УДК 343.983, 004

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА И ИСПОЛЬЗОВАНИЯ АППАРАТНО-ПРОГРАММНЫХ КОМПЛЕКСОВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

П.М. Олейник, [1] ***И.В. Ильин,*** [2] ***С.Н. Сухов***[2]

[1]Нижегородский филиал Санкт-Петербургской академии
Следственного комитета России, Н. Новгород
[2]Нижегородская академия Министерства внутренних дел России, Н. Новгород

amlawdd@yandex.ru

Поступила в редакцию 01.10.2019

Описываются проблемные аспекты организации образовательного процесса и формирования компетенций в части использования имеющихся у правоохранительных органов и экспертных организаций аппаратно-программных комплексов, позволяющих извлекать и анализировать данные мобильных устройств. Информация может быть полезна сотрудникам правоохранительных органов, ведомственных образовательных организаций, педагогическим работникам образовательных организаций, осуществляющих подготовку по уголовно-правовым специализациям по специальности «Юриспруденция», а также по экспертным специальностям в сфере компьютерных технологий. Приведены рекомендации по формированию программы повышения квалификации в рассматриваемой сфере.

Ключевые слова: аппаратно-программные комплексы, исследование данных, правоохранительные органы, образование, взаимодействие.

В Стратегии развития отрасли информационных технологий в России [1] отмечается, что одним из важнейших факторов, которые способствуют решению ключевых экономических, социальных задач государственной политики, является развитие информационных технологий. Не могут оставаться в стороне и сотрудники правоохранительных органов. Одним из важных элементов, составляющих успешное выполнение ими своих профессиональных функций и задач, является наличие у них специальных знаний в области компьютерной техники и технологий, современного программного обеспечения.

Развитие информационных технологий, «бесконтактные» способы совершения преступления значительно меняют классическую методику поиска и фиксации следовой картины, что вызывает необходимость готовить квалифицированные кадры. Однако большинство образовательных программ для сотрудников правоохранительных органов сформированы по традиционной схеме подготовки специалистов, а имеющиеся курсы по криминалистике, уголовному процессу, оперативно-розыскной деятельности не адаптированы к реалиям сегодняшнего дня. Современные технологии развиваются так стремительно, что потребность в сотрудниках, имеющих специальные познания, увеличивается с появлением новых видов и способов совершения преступлений. Даже коммерческие структуры, комплектуя штат сотрудников подразделений внутренней безопасности, в качестве предъявляемых требований зачастую выставляют необходимое образование или опыт работы по IT-направлению, например сотрудник службы безопасности должен быть системным администратором.

Техническое обеспечение сотрудников правоохранительных органов также не стоит на месте, и постоянно появляются новые высокотехнологичные комплексы по исследованию компьютерной и телекоммуникационной техники.

Необходимость формирования компьютерной криминалистики как отрасли знаний, умений и навыков, набора компетенций, обеспечивающих деятельность по выявлению информационных преступлений, криминалистическому исследованию электронной доказательственной информации, все активнее обсуждается в трудах видных ученых [2].

Необходимость формирования подобных компетенций подтверждается эмпирическим опытом [3], накопленным авторами статьи в 2014 – 2019 гг. при проведении занятий как со слушателями факультета переподготовки и повышения квалификации Нижегородской академии МВД России, так и слушателями Нижегородского филиала Санкт-Петербургской академии Следственного комитета Российской Федерации[1]. К примеру, при проведении занятий с сотрудниками и руководителями оперативных и следственных подразделений МВД России выявлен крайне низкий уровень знаний о наличии

следов, способах их сохранности и изъятия при обращении с компьютерной и телекоммуникационной техникой, программным обеспечением. Следователи органов внутренних дел крайне слабо ориентируются в вопросах назначения судебной компьютерно-технической экспертизы, которая необходима для всестороннего изучения компьютерных средств и систем с целью получения доказательственной, розыскной и ориентирующей информации по уголовным и гражданским делам, делам об административных правонарушениях. Необходимо понимать, что судебная компьютерно-техническая экспертиза может проводиться в различных организациях и учреждениях, как государственных, так и частных. Для следователя принципиально важно понимать, какой вид экспертизы он будет проводить в каком органе или учреждении, так как специальность эксперта может быть различная. Соответственно и процессуальные документы необходимо готовить с учетом специальности эксперта. К примеру, в учреждениях Минюста России проводится компьютерно-техническая экспертиза по экспертной специальности 21.1 «Исследование информационных компьютерных средств», а в МВД России [4] – компьютерная экспертиза по экспертной специальности 11.1 «Компьютерная экспертиза (исследование компьютерной информации)». В случае неправильного определения вида экспертизы (без учета специальности эксперта, которая может зависеть от места работы последнего) в последующем данная экспертиза может быть оспорена.

