М. С. Абламейко
(M. S. Ablameyko)

УДК 343.9

КРИМИНАЛИСТИЧЕСКОЕ КОМПЬЮТЕРОВЕДЕНИЕ КАК НОВАЯ ДИСЦИПЛИНА ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ДЛЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

(FORENSIC COMPUTER SCIENCE AS A NEW DISCIPLINE FOR THE TRAINING OF SPECIALISTS FOR THE INVESTIGATION OF HIGH-TECH CRIMES)

Стремительное развитие информационно-коммуникационных технологий делает актуальной и значимой проблему предупреждения интернет-преступности. В этой связи для расследования киберпреступлений необходима подготовка высококвалифицированных специалистов, владеющих как правовыми, так и техническими знаниями. С целью повышения цифровой грамотности юристов в данной статье предлагается ввести специальный курс подготовки специалистов для углубленного изучения основ криминалистики, информационного права и компьютерной техники. Показано место данного курса в учебном процессе.

Ключевые слова: подготовка кадров; криминалистика; компьютерная техника

Введение. Неуклонный технический прогресс, развитие информационных технологий и самой техники привели к цифровой трансформации общества. Сегодня сложно представить себе человека, который не пользуется различного рода «гаджетами» для получения, хранения и распространения информации. Развитые страны идут по пути предоставления доступа в Интернет для реализации прав и потребностей своих граждан. Республика Беларусь занимает 32 место среди 176 стран мира и первое место среди стран СНГ в рейтинге Международного союза электросвязи по развитию информационно-коммуникационных технологий.

Количество пользователей сети стремительно растет. При этом, чем дальше, тем моложе становится пользователь. Это обусловлено рядом факторов: с одной стороны, техника стала доступной для большинства людей развитых стран, с другой стороны, государства всего мира уделяют пристальное внимание развитию цифрового общества и предоставлению все больших возможностей в сети Интернет, с третьей стороны, из года в год растет цифровая грамотность населения. Последнее связано с тем, что с течением времени сеть Интернет предоставляет все более широкий круг возможностей. Помимо передачи информации и общения все более распространенным стали сервисы осуществления транзакций, электронная торговля и т. д.

Наряду со всеми положительными моментами развития информатизации постоянная трансформация общества приводит к возникновению новых видов преступной деятельности, включая сферу высоких технологий. Рост преступности в данной сфере обусловлен рядом факторов. Во-первых, «омоложением» преступников. Еще совсем недавно потрет преступника в сфере высоких технологий представлялся следующим образом: человек от 30 лет с техническим образованием, имеющий доступ к сети Интернет. В настоящее время все изменилось: это уже человек от 12 лет, способный к самообразованию в сети, ведь подростки являются активными пользователями всевозможных «гаджетов» и в целом «живут в сети». Вторым существенным фактором является отсутствие понимания последствий совершаемых действий. Все больше противоправных действий в сети совершается несовершеннолетними. При этом для данной категории преступлений характерен высокий уровень латентности.

По имеющимся данным, Следственный комитет ожидает увеличения числа киберпреступлений

Абламейко Мария Сергеевна, доцент кафедры конституционного права юридического факультета Белорусского государственного университета (Беларусь, 220030, г. Минск, ул. Ленинградская, 8), кандидат юридических наук, доцент, специалист по информационному праву

Maria S. Ablameyko, Belarusian State University (Minsk, Belarus), Ph. D. in law, Associate professor

e-mail: m.ablameyko@mail.ru; тел. / tel.: +375172095576

и роста использования преступниками криптовалюты. По данным МВД, в 2019 году значительно выросло число зарегистрированных киберпреступлений – до 10,5 тыс. (в 2018 г. их было свыше 4,7 тыс.). Более двух третьих из зафиксированных в прошлом году преступлений относятся к хищениям путем использования компьютерной техники (ст. 212 УК). Число преступлений против информационной безопасности (ст. 349-355 УК) возросло в целом по стране в 2,2 раза. Обусловлено это, по мнению правоохранителей, увеличением количества фактов несанкционированного доступа к компьютерной информации – с 912 до 2185 [1].

