

УДК 34

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО СБОРУ ЦИФРОВЫХ ДАННЫХ КАК УЛИК ДЛЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Го Цзин, Хэйлуницзянский институт профессиональной подготовки офицеров общественной безопасности, факультет информационной и сетевой безопасности

Вслед за непрерывным развитием интернет технологий, интернет стал оказывать влияние на социально-экономическое развитие и образ жизни людей. В частности, распространение применения смартфонов привело к повышению числа сетевых преступлений, таких как: телекоммуникационное мошенничество, трансляция порнографии, азартные онлайн игры. Вопрос регулирования сетевого сообщества стал наиболее насущным. Традиционные преступления стремительно переходят в категорию бесконтактных, увеличивается число преступлений, совершаемых через сеть, повышается масштабы потерпевших и социальный вред. Интернет пространство стало полем битвы с преступностью. Образовательные учреждения общественной безопасности, являясь базой подготовки специалистов кибербезопасности и специалистов правоохранительных органов, должны идти в ногу со временем, разработать стратегию подготовки кадров для ведения расследования в сети интернет и сбора цифровых данных, для того, чтобы легко адаптироваться к эпохе «Интернет +» и стать выдающимися сотрудниками органов общественной безопасности.

Ключевые слова: сбор цифровых данных в качестве доказательств, подготовка кадров, киберпреступление

1. Важность подготовки специалистов по сбору цифровых данных в качестве доказательств. [1,2]

Вслед за непрерывным развитием интернет технологий, интернет стал оказывать влияние на социально-экономическое развитие и образ жизни людей. В частности, распространение применения смартфонов привело к повышению числа сетевых преступлений, таких как: телекоммуникационное мошенничество, трансляция порнографии, азартные онлайн игры. Вопрос регулирования сетевого сообщества стал наиболее насущным. На примере 2020 года мы видим, что всемирная эпидемия оказала серьезное влияние на образ жизни, работу и различные виды экономической деятельности людей. В 2020 году большинство предприятий

перешли на дистанционную работу на дому для того, чтобы максимально контролировать распространение эпидемии и уменьшить необходимость выходить из дома для людей. Уровень преступности в большей степени понизился, но что касается телекоммуникационного мошенничества и распространения информации, то тут наблюдается тенденция к быстрому увеличению. Люди постоянно находились дома, работали по удаленной системе через сеть, помимо этого, общение с друзьями, развлечения и прочие виды жизнедеятельности перешли в интернет пространство, что также предоставило возможности для преступников совершать противоправные действия. Так в прошлом году ущерб от преступных действий, связанных с телекоммуникационным мошенничеством, достиг 353,7 миллиарда. Большинство мошеннических притонов переместилось за границу. Незаконные операции с сим картами, банковскими картами стали безудержными. В судебной практике также появилось множество проблем, преступность бросила новый вызов борьбе с таким видом противоправных действий, стали выдвигаться более высокие требования к органам общественной безопасности. [3,4] Традиционные виды преступлений стремительно перешли в область бесконтактных преступлений, совершаемые через сеть интернет. Бесперывно повышается количество киберпреступлений, растет масштаб потерпевших и наносимый социальный вред. Интернет пространство стало полем борьбы с преступностью. Согласно исследований, в настоящее время более 40 % уголовных преступлений и более 60 % экономических споров связаны со сбором, анализом и исследованием электронных данных в качестве доказательств. Все больше и больше интеллектуальных устройств, беспилотных транспортных средств, приложений для мобильных телефонов, услуг интернет + тесно связаны с бизнесом, который ведется офлайн. Поэтому, технологии извлечения и анализа электронных данных в качестве улики станут центром развития отрасли еще на длительный период времени. Извлечение электронных данных – это междисциплинарная технология, которая охватывает широкую сферу и имеет прочную основу. Многие эксперты и ученые практиковали подготовку специалистов в этой области, и многие добились ярких результатов. [5,6]. Образовательные учреждения общественной безопасности, являясь базой подготовки специалистов кибербезопасности и правоохранительной деятельности, должны идти в ногу со временем, разрабатывать стратегию подготовки специалистов по сбору электронных данных в качестве доказательств в эпоху «Интернет +», готовить выдающиеся кадры для органов общественной безопасности.