В большинстве случаев сотрудники оперативных и следственных подразделений рассчитывают на помощь и наличие специальных знаний экспертов, которых привлекают по имеющимся у них материалам и уголовным делам. Анализ правоприменительной практики показывает, что компьютерная техника может либо выступать в качестве предмета преступного посягательства, либо являться орудием (средством) совершения противоправного деяния, либо выступать хранилищем доказательственной информации. По каждому направлению есть свои специфические особенности при выявлении и документировании следов противоправной деятельности.

Сложность заключается также в том, что специалисты и сотрудники экспертных подразделений как правоохранительных органов, так и иных учреждений, имея профильное образование, должны уметь интерпретировать сложные технические процессы в понятный для понимания другими сотрудниками правоохранительных органов язык.

Еще одной актуальной проблемой является использование удаленного доступа при работе с банком документов или финансовыми базами данных (например, 1С). Сотрудникам правоохранительных органов (следственные, оперативные подразделения) зачастую достаточно сложно разобраться в особенностях сетевой инфраструктуры предприятия, в направлениях оперативной или следственной работы по выявлению, фиксации и изъятию интересующей информации. Сотрудники следственных и оперативных подразделений в данных ситуациях в основном также рассчитывают на помощь привлекаемых специалистов и экспертов, которые имеют специальные знания, позволяющие грамотно организовать первоначальный этап работы и в последующем грамотно использовать имеющиеся аппаратно-программные комплексы и программное обеспечение для проведения исследований и экспертиз.

Современные носители информации, системы хранения данных занимают десятки и сотни гигабайт, исследование подобных массивов информации ручным способом крайне неэффективно и занимает много времени. Современные разработчики предлагают решения различного уровня, которые помогают максимально ускорить и упростить процедуру сбора и фиксации цифровых доказательств.

Эффективным средством исследования мобильных телефонов по-прежнему остается аппаратно-программный комплекс Cellebrite UFED [5], который позволяет правоохранительным органам извлекать важную информацию из мобильных телефонов, смартфонов и планшетов.

Имеется возможность извлекать данные мультимедийного контента (видео, фото, звуковые файлы), телефонной книги, текстовых сообщений, журналы вызовов (входящих, исходящих, пропущенных), включая удаленную, т.е. стертую, историю звонков SIM-карты и другое.

Система не требует стационарного компьютера для работы в полевых условиях и легко может хранить большой объем извлеченной информации на карте SD или на флеш-накопителе USB. Cellebrite UFED поддерживает все известные интерфейсы сотовой связи, включая последовательный и инфракрасный интерфейсы, USB и Bluetooth.

Благодаря системе Cellebrite UFED возможно работать с подавляющим большинством телефонов, которые сегодня представлены на мировом рынке. Программа производства компании Cellebrite совместима с 95% всех моделей мобильных телефонов, использующихся повсеместно, – а это более чем 1700 устройств – и ежемесячно выпускает автоматические обновле-

ния для поддержки новых моделей. Кроме того, поддержка телефонов включает в себя набор из более 72 кабелей данных, обеспечивающий надлежащее соединение с любым телефоном.

Программное решение «Мобильный Криминалист Детектив» компании «Оксиджен Софтвер» [6] представляет собой универсальный программный комплекс для исследования мобильных устройств, извлечения данных из облачных хранилищ и анализа биллингов операторов сотовой связи, обладает внушительным арсеналом возможностей и позволяет:

– извлекать и исследовать данные мобильных устройств. Во многих случаях имеется возможность обхода пароля на блокировку экрана;

– загружать и анализировать резервные копии iOS и Android, находить пароли на зашифрованные паролем резервные копии;

– получать данные из облачных хранилищ по логину/паролю. Например, данные из учетной записи iCloud, Google, Microsoft, переписку с Email-сервера, документы из Dropbox и других облачных сервисов и хранилищ;

– извлекать данные даже из защищенных и зашифрованных приложений: база сообщений WhatsApp, Telegram, Snapchat и т.д.;

– восстанавливать удаленную информацию: любой тип переписки (iMessage, WhatsApp, Skype и т.д.), контакты, звонки, файлы, видео, фото, заметки и многое другое.