Технический потенциал сети Интернет предоставляет неограниченные возможности для совершения противоправных действий, что вызывает опасения как со стороны правоохранительных органов, так и общества в целом. При этом Интернет позволил более эффективно и безнаказанно совершать ранее традиционные преступления и породил новые, неизвестные мировому сообществу виды общественно опасных посягательств [2].

Проблема интернет-преступности становится все более актуальной, что, в свою очередь, диктует необходимость ее исследования с целью выработки конкретных предупредительных мер. В этой связи возрастает необходимость подготовки высококвалифицированных специалистов, понимающих не только правовые вопросы, но и техническую сторону данного вопроса. Для этого мы предлагаем ввести специальный курс для подготовки профессиональных специалистов, глубоко знакомых как с основами криминалистики, информационного права, так и с основами компьютерной техники.

Основная часть. Вопросам криминалистического исследования компьютерной информации, средств ее обработки и защиты было уделено определенное внимание в отечественных и зарубежных монографиях, учебниках и учебных пособиях, научных статьях, выступлениях на различных конференциях и семинарах, сообщениях средств массовой информации. Эти вопросы рассматривались и изучались в рамках частных методик расследования компьютерных преступлений, общей теории судебной экспертизы, криминалистической тактики и техники [3].

В связи с быстрыми темпами развития информатизации большое внимание уделяется проблемам использования компьютерной информации при раскрытии, расследовании и предупреждении преступлений. Реалии сегодняшнего дня определяют существенные изменения в сложившихся фундаментальных подходах в криминалистике. В настоящее время при раскрытии практически любого преступления изымается компьютерная техника, производится ее осмотр с точки зрения получения значимой информации по уголовному делу. Именно социализация человека в сети позволяет устанавливать связи с людьми, определять местоположение, используя геолокацию, отслеживать проведение транзакций и многое другое. По сути жизнь человека зеркально отражается в сети и впоследствии продолжает существовать даже после фактического удаления.

Впервые курс дисциплины «Криминалистическое компьютероведение» был предложен и научно обоснован В. Б. Веховым, который определил его как отрасль криминалистической техники, представляющей собой систему научных положений и основанных на них методических рекомендаций по исследованию и использованию компьютерной информации, а также средств ее создания, обработки и передачи для выявления, раскрытия, расследования и предотвращения преступлений [4]. По данному направлению автором написано достаточно большое количество статей, а также защищена докторская диссертация. Считаем целесообразным использовать данный опыт и модифицировать предложенный курс с учетом происходящих изменений.

Курс «Криминалистическое компьютероведение» должен быть междисциплинарным и включать в себя как юридические науки, такие как уголовный процесс, криминалистику, судебные экспертизы, так и технические: информатику, математику, физику, электронику и другие науки. Понятно, что за четыре года подготовки юристов нет возможности дать основы всех этих дисциплин. Но для студентов, которые выберут для себя данное направление, возможно на младших курсах предусмотреть ознакомление с основами компьютерной техники, защиты информации, сетевых технологий. Это позволит им в дальнейшем легче воспринимать предлагаемый курс, который целесообразно внедрить на второй ступени высшего образования – магистратуре по профилизации «Прокурорско-следственная деятельность» на юридическом факультете БГУ. Кроме того, представляется, что подобный курс может быть интересен для Академии МВД, а также для Академии управления при Президенте Республики Беларусь в связи с образованием кафедры правового обеспечения правоохранительной деятельности.

Предлагаемый курс может, по нашему мнению, включать следующие разделы:

1. *Понятие и сущность компьютерной информации как объекта криминалистического исследования.* Компьютерная информация, закрепленная на материальном носителе, имеет большую ценность при расследовании преступлений.

