Министерство образования и науки Российской Федерации
Байкальский государственный университет экономики и права

АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ РАЗВИТИЯ ЮРИДИЧЕСКОГО ОБРАЗОВАНИЯ: ПРОБЛЕМЫ, ТЕНДЕНЦИИ, ПЕРСПЕКТИВЫ

Сборник статей и эссе студентов

Иркутск
Издательство БГУЭП
2015

УДК 378:34(06)
ББК 74.58
А43

Печатается по решению редакционно-издательского совета
Байкальского государственного университета экономики и права

Издается при финансовой поддержке проекта «Пределы ограничения прав личности в уголовном судопроизводстве в целях обеспечения национальной безопасности государства: уголовно-процессуальный и криминалистический анализ», реализуемого в рамках проектной части государственного задания Минобрнауки РФ в 2014–2016 гг. в сфере научной деятельности (номер задания 29.1247.2014/К).

А43 Актуальные вопросы теории и практики развития юридического образования: проблемы, тенденции, перспективы : сб. ст. и эссе студентов / отв. ред. И.Г. Смирнова, Л.А. Тетерина, Е.М. Якимова. – Иркутск : Изд-во БГУЭП, 2015. – 188 с.

ISBN 978-5-7253-2844-8

Сборник содержит статьи, отражающие результаты научно-практической деятельности студентов, проходивших в 2014/15 учебном году обучение в юридической клинике Байкальского государственного университета экономики и права, а также научные эссе, представленные на международный конкурс работ «Проблемы борьбы с киберпреступностью».

Для практических работников, преподавателей, аспирантов, магистрантов и студентов юридических вузов и факультетов.

УДК 378:34(06)
ББК 74.58

ISBN 978-5-7253-2844-8

СОДЕРЖАНИЕ

Защита прав граждан как одно из направлений деятельности юридических клиник

Проблемы борьбы с киберпреступностью: научные эссе, представленные на международный конкурс студенческих научных работ

УДК 347

А.Г. Агаева

ДОГОВОР ДАРЕНИЯ И ПРАВОВЫЕ ПОСЛЕДСТВИЯ ЕГО ЗАКЛЮЧЕНИЯ

В статье уделяется внимание порядку заключения договора дарения на земельный участок.

Ключевые слова: договор дарения, земельный участок, кадастровый паспорт, государственная пошлина.

A.G. Agaeva

DEED OF GIFT AND LEGAL CONSEQUENCES

The article includes information about the order conclusion deed of gift to the land lot.

Keywords: deed of gift, land lot, cadastral passport, state tax.

За время моей деятельности в юридической клинике ко мне обратилось немало людей. Их дела были связаны со многими отраслями права-гражданское, семейное, жилищное и другие. Но наиболее интересным из моих дел я считаю дело, которое касается института дарения.

Одним из институтов гражданского права является институт дарения. Институт дарения относится к числу древнейших не только в России, но и во всей мировой цивилизации. Издревле люди дарили друг другу подарки и, тем самым, оказывали свое уважение, дружеское отношение (а порой и любовь) к одаряемому лицу. Дарение – достаточно распространенная сделка, которая чаще всего заключается между близкими родственниками. Как правильно составить соответствующий договор, чтобы избежать проблем в будущем?

В связи с этим я рассмотрю свое дело, с которым ко мне обратились в юридическую клинику. В 2001 году родители моей клиентки бесплатно приватизировали земельный участок на дочь, то есть на мою клиентку. В то время моя клиентка уже состояла в браке. В настоящее время моя клиентка хочет оформить договор дарения на своих родителей. Удобно использовать дарение между близкими родственниками, потому что при этом не нужно платить никаких налогов (если же дарственная оформляется на чужого человека, последний должен будет заплатить подоходный налог в размере 13 %).

Для того чтобы подарить участок, необходимо подготовить пакет документов. В него входит, прежде всего, свидетельство о государственной регистрации права собственности на земельный участок.

Второй важный документ – кадастровый паспорт земельного участка, в котором содержится его описание (границы, площадь), категория и вид разрешенного использования земли, кадастровая стоимость.

Если даритель, как в нашем случае, стал обладателем участка, находясь в браке, то ему также потребуется представить свидетельство о заключении брака и нотариально заверенное согласие мужа (жены) на отчуждение земельного надела. Естественно, даритель и одаряемый должны иметь при себе документы, удостоверяющие их личности (паспорта).

В соответствии со ст. 572 ГК РФ по договору дарения одна сторона (даритель) безвозмездно передает или обязуется передать другой стороне (одаряемому) вещь в собственность либо имущественное право (требование) к себе или к третьему лицу, либо освобождает или обязуется освободить ее от имущественной обязанности перед собой или перед третьим лицом. Договор дарения земельного участка содержит ряд обязательных описаний: собственно, предмет договора (кто, что и кому дарит), права, обязанности и ответственность сторон, порядок разрешения споров. В этом документе также должно быть отражено, имеет ли участок какие-либо обременения, ограничения в использовании, построены ли на нем те или иные объекты недвижимости. Также нужен документ, подтверждающий уплату государственной пошлины за регистрацию договора дарения. В соответствии со ст. 574 договор дарения недвижимого имущества (в нашем случае – земельный участок) подлежит государственной регистрации.

Собрав все необходимые документы, нужно оформить в Росреестре государственную регистрацию. Моей клиенткой были собраны

все необходимые документы, и по ее просьбе мною был составлен договор дарения. Также нужно учесть, во-первых, тот момент, что многие занимаются дарением между близкими родственниками, так как это очень удобно, и не надо платить подоходный налог 13 %, во-вторых, то что налоги в настоящее время очень выросли и людям приходится дарить свою собственность, например родителям на пенсии, так как с них не берут налог. В ходе рассмотрения этого дела, меня очень заинтересовал вопрос института дарения, поэтому я решила посвятить свою статью данной теме.

Информация об авторе

Агаева Арзу Гусейновна – студентка, факультет государственного права и национальной безопасности, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, 11, e-mail: mega.agaev@mail.ru.

Author

Agaeva Arzu Guseynovna – student, Faculty of national law and national security, Baikal State University of Economics and Law, 11, Lenin str., Irkutsk, 664003, e-mail: mega.agaev@mail.ru.

УДК 347.6

К.Л. Нуроян

ПРОБЛЕМЫ, СВЯЗАННЫЕ С ЗАКЛЮЧЕНИЕМ БРАЧНОГО ДОГОВОРА В СОВРЕМЕННОМ СЕМЕЙНОМ ПРАВЕ

Статья посвящена вопросам правового режима имущества супругов и способам его урегулирования.

Ключевые слова: имущество супругов, брачный договор, семейное право.

K.L. Nuroyan

THE PROBLEMS CONNECTED WITH THE CONCLUSION OF THE MARRIAGE CONTRACT IN A MODERN FAMILY LAW

Article is devoted to questions of a legal regime of property of spouses and ways of its settlement.

Keywords: property of spouses, marriage contract, family law.

Законный режим имущества супругов может быть изменен супругами по их взаимному соглашению путем заключения брачного договора. Установленный брачным договором режим супружеского имущества называется договорным режимом имущества супругов. Его правовая регламентация осуществляется в соответствии со ст. 40–44 СК РФ.

Введение в России брачного договора, однако, не означает, что все лица при вступлении в брак обязаны его заключать. Закон предоставляет только возможность выбора в установлении тех или иных имущественных взаимоотношений в семье: на основании закона или брачного договора. При заключении брачного договора речь идет не о взаимном недоверии, не о жадности и не о расчете. Просто при помощи такого договора гораздо удобнее распоряжаться своей собственностью, возможно избежать серьезных конфликтов в случае расторжения брака.

Конечно, кто-то вполне может обойтись без брачного договора. Вряд ли целесообразно, например, заключать брачный договор, если имущество супругов состоит в основном из предметов потребительского назначения, а доходами супругов является только заработная плата. Заключение брачного договора может представлять интерес главным образом для тех людей, в собственности которых находится квартира, жилой дом, дача, земельный участок или другое недвижимое имущество, а также для лиц, занимающихся предпринимательской деятельностью, имеющих доли в капитале, акции и т.п.

Опыт таких стран, как Франция, Германия, свидетельствует о том, что, как правило, брачные договоры (контракты), известные там издавна, заключают только 5 % лиц, вступающих в брак впервые, и большинство (до 60 %) вступающих в повторный брак.

Брачный договор – это соглашение лиц, вступающих в брак (т.е. будущих супругов), или супругов (лиц, уже состоящих в браке), определяющее имущественные права и обязанности супругов в браке и (или) в случае его расторжения.

Брачный договор может быть заключен до брака или в любое время во время брака.

Брачный договор, заключенный до брака, приобретает силу со дня регистрации заключения брака в органах загса. Если брак по каким-либо причинам не будет заключен, брачный договор не будет иметь юридической силы, и не породит никаких правовых последствий.

Так, М.В. Антокольская предполагает, что все же, пожалуй, абсолютное большинство людей, подписывая этот документ надеется никогда больше в него не заглядывать. Так покупают лекарства – те, что обязательно должны быть в домашней аптечке, но которые всегда рассчитывают выбросить по истечении срока годности [1, с. 156].

Некоторые юристы, специализирующиеся на семейном праве, не пришли к единому мнению относительно брачного контракта. Некоторые из них поговаривают, что такой документ можно изначально признавать недействительным в силу «невменяемости» подписывающих его сторон, пребывающих в состоянии влюбленности.

Целесообразно было бы выделить достоинства и недостатки заключения брачного договора. Э.В. Белопольский выделяет следующие аргументы за [2, с. 2–5]:

1. Брачный договор содержит в себе лишь права и обязанности сторон (мужа и жены) по поводу распределения имущества и собственности супругов, поэтому необходимо понятия любовь и собственность разделять: брачный договор – отдельно, любовь – отдельно. Манипулировать словом «любовь» при подписании юридических документов – непорядочно. Если человек любит, то он будет любить независимо от того, подписал он брачный контракт или нет.

Если человек не любит и преследует личные, корыстные интересы, то, естественно, ему невыгодно будет составлять и подписывать брачный договор, и тогда он будет манипулировать своей любовью, давить на жалость и взывать к чувствам. Человек, который охотится за благополучием и деньгами, обязательно скажет: «Разве ты меня не любишь? Если ты меня любишь, то ты не будешь меня унижать, заставляя подписать брачный контракт…».

В действительности нет ничего унизительного в том, чтобы предусмотреть все варианты развития событий, учитывая то, что разводы сегодня – это не некий форс-мажор, а вообще привычное, обыденное для современного общества явление. Проявления дальновидности, наоборот, должны поощряться, поскольку простой письменный брач-

ный контракт сумеет сделать развод максимально гуманным и менее травматичным для всех сторон, включая детей.

2. Развод в любом случае – это сильнейший стресс, который сопровождается переоценкой жизни и глубокой депрессией. Но если брачные отношения и вопросы собственности еще и не были предусмотрительно урегулированы брачным договором, то долгоиграющий раздел имущества и «распределения» детей на выходные дни вымотает нервы всем участникам бракоразводного процесса, опустошит их души и психику.

Чтобы избежать этой адской бракоразводной круговерти надо обязательно составлять и подписывать грамотный и справедливый брачный договор: во имя когда-то пылавшей в сердцах супругов любви и ради их здоровья и здоровья их детей.

3. Глупо говорить, что вообще незачем заключать брак, если ты «не доверяешь» любимому человеку и требуешь в качестве обеспечения его порядочности подписать брачный контракт. Любовь она на то и любовь, чтобы соединять судьбы людей. Но если один человек богаче и уже имел отрицательный опыт – у него уже есть одним или нескольких разводов за плечами, то глупо игнорировать этот факт – естественно у него уже в душе есть психологическая травма, естественно, что он уже с подозрением относится ко всем подряд. И чтобы развеять эти подозрения, чтобы предоставить настоящее доказательство искренности своей любви и существует брачный договор.

К тому же, по истечении нескольких лет, более состоятельный супруг может, уже точно-точно убедившись в любви своей второй половинки, и сам выступить с инициативой об изменении некоторых условий брачного договора в пользу своего супруга или вообще расторгнуть брачный контракт.

Аргументы против:

1. Брачный договор не нужен, если оба супруга имеют равное имущественное положение, оба вносят равный материальный или посильный (например, работа по домашнему хозяйству – это тоже работа) вклад в семью.

2. Брачный договор не нужен, если любящие друг друга люди безраздельно друг другу доверяют и у них нет отрицательного опыта в форме одного или нескольких разводов.

3. Брачный договор не нужен, если у супругов вообще нет ценного имущества.

В заключение, хотелось бы отметить, что тем самым наш законодатель воспринял нормы зарубежного законодательства о брачном договоре, предоставив супругам право устанавливать режим супружеского имущества по своему усмотрению.

Основная цель брачного договора – определение правового режима имущества супругов и иных имущественных взаимоотношений во время брака и в случае его расторжения. Практика заключения таких договоров пока еще не нашла широкого применения в нашей стране.

Список использованной литературы

1. Антокольская М.В. Семейное право: учебник. М.: Юристъ, 2012. 336 с.

4. Белопольский Э.В. Ответственность по брачному договору // Домашний адвокат. 2013. № 23. С. 2–5.

2. Вишнякова А.В. Комментарий к Семейному кодексу Российской Федерации. М.: Контракт, 2013. 317 с.

Информация об авторе

Нуроян Кристина Львовна – студентка, судебно-следственный факультет, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, 11. e-mail: nurojan777@gmail.com.

Author

Nuroyan Christina Lvovna – the student, judicial and investigative faculty, Baikal State University of Economics and Law, 11, Lenin str., Irkutsk, 664003, e-mail: nurojan777@gmail.com.

УДК 347.4

Л.З. Долсонова

РАЗДЕЛ ИМУЩЕСТВА. ПРАКТИКА ИСПОЛНИТЕЛЬНОГО ПРОИЗВОДСТВА

Раскрывается понятие совместно нажитого имущества супругов, перечисляются особенности раздела общего имущества супругов.

Ключевые слова: брак, расторжение брака, совместно нажитое имущество, раздел имущества.

L.Z. Dolsonova

DIVISION OF PROPERTY. THE PRACTICE OF ENFORCEMENT PROCEEDINGS

The article presents the concept of jointly acquired property of the spouses, lists the features section of the common property.

Keywords: marriage, divorce, jointly acquired property, property division.

С большим интересом начали работу в юридической клинике. На одном из первых дежурств к нам пришла посетительница – 78-летняя женщина, Анна Ивановна. Казалось бы, о чем беспокоиться бабуле кроме как воспитанием своих внуков. «Наверное, к нам ее привели какие-либо проблемы с соседями или что-то, связанное с жилищно-коммунальными услугами», подумали мы. Но оказалось, бедная женщина, ветеран труда, под старость своих лет осознала, что больше не может жить со своим мужем.

Прожили вместе более полувека, воспитали троих детей, сейчас растут внуки. Естественно, за такое время накопилось определенное совместное имущество. Совместно нажитым имуществом признается движимое и недвижимое имущество, которое приобреталось и постепенно накапливалось супругами во время их проживания друг с другом. Таковым в соответствии с Семейным кодексом РФ являются:

– доходы супругов от трудовой, предпринимательской, интеллектуальной и творческой деятельности;

– полученные пенсии, денежные компенсации, не имеющие целевого назначения (к примеру, на содержание ребенка);

– приобретенное за счет общих доходов движимое и недвижимое имущество;

– денежные вклады, паи инвестиционных фондов, ценные бумаги, доля в бизнесе, если таковой создан в период совместного проживания. Ну а в нашем случае в качестве совместно нажитого имущества выступили: жилой дом и кооперативный гараж.

Получилось так, что супруги уже два года проживали отдельно друг от друга. Места для дальнейшего раздельного от мужа прожива-

ния у женщины не было. В связи с этим возник вопрос о разделе имущества. Как правило, раздел имущества – это один из наиболее длительных и непростых процессов в сфере семейного права, при котором возникают сложные правовые ситуации. Согласно закону, разделом имущества является закрепление прав на определенную долю за каждым супругом после ее определения.

В таких случаях, когда дело подходит к разделу имущества договориться о деталях его совершения можно двумя способами – по соглашению или через суд. Первый вариант, безусловно, предпочтительнее. По статистике, мирно договориться о разделе имущества россиянам при расторжении брака удается крайне редко – в 90 % случаев такие дела рассматриваются в суде. К сожалению, и дело нашей посетительницы отнеслось к этим 90 %.

Понятное дело, что Анна Ивановна совершала не одну попытку мирно договориться со своим мужем, без обращения в суд. Супруг не только отказался от принятия соглашения о разделе имущества, но еще потребовал развод. Исходя из этого, Анна Ивановна решила не ждать действий супруга, а подать исковое заявление, и обратилась к нам за помощью.

Для составления грамотного искового заявления необходимо четко соответствовать требуемой форме и содержанию, указанной в статье 131 ГПК, что нами и было произведено. И в дальнейшем в соответствии со ст. 34, 38, 39 СК РФ было оформлено заявление в суд.

При нашей последней встрече с Анной Ивановной, она с нами поделилась тем, что недавно справляла свой день рождения. Поздравить любимую маму, бабушку, подругу пришли ее дети, внуки, друзья, к удивлению, и супруг. В голосе было заметно, что женщина уже не так сильно обеспокоена сложившимися проблемами. И тут мы подумали, может быть, пожилые люди вспомнили, как много светлых моментов связывает их друг с другом, какие жизненные тяжбы они преодолели вместе, и в конце концов все же осознали, что остаток жизни они смогут провести вместе.

Информация об авторе

Долсонова Лиана Зориктоевна – студент, факультет государственного права и национальной безопасности, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина 11, e-mail: liana_dolsonova@mail.ru.

Author

Dolsonova Liana Zoriktoevna – student, the faculty of the state law and national security. Baikal National University of Economics and Law, 11 Lenin str. Irkutsk, 664003, e-mail – liana_dolsonova@mail.ru.

УДК 347.64

К.В. Дресвянская

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ЖИЛЬЕМ ДЕТЕЙ-СИРОТ, ЛИЦ ИЗ ЧИСЛА ДЕТЕЙ-СИРОТ И ЛИЦ, ОСТАВШИХСЯ БЕЗ ПОПЕЧЕНИЯ РОДИТЕЛЕЙ

В статье проводится анализ правового регулирования обеспечения жильем детей – сирот, и детей, оставшихся без попечения родителей. Анализируется федеральное и региональное законодательство. Ставится вопрос о необходимости внесения поправок в Федеральный закон «О дополнительных гарантиях по социальной поддержке детей-сирот и детей, оставшихся без попечения родителей».

Ключевые слова: дети-сироты, дети, оставшиеся без попечения родителей, право на внеочередное предоставление жилого помещения по договору социального найма, договор найма специализированного жилого помещения.

K.V. Dresvyanskaya

THE PROBLEM OF HOUSING CHILDREN – ORPHANS, PERSONS FROM THE NUMBER OF CHILDREN – ORPHANS AND THOSE LEFT WITHOUT CARE PARENTS

The article analyzes the legal regulation of maintenance with habitation of children – orphans and children left without parental care. Analyzed federal and regional legislation. The question of the need for amendments to the federal law «About additional guarantees on social support of children – orphans and children left without parental care».

Keywords: orphans, children left without their parents' care, the right to claim the priority in granting living quarters on the basis of social lease arrangement, special dwelling lease arrangement.

Одним из важнейших направлений государственной социальной политики Российской Федерации является защита имущественных и жилищных прав детей-сирот. Как справедливо отмечается специалистами, в настоящее время в Российской Федерации разработана и принята законодательная база, определяющая права, льготы, дополнительные гарантии для указанной категории граждан в части обеспечения их жилыми помещениями [1, с. 26–31]. Однако в реальной жизни правоприменительная практика имеет ряд существенных проблем, не позволяющих в достаточной мере реализовать жилищные права детей-сирот. В ч. 1 ст. 40 Конституции Российской Федерации закреплено, что каждый имеет право на жилище, и никто не может быть произвольно его лишен. Тем не менее, невзирая на законодательное закрепление и признание данных прав, огромное количество сирот в России остается без жилья. Ежегодно из российских детских домов выпускается примерно около десяти – пятнадцати тысяч сирот. Более 76 % детей – сирот после выпуска не могут реализовать свое конституционное право, на получение жилья, следовательно, оказываются на улице. Стремление обрести собственное жилье и начать новую жизнь, это желание каждого выпускника детского дома. Однако, чтобы получить жилье, необходимо преодолеть и решить ряд проблем.

С одной из таких проблем столкнулся наш клиент, с чем и обратился за помощью к нам в юридическую клинику.

В марте 2015 г. к нам в юридическую клинику обратилась гражданка Б. 1990 года рождения. В 1997 г. у нее погибли родители. В 2005 г. попечителем гражданке Б. была назначена ее старшая сестра, в этом же году за ней закрепили право пользования ½ долей жилого помещения, собственником которого являлся ее покойный дядя. В начале 2013 г. она обратилась в орган опеки и попечительства для постановки ее на учет, как ребенка сироту для получения жилья. Орган опеки и попечительства ей отказал на том основании, что в 2005 г. за ней было закреплено право пользования жилым домом. 25 июня 2013 г. гражданка Б. в судебном порядке отказалась от ½ доли дома (наследства), который достался им с сестрой от покойного дяди. После чего, наша клиентка неоднократно писала в орган опеки и попечительства, в администрацию Ленинского района о том, что ей неза-

конно отказывают в постановке на учет, так как в закрепленном за ней жилом помещении, она имеет только прописку и никаких правообладающих документов на дом у нее не имеется. Только в конце 2013 г. гражданке Б. администрацией Ленинского района был дан ответ на ее заявление. В ответе сказано, что наличие у нее закрепленного за ней права пользования жилым помещением не является основанием для отказа включения ее в список детей-сирот, подлежащих обеспечению жилыми помещениями.

Основной проблемой является то, что на момент получения вышеуказанного ответа, нашей клиентке уже исполнилось 23 года. За реализацией и защитой своего права по достижению 23 лет, она обращалась к Уполномоченному по правам ребенка, к адвокатам, которые дали ей ответ, что реализовать свое право она могла только до достижения 23 летнего возраста.

В настоящий момент она проживает на съемной квартире. В юридическую клинику она обратилась с вопросом «Является ли достижение лицом из числа детей-сирот и детей, оставшихся без попечения родителей, возраста 23 лет основанием для отказа компетентными органами во внеочередном предоставлении ему жилого помещения, если он предпринимал меры для постановки на учет до 23 лет?»

Правовые основания обеспечения жилыми помещениями детей-сирот закреплены в ст. 57, 109.1 Жилищного кодекса Российской Федерации, в ст. 8 Федерального закона от 21 декабря 1996 г. № 159-ФЗ «О дополнительных гарантиях по социальной поддержке детей-сирот и детей, оставшихся без попечения родителей» (далее – Федеральный закон № 159).

В соответствие с п. 1 ст. 8 Федерального закона № 159, детям-сиротам и детям, оставшимся без попечения родителей, лицам из числа детей-сирот и детей, оставшихся без попечения родителей, которые не являются нанимателями жилых помещений по договорам социального найма или членами семьи нанимателя жилого помещения по договору социального найма либо собственниками жилых помещений, а также детям-сиротам и детям, оставшимся без попечения родителей, лицам из числа детей-сирот и детей, оставшихся без попечения родителей, которые являются нанимателями жилых помещений по договорам социального найма или членами семьи нанимателя жилого помещения по договору социального найма либо собственниками жилых помещений, в случае, если их проживание в ранее занимаемых жилых помещениях признается невозможным, органом ис-

полнительной власти субъекта Российской Федерации, на территории которого находится место жительства указанных лиц, в порядке, установленном законодательством этого субъекта Российской Федерации, однократно предоставляются благоустроенные жилые помещения специализированного жилищного фонда по договорам найма специализированных жилых помещений[1].

Аналогичная норма содержится в ст. 2 Закона Иркутской области от 28 декабря 2012 года (с изменениями на 11 июля 2014 г.) № 164 «О порядке обеспечения детей-сирот и детей, оставшихся без попечения родителей, лиц из числа детей-сирот и детей, оставшихся без попечения родителей, жилыми помещениями в Иркутской области»[2].

Так же в п. 3 ст. 1 Федерального закона № 159, указано, что под лицами из числа детей-сирот и детей, оставшихся без попечения родителей, следует понимать лиц в возрасте от 18 до 23 лет. Это значит, что законодатель установил возрастной порог, согласно которому, положения Федерального Закона № 159 распространяется только, на детей-сирот, детей, оставшихся без попечения родителей, и лиц из их числа до достижения ими 23-летнего возраста.

Согласно п. 9 ст. 8 этого же Федерального закона: «Право на обеспечение жилыми помещениями сохраняется за лицами, которые относились к категории детей-сирот и детей, оставшихся без попечения родителей, лиц из числа детей-сирот и детей, оставшихся без попечения родителей, и достигли возраста 23 лет, до фактического обеспечения их жилыми помещениями». То есть, согласно п. 9 ст. 8 вышеуказанного закона, достижение 23 летнего возраста не является основанием для отказа в постановке на учет детей-сирот, если они до 23 лет не были обеспечены жилыми помещениями.

Как показывает судебная практика, суды исходят из того, что достижение лицом из числа детей-сирот и детей, оставшихся без попечения родителей, возраста 23 лет, которое было принято на учет нуждающихся в жилом помещении до 23-летнего возраста, не может служить основанием для отказа в реализации таким лицом права на

---

[1] О дополнительных гарантиях по социальной поддержке детей-сирот и детей, оставшихся без попечения родителей: федеральный Закон от 21 декабря 1996 г. (в ред. от 31 декабря 2014) // Собрание Законодательства РФ. 1996. № 52. Ст. 5880.

[2] О порядке обеспечения детей-сирот и детей, оставшихся без попечения родителей, лиц из числа детей-сирот и детей, оставшихся без попечения родителей, жилыми помещениями в Иркутской области: Закон Иркутской области от 28 декабря 2012 года № 164-ОЗ // Ведомости Законодательного Собрания Иркутской области. 2013. № 52 (Т. 2).

внеочередное предоставление жилья, которое не было им получено в период до достижения возраста 23 лет[1].

Вместе с тем, суды выясняют причины, в силу которых истец своевременно не встал (не был поставлен) на учет в качестве нуждающегося в жилом помещении. В случае признания таких причин уважительными суды удовлетворяли требование истца об обеспечении его вне очереди жилым помещением по договору социального найма[2].

Наиболее распространенными причинами несвоевременной постановки детей-сирот, детей, оставшихся без попечения родителей, и лиц из их числа на учет нуждающихся в жилом помещении, являются: 1) незаконный отказ органа местного самоуправления в постановке на учет в качестве нуждающихся в жилом помещении лиц из числа детей-сирот и детей, оставшихся без попечения родителей, не достигших возраста 23 лет; 2) установление обстоятельств того, что лицо до достижения возраста 23 лет предпринимало попытки встать на учет в качестве нуждающегося в жилом помещении, но не было поставлено на учет.

Таким образом, как показывает практика достижение лицом из числа детей-сирот и детей, оставшихся без попечения родителей, возраста 23 лет не является основанием для отказа компетентными органами во внеочередном предоставлении ему жилого помещения.

На сегодняшний день гражданка Б. подала исковое заявление, на предоставление ей жилого помещения на основание того, что до достижения возраста 23 лет, она предпринимала попытки встать на учет в качестве нуждающегося в жилом помещении, но не была поставлена на учет.

На основании всего вышеизложенного необходимо отметить, что в действующем законодательстве существует пробел, который в настоящее время никак не урегулирован. Федеральный закон от 21 декабря 1996 года № 159-ФЗ «О дополнительных гарантиях по социальной поддержке детей-сирот и детей, оставшихся без попечения родителей», не содержит никакой нормы, которая бы предусматривала возможность реализовать свое право детям-сиротам и детям, оставшимся без попечения родителей, после достижения ими возраста 23 лет.

---

[1] Обзор законодательства и судебной практики Верховного Суда Российской Федерации за второй квартал 2006 года от 27 сентября 2006 // Бюллетень Верховного Суда РФ. 2007. № 1.

[2] Обзор практики рассмотрения судами дел, связанных с обеспечением детей-сирот и детей, оставшихся без попечения родителей, лиц из числа детей-сирот и детей, оставшихся без попечения родителей, жилыми помещениями от 20 ноября 2013 г. // Бюллетень Верховного Суда РФ. 2014. № 3.

Таким образом, представляется целесообразным внести изменения в действующее законодательство путем внесения дополнений и поправок. Дополнить Федеральный Закон от 21 декабря 1996 № 159-ФЗ «О дополнительных гарантиях по социальной поддержке детей-сирот и детей, оставшихся без попечения родителей» соответствующей статьей, посвященной продлению сроков для реализации своего права в зависимости от причин, по которым они были пропущены.

Список использованной литературы

1. Карибян С.О. Правовые проблемы обеспечения жильем детей-сирот // Вопросы ювенальной юстиции. 2014. № 1 (51). С. 26–31.

Информация об авторе

Дресвянская Кристина Владимировна – студентка, факультета государственного права и национальной безопасности, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, 11, e-mail: dkv-93@mail.ru.

Author

Dresvyanskaya Kristina Vladimirovna – student, Faculty of national law and toward national security, Baikal State University of Economics and Law, 11, Lenin str., Irkutsk, 664003, e-mail: dkv-93@mail.ru.

УДК 347.254

Е.С. Завгородняя

ДОЛЕВАЯ СОБСТВЕННОСТЬ И ПРОБЛЕМЫ РЕАЛИЗАЦИИ ЖИЛИЩНЫХ ПРАВ: НА ПРИМЕРЕ КОНКРЕТНОГО ДЕЛА

В статье рассматривается возможность выдела доли в натуре из общей долевой собственности на основе конкретного дела.

Ключевые слова: долевая собственность, участник долевой собственности, выдел доли в натуре.

E.S. Zavgorodnyaya

FRACTIONAL OWNERSHIP AND PROBLEMS OF REALIZATION OF HOUSING RIGHTS: THE CASE OF THE PARTICULAR CASE

The article discusses the possibility of separation of a share in kind from the general share property on the basis of a specific case.

Keywords: fractional ownership, a participant in share ownership, the apportionment of a share in kind.

В настоящее время квартирный вопрос является одним из злободневных. Нередко люди сталкиваются с невозможностью осуществления, принадлежащего им права собственности на жилое помещение – квартиру, в особенности, если речь идет об общей долевой собственности, причины могут быть разнообразные. Участники долевой собственности пытаются различными способами решить эту проблему. Поэтому поводу в юридическую клинику обратилась женщина с просьбой составить исковое заявление о выделе доли в натуре.

Женщина рассказала, что проживает с бывшим мужем в четырехкомнатной квартире, принадлежащей им на праве общей долевой собственности. Так же в квартире вместе с ними проживает их общая совершеннолетняя дочь. Матери с дочерью принадлежит на праве собственности по ¼ доли каждой в указанной квартире, а бывшему супругу – ½ доля в праве собственности. Мать с дочерью решили выделить в натуре свои доли, по причине сложившихся конфликтных отношений с ответчиком, закрепив за собой право собственности на жилые комнаты в соответствии со сложившимся за время проживания порядком пользования. Так как истцы не достигли с ответчиком соглашения о выделе доли, ввиду того, что он не согласен с предложенными условиями, то они решили обратиться в суд.

Согласно ст. 252 ГК РФ, участник долевой собственности может в судебном порядке требовать выдела в натуре своей доли из общего имущества, если с другими собственниками не достигнуто соглашение о способе и условиях выдела доли одного из них.