На государственном уровне уже выделяется особое внимание вопросам киберпреступности и электронным данным. 4 февраля 2015 года, Верховный суд КНР опубликовал «Судебное толкование применения «Гражданско-процессуального кодекса КНР»», в котором дополнительно разъясняется форма электронных доказательств. В сентябре 2016 года, Верховный народный суд,

Верховная народная прокуратура и Министерство общественной безопасности обнародовали «Положение о некоторых вопросах, касающихся сбора, извлечения, проверки и вынесения решения по электронным данным в уголовных делах». В ноябре 2016 года был обнародован «Закон КНР о сетевой безопасности», 22 июня 2021 года, Верховный народный суд, Верховная народная прокуратура и Министерство общественной безопасности опубликовали «Заключения по некоторым вопросам, касающимся применения закона при рассмотрении уголовных дел, касающихся мошенничества и других уголовных дел (2)». Таким образом, были даны уточнения правовых стандартов для того, чтобы в соответствии с законом строго наказывать и пресекать телекоммуникационное мошенничество и связанные с ним преступления. В ответ на новые нерешенные вопросы в судебной практике, таких как подсудность в делах о телекоммуникационном мошенничестве и связанных с ним делах, вопросы сбора доказательств по уголовным делам, связанным с трансграничным телекоммуникационным мошенничеством и рассмотрения уголовных дел, связанных с использованием сим карты мобильного телефона и кредитных карт, так называемые дела «двух карт», были предусмотрены положения применения стратегий при рассмотрении вышеперечисленных уголовных дел. Все вышеперечисленные законы и судебные толкования содержат руководящие принципы извлечения и анализа электронных доказательств.

2. Методы подготовки специалистов правоохранительной области по извлечению электронных доказательств.

Хэйлуңцзянский институт профессиональной подготовки офицеров общественной безопасности на протяжении всего времени формирует особую учебную среду, характерную для образовательного учреждения общественной безопасности, а именно: занимается подготовкой полицейских кадров, соответствующих новым требованиям работы по обеспечению общественной безопасности, посредством приближения содержания обучения реалиям практической работы органов общественной безопасности придерживается направления приближения к практике, стремится к объединению учебного процесса и реальной деятельности по обеспечению общественной безопасности, всесторонне проводит полноценное и всестороннее образование, осуществляет объединение официального стандартного образования и обучения сотрудников, находящихся на службе, одновременно проводит обычное обучение и обучение взрослых людей, объединяет обучение, научные исследования и практику.

(1) Непрерывное изучение новых технологий

Цифровые технологии непрерывно развиваются, одно за другим возникают новые электронные продукты и виды преступлений. Специалистам по сбору электронных данных в качестве улик постоянно нужно следить за развитием технологий и изучать ситуацию на рынке. Хэйлуңцзянский институт профессиональной подготовки офицеров общественной безопасности является известным

образовательным заведением системы общественной безопасности в нашей стране, на базе которого имеется специальность информационной и сетевой безопасности, являясь базой подготовки кадров полицейских общественной безопасности провинции, выполняет задачи по оказанию технической поддержки и обеспечения информационной и сетевой безопасности. Для того, чтобы способствовать развитию технологий извлечения и исследования электронных данных, продвигать применение технологий для обеспечения общественной безопасности, повысить уровень квалификации всех сотрудников, наш институт нашел передовых производителей специального оборудования для сбора электронных данных, а также и учреждения, обладающие государственной аккредитацией в области судебной аутентификации, научно-исследовательские учреждения с обширным техническим накоплением, а также известных экспертов и ученых, непрерывно проводит курсы повышения квалификации для преподавателей и курсантов. Все эти эксперты и ученые постоянно работают в сфере извлечения электронных данных и уже накопили богатый опыт в области организации лабораторий по информационной безопасности и извлечению улик, технических исследований, подготовке профессиональных кадров и развитию отрасли в целом, сформировали стабильные и долгосрочные отношения сотрудничества с государственными органами, такими как органы общественной безопасности, прокуратурой и юридическими агентствами, а также с многими известными отечественными предприятиями и научно-исследовательскими институтами. Повышение квалификации проходит посредством приглашения специалистов этих структур для преподавания в нашем институте и командирования курсантов и преподавателей на прохождение обучения. Таким образом, обе стороны имеют очевидные успехи в своих областях и обширное поле для сотрудничества. Для того, чтобы добиться еще больших результатов, соответствовать новым требованиям в области борьбы с киберпреступностью, преподаватели факультета сетевой и информационной безопасности постоянно обращаются с передовыми технологиями по сбору электронных данных практических органов общественной безопасности и достигают отличных результатов.