Термин «компьютерная информация» широко трактуется в научных кругах, однако законодательное закрепление в белорусском праве отсутствует до сих пор. Рекомендации по правовому регули-

рованию эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях, принятые Постановлением Межпарламентской Ассамблеи государств – участников СНГ от 29 ноября 2013 г. № 39-25, указали на необходимость единообразного понимания и законодательного закрепления трактовки такой общетехнической категории, как «компьютерная информация» [5]. Данное понятие нашло отражение в Протоколе о взаимодействии государств – членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере, подписанном в г. Москве 23.12.2014, в Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий, заключенном в г. Душанбе 28.09.2018.

Вопрос о выделении и разграничении терминов «электронная информация» и «цифровая информация» является дискуссионным. В связи с этим данный вопрос должен быть широко рассмотрен в рамках данного раздела.

2. *Криминалистическое исследование аппаратно-программных средств компьютерных систем и сетей*. В данном разделе возможно изучение как стационарных компьютеров, серверов, носителей данных, так и мобильных устройств сотовой связи, смартфонов, планшетных компьютеров и программного обеспечения к ним.

Особенности компьютерных средств и систем послужили причиной того, что в зарубежной практике выделен особый класс цифровых доказательств и описаны методы и приемы работы с ними. Выделяются следующие виды: оригинал цифрового доказательства, его дубликат и копия. Оригинальным цифровым доказательством являются материальные носители и такие информационные объекты, которые связаны с этими носителями на момент изъятия (получения). Дубликатом является точная цифровая репродукция всех информационных объектов, хранящихся на оригинальном материальном носителе, в то время как копия – это точная репродукция информации, содержащейся в информационных объектах, независимая от материального носителя [6].

3. *Криминалистическое исследование сетевых средств компьютерных систем и сетей*. В данном разделе целесообразно рассмотреть локальные и глобальные сети. Отметим, что информационные сети могут выступать не только как техническая среда, где совершаются преступления, но и как инструмент и орудие для совершения преступлений и обеспечения преступной деятельности [7]. В этой связи особенно актуальным является исследование феномена «теневого интернета», или «DARKNET». Именно в этой среде анонимность (рассматриваемая как отрицательный признак сети в целом) позволила развиваться организованной преступности быстрыми темпами. На сегодняшний день международное сообщество в целом и отдельные государства в частности пытаются бороться с распространением преступности в данной среде. Многие виды преступлений (распространение порнографии, наркотических и психотропных средств, торговля людьми и др.) практически полностью переместились в сеть. Однако следует констатировать, что искоренить преступность в сети «DARKNET» не получится, поэтому следует максимально уделять внимание профилактике.

4. *Криминалистическое исследование средств защиты информации*. Данный раздел можно условно разделить на две части. Первая будет посвящена несанкционированному доступу к компьютерной информации как способу совершения преступления. Анализ законодательства свидетельствует о наличии правового режима информации ограниченного доступа (охраняемые законом тайны, персональные данные и т. д.) и порядка регламентации доступа к такого рода информации. Создание единых баз и банков данных во всех сферах, электронный документооборот, распространение персональных данных в сети Интернет привело к полной автоматизации процессов сбора, обработки, хранения информации, доступ к которой ограничен в соответствии с законом. В связи с этим во всем мире участились случаи хакерских атак на автоматизированные системы с целью хищения информации. Общественная опасность таких деяний обусловливается причинением (возможностью причинения) существенного вреда в результате неправомерного обладания данной информацией, включая последующее ее использование (разглашение) [8].

Во второй части данного раздела следует освещать меры обеспечения защиты информации от несанкционированного доступа, включающие технические, программные и организационные. Особое внимание должно быть уделено программным средствам с учетом развития современных технологий, в том числе искусственного интеллекта и нейронных сетей. Примером является переход от дактилоскопической идентификации личности при контроле доступа к распознаванию радужной оболочки глаза и лица в целом.