Возможность выдела доли в натуре предполагает, что выделяемое помещение должно быть изолированным. Выделение части имущества (жилой площади, жилой комнаты) в натуре должно быть соразмерно идеальной доле в праве общей долевой собственности.

Поэтому возник вопрос о соразмерности выделяемой истцами части имущества их доле. Как оказалось, те комнаты, которые хотят выделить истцы, не соответствуют их доле в праве собственности, они меньше по площади.

Этот вопрос решается в соответствии с п. 4 ст. 252 ГК РФ, если же выделяемые жилые комнаты несоразмерны доле участника в праве общей долевой собственности, то существующая разница устраняется выплатой соответствующей денежной суммы или иной компенсацией. Поэтому ответчик должен выплатить компенсацию.

В результате выдела доли происходит прекращение права общей собственности и возникновение у выделяющегося собственника единоличной собственности на соответствующую его доле часть жилого помещения.

Информация об авторе

Завгородняя Евгения Сергеевна – студентка, судебно-следственный факультет, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, 11. E-mail: tituxa@yandex.ru.

Author

Zavgorodnyaya Evgenia Sergeevna – student, judicial-investigation faculty, Baikal National University of Economics and Law, 11, Lenin str., Irkutsk, 664003. E-mail: tituxa@yandex.ru.

УДК 340

О.В. Караульская

ЮРИДИЧЕСКАЯ КЛИНИКА – ПЕРВЫЙ ШАГ СТУДЕНТА В ПРАКТИКУ, ПЕРВОЕ ДЕЛО, ПЕРВЫЙ СУДЕБНЫЙ ПРОЦЕСС, ПЕРВАЯ ПОБЕДА

В статье рассматривается ситуация неправомерного взимания платы за коммунальные услуги, приводится правовая позиция Конституционного Суда Российской Федерации по этому вопросу, исследуется судебная практика, а также описывается ход судебного про-

цесса в мировом суде по защите клиента, обратившегося за помощью в юридическую клинику.

Ключевые слова: договор управления многоквартирным домом, плата за коммунальные услуги, разрешение на ввод многоквартирного дома в эксплуатацию, неосновательное обогащение, проценты за пользование чужими денежными средствами.

O.V. Karaulskaya

THE LEGAL CLINIC – THE FIRST STEP STUDENTS IN PRACTICE, THE FIRST CASE, THE FIRST TRIAL, THE FIRST VICTORY

The article examines the situation of illegal collection of fees for public services, given the legal position of the Constitutional Court of the Russian Federation on this issue, we analyze the jurisprudence, and describes the course of the trial in the Magistrate's Court for the protection of the client, ask for help in a legal clinic.

Keywords: contract management of an apartment house, fees for public services, permission to enter the apartment house in operation, unjust enrichment, interest on borrowed funds.

Приняв участие в деятельности Юридической клиники Байкальского Государственного Университета Экономики и Права, могу с уверенностью сказать, что время мной не было потрачено напрасно. Говорят, в любом деле главное сделать первый шаг. Юридическая клиника стала для меня таким шагом, он же и оказался шагом в правильном направлении. Полагаем далеко не каждый, поступая после школы на тот или иной факультет, делает этот выбор осознанно. И только лишь в процессе обучения начинает задумываться: «А то ли это, чем я хочу заниматься?» А потом начинаются проблемы и последствия в виде того, что человек, вовремя не изменив ситуацию, всю свою жизнь занимается без какого-либо желания не своим делом, а, следовательно, и уровень качества его деятельности страдает. Слава богу, со мной такого казуса не произошло. И юридическая клиника, позволившая прикоснуться непосредственно к практике, к работе с реальными людьми, с их проблемами, окончательно убедила меня в том, что иду я правильной дорогой. Именно для своевременного вы-

явления вышеописанных коллизий должны создаваться проекты, похожие на юридическую клинику.

В данной статье хотелось бы рассказать о самом первом опыте в суде и поделиться теми основополагающими положениями, рекомендациями, идеями, которые были вынесены из этой работы, которые родились из приобретенного опыта, и которыми я буду руководствоваться в своей дальнейшей профессиональной деятельности.

Итак, в октябре 2014 г., в самом начале нашей деятельности в рамках юридической клиники, к нам обратился гражданин Д. Суть проблемы состояла в следующем: 5 мая 2012 г. наш клиент заключил договор управления многоквартирным домом с Управляющей компанией «***», в соответствии с которым с 5 мая 2012 г. ему начисляется плата за жилое помещение и коммунальные услуги. Однако разрешение на ввод объекта в эксплуатацию Администрацией г. Иркутска было выдано только 28 сентября 2012 г., а квартира была передана нашему клиенту по акту приема-передачи 29 сентября 2012 г. В связи с чем гражданин Д. полагал, что плата за коммунальные услуги в период с 5 мая 2012 г. по 29 сентября 2012 г. взималась неправомерно.

Именно на этапе интервьюирования клиента и родился первый тезис – не позволяй клиенту усомниться в твоей компетентности.

Клиенты бывают разные. В юридической клинике помощь оказывается бесплатно преимущественно для социально слабых слоев населения, поэтому чаще всего приходят люди, совершенно не подготовленные в правовой сфере, которые имеют проблему и желают ее разрешения. С такими клиентами довольно просто казаться уверенным и компетентным. Именно, работая с такой категорией людей, в полной мере пришлось ощутить негативное явление, обозначающееся термином «раболепие». Это когда человек, приходит с совершенно несложной для разрешения (с точки зрения юриста) проблемой и смотрит так «снизу вверх», как бы преклоняясь (не из приятных чувство) и ждет помощи и разрешения своей проблемы, при условии, что в органах власти человек уже побывал. Именно тогда и пришло осознание всеобщего русского угодничества и возникли мысли, что может быть именно это и есть одна из причин нашей непобедимой коррупции. Попадая в такую ситуацию, возникает желание изменить реальную действительность, во чтобы то не было помочь человеку. Однако, следует соблюдать второе правило – никогда ничего не обещай, держи дистанцию. Попадая под влияние своих эмоций и чувств (жалость в частности) не позволяй себе, что бы то ни было обещать кли-

енту, тем более в начале карьеры, когда не знаешь полностью всех тонкостей профессиональной деятельности.

Однако гражданин Д. совершенно из другой категории клиентов, это был человек, пусть и не обладающий специальными знаниями в юриспруденции, однако знающий свою проблему вдоль и поперек, знающий законодательство по своей проблеме и желающий конкретного результата. Общаясь с клиентами из этой категории необходимо выглядеть как можно увереннее и, если не понимаешь, о чем речь, необходимо сделать вид, что все под контролем, а уже в дальнейшей работе как можно подробнее разобраться в ситуации. Что и было сделано.

По итогам работы было подготовлено первое исковое заявление. Основное, что необходимо отметить – будь внимателен к мелочам, вплоть до дотошности в составлении документов. Грамматические ошибки в тексте, опечатки, описки – все это, не есть показатель профессионализма. Не допускай случаев изобличения себя в неграмотности.

И четвертое правило – документ должен выглядеть красиво. Шапочка, текст и стиль. Документ должен быть документом, а не просто запиской соседу по парте.

Также, прежде чем, составлять исковое заявление необходимо определить правовые основания для обращения в суд за защитой. Следующее, пятое правило – в суд нужно идти с твердой уверенность в своей правоте, иначе, зачем писать исковое заявление, если заведомо знаешь, что это не принесет должных результатов.

В нашей ситуации основанием стала статья 1102 ГК РФ, обязывающая возвратить неосновательное обогащение. Плата за коммунальные услуги в период с 5 мая 2012 г. по 29 сентября 2012 г. являлась именно неосновательным обогащением, т.к. управляющая компания приобрела денежные средства гражданина Д. без установленных законом оснований. В подп. 6 п. 2 ст. 153 Жилищного кодекса РФ установлено, что обязанность по внесению платы за жилое помещение и коммунальные услуги возникает у лица, принявшего от застройщика (лица, обеспечивающего строительство многоквартирного дома) после выдачи ему разрешения на ввод многоквартирного дома в эксплуатацию помещения в данном доме по передаточному акту или иному документу о передаче, с момента такой передачи.

Судебное заседание состоялось 6 декабря 2015 г. Необходимо отметить очень интересный момент, что в ходе судебного заседания представитель застройщика, привлеченный в процесс в качестве

третьего лица, цитировал данную норму, упустив слова «после выдачи ему разрешения на ввод многоквартирного дома в эксплуатацию» На что было обращено внимание суда. Правило № 6 – акцентируй внимание суда на нарушения другой стороны, возражай своевременно и по любой мелочи, которая не соответствует твоей позиции.

Администрацией г. Иркутска 28 сентября 2012 г. было выдано разрешение на ввод объекта в эксплуатацию. Квартира была передана по акту приема-передачи от 29 сентября 2012 г. Однако основная проблема и трудность состояла в том, что имелось два акта приема и оба надлежащим образом подписаны сторонами: от 29 сентября 2012 г. и от 05 мая 2012 г.

На что своевременно была сформирована позиция. Седьмое правило – все необходимо готовить в письменном виде и предоставлять суду. Суд, принимая решение, не будет вспоминать, что и как было сказано в судебном заседании, а если вами были представлены письменные возражения с приложениями копий прецедентных решений, вероятность, что позиция суда совпадет с вашей, значительно возрастает. (Тем более, что вы же уверенны в своей правоте (правило № 6).

А проблема с наличием двух актов была решена следующим образом:

В соответствии с ч. 2 ст. 8 Федерального закона от 30 декабря 2004 г. № 214-ФЗ[1] передача объекта долевого строительства осуществляется не *ранее чем после* получения в установленном порядке разрешения на ввод в эксплуатацию многоквартирного дома и (или) иного объекта недвижимости.

Разрешение на ввод в эксплуатацию было получено только 28.09.2012 г., а акт приема передачи подписан 05.05.2012 г., т.е. акт подписан раньше срока получения разрешения на ввод объекта в эксплуатацию, что не соответствует требованиям ч.1 ст. 4 и ч. 2 ст. 8 Федерального закона Российской Федерации от 30.12.2004 г. № 214-ФЗ, являющихся императивной нормой, подлежащей обязательному применению.

В соответствии с п. 1 ст. 166 ГК РФ сделка недействительна по основаниям, установленным законом, в силу признания ее таковой

[1] Об участии в долевом строительстве многоквартирных домов и иных объектов недвижимости и о внесении изменений в некоторые законодательные акты Российской Федерации: Федеральный закон № 214-ФЗ от 30 декабря 2004 г. // Российская газета. 2014. 31 дек. (№ 292).

судом (оспоримая сделка) либо независимо от такого признания (ничтожная сделка).

Как установлено в ч. 1 ст. 168 ГК РФ за исключением случаев, предусмотренных п. 2 ст.168 ГК РФ или иным законом, сделка, нарушающая требования закона или иного правового акта, является оспоримой, если из закона не следует, что должны применяться другие последствия нарушения, не связанные с недействительностью сделки.

Правило № 8 – обращай внимание на изменения законодательства. Лучше лишний раз перепроверить, действовала ли норма в момент того или иного события.

Нормы ГК РФ (в редакции Федерального закона от 7 июля 2013 г. № 100-ФЗ) об основаниях и о последствиях недействительности сделок (ст.ст. 166 – 176, 178 – 181) применяются к сделкам, совершенным после дня вступления в силу указанного Закона.

Акт был подписан 5 мая 2012 г., т.е. до дня вступления в силу федерального закона от 7 мая 2013 г. № 100-ФЗ, значит необходимо обратится к предыдущей редакции данной нормы, которая гласит: «Сделка, не соответствующая требованиям закона или иных правовых актов, *ничтожна*, если закон не устанавливает, что такая сделка оспорима, или не предусматривает иных последствий нарушения»

Согласно п.1. ст. 167 ГК РФ недействительная сделка не влечет юридических последствий, за исключением тех, которые связаны с ее недействительностью, и недействительна с момента ее совершения.

Соответственно, акт приема-передачи от 5 мая 2012 г., является частью сделки договора участия в долевом строительстве, признается недействительным (ничтожным) со дня его совершения, несмотря на довод стороны ответчика, что факт получения квартиры именно 5 мая 2012 г. подтверждается решением Куйбышевского районного суда г. Иркутска[2].

В соответствии со ст. 180 ГК РФ недействительность части сделки не влечет недействительности прочих ее частей, если можно предположить, что сделка была бы совершена и без включения недействительной ее части. Следовательно, недействительность акта от 5 мая 2012 г. не влечет недействительности самого договора участия в долевом строительстве.

[2] Решение Куйбышевского районного суда г. Иркутска от 20 сент.2013 г. // Архив Куйбышевского районного суда г. Иркутска, 2013 г.

Согласно ст. 12 ГК РФ защита гражданских прав осуществляется путем, в том числе, применение последствий недействительности сделки.

Следовательно, законным, действительным актом приема-передачи является акт от 29 сентября 2012 г. и с этого момента, согласно ст. 153 ЖК РФ, возникает обязанность по внесению платы за жилое помещение и коммунальные услуги.

Еще одним спорным моментом, пробующим предварительной подготовки был тот факт, что отказ в выдаче разрешения на ввод объекта в эксплуатацию был оспорен в судебной порядке и судом признан неправомерным[3]. На что, конечно же, активно ссылалась сторона ответчика. Правило № 9 – четко разделяй правоотношения и субъектов этих правоотношений. В противовес данному аргументу, представленному ответчиком, было отмечено, что взаимоотношения между администрацией г. Иркутска и застройщиком, никак не влияют на отношения между Управляющей компанией и собственником (плательщиком, потребителем). А также приведен аргумент, что заведомо не было известно правомерен ли отказ (неправомерность отказа была установлена только в ходе судебного заседания 8 июня 2012 г.), а также отмечена невозможность взимания платы за оказание коммунальных услуг, т.е. по сути платы за обслуживание помещения, за его эксплуатацию, до того как компетентный орган выдал это самое разрешение на ввод в эксплуатацию.

Помимо прочего ответчик утверждал, что по факту услуги были предоставлены управляющей компанией и были потреблены гражданином Д.

Однако в силу подп. «а» п. 3 Постановления Правительства РФ от 6 мая 2011 г. № 354[4] коммунальные услуги предоставляются потребителям начиная с установленного Жилищным кодексом РФ момента, а именно: с момента возникновения права собственности на жилое помещение – собственнику жилого помещения и проживающим с ним лицам. Однако без разрешения на ввод объекта в эксплуатацию невозможно получить свидетельство права собственности на квартиру, которое было получено только 11 июня 2013 г.

---

[3] Решение Арбитражного суда Иркутской области по делу № А19-10236/2012 от 08 июня 2012 г.// Архив Арбитражного суда Иркутской области, 2012 г.

[4] О предоставлении коммунальных услуг собственникам и пользователям помещений в многоквартирных домах и жилых домов: Постановление Правительства РФ № 354 от 06 мая 2011 г. // Российская газета. 2011. 1 июня (№ 116).

И наконец, десятое правило – готовься к процессу заранее, подготовь комплект прецедентных решений (естественно, подтверждающих вашу правовую позицию по делу).

Несмотря на приведенный стороной ответчика прецедент, когда истцу было отказано в аналогичных требованиях[5], нами по данному делу был найден ряд судебных решений[6], оспаривающих данное решение.

Правовая позиция Конституционного Суда Российской Федерации, изложенная в данном определении определяет моментом возникновения обязанности по оплате коммунальных услуг, которым является дата приемки объекта строительства в *эксплуатацию* и внесения заявителем оплаты по договору долевого строительства с учетом того, что обязанность по оплате коммунальных услуг в равной мере распространяется на лиц, использующих жилое помещение как на праве собственности, по договору найма жилого помещения, так и на иных законных основаниях, а не моментом государственной регистрации права собственности заявителя на занимаемое помещение.

В заключение хотелось бы сказать об итогах работы по данному делу. Было вынесено определение суда о прекращении производства по делу, в связи с отказом от иска. Ответчик после судебного заседания, еще до вынесения решения, предложил выплатить спорную сумму. Клиента это устроило, и мы заявили отказ от иска. Несмотря на процессуальное прекращение дела, интересы доверителя были соблюдены, и я по праву считаю это своей первой победой.

Информация об авторе

Караульская Олеся Владимировна – студентка, факультет государственного права и национальной безопасности, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, 11, e-mail: avocatolawyer@mail.ru.

[5] Решение Октябрьского районного суда г. Иркутска по делу № 2-1676/2013 от 22 мая 2013 г. // Архив Октябрьского районного суда г. Иркутска, 2013 г.

[6] Постановление Федерального арбитражного суда Поволжского округа от 26 октября 2010 г. по делу № А65-36875/2009; Постановление Одиннадцатого Арбитражного апелляционного суда от 26 июля 2013 г. по делу № А55-31915/2012; Постановление Федерального арбитражного суда поволжского округа от 12 ноября 2013 г. по делу № А55-31915/2012.

Author

Karaulskaya Olesya Vladimirovna – student, Department of the State Law and National Security, Baikal State University of Economics and Law, 11, Lenin str., Irkutsk, 664003, e-mail: avocatolawyer@mail.ru.

УДК 349.3

А.Д. Махазагдаева

ПРАВОВЫЕ ВОПРОСЫ ОПЛАТЫ ТРУДА В БЮДЖЕТНЫХ ОРГАНИЗАЦИЯХ

В статье раскрывается проблема оплаты труда в бюджетных организациях.

Ключевые слова: Трудовой кодекс РФ, трудовой договор, выплата работникам, заработная плата.

A.D. Makhazagdaeva

LEGAL ISSUES OF WAGES IN THE BUDGETARY ORGANIZATONS

The article deals with the problem of wages in the budgetary organizations.

Keywords: Labor code of the Russian Federations, the employment contract, payment of employees wages.

На протяжении последних десятилетий в России сложилась критическая ситуация в сфере соблюдения прав граждан на оплату труда. Чаще всего причинами нарушений являются злоупотребление со стороны работодателя, экономические и иные просчеты в управленческой деятельности. Так же нередки случаи незаконного уменьшения заработной платы работника. Она связана с тем, что должностные лица не знают норм действующего законодательства, включая правила об ответственности за незаконное удержание. Иногда работодатель намеренно игнорирует законодательство, надеясь, что работник не будет оспаривать удержания, а при проверке о данном факте никто не

узнает. Однако такая позиция приводит к негативным последствиям, как для самого работодателя, так и для должностных лиц.

С подобной проблемой столкнулась клиентка нашей юридической клиники. В декабре 2014 года гражданка К. обратилась с просьбой помочь ей решить вопрос по незаконным удержаниям из заработной платы. Просьба гражданки К заключалась в том, чтобы написать жалобу в прокуратуру о неправомерных действиях работодателя в отношении выплаты заработной платы.

В ходе беседы с клиенткой выяснилось следующее: Гражданка К. в апреле 2014 года была принята в государственную бюджетную организацию на должность подсобного рабочего. В трудовой книжке была произведена соответствующая запись о приеме на работу. Между гражданкой К. и работодателем был заключен трудовой договор, один экземпляр которого был выдан ей без подписи работодателя. В соответствии со ст. 57 ТК РФ в трудовом договоре указываются наименование работодателя, сведения о представителе работодателя, подписавшем трудовой договор, и основание, в силу которого он наделен соответствующими полномочиями.

Согласно ст. 61 ТК РФ Трудовой договор вступает в силу со дня его подписания работником и работодателем, если иное не установлено трудовым договором, либо со дня фактического допущения работника к работе с ведома или по поручению работодателя или его представителя. В соответствии со ст. 67 ТК РФ трудовой договор заключается в письменной форме, составляется в двух экземплярах, каждый из которых подписывается сторонами. Один экземпляр трудового договора передается работнику, другой хранится у работодателя. Получение работником экземпляра трудового договора должно подтверждаться подписью работника на экземпляре трудового договора, хранящемся у работодателя. Трудовой договор, не оформленный в письменной форме, считается заключенным, если работник приступил к работе с ведома или по поручению работодателя или его представителя. При фактическом допущении работника к работе работодатель обязан оформить с ним трудовой договор в письменной форме не позднее трех рабочих дней со дня фактического допущения работника к работе.

Таким образом, трудовой договор должен быть подписан руководителем или лицом, уполномоченным на это, и составлен в двух экземплярах.

В августе 2014 года с заработной платы гражданки К. были произведены удержания за нарушения сроков прохождения медицинского осмотра, хотя медицинский осмотр проходили все работники организации в одно время, и гражданка К. в том числе.

Затем в октябре того же года в организации была проведена проверка санитарно-эпидемиологической станцией, в результате которой в столовой была обнаружена кишечная палочка. За установленные нарушения санитарно-эпидемиологическая станция наложила на организацию штраф. Не понятно, по каким причинам за данное нарушение удержания были произведены только из заработной платы гражданки К.

В ноябре 2014 года так же с заработной платы гражданки К. были произведены удержания за то, что она помогала повару, в связи с тем, что последняя не успевала обслужить детей.

Таким образом, работодатель нарушил трудовое законодательство, которое устанавливает достаточно жесткие правила определяющие случаи, размеры и порядок удержаний из заработной платы работника. Далее в соответствии со ст. 136 ч.3 ТК РФ работодатель обязан при выплате заработной платы в письменной форме известить работника о размерах и основаниях удержаний.

Гражданка К. неоднократно обращалась в бухгалтерию организации по вопросу необоснованных удержаний, не получив ответа в бухгалтерии организации, она решила обратиться в Государственную инспекцию по труду Иркутской области, за консультацией о правомерности действий работодателя, но и там не получила ответа.

Проанализировав данную ситуацию мной была составлена жалоба в прокуратуру о необоснованных удержаниях с заработной платы.

В настоящее время в организации, где работала гражданка К. проводится прокурорская проверка.

Информация об авторе

Махазагдаева Алена Дагбасамбуевна – студентка, факультет государственного права и национальной безопасности, Байкальский государственный университет экономики и права, 664003, г.Иркутск, ул. Ленина,11, e-mail: makhazagdaeva_a@mail.ru.

Author

Makhazagdaeva Alena Dagbasambuevna – student, faculty of state law and national security, Baikal State University of Economics and Law, 11, Lenin str., Irkutsk, 664003, e-mail: makhazagdaeva_a@mail.ru.

УДК 349.3

М.Р. Бардаханов

ПРАВО НА ПРИСВОЕНИЕ ЗВАНИЯ «ВЕТЕРАН ТРУДА» И ПРОБЛЕМЫ, ВОЗНИКАЮЩИЕ ПРИ ЕГО РЕАЛИЗАЦИИ

В статьей раскрывается понятие «Ветеран труда», основания и порядок присвоения данного звания, перечисляются проблемы, возникающие при реализации указанного права.

Ключевые слова: ветеран труда, ВЛКСМ, ведомственные знаки отличия в труде.

M.R. Bardakhanov

THE RIGHT TO THE TITLE OF VETERAN LABOUR AND PROBLEMS ARISING FROM ITS IMPLEMENTATION

The article presents the concept of Veteran of labour, the grounds and the procedure for awarding this title, lists the problems arising from implementation of this right.

Keywords: veteran of labour, All-Union Leninist Young Communist League, departmental awards.

Некоторое время назад к нам в юридическую клинику обратилась женщина-пенсионер, как оказалось, с довольно-таки актуальным вопросом для данной категории населения – вопросом о присвоении ей звания ветеран труда. Для начала остановимся поподробнее на порядке и условиях присвоения данного звания, установленного законодательством.

В соответствии со статьей 7 ФЗ №5 от 12 января 1995 г. «О ветеранах» ветеранами труда признаются лица, награжденные ордена-

ми и медалями, либо удостоенные почетных званий СССР или РФ, либо награжденные ведомственными знаками отличия в труде и имеющие трудовой стаж, необходимый для назначения пенсии по старости или по выслуге лет.

Порядок и условия присвоения звания определяются законами и иными нормативными актами субъектов РФ. Присвоение звания также осуществляется исполнительными органами государственной власти субъектов РФ.

Согласно ст. 4 Закона Иркутской области «О порядке и условиях присвоения звания ветеран труда» (далее – закон Иркутской области)[1], к ведомственным знакам отличия в труде относятся учрежденные за особые отличия в труде и продолжительный добросовестный труд награждения, которые произведены: Правительством, руководителями федеральных органов исполнительной власти – министерств, ведомств; руководителем Администрации Президента; Советом Федерации, Государственной Думой, судебными органами и прокуратурой, государственными органами СССР. Как ведомственные также рассматриваются награды Академии наук РФ и СССР, Академии художеств, ДОССАФ, ЦК ВЛКСМ и ряда других организаций, при условии, что они непосредственно состояли их в штате.

Итак, наша посетительница, согласно законодательству, подала заявление и необходимые документы в управление соц. развития, опеки и попечительства Иркутской области. Основанием для получения данного звания она считает знак ЦК ВЛКСМ «Молодой гвардеец 11 пятилетки» второй степени, которым награждались комсомольцы, юноши и девушки за успешное выполнение плановых заданий и социалистических обязательств, достижение высоких показателей в социалистическом соревновании.

Министерство ответило на данное заявление отказом на основании следующего: 1) согласно пункту второму статьи 4 закона Иркутской области, награды ЦК ВЛКСМ рассматриваются как ведомственные отличия в труде при условии, что ими награждены работники, непосредственно состоявшие в штате указанных организаций (согласно записям в трудовой книжке). Документы, подтверждающие, что наша посетительница состояла в штате ЦК ВЛКСМ или работала в системе данной организации не были выявлены; 2) награда нашей посетитель-

[1] Об условиях и порядке присвоения звания «Ветеран труда» в Иркутской области: Закон Иркутской области №44/16-ЗС от 25 июня 2008 г. №44/16-ЗС [эл. ресурс] // http://edu.irkutsk.ru/data/1050/zakon_IO_veteran_truda.doc

ницы не является знаком отличия в труде, в части их учреждения за особые отличия и продолжительный добросовестный труд.

Наша посетительница не согласилась с данным ответом и обратилась в юридическую клинику за консультацией. Изучив законодательство и судебную практику по всей стране, мы посчитали отказ министерства необоснованным, потому что:

Во-первых, одно основание можно разрушить, предъявив архивную выписку с протокола заседания, на котором происходило награждение. Например, так, в схожей ситуации, поступил гражданин N в Мордовии, тем самым убедив суд в обоснованности своих притязаний; Также в аналогичном разбирательстве, судебная коллегия по гражданским делам Смоленского областного суда не посчитала подобное обоснование достаточным для отказа, поскольку данный знак вручался комсомольцам, независимо от их места работы.

Во-вторых, следующее основание мы и вовсе посчитали грубой ошибкой, ибо как может знак, выдаваемый за успешное выполнение своих обязанностей, не являться знаком отличия в труде?

При обзоре судебной практики мы заметили очень много интересных положений, которые позволили выявить основную проблему, возникающую при присвоении данного звания – отсутствие на федеральном уровне нормативных актов, устанавливающих критерии, предъявляемые к ведомственным знакам отличия в труде или примерный перечень наград, которые можно отнести к указанной категории знаков. Данный пробел законодательства порождает значительное различие в судебной практике, причем даже в пределах одного субъекта РФ.

Стоить отметить, что примерный перечень наград на федеральном уровне был установлен письмом Министерства труда от 7 октября 1998 года «О ведомственных знаках отличия в труде, учитываемых при присвоении звания «Ветеран труда», но оно было отозвано Министерством здравоохранения и социального развития РФ в 2008 году, которое проинформировало субъекты федерации о невозможности его дальнейшего использования. Несмотря на данное указание, суды общей юрисдикции продолжают его использование, поскольку никаких других ориентиров у них не имеется. Так, например, в 2014 году Кировский районный суд г. Иркутска, в своем определении сослался на этот перечень, в котором к ведомственным знакам отнесены знаки и грамоты РАО «ЕЭС России».

В упомянутом перечне также указан знак ЦК ВЛКСМ «Молодой гвардеец 11 пятилетки», что давало нам надежду на отмену решения министерства судом, поскольку нет гарантий, воспользуется ли перечнем один районный суд г. Иркутска, подобно другому, или примет решение, основываясь на положениях, закрепленных в законе.

Основываясь на выше перечисленных положениях и особенностях, мы составили для нашей посетительницы исковое заявление в суд.

Информация об авторе

Бардаханов Михаил Рубенович – студент, факультет государственного права и национальной безопасности, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина 11, e-mail: bardakhanovmichael@mail.ru.

Author

Bardakhanov Mikhail Rubenovich – student, the faculty of the state law and national security, Baikal State University of Economics and Law, 11 Lenin str. Irkutsk, 664003, e-mail: bardakhanovmichael@mail.ru.

ПРОБЛЕМЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ: НАУЧНЫЕ ЭССЕ, ПРЕДСТАВЛЕННЫЕ НА МЕЖДУНАРОДНЫЙ КОНКУРС СТУДЕНЧЕСКИХ НАУЧНЫХ РАБОТ*

В начале года Байкальским государственным университетом экономики и права был объявлен конкурс научных студенческих работ (эссе) «Проблемы борьбы с киберпреступостью», в котором могли принять участие студенты, обучающиеся по программе бакалавриата, специалитета, магистратуры, а также аспирантуры.

Конкурс студенческих научных работ проводился в **целях**:

– создания и развития условий, обеспечивающих возможность для каждого студента реализовать свое право на творческое развитие личности и участие в научных исследованиях;

– активизации научных исследований по актуальным направлениям развития науки криминалистики, уголовного процесса и криминологии;

– обеспечения единства образовательного, научного, практического и воспитательного процессов с формированием и развитием творческих способностей, улучшением профессионально-творческой подготовки студентов, совершенствованием форм привлечения молодежи к научным исследованиям.

Участникам конкурса были предложены следующие научные темы:

– киберпреступность как социальное явление;

– актуальные криминологические проблемы исследования киберпреступности на современном этапе;

– криминалистическая характеристика киберпреступлений;

– личность киберпреступника;

– общие вопросы организации расследования киберпреступлений;

– тактика производства отдельных следственных действий при расследовании киберпреступлений.

* *Данный раздел подготовлен в рамках реализации договора № 14.Z56.14.2691-МД об условиях использования гранта Президента Российской Федерации для государственной поддержки молодых российских ученых с организациями – участниками конкурсов, имеющими трудовые отношения с молодыми учеными МД-2691.2014.6.*

Проведя анализ и оценку представленных на конкурс научных эссе, экспертная конкурсная комиссия с особым чувством удовлетворения отметила обширную географию участников, высокий научно-технический уровень конкурсных эссе, глубокую степень осведомленности авторов по исследуемым вопросам, а также разносторонность поднятых проблем. Все это в полной мере показывает необходимость борьбы с киберпреступлениями и расширения арсенала правоприменителей, серьезный уровень подготовки участников конкурса.

На основании вышеизложенного конкурсной комиссией было принято решение о целесообразности опубликования представленных на конкурс научных эссе.