(2) Создание линии обучения технологиям

Необходимо учитывать рабочий график сотрудников правоохранительных органов, которые специализируются на борьбе с киберпреступностью и команд, которые занимаются извлечением и анализом электронных данных и в соответствии с этим составлять учебный план. Каждый преподаватель факультета информационной и сетевой безопасности должен строго следовать плану обучения и своевременно восполнять пробелы в своих технических знаниях, повышать уровень и обмениваться знаниями. При построении содержания урока по извлечению и исследованию электронных данных необходимо следовать тенденциям развития электронных технологий, учитывать имеющиеся оборудование

в лабораториях по расследованию киберпреступлений факультета информационной и сетевой безопасности и возможности, для того, чтобы целенаправленно организовывать процесс обучения в области извлечения электронных данных и судебной экспертизы для курсантов нашего факультета. Учебная программа формируется, основываясь на базовых исследованиях, практическом опыте рядовых практических работников органов общественной безопасности по сбору электронных данных, судмедэкспертов и производителей оборудования. Учебная программа формируется от простого к сложному, управление и организация может организовывать как параллельно нескольких уровней так и в одиночном порядке, содержание обучения должны формироваться от теории к практике и обозначается метками разных цветов: «серый», «желтый», «зеленый», «красный». При этом необходимо фиксировать уровень обучения курсантов для своевременной корректировки учебной программы и содержания обучения.

(3) Проведение обменов опытом и знаниями специалистами

Необходимо чтобы как можно большее число курсантов и офицеров, проходящих курсы повышения квалификации посещали как можно больше мероприятий таких как: «Лекции по технологиям обеспечению общественной безопасности», «Конференция экспертов», «Анализ классических случаев», «Изучение и разбор стенограмм расследований, фиксированных записей полученных доказательств, отчетов о передаче доказательств, отчетов судебно-медицинской экспертизы», «Интерпретация стандартов общественной безопасности и судебной экспертизы», «Введение в разработку существующих технологий и оборудования». Если отсутствует возможность отправлять студентов на участие в этих мероприятиях, можно использовать видеоматериалы и презентации.

В каждом разделе обучения разбирается один случай киберпреступности, исследуются как технические так и юридические аспекты, интерпретируются криминальные и некриминальные границы киберпреступления в каждом случае отдельно и предлагаются меры по наиболее эффективному предотвращению за соблюдению преступности и контролю за соблюдением уголовного законодательства.

Возможно приглашение к участию в мероприятиях судей, прокуроров, экспертов общественной безопасности, специалистов по сетевой безопасности различных предприятий, ученых, судебных экспертов, юристов, которые проводили практические и теоретические исследования по вопросам киберпреступности.

Необходимо всеми силами достигать наибольшего количества участников (включая полицейских сетевой безопасности, нуждающихся в повышении уровня квалификации, сотрудников дорожной полиции, уголовных следователей и гражданских следователей, нуждающихся в расширении операционных знаний), например проводить мероприятия онлайн по каналам Tencent. Для того, чтобы обеспечить защиту от утечки информации необходимо принять

необходимые меры, ограничить доступ незарегистрированных пользователей и допускать только реально зарегистрированных пользователей. При передаче данных и материалов необходимо удостовериться об утвержденном списке участников. Участники из Хэйлунцзянского института профессиональной подготовки офицеров полиции общественной безопасности могут загружаться через BBS специальности информационной и сетевой безопасности, остальные студенты могут сделать запрос в наш институт. После подтверждения количества и состава всех участников вся информация может быть передана.