В последнее время все большее распространение получают криптовалюты, которые представляют собой зашифрованный специальной программой код в распоряжении владельца, который фиксируется и хранится на электронном носителе и принимается как средство платежа другими пользователями и организациями [9]. Поскольку это получает все большее распространение, то в данном разделе необходимо дать основные понятия о криптовалютах и методах их защиты.

5. *Криминалистическое обеспечение выявления и расследования преступлений, в которых облачные технологии выступают как место и средство их совершения*. Особое внимание следует обратить на трансформацию электронных носителей компьютерной информации с течением времени в нашей стране. Еще 30 лет назад хранение информации осуществлялось на магнитных носителях (дискетах, кассетах и т. д.), в конце 90-х годов появились оптические носители (CD, DVD диски), в начале 2000-х появились полупроводниковые носители (флеш-память, объем памяти составлял до 1-2 ГБ), в настоящее время флеш-накопители стали объемом на терабайт. Данная динамика развития показывает насколько быстро меняются подходы к хранению информации и также ее объемы. Следует особо выделить возможность хранения информации в «облаке», т. е. облачные технологии, предоставляющие практически неограниченное пространство для хранения информации, которые в последние годы получают широкое распространение. В настоящее время возникает много вопросов, касающихся обнаружения, изъятия и осмотра информации, находящейся в «облаке».

В своей работе «Об учебной дисциплине «Облачные технологии в правоохранительной деятельности» Козлов В. Е. предлагает ввести дисциплину «Облачные технологии в правоохранительной деятельности» в систему подготовки юристов в Академии МВД. Мы считаем, что можно ограничиться разделом в указанном курсе.

6. *Электронные следы и судебные компьютерно-технические экспертизы*. Существует обоснованное мнение о том, что информацию нельзя удалить из сети полностью, она в любом случае оставит электронный след. В большинстве случаев компьютерная информация оставляет специфические следы: следы переписки, следы проведения транзакции, следы отслеживания активности пользователя и др. В этой связи возможность их обнаружения будет способствовать раскрытию преступлений. На сегодняшний день электронные следы являются объектом различных экспертиз: фототехнической, портретной, фоноскопической и др.

Следует отметить, что в учебной программе «Уголовно-правовая охрана информационной безопасности и электронные доказательства» на кафедре криминалистики БГУ есть упоминание электронных следов в разделе «Особенности проведения следственных действий с электронными доказательствами». Однако считаем целесообразным уделить данной теме больше внимания.

В последние годы для создания доказательственной базы и установления фактических обстоятельств по делам, связанным с расследованием преступлений, совершаемых с использованием компьютерной техники, все больше назначается судебных компьютерно-технических экспертиз (СКТЭ). Отметим, что все больше расширяется аппаратный комплекс СКТЭ в связи с появлением новых технических устройств. В рамках расследования большинства уголовных дел изымается компьютерная техника, мобильные телефоны и другие устройства, в связи с чем сотрудникам правоохранительных органов необходимо иметь определенные знания в технической сфере.

Заключение. В условиях постоянно растущего количества преступлений в сфере высоких технологий возникает потребность в подготовке все большего количества специалистов, хорошо знакомых со спецификой расследования преступлений в данной сфере.

Специалист сегодняшнего дня должен владеть не только знаниями в своей области, но и постоянно совершенствоваться, получая новые навыки. Междисциплинарный подход все больше прослеживается во всех отраслях. При подготовке специалистов в юридической сфере следует больше внимания уделять и техническому аспекту. Необходимо построить систему криминалистических знаний и основанных на них навыков и умений специалистов использовать современные криминалистические и оперативно-технические технологии для предотвращения, выявления, раскрытия и расследования преступлений, совершаемых с использованием средств компьютерной техники.