Победителями конкурса стали:

I место

Козленко Виктория Витальевна

Научный руководитель: Земцова Светлана Игоревна

Тема работы «К вопросу о расследовании преступлений, связанных со сбытом наркотических средств и психотропных веществ с использованием сети «Интернет» (ФГКОУ ВПО «Сибирский юридический институт Федеральной службы Российской Федерации по контролю за оборотом наркотиков»)

II место

Земзикова Екатерина Юрьевна

Научный руководитель: Васюков Виталий Федорович

Тема работы: «Особенности изъятия электронных носителей информации при производстве выемки» (ФГКОУ ВПО «Орловский юридический институт МВД РФ им. В.В. Лукьянова»)

III место

Пахорукова Юлия Евгеньевна

Научный руководитель: Карлов Андрей Леонидович

Тема работы: «Правовая оценка использования различных средств процессуального закрепления в качестве доказательств электронной переписки в сети Интернет» (ФГКОУ ВПО «Сибирский юридический институт Федеральной службы Российской Федерации по контролю за оборотом наркотиков»)

Также необходимо отметить ряд работ по следующим номинациям:

«***Развитие и укрепление международного сотрудничества в области образования***»:

Абенова Кымбат Есмуханбетовна (Карагандинский государственный университет им Е.А.Букетова (Казахстан) юридический факультет)

Лашина Дарья Александровна (Белорусский государственный университет Юридический факультет)

Санок Елена Эдуардовна (Белорусский государственный университет Юридический факультет)

«Научная самостоятельность»:

Измайлов Алексей Викторович («Саратовская государственная юридическая академия». Институт правоохранительной деятельности»)

«Креативность мышления»:

Агапов Даниил Владиславович (ФГКОУ ВПО КрУ МВД России факультет по подготовке следователей)

«Развитие и укрепление региона»:

Макушев Дмитрий Иванович (ФГКОУ ВПО «Академия Генеральной прокуратуры Российской Федерации» Иркутский юридический институт (филиал)

Скуратовский Алексей Юрьевич (ФГКОУ ВПО «Академия Генеральной прокуратуры Российской Федерации» Иркутский юридический институт (филиал)

Цынгеева Бимбасо Солбоновна (ФГБОУ ВПО «Российский государственный университет правосудия»» Иркутский филиал)

Черных Анастасия Юрьевна (Иркутский юридический институт (филиал) ФГБОУ «Российская правовая академия Министерства юстиции Российской Федерации»)

Следует отметить, что в данном разделе научные эссе конкурсантов публикуются вне зависимости от занятого места или принадлежности к указанным номинациям. Очередность опубликования работ обусловлена их тематическим содержанием.

Все работы представлены в авторской редакции.

УДК 343.9

К. Абенова
Научный руководитель: З.Б. Жуманбаева

КИБЕРПРЕСТУПНОСТЬ КАК ПОТЕНЦИАЛЬНАЯ УГРОЗА ВСЕГО МИРА

Из всех криминальных действий, самая глобальная проблема и непонятная это киберпреступность. Такие преступления трудно отследить, и несомненно тяжело проследить какие антивирусные программы на данный момент лучше и от чего именно они защищают. Мы сейчас попали в тот период когда компьютеры и системы новейших технологий практически овладели всем миром. Но сами люди не предполагли того, что созданная ими технология превзойдет все, и наступит то время, когда она будет направлена против самих же себя. Сегодня безопасность тысяч пользователей может оказаться в зависимости от нескольких преступников. Количество киберпреступности несомненно растет, и мы, молодое общество должны противостоять этому всеми силами.

Сейчас наша жизнь и работа пребывает в таком состоянии, где одним из ценнейших ресурсов становится информация, где во главе приходится ставить информационные технологии. Причем это становится не только удобно, но, прежде всего, недорого и быстро. Но, минус в том, что этими полезными вещами начинают пользоваться недобросовестно. Поэтому многим приходится сталкиваться с термином «киберпреступление». Итак, что же представляет собой «киберпреступность»?

Киберпреступность – это преступность в так называемом виртуальном пространстве. Виртуальное пространство, или киберпространство можно определить как моделируемое с помощью компьютера информационное пространство, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в математическом, символьном или любом другом виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого физического или виртуального устройства, а также другого носителя, специ-

ально предназначенного для их хранения, обработки и передачи. Это определение соответствует рекомендациям экспертов ООН [1; 2].

Термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Следует различать киберпреступления как правовую категорию и киберпреступность как социальное явление. Последнее включает в себя не только совокупность всех данных преступлений, но и различные формы тесно связанных с ними «поддерживающей» и организационной деятельности. В этом смысле обмен электронной почтой между лицами, готовящими преступление, размещение соответствующей криминально ориентированной информации на web-сайтах также относятся или, во всяком случае, примыкают к киберпреступности как социальному явлению. Профилактика и борьба с преступлениями в сфере компьютерных технологий или совершенных с помощью компьютерных информационных систем требует иного подхода, нежели к борьбе с обычными преступлениями «существующими веками»[3].

Говоря об особенностях киберпреступности, возникает целый комплекс технических и юридических проблем, связанных с отсутствием:

1. Законодательных актов, регулирующих уголовно-процессуальные действия;

2. Специально подготовленных кадров (оперативного и следственного аппарата, специализирующегося на выявление и раскрытие преступлений в информационно-телекоммуникационной сфере);

3. Необходимых технических средств.

Преступления, совершаемые в глобальных информационных сетях или посредством компьютерных информационных технологий, практически не поддается расследованию, так как отследить хакера практически можно в течение 15 минут. Если правоохранительные органы не уложились в 15 минут, то с помощью программы «скользящего IP-адреса» хакер имеет возможность скрыться [4].

Следует сделать следующий подход для пресечения таких преступлений:

1. Не выкладывать в социальные сети важные документы, фотографии;

2. Вести непрерывную борьбу против противоправного содержания информации и противоправного поведения в сети Интернет;

3. Регулирование электронных сообщений.

4. Когда выявляются признаки киберпреступности всевозможно отключить свет и интернет, в тех местах где выявляются эти признаки.

Повысить плату за пользование интернетом, так как не все могут позволить себе, а все эти махинации совершаются в большинстве случаев из-за тяжелого материального положения, допустим не каждый будет идти в интернет салон и совершать преступления, так как там сразу будет это фиксироваться, следовательно преступнику будет намного тяжелее совершить злодеяние.

Само понятие «киберпреступность» и правовые нормы против этого преступления распространено не во всех странах мира. Учитывая всю сложность и опасность киберпреступлений, необходима выработка совместных действий ученых-юристов, и конечно же законодателей и специалистов в области компьютерных информационных технологий, направленных на борьбу с преступлениями в глобальных информационных сетях. Так как внедрение нормативного акта, как национального, так и международного характера недостаточный шаг на пути решения проблемы борьбы с киберпреступностью, в данном случае необходимы специальные знания информационных технологий и программного обеспечения.

Мы максимально должны фиксировать эти преступления и пресекать их, и конечно же, существуют различные информации в различных литературах мира по развитию технологии, в следствии чего, преступники развивают новые навыки по совершенствованию своих замыслов. Непосредственно в людях мы должны выработать дружелюбие, честность, и то что нельзя совершать такие преступления. Но, хотела бы отметить что многие, кто совершает такие преступления могут быть и сами сотрудники данного учреждения. Все это зависит от человеческих качеств развития, воспитания и психологии человечества. Если же человек растет вполне нормальной, достаточной в материальных средствах семье, то он не будет совершать такие преступления. А сейчас практически все происходит из-за большинства безработных людей, это объясняется тем что, в Советский Союз безработицы не было, и все были в достатке и мире, а на данный момент это проблема безработицы перешла на совершение таких преступлений в которых быстро можно добиться легких денег.

Пресечь киберпреступность, я предполагаю нужно с самого корня, то есть, задасться таким вопросом «Почему на самом деле они

совершаются, и с какой целью?». Предотвращая такие преступления мы постепенно положим конец таким правонарушениям.

Список использованной литературы

1. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. … канд. юрид. наук. Владивосток, 2005. 27 с.

2. Конвенция о компьютерных преступлениях (Будапешт, 23 ноября 2001 года).

3. Щетилов А. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом // Официальный сайт Центра исследований компьютерных преступлений http://www.crime-research.ru/library/chetilov.htm.

4. Багдеева В.А. Проблемы международной киберпреступности // Материалы работ победителей конкурса на соискание грантов содружества выпускников МГЮА в 2008 году www.nbpublish.com/view_articles/20675.pdf.

Информация об авторе

Абенова Кымбат – студентка, Карагандинский государственный университет им Е.А. Букетова (Казахстан), юридический факультет, email:kimka.kz@mail.ru

УДК 343.9

Д.И. Макушев
Научный руководитель: К.Н. Евдокимов

КИБЕРПРЕСТУПНОСТЬ КАК СОЦИАЛЬНОЕ ЯВЛЕНИЕ

Одной из социальных проблем современного российского общества явилось возникновение и активное развитие киберпреступности, причиняющей колоссальный вред существующим экономическим, политическим, культурным, научным, образовательным и информационным отношениям в Российской Федерации.

Все более актуальным становится вопрос об информационной безопасности граждан, муниципальных и государственных учрежде-

ний, предприятий, органов власти от несанкционированного доступа к компьютерной информации, вредоносных компьютерных программ и иных компьютерных угроз.

Масштабы ущерба, причиняемого компьютерными преступлениями, впечатляют. Так, по оценкам аналитиков компании Group-IB объем рынка киберпреступности в Российской Федерации в 2012 году составил 1,93 млрд дол. [12], а с середины 2013 по середину 2014 года в России и СНГ русскоговорящие хакеры «заработали» 2,5 млрд дол., что составляет 2 % от глобального рынка [13].

В свою очередь, американская корпорация Symantec оценила ущерб от киберпреступности в России за 2013 год в 1 миллиард долларов, а в 2012 году в 1,48 миллиарда долларов. При этом общий ущерб от киберпреступности в мире в 2013 году составил 113 млн дол. [14].

По данным исследования CostofCyberCrimeStudy, проведенного компанией PonemonInstitute при поддержке HP EnterpriseSecurity, среднегодовой ущерб российской организации от киберпреступлений в 2014 году достигает 3,3 млн дол. [15].

По данным «Лаборатории Касперского», в мире ежедневно появляется до 70 тыс. вредоносных программ. При этом, за последний год в 96 % российских компаний фиксировались инциденты в области IT-безопасности. Больше половины опрошенных специалистов признали факт потери данных в результате заражения вредоносным программным обеспечением. При этом чаще всего инциденты в области IT-безопасности приводят к потере данных о платежах (13 %), интеллектуальной собственности (13 %), клиентских баз (12 %) и информации о сотрудниках (12 %) [16].

Поэтому в настоящее время борьба с киберпреступностью является одним из главных направлений деятельности правоохранительных органов по обеспечению информационной безопасности российского общества.

Что же понимать под киберпреступностью и как она соотносится с понятием «компьютерная преступность?

В настоящее время существует несколько подходов к определению понятия «компьютерная преступность».

Во-первых, компьютерная преступность – это совокупность преступлений, в которых предметом преступных посягательств выступает компьютерная информация. При этом понятия компьютерное

преступление и преступление в сфере компьютерной информации являются синонимами [1, с. 9].

Во-вторых, компьютерная преступность – это совокупность совершенных на определенной территории за определенный период преступлений (лиц, их совершивших), непосредственно посягающих на отношения по сбору, обработке, накоплению, хранению, поиску и распространению компьютерной информации, а также преступлений с использованием компьютера в целях извлечения материальной выгоды или иной личной заинтересованности [8, с. 39].

В-третьих, компьютерная преступность – это совокупность всех преступлений в сфере «информационных технологий», а не только общественно опасных деяний, предметом которых является компьютерная информация [2, с. 45–46].

В-четвертых, компьютерная преступность – это совокупность преступлений, совершаемых с помощью компьютерной системы или сети, в рамках компьютерной системы или сети и против компьютерной системы или сети. Данный подход предполагает, что кроме преступлений в сфере компьютерной информации, компьютерными преступлениями также являются и преступления, связанные с компьютерами. То есть такие традиционные по характеру преступные деяния, совершенные с помощью вычислительной техники, как кража, мошенничество, причинение вреда и некоторые другие, за которые предусматриваются уголовные санкции в законодательствах большинства стран [6, с. 18–19].

Между тем, в ряде научных работ российских авторов можно встретить упоминание о «киберпреступности», юридическом понятии, которое часто употребляется в научном обороте за рубежом и более полно отражает преступные деяния в сфере компьютерной информации, а также преступления, совершенные с помощью компьютерных устройств, информационно-телекоммуникационных сетей и информационных технологий.

Поэтому, пятый подход предполагает, что компьютерная преступность является только частью киберпреступности, как более широкого понятия.

Например, Т.Л. Тропина считает, что понятие «компьютерная преступность» недостаточно для охвата всех деяний, совершаемых при помощи вычислительной техники, глобальных сетей. Киберпреступность, по ее мнению, – это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компью-

терных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, сетей или данных [9, с. 36].

Схожей позиции придерживается И.Г. Чекунов, считая, что киберпреступность предлагается рассматривать в качестве самостоятельного вида преступности, определяемого на основе обнаружения обязательного присутствия в преступлениях таких признаков объективной стороны, как средство или орудие, в качестве которых выступает вредоносная компьютерная программа или программно-техническое средство, подключенное к компьютерной сети или сотовому оператору связи [11, с. 7].

Таким образом, по-нашему мнению, понятие «компьютерная преступность» целесообразно рассматривать в широком и узком значениях.

Компьютерная преступность в «узком смысле» представляет собой совокупность преступлений, где в качестве непосредственного основного объекта преступного посягательства выступают охраняемые законом общественные отношения в сфере безопасного создания, хранения, обработки и передачи компьютерной информации, а предметом преступления являются компьютерная информация, средства защиты компьютерной информации, информационно-телекоммуникационные сети, средства хранения, обработки и передачи компьютерной информации.

Компьютерная преступность в широком смысле представляет собой совокупность преступлений, где основным непосредственным объектом преступного посягательства выступают общественные отношения в сфере компьютерной информации и информационных технологий, безопасного функционирования средств создания, хранения, обработки, передачи, защиты компьютерной информации, но при этом компьютерная информация, информационно-телекоммуникационные сети являются не только предметом преступного деяния, но и используются в качестве средства и орудия совершения преступления.

К характерным чертам киберпреступности относят следующие [10, с. 40]:

– уголовная наказуемость деяния и запрещенность его уголовным законом;

– неправомерное использование информационных коммуникационных технологий (ИКТ);

– выход за национальные границы (трансграничность);

– активная динамика использования высоких технологий;

– преступления совершаются скрытно и могут иметь как длящийся, так и разовый, одномоментный характер;

– масштабность правонарушений;

– сложность сбора доказательств и осуществления процессуальных действий;

– большая латентность, проблемы юрисдикционности, экстрадиции;

– субъектом противоправного деяния является интеллектуально развитый и высокопрофессиональный специалист в области IT-технологий;

– преступления в основном совершаются для достижения экономических целей, и зачастую в особо крупных размерах;

– наличие возрастающей и устойчивой тенденции к «организованности» киберпреступности, групповом характере совершения таких правонарушений.

Рассмотрев основные черты киберпреступности, представляется целесообразным провести классификацию киберпреступлений. Например, по объекту правонарушения выделяют четыре основные группы [10, с. 42].

В первую группу преступлений, т.е. преступлений, направленных против конфиденциальности, целостности и доступности компьютерных данных и систем, входят: «незаконный доступ», «незаконный перехват», «воздействие на компьютерные данные или системы».

Во вторую группу входят преступления, непосредственно связанные с использованием компьютерных средств. К ним относятся «подлог» и «мошенничество с использованием компьютерных технологий».

Третью группу составляют преступления, связанные с содержанием данных. Речь здесь идет о производстве, предложении и (или) предоставлении в пользование, распространении и приобретении, а также владении детской порнографией, находящейся в памяти компьютера.

В четвертую группу вошли преступления, связанные с нарушением авторского права и смежных прав.

В соответствии с Уголовным кодексом Российской Федерации, к компьютерным преступлениям относятся такие преступные деяния, как:

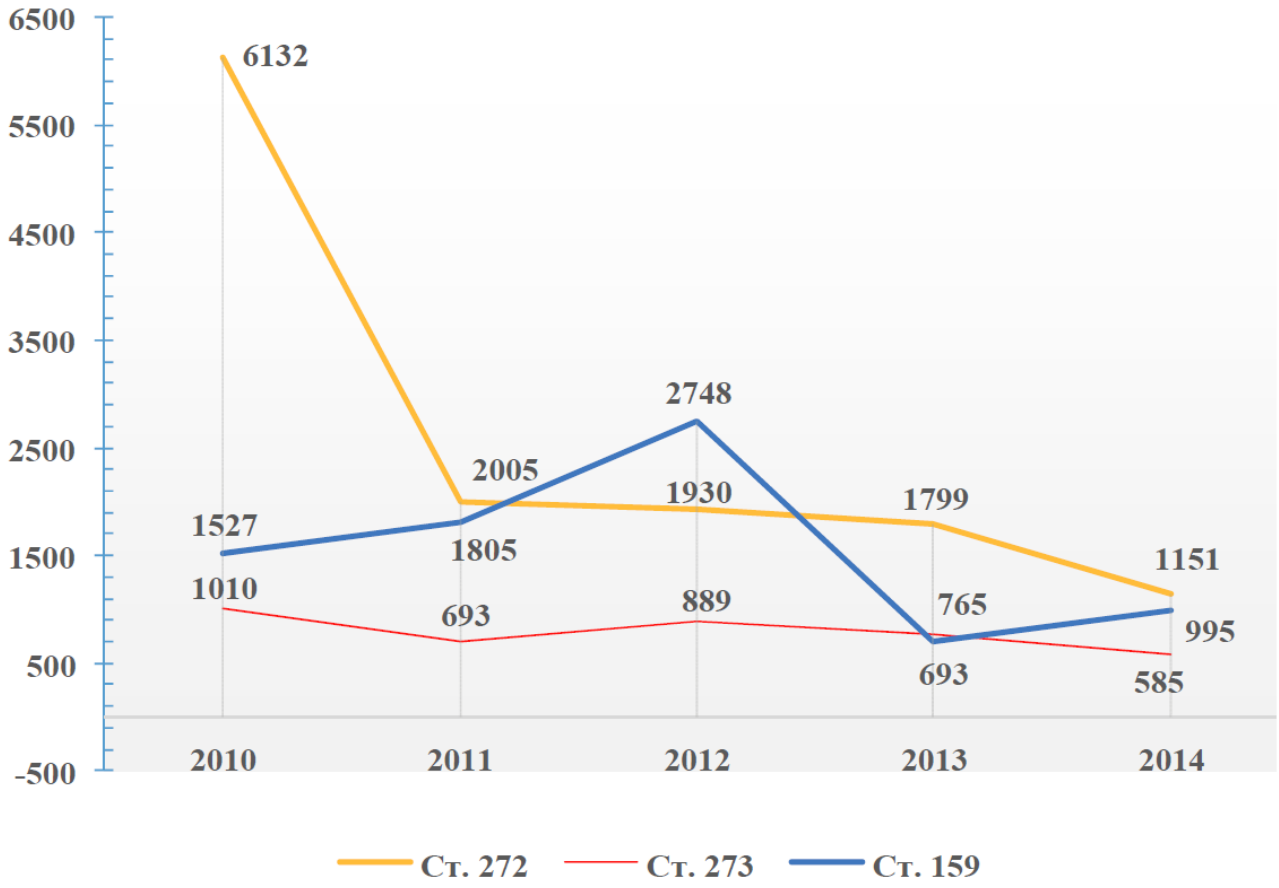
1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ);

2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);

3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ);

4. Кража, совершенная с использованием компьютерных и телекоммуникационных технологий (ст. 158 УК РФ) и другие.

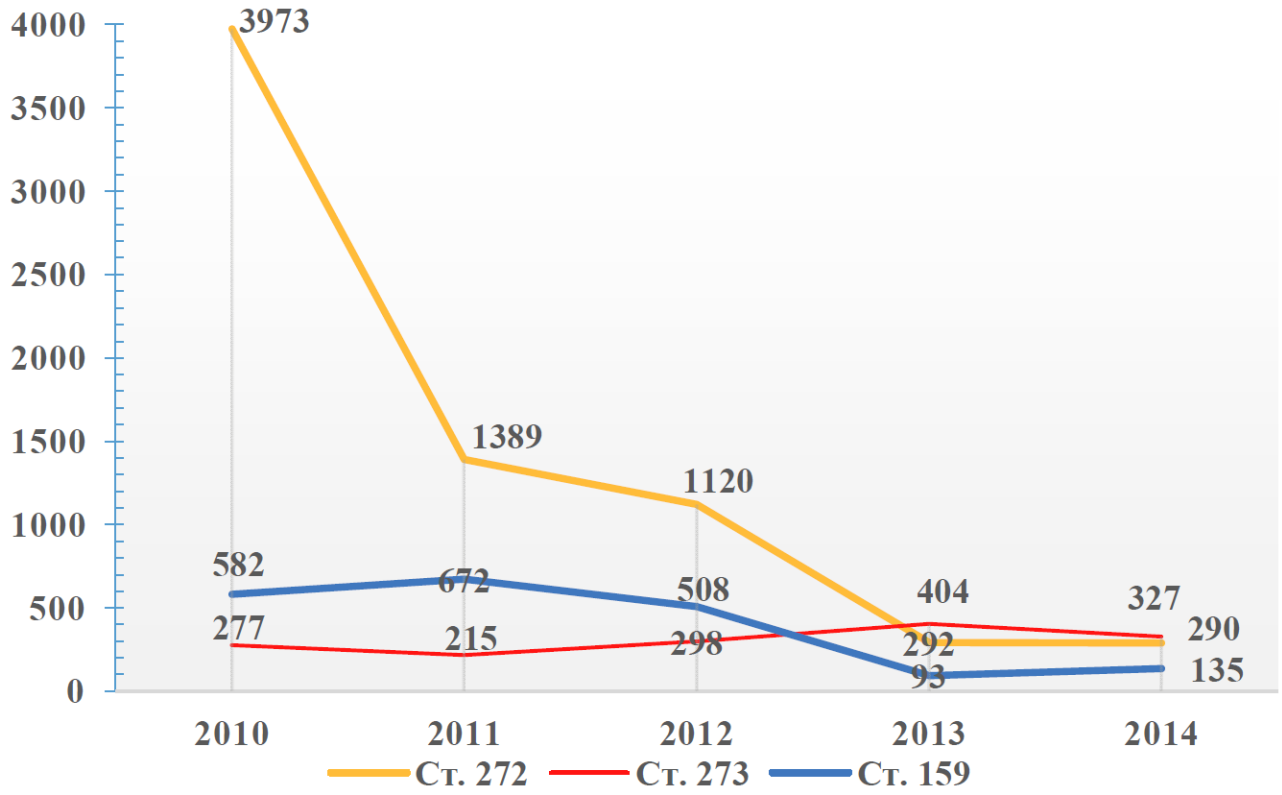
Рассмотрим динамику количества зарегистрированных преступлений в рассматриваемой сфере.



Количество преступлений
зарегистрированных в отчетном периоде

Исходя из данный представленной диаграммы, можно наблюдать снижение количества зарегистрированных преступлений, что свидетельствует о латентном состоянии киберпреступности в России .Говоря о динамике развития компьютерной преступности 2015 году, ожидается рост количества атак на правительственные сайты и сайты

средств массовой информации для продвижения социальных и политических идей; рост атак на банкоматы, банки и финансово-кредитные организации; а также увеличение количества заражений POS-терминалов и мобильных устройств.



Выявлено лиц, совершивших преступления в России

На данном графике прослеживается снижение раскрываемости компьютерных преступлений. Это свидетельствует о трудностях в расследовании дел и поиске виновных лиц.

С учетом вышеизложенного, следует отметить, что в узком значении понятие «компьютерные преступления» полностью совпадает с установленным законодателем понятием «преступления в сфере компьютерной информации». В «широком смысле» компьютерная преступность больше по объему и содержанию таких понятий как «киберпреступность», «интернет-преступность», «преступность в сфере компьютерной информации», включая их в себя в качестве составных элементов.

Наиболее подходящим видится определение киберпреступности как совокупности преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках

компьютерных систем или сетей, а также против компьютерных систем, компьютерных сетей и компьютерных данных. К киберпреступлению, на наш взгляд, относится любое преступление, совершенное с применением электронных способов и средств.

В связи с тем, что киберпреступность имеет трансграничный характер, для эффективного противодействия таким преступлениям необходима организация эффективного взаимодействия различных государств. Также необходимо внутригосударственное сотрудничество в целях противодействия данному явлению. Необходимо совершенствование методик выявления преступлений и способов поиска виновных лиц. Как социальное явление, киберпреступность приникает во все сферы жизни общества, и в руках умелого пользователя может принести ему большую пользу или существенный вред как отдельным лицам, так и мировому сообществу в целом.

Список использованной литературы

1. Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): автореферат дисс. ... канд. юрид. наук. Махачкала, 2004.

2. Добровольский Д. В. Актуальные проблемы борьбы с компьютерной преступностью: дис. … канд. юрид. наук: 12.00.08. М., 2005.

3. Евдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации // Академический юридический журнал. 2015. № 1 (59). С. 21–31.

4. Евдокимов К.Н. Политические факторы компьютерной преступности в России // Информационное право. 2015. № 1. С. 41–47.

5. Евдокимов К.Н. Причины компьютерной преступности в современной России // Российский следователь. 2015. № 3. С. 33–37.

6. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. … канд. юрид. наук: 12.00.08. М., 2003.

7. Липинский Д.А., Евдокимов К.Н. Политические причины как современные факторы эволюции компьютерной преступности в Российской Федерации // Криминологический журнал Байкальского государственного университета экономики и права. 2015. Т. 9. № 1. С. 101–110.

8. Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. ... д-ра юрид. наук: 12.00.08. М.: РГБ, 2007.

9. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. … канд. юрид. наук: 12.00.08. Владивосток, 2005.

10. Чекунов И.Г. Киберпреступность : понятие и классификация // Российский следователь. 2012. № 2.

11. Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореферат дис. … канд. юрид. наук: 12.00.08. М, 2013.

12. URL:http://digit.ru/business/20130910/405335397.html#ixzz2r1xUjpbf.

13. URL: http://www.group-ib.ru/index.php/investigation/1063-link-nezavisimye.

14. URL: http://go.symantec.com/norton-report-2013.

15. URL: http://www.octree.co.uk/Documents/2014-Global-Report-on-the-Cost-of-Cybercrime.pdf.

16. URL: http://www.kaspersky.ru/downloads/pdf/kaspersky_ security_network.pdf.

Информация об авторе

Макушев Дмитрий Иванович – студент, ФГКОУ ВПО «Академия Генеральной прокуратуры Российской Федерации» Иркутский юридический институт (филиал).

УДК 343.9

А. Смолякова
Научный руководитель: С.И. Земцова

КИБЕРТЕРРОРИЗМ – УГРОЗА XXI ВЕКА

Мы живем в эпоху информационного общества, когда компьютеры и телекоммуникационные системы используются во всех сферах жизнедеятельности человека и государства – от решения проблем на-

циональной безопасности, здравоохранения и управления транспортом до торговли, финансов, и даже просто межличностного общения.

Практически каждый человек на нашей планете стал зависим от информационных технологий. И эти технологии не стоят на месте. Значит, очень скоро в зависимость попадут буквально все жители Земли. Поэтому для каждого будет очень интересно взглянуть со стороны на одну из главных опасностей, которая поджидает сейчас и в будущем – кибертерроризм.

По данной теме, интересно мнение главы «Лаборатории Касперского» Евгения Касперского: «Мир в настоящее время входит в эпоху кибертерроризма, а компьютерная безопасность становится такой же важной, как физическая или экономическая безопасность. Люди уже сейчас повсеместно ощущают на себе эту угрозу. Полномасштабные кибератаки и кибертерроризм станут для жителей планеты самым настоящим «глобальным шоком».

Причем речь, отмечает он, идет вовсе не о компьютерных вирусах, троянах или распространении порнографии. Под угрозой находятся более серьезные объекты: ядерные системы. При этом глава «Лаборатории Касперского» обратил внимание на тот факт, что в мире не существует государства, которое было бы защищено от такого рода атак.

Касперский выразил озабоченность тем, что далеко не все представляют себе масштаб исходящей угрозы. «Физическим миром управляют компьютеры», и, к сожалению, довольно просто подвергнуть атаке эти довольно простые системы. «Речь идет как о физическом разрушении, так и о сознательном производстве с дефектами», – отметил он, добавив, что компьютерные системы сейчас управляют всем – и шахтами, и космическими станциями.

«Многие попросту не понимают, насколько в наши дни легко и дешево организовать кибератаку», – продолжил он. «Достаточно нескольких инженеров, компьютерщиков и небольшой бюджет, чтобы спроектировать эту атаку. И вы даже не будете знать, кто или что за ней стоит», – резюмировал Касперский [1].

В настоящее время в литературе встречаются различные трактовки понятия кибертерроризм. По-моему мнению, самым полным определением компьютерного терроризма является: «преднамеренная, политически мотивированная атака на информацию, обрабатываемая компьютером, компьютерная система и сеть, которая создает опасность для жизни или здоровья людей или наступления других

тяжких последствий, если такие действия были содеянные с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта» [2].

В связи с тем, что виртуальное пространство не имеет границ, мерами противодействия и пресечения кибертерроризма озабочены различные органы и организации международного уровня: ООН, Совет Европы, Международная организация экспертов, Интерпол. В России в этом направлении работают такие службы, как ФСБ, МВД, Служба информационной безопасности, Центра анализа террористических угроз.

Совет Европы в 2001 г. принял Конвенцию «О киберпреступности», которую также подписали США и Япония. Конвенция определяет перечень преступлений, совершаемых в информационной сфере, против информационных ресурсов или с помощью информационных средств и признает их киберпреступлениями. К таким преступлениям, в частности, относятся: незаконный доступ, незаконный перехват, вмешательство в данные и в систему, подлог и мошенничество с использованием информационных технологий, покушение, соучастие или подстрекательство к совершению преступления.

Но в настоящее время выполнение положений Конвенций Совета Европы 2001 г. уже недостаточно для эффектного противодействия террористам. Назрела объективная потребность выработки в различных странах мира законодательств и принятия мер для борьбы с кибертерроризмом. Так, 18 января 2013 г. в Гааге официально открыт Европейский центр по борьбе с киберпреступностью. Он будет заниматься сбором и обработкой данных по киберпреступлениям, производить экспертную оценку интернет-угроз, а также разрабатывать и внедрять передовые методы профилактики и расследования киберпреступлений, готовить новые кадры, оказывать помощь правоохранительным и судебным органам, а также координировать совместные действия заинтересованных сторон, направленные на повышение уровня безопасности в европейском киберпространстве [4].

Таким образом, задача обеспечения информационной безопасности (кибербезопасности) стала одной из ключевых для большинства мировых держав.

В связи с этим возникает вопрос: каким образом осуществляются законодательные меры противодействия российского кибертерроризма и какие исполнительные органы осуществляют данные меры?

Так, 05.10.2009 года Президент Российской Федерации утвердил Концепцию противодействия терроризму в Российской Федерации. В соответствии с которой, предупреждение (профилактика) терроризма предполагает противодействие распространению идеологии терроризма путем:

– обеспечения защиты единого информационного пространства Российской Федерации;

– совершенствование системы информационного противодействия терроризму;

– усиление взаимодействия федеральных органов исполнительной власти и укрепление международного сотрудничества в области противодействия терроризму.

К основным мерам по его предупреждению (профилактике) относятся информационные – разъяснение сущности терроризма и его общественной опасности, формирование стойкого неприятия обществом идеологии насилия, а также привлечение общественности к борьбе с ним[1].

В Федеральном законе от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а именно в статье 10 пункте 6 сказано: «запрещено распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность»[2].

В соответствии со статьями 12-13 Федерального закона от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности», запрещается использование сетей связи общего пользования для осуществления экстремистской деятельности, а также распространение экстремистских материалов, их производство или хранение в целях распространения[3].