Программа «Мобильный Криминалист Детектив» позволяет исследовать взаимодействие между несколькими устройствами и их владельцами. С помощью этой функции строится диаграмма прямых связей для двух и более устройств, наглядно и понятно визуализируя факты общения между их пользователями.

Программное решение Belkasoft Evidence Center [7] облегчает получение, поиск, анализ, хранение и передачу цифровых улик, находящихся внутри компьютеров и мобильных устройств. Программа быстро извлечёт цифровые улики из различных источников путем анализа жёстких дисков, образов, облачных приложений, содержимого рабочей памяти, резервных копий iOS, Blackberry и Android, UFED, JTAG и chip-off дампов. Evidence Center автоматически проанализирует источник данных и представит наиболее значительные улики для обзора, подробного изучения или включения в отчёт.

Данные аппаратные и программные решения, а также другие комплексы имеются в большинстве экспертных подразделений правоохранительных органов. Эксперты имеют опыт и навыки работы с ними, однако сотрудники следственных и оперативных подразделений либо не знакомы с функциональными возможностями подобных комплексов, либо вообще не имеют представления, что используют экспертные подразделения в своей деятельности, в связи с чем образуется значительный пробел во взаимодействии, в корректной формулировке вопросов для исследований и экспертиз, полноте запрашиваемой информации. Поэтому крайне актуальной становится задача формирования на базе образовательных организаций правоохранительных органов курсов повышения квалификации и переподготовки сотрудников оперативных и следственных подразделений, на которые в обязательном порядке необходимо приглашать сотрудников экспертных подразделений. Накопленный в Нижегородской академии МВД России опыт реализации дополнительных образовательных программ с сотрудниками следственных и оперативных подразделений (за период 2014–2019 гг. обучено более тысячи сотрудников) позволяет сформировать следующие рекомендации по программе повышения квалификации:

– объем программы повышения квалификации: 72 часа;

– распределение времени осуществлялось по следующей схеме: одна треть учебного времени отводится на лекционные занятия по современной цифровой криминалистике и имеющимся аппаратно-программным комплексам; две трети учебного времени отводятся на практические занятия в специализированных компьютерных классах, в которых развернуты демонстрационные версии описанных в статье аппаратно-программных комплексов;

– особенность формирования учебных групп заключалась в том, что в состав одной группы входили сотрудники оперативных, следственных и экспертных подразделений, которые работают по одному профилю, в связи с чем большинство проблемных моментов по осуществлению взаимодействия разбирались на проводимых занятиях;

– при проведении практических занятий по работе с аппаратно-программными комплексами преобладали методы «проблемного обучения», основанные на реальных ситуациях в деятельности практических органов.

Подводя итог, в дополнение к выводу о необходимости регулярного повышения квалификации сотрудников правоохранительных органов, хочется сделать ряд предложений, направленных на увеличение эффективности использования аппаратно-программных комплексов по извлечению и исследованию данных мобильных устройств, а также устранение проблемных моментов взаимодействия экспертных, следственных и оперативных подразделений правоохранительных органов:

– необходимо оснащать образовательные организации правоохранительных органов учеб-

ными стендами, демонстрирующими возможности современных решений в области цифровой криминалистики (в формате учебных полигонов или профильных лабораторий);

– необходимо стандартизировать подготовку квалифицированных кадров для работы с цифровой информацией.

Реализация подобных предложений позволит эффективнее противодействовать современным вызовам, повысит качество оперативно-розыскной, уголовно-процессуальной и экспертной деятельности.

Примечание

1. Нижегородский филиал ФГКОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации» создан в декабре 2018 года на базе Четвертого факультета Института повышения квалификации (с дислокацией в городе Нижний Новгород) ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации».

Список литературы

1. Распоряжение Правительства РФ от 01.11.2013 № 2036-р (ред. от 18.10.2018) «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года» // Официальный интернет-портал правовой информации. URL: www.pravo.gov.ru (дата обращения: 08.11.2013).

