения, относящиеся к сбору и аналитической обработке Больших данных, что позволит выявлять так называемые исключения – подозрительные факты.

II группа – *компетенции по компьютерной криминалистике*. В состав этой группы входят умения и практические навыки поиска цифровых следов в компьютерных системах, фиксации этих следов в качестве доказательств по гражданским и уголовным делам, анализа собранных материалов с целью выявления источника атаки и восстановления работоспособности системы, а также документирования противоправных действий злоумышленников [3].

К умениям и знаниям этой группы следует отнести особенности производства компьютерно-технической экспертизы, применяемое при этом оборудование и программные средства, методы поиска уликовой информации на компьютерах, методы сокрытия данных от обнаружения, основы исследования операционных систем, сообщений электронной почты.

Учитывая специфику современных средств хранения и обработки информации при формировании компетенций компьютерной криминалистики обеспечить выработку умений и навыков работы с криптографией, в том числе поиска и вскрытия зашифрованных данных, извлечения паролей из браузеров и мессенджеров, а также уделить внимание вопросам фиксации содержимого мобильных устройств, обеспечивая при этом изоляцию от беспроводных сетей передачи данных, предотвращение блокировки устройств, модификации или уничтожения данных.

Так как основная часть ИТ-преступлений совершается в информационно-телекоммуникационных сетях, то знания основных принципов и источников данных для сетевой криминалистики позволят осуществлять противодействие таким преступлениям на более высоком техническом уровне.

III группа – *компетенции этичного хакинга*. В этой группе представлены умения и навыки, направленные на выявление кибератак, в том числе путем подмены сайтов на мошеннические, оперативное определение местоположения киберпреступников, определение источника распространения нежелательной информации в интернет, сбор данных с цифровых устройств, мобильных устройств, GPS-трекеров, данных камер и других устройств, относящихся к так называемому «интернету вещей».

В ходе формирования компетенций III группы предполагается изучение вопросов, связанных с особенностями сетевых атак и их классификацией, способами сбора информации регистрационного характера о составе, структуре и топологии сети, выявлением уязвимостей, методам восстановления паролей, применением шпионского программного обеспечения, стеганографией и сокрытием следов, методами обнаружения атак. Комплекс знаний и умений по применению криптографических защитных механизмов позволит обеспечить необходимый уровень защиты служебной информации в ходе профессиональной деятельности.

Следует отметить, что объем вопросов, представленных в отмеченных выше трех группах компетенций, достаточной большой и не может быть реализован в рамках только одной из программ повышения квалификации. Поэтому, по нашему мнению, целесообразно расширять не только тематику дополнительных профессиональных программ, но и реализовывать указанные вопросы в рамках изучения дисциплин основных образовательных программ высшего образования.

Список источников

1. Комплекс мероприятий по переподготовке и повышению квалификации сотрудников МВД России, специализирующихся на противодействии преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, в образовательных организациях, не входящих в систему МВД России (на 2020–2021 годы): утв. министром внутренних дел от 26.03.2020 г. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».
2. Комплекс мероприятий по формированию эффективной системы подготовки кадров для органов внутренних дел Российской Федерации, специализирующихся на предотвращении, выявлении, раскрытии и расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (на 2021–2022 гг.): утв. министром внутренних дел от 30.04.2021 г. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

3. Компьютерная криминалистика (Форензика) // Информационная безопасность: [сайт]. URL: https://spy-soft.net/computer-forensics/ (дата обращения 22.07.2021).
4. Краткая характеристика состояния преступности в Российской Федерации за январь – октябрь 2020 года // Официальный сайт МВД России: [сайт]. URL: https://мвд.рф/reports/item/21933965/ (дата обращения 22.07.2021).
5. Что такое OSINT? – основные инструменты и методы // Школа профессиональных аналитиков – ИАС Буратино: [сайт]. URL: https://spspa.ru/chto-takoe-osint-osnovnye-instrumenty-i-metody/ (дата обращения 22.07.2021).

УДК 343.296

ПРАВОВЫЕ СРЕДСТВА, ОБЕСПЕЧИВАЮЩИЕ ВОЗМЕЩЕНИЕ ПРЕСТУПНОГО ВРЕДА ПОТЕРПЕВШЕМУ В ЗАКОНОДАТЕЛЬСТВЕ СТРАН СНГ

Н. К. Сливко, *преподаватель кафедры Дальневосточного юридического института МВД России*

Статья посвящена анализу правовых средств, обеспечивающих восстановление прав потерпевших от преступлений, предусмотренных законодательством некоторых стран-участников Содружества Независимых Государств. Автор приходит к выводу о прогрессивном характере данных средств в части их непосредственной направленности на восстановление социальной справедливости, нарушенной преступным деянием.

Ключевые слова: потерпевший; уголовное законодательство; возмещение преступного вреда; восстановление социальной справедливости; позитивное посткриминальное поведение.

LEGAL MEANS OF PROVIDING COMPENSATION OF CRIMINAL HARM TO THE VICTIM OF CRIME IN THE LEGISLATION OF CIS COUNTRIES

N. K. Slivko, *lecturer of the department of the Far Eastern Law Institute of the Ministry of Internal Affairs of Russia*

The article is devoted to the analysis of criminal legal means of providing the restoration of victims of crimes rights, provided in the legislation of some countries-participants of the Commonwealth of Independent