С 1 июня 2012 года действует Федеральный закон № 436-ФЗ «О защите детей от информации, причиняющий вред их здоровью и развитию», который направлен на защиту детей от разрушительного,

---

[1] Концепция противодействия терроризму от 05 октября 2009 г. [Электронный ресурс] // Режим доступа: Консультант Плюс.

[2] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

[3] О противодействии экстремистской деятельности: Федеральный закон от 25 июля 2002 г. № 114-ФЗ // Собрание законодательства РФ.2002. № 30. Ст. 3031.

травмирующего их психику информационного воздействия, а также от информации, способной развить в них порочные наклонности[1].

Также, в Правительстве Российской Федерации обсуждается вопрос о криминализации неправомерного доступа к государственным информационным системам и содержащимся в них информационным ресурсам, в том числе, размещенным в сети Интернет или функционирующим в составе критически важных объектов.

Кроме того, в июне 2012 года Минкомсвязи подготовило поправки в ст. 20.29 КоАП РФ, предусматривающие штраф в размере от 1 до 3 тыс. руб. или административный арест до 15 суток за проставление гиперссылок на экстремистские материалы.

В настоящее время можно выделить еще несколько мер по противодействию кибертерроризма, которые активно разрабатывают и принимают органы власти Российской Федерации:

В июле 2013 года президент России Владимир Путин подписал документ «Основы государственной политики России в области международной информационной безопасности на период до 2020 года», определяющий политику страны в сфере обеспечения международной информационной безопасности.

В документе выделены четыре основные угрозы для РФ в этой сфере:

– первая – использование информационно-коммуникационных технологий в качестве информационного оружия в военно-политических целях, для осуществления враждебных действий и актов агрессии;

– вторая – применение ИКТ в террористических целях;

– третья – киберпреступления, включая неправомерный доступ к компьютерной информации, создание и распространение вредоносных программ;

– четвертая угроза, обозначенная в документе, отражает чисто российский подход – речь идет об использовании интернет-технологий для «вмешательства во внутренние дела государств», «нарушения общественного порядка», «разжигания вражды» и «пропаганды идей, подстрекающих к насилию» [5].

12 декабря 2014 года Президент РФ утвердил нормативный документ под названием «Концепция государственной системы обнаруже-

[1] О защите детей от информации, причиняющий вред их здоровью и развитию: Федеральный закон от 29 дек. 2010 г. № 436-ФЗ // Собрание законодательства РФ. 2011. № 1. Ст. 48.

ния, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Согласно «Концепции…» данная Система описывается как «единый централизованный, территориально распределенный комплекс», в состав которого входят силы (уполномоченные силовые подразделения) и средства (технологические решения) обнаружения, предупреждения и ликвидации последствий компьютерных атак. А также перечислены 12 функций по обеспечению информационной безопасности интернет-ресурсов, возложенных на систему. Основная цель системы в «Концепции» – защита сайтов госорганов (информационных ресурсов РФ) [3].

Ясно одно, данное явление, возникшее лишь несколько десятилетий назад, охватывает все новые сферы деятельности человека, растет быстрыми темпами и требует принятия адекватных и своевременных мер реагирования, как на национальном, так и на международном уровне.

Кибертерроризм – неизбежное следствие глобализации информационных процессов. Простота, легкость, анонимность, доступность и экономия времени – качества, делающие информационные технологии привлекательными для человечества – не могли не привлечь к себе внимания лиц, осуществляющих противоправную деятельность. С ростом использования информационных технологий в различных областях деятельности человека растет и использование их в целях совершения преступлений.

Этот рост также является неизбежным процессом, поскольку законодательное регулирование отношений в сфере информационных технологий не может ни опередить их развитие, ни даже идти с ним в ногу.

Список использованной литературы

1. Аркадий А. Миру предрекли эпоху кибертерроризма. 14.09.2012 г. URL: http://www.utro.ru/articles/2012/09/14/1071860.shtml.

2. Голубев. В.А. Проблемы борьбы с кибер-терроризмом в современных условиях. URL: http://www.crime- research.org/library/e-terrorism.htm.

3. Киберпреступность и киберконфликты. URL:http://www. tadviser.ru/index.php/.

4. Кибертерроризм: угроза национальной и международной безопасности. 14.03.13 г. URL: http://www.arms-expo.ru/news/archive/

kibertmezhdunarodnoy-bezopasnosti14-03-2013-18-35-00/mezhdunarodnoy-bezopasnosti14-03-2013-18-35-00/.

5. Россия определила главные киберугрозы. 01.08.2013 г. URL: http://www.dni.ru/tech/2013/8/1/257246.html.

Информация об авторе

Смолякова Алена – студентка, ФГКОУ ВПО Сибирский юридический институт ФСКН России, e-mail: smolyakova.alena@mail.ru.

УДК 343.98

А.Ю. Черных
Научный руководитель: И.В. Медведев

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА КИБЕРПРЕСТУПЛЕНИЙ

Информационные преступления – одна из наиболее важных и актуальных тем на сегодняшний день. В рамках расследования таких преступлений важно определить их криминалистическую характеристику. Проблема криминалистического раскрытия и расследования преступлений в сфере информационных технологий приобретает особую значимость в современный период российского общества, ведь решение таких проблем представляет задачу более сложную, чем задачи об их предупреждении. Общеизвестно, что информационные технологии стали неотъемлемой частью практически всех сфер жизни общества. Но есть ли обеспеченная защита граждан от преступлений в этой сфере? Вслед за совершенствованием информационных технологий повышается число пользователей компьютерных сетей, количество киберпреступников и, как следствие, создание очередных угроз для информационных систем и общества в целом.

Для успешного раскрытия любого вида преступления следователю необходимо проникнуть в его сущность, то есть дать его криминалистическую характеристику и понимание именно этого вида методики следственных действий позволяет в каждом конкретном случае выбрать наиболее продуманные его направления, средства и методы.

Таким образом, криминалистическая характеристика носит вспомогательный характер, облегчающий решение задач криминалистической деятельности.

Нужно иметь в виду, что понятия «киберпреступление», «информационное преступление» и «компьютерное преступление» по своей сути являются синонимами.

Киберперступность – это совокупность преступлений, совершаемых в так называемом киберпространстве. Значит, преступление, совершенное в киберпространстве – это виновное противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ [5].

Типовую криминалистическую характеристику преступлений можно определить как систему данных о криминалистически значимых признаках преступлений конкретного вида или группы, отражающих закономерные связи между этими признаками, и служащую построению типовых версий, которые берутся за основу при планировании расследования преступлений данного вида или группы [2, с. 30].

Основными структурными элементами криминалистической характеристики преступления, которые определяют ее содержание, можно считать:

1) непосредственный предмет преступного посягательства;

2) способ совершения и сокрытия преступления;

3) обстоятельства, при которых готовилось и было совершено преступление (время, место, и т.д.);

4) особенности оставляемых преступниками следов (механизм следообразования в широком смысле);

5) личность преступника и потерпевшего [1, с. 509]

Зная, например, способ совершения преступления, характерные черты самого преступного события и обстановки совершения преступления, следы, которые были оставлены преступниками, можно с большой вероятностью определить неизвестные элементы, в том числе личность преступника.

Таким образом, можно сделать вывод, что элементы криминалистических характеристик неразрывно связаны между собой.

В Уголовном кодексе Российской Федерации (далее – УК РФ) три статьи, описывающие преступления сфере информационных тех-

нологий – 272, 273 и 274. Одной такой статьей УК РФ охватывается сразу несколько преступных деяний, сильно отличающихся по личности преступника, способу и оставляемым следам.

Производя оценку вероятного преступника, прежде всего, нужно установить уровень его компетенции в области информационных технологий (далее – ИТ). Когда квалификация подозреваемого неизвестна, то ее следует предполагать высокой [6, с. 41].

Предметом преступного посягательства является компьютерная информация.

Типичные образы компьютерных преступников и их вероятные мотивы:

«Хакер» – лицо, рассматривающее защиту компьютерных систем как личный вызов и взламывающее их для получения полного доступа к системе и удовлетворения собственных амбиций [3, с. 326]. Чертой личности «хакера» является эскапизм – стремление уйти от реальности, от общепринятых норм общественной жизни в мир иллюзий. Следовательно, «хакер» имеет узкий круг общения, поэтому информацию о нем и его сообщниках стоит искать прежде всего среди его виртуальных знакомых.

«Инсайдер» – человек, не слишком хорошо владеющий знаниями в области ИТ, зато владеющий доступом в информационную систему в силу служебного положения.

«Белый воротничок» – так называемый – казнокрад, но в отличие от «инсайдера», имеет минимальную квалификацию в сфере ИТ и компьютер как орудие совершения преступления не использует. Компьютер выступает лишь как носитель следов совершения преступления.

По своим мотивам «белые воротнички» могут быть разделены на три группы:

1. Злоупотребляющие своим служебным положением из чувства обиды на компанию или начальство. Их следует искать среди долго работающих сотрудников. Обычно такой обиженный злоумышленник чаще всего ворует, чтобы «компенсировать» якобы недополученное от работодателя.

2. Беспринципные расхитители, ворующие только потому, что представилась такая возможность. Для таких злоумышленников характерен недолгий срок пребывания на должности. Довольно часто за таким имеется криминальное прошлое.

3. Квазивынужденные расхитители, попавшие в тяжелое материальное положение, в материальную или иную зависимость от лица, требующего совершить хищение или мошенничество. Как правило, такие проблемы трудно скрыть от окружающих – крупный проигрыш, наркомания, семейный кризис и т.п. Эта группа преступников, в отличие от первых и вторых, не может долго подготавливать свои преступления.

«Е-бизнесмен». Этот тип вероятного преступника не является квалифицированным ИТ-специалистом и не имеет служебного положения, которым можно злоупотребить. Изначально он планирует именно криминальное предприятие и совершение им правонарушения именно в компьютерной среде носит характер извлечения наибольшей выгоды [5, с. 46]. Чертой личности «е-бизнесмена» является наличие организаторских способностей.

«Антисоциальный тип». Злоумышленник страдает психическим расстройством и преступления совершает на основе патологической тяги. Такие типы не склонны к планированию правонарушения.

Способ совершения посягательства отражает особенности преступников и их мотивы.

Характерной чертой всех киберпреступлений является то, что место и время совершения противоправных деяний не совпадает с местом и временем неправомерного доступа к информации и наступления вредных последствий.

Рассмотрим такой вид компьютерного преступления как дефейс и дадим ему криминалистическую характеристику.

Предмет преступного посягательства:

Предметом преступного посягательства, как говорилось ранее, является компьютерная информация.

Способ совершения. Злоумышленник тем или иным способом изменяет внешний вид публичного веб-сайта потерпевшего, чаще всего его титульную страницу. Технически это можно осуществить, получив доступ на запись к директории, где хранятся данные веб-сервера. Также дефейс часто производят, воспользовавшись уязвимостью в само́м веб-сервере. Бывает, что злоумышленник изменяет веб-страницу, воспользовавшись штатной функцией, под аккаунтом одного из законных пользователей.

Способ сокрытия. При непосредственном доступе сокрытие следов сводится к повторению обстановки, предшествующей совершению преступления, то есть уничтожению оставленных следов.

Вероятный преступник соответствует модели «хакер» или реже – «инсайдер».

Мотивы для дефейса бывают следующие:

– стремление указать администратору сайта на уязвимость;

– стремление продемонстрировать публично свою квалификацию;

– политические, религиозные, иные идеологические мотивы;

– личная неприязнь, личный конфликт с потерпевшим или кем-либо из его работников;

– стремление испортить деловую репутацию владельцу веб-сайта в целях конкурентной борьбы, повлиять на его капитализацию в целях биржевой спекуляции.

Следы. На взломанном компьютере не удастся найти следов или их останется не много, так как злоумышленник по возможности старается их уничтожить. Больше следов можно найти либо на компьютерах, используемых хакером в качестве промежуточных узлов для исследования атакуемого веб-сайта и доступа к нему, либо непосредственно на его личном компьютере. Там можно найти переработанную или заново изготовленную веб-страницу, а также ее промежуточные варианты, средства для осуществления несанкционированного доступа и т.п.

Злоумышленнику необходимо привлечь общественное внимание к дефейсу. Следовательно, сразу после совершения преступления или незадолго до него он оповестит общество о нем. Этого он достигнет путем рассылки сообщений по электронной почте или размещения статьи на веб-форуме. Такие действия оставят дополнительные следы.

Потерпевший. Чаще потерпевшим является юридическое лицо. Обычно предприятие – потерпевший не заинтересовано в разглашении информации об инциденте, дабы не испортить свою деловую репутацию. Но если широкая огласка уже произошла, позиция потерпевшего может измениться, ведь привлечь к ответственности злоумышленника – это некоторая компенсация в плане репутации и общественных связей.

Несколько лет назад информационная безопасность представляла интерес только для узкого круга профессионалов. Сейчас же эта тема беспокоит практически каждого пользователя «гаджетов» – данная выдержка из журнала «Полиция России» точно отображает настоящую действительность и подтверждает, что информационная

безопасность на сегодняшний день одна из основных составляющих национальной безопасности страны.

Зарегистрированные преступления в сфере компьютерной информации								
Главный информационно аналитический центр главного управления МВД по Иркутской области					Главный информационно аналитический центр МВД РФ			
По Иркутской области					По стране			
ст.\год	2012	2013	2014		ст.\год	2012	2013	2014
272	19	46	34		272	2820	1799	1150
273	0	5	1		273		764	583
274	0	0	0		274		0	3

Статистика, составленная Главным информационно-аналитическим центром Министерства внутренних дел (далее – МВД) Российской Федерации и информационно-аналитическим центром главного управления МВД по Иркутской области наглядно показывает, что динамику компьютерных преступлений проследить довольно-таки сложно. Но этому есть свое объяснение. Неоспоримо, что благодаря знанию криминалистических характеристик видов и групп преступлений можно выдвинуть наиболее обоснованные версии по конкретному преступлению данного вида или группы. Но нужно учитывать тот факт, что криминалистическая характеристика преступлений динамична и изменяема в зависимости от криминальной практики. Такие изменения связаны с появлением новых видов преступлений, способов их совершения и сокрытия, также изменяется и круг преступников, их мотивация. Следовательно, типовые криминалистические характеристики уже через несколько лет могут оказаться устаревшими.

Таким образом, можно с уверенностью сказать, что глобальная сеть Интернет является благоприятной средой для развития компьютерных преступлений и для того, чтобы повысить их раскрываемость, нужно отслеживать современные информационные тенденции.

Список использованной литературы

1. Криминалистика. Полный курс: учебник / под общей ред. А.Г. Филиппова. 4-е изд., перераб. и доп. М.: Издательство Юрайт; ИД Юрайт, 2011. 835 с.

2. Криминалистика: учебник для вузов / под ред. А.А. Хмырова, В.Д. Зеленского. Краснодар, 1998. 137 с.

3. Криминалистика: учебник / отв. ред. Н.П. Яблоков. 2-е изд., перераб. и доп. М.: Юристъ, 2001. 718 с.

4. Рассолов И.М. Право и Интернет. Теоретические проблемы. 2-е изд., доп. М.: Норма, 2009. 384 с.

5. Соловьев И.Н. Правовое обеспечение борьбы с преступлениями в сфере информационных технологий // Административное и муниципальное право. 2009. № 3.

6. Федотов Н.Н. Форензика – компьютерная криминалистика. М.: Юридический Мир, 2007. 432 с.

Информация об авторе

Черных Анастасия Юрьевна – студентка, ИрЮИ (ф) РПА Минюста России, e-mail: Nastya_ru96@mail.ru.

УДК 343.98

А.В. Измайлов
Научный руководитель: О.А. Гарига

НЕКОТОРЫЕ ВИДЫ КИБЕРПРЕСТУПЛЕНИЙ И МЕТОДИКА ИХ РАССЛЕДОВАНИЯ

Каждый день во всем мире происходят десятки тысяч инцидентов, связанных с информационной безопасностью. Перечень таких инцидентов достаточно широк. Условно их можно выделить в 2 группы: внутренние (компрометация данных, утечка конфиденциальной информации, аномальная сетевая активность, и т.д.) и внешние (фишинг, кардинг, DDoS-атаки («Отказ в обслуживании»), целевые атаки и т.д.).

Согласно представленному отчету «NORTON REPORT 2013» международной корпорацией Symantec [4], ущерб от компьютерных преступлений во всем мире оценивается в 113 миллиардов долларов США. По оценкам другой авторитетной международной компаний по предотвращению и расследованию киберпреступлений «Group-IB» в России и СНГ за 2013–14 год совершено хищений на сумму 2,5 миллиарда долларов США, что составляет 2 % от глобального рынка, оцененного корпорацией Symantec. Отмечается активный рост хище-

ний со счетов российских банков с использованием зараженных мобильных устройств. За период с третьего квартала 2013 года по второй квартал 2014 года было выявлено 5 организованных преступных групп, использующих уникальное вредоносное программное обеспечение. Компанией Group-IB было зафиксировано множество целевых атак на финансовые организации, которые завершились успешным проникновением злоумышленников извне во внутренние сети, а также получением доступа к банковским и платежным системам [1].

Безусловно, такие явления требуют немедленного реагирования правоохранительных органов. Основная масса киберпреступлений расследуются Управлением «К» БСТМ МВД России [5] и региональными структурными подразделениями, а также специализированными подразделениями ФСБ России. Особое значение, как отметил В.В. Путин [6] 26 марта 2015 года на заседании коллегии ФСБ России, имеют случаи, когда затрагиваются интересы национальной информационной безопасности государства. Так, в прошлом году было пресечено около 74 миллионов кибератак на официальные сайты и информационные системы органов власти.

Как правило, заявления о несанкционированном доступе, хищении денежных средств поступают от организаций, намного реже от граждан. Объяснением этому может быть то, что граждане бояться разглашения в ходе следствия украденной информации, которая может содержать тайные, интимные и иные подробности личной жизни. Поэтому при возникновении подобной ситуации следователю необходимо наладить психологический контакт, объяснить гражданину, что следствие интересуют только те данные, которые имеют значение для расследования преступления и не могут быть разглашены третьим лицам.

Первоначально проводятся неотложные следственные действия, связанные со сбором вещественных доказательств: осмотр места происшествия, который неразрывно связан с осмотром компьютера, периферийного оборудования и иных объектов. Практически вся следовая информация хранится в памяти компьютера, поэтому особое внимание следует уделять осмотру машинных носителей. Необходимо учитывать и то, что существует угроза потери данных указанных объектов, поэтому в этом случае целесообразно их изымать для последующего исследования в лабораторных условиях в рамках компьютерной технической экспертизы.

Далее проводим допрос заявителя-потерпевшего, в ходе которого максимально подробно следователь получает и фиксирует в протоколе

информацию, а именно о совершенных за последние 3–4 дня компьютерных операциях, действиях: какая сумма была украдена, какие сайты посещались, какие программы (приложения) были установлены и тд. При этом следователь должен исключить возможность инсценировки преступления, что бывает достаточно часто на практике, путем постановки дополнительных вопросов, изучением личности потерпевшего, установлением наличия профессиональных знаний в области информатики у допрашиваемых лиц и назначением экспертизы.

Далее, согласно ст. 195 УПК РФ, следователь выносит постановление о назначении компьютерно-технической экспертизы, поскольку она имеет огромное значение для сбора доказательственной информации. Для этого эксперту необходимо предоставить материалы для сравнительного исследования, объекты, изъятые в ходе осмотра места происшествия, которые были упомянуты выше. Если предоставить устройства на исследование эксперту не представляется возможным, то следователю целесообразно делать побитовую копию жесткого диска на месте совершения преступления, например, в организации. Для таких мероприятий существует криминалистический дубликат – разработка российских ученых, которая позволяет с идентичностью снять копию с любого цифрового устройства. Самостоятельно следователю в виду недостаточных знаний будет достаточно сложно или вовсе невозможно правильно изъять копию, поэтому тактически целесообразно при проведении всех следственных действий, как на первоначальном, так и последующих этапах расследования, привлекать специалиста в области компьютерной информации и компьютерной техники.

Конечно, привлекать квалифицированных специалистов по таким категориям дел не всегда представляется возможным по экономическим соображениям и узконаправленной сферой специализации. Тем не менее, многие крупные компании, банки и другие учреждения, где проходят большие обороты финансовых средств в электронной среде, заключают договоры на оказание услуг по предотвращению и расследованию киберпреступлений с авторитетными специализированными организациями, такими как Group-IB [2] и LETA IT-company [3], деятельность которых осуществляется не только в России, но и в других странах. Данные организации в своем штате имеют высококвалифицированных специалистов, криминалистические лаборатории, оборудование и готовы оказывать содействие правоохранительным органам. Безусловно, такое сотрудничество, обмен опы-

том передовых технологий в разы позволяет эффективнее расследовать компьютерные преступления.

В ходе компьютерно-технической экспертизы будут исследованы системные и программные файлы на наличие несанкционированного доступа, аномальная сетевая активность, время начала и окончания атак, типы, характеристика. Огромное значение для экспертов имеют лог-файлы (файлы расширения .log). Лог-файлы представлены в виде текстовой информации, которые хранят историю о всех интернет соединениях, исходящих и входящих запросах на компьютер потерпевшего. В лог-файлах будут так же перечислены IP-адреса, с которых производились запросы к серверу, устройству потерпевшего. По результатам экспертизы следователю предстоит выполнить огромную работу совместно с оперативными сотрудниками путем проведения следственных действий и оперативно-розыскных мероприятий по установлению принадлежности IP-адресов к конкретным лицам. Например, это могут быть запросы к хостинг-провайдерам о предоставлении данных о владельце IP-адреса (сервера), которые обслуживаются данным провайдером. При регистрации серверов владельцы указывают данные, в основном это номер телефона, почтовый адрес, адрес места жительства, однако некоторые хостинг-провайдеры в своей политике безопасности требуют указывать и паспортные данные, что упростит процедуру идентификации преступника. К сожалению, в России преимущественно используются динамические IP-адреса, намного реже статические. Так один динамический IP-адрес может принадлежать 10, 100, 1000 клиентам, что существенно затрудняет поиск злоумышленника.

Эксперту предстоит проделать кропотливую работу тогда, когда имеются признаки заражения компьютера (планшета, смартфона) трояном, вирусом-шпионом и прочими вредоносными программами. Как показывает практика, в 86 % случаев на зараженных устройствах было установлено антивирусное программное обеспечение. Поэтому эксперту предстоит буквально вручную отыскать вредоносный код (скрипт) путем декомпиляции всех установленных программ, что требует значительного количества времени. Так, например, при заражении смартфона с предустановленной операционной системой «Android» будут исследоваться подозрительные приложения (файлы расширения .apk формата). При исследовании вредоносного кода (скрипта) эксперт обнаружит в части кода IP-адрес, на который несанкционированно троян отправляет скомпрометированную инфор-

мацию. Остается определить принадлежность IP-адреса лицам по вышеописанной схеме.

Путем дальнейших оперативно-розыскных мероприятий необходимо установить местонахождения преступника и провести его задержание. Следователю по месту жительства злоумышленника осуществить обыск (выемку), в результате чего будет собрана доказательственная информация, которая будет положена в основу обвинения.

Таким образом, качественно проведенные первоначальные следственные действия и оперативно-розыскные мероприятия, своевременный сбор доказательственной информации с привлечением высококвалифицированных специалистов, назначение экспертиз влияют на результат, от которого будет зависеть эффективность предотвращение и расследование компьютерных преступлений.

Список использованной литературы

1. Отчет Group-IB: тенденции развития преступности в области высоких технологий 2014.

2. Официальный сайт Group-IB. (Дата обращения 26.04.2015 г.) URL: http://www.group-ib.ru/index.php/kriminalistika/79-link-investigation.

3. Официальный сайт LETA IT-company. (Дата обращения 26.04.2015 г.) URL: http://www.leta.ru/services/cybercrime-investigation/cybercrime-laboratory.html.

4. Официальный сайт корпорации Symantec. Отчет (Дата обращения 27.03.2015 г.) URL: http://go.symantec.com/norton-report-2013/.

5. Официальный сайт МВД России. Структура (Дата обращения 07.04.2015 г.) URL: https://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii.

6. Официальный сайт Президента РФ. (Дата обращения 09.04.2015 г.) URL: http://www.kremlin.ru/events/president/transcripts/49006.

Информация об авторе

Измайлов Алексей – студент, ФГБОУ ВПО «Саратовская государственная юридическая академия», Институт правоохранительной деятельности, email: aleshka-mail@ya.ru.

УДК 343.9

Б.С. Цынгеева
Научный руководитель: А.В. Вишневский

О ПРОБЛЕМАХ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ И КИБЕРТЕРРОРИЗМУ В РОССИИ

В настоящее время развитие общества, обеспечение жизни отдельного индивида и целых государств зависит от компьютерных и информационных технологий. При этом следует отметить, что преступность в сетях развивается динамично, а созданные антивирусные программы запросто уничтожаются компьютерными вирусами [1].

В этой связи нарастает угроза компьютерных преступлений и кибертерроризма, что в итоге является проблемой международного характера. Таким образом, огромное значение приобретает сотрудничество государств, с целью превенции и устранения последствий кибератак. В России по данным Федеральной службы безопасности, только на объекты информационной инфраструктуры Президента РФ, Правительства РФ, Государственной Думы и Совета Федерации каждый день совершаются около пятидесяти тысяч кибератак. Такое применение информационных технологий способно подорвать независимость и основы государственного устройства, дестабилизировать экономику и нарушить целостную систему жизнеобеспечения, что может привести к угрозе национальной безопасности. Помимо этого атаке подвергаются сайты органов судебной власти с целью модификации существующей информации, что может привести к утрате авторитета судебной власти.

Развитие информационных технологий способствует не только совершенствованию и укреплению общественных связей, но и появлению новых источников риска. Причем, следует отметить, что степень угрозы киберпреступности недостаточно изучена и не осознана в силу своей новизны.

В юридической литературе кибертерроризм определяется неоднозначно. Некоторые авторы полагают, что кибертерроризм можно сопоставить с террористическими актами с применением ядерных, бактериологических и химических оружий.

По мнению российского политика В.А. Голубева, кибертерроризм представляет собой преднамеренную атаку на информацию, компьютерную систему или глобальную сеть, которая создает опас-

ность для жизни и здоровья людей или влечет наступление других тяжких последствий. Такие действия совершаются с целью нарушения общественной безопасности, оказания давления на органы, дестабилизации общественно-политической обстановки запугиванием населения и осложнения международных отношений.

Кибертерроризм обусловлен бесконтрольным использованием глобальных сетей и отсутствием должного внимания со стороны государства. Киберпреступники в своей деятельности имеют целью создание опасности, устрашения общества для достижения целей субъектов террористической деятельности путем модификации информации, создания вирусных баз, блокировки данных и т.д. Неограниченное пространство сетей и анонимность обеспечивают злоумышленникам эффективность их действий.

Основной формой преступлений в сетях является атака на компьютерную информацию, вычислительные системы, аппаратуру передачи данных, что позволяет осуществлять различные деструктивные действия. В связи с появлением множества новых информационных технологий назревает необходимость выработки законодательства и принятия мер для борьбы с киберпреступностью и кибертерроризмом.

Законодательная деятельность по предотвращению киберпреступности и кибертерроризма России отражена в Уголовном кодексе Российской Федерации, в котором статьями 272, 273, 274 предусмотрена ответственность за неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ, повлекшее уничтожение, блокирование, модификацию компьютерной информации и т.д.

Правовую основу противодействия кибертерроризму составляют Конституция Российской Федерации, Закон о противодействии терроризму, Концепция противодействия терроризму в Российской Федерации, Закон об информации, информационных технологиях и о защите информации, Закон о противодействии экстремисткой деятельности.

В соответствии с п.15 Концепции противодействия терроризму предупреждение терроризма предполагает противодействие распространению идеологии терроризма путем обеспечения защиты единого информационного пространства Российской Федерации; совершенствование системы информационного противодействия терроризму; усиление взаимодействия федеральных органов исполнительной вла-

сти и укрепление международного сотрудничества в сфере противодействия терроризму. Основными мерами по его профилактике являются: формирование стойкого неприятия обществом идеологии насилия, разъяснение сущности терроризма и его общественной опасности и привлечение общества к борьбе с ним[1].

Согласно ст.ст. 12-13 Федерального закона от 25 июля 2002 года № 114-ФЗ «О противодействии экстремисткой деятельности» запрещается использование сетей связи общего пользования для осуществления экстремисткой деятельности, а также распространение экстремистских материалов, их производство или хранение в целях распространения[2].

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» устанавливает запрет на распространение информации, направленной на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность[3].

Однако следует отметить, что угрозы любого терроризма могут быть нейтрализованы только путем сплочения всего мирового сообщества с целью ликвидации идеологических, экономических и социальных корней этого явления. И с этой целью, в 2013 году был создан Европейский центр по борьбе с киберпреступностью, деятельность которого сразу после создания ознаменовалась раскрытие одной из самых больших и сложных сетей киберпреступности, основанной в России, и которая заразила миллионы компьютеров с помощью вирусной программы «Police Ransom ware».

Следует отметить, что компьютерная преступность представляет собой реальность современного мира, и таким образом, необходимо закрепить на законодательном уровне обязанность государственных структур по принятию технических мер, обеспечивающих защиту компьютерных сетей, как одного из наиболее уязвимых элементов современного общества. В противодействии преступности в сетях

---

[1] Концепция противодействия терроризму в Российской Федерации от 5 октября 2009 г. // Рос. газ. 2009. № 198.

[2] О противодействии экстремисткой деятельности: Федеральный закон от 25 июля 2002 г. № 114-ФЗ // Собрание законодательства РФ.2002. №30. Ст. 3031.

[3] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 года № 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

приоритетное значение должно принадлежать оперативному пресечению атак на подготовительной стадии, а также проведению мониторинга состояния информационно-коммуникационного пространства, предоставление необходимой информации обществу и профилактической работе. Эти меры должны приниматься федеральными и региональными властями для более эффективного результата.

Более того, одним из главных приоритетов национальной безопасности России является обеспечение безопасности в рамках реализации основных принципов построения информационного общества. Использование систем и сетей в государственном управлении, судебной системе, военной и промышленной сферах, и в бизнесе является первоначальным объектом для кибертеррористов [2]. Обеспечения безопасности компьютерной информации и информационных технологий на данный момент является для большинства государств одной из острых проблем. Это обуславливает необходимость создания общенациональной системы безопасности информационно-коммуникационной инфраструктуры, которая обеспечивала бы надежную защиту от террористических угроз.

Также стоит отметить, что существуют противоречия в реализации политики противодействия кибертерроризму. Так, например, реализация гражданином конституционного права на свободное получение информации и пользование ею ограничивается или вообще исключается необходимостью обеспечения безопасности государства в информационно-коммуникационной сфере и повышенным вниманием государства к информации, всплывающей в сетях. В то же время, кибертеррористы реализуют данные права и свободы для пропаганды своей деятельности, изменения основ государственного строя. Такие противоречия обуславливает необходимость безусловного обеспечения законности и правопорядка, закрепления права за правоохранительными органами осуществлять мониторинг информации виртуального пространства и принятия мер к прекращению деятельности в нем террористических структур.

Расширение и глобализация информационных процессов открыла новые пути и возможности прогрессивного развития человечества, а также вызвала ряд качественно новых глобальных угроз национального безопасности.

Одной из главных проблем на сегодняшний день является разрешение вопроса о контроле над информацией. С одной стороны, право человека на свободный доступ к информации является одной из плат-

форм, на которой держится свободное общество, а с другой – права и свободы с успехом используются террористами для реализации их замыслов. По мере развития информационно-коммуникационных систем и технологий, угроза кибертерроризма будет непременно нарастать и совершенствоваться.