В данной статье предложено введение в вузах Беларуси, готовящих юристов, специального курса для магистратуры «Криминалистическое компьютероведение» с примерной структурой. Данный курс предназначен для более глубокой подготовки специалистов, которые будут заниматься расследованием преступлений в сфере высоких технологий.

В результате введения данного курса повысится цифровая грамотность, и специалисты смогут применять полученные знания в практической деятельности в правоохранительных органах при противодействии высокотехнологичной преступности.

С течением времени, возможно, станет вопрос о выделении отдельного учения – цифровой криминалистики.

Список литературы

1. СК ожидает увеличение числа киберпреступлений и роста использования преступниками криптовалюты [Электронный ресурс]. – Режим доступа: https://www.belta.by/tech/view/sk-ozhidaet-uvelichenija-chisla-kiberprestuplenij-i-rosta-ispolzovanija-prestupnikami-kriptovaljuty-380252-2020/. - Дата доступа: 02.02.2020.

2. Селятыцкий, Ю. И. Интернет-преступность в молодежной среде [Электронный ресурс] / Ю. И. Селятыцкий. - Режим доступа: https://elib.amia.by/bitstream/docs/734/1/24012018_197.pdf. - Дата доступа: 02.02.2020.
3. Вехов, В. Б. О необходимости разработки криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки [Электронный ресурс] / В. Б. Вехов. - Режим доступа: http://www.crime-research.ru/articles/Wechov/2. - Дата доступа: 02.02.2020.
4. Вехов, В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки. Монография. [Электронный ресурс] / В. Б.Вехов. - Режим доступа: https://studylib.ru/doc/838680/osnovy-kriminalisticheskogo-ucheniya-ob-issledovanii-i. - Дата доступа: 02.02.2020.
5. О Рекомендациях по правовому регулированию эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях [Электронный ресурс]: Пост. Межпарлам. Ассамблеи государств - участников СНГ, 29 нояб. 2013 г., № 39-25 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. - Минск, 2020.
6. Россинская, Е. Р. Новый раздел криминалистики: криминалистическое исследование компьютерных средств и систем [Электронный ресурс] / Е. Р. Россинская, Г. П. Шамаев. - Режим доступа: https://cyberleninka.ru/article/n/novyy-razdel-kriminalistiki-kriminalisticheskoe-issledovanie-kompyuternyh-sredstv-i-sistem/viewer. - Дата доступа: 01.02.2020
7. Бондаренко, Ю. А. Проблемы выявления и использования следов преступлений, оставляемых в сети «DARKNET» [Электронный ресурс] / Ю. А. Бондаренко, Г. М. Кизилов. - Режим доступа: https://cyberleninka.ru/article/n/problemy-vyyavleniya-i-ispolzovaniya-sledov-prestupleniy-ostavlyaemyh-v-seti-darknet/viewer. - Дата доступа: 01.02.2020.
8. Дубко, М. А. Несанкционированное копирование как способ неправомерного завладения компьютерной информацией / М. А. Дубко // Законность и правопорядок. - 2017. - № 4. - С. 58-63.
9. Вахрушев, Д. С. Криптовалюта как феномен современной информационной экономики: проблемы теоретического осмысления [Электронный ресурс] / Д. С. Вахрушев, О. В. Железов. - Режим доступа: https://cyberleninka.ru/article/n/kriptovalyuta-kak-fenomen-sovremennoy-informatsionnoy-ekonomiki-problemy-teoreticheskogo-osmysleniya/viewer. - Дата доступа: 01.02.2020.