Криминалистический анализ электронных данных – это комплексная дисциплина, сочетающая в себе информатику, право, криминалистику и т. д. От практикующих специалистов требуется не только отличные знания ПК и технологий, необходимо обладать юридической грамотностью, иметь пылливый ум для расследования и иметь обширные знания по сетевым приложениям. Наш институт уделяет огромное внимание подготовке высококвалифицированных практических специалистов общественной безопасности, обозначив как центр обучения – формирование профессионального духа, базовых навыков и способностей и профессиональных качеств, а направление – приближение к практике и реальной деятельности, достиг очевидных результатов и успеха в вопросах организации обучения и практики, разработал новые механизмы и модели для обучения сотрудников полиции, находящихся на службе и обозначил новый путь для развития образовательных учреждений общественной безопасности.

Список источников

1. Дин Липин. Размышления о развитии талантов в области судебной экспертизы электронных данных. Информационная безопасность Китая, выпуск 5, 2019 г.
2. Ян Итао, Юань Аньсинь. Мои мнения о развитии особых талантов в области судебной экспертизы электронных данных, информационной безопасности и конфиденциальности связи, выпуск 5, 2014 г.
3. Сунь Сяодун. Развитие исследовательского сознания в ходе преподавания курса «Электронная криминалистика данных», Журнал полицейского колледжа Ляонин, выпуск 4, 2020 г.
4. Ту Минь, Чжан Лян. Междисциплинарное исследование курса "Электронная криминалистика данных", 5-й национальный семинар по технологиям компьютерной криминалистике.
5. Го Цзин. Говоря о том, как обучать высококачественных специалистов по кибербезопасности правоохранительных органов в учебных заведениях общественной безопасности в новых условиях, 3-й Национальный колледж общественной безопасности Форум профессиональных руководителей по кибербезопасности и правоохранительной деятельности, 2017 г.
6. Го Цзин. Говоря о том, как в полной мере использовать роль компьютерной сети общественной безопасности, Информация и компьютер, 2015, 20

论执法机关电子数据取证人员的培养

郭静

黑龙江公安警官职业学院公安信息化与网络安全系

摘要：随着互联网技术的不断发展，互联网已经深入的影响了社会经济发展和人们的生活方式。尤其是智能手机的迅速普及，以电信诈骗、色情直播、网络赌博等为代表的网络犯罪逐年提升，网络社会综合治理问题愈发凸显。传统犯罪加速向以互联网为媒介的非接触性犯罪转移，涉网犯罪数量、受害人规模和社会危害持续激增，互联网成为打击违法犯罪的主战场。公安院校作为培养网络安全与执法专业人才的重要基地，更是要紧跟时代构建适应“互联网+”时代特点的电子数据调查取证人才培养策略，为公安机关培养输送优秀的专业人才。

关键词：电子数据取证 人才培养 网络犯罪

一、电子数据取证执法人员培养的重要性

随着互联网技术的不断发展，互联网已经深入的影响了社会经济发展和人们的生活方式[1, 2]。尤其是智能手机的迅速普及，以电信诈骗、色情直播、网络赌博等为代表的网络犯罪逐年提升，网络社会综合治理问题愈发凸显。以2020年为例，全球受疫情影响，人们的生活、工作以及各种经济活动都受到了严重影响。我国在2020上半年的部分时间也采取了居家办公、尽量减少人员外出的疫情管控。犯罪活动也大幅度降低，只有电信诈骗、网络传销迅速增长。人们居家不见面，依靠网络来工作、休闲、交友等生活方式，为网络犯罪提供了可乘之机。仅去年，全国电信网络诈骗案件涉及财产损失即达353.7亿元。大批诈骗窝点向境外转移，非法交易手机卡、信用卡愈加猖獗，司法实践中亦出现了许多新的问题，打击此类犯罪面临更严峻的挑战和更高的要求。传统犯罪加速向以互联网为媒介的非接触性犯罪转移，涉网犯罪数量、受害人规模和社会危害持续激增，互联网成为打击违法犯罪的主战场[3, 4]。据调查，目前有超过四成的刑事犯罪、超过六成的经济纠纷涉及到电子数据的取证、分析、调查等情况。越来越多智能设备、无人驾驶车辆、手机APP应用、互联网+服务与线下商业活动的紧密对接，使得电子数据取证和分析技术在今后相当长的一段时间内都会成为行业发展热点方向。电子数据取证是一种涉及领域宽、范围广、基础性强的跨学科技术，很多专家学者对于本专业人才的培养都做出过实践，其中不乏闪光点[5, 6]。公安院校作为培养网络安全与执法专业人才的重要基地，更是要紧跟时代构建适应“互联网+”时代特点的电子数据取证执法人才培养策略，为公安机关培养输送优秀的专业人才。