Борьба с киберпреступностью, как и с преступностью в обществе в целом, не может быть проблемой отдельных государств, поэтому необходимо обеспечить эффективное сотрудничество специальных служб на национальном, региональном и международном уровнях, в области предупреждения и ликвидации последствий кибератак.

Список использованной литературы

1. Голубев В.А. Кибертерроризм – угроза национальной безопасности [Электронный ресурс]. – Режим доступа: www.crive-research.ru, свободный (дата обращения: 26.03.2015).

2. Молодчая Е.Н. Политика противодействия кибертерроризму в современной России: политологический аспект: автореф. дис. … канд.полит.наук. М., 2011. 26 с.

Информация об авторе

Цынгеева Бимбасо Солбоновна – студентка, Российский государственный университет правосудия (Восточно-Сибирский филиал), факультет подготовки специалистов для судебной системы (юридический факультет), e-mail: bimbasu.cyngeeva.95@mail.ru.

УДК 343.3/.7

Д.С. Хлыстова
Научный руководитель: А.Ю. Решетников

ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОГО ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В РОССИИ

Стремительное развитие информационных технологий (IT) не только упрощает нашу жизнь, но и создает еще одно поле деятельности для преступников-интеллектуалов. Причем, сфера IT является крайне привлекательной, поскольку дает возможность нанести ущерб

не только быстро, но еще и дистанционно. Именно поэтому проблемы изучения киберпреступности и кибертерроризма в настоящее время особенно актуальны.

Практика показывает, что любые инновации порождают новые возможности для совершения преступлений. И информационные технологии – не исключение. Как и следовало ожидать, расширение использования электронно-вычислительной техники породило не только технические, но и правовые проблемы.

О теоретической возможности совершать преступления через сеть «Интернет» было известно еще в 70-х годах XX века. До создания Анди Хопкинсом в 1984 году первой антивирусной программы, для этого практически не существовало препятствий. Чем и пользовались в основном те правонарушители, которые имели доступ к сети благодаря служебному положению. Тем не менее еще несколько лет назад можно было говорить о том, что процент Интернет-преступлений в России был невелик, чего нельзя сказать о настоящем времени.

Рассматривая современное состояние киберпреступности в России, нельзя не учитывать тот факт, что компьютерные преступления не являются очевидными, могут иметь как длящийся, так и одномоментный характер, что делает их особо опасными. Не стоит забывать и о ее высокой латентности таких преступлений. По данным НИИ Генеральной прокуратуры РФ показатель латентности компьютерных преступлений в зависимости от вида совершаемых преступлений колеблется от 4,8 (ст. 272 УК РФ) до 30 (ст. 274 УК РФ) [4, с. 481–483].

По данным МВД России, в 2007 г. число преступлений, совершаемых с использованием компьютерных технологий, составляло 7236, в 2008 г. – 9010, в 2009 г. – 11590. Вместе с тем, в 2010 г. зарегистрировано всего 7540 преступлений (на треть меньше, чем в 2009 г.) [5].

После существенных изменений, внесенных в УК РФ в 2011 г., показатели регистрации компьютерных преступлений вновь показали рост. Так, по данным за 2014 г. в стране было зарегистрировано около 11000 компьютерных преступлений, что почти на 4000 больше показателя четырехлетней давности. Вместе с тем, остается неясным, какой процент потерпевших заявляет о совершенных против них киберпреступлениях. Это связано также с тем, что некоторые жертвы (особенно это касается юридических лиц, осуществляющих деятельность в финансовом секторе) не раскрывают информацию о фактах преступлений из опасения, что распространение негативных сведений подобного рода нанесет ущерб их репутации. Если компания объявит,

что ее сервер был взломан хакерами, то клиенты могут утратить к ней доверие, и в результате совокупные издержки и другие последствия по своей тяжести могут превзойти потери от взлома. [3, с. 4-6] Кроме того, последствия киберпреступлений зачастую могут наступать вне пределов России, что также затрудняет их выявление.

Проблема несообщения властям о фактах нападений киберпреступников очень остро стоит в наши дни как в России, так и за рубежом. Одной из причин оказалось недоверие правительствам и правоохранительным органам. Почти треть компаний, пострадавших от вымогательского программного обеспечения, готовы выплатить киберпреступникам выкуп за разблокировку файлов, – сообщает компания ThreatTrack, проводившая исследования на эту тему. (Ransomware (программы-вымогатели) – тип вредоносных программ, которые ограничивают доступ пользователя к операционной системе и требуют уплаты выкупа за снятие ограничения [6]).

Поскольку в данной ситуации основной причиной является отсутствие у компаний веры в то, что правоохранители смогут защитить их, полагаем целесообразно будет усилить контроль властей за исполнением законодательства в сфере компьютерной информации, а также активизировать работу, стимулирующую граждан сообщать об атаках киберпреступников.

Огромные трудности в преследовании преступника и расследовании киберпреступлений создает сочетание относительной анонимности и огромной аудитории. Благодаря этому преступникам предоставляется возможность совершать преступления и против свободы, чести и достоинства личности, и против половой неприкосновенности, и против конституционных прав и свобод человека и гражданина. Вариантов масса. Этим и пользуются киберпреступники.

Личностные характеристики киберпреступника, судя по результатам анализа официальных данных, не обладают особой спецификой. Согласно статистике, компьютерные преступления совершаются лицами в возрасте от 15 до 45 лет, независимо от пола. Что также усложняет преследование правонарушителей.

Не следует забывать и о том, что помимо непосредственных нарушителей закона, существуют также привлекаемые ими лица, которые помогают осуществлять преступную деятельность. В эту категорию прежде всего попадают несовершеннолетние. Например опытный хакер может склонить лицо, не достигшее 18 лет к совершению преступления, рассказав о механизме взлома интернет-сайта и убедив

в безнаказанности, таким образом воспользовавшись неопытностью и доверием. Не говоря уже о том, что некоторые сайты, рассчитанные на молодую аудиторию, призывают употреблять спиртные напитки и наркотические вещества, совершать действия экстремистского и террористического характера, и, к сожалению, находят своего посетителя. В данной ситуации, хотя и ведется борьба с такого рода ресурсами, я считаю, что следует ужесточить ответственность за онлайн-пропаганду антиобщественного и преступного поведения.

Что касается квалификации компьютерный преступлений, необходимо отметить, что, не смотря на то, что глава 28 УК РФ (Преступления в сфере компьютерной информации) включает в себя всего лишь три статьи, все же возникает множество проблем, особенно при разграничении составов.

По мнению многих авторов, рассматривая ст. 272 УК РФ, не каждый факт неправомерного доступа к компьютерной информации попадает под признаки этой статьи. В каждом конкретном случае «уничтожения, блокирования, модификации либо копирования компьютерной информации» правоприменителю трудно доказывать, что такие действия повлекли соответствующие последствия, обозначенные диспозиции ст. 272 УК РФ, а также умысел, направленный на совершения именно этого деяния. А ведь в некоторых случаях общественно опасным может быть лишь ознакомление с той или иной информацией, что не попадает под признаки состава ст.272 УК РФ.

Существует несколько путей решений данной проблемы. Например, Быков В.М. предлагает внести изменения в текст закона: «…ч. 1 ст. 272 УК РФ в новой редакции нового закона следует после слова «повлекло» добавить такие слова: «несанкционированное ознакомление» и далее по тексту закона. Уголовный закон должен пресекать незаконное любопытство некоторых лиц, тем более, что это может иметь общественно опасные последствия для владельца той или и иной информации» [2, с. 14].

Также, одной из основных проблем является нечеткость формулировок ст. 272 и 273 и разграничения их, например, со ст.146 УК РФ (Нарушение авторских и смежных прав). На практике часто возникают проблемы, и деяния, связанные с нарушением авторских и смежных прав, правоприменитель зачастую оценивает по ст. 272 и ст. 273 УК РФ. Это связано с тем, что определения составов являются не совсем удачными и отстают от современного состояния научно-технического прогресса [3, с. 50–52].

Нельзя оставить без внимания проблемы квалификации ст. 274 УК РФ (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей). По нашему мнению, большинство проблем создает опять же формулировка данной статьи (ключевое слово – «правила эксплуатации»). Это довольно широкое понятие, которое может включать в себя что угодно: начиная от правил, которые создаются самими разработчиками электронно-вычислительной техники, заканчивая теми, которые действуют только на конкретных предприятиях и фирмах [1, с. 17]. То есть, для того чтобы привлечь лицо к уголовной ответственности по ч. 1 ст. 274 необходимо установить, какие именно правила эксплуатации нарушены, что, как мы уже выяснили, довольно не просто в отдельных случаях.

Эти, и многие другие вопросы правоприменительной практики и проблемы квалификации компьютерных преступлений являются предметом острых дискуссий и обсуждений, однако объем работы не позволяет нам рассмотреть каждую из них подробно. Ведь компьютерные преступления выходят далеко за рамки 28 главы УК РФ.

Подводя итог вышесказанному, отметим, что высокая общественная опасность киберпреступности не вызывает сомнений на современном этапе развития Российской Федерации и всего мирового сообщества. Согласно статистическим данным она имеет как стойкую тенденцию к росту, так и довольно высокий уровень латентности. Личность преступника неоднородна, а проблемы квалификации имеют место быть.

Киберпреступность – одна из угроз национальной и глобальной безопасности, а поэтому противодействие ей уголовно правовыми и иными средствами требует повышенного внимания.

Список использованной литературы

1. Быков В.М. Новое: об уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ / В.М. Быков, В.Н. Черкасов // Российский судья. – 2012. – № 7.

2. Быков В.М. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ / В.М. Быков, В.Н. Черкасов // Российский судья. – 2012. – № 5.

3. Побегайло А.И. Киберпреступность: учеб. пособие. Акад. Ген. прокуратуры Рос. Федерации. М., 2013.

4. Теоретические основы исследования и анализа латентной преступности / под ред. С.М. Иншакова. М., 2011.

5. Чекунов И.Г. Киберпреступность: проблемы и пути их решения // М.: Вестник академии права и управления. 2011. № 25.

6. http://www.cybersecurity.in.ua/ru/term/ransomware-programmy-vymogateli.

Информация об авторе

Хлыстова Дарья – студентка, юридический факультет Академии Генеральной прокуратуры РФ, e-mail: d.khlystova@yandex.ru

УДК 343.9

А.Ю. Скуратовский
Научный руководитель: К.Н. Евдокимов

ЛИЧНОСТЬ КИБЕРПРЕСТУПНИКА

Изучение особенностей личности преступника, совершающего киберпреступления, является необходимым условием для эффективной борьбы с данным видом преступных деяний. Сравнительный анализ личности преступника, совершающего преступления, предусмотренные ст. ст. 272–274 УК РФ приобретает особую актуальность в свете стремительного развития информационных технологий, а также давно назревшей необходимостью защиты интересов личности, общества, государства в сфере безопасного обращения компьютерной информации.

Киберпреступники наносят огромный вред российской экономике и политической системе. Так, по оценкам аналитиков компании Group-IB объем рынка киберпреступности в РФ в 2012 году составил 1,93 миллиарда долларов [10], а с середины 2013 года по середину 2014 года в России и СНГ русскоговорящие хакеры «заработали» 2,5 млрд долларов, что составляет 2 % от глобального рынка [11].

В свою очередь, американская корпорация Symantec оценила ущерб от киберпреступников в России за 2013 год в 1 млр. долларов, а

в 2012 году в 1,48 млрд долларов. При этом общий ущерб от киберпреступности в мире в 2013 году составил 113 млрд долларов [12].

По данным исследования Cost of CyberCrimeStudy, проведенного компанией PonemonInstitute при поддержке HP EnterpriseSecurity, среднегодовой ущерб российской организации от киберпреступников в 2014 году достигает 3,3 млн долларов [13].

В криминологии под личностью преступника принято понимать личность человека, который совершил преступление вследствие присущих ему психологических особенностей, антиобщественных взглядов, отрицательного отношения к нравственным ценностям и выбора общественно опасного пути для удовлетворения своих потребностей или не проявлении необходимой активности в предотвращении отрицательного результата [6, с. 126].

Поэтому для получения реального образа личности преступника, совершающего преступления в сфере компьютерной информации, необходимо уделять пристальное внимание социально-демографическим, биофизиологическим, психологическим, нравственным, образовательно-техническим, социально-ролевым, уголовно-правовым и иным особенностям таких лиц, вероятным мотивам и поведенческим признакам, обуславливающих их преступный выбор.

Представляется, что для всестороннего рассмотрения данной проблемы, в первую очередь необходимо определиться с оптимальным пониманием личности преступника. Стоит сказать, что в доктринальной базе нет единого подхода к определению личности преступника. Н. Ф. Кузнецова, например, считает, что под личностью преступника надо понимать систему социальных и психических свойств, образующих ее общественную опасность, которая детерминирует совершение преступления [7, с. 44]. Н. Д. Ведерников понимает под личностью преступника общий социальный тип, к которому можно отнести всех тех, кто совершил преступление [2, с. 99]. Можно согласиться с точкой зрения Ю. М. Антоняна, который определяет личность преступника как совокупность социально значимых негативных свойств, образовавшихся в нем в процессе многообразных и систематических взаимодействий с другими людьми [1, с. 21].

В обыденном понимании людей любого киберпреступника называют хакером, отчасти это верно, но данное трактование не всецело отображает суть всего содержания проблемы. Чтобы дать криминологическую характеристику личности компьютерного преступника не-

обходимо учитывать различные виды признаков, от биофизических до социально-демографических и образовательно-технических.

Довольно спорным является вопрос об использовании термина «хакер» для всей совокупности преступлений. Понятие «хакер» распространилось с появлением сети ARPANET и означало оно человека, который разбирается в компьютерах. Такие люди стремились к обмену информацией, что повлияло на развитие всемирной сети Интернет. Хакеры создавали FIDO – любительскую компьютерную сеть, которая основывалась на принципе «точка в точку». Особенностью этой сети являлась возможность бесплатного подключения и возможность использования ресурсов сети, а для подключения необходимо было наличие домашнего стационарного телефона. Также хакеры стали создавать и развивать UNIX-подобные системы с открытым кодом, на которых сейчас работает большинство серверов. Вся деятельность хакеров была направлена на изучение структуры программ, систем, понимание специфики работы. Но с развитием технологий из хакеров начали выделяться люди, которые занимались взломом программ, сетей и т. п. в корыстных целях. Таких людей Интернет-сообщество назвало «крэкерами» (взломщики, вандалы) [9, с. 5].

К «крэкерам» относят:

1. Вирусописателей – лица, применяющие свои знания для создания вирусный программ.
2. Вандалы – лица, стремящиеся уничтожить систему, удалить файлы, нарушить работу сервера.
3. Взломщики – лица, совершающие кражу со взломом с корыстной целью, либо по заказу либо производят взлом программ и предоставляют ее в сеть для свободного пользования и др.

Представляется, что при изучении личности данного вида преступников необходимо использовать комплексный подход. Само явление киберпреступности является самым молодым видом преступлений. Уровень компьютеризации и использования сети Интернет в нашей стране является одним из первых в мире. Поэтому, в основном, данными видами преступлений занимаются молодежь [4, с. 204].

Так, на основе судебной практики проводились исследования личности преступников. Исследования показали, что подавляющее большинство преступлений совершают, как правило, мужчины в возрасте от 18 до 24 лет, многие из которых проживают с родителями, на учете в наркологических диспансерах не состоят. Стоит отметить, что появляется тенденция на снижение возраста преступности т. к. под-

ростки характеризуются наличием низкой правовой культуры, отчасти правовым нигилизмом. Большинство преступлений ими совершается с домашнего компьютера, таким образом, правоохранительными органами раскрываются наиболее простые и мелкие преступления.

Также отмечается тенденция, согласно которой компьютерные преступления совершают лица, которые не удовлетворены своим внешним видом, в связи с чем они уходят в виртуальную реальность, пытаются самоутвердиться.

Так, анализируя судебную практику, можно сделать вывод о том, что компьютерные преступления всегда производятся с помощью компьютерной техники: компьютеры, смартфоны и другие электронно-вычислительные устройства. Также используются беспроводные технологии, программы, находящиеся в открытом доступе (например, браузеры), но основную роль играет программное обеспечение. Во многом, чтобы совершить преступление в данной сфере, преступнику не нужно вставать с рабочего места, вполне достаточно наличие стандартного домашнего ПК без наличия каких-либо специальных знаний [3, с. 136].

Необходимо отметить и тот факт, что поимка хакеров не является первоочередной задачей. «Установление личности хакеров и аресты не обязательно являются частью изначальной операции. Но когда лаборатория действует для защиты экосистемы и обнаруживает что-то важное, результаты работы могут быть переданы правоохранительным органам, чтобы принять правовые меры. Работа должна быть проведена на высоком уровне, поскольку она будет показана в суде и обязана вызывать у юристов доверие» – заявил Дж. Вильямс, сотрудник Лаборатории Касперского. Поэтому составить личность преступника крайне сложно.

Д. И. Ковалев выделяет 3 группы киберпреступников:

1. Начинающие. В основном студенты технических вузов. Средний возраст от 15 до 20 лет, как правило, мужчины. Семьи характеризуются средним достатком. В доме имеется доступ в Интернет и 1 (и более) персональных компьютеров. Обычно преступники не работают, связь с окружающим миром поддерживают в ограниченном доступе. Пользуются компьютерным слэнгом, грамотность невысокая, интересуются профессиональной литературой.

2. Закрепившиеся. Лица в возрасте от 20 до 25 лет, в основном мужчины. Образование техническое. Используют наработки начинающих, используют их, либо являются лидерами и организаторами

хакерских групп. Обычно работают техническими консультантами, системными администраторами. Основное направление преступной деятельности – сетевой взлом.

3. Профессионалы. Лица в возрасте от 25 до 45 лет, преобладают мужчины, доля женщин от общего числа составляет всего 8– 10 %, семьи с достатком высшее среднего, высшее техническое образование, обладают несколькими языками программирования, отлично разбираются в технической составляющей компьютеров. Психологические аспекты характеризуются уравновешенностью психотипа, устойчивостью взглядов, амбициозностью. Как правило, работают заместителями начальника информационных отделов фирм, банков, основная деятельность разворачивается в нелегальной или полулегальной сфере [5, с. 91].

В свою очередь, Т. М. Лопатина выделяет 4 группы личностей киберпреступника. К первой группе она относит людей с ярко выраженными целями на совершение преступления. Они отличаются профессиональной подготовкой, должностным положением, благодаря специальным знаниям. Руководствуясь различными мотивами, данные преступники чаще всего совершают наиболее опасные преступления в сфере компьютерной безопасности. Обычно такими преступниками являются высокопрофессиональные программисты, которые могут создавать и изменять различные вредоносные программы [8, с. 148–163].

Ко второй группе Т. М. Лопатина относит пользователей с высоким уровнем профессионализма и с определенным уровнем фанатизма, любопытства. К ним относятся хакеры и «крэкеры». Первые занимаются поиском и устранением слабых мест в системе в исследовательских целях, «крэкеры» же используют знания в корыстных целях, взламывают системы защиты, крадут данные и т. п. Поведение людей этой группы характеризуется дерзостью, открытостью преступлений, применением «ноу-хау».

К третьей группе она относит людей, страдающих зависимостью от Интернета. Такие люди тратят все свободное время на проведение времени в виртуальной среде. Из-за своей неопытности, невнимательности данные люди могут причинять вред путем заражения вирусами компьютеров, несанкционированным копированием данных и т. п.

В четвертую группу входят люди страдающие игровой зависимостью. Они реализуют себя в уничтожении, блокировании, модификации, копировании ничем не защищенной информации, занимаются созданием и распространением вирусных программ, которые порождают нежелательные для пользователя последствия: вывод на экран

мешающих работе сообщений, рисунков, стирание или модификацию содержимого памяти и т. п.

Анализируя все вышеизложенное, можно сделать следующий вывод о примерном криминологическом портрете личности киберпреступника, совершающего преступления в России. Основные черты преступника будут выглядеть следующим образом: это, как правило, мужчина, возраст которого от 16 до 25 лет, неженатый, имеющий среднее специальное или высшее техническое образование, молодой специалист, городской житель, обладающий одним или более персональным компьютером, имеющим доступ в Интернет, ранее не судимый, по психологическим признакам характеризующийся мыслящей неординарной личностью, способностью принимать рискованные и оригинальные решения, общаться с людьми предпочитает виртуально, занимается самообразованием, зависит от доступа в Интернет.

Список использованной литературы

1. Антонян Ю. М. Преступник как предмет криминологического изучения // Вопросы борьбы с преступностью, Вып. 34. М., 1981.
2. Ведерников Н. Т. Личность обвиняемого как объект изучения на предварительном следствии // Актуальные вопросы борьбы с преступностью. Томск : Изд-во ТГУ, 1990.
3. Дремлюга Р. И. Интернет-преступность: монография. Владивосток : Изд-во Дальневосточного университета, 2008.
4. Евдокимов К. Н. Создание, использование и распространение вредоносных компьютерных программ : уголовно-правовые и криминологические аспекты : монография. Иркутск : Изд-во ИЮИ (ф) АГП РФ, 2013.
5. Ковалев Д. И. Криминологическая характеристика личности преступника, совершающего преступление в сфере компьютерной информации. М., 2011.
6. Криминология : учебник / под ред. В.Н. Кудрявцева и В.И. Эминова. М.: Юристъ, 2000.
7. Криминология / под ред. Н. Ф. Кузнецовой. М. : Зерцало, ТЕИС, 1996.
8. Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности : дис. … д-ра юрид. наук : 12.00.08. М., 2007.

9. Фленов М. Е. Компьютер глазами хакера. СПб. : БХВ-Петербург, 2008.
10. URL:http://digit.ru/business/20130910/405335397.html#ixzz2r1xUjpbf.
11. URL: http://www.group-ib.ru/index.php/investigation/1063-link-nezavisimye.
12. URL: http://go.symantec.com/norton-report-2013/.
13. URL: http://www.octree.co.uk/Documents/2014-Global-Report-on-the-Cost-of-Cybercrime.pdf.

Информация об авторе

Скуратовский Алексей Юрьевич – студент, Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Академия Генеральной прокуратуры Российской Федерации», Иркутский юридический институт (филиал).

УДК 343.3/.7

А.С. Мананников
Научный руководитель: В.В. Поляков

ЛИЧНОСТЬ КИБЕРПРЕСТУПНИКА

В настоящее время, практически все сферы жизнедеятельности, так или иначе, связанны с доступом к информационно-телекоммуникационной сети «Интернет» и использованием компьютерных программ. Преступления в данной сфере причиняют масштабный ущерб.

В настоящее время, исследование личности компьютерного преступника представляется наиболее актуальным. Обуславливается это тем, что знание их особенностей, позволит правоохранительным органам сузить и оптимизировать процесс выявления круга лиц, среди которых целесообразно вести поиск преступника и точнее определить способы их установления и изобличения. При этом очевидно, что знание личностных характеристик киберпреступника способствует повышению эффективности борьбы с рассматриваемым видом преступлений.

«Личность преступника» – понятие, изучаемое многими науками.

В уголовном праве личность преступника – это, прежде всего личность субъекта преступления, вменяемого, достигшего возраста уголовной ответственности и совершившего деяние виновно.

Криминологическое изучение личности преступника осуществляется главным образом для выявления и оценки тех ее свойств и черт, которые порождают преступное поведение, в целях его профилактики. В этом проявляется теснейшее единство трех узловых криминологических проблем: личности преступника, причин и механизма преступного поведения, профилактики преступлений.

В юридической психологии под личностью преступника понимают совокупность типологических качеств индивида, обусловивших совершенное им преступное деяние определенного вида [4, с. 79].

Криминалистическое рассмотрение личности преступника является составным элементом такого раздела криминалистики, как криминалистическая характеристика преступлений. Изучение личности носит несколько иной характер, чем в криминологии, психологии, уголовном праве. Объясняется это тем, что основной задачей криминалистического установления личности является использование информации для разработки тактики предварительного расследования. Личность преступника в криминалистике изучается постольку, поскольку знание ее особенностей может позволить облегчить расследование конкретных преступлений.

Криминалистику интересует, прежде всего, то, как психические качества конкретной криминальной личности могут проявиться в объективной действительности и какие следы могут быть оставлены.

Помимо междисциплинарного определения сущности понятия личности компьютерных преступников, таковых принято классифицировать по различным основаниям.

По уровню знаний и степени подготовки компьютерных преступников можно поделить на три группы:

1. Новички. Выпускники или студенты старших курсов технических ВУЗов, имеющие определенный уровень специальных знания. Средний возраст – 18–20 лет. Пол – в подавляющем большинстве случаев мужской. Образование – среднее, среднее специальное. Происходят из семей среднего достатка. Интерес к компьютерной технике проявился в большинстве случаев уже с 5–7 класса средней школы. Зачастую имеют дома один или несколько компьютеров, планшетов. Имеют свободный доступ к сети Интернет. Их знания не ограни-

чиваются языками программирования, и дополнительно включает в себя знание аппаратной части выбранной платформы. Рассматриваемые субъекты, как правило, не трудоустроены. Связь с обществом поддерживают в ограниченном объеме, предпочитая общение с людьми своего круга. В разговоре употребляют особый компьютерный сленг, смешивают русский и английский языки. Уровень гуманитарного образования явно ниже, чем технического. Характеризуются несобранностью, некоторой небрежностью, увлечены чтением специализированной литературы.

2. Сложившиеся. Возраст 20–25 лет. Пол – в основном, мужской, но наблюдается тенденция к увеличению числа лиц женского пола. Образование – среднее, среднее специальное, высшее, в основном – техническое. В большинстве случаев лица, принадлежащие к этой группе, имеют постоянную работу в качестве системных администраторов, консультантов в организациях специализирующихся на работе с информационными технологиями, что позволяет им в определенных случаях осуществлять модификации программного обеспечения потерпевшего в целях получения необходимой информации в личных, преступных целях.

3. Профессионалы. Возраст от 25 лет. Пол в большинстве случаев мужской. Семейное положение – с достатком выше среднего. Образование – высшее техническое, возможно дополнительно и иное. Обладают наивысшей степенью знаний в области компьютерных технологий. Владеют несколькими языками программирования, в совершенстве знают особенности аппаратной части компьютерных систем, имеют навыки профессиональной работы с несколькими компьютерными платформами. Личности крайне амбициозные. Пробуют профессионально программировать, но зачастую понимают, что официально в данной сфере много не заработать, и переходят в «теневую область». Работают в криминальной сфере довольно успешно. Добиваются очень многого. Для прикрытия, обычно трудоустраиваются в организации связанные с информационными технологиями.

В настоящее время все в большей степени становится актуальным изучение высококвалифицированных преступников, обладающих высоким уровнем специальной подготовки, позволяющим преодолевать современные средства защиты. Данные преступники представляют наибольшую опасность. Как правило, преступления совершаются ими дистанционным образом. Способы совершаемых преступлений высокотехнологичны, а их следы, как правило, сокрыты [6, с. 77].

Существенные коррективы в вопрос о личности преступника может вносить региональный аспект. Так, изученные на примере Алтайского края уголовные дела показали, что некоторые из высказываемых в криминалистической литературе мнений не являются для них характерными. Например, это относится к положению о том, что данные преступления совершаются в основном высококвалифицированными программистами и бывшими служащими потерпевших организаций. В Алтайском крае в качестве преступников выступали в основном мужчины, преимущественно в возрасте до 35 лет. Среди них – учащиеся ПТУ и школ (16 %), студенты вузов (25 %), работники предприятий, коммерческих организаций (17 %), частные предприниматели (4 %), работники государственных организаций и учреждений (4 %), значительную группу составляли нигде не работающие (30 %). Высшее или незаконченное высшее образование имели 48 % преступников. Профессиональной компьютерной подготовке большинство из этих лиц не обладало. Совершавшие данные преступления лица ранее были не судимы и часто при судебном разбирательстве характеризовались положительно [7, с. 15].

Также, для лучшего понимания личности компьютерного преступника важно рассмотрение их классификации по типу.

Существуют разные типологии компьютерных преступников. Согласно одной из них, следует проводить разграничение между следующими группами: профессиональные преступники (террористы – участники кибервойн), преступники в белых воротничках, недовольные служащие и подростки. М. Роджерс выделяет подгруппы хакеров по уровню компетентности, сферам интересов (мобильные телефоны, ПК, Интернет, кредитные карты) и характеру поведения: новички, кибер-панки, кодировщики, «старая гвардия», профессиональные преступники, пользующиеся своим знанием устройства системы служащие фирм (internals), кибер-террористы. Очевидно, что между группами нет четкой границы. В полном согласии с жизненной реальностью во все группы входят дети и подростки. Наименее квалифицированные подростки известны как «новички». Каждый день появляются «новички», которые видят в хакерстве модное хобби или выгодное занятие. «Новички» начинают с простейших заданий – просто для развлечения, далее некоторые из них обращаются к более сложным заданиям и постепенно становятся либо квалифицированными хакерами, либо профессионалами в области компьютерной безопасности; большинство же тех, кто пробует себя в этой сфере,

бросают ее на уровне «новичка» и, таким образом, покидают популяцию хакеров [1, с. 33–34].

Использование такого понятия, как хакер неслучайно. Хакер – это основное, базовое понятие обозначающее «компьютерных деятелей». Хакерами чаще всего именуются лица, которые осуществляют различные, в том числе иногда и противоправные действия в сфере высоких технологий. В большинстве же случаев, хакерами следует называть тех лиц, которыми движет позитивная мотивационная установка – обнаружить слабые места в компьютерных программах, системах, средствах защиты компьютерной информации с целью устранения найденных недостатков и/или внесением предложений по их устранению.

В зависимости от вида деятельности хакеры могут быть разделены на несколько групп.

Если хакер, в большинстве случаев действует с положительными намерениями, то его противоположностью выступает так называемый «крэкер».

При взломе компьютерной системы данное лицо стремится получить несанкционированный доступ к чужой информации, для использования ее именно в своих, как правило, корыстных или иных преступных целях (месть, хулиганские побуждения, озорство, промышленный или иной вид шпионажа и пр.).

Группа «крэкеров» также не является однородной и делится на три подгруппы:

1) «взломщики» – профессиональные «крэкеры», осуществляющие взлом компьютерных систем с целью хищений дорогостоящего программного обеспечения и денежных средств, а также промышленного и коммерческого шпионажа и т.д. Данная группа лиц обладает устойчивыми криминальными навыками. А совершаемые ими преступные посягательства, как правило, носят серийный характер. Профессиональный «крэкер» может действовать как в своих интересах, так и интересах третьих лиц;

2) «вандалы». Целью данной категории делинквентов является взлом компьютерной системы для ее последующего разрушения;

3) «шутники». Основная цель – незаконное внедрение в действующую компьютерную программу различных звуковых и/или визуальных эффектов [5, с. 35].

Также, представляется интересным, мнение Л. Джеймса, который считает, что наиболее распространенным видом компьютерных

преступников в XXI веке являются скрипт-кидди. В качестве основных признаков скрипт-кидди он называет: они молоды; они не очень хорошие хакеры; у них много свободного времени; они очень упорны; они используют прототипы кода, разработанного специалистами по обеспечению безопасности [3, с. 42–43].

Важно отметить, что приведенные вариации личности компьютерного преступника не носят исчерпывающего характера. Могут существовать и иные классификации.

В свою очередь, говоря о мотивационных психических состояниях лиц, совершающих преступления в сфере высоких технологий, важно отметить, что в большинстве случаев, такими преступниками движет стремление самоутвердиться, а также корысть и хулиганство.