References

1. SK ozhidaet uvelichenie chisla kiberprestuplenij i rosta ispol'zovanija prestupnikami kriptovaljuty [The Investigative Committe expects an increase in the number of cybercrimes and an increase in the use of cryptocurrency by criminals]. Available from: https://www.belta.by/tech/view/sk-ozhidaet-uvelichenija-chisla-kiberprestuplenij-i-rosta-ispolzovanija-prestupnikami-kriptovaljuty-380252-2020/. (accessed: 02.02.2020). (Russian).
2. Seljatyckij Ju. I. Internet-prestupnost' v molodezhnoj srede [Internet crime among young people]. Available from: https://elib.amia.by/bitstream/docs/734/1/24012018_197.pdf. (accessed: 02.02.2020). (Russian).
3. Vehov V. B. O neobhodimosti razrabotki kriminalisticheskogo uchenija ob issledovanii i ispol'zovanii komp'juternoj informacii i sredstv ee obrabotki [On the need to develop a forensic doctrine on the study and use of computer information and its processing tools]. Available from: http://www.crime-research.ru/articles/Wechov/2. (accessed: 02.02.2020). (Russian).
4. Vehov V. B. Osnovy kriminalisticheskogo uchenija ob issledovanii i ispol'zovanii komp'juternoj informacii i sredstv ee obrabotki [Fundamentals of forensic science about the study and use of computer information and its processing tools]. Monografija. Available from: https://studylib.ru/doc/838680/osnovy-kriminalisticheskogo-ucheniya-ob-issledovanii-i. (accessed: 02.02.2020). (Russian).
5. O Rekomendacijah po pravovomu regulirovaniju jekspluatacii otkrytyh telekommunikacionnyh setej dlja preduprezhdenija ih ispol'zovanija v terroristicheskih i inyh protivopravnyh celjah [On Recommendations on legal regulation of operation of open telecommunication networks for the prevention of their use for terrorist and other illegal purposes]. *Nacionalnij centr pravovoj informacii Respubliki Belarus'*. Minsk, 2020. (Russian).
6. Rossinskaja E. R., Shamaev G. P. Novyj razdel kriminalistiki: kriminalisticheskoe issledovanie komp'juternyh sredstv i system [New section of criminology: forensic research of computer tools and systems]. Available from: https://cyberleninka.ru/article/n/novyy-razdel-kriminalistiki-kriminalisticheskoe-issledovanie-kompyuternyh-sredstv-i-sistem/viewer. (accessed: 01.02.2020).
7. Bondarenko Ju. A., Kizilov G. M. Problemy vyjavlenija i ispol'zovanija sledov prestuplenij, ostavljaemyh v seti «Darknet» [Problems of detecting and using traces of crimes left in the «Darknet» network]. Available from: https://cyberleninka.ru/article/n/problemy-vyyavleniya-i-ispolzovaniya-sledov-prestupleniy-ostavlyaemyh-v-seti-darknet/viewer. (accessed: 01.02.2020).
8. Dubko M. A. Nesankcionirovannoe kopirovanie kak sposob nepravomernogo zavladenija komp'juternoj informaciej [Unauthorized copying as a method of illegal acquisition of computer information]. Zakonnost' i pravoporjadok. 2017. № 4. P. 58-63. (Russian).
9. Vahrushev D. S., Zhelezov O. V. Kriptovaljuta kak fenomen sovremennoj informacionnoj ekonomiki: problemy teoreticheskogo osmyslenija [Cryptocurrency as a phenomenon of modern information economy: problems of theoretical understanding]. Available from: https://cyberleninka.ru/article/n/kriptovalyuta-kak-fenomen-sovremennoy-informatsionnoy-ekonomiki-problemy-teoreticheskogo-osmysleniya/viewer. (accessed: 01.02.2020).

Abstract. Keywords

The rapid development of information and communication technologies makes the problem of the prevention of Internet crime relevant and relevant. In this regard, it is necessary to train highly qualified specialists to investigate cybercrimes that possess both legal and technical knowledge. This requires improved digital literacy for lawyers. To this end, this article proposes to introduce a special training course for specialists for an in-depth study of the basics of forensics, information law and the basics of computer technology. The place of this course in the educational process is shown.

Keywords: training; forensics; computer technology

Received (дата поступления): 26.02.2020