国家层面对于涉及网络犯罪、电子数据早已经有了更多的关注。2015年2月4日，最高人民法院颁布《关于适用《中华人民共和国民事诉讼法》的司法解释》，其中对电子证据的形式作了进一步明确；2016年9月，最高人民法院、最高人民检察院、公安部颁布《关于办理刑事案件

收集提取和审查判断电子数据若干问题的规定》；2016年11月，《中华人民共和国网络安全法》颁布；2021年6月22日，最高人民法院、最高人民检察院、公安部发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》，进一步明确法律标准，依法严厉惩治、打击电信网络诈骗及其关联犯罪。针对司法实践中存在的新的突出问题，如电信网络诈骗犯罪案件及关联犯罪案件的管辖，跨境电信网络诈骗犯罪案件的取证，涉手机卡、信用卡即所谓“两卡”犯罪案件的处理，办理电信网络诈骗犯罪案件的政策适用等问题进行了规定。所有这些法律及司法解释，为电子数据的取证、分析等业务提供了指引和遵循标准。

二、电子数据取证执法人员培养的方法

黑龙江公安警官职业学院始终坚持以培养适应新形势下公安工作的合格人民警察为中心，以警务实战需求为导向，教学内容贴近、服务于公安工作实践，实现教育教学工作与公安实际工作的融合与对接，全面实施素质教育，形成了学历教育与在职培训并重，普通教育与成人教育同步，教学、科研、实战一体化，具有鲜明公安特色的办学格局。

（一）紧跟技术发展不断学习

电子技术发展迅速，各种电子产品和犯罪形式层出不穷。电子数据取证执法人员需要紧跟技术发展、关注市场应用情况不断学习。黑龙江公安警官职业学院是国内的知名公安院校，拥有信息安全监察专业，是全省公安机关警察的培训基地，承担着全省网络技术专业支持的重要职责。为了促进电子数据调查取证技术发展，实现技术在公安行业的落地应用和工作促进，提升全员技能水平，我院寻找国内一线的电子数据调查取证设备生产厂商、有国家级司法鉴定资质的机构，有雄厚技术积累的科研院校及知名专家学者，不断的为我院教师及学员开展专题培训。这些专家学者一直工作在电子数据调查取证一线，在信息安全与取证领域的实验室建设、技术研究、专业人才培养、业务开展等方面积累了丰富的经验，并与公检法等政府机构、国内多家主流知名企业和科研院所形成了稳定长期的合作关系。具体的培训方式是由这些机构派遣人员到我院授课，我院也派遣教师、学员到对方学习等方式。双方均在各自专业领域中具有明显优势，具备较大的合作空间。为了获得更好的效果，适应新形势下打击网络犯罪的要求，学院公安信息化与网络系的教师经常与一线实战部门的电子数据取证技术骨干进行交流，并从育人成效上看取得了良好的效果。

（二）制定技术学习路线

对于专门从事网络犯罪案件打击的执法人员，对于电子数据取证、分析的专业团队，需要考量其工作特点，制定专属的学习计划。我院公安信息化与网络安全系的每个教师都根据自己的技术特长和不足，严格按照预先制定的技术学习路线全面推进，互相学习，取长补短。电子数据取证与分析课程的内容设置充分考虑到电子数据取证技术的前沿应用

需求和研究方向，依据公安信息化与网络安全系网络案件侦查实验室现有的设备条件和师资力量，有针对性的对我系的学生进行实验室建设、电子数据取证司法鉴定等方面的培养。培养方案经过了基层调研，根据一线工作实际，收录了基层电子数据取证实战公安人员、法鉴人员和设备生产厂商的想法，完成相关课程培养方案的设置。课程设置从简单到复杂、流程管理从单一到并发、学习思路从理论到实战，分别用“灰色”、“黄色”、“绿色”“红色”这些颜色标记出来。同时记录每位学员的掌握进度，便于授课计划和教学内容的调整。