Помимо мотивационных стремлений, большое значение для расследования преступлений имеет цель. Сведения о наиболее распространенных целях совершения компьютерных преступлений используются при организации целенаправленного поиска преступника, а также при выдвижении версий относительно таких элементов состава преступления, как субъект и субъективная сторона.

Наиболее типичными преступными целями являются: хищение наличных и безналичных денежных средств; подделка счетов и платежных ведомостей; приписка сверхурочных часов работы; фальсификация платежных документов; вторичное получение уже произведенных выплат; перечисление денежных средств на фиктивные счета; легализация преступных доходов; незаконные валютные операции; незаконное получение кредитов; манипуляции с недвижимостью; получение незаконных льгот и услуг; продажа конфиденциальной информации; хищение материальных ценностей, товаров и т.п.

Значение цели и мотивов выражается в том, что они несут на себе субъективный отпечаток, то есть выбор способа достижения преступного результата определяется конкретными свойствами личности. Следовательно, зная эти свойства, можно предположить, каким способом было совершено преступление. Конкретные мотивы и цели для ряда составов преступлений являются необходимыми или квалифицирующими признаками [2, с. 52].

Вместе с тем действия хакеров не всегда представляют общественную опасность, хотя формально и носят противоправный характер. Такое возможно, когда действия хакера продиктованы стремлением продемонстрировать свое «эго», бросить вызов обществу, показать свою независимость, бесстрашие и пр [5, с. 37].

Подводя итог, важно заметить, что знание основных черт и характеристик личности компьютерного преступника, а также тех целей, которых он желает достичь и мотивов подталкивающих на совершение преступлений, поспособствует повышению эффективности предварительного расследования и превенции компьютерных преступлений.

Список использованной литературы

1. Войскунский А.Е., Нафтульев А.И. Актуальные психологические проблемы кибер-этики // Гуманитарная информатика. 2007. № 3.

2. Гавло В.К., Поляков В.В. Криминалистическая характеристика преступлений в сфере компьютерной информации // Право и государство: приоритеты XXI века : матер. Всерос. науч.-практ. конф. / под ред. В.Я. Музюкина, Е.С. Аничкина. Барнаул : Изд-во Алт. ун-та, 2007.

3. Джеймс Л. Фишинг. Техника компьютерных преступлений / пер. с англ. Р. В. Гадицкого. М. : НТ Пресс, 2008.

4. Кирюшина Л.Ю. Юридическая психология: учебное пособие. Барнаул: Изд-во Алт. ун-та, 2011. С. 79.

5. Морар И.О. Как выглядит социально-правовой портрет участника преступного формирования, совершающего компьютерные преступления? // Российский следователь. 2012. № 13.

6. Поляков В.В. Региональные особенности криминалистической характеристики преступлений в сфере компьютерной информации // Региональные аспекты технической и правовой защиты информации : монография / В.В. Поляков, В.А. Трушев, И.А. Рева, Вит. В. Поляков, П.В. Малинин и др. Барнаул : Изд-во Алт. ун-та, 2013. Гл. 1.

7. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: автореф. дис. … канд. юрид. наук. Омск, 2008.

Информация об авторе

Мананников Антон Сергеевич – студент, федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Алтайский государственный университет», e-mail: manannikovanton35@mail.ru.

УДК 343.3/.7

Е.Э. Санок
Научный руководитель: О.В. Петрова

ЛИЧНОСТЬ КИБЕРПРЕСТУПНИКА

На современном этапе развития использование информационно-коммуникационных технологий в различных сферах человеческой жизнедеятельности является объективной реальностью. Развитие телекоммуникационных систем, всеобщая доступность в сети Интернет различного рода информационных ресурсов предоставляют злоумышленникам массу невиданных доселе возможностей по достижению преступных целей.

Быстрое внедрение во все сферы жизни электронных технологий, активное развитие телекоммуникационных сетей, всеобщая доступность персональных компьютеров и вед-ресурсов сети Интернет, наряду с положительными моментами, создает предпосылки к появлению принципиально нового вида нарушения Закона – киберпреступности.

Как показывает мировой опыт, проявление киберпреступности свойственно тем странам, которые в силу научно-технического прогресса перешли на новую – инновационную ступень своей развития. Число таких преступлений увеличивается прямо пропорционально росту телекоммуникационной инфраструктуры, парка ЭВМ и общему количеству лиц, освоивших их использование.

Также, следует отметить актуальность борьбы с киберпреступностью для стран СНГ, в которых показатели использования информационных технологий еще не достигли уровня западных государств и в дальнейшем компьютерные преступления могут стать серьезным препятствием для создания надежной информационной инфраструктуры.

Первое высокотехнологичное преступление на территории Республики Беларусь было зарегистрировано 20 ноября 1998 года. Внедрив в программное обеспечение «компьютера-жертвы» вредоносную программу типа «троянский конь» под названием «BackOrifice», злоумышленник осуществил несанкционированный доступ к сетевым реквизитам пользователей сети Интернет из числа клиентов крупнейшего в Беларуси столичного сервис-провайдера [11].

Очень важно понимать глобальность проблемы киберпреступности. Как верно заметил международный эксперт по гармонизации законодательства в сфере киберпреступности Штайн Шьольберг (Stein Schjolberg), «киберпространство, как пятое общее пространство, после наземного, морского, воздушного и космического, требует координации, сотрудничества и особых правовых мер на международном уровне» [15].

При выработке средств и методов борьбы с киберпреступностью следует помнить о латентности данного вида преступлений. Международная практика говорит о том, по оценкам экспертов латентность «компьютерных преступлений» в США достигает 80 %, в Великобритании – до 85 %, в ФРГ – 75 %, в России – более 90 % [2, с. 151].

Практика свидетельствует, что обнаружение таких преступлений затруднено и зачастую носит случайный характер. С учетом общественной опасности, высокой латентности, сложности расследования такого рода преступлений, особое внимание правоохранительных органов должно быть сосредоточено на их выявлении и качественном расследовании. Этому процессу способствует криминалистическая характеристика преступлений в сфере компьютерной информации, как часть методики расследования преступления, где большое значение имеет элемент, характеризующий личность преступника.

Для исследования психологии преступников наиболее подходит широкое толкование термина «киберпреступность», которое было рекомендовано экспертами ООН, данный термин охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. [9]. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде

Применение юридической психологии в расследовании киберпреступлений важно по целому ряду причин: отсутствие достаточного количества материальных следов преступника, широкое разнообразие возможных мотивов некоторых категорий киберпреступлений, порой неограниченный круг лиц, имевших возможность совершить преступление, а также потенциально большой вред, который может нанести киберпреступление. Кроме того, знание основ психологии киберпреступников поможет при разработке средств борьбы с киберпреступлениями, поскольку злоумышленники достаточно часто используют психологические приемы в своей деятельности.

Поскольку причины преступного поведения заключены в личности преступника, то, чтобы понять их, необходимо изучить эту личность, выявить те внешние по отношению к ней социальные явления и процессы, которые сформировали ее криминогенные черты. И само преступное поведение нужно изучать не только для его предотвращения или пресечения, но и для понимания его причин.

Кроме того, глубокие знания био-психо-социальных особенностей личности преступника, установление роли личностных факторов в механизме преступного поведения, изучение и анализ их субъективного восприятия индивидом – все это, вне всяких сомнений, значительно расширяет возможности правоохранительных органов в сфере борьбы с преступностью.

Преступления в сфере компьютерной информации обладают определенной спецификой, требующей от преступников наличие навыков, умения, знаний о функционировании компьютерных систем, свойств компьютерной информации, определенного программного обеспечения.

Для начала, мы проанализируем среду совершения киберпреступлений так называемое киберпространство. Данное понятие представляет собой образованную электронным устройством и их сетями среду, в которой с помощью технически-программных средств возможно создание эффекта присутствия пользователя в другом, отличном от реального – искусственном мире [3]. Для личности киберпреступника виртуальная реальность является самой желаемой и единственной реальностью, воплощающей для него действительность, в которой он существует и реализовывает свои преступные деяния. Настоящая объективная реальность для него скучна и неинтересна, однако биологически необходима.

В связи с этим, в условиях киберпространства существенно меняется психологическое содержание взаимосвязей преступник – предмет преступления, а также преступник – потерпевший, которые из прямых превращаются в опосредованные: преступник – электронное устройство (Сеть) – потерпевший (предмет преступления), что ведет к устранению материальной составляющей как действий человека, так и социального взаимодействия. При этом «виртуальные» предметы психологически кажутся более доступными, в том числе для незаконного завладения ими. Любые действия в таких условиях воспринимаются изначально как нематериальные по природе, соответственно, не несущие материальных, «серьезных» последствий. По

справедливому замечанию директора Центра безопасного и ответственного использования Интернета Нэнси Виллард (Nancy Willard), «информационно-коммуникационные технологии существенно ограничивают обратную связь, любое чувство осязаемой обратной связи наших действий. Поэтому отсутствует влияние осознания того, что мы причинили вред, но также мы считаем, что наше поведение не может причинить никакого вреда, потому что мы не видим вреда» [10].

Круг лиц, совершающих преступление в сфере компьютерной информации довольно широк. По данным специальных исследований это могут быть, как и высококвалифицированные специалисты, так и дилетанты, имеющие различный социальный статус и уровень образования [4].

Образовательный уровень лиц, совершивших данную категорию преступлений, является важным показателем интеллектуального уровня преступников и находится в определенной взаимосвязи с характером их преступных действий.

Одной из основ мотивации совершения киберпреступниками данных преступлений является высокая латентность преступлений, вследствие чего личности киберпреступника присуща полная анонимность. Анонимность позволяет быть не идентифицированным в определенный момент времени, а также предоставлять о себе ложную информацию, создавать новый образ собственной личности или сразу несколько образов, отличающихся от реального мира и не отягощенных психологической обязанностью следовать реальному образу, а также вступать при этом в социальное взаимодействие, представляясь другим лицом.

Кроме того, киберпреступник старается повысить уровень «компьютерной грамотности», что увеличивает латентность преступлений данного вида. Преступники заботятся о том, чтобы их неправомерных действия остались незамеченными для правоохранительных органов, поэтому раскрываемость таких преступлений представляет особую сложность.

Следует отметить, что в условиях анонимности любой человек ощущает возможность безнаказанно совершать поступки отрицательного характера, при этом отсутствие эффективных механизмов порицания только усиливает желание совершать негативные действия, особенно, если первопричина таких действий лежит в реальном мире. В то же время подобное ощущение безнаказанности влияет не только на отдельных лиц, но и создает атмосферу вседозволенности, которая

способствует дальнейшему распространению и развитию общественноопасных идей. Так, после терактов в Норвегии было установлено, что Андреас Брейвик был активным посетителем различных праворадикальных интернет-ресурсов [13]. Адвокат Брейвика заявил, что его подзащитный поддавался влиянию со стороны других интернет-пользователей ультраправых взглядов, в частности, со стороны блогера под ником «Fjordman», личность которого была установлена только после терактов [14].

Изучая категории лиц, привлекаемых к уголовной ответственности за нарушение закона в области информационной безопасности, сотрудники Управления «К» МВД Республики Беларусь пришли к выводу, что подавляющее большинство среди них составляют молодые люди в возрасте 18–29 лет (60,7 %). Вторым по массовости шли граждане от 30 лет и старше (33,3 %) [11].

Следует отметить, что удельный вес привлеченных несовершеннолетних составлял на тот момент всего 6,0 % от общего числа. Последнее взыскание опровергало бытующее мнение о том, что высокотехнологичные преступления, в подавляющем большинстве случаев, совершаются детьми.

На основании данного анализа был сделан вывод: «Киберпреступления – удел взрослых, уже сформировавшихся личностей, выбравших вполне осознанно модель своего поведения в обществе». В то же время, постоянный мониторинг ситуации показывает, что вышеуказанная аксиома в обозримом будущем рискует превратиться в теорему.

В отечественной практике имел место случай, когда тринадцатилетний белорус создал в интернете ресурс, на который предлагал перечислять средства для пострадавших от теракта 11 сентября 2001 года, который произошел в США. Данный случай был достаточно быстро изобличен белорусскими правоохранителями, но лицо и не было привлечено к уголовной ответственности в силу своего возраста [6]. В зарубежной практике также известные случаи совершения преступлений данного вида малолетними. Так, в Канаде в 2013 году был пойман одиннадцатилетний подросток, который написал вирус для хищения паролей в популярной игре [8].

По мнению специалистов, среди наиболее распространенных качеств «сетевых» преступников преобладает правовой нигилизм и завышенная самооценка [2, с. 170]. Такие лица, ощущая безнаказанность своих противоправных действий в глобальных сетях, часто

пренебрегают требованиями норм права, считают допустимым определять моральность тех или иных правовых норм на основе собственных критериев, часто проявляя определенный инфантилизм, безответственность, непонимание возможных опасных последствий противоправных действий. Как правило, при этом игнорируются интересы социума.

Рассматривая качества личности киберпреступников, нельзя не отметить присутствие у них определенных специфических положительных свойств. Эти люди, как правило, являются яркими, мыслящими личностями с активной жизненной позицией, обладающие оригинальностью (нестандартностью) мышления и поведения, осторожностью, внимательностью.

Отличительной особенностью некоторых киберпреступников является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и избирательности. Они весьма любознательные, обладают незаурядным интеллектом. При этом не лишены некоторого своеобразного озорства и спортивного азарта в достижении результата. Для многих из них характерны достаточный уровень квалификации, глубокие познания в области информационных технологий, высокая работоспособность, упорство. Эти сами по себе позитивные качества при выборе субъектом преступных способов достижения целей становятся элементами преступного профессионализма. В частности, высокий интеллект и профессиональная подготовленность позволяют преступнику достаточно полно оценить все возможные препятствия на пути достижения поставленных целей и выбрать оптимальный вариант поведения, просчитав вероятные действия правоохранительных органов.

Следует отметить, что лица, совершающие компьютерные преступления имеют коэффициент интеллекта (IQ) выше среднего, поскольку высокий уровень интеллекта необходим для написания компактной программы.

Подготовленность субъекта к реализации преступных замыслов определяется и наличием необходимых навыков. Изучаемые лица наиболее важными считают для себя такие качества, как опыт работы с информационными системами, умение программировать, способность быстро изучать новые языки программирования, умение общаться с людьми.

Как известно «мотивационная сфера является центром внутренней структуры личности, интегрирующим ее активность» [7, с. 107], а ее понимание позволяет решать сотрудникам правоохранительных органов целый ряд задач.

Анализ результатов зарубежных исследований называет пять распространенных мотивов компьютерных преступлений, расположив их в рейтинговом порядке:

1) корыстные соображения – 66 %,

2) политические цели – 17 %,

3) исследовательский интерес – 7 %

4) хулиганские побуждения и озорство – 5 %,

5) месть – 5 % [2].

Некоторые исследователи высказывают точку зрения о том, что данный список должен быть дополнен игровым мотивом, который криминологи считают одним из основных мотивов преступного поведения, отмечая его сложность и недостаточную изученность [1, с. 174]. Вступая в интеллектуальное противоборство с системами сетевой безопасности, подобные индивиды воспринимают свои действия как проверку своих навыков и сообразительности, способности адекватно оценивать ситуацию и быстро принимать решения. Также, в основе данного мотива лежит желание продемонстрировать собственный профессионализм – так называемый «интеллектуальный вызов» обществу и прославиться в кругу друзей.

Следует отметить, что в отдельных случаях у личности киберпреступника наблюдается определенная психологическая зависимость, выражающееся в навязчивой потребности осуществить взломы компьютерных сетей.

Так, в 1993 году в Англии на судебном слушании было признано, что обвиняемый в сетевых проникновениях Бедворт страдает такой зависимостью. Аналогичная потребность наблюдалась и у Кевина Митника, которого ФБР включало в список 10 наиболее опасных преступников США. Судья, выносивший приговор Митнику, объявил, что «видит определенную параллель между его пристрастием к взлому компьютерных сетей и влечением других людей к наркотикам»[5, с. 48–49].

Следует отметить, что мотивация киберпреступников формируется сразу в двух пространствах: реальном и киберпространстве. При этом на формирование мотивации большее влияние может оказывать и то и другое пространство. Киберпространство по-иному влияет на

мотивацию преступного поведения, так как оно является внетерриториальным и в нем происходит формирование своей собственной культурной среды – киберкультуры. Совершаются тяжкие преступления, явно исходя из мотивов, сформированных в киберсреде. Под воздействием ряда негативных факторов, присущих киберпространству, формируются новые нормы. Можно предположить, что поскольку киберпространство играет достаточно большую роль в жизни молодежи, то в сознании молодых активных пользователей Интернета происходит замещение социальных норм нормами киберпространства, точно так же могут нивелироваться социальные нормы реальной жизни, неприменимые во Всемирной сети.

Значительное место занимают психологические процессы, протекающие у личности киберпреступника при непосредственном совершении преступления. При совершении преступлений в сфере телекоммуникаций и компьютерной информации, преступник в отличие от других видов совершения преступных деяний, не контактирует с жертвой и зачастую находится от нее на значительном расстоянии: дома, месте с бесплатным доступом в Интернет, любом ином комфортном для него месте, вследствие чего киберпреступники могут не ощущать, или ощущать в значительно меньшей степени, дискомфорт, страх быть случайно обнаруженным и задержанным. Это, в свою очередь, позволяет злоумышленнику не ощущать неопределенности ситуации, планировать свои действия даже при неблагоприятных для него обстоятельствах, а значит, чувствовать себя более уверенно и спокойно во время совершения преступления.

Следует отметить, что если после совершения обычного преступления «на преступника, как правило, в большей степени начинает воздействовать фактор неопределенности своего положения, обусловленный, сознанием виновности и боязнью наказания, в случае же совершения киберпреступления действие данного фактора может уменьшаться, либо исключаться по двум причинам:

– во-первых, при совершении специальных киберпреступлений преступники, уверенные в высоком уровне своих знаний и возможностей, а порой и своей гениальности, предполагают, что не оставили ни единого следа, который мог бы помочь изобличить их;

– во-вторых, в настоящее время, особенно в странах СНГ, органы, ведущие борьбу с киберпреступностью, не всегда обладают достаточным интеллектуальным и кадровым потенциалом, что ведет к недооценке их киберпреступниками.

Таким образом, можно выделить основные теоретические положения о личности киберперступника, которому свойственны: повышенная скрытность совершения преступления, обеспечиваемая специфическим сетевым пространством, возможность совершать киберпреступления в автоматизированном режиме в нескольких местах одновременно, ощущение возможности совершать поступки отрицательного характера, инфантилизм, безответственность, непонимание возможных опасных последствий противоправных действий, достаточный уровень «компьютерной грамотности», необходимые навыки, специфические положительные свойства, правовой нигилизм и завышенная самооценка.

Предпосылки для совершения компьютерных преступлений появляются в результате сочетания таких факторов как мотивация, незанятость, отсутствие должного противодействия, наличие возможности.

Следует отметить выделение типовых характеризующих черт разных категорий «компьютерных» преступников, знание их основных черт способствует оптимизации процесса выявления лиц, облегчает процесс расследования. Так, знание личностных свойств субъектов преступной деятельности в сфере использования компьютерных технологий позволит оперативным работникам, следователям своевременно выявлять, раскрывать и расследовать такие преступления, определять тактику проведения допроса, криминалистических операций.

При разработке мер профилактики в борьбе с компьютерными преступлениями, в каждом государстве следует уделять особое внимание системе воспитания правосознания в области компьютерной информации среди молодежи и подростков.

Большое значение в борьбе с киберпреступностью имеет обмен полученной информацией между правоохранительными органами разных стран. В настоящее время достижения, полученные в области психологии киберпреступников, уже активно применяются в других странах при расследовании преступлений, в основном, при определении типа преступников. Исследования в данной сфере являются также важным теоретическим материалом и могут способствовать развитию изучения психологии девиантного поведения.

Как показывает сложившаяся ситуация, в борьбе с киберпреступностью и ее профилактике необходим мультидисциплинарный подход, в котором не последнее место занимает психология. Поэтому создание эффективной системы противодействия киберпреступлени-

ям требует активизации исследований психологии киберпреступников и подготовки кадров в данном направлении.

Кроме того, особое внимание необходимо уделять научному поиску эффективных путей повышения уровня информационной безопасности посредством совершенствования организационно-правовой защиты информации в компьютерных системах, а также совершенствованию правовых механизмов и законодательных норм.

Список использованной литературы

1. Антонян Ю.М. Психология преступника и расследования преступлений / Ю.М. Антонян, М.И. Еникеев, В.Е. Эминов; под ред. Ю.М. Антонян. М.: Юристъ, 1996. 336 с.
2. Варданян А.В. Расследование преступлений в сфере высоких технологий и компьютерной информации / А.В. Варданян, Е.В. Никитина. М.: Юрлитинформ, 2007. 307 с.
3. Голубев В.А. «Кибертерроризм» – миф или реальность? [Электронный ресурс]. 2015. Режим доступа: http://www.crime-research.org. Дата доступа: 05.04.2015.
4. Голубев В.А. Криминалистическая характеристика субъектов преступной деятельности в сфере использования компьютерных технологий. [Электронный ресурс]. 2015. Режим доступа: http://www.crime-research.org/library/Golubev0104.html. Дата доступа: 05.04.2015.
5. Зубков А. Кевин Митник вышел на свободу /А. Зубков // Мир Internet. – 2000. – № 3 – С.48-49.
6. Как не попасться на удочку интернет-мошенников? Советы из Управления «К»: [Электронный ресурс]. – 2015. – Режим доступа: http://42.tut.by/202087 – Дата доступа: 15.04.2015.
7. Лунеев В.В. Мотивация преступного поведения / В.В. Лунеев. – Москва: Наука, 1991. – 383 с.
8. Обзор СМИ: одиннадцатилетний преступник в Канаде [Электронный ресурс]. 2015. – Режим доступа: http://www.imena.ua/blog/cancybcr/. Дата доступа: 15.04.2015.
9. Преступления, связанные с использованием компьютерной сети / Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями [Электронный ресурс]. 2015. Режим доступа: http://www.uncjin.org/Documents/congr10/1r.pdf. Дата доступа: 05.04.2015.

10. Стенограмма Национальной конференции США по киберэтике [Электронный ресурс]. 2015. Режим доступа: https://connect. marymount.edu/ethics/cyberethics/track_3/session1_t3.PDF Дата доступа: 07.04.2015.

11. Управление по раскрытию преступлений в сфере высоких технологий (Управление «К») [Электронный ресурс]. 2015. Режим доступа: http://mvd.gov.by/ru/main.aspx?guid=3291 Дата доступа: 07.04.2015.

12. Чирков Д.К., Саркисян А.Ж. Преступность в сфере высоких технологий: тенденции и перспективы // NB: Национальная безопасность. [Электронный ресурс]. 2015. №2. Режим доступа: http://e-notabene.ru/nb/article_608.html Дата доступа: 07.04.2015.

13. How far right views created Anders Behring Breivik. [Электронный ресурс]. 2015. Режим доступа: http://mg.co.za/article/2011-07-31-how-far-right-views-created-anders-behring-breivik. Дата доступа: 15.04.2015.

14. Lippestad: Nettdebattanter har ansvar for terroren. [Электронный ресурс]. 2015. Режим доступа: http://www.aftenposten.no/ incoming/Lippestad-Nettdebattanter-har-ansvar-for-terroren-6714368.html – Дата доступа: 15.04.2015.

15. Stein Schjolberg. A cyberspace treaty – A United Nations convention or protocol on cybersecurity and cybercrime. [Электронный ресурс]. 2015. Режим доступа: http://cybercrimelaw.net/ documents/UN_12th_Crime_Congress.pdf. Дата доступа: 05.04.2015.

Информация об авторе

Санок Елена Эдуардовна – студент, Белорусский государственный университет, юридический факультет.

УДК 343.98

Р. Шагеев
Научный руководитель: С.И. Земцова

РАСПРОСТРАНЕНИЕ НАРКОТИКОВ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ КАК КИБЕРПРЕСТУПЛЕНИЕ

До середины 80-х годов в России одной из самых актуальных была проблема алкоголизма, но позже наметилась тенденция к ее перетеканию в проблему наркомании. Самое неутешительное то, что проблема наркомании в России затрагивает не только взрослых, но также детей и молодежь. После преступности, наркомания является второй по важности проблемой нашей в стране. Количество наркоманов увеличивается с катастрофической скоростью.

Современный мир характеризуется стремительным прогрессом в сфере распространения и развития информационно-коммуникационных технологий. Динамическое использование новых средств телекоммуникации, в частности Интернета, как мощного глобального информационного ресурса, привлекает широкие слои населения независимо от возраста, образования и социального статуса.

Сегодня наибольшую обеспокоенность вызывает вовлечение в наркопотребление и наркопреступность подрастающего поколения. Наркомания в России «молодеет» – 84 % наркоманов признаются, что впервые попробовали наркотики в возрасте менее 15 лет [4]. Используя несформированность мировоззрения и жизненных ориентиров подростков в их среде через средства массовой информации, в том числе Интернет, культивируется образ жизни, связанный с потреблением наркотиков и иных психостимуляторов, а также осуществляется их распространение.

Организация противодействия пропаганде наркотиков в условиях быстрого развития сферы информационных технологий, и особенно сети Интернет, потребовала принятия законодательных мер на национальном уровне, но является сложным и долгим процессом.

Интернет является общедоступным источником информации. Любой человек, имея компьютер и подключение к сети, может мгновенно получить сведения в любой области. Информация является абсолютно бесплатной и бесцензурной. Сеть предоставляет пользователю выбор, он сам решает, что смотреть. Сведения в Интернет обновляются ежесекундно, в режиме онлайн. Это объясняет, почему данное

средство массовой коммуникации является приоритетным для большой аудитории [1].

В связи с быстрым развитием сети Интернет, социальных сетей и разного рода мессенджеров множество людей стало заниматься предпринимательством в сети. Можно выделить ряд преимуществ такого предпринимательства:

Во-первых, сегодня Интернет доступен практически везде, а значит, создается возможность заявить о себе, предлагаемых товарах и услугах, в любом уголке Земли круглосуточно.

Во-вторых, для ведения бизнеса с помощью Интернет, достаточно иметь только компьютер, подключенный к Сети. Значит, есть возможность существенно сэкономить на аренде офисных, торговых и складских помещений. Виртуальные торговые витрины позволяют, не увеличивая товарные запасы, предлагать покупателям широкий ассортимент товаров от большого количества производителей.

Кроме того, для организации магазина в Интернет-сети требуется значительно меньше сотрудников, как результат, уровень издержек Интернет-бизнеса значительно ниже и предприниматели, поддерживая конкурентные цены, получают максимальную прибыль.

Развитию Интернет-коммерции способствуют следующие факторы:

1. Широкий охват населения возможностью доступа к сети Интернет (причем непрерывно растет доля населения, обладающая широкополосным доступом);

2. Распространение смешанных (традиционно-виртуальных) моделей ведения бизнеса и развитие комплексных каналов сбыта, включающих в себя электронную и традиционную составляющие [3];

3. Распространение мобильных устройств с возможностью подключение к Интернету.

Именно поэтому распространение и пропаганда наркотических средств перешло с улиц на просторы Интернет ресурсов и социальных сетей.

По данным многих социологических исследований, каждый второй подросток узнает о наркотиках из широкодоступных средств массовой информации, и в первую очередь из сети Интернет, которая сегодня является главным источником информации о наркотиках, в том числе о свойствах разных видов наркотиков, эйфорических ощущениях после их приема, местах приобретения и сбыта, способах и методах разработки наркотических средств, способах их домашнего

изготовления из свободно продаваемых в аптеках кодеиносодержащих препаратов, ценах на различные наркотики, преимуществах использования отдельных наркотических средств над другими [2].

Можно выделить два направления сетевой деятельности, поразному влияющие на наркотизм: пронаркотическое и антинаркотическое. Оба эти направления имеют довольно обширные сетевые ресурсы, немалая часть их сосредоточена и в русскоязычном пространстве [5].

Пронаркотические ресурсы насчитывают огромное количество WEB-страниц: реклама наркотических средств и их аналогов и связанного с их потреблением образа жизни получила широкое распространение в сети глобальной коммуникации Интернет. На поисковых серверах ведется статистика наиболее посещаемых сайтов по различным тематикам, и практически везде в первой десятке один-два пронаркотических сервера.

Существуют серверы, которые содержат большое количество текстов, подробно описывающих различные виды наркотиков и призывающих к их употреблению, а также описания психоделических переживаний. На многих «страничках» подробно указаны способы приготовления, пути введения, «дозировки», возможность сочетанного приема различных психоактивных веществ, даются советы, как вести себя при задержании органами правопорядка за хранение наркотиков, как уклониться или «обмануть» тест-контроль и т. п.

Антинаркотические ресурсы гораздо менее многочисленны. Альтернативная антинаркотическая деятельность в русскоязычном варианте находится в состоянии развития и представлена единичными и не всегда достаточными по объему серверами.

Как я уже говорил, большое распространение и развитие в последнее время имеют социальные сети. Они, как направление развития сети Интернет являются наиболее эффективными, так как данные ресурсы имеют большое количество активных пользователей. Такие пользователи просматривают страницы сайта ежедневно.

В последнее время доступ к социальным сетям все чаще получают несовершеннолетние в возрасте от 10 лет, так как их реальный указанный возраст никто не может проверить. Здесь люди находят друг друга, знакомятся и объединяются в группы по интересам. И один из самых страшных «интересов» – наркотики – не обошел и социальные сети. Пользователи Рунета активно создают в социальных сетях группы, пропагандирующие наркоманию, в которых они открыто заявляют о

своих пристрастиях. Таким образом, пропаганда наркотиков в социальных сетях охватывает практически все киберпространство. В группах не только предлагают наркотики, советуют, где лучше их приобрести, указывают цену, адреса наркодилеров, но и выступают за легализацию наркотиков. Восхваляют незаконные психотропные вещества в фильмах, песнях, книгах. Рассказывают об успешных людях, употребляющих наркотики, всячески поддерживают новичков.

В рамках борьбы с наркотиками, их распространением, пропагандой, а также во исполнение взятых на себя международных обязательств Российской Федерацией установлен запрет на пропаганду и рекламу наркотических средств, психотропных веществ и их прекурсоров, предусмотренный ст. 46 Федерального закона от 8 января 1998 г. № 3-ФЗ «О наркотических средствах и психотропных веществах»[1].

Кроме того, в Закон Российской Федерации «О средствах массовой информации»[2] внесены поправки, запрещающие распространение в СМИ, в том числе в компьютерных сетях, сведений о способах и методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, а также запрещающие пропаганду каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров, за исключением рекламы, рассчитанной на медицинских и фармацевтических работников.

В соответствии со ст. 7 Федерального закона от 13 марта 2006 г. № 38-ФЗ «О рекламе»[3] не допускается реклама наркотических средств, психотропных веществ и их прекурсоров. В качестве общего требования к рекламе установлен запрет побуждать к совершению противоправных действий.

Противодействие пропаганде наркотиков предусмотрено в качестве одной из основных задач по снижению спроса на наркотики в Стратегии государственной антинаркотической политики Российской

---

[1] О наркотических средствах и психотропных веществах: Федеральный закон от 8 янв. 1998 г. № 3-ФЗ // Собрание законодательства РФ.1998. № 2. Ст. 219.

[2] О средствах массовой информации: Закон РФ от 27 декабря 1991г. № 2124-1 // Российская газета. 1992. № 32.

[3] О рекламе: Федеральный закон от 13 марта 2006г. № 38-ФЗ (ред. от 28.12.2013) (с изм. и доп., вступ. в силу с 22.06.2014) // Собрание законодательства РФ. 2006. № 12. Ст. 1232.