2. Пастухов П.С. О необходимости развития компьютерной криминалистики / Под ред. О.А. Кузнецовой, В.Г. Голубцова, Г.Я. Борисевич и др. // Пермский юридический альманах. Ежегодный научный журнал. 2018. № 1. С. 479–488.

3. Сухов С.Н., Крыгин С.В. Особенности подготовки слушателей факультета переподготовки и повышения квалификации в сфере информационно-коммуникационных технологий // Передовой опыт и проблемы профилизации учебной, учебно-методической и научно-исследовательской деятельности в образовательных организациях системы МВД России: Доклады Всероссийской научно-практической конференции (Н. Новгород, 15–16 ноября 2017 г.). Н. Новгород, 2018. С. 48–51.

4. Приказ МВД России от 29.06.2005 № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» (Зарегистрирован в Минюсте России от 23.08.2005 № 6931) (ред. 11.10.2018) // Российская газета. 30.08.2005. № 191.

5. Официальный сайт Cellebrite. URL: www.cellebrite.com/en/home (дата обращения: 02.09.2019).

6. Официальный сайт «Мобильный Криминалист» URL: www.oxygensoftware.ru (дата обращения: 02.09.2019).

7. Официальный сайт Belkasoft. URL: www.belkasoft.com/ru/ (дата обращения: 02.09.2019).

CURRENT PROBLEMS OF THE EDUCATIONAL PROCESS AND THE USE OF HARDWARE AND SOFTWARE IN LAW ENFORCEMENT

P.M. Oleynik, I.V. Ilyin, S.N. Sukhov

The article describes some problematic aspects in the organization of the educational process and the development of competencies in relation to the use by law enforcement agencies and expert organizations of hardware and software systems for extracting and analyzing data from mobile devices. The information can be useful to law enforcement officers, educational organizations, teachers of educational organizations that provide training in criminal law specialties in the field of jurisprudence, as well as in expert specialties in the field of computer technology. Some recommendations on the development of advanced training programs in this area are given.

Keywords: hardware and software systems, data research, law enforcement agencies, education, interaction.

References

1. Rasporyazhenie Pravitel'stva RF ot 01.11.2013 № 2036-r (red. ot 18.10.2018) «Ob utverzhdenii Strategii razvitiya otrasli informacionnyh tekhnologij v Rossijskoj Federacii na 2014–2020 gody i na perspektivu do 2025 goda» // Oficial'nyj internet-portal pravovoj informacii. URL: www. pravo.gov.ru (data obrashcheniya: 08.11.2013).

2. Pastuhov P.S. O neobhodimosti razvitiya komp'yuternoj kriminalistiki / Pod red. O.A. Kuznecovoj, V.G. Golubcova, G.Ya. Borisevich i dr. // Permskij yuridicheskij al'manah. Ezhegodnyj nauchnyj zhurnal. 2018. № 1. S. 479–488.

3. Suhov S.N., Krygin S.V. Osobennosti podgotovki slushatelej fakul'teta perepodgotovki i povysheniya kvalifikacii v sfere informacionno-kommunikacionnyh tekhnologij // Peredovoj opyt i problemy profilizacii uchebnoj, uchebno-metodicheskoj i nauchno-issledovatel'skoj deyatel'nosti v obrazovatel'nyh organizaciyah sistemy MVD Rossii: Doklady Vserossijskoj nauchno-prakticheskoj konferencii (N. Novgorod, 15–16 noyabrya 2017 g.). N. Novgorod, 2018. S. 48–51.

4. Prikaz MVD Rossii ot 29.06.2005 № 511 «Voprosy organizacii proizvodstva sudebnyh ekspertiz v ekspertno-kriminalisticheskih podrazdeleniyah organov vnutrennih del Rossijskoj Federacii» (Zaregistrirovan v Minyuste Rossii ot 23.08.2005 № 6931) (red. 11.10.2018) // Rossijskaya gazeta. 30.08.2005. № 191.

5. Oficial'nyj sajt Cellebrite. URL: www.cellebrite.com/en/home (data obrashcheniya: 02.09.2019).

6. Oficial'nyj sajt «Mobil'nyj Kriminalist» URL: www.oxygensoftware.ru (data obrashcheniya: 02.09.2019).

7. Oficial'nyj sajt Belkasoft. URL: www.belkasoft.com/ru/ (data obrashcheniya: 02.09.2019).