（三）开展专家团队的经验总结与知识分享会

尽量创造机会，让更多的学生和进修学员参加“公安技术讲堂”“英模报告会”“破案思路”“典型案例及行为分析”“调查笔录、证据固定记录、移交报告、司法鉴定报告学习及品读”“公安、司法鉴定标准解读”“现有技术及设备发展介绍”等活动。如果不能大批量的派遣学生到现场，也可以使用视频、PPT等方式进行。

每一期选取一个网络犯罪方面的话题，以案例分析作为切入点，从技术和法律两个方面，解读每个业务场景下网络犯罪的罪与非罪界限，最后给予刑事合规防控提出相应建议。邀请网络犯罪领域有实务和理论研究的法官、检察官、公安、互联网企业网络安全部专家、学者、司法鉴定专家、律师共同参与活动。

为了尽量的让更多的学员（也包括有经验提升需求的网安民警、有业务知识拓展需求的经侦、刑侦或者交警）参与进来，可以在组织形式上主要通过线上的方式开展活动，例如：腾讯会议直播平台开展。为了保护调查取证专业技术不外泄，应做好必须的防护手段，与会者须实名制，并且没有录制视频权限。在资料的传播上，要根据实际情况与主讲嘉宾内容确认后，形成最终的文档，在校学员能以实名信息通过“黑龙江公安警官职业学院-信息网络安全监察专业BBS”下载，其他学员可以向我院申请，审批完成后所有的资料应在公安内部网络发送。

电子数据取证分析是计算机科学、法学、侦查学等专业知识相结合的综合学科，不仅要求从业人员掌握过硬的计算机技术，还要有侦查学的思维，法律相关素养，更要有丰富的网络应用经验。我院紧紧围绕培养应用型、复合型高素质公安专门人才的目标要求，以职业精神、基本技能和专业能力教育为核心，坚持贴近实际、贴近实战的教学导向，在组织管理、教育训练、实践教学等方面都取得了明显成效，创新了公安后备人才和在职警察培养的新机制、新模式，为公安院校今后发展探索了新的道路。

参考文献：

1. 丁丽萍. 电子数据取证人才培养的思考. 中国信息安全, 2019年5期
2. 杨一涛, 袁安心. 电子数据取证特色人才培养之我见, 信息安全与通信保密, 2014年5期

3. 孙晓冬. 电子数据取证”课程教学中侦查意识的培养, 辽宁警察学院学报, 2020年4期
4. 涂敏, 张亮. 跨学科的《电子数据取证》课程研究, 第五届全国计算机取证技术研讨会
5. 郭静. 浅谈新形势下公安院校如何培养高素质网络安全与执法专业公安人才, 2017第三届全国公安院校网络安全与执法专业主任论坛
6. 郭静. 浅谈如何充分发挥公安计算机网络的作用, 信息与电脑, 2015年20期

УДК 343.98

УЧАСТИЕ ПРЕДСТАВИТЕЛЕЙ ОБЩЕСТВЕННОСТИ ПРИ ПРОВЕДЕНИИ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ ПРОВЕРОЧНАЯ ЗАКУПКА

*Д. С. Гольченко, адъюнкт Барнаульского юридического института
МВД России, майор полиции*

Статья посвящена анализу некоторых актуальных проблем привлечения «представителей общественности» к участию в оперативно-розыском мероприятии «Проверочная закупка». Автор приходит к выводу о том, что решение об участии таких лиц должно приниматься на усмотрение оперативных сотрудников в каждом конкретном случае.

Ключевые слова: понятие; незаинтересованные лица; представители общественности; оперативно-розыскное мероприятие; проверочная закупка; оперативно-розыскная деятельность.

PARTICIPATION OF MEMBERS OF THE PUBLIC DURING THE OPERATIONAL SEARCH EVENT A TEST PURCHASE

*D. S. Golchenko, postgraduate student of the Barnaul Law Institute
of the Ministry of Internal Affairs of Russia, police Major*

The article is devoted to the analysis of some actual problems of attracting «representatives of the public» to participate in the operational search event «Verification purchase». The author comes to the conclusion that the decision on the participation of such persons should be made at the discretion of the operational staff in each specific case.

Keywords: witnesses; disinterested persons; members of the public; operational search action; test purchase; operational search activity.