Федерации до 2020 года[1]. Также ответственность за правонарушения в сфере пропаганды и рекламы наркотиков закреплена в статье 6.13 КоАП РФ.

Одно из последних изменений в законодательстве по противодействию наркотическим средствам было в ФЗ от 08.01.1998 № 3-ФЗ (ред. от 03.02.2015) «О наркотических средствах и психотропных веществах» (08 января 1998 г.), в котором вводится понятие – новые потенциально опасные психоактивные вещества, определяемые как вещества синтетического или естественного происхождения, включенные в Реестр новых потенциально опасных психоактивных веществ, оборот которых в РФ запрещен, а ст. 234.1 УК РФ предусматривается уголовная ответственность за их незаконные производство, изготовление, переработка, хранение, перевозка, пересылка, приобретение, ввоз на территорию РФ, вывоз с территории РФ в целях сбыта, а равно незаконный сбыт. Также изменения дают полномочия Федеральной службе по контролю за оборотом наркотиков (ФСКН) запрещать оборот новых потенциально опасных синтетических психотропных веществ.

ФСКН России обязана будет составлять реестр новых потенциально опасных психоактивных веществ, оборот которых в РФ запрещен; этот список должен публиковаться, в том числе в сети Интернет.

В заключении хотелось бы сказать, что, на мой взгляд, киберпреступность в виде распространения и пропаганды наркотиков в сети Интернет развивается по причине отсутствия грамотной, систематической работы по пресечению и профилактике таких преступлений. Также выявление и раскрытие таких преступлений требует специальных знаний как в области правового регулирования оборота наркотических средств, криминологической характеристики и профилактики наркопреступности, так и в области компьютерных и интернет-технологий. Также, правоохранительные органы должны заняться отслеживанием и последующим закрытием наркогрупп в социальных сетях, модераторам и администраторам надо быть более внимательными и проверять те группы и приложения, в названии которых содержится призыв даже к антинаркотической деятельности.

[1] Об утверждении Стратегии государственной антинаркотической политики Российской Федерации до 2020 года: Указ Президента РФ от 09 июня 2010г. № 690 (ред. от 28.09.2011) // Собрание законодательства РФ .2010. № 24. Ст. 3015.

Список использованной литературы

1. Бостанова Л.К. Особенности Интернета как канала коммуникации // Журналист. Социальные коммуникации. 2012. № 4.
2. Законопроект: за пропаганду наркотиков в интернете могут дать два года [Электронный ресурс]. Режим доступа: http://ria.ru/beznarko_law/20120709/695524827.html (дата обращения 01.07.2014)
3. Котляров И. Д. Тенденции эволюции электронной коммерции // Интернет-маркетинг. 2012. № 4.
4. Наркомания в России [Электронный ресурс]. Режим доступа: http://prozavisimost.ru/narkomaniya/narkomaniya-v-rossii.html (01.07.2014)
5. Щукин А.М. Интернет как средство влияния на потребление наркотических средств и их аналогов // Преступность в Западной Сибири: актуальные проблемы профилактики и расследования преступлений. Сборник статей по итогам всероссийской научно-практической конференции (28 февраля-1 марта 2013 года). Тюмень: ТюмГУ, 2013.

Информация об авторе

Шагеев Равиль – студент, ФГКОУ ВПО «Сибирский юридический институт ФСКН России», e-mail: ravil.95@mail.ru

УДК 343.98

В.В. Козленко
Научный руководитель: С.И. Земцова

К ВОПРОСУ О РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ СО СБЫТОМ НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»

На сегодняшний день очень сложно представить нашу жизнь без Интернета, ведь XXI век – это век информационных технологий. «Всемирная паутина» помогает нам на работе, в общении с родными и близкими, школьникам и студентам – в учебе. Вместе с тем, имеет-

ся и обратная сторона: использование информационных возможностей сети Интернет для совершения преступлений. Киберпреступность превратилась в целую криминальную отрасль, где действуют мошенники, взломщики-хакеры, педофилы, сутенеры, торговцы людьми и многие другие нарушители закона.

В последние несколько лет информационные возможности сети Интернет используются и для совершения преступлений, в сфере незаконного оборота наркотиков. Анализ судебно-следственной практики произведенной нами (всего было изучено 17 обвинительных заключений, находящихся в архиве кафедры криминалистики СибЮИ ФСКН России по уголовным делам, расследовавшимся в различных регионах России за период с 2012 по 2014 год) свидетельствует, что таким образом (с использованием сети Интернет) совершаются преступления связанные со сбытом и контрабандой наркотиков, легализацией наркодоходов и некоторые другие. Причем преобладающему их количеству присущ – организованный характер (только за 2014 год органами наркоконтроля расследовано 10,1 тысяч наркопреступлений, совершенных в организованных формах, что составляет 82 % от преступлений этой категории, расследованных всеми правоохранительными органами Российской Федерации (12,4 тысяч преступлений)).

При этом наиболее часто сеть Интернет используется для сбыта наркотических средств и психотропных веществ или их аналогов.

Законодатель был вынужден отреагировать на данную ситуацию. И 1 марта 2012 Федеральным законом №18-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» статья 228.1 УК РФ дополнена квалифицирующим признаком сбыт наркотических средств, психотропных веществ или их аналогов с использованием средств массой информации, электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») (наказывается лишением свободы на срок от пяти до двенадцати лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до одного года либо без такового).

С этого времени истекло три года, однако до настоящего времени не сформирована единая правоприменительная практика, отсутствуют соответствующие разъяснения Верховного Суда, а исследователями в криминалистики опубликованы лишь единичные работы [2, 3] посвященные данному вопросу.

Этот пробел негативно сказывается как на образовательной деятельности по преподаванию методики расследования данной категории преступлений, так и практической работе сотрудников правоохранительных органов. Не претендуя на его разрешение в полном объеме (в связи с ограниченным объемом эссе) на основе анализа судебно-следственной практики и научно-правовых источников, попытаемся раскрыть сущность способа совершения данной категории преступлений.

Способ совершения преступления – выражает функциональную сторону преступной деятельности; позволяет установить не только каким путем подготавливалось, совершалось и скрывалось преступление, но и о том, какие «действия преступника отразились в окружающей среде, т.е. какие следы, «отпечатки» действий преступника возникают в результате преступного посягательства, где их искать и как по ним восстанавливать механизм преступления [1, с. 688–689].

Отражение его специфики по рассматриваемой категории дел в свою очередь практически невозможно без уяснения *что же вообще понимается под сбытом наркотических средств, психотропных веществ или их аналогов?* Согласно Постановлению Пленума Верховного Суда РФ «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» № 14 от 15 июня 2006 г. под ним следует понимать *любые способы* их возмездной либо безвозмездной передачи другим лицам (продажу, дарение, обмен, уплату долга, дачу взаймы и т.д.), а также *иные способы* реализации, например путем введения инъекций». Упоминание в данном Постановлении «иных способов» полагаем, является обоснованным и принципиально значимым, поскольку перечисление всех традиционных являлось бы не логичным, а возникновение новых сложно было предполагать. В этой связи, используемый в последние годы и получивший широкое распространение способ сбыта: с использованием электронных или информационно – телекоммуникационных сетей (включая сеть Интернет), полагаем возможно отнести к ним («иным способам»).

Не менее значимым для уяснения рассматриваемого способа сбыта является получения ответа на вопрос о том, что понимается под электронными или информационно – телекоммуникационных сетями (включая сеть Интернет)? Ответ на него, впрочем как и на предыдущий, содержится в нормативно-правовых актах: в п. 4 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации,

информационных технологиях и о защите информации», а также в п. 2 раздела 1 Правил оказания телематических услуг связи, утвержденных Постановлением Правительства РФ от 10 сентября 2007 г. № 575. В частности, в них (данных нормативно-правовых актах) указывается, что информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Кроме того в указанных правилах содержится определение телематического электронного сообщения, под которым понимается одно или несколько сообщений электросвязи, содержащих информацию, структурированную в соответствии с протоколом обмена, поддерживаемым взаимодействующими информационной системой и абонентским терминалом [2].

Другими словами, электронной или информационно-телекоммуникационной является сеть, предназначенная для передачи и получения информации посредством проводных и сотовых телефонов, компьютеров и электронных терминалов перевода денежных средств.

Именно в использовании указанных сетей и проявляется специфика данного способа.

В связи с тем, что преобладающее количество преступлений совершается организованными преступными формами, участники которых состоят в определенной иерархии, рассмотрение способа совершения данной категории преступлений практически невозможно без уяснения функциональной роли каждого звена.

В частности, в организованных формах по данной категории преступлений возможно выделить: криминального лидера и рядовых членов.

Криминальный лидер, как правило, не имеет никакого контакта, как с наркотическими средствами, так и со многими участниками, выполняя лишь функции координатора, поэтому доказывании его причастности к совершению преступлений не всегда представляется возможным.

К функциям криминального лидера возможно отнести – осуществление общего руководства созданной им организованной группой и координацию ее действий, определение порядка и правил поведения, установление методов конспирации, способов связи при совершении преступлений с целью сокрытия совершаемых ими преступлений от правоохранительных органов; выработка способов в привле-

чения большего числа покупателей; подыскание поставщиков наркотических средств и т.д. [2].

Так, например по одному из уголовных дел, «Иное лицо», личность которого в процессе расследования установлена не была, используя созданные им в сети «Интернет» личный сайт « » и страницу « » в социальной сети «В контакте» в качестве завуалированной рекламы якобы «легальных наркотиков» для популяризации синтетических наркотических средств и приискания участников преступного сообщества, соблюдая конспирацию для сохранения в тайне своей личности привлек к участию в сообществе иных лиц. Разработал принципы действия, структуру преступного сообщества (преступной организации), составил план и схемы действия организованных групп, распределил роли между членами сообщества, установил единую стоимость реализуемого наркотического средства, организовал каналы поставки крупных партий наркотических средств, для сохранения монополизации наркорынка, давал указание на организацию сбытов других уже известных для потребителей видов наркотических средств, психотропных и сильнодействующих веществ [5].

К рядовым членам возможно отнести:

– *диспетчера*. Он отвечает за получение «заказов» от потребителей наркотических средств и их отправку закладчикам; контролирует поступление оплаты от потребителей наркотиков; получает адреса «закладки» наркотиков от закладчиков и отправляет их (данные адреса) наркопотребителям (прил. 4).

– *закладчика*. Последний по указанию диспетчера закладывает наркотическое средство в определенное место, адрес которого, а иногда и фотографию места закладки присылает диспетчеру.

Так, например по одному из уголовных дел, гражданин С в начале января 2013 года согласился вступить в преступную группу. В обязанности С входило: получение от Ш расфасованных мелким оптом партий наркотического средства героин; хранение мелких партий наркотического средства героин в целях совместного незаконного сбыта при себе и по месту своего проживания; помещение необходимого количества наркотического средства – героин, по указанию членов преступной группы, в заранее приготовленные тайники, места которых С определял сам, о чем сообщал неустановленному в ходе следствия лицу и Ш по своему мобильному телефону через глобальную телекоммуникационную сеть «Интернет» посредством программы «ICQ» и «Яндекс Почта». За выполнение своих функций в дея-

тельности преступной группы С получал от Ш денежное вознаграждение в сумме не менее 5000 рублей в зависимости от количества сбытого наркотического средства героин [4].

– *курьера.* Данный участник осуществляет расфасовку наркотических средств и периодически пополняет его количество у «закладчиков».

– *кассира*. Он снимает денежные средства, полученные через платежные терминалы, с банковских счетов и распределяет их между определенными членами группы, либо передает организатору данной группы.

Так, 38-летний житель г. Ухты входил в организованную преступную группу, которая занималась распространением на территории Республики Коми героина, поставляемого из Московской области. Он работал менеджером по продажам в одной из коммерческих фирм и подрабатывал «казначеем» в группировке – распределял и переводил на счета и банковские карты подельников деньги, полученные от продажи наркотиков. После ликвидации наркогруппировки и задержания ее членов, «кассир» находился под подпиской о невыезде. Все участники группировки получили наказание в виде лишения свободы от 6 до 12 лет. Понимая, что и ему грозит довольно большой срок, Мишарин скрылся в Голландии. Однако благодаря оперативному обмену информацией с компетентными органами Королевства Нидерланды преступника удалось задержать в кратчайшие сроки [8].

Достаточно часто функции нескольких участников выполняет одно лицо.

Анализ судебно-следственной практики выполненный С.И. Земцовой, свидетельствует, что электронные или информационно-телекоммуникационные сети (включая сеть «Интернет») перечисленными участниками при сбыте могут быть использованы [2]:

1. для рекламы наркотических средств, психотропных веществ и их аналогов посредством:

1.1. размещения специализированной страницы или группы уже в известных социальных сетях,

1.2. создания в сети «Интернет» web-сайта (или так называемого «интернет-магазина курительных смесей»).

Так, например, по одному уголовному делу было установлено, что Б. являясь организатором и руководителем организованной группы, сначала самостоятельно, а затем при помощи З., не осведомленного о его преступных намерениях, создал и обслуживал в сети «Ин-

тернет» web-сайт «…» (так называемый «интернет-магазин курительных смесей») для поиска покупателей и осуществления наркозависимыми лицами заказов наркотических средств и их аналогов под видом легальных благовоний (так называемых «аромомиксов»). Создавая и поддерживая в сети «Интернет» web-сайт «…» Б. преследовал цель расширения количества потребителей наркотических средств и их аналогов за счет неограниченного круга лиц, проживающих на всей территории Российской Федерации и пользующихся сетью «Интернет». Б. как сам лично, так и с помощью З. размещал на данном web-сайте информацию о сбываемых курительных смесях, содержащих наркотические средства и их аналоги, указывая ложную информацию о том, что они являются легальными, не запрещенными в гражданском обороте; создал и администрировал на данном web-сайте форум для общения пользователей с целью поддержания и повышения интереса к сбываемым веществам [6].

Кроме этого, электронные или информационно-телекоммуникационные сети (включая сеть «Интернет») могут быть использованы и для: *2. контактирования с потенциальным покупателем, 3. получения сведений об оплате 4. информирования о месте нахождения закладки.*

В частности, в рассмотренных нами ситуациях (создание специализированной страницы, группы в социальных сетях, либо «Интернет-магазина курительных смесей») данные цели как правило, реализуются посредством *переписки или звонков через социальные сети (например, Skype, ISQ.),*

Так, гражданин Т. имея умысел на незаконный сбыт наркотиков для воплощения своего преступного намерения в один из дней февраля 2012 года на территории города Архангельска объединился с гражданином М. на совершение преступлений, а именно на незаконное приобретение через сеть «Интернет», хранения в целях сбыта, а также незаконный сбыт наркотика на территории города Архангельска и Архангельской области бесконтактным способом, с использованием сети «Интернет». Для осуществления задуманного Т. создал на одном из сайтов страницу, на которой разместил объявление о продаже наркотического средства, зарегистрировался в программах «Skype» и «icq» под ник – неймом «….», и зарегистрировал банковскую карту на подставное лицо О., для последующего перечисления на нее денежных средств, выручаемых от незаконного сбыта наркотического средства.

В дальнейшем, посредством программ «Skype» и «icq» вышеуказанные лица (Т. и М.) получали заказы от потребителей наркотических средств, *вели с ними переписку*, в которой сообщали реквизиты банковской карты, после чего отслеживали поступление электронных платежей, поступающих в качестве оплаты, и таким же путем в ходе переписки уведомляли о месте закладки наркотического средства, так же высылали фотографию точного места закладки [7].

Вместе с тем, встречаются ситуации, размещения рекламы на фасадах зданий в виде номера телефона с зашифрованным наименованием распространяемого наркотика. В этом случае, контактирование, получения сведений об оплате, информировании о месте нахождения закладки осуществляется *посредством СМС – сообщений*. Оплата за продаваемые наркотические средства перечисляется на электронный кошелек. При этом номер электронного кошелька, как правило идентичен номеру сотового телефона, по которому диспетчер обращается с покупателем

Важную роль в установлении способа совершения преступления имеют сведения, полученные при производстве экспертиз – компьютерно-технической, компьютерно-сетевой аппаратно-компьютерной, экспертизы информации, содержащейся на устройстве и других.

Подводя итог, следует отметить что при расследовании сбыта, совершенного с использованием сети Интернет, должна быть доказана роль и функции каждого из перечисленных участников (закладчика, оператора, кассира, оператора). При этом особую сложность представляет установление личности криминального лидера, его взаимосвязь с остальными участниками преступной группы. Однако это тема для дальнейших научных исследований....

Список использованной литературы

1. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика. Ученик для вузов. Под ред. Р.С. Белкина. – М.: Норма – ИНФРА. М, 1999.

2. Земцова С.И. О некоторых элементах криминалистической характеристики сбыта наркотических средств, психотропных веществ и их аналогов, совершаемым с использованием электронных или информационно – телекоммуникационных сетей (включая сеть «Интернет») // Библиотека-криминалиста. 2015. № 1.

3. Контемирова Ю.В. К вопросу о выявлении и раскрытии незаконного сбыта наркотических средств и психотропных веществ, осуществляемого через терминалы экспресс оплаты, совершаемого организационными преступными группами // Актуальные проблемы выявления и предупреждения незаконного оборота и потребления наркотических средств: сборник материалов Всероссийской научно-практической конференции, г. Уфа, 23–24 июня 2011 года: под общ. ред. З.З. Абубакирова. – Уфа: УФСЗИПК ФСКН России, 2011.

4. Обвинительное заключение по обвинению гр. Шилко Д. М. в совершении преступлений, предусмотренных ч. 3 ст. 30 УК РФ, п. «г» ч. 4 ст. 228.1 УК РФ; ч. 3 ст. 30 УК РФ, п. «г» ч. 4 ст. 228.1 УК РФ и гр. Старчикова В.В., / Дело № 851110// Архив кафедры криминалистики СибЮИ ФСКН России за 2013 г.

5. Приговор Забайкальского краевого суда в отношении гр. Р, , обвиняемой в совершении преступлений, предусмотренных ч. 2 ст. 210 УК РФ, ч. 3 ст. 30, п.п. «а, г» ч. 3 ст. 228.1 УК РФ, ч. 3 ст. 30, п. «а» ч. 3 ст. 228.1 УК , ч. 3 ст. 30, п.п. «а, г» ч. 3 ст. 228.1 УК РФ РФ, ч. 3 ст. 30, п.п. «а, г» ч.3 ст. 228.1 УК РФ РФ, ч. 3 ст. 30, ч. 3 ст. 234 УК РФ, ч. 3 ст. 30 п.п. «а» ч. 3 ст. 228. 1 УК РФ, ч. 2 ст. 228 УК РФ от 9 апреля 2013 г. / Дело № 2-30-2013.

6. Уголовное дело № 1153-50/54 в отношении Б1, Б2, Б3, Б4 и П. обвиняемых в совершении преступлении предусмотренных частью 3 статьи 228.1 УК РФ и иных составов, расследованное СС УФСКН России по Оренбургской области и направленное прокурору в октябре 2012 года // Архив кафедры криминалистики СибЮИ ФСКН России за 2013 г.

7. Уголовное дело № 12850164 в отношении Т., обвиняемого в совершении преступлений, предусмотренных ч. 2 ст. 228; ч. 1 ст. 30, п.п. «а», «г» ч. 3 ст. 228.1; ч. 1 ст. 228 УК РФ расследованное СО Регионального УФСКН России по Архангельской области, направленное прокурору 04 октября 2012 года // Архив кафедры криминалистики СибЮИ ФСКН России за 2013 г.

8. http://www.fskn.gov.ru/includes/periodics/news_all/2012/1022/001520969/detail.shtml (дата обращения 27.04.2015).

Информация об авторе

Козленко Виктория Витальевна – студентка, Федеральное государственное казенное образовательное учреждение высшего профес-

сионального образования «Сибирский юридический институт Федеральной службы по контролю за оборотом наркотиков».

УДК 343.98

Д.В. Агапов
Научный руководитель: С.Ю. Ударцев

СКИММИНГ КАК УГРОЗА СОВРЕМЕННОГО ОБЩЕСТВА

В эпоху информационного общества, когда компьютеры и телекоммуникационные системы охватывают все сферы жизнедеятельности человека и государства, общество поставило себе на службу телекоммуникации и глобальные компьютерные сети, не предвидев, какие возможности для злоупотребления создают эти технологии. Сегодня жертвами преступников, орудующих в виртуальном пространстве, могут стать не только люди, но и целые государства.

По данным Бюро специальных технических мероприятий МВД России (далее – БСТМ МВД России), число компьютерных преступлений в России в 2013 году увеличилось на 8,6 % [5]. В 2013–2014 гг. наиболее крупная доля компьютерных преступлений, приходилась на мошенничество (37 %), за которым следует неправомерный доступ к компьютерной информации (19 %) и распространение детской порнографии (16 %). По 8 % от всех совершенных за этот период компьютерных преступлений приходится на компьютерное пиратство и распространение вредоносных программ.

По данным отчета Group-IB [7], со второй половины 2013 года по первую половину 2014 года русскоговорящие киберпреступники заработали в России и СНГ порядка 2,5 млрд дол. Из указанной суммы 426 млн дол. пришлось на интернет-мошенничество, существенная часть которого – 289 млн дол. – происходит в системах интернет-банкинга. На обналичивании денежных средств в России киберпреступники заработали 59 млн дол., на банковском фишинге (скиммиг) и мошенничестве с электронными деньгами – 50 млн дол., на хищении электронных денег – 28 млн дол.

Скимминг (от англ. skimming – в дословном переводе – снятие пенок с молока) при котором используется скиммер – инструмент злоумышленника для считывания, например, магнитной дорожки

платежной карты. При осуществлении данной мошеннической операции используется комплекс скимминговых устройств.

Исходя из вышеизложенного, в целях предупреждения преступлений представляется важным исследование способов хищений денежных средств граждан с использованием скимминговых устройств, чем и обуславливается актуальность рассмотренных вопросов.

Объектом исследования являются общественные отношения, возникающие в результате совершения преступлений с использованием скимминговых устройств, а предметом исследования выступают закономерности преступной деятельности по совершению рассматриваемых преступлений.

Целью настоящей научной работы является изучение и анализ основных способов скимминга для формулирования рекомендаций по противодействию указанным преступлениям. Гипотеза научного исследования заключается в том, что существующие методы предупреждения и раскрытия преступлений с использованием скимминговых устройств не соответствуют уровню «профессионализма» преступников и способам совершения указанных преступлений.

Основной задачей настоящей работы является обобщение имеющегося опыта по изучению способов совершения преступлений с использованием скимминговых устройств.

Теоретико-методологической основой работы являются результаты проведенных исследований специалистами в области уголовного права, криминологии, криминалистики, оперативно-розыскного права и др., а так же мнения специалистов в области противодействия киберпреступности, находящиеся в сети Интернет и других информационных массивах.

Что касается технологии скримминга, то можно отметить следующее.

Скимминг является один из распространенных способов мошенничества. Технология скимминга проста: с магнитной полосы карточки снимается копия с использованием специального оборудования, затем наносится на «белый пластик», которую впоследствии используют для получения денежных средств в банкоматах, после чего мошенник преспокойно снимает деньги с карточного счета. Для расчетов в магазинах, изготавливается карта с графическим дизайном, чтобы кассир не смог определить, что она поддельная.

Мошенники, занимающиеся скиммингом, используют специальные технические средства, которые устанавливаются непосредст-

венно на банковский терминал. К примеру, на банкомат устанавливается микровидеокамера, которая фиксирует, как вы набираете ПИН-код, а также фотографирует номер карты. Иногда этой информации достаточно, чтобы оплатить покупки в интернете, поэтому мошенникам даже нет необходимости считывать данные с магнитной ленты кредитного пластика.

Скимминговое устройство представляет собой электронное устройство, выполненное на полимерном основании Г-образного сечения габаритными размерами 332х38х13 мм, которое с внешней стороны имеет лакокрасочное покрытие серого цвета. В центральной части основания имеется отверстие диаметром приблизительно 1 мм. С внутренней стороны основания закреплены устройство в полимерном корпусе черного цвета, розетка двухконтактного электрического разъема, электрический движковый переключатель и две аккумуляторные батареи номинальным напряжением 3,7 В, соединенные параллельно.

Устройство в полимерном корпусе черного цвета представляет собой печатную плату со смонтированными радиоэлектронными элементами, в том числе модулем видеокамеры, микрофоном и держателем с установленной картой памяти типа microSD. По внешнему виду и характерным конструктивным особенностям устройство является миниатюрным видеорекордером. По внешнему виду представленное устройство похоже на элемент передней панели некоторых моделей терминалов дистанционного банковского обслуживания – банкоматов.

Но есть и более сложные технологии скимминга. В этом случае на банкомат устанавливается специальная накладка (скиммер), которая считывает информацию с самого сердца кредитной карты – с ее магнитной ленты. Естественно, если клиент банка заметит такое устройство, он не станет пользоваться таким банкоматом. Поэтому мошенники изобрели скиммеры, которые очень трудно заметить неискушенным взглядом.

Одно из скимминговых устройств представляет собой электронное устройство, смонтированное в корпусе сложной формы, имеющем окружность в основании, и выполненном из полимерного полупрозрачного материала зеленого цвета. Наибольший диаметр корпуса 87 мм, высота 49 мм. В корпусе устройства имеется прямоугольное отверстие размерами 55х2,5 мм, в правой части которого закреплены расположенные друг напротив друга магнитная головка и прижимной выступ.

На внутренних поверхностях корпуса с помощью двухсторонней клеящей ленты закреплены радиоэлектронная сборка, состоящая из печатной платы с установленными радиоэлектронными элементами и источник электрического питания (миниатюрная аккумуляторная батарея). Источник электрического питания присоединен к радиоэлектронной сборке отрезками монтажного электрического провода с помощью разъемного соединения. По внешнему виду представленное устройство похоже на элемент антискиммингговой защиты некоторых моделей терминалов дистанционного банковского обслуживания (банкоматов).

Изготавливается специальное устройство, которое чаще всего помещается поверх картоприемника банковского терминала. Карта, помещенная в такой картоприемник с «сюрпризом», проходит через миниатюрный запоминающий чип, который считывает конфиденциальные данные с магнитной ленты и записывает в устройство память скиммера. Клиент ничего не заметит, ведь карта не задерживается в банкомате дольше обычного, поскольку процедура считывания работает автоматически и мгновенно.

Другое сложное устройство представляет собой электронное устройство, смонтированное в полимерном корпусе сложной формы габаритными размерами 76х32х26 мм, имеющем лакокрасочное покрытие серого цвета. В корпусе устройства имеется прямоугольное отверстие (щель) размерами 55х2 мм. В левой части отверстия с внутренней стороны корпуса устройства закреплена магнитная головка, над которой закреплен эластичный прижимной ролик, выполненный из полимерного материала черного цвета. С внутренней стороны корпуса имеются две ниши, в одной из которых полупрозрачным полимерным компаундом закреплены радиоэлектронная сборка, розетка четырехконтактного электрического разъема и электрический движковый переключатель, а в другой миниатюрная аккумуляторная батарея и розетка двухконтактного электрического разъема. По внешнему виду представленное устройство похоже на элемент картоприемника некоторых моделей терминалов дистанционного банковского обслуживания (банкоматов).

Для считывания ПИН-кода применяются накладные клавиатуры (тонкие и незаметные), миниатюрные видеокамеры, прикрепленные на козырьках или на других поверхностях банкоматов. Но самое обидное, что иногда скимминг «работает» даже не в банковских терминалах, а в кассах магазинах, поскольку известны случаи мошенни-

чества со стороны работников торговых точек, которые применяют для этого портативные скиммеры. В этом случае вам еще труднее будет обнаружить аферу: ведь вы психологически доверяете сотруднику магазина, а операции, выполняемые ими с вашей картой, виртуозны и отточены.

Представляет интерес и способ, получивший название «ливанская петля». Суть его заключается в том, что мошенник изготавливает из фотопленки специальный карман, который помещает в считыватель карт банкомата. Концы кармана мошенник незаметно закрепляет снаружи считывателя и ждет. Владелец карты, решив снять деньги, вставляет в банкомат карту, вводит пин-код и снимает некоторую сумму. Только банкомат в данном случае карту не возвращает. Вдруг «добрый» человек из очереди вызывается ему помочь, мотивируя тем, что с ним такое тоже случалось. Он нажимает какие-то кнопки, успокаивает попавшего в беду клиента, а по сути через минуту-две владелец невольно сообщаете ему пин-код. Извлечь карту никак не получается, и «добрый» человек советует обратиться в банк. Даже если позвонить в банк, то скорее всего скажут, что карту извлекут лишь в конце дня при инкассации. Жертве ничего не остается, как пойти дальше и ждать звонка из банка. В это время мошенник извлекает петлю и забирает банковскую карту, а ПИН-код ему уже известен [5].

В настоящее время на территории Российской Федерации распространенными преступлениями в сфере высоких технологий являются кардинг (вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем) и скимминг.

Проблема противодействия указанным выше преступлениям – это комплексная проблема. Для противодействия рассматриваемым преступлениям необходимо проводить целенаправленную работу по совершенствованию законодательства, регулирующего распространение информации в телекоммуникационных сетях, наладить взаимодействие и координацию усилий правоохранительных органов, спецслужб, судебной системы, обеспечение их необходимой материально-технической базой. Способствовать повышению эффективности мер, принимаемых правоохранительными органами, будет знание их сотрудниками способов совершения преступлений с использованием скимминговых устройств.

Список использованной литературы

1. «Пластик» защитят от мошенников чипом. Режим доступа: http://www.rg.ru/2013/08/13/karti-site.html.
2. Защита банкоматов: почему цены на скиммеры падают, а на антискиммеры растут? Режим доступа: http://sia.ru/?section=492&action=show_news&id=273828.
3. Идет вторая волна воровства денег с банковских карт. Режим доступа: http://www.gazeta.ru/techzone/2011/10/21_a_3808934.shtml.
4. МВД заявило об увеличении числа киберпреступлений. Режим доступа: http://www.festinato.ru/news/obschestvo/mvd-zayavilo-ob-uvelichenii-chisla-kiberprestuplen/.
5. Мошенничество с пластиковыми картами. Режим доступа: http://vlfin.ru/posts/moshennichestvo-s-plastikovimi-kartami.html.
6. Шимминг – новая разновидность скимминга. Режим доступа: http://www.securitylab.ru/news/395811.php.
7. http://www.group-ib.ru/.

Информация об авторе

Агапов Даниил Александрович – курсант факультета по подготовке следователей Краснодарского университета МВД России.

УДК 343.98

Д.А. Лашина
Научный руководитель: О.В. Петрова

ТАКТИКА ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

В современном мире наука представляет собой основополагающий фактор производства. В результате научно-технической революции место человека в системе управления и производства значительно изменились. Благодаря применению компьютерных технологий существенно ускоряются процессы, связанные с выработкой и использованием информации. На современном этапе развития, как отмечают ав-

торы Крис Просис и Кевин Мандиа, компьютер является сокровищницей личной и профессиональной информации. Типичный компьютер является хранителем личных контактов, финансов и корреспонденции для обычного человека, а также средством помощи в решении задач и достижении целей государственного масштаба [11, с. 94]. Компьютер представляет собой уникальное устройство, способное упростить жизнь его пользователей, выполнить сложные вычислительные процессы и просто является неотъемлемым атрибутом современного человека. В то же время, по мере модернизации и совершенствования техники, видоизменяются и усложняются общественные отношения, а, следовательно, нарушения, которые происходят в обществе, начинают приобретать новую, ранее неведомую форму.

Если обратиться к истории, то следует отметить, что компьютерные преступления впервые попали в сферу специального контроля в начале 70-х гг. в США. Первым преступником относительно данной категории преступлений стал Альфонсо Конфессоре, совершивший налоговое преступление на сумму 620 тысяч долларов и в 1969 г. представший за это перед американским судом. Его признали виновным в 20 окружных судах США.

Изначально борьба с компьютерными преступлениями велась при помощи правовых норм, которые предусматривали ответственность за кражу, мошенничество, присвоение и т.д. Однако уже стал очевидным тот факт, что сформировался новый уровень общественных отношений, нарушение которых не соответствовало на тот момент существующим составам преступлений. Решение данной проблемы осуществлялось в двух направлениях:

– во-первых, происходило более широкое толкование традиционных норм и их применение по аналогии;

– во-вторых, разрабатывались специализированные нормы о компьютерных преступлениях [7, с. 8].

Среди стран, которые первыми пошли по пути разработки и принятия специальных норм о компьютерных преступлениях, можно назвать Швецию (1973 г.), США, Великобританию, Австрию, Канаду (июль 1985 г.), Данию (декабрь 1985 г.), Австралию, Францию, Португалию (1982 г.) и другие страны. В странах СНГ разработка соответствующей правой базы осуществлялась позже, в начале 90-х гг. [7, с. 9, 11]. Если конкретно говорить про Республику Беларусь, то впервые о проблеме борьбы с компьютерной преступностью в Беларуси было официально заявлено в 1998 году – с момента выявления перво-

го преступления, совершенного с помощью компьютерных технологий. Дальнейшее развитие борьбы с компьютерной преступностью проводилось с принятием нового Уголовного кодекса, который вступил в силу 1 января 2001 года, и в который вошла глава 31 – «Преступления против информационной безопасности».

28 ноября 2002 года было создано управление по раскрытию преступлений в сфере высоких технологий (УРПСВТ, или управление «К»), а спустя два года появились аналогичные отделы в структуре криминальной милиции УВД облисполкомов (кроме ГУВД Мингорисполкома, УВД Минского облисполкома и УВД на транспорте, где раскрытием данных преступлений занимаются сотрудники управления «К») [10].

Однако современные технологии развиваются неимоверно быстро в наши дни, и порой уголовное законодательство не успевает приводиться в соответствие с такого рода изменениями. Если обратиться к статистике, то за 12 месяцев 2014 года в Республике Беларусь число выявленных преступлений в сфере высоких технологий составило 2290 преступлений, в том числе по областям: Брестская – 243, Витебская – 261, Гомельская – 351, Гродненская – 205, Минская – 273, Могилевская – 249, Минск – 708. Доля хищений путем использования компьютерной техники (статья 212 УК РБ) от общего числа выявленных по-прежнему велика (88,8 %) и составила 2033 преступления данной категории [13].

Среди основных тенденций развития компьютерной безопасности можно выделить следующие:

1) крайне высокие темпы роста;

2) корыстная мотивация большинства совершенных компьютерных преступлений;

3) усложнение способов совершения компьютерных преступлений и появление новых видов противоправной деятельности в сфере компьютерной информации;

4) рост криминального профессионализма компьютерных преступников;

5) высокий уровень латентности компьютерных преступлений;

6) перенос центра тяжести на совершение компьютерных преступлений с использованием компьютерных сетей [6].

Нельзя обойти стороной тот факт, что компьютерные преступления не являются проблемой национального уровня, а носят транснациональный характер. В связи с этим особого внимания по указан-

ным категориям дел требует оказание международной правовой помощи. Исходя из вышесказанного, считаю необходимым отразить в своей работе наличие ограниченного количества уголовно-процессуальных норм, регламентирующих порядок оказания международной правовой помощи по делам о преступлениях в сфере высоких технологий.

Серьезным шагом в борьбе с киберпреступностью на мировом уровне явилось принятие Европейской Конвенции по киберпреступлениям (преступлениям в киберпространстве) Будапешт, 23 ноября 2001 г. Однако, принимая во внимание тот факт, что современный мир живет в эпоху глобализации, между государствами происходят непрерывные процессы интеграции, в борьбе с компьютерными преступлениями не все государства согласны оказывать взаимную помощь друг другу и стараться выработать единую тактику борьбы. Вышеупомянутая Конвенция не была подписана такими крупными государствами, как Россия и Китай, не подписали ее также страны Латинской Америки и Республика Беларусь. На мой взгляд, интеграция в данной сфере является необходимым условием, т.к. компьютерными преступлениями причиняется вред основополагающим Конституционным правам личности таким как: право собственности, закрепленное впервые во Французской Декларации прав человека и гражданина 1789 г.; право на защиту от незаконного вмешательства в личную жизнь, в том числе от посягательства на тайну корреспонденции, телефонных и иных сообщений, на честь и достоинство личности и иным правам [5].

В своей работе я также хотела бы обратить внимание на недостатки, которые, на мой взгляд, имеют место на стадии предварительного расследования, а также на обычные ошибки, которые происходят при получении доказательств из-за того, что не учитывается специфика совершенного деяния. Часто имеет место недооценка области действия инцидента; отсутствие плана реагирования на инцидент; небрежность в поддержке надлежащей документации; небрежность в уведомлении или предоставлении аккуратной информации специалистам, принимающим решения [11, с. 96].

Сегодня опасной угрозой киберпреступности являются распространение и передача материалов, связанных с детской порнографией, через глобальную сеть Интернет. Ощущается необходимость принятия неотлагательных мер, способствующих снижению случаев рас-

пространения и передачи таких материалов через глобальную сеть Интернет.

Проблемы правовой регламентации оказания международной правовой помощи по делам о компьютерных преступлениях.

В наши дни компьютерные технологии все больше и больше стирают границы между государствами, позволяя совершать опасные деяния мирового масштаба. Как уже было отмечено, серьезный шаг в борьбе с киберпреступностью на мировом уровне был сделан с принятие Европейской Конвенции по киберпреступлениям (преступлениям в киберпространстве) Будапешт, 23 ноября 2001 г. (далее – Конвенция), возможность присоединения к которой была рассмотрена Республикой Беларусь. Аргумент против присоединения к Конвенции приводит Российская Федерация, считая, что Будапештская конвенция предусматривает возможность, не ставя в известность то или иное государство, правоохранительным органам другого государства иметь доступ к ресурсам, размещенным в сетях общего пользования этого государства [12]. Указанное положение закреплено в ст. 32 Конвенции [3].

Опасаясь за свою национальную безопасность, Россия придерживается подхода оперативного и адекватного взаимодействия правоохранительных органов стран между собой и недопущения расследований преступлений на чужой территории, не ставя в известность правоохранительные органы соответствующего государства [12]. Однако нельзя не принимать во внимание тот факт, что на сегодняшний день компьютерные преступления – это явление, которое «не имеет границ». Данные преступления носят транснациональный характер, поскольку подпадают под все критерии, предусмотренные Конвенцией Организации Объединенных Наций против транснациональной организованной преступности 15.11.2000 г. (г. Палермо), участницей которой является и Республика Беларусь [8].

Расследование данных преступлений требует незамедлительной реакции со стороны органа уголовного преследования. Существенные трудности возникают, если составом определенного преступления причиняется вред нескольким государствам одновременно.

На сегодняшний день в Республике Беларусь помощь другим государствам в расследовании компьютерных преступлений может осуществляться лишь на основе норм об оказании международной правовой помощи по уголовным делам или на основе принципа взаимности. Согласно ст. 1 Закона Республики Беларусь «О международ-

ной правовой помощи» от 18 мая 2004 г. № 284-З *международная правовая помощь по уголовным делам* – это выполнение органами Республики Беларусь, ведущими уголовный процесс, процессуальных и иных действий по просьбе органов иностранных государств, компетентных принимать решения по вопросам оказания международной правовой помощи по уголовным делам, а также выполнение аналогичных действий органами иностранных государств, ведущими уголовный процесс, по просьбе органов Республики Беларусь, ведущих уголовный процесс, в соответствии с международными договорами Республики Беларусь или на основе принципа взаимности [9]. В Уголовно-процессуальном кодексе Республики Беларусь не регламентируются особенности оказания международной правовой помощи на основе принципа взаимности в расследовании преступлений в сфере высоких технологий, а также иных преступлений, при расследовании которых необходимо получение доступа к компьютерным данным [8].

Неоднозначно трактуется в различных правовых системах понятие преступления. Необходимо отметить, что если деяние, в связи с которым поступила просьба органа иностранного государства, не является преступлением, то в оказании международной правовой помощи будет отказано, что опять возвращает к проблеме отсутствия единого международного акта, который бы позволил привести национальное законодательство в соответствие с международными стандартами.

Касаясь непосредственно процедуры оказания международной правовой помощи, хочу заметить, что Будапешская Конвенция призывает к непосредственному контакту органов уголовного преследования по вопросам оказания международной правовой помощи, закрепляя это положение в пункте 3 статьи 25 [3].

Законодательство Республики Беларусь не предусматривает такого упрощенного порядка взаимодействия. Соблюдая порядок, установленный Уголовно-процессуальным кодексом Республики Беларусь для данной процедуры, взаимодействие происходит через Генеральную прокуратуру Республики Беларусь, что, на мой взгляд, значительно усложняет и затягивает процедуру [14].

Одним из способов решения этой проблемы, способствующему как повышению эффективности работы в противодействии киберпреступности, так и дальнейшему развитию международного сотрудничества, является Римская/Лионская группа. Римская/Лионская группа – это рабочий орган «Группы восьми», который специализируется на

проблематике противодействия терроризму и транснациональной организованной преступности. В настоящее время указанная международная сеть национальных контактных пунктов имеется в 58 странах всего мира, среди которых Россия, Украина, Германия, Великобритания, США, Испания, Швеция, Бразилия и др. Однако данный рабочий орган не имеет возможности обеспечить контакт органов уголовного преследования в полной мере, а лишь оказывает содействие по отдельным вопросам. В то же время национальный контактный пункт (НКП) УРПСВТ МВД Республики Беларусь позволяет оперативно обмениваться информацией о готовящихся, совершаемых либо совершенных преступлениях в киберпространстве, а также запрашивать необходимую для проведения оперативно – розыскных мероприятий и следственных действий техническую и иную информацию из аналогичных подразделений правоохранительных органов государств–участников информационного обмена [4].

Однако, на мой взгляд, существует необходимость того, чтобы уголовно-процессуальное законодательство закрепило нормы, регламентирующие оказание срочной международной правовой помощи в сокращенном порядке. Также законодательство должно быть восполнено нормами, которые бы делали отсылку к Международным договорам по взаимодействию в оказании международной помощи органам ведущий уголовным процесс при расследовании компьютерных преступлений, и которые позволяли бы беспрепятственно выходить на прямой контакт с соответствующими органами другим государств.

Особенности проведения обыска и выемки цифровой информации на стадии предварительного расследования.

Обыск и выемка являются важными следственными действиями при расследовании компьютерных преступлений. Основанием для проведения обыска является наличие достаточных данных полагать, что в каком-либо помещении или ином месте либо у какого-либо лица находятся орудия преступления, предметы, документы и ценности, которые могут иметь значение для уголовного дела, а также могут быть обнаружены разыскиваемые лица и трупы. Данное положение закреплено в ст. 208 Уголовно-процессуального кодекса Республики Беларусь (далее – УПК РБ) от 16 июля 1999 г. № 295-З и практически идентично с тем положением, которое закрепляет Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (далее – УПК РФ).

Согласно ст. 209 УПК РБ основанием для проведения выемки являются достаточные данные о наличии определенных предметов и документов, имеющих значение для уголовного дела, если точно известно, где и у кого они находятся. Сразу следует отметить, что никаких специальных норм, которые регламентируют проведение обыска и выемки по делам о компьютерных преступлениях, в уголовно-процессуальном законодательстве Республики Беларусь, не содержится, и, следовательно, данные следственные действия подпадают под сферу действия общих правил, что изначально является не совсем правильным. Обыск и выемка проводятся с участием понятых. Согласно ч. 4 ст. 210 УК РБ допускает, что в необходимых случаях при обыске и выемке участвует специалист. Ч. 3.1 ст. 183 УПК РФ императивно устанавливает, что при производстве выемки изъятие электронных носителей информации производится с участием специалиста [14, 15].

На мой взгляд, для эффективного расследования компьютерных преступлений при производстве таких следственных действий как обыск и выемка необходимо обязательное участие *специалиста, обладающего соответствующими познаниями в области компьютерных технологий*. Участие понятых в данном случае я считаю достаточно бесполезным, т.к. они не обладают специальными знаниями в области техники, они лишь выполняют возложенную на них Законом обязанность удостоверения производства следственного действия, его факта, хода и результатов, а значит, что при участии квалифицированного специалиста эти функции возлагались бы на него.

Обязательное участие квалифицированного специалиста в ходе проведения обыска и выемки позволило бы избежать ошибок, которые совершаются при производстве указанных следственных действий, а именно:

Во-первых, расследование компьютерных преступлений требует совершения незамедлительных действий, и на момент обыска компьютерное устройство может оказаться включенным. В таком случае необходимо оценить информацию, отображенную на мониторе, узнать, что она из себя представляет, и определить, какая программа выполняется в данный момент. Без наличия специальных познаний достаточно трудно определить, можно ли вообще отсоединить устройство от питания для изъятия и, тем самым, не нарушить материалы и информацию, относящиеся к следствию.

Во-вторых, ошибкой является допуск к исследуемому компьютеру владельца для оказания помощи в его эксплуатации, т.к. в процессе его работы могут быть зашифрованы либо уничтожены материалы, имеющее значение для дела.

В-третьих, необходимо проверять компьютер на наличие вирусов и программных закладок, необходимо загрузить компьютер не с его операционной системы, а со своей заранее подготовленной дискеты, либо со стендового жесткого диска, проверке подвергаются все носители [2, с. 207].

Для недопущения ошибок, которые явно могут навредить следствию, необходимо принять ряд предохранительных мер, которые будут проводиться с участием квалифицированного и независимого специалиста. Следовательно, на мой взгляд, Республика Беларусь должна последовать примеру Российской Федерации и предусмотреть в уголовно-процессуальном законодательстве нормы, регламентирующие обязательное участие специалиста. Также предлагаю вышеуказанным государствам пересмотреть необходимость участия понятых, при проведении обыска и выемки цифровой информации на стадии предварительного расследования компьютерных преступлений, т.к. порой они плохо представляют, с какой техникой работает следствие и какие вещи подлежат изъятию, являясь не специалистами в области компьютерных технологий. Такой маленький шаг позволит достичь лучших результатов в борьбе в кибепреступлениями.

Принятие неотлагательных мер, способствующих снижению случаев распространения и передачи материалов, связанных с детской порнографией, через глобальную сеть Интернет.

Согласно ст. 2 Факультативного протокола к конвенции о правах ребенка, касающейся торговли детьми, детской проституции и детской порнографии *детская порнография* означает любое изображение какими бы то ни было средствами ребенка, совершающего реальные или смоделированные откровенно сексуальные действия, или любое изображение половых органов ребенка главным образом в сексуальных целях [16]. Всемирная сеть Интернет способствует быстрому и многочисленному распространению такого рода файлов.

Заслуживает внимания опыт Российской Федерации, которая борется с распространением детской порнографии следующим путем: в 2012 г. Роскомнадзор внес в реестр запрещенных материалов список сайтов с детской порнографией, что было обусловлено вступле-

нием в силу Закона «О защите детей от информации, причиняющей вред их здоровью и развитию».

На сегодняшний день проблема заключается в том, что доступ на иные сайты порнографического содержанию остается открытым и доступным широкому кругу лиц. Введя в любую поисковую систему название порно сайта, вам откроется целый список возможных ссылок, в большинстве случаев доступ на них остается открытым, в некоторых случаях может использоваться фильтр, который потребует подтверждения, что вам уже есть 18 лет или подтвердить вход при помощи отправления СМС. Раздела под названием «Детская порнография» вы не найдете, однако это не исключает возможности «всплывания окон», которые предложат вам перейти по соответствующим ссылкам.

Я бы хотела привести пример судебного разбирательства в Соединенных Штатах Америки «Эшкрофт (министр юстиции США) против Американского союза защиты гражданских свобод» в ходе которого Верховный США пришел к выводу, что запрет на просмотр порносайтов нарушает конституционное право на свободу слова. На тот момент Суд во второй раз заблокировал принятый в 1998 году Закон «О защите детей от материалов непристойного содержания в компьютерной сети». Метод борьбы заключался в следующем: владельцам порноресурсов предлагалось устанавливать фильтр, который будет запрашивать номер кредитной карты у желающих посмотреть сайт. Если владельцы отказывались от установки или применили «некачественный фильтр», то нарушителям грозил штраф от 50 тысяч долларов или 6 месяцев тюрьмы [1].

Таким образом, я бы хотела обратить внимание, что не исключается возможность наличия на порноресурсах детской порнографии. На мой взгляд, установка соответствующих фильтров, является крайне невыгодной для провайдеров и порноиндустрии, однако является хорошим решением для законодателя в случае распространения и передачи материалов, связанных с детской порнографией, через компьютерную систему. Это позволит отследить, кто, в какой день и в какое время имел доступ к соответствующим файлам.

За последние полвека современный мир претерпел существенные изменения, существующая реальность безостановочно усложняется новыми видами ранее неизвестных общественных отношений. Компьютерные технологии в наши дни позволяют человеку выполнять сложные задачи, на которые раньше приходилось затрачивать

больше сил и энергии. Однако еще Ньютон утверждал, что любому действию всегда есть равное и противоположное противодействие. Поэтому, к сожалению, компьютерные технологии не всегда являются источником положительных результатов.

Благодаря компьютерам и глобальной сети Интернет ускоряются процессы межнациональной интеграции, люди вступают в непосредственный контакт друг с другом, доверяют современным технологиям неограниченное количество личной информации, такой как:

– личная переписка по электронной почте,
– журнал конфиденциальных контактов,
– фото- и видеосъемку личного содержания.

Компьютер является пособником в совершении покупок в интернет магазинах, оплаты услуг и банковских счетов.

Вложив так много информации и функций в это устройство, человек поставил под угрозу свое материальное и духовное благосостояние. В случае хищения путем использования компьютерной техники может наноситься материальный ущерб в миллионы долларов. Поэтому расследования компьютерных преступлений не терпят промедления и требуют мгновенной реакции со стороны органа уголовного преследования.

Доказательства, добытые на стадии предварительного расследования, подлежат тщательной оценки с точки зрения:

– относимости,
– допустимости,
– достоверности,
– достаточности.

Проблемы могут возникнуть относительно «допустимости» доказательств, т.к. зачастую имеет место небрежность, когда нарушается порядок и форма их получения.

Следует отметить, что в процессе интеграции современного мира стираются границы, люди обмениваются опытом во всех сферах общественной жизни. В борьбе с киберпреступностью важно «учиться на чужих ошибках», чтобы вовремя прослеживать и пресекать негативные тенденции развития преступного мира. На современном этапе инновационные технологии существенно способствуют в совершении различного рода преступлений, поэтому важно находить «средства противодействия» такого рода действиям, научиться использовать их в своих целях. Однако это невозможно сделать, если государства бу-

дут идти своим путем развития, отрицая и игнорируя опыт иностранных государств.

Страны СНГ, на мой взгляд, отстают в своих методах борьбы с компьютерными преступлениями, что является логичным явлением, т.к. инновационные технологии появились здесь значительно позже. И только совместная работа и сотрудничество помогут достичь существенных результатов в «компьютерной войне» и защитить общество от посягательств на их конституционные права и свободы.

Список использованной литературы

1. Верховный суд США разрешил порносайты в интернете [Электронный ресурс]. 2015. Режим доступа: http://izvestia.ru/news/291668. Дата доступа: 10.04.2015.

2. Вехов, В.Б. Расследование компьютерных преступлений в странах СНГ: Монография / В.Б. Вехов, В.А. Голубев; под ред. Заслуженного деятеля науки Российской Федерации, д-ра юрид. наук, проф. Б.П. Смагоринского. Волгоград: ВА МВД России, 2004. 304 с.

3. Европейская Конвенция по киберпреступлениям (преступлениям киберпространстве): Будапешт, 23 ноября 2001 г. [Электронный ресурс]. – 2015. – Режим доступа: http://mvd.gov.by/main.aspx?guid=4603. – Дата доступа: 07.04.2015.

4. Исторические вехи [Электронный ресурс]. – 2015. – Режим доступа: http://mvd.gov.by/ru/main.aspx?guid=3291. Дата доступа: 03.04.2015.

5. Конституция Республики Беларусь 1994 года (с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 1996 г. и 17 октября 2004 г.). Минск: Амалфея, 2005. 48 с.

6. Лопатина, Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: автореф. дис. … д-ра. юрид. наук: 12.00.08 / Т.М. Лопатина; Всероссийский научно-исследовательский институт МВД России. М., 2006. 418 с.

7. Мазуров, В.А. Компьютерные преступления: классификация и способы противодействия: Учебно-практическое пособие / В.А. Мазуров. М.: Палеотип, Логос, 2002. 148 с.

8. Мороз Н.О., Перспективы совершенствования законодательства Республики Беларусь о международной правовой помощи в контексте Европейской конвенции о киберпреступности / Н.О. Мороз // Консультант Плюс: Беларусь. Технология 3000 [Электронный ре-

сурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2015.

9. О международной правовой помощи по уголовным делам: Закон Респ. Беларусь, 18 мая 2004 г. № 284-З с изм. и доп. // Консультант Плюс: Беларусь. Технология Проф [Электронный ресурс] / ООО «ЮрСпектр». Минск, 2015.

10. Опасности в сетях Интернета [Электронный ресурс]. 2015. Режим доступа: http://www.mvd.gov.by/main.aspx?guid=38153. Дата доступа: 07.04.2015.

11. Просис К. Расследование компьютерных преступлений / К. Просис, К. Мандиа. Лори, 2005. 496 с.

12. Россия отказалась ратифицировать конвенцию СЕ о киберпреступности [Электронный ресурс]. 2015. Режим доступа: http://www.vz.ru/news/2010/11/9/445958.html. Дата доступа: 07.04.2015.

13. Статистические данные Министерства внутренних дел Республики Беларусь по преступлениям в сфере высоких технологий за 2014 год [Электронный ресурс]. 2015. Режим доступа: http://mvd.gov.by/ru/main.aspx?guid=3311. Дата доступа: 07.04.2015.

14. Уголовно-процессуальный кодекс Республики Беларусь: принят Палатой представителей 24 июня 1999 г.: одобр. Совет Респ. 30 июня 1999 г. с изм. и доп. // Консультант Плюс: Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2015.

15. Уголовно-процессуальный кодекс Российской Федерации: принят Государственной Думой 22 нояб. 2001 г.: одобр. Совет Федерации 5 дек. 2001 г. с изм. и доп. [Электронный ресурс]. 2015. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_177263/. Дата доступа: 05.04.2015.

16. Факультативный протокол к конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии: принят Резолюцией Генеральной Ассамблеи Организации Объединенных Наций 25 мая 2000 г. № 54/263 // Консультант Плюс: Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2015.

Информация об авторе

Лашина Дарья Александровна – студентка, Белорусский государственный университет, юридический факультет.

УДК 343.13

Ю.Е. Пахорукова
Научный руководитель: А.Л. Карлов

ПРАВОВАЯ ОЦЕНКА ИСПОЛЬЗОВАНИЯ РАЗЛИЧНЫХ СРЕДСТВ ПРОЦЕССУАЛЬНОГО ЗАКРЕПЛЕНИЯ В КАЧЕСТВЕ ДОКАЗАТЕЛЬСТВ ЭЛЕКТРОННОЙ ПЕРЕПИСКИ В СЕТИ ИНТЕРНЕТ

Многообразие жизненных ситуаций, и прежде всего противоправная деятельность граждан в настоящее время приобретает все новые формы. Интернет пространство так плотно «окутало» нашу жизнь, что многие из преступлений, предусмотренных Уголовным кодексом, видоизменяются, появляются новые составы преступлений, сеть Интернет существенно облегчает совершение преступлений, и одновременно служит средством конспирации для преступников.

Зачастую для совершения противоправных деяний злоумышленники используют различные средства коммуникации, такие как смартфоны и ноутбуки. В последнее время именно для преступлений в сфере незаконного оборота наркотиков все более актуальным становится использование сети Интернет. С ее помощью производятся так называемые бесконтактные сбыты, контрабанда посредством почтовой связи, пересылка наркотических веществ.

Сама по себе переписка преступников в сети Интернет имеет большое доказательственное значение, так как ее содержание позволяет установить время, место совершения преступления, подтвердить умысел, установить соучастников. Так, например в изученных нами материалах следственной практики УФСКН России по Красноярскому краю имелись случаи, когда интернет-перепиской подтверждался факт осознания преступником того, что наркотик перемещался через государственную границу; через поисковые запросы – осознание лицом того, что вещество является наркотическим и т.д.

Таким образом, вопрос электронной переписки из сети Интернет является на сегодняшний день очень актуальным. Необходимо пояснить, что сама по себе переписка может храниться как на серверах оператора связи, так и на жестком диске компьютера злоумышленника. При изъятии переписки и других сведений, находящихся на жестком диске, процессуальных проблем не возникает, поскольку УПК РФ предусматривает такое следственное действие как осмотр пред-

метов (предметом будет выступать компьютер или иной электронный носитель информации), также в данном случае не возникает проблем с режимом доступа к данной переписке, так как одним из критериев отнесения информации к тайне связи является ее нахождение в ведении оператора связи [1, с. 194], тогда как переписка, сохранившаяся на жестком диске уже выбыла из ведения оператора связи, соответственно получение судебного решения для осмотра не требуется.

На наш взгляд, переписка, находящаяся на сервере, имеет большее доказательственное значение, поскольку в отличие от сведений на жестком диске – ее содержание не может быть изменено кем-либо, кроме того, сведения, находящиеся на жестком диске, злоумышленник может удалить, а восстановить их в ходе компьютерно-технической экспертизы не всегда представляется возможным, соответственно переписка, полученная с сервера должна оцениваться как более достоверная.

Вместе с тем при необходимости в ходе расследования уголовного дела ознакомиться с перепиской, расположенной на сервере оператора связи возникает целый ряд вопросов, которые связаны как с выбором подходящего следственного действия, так и с возможностью ограничить предусмотренное ч. 2 ст. 23 Конституции РФ право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Как известно, ограничение этого права допускается только на основании судебного решения.

Разрешению вопросов, связанных с получением переписки с сервера при расследовании уголовного дела и посвящена данная работа. Перед нами стояли следующие задачи: исследовать складывающуюся в территориальных подразделениях ФСКН России практику получения переписки, хранящейся на серверах оператора связи; соотнести применяемые средства фиксации (получения) переписки с действующим законодательством; определить наиболее оптимальные и отвечающие требованиям законности варианты.

В ходе анализа следственно-судебной практики нами были проанкетированы 32 действующих сотрудника ФСКН России (преимущественно следователи), изучены отдельные материалы уголовных дел по рассматриваемым вопросам, а также соответствующие научные труды и учебный материал.

Анкетирование показало, что сотрудники практических органов часто сталкиваются с проблемой определения правового режима получения и процессуальной фиксации интернет-переписки, а также,

что далеко не все следователи правильно оценивают законность тех или иных методов получения сведений из сети Интернет, что также указывает на актуальность и важность данной проблемы.

По результатам опроса и анкетирования следователей, а также изучения уголовных дел, нами были выявлены наиболее часто применяемые способы получения переписки из сети Интернет, к которым относятся:

1) фиксация переписки в протоколе осмотра предметов и документов, проводимого с согласия и с участием лица, переписка которого осматривается (без получения судебного решения);

2) фиксация переписки в протоколе осмотра предметов и документов без согласия лица, переписка которого осматривается, с использованием имеющегося в распоряжении следователя логина и пароля, либо путем подбора пароля (без получения судебного решения);

3) фиксация переписки в протоколе осмотра предметов и документов (осмотр сведений, расположенных в сети Интернет) при условии получения судебного решения;

4) получение переписки посредством производства выемки носителей с необходимыми сведениями у представителя соответствующего Интернет-ресурса (с обязательным получением судебного решения на производство такой выемки);

5) получение переписки посредством направления поручения органу дознания на проведение соответствующего ОРМ, с последующим предоставлением материалов в качестве результатов ОРД.

В первую очередь необходимо отметить, что с точки зрения процессуального средства получения (фиксации) переписки, она может быть применена только при проведении таких следственных действий как осмотр и выемка. Также встречаются случаи, когда следователь решает вопрос с получением переписки посредством направления поручения в порядке, предусмотренном ч. 1 ст. 152 УПК РФ органу дознания, который получает переписку при проведении соответствующего оперативно-розыскного мероприятия с последующим предоставлением его результатов.

Рассмотрим два варианта ознакомления с перепиской:

1) при наличии добровольного согласия подозреваемого, обвиняемого;

2) при отсутствии такого согласия.

Анализ первого варианта следует начать с позиций Конституционного права. Часть 2 ст. 17 Конституции РФ предусматривает, что

основные права и свободы не отчуждаемы и принадлежат человеку, в их число входит и право на тайну переписки. Это право является субъективным что означает прежде всего возможность самостоятельно выбирать вид и меру своего поведения [2, с. 22], а также свободу поведения и поступков в границах, установленных нормой права [3, с. 170]. Исходя из такой трактовки любой человек может самостоятельно распоряжаться своим правом. В то случае если он соглашается на предоставление своей переписки, тем самым он непосредственно реализует свое субъективное право. Таким образом, становится очевидно, что ознакомление с перепиской при согласии лица предоставить свои сообщения, отправленные посредством сети Интернет, не влечет ограничение тайны связи, соответственно не возникает необходимости в получении судебного решения, как это предусмотрено в ч. 2 ст. 23 Конституции РФ.

Также проблемным является вопрос о возможности лица выдать входящие сообщения, ведь разрешение их отправителей в данном случае мы не получаем, а следовательно, может возникнуть проблема с ограничением права на тайну переписки отправителя.

По этому поводу существует две позиции.

Первая заключается в том, что отправляя электронное письмо лицо тем самым предоставляет право распоряжаться перепиской другому, а значит получатель этого письма может предоставить его следователю. Данный вывод косвенно подтверждается посредством анализа практики применения ст. 138 УК РФ (нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений). Так решением Железнодорожного суда г. Новосибирска судья пришел к выводу, что ознакомление с содержанием переписки или телефонных переговоров с согласия одного из абонентов не образует рассматриваемого состава преступления (Постановление Железнодорожного районного суда города Новосибирска по делу № 3/10-88/14).

Второй подход предполагает действие тайны связи в отношении отправленных сообщений и после их получения вне зависимости от волеизъявления получателя. Здесь можно говорить о праве отправителя на тайну связи, и соответственно о необходимости получения его согласия, либо получения судебного решения, однако мы данный подход не поддерживаем. Одним из доводов здесь может послужить норма УПК РФ (ст. ч.2 ст. 186), которая позволяет ограничить тайну связи только лишь на основании заявления лица, которому поступили

угрозы, хотя прослушке в этом случае, несомненно, подлежат и входящие звонки.

Следует отметить, что во многих случаях злоумышленники не дают согласие на осмотр их переписки, так как получаемые в этом случае сведения зачастую носят обвинительный характер. В таком случае без соответствующего судебного решения обойтись уже нельзя.

При отсутствии согласия также может возникнуть еще одна проблема, а именно – необходимость получить пароль от страницы злоумышленника в социальной сети, либо иного средства отправки и получения сообщений. Существует несколько способов получение такой информации, например, он может быть установлен в ходе оперативно-розыскным мероприятий, имеется возможность подобрать его с использованием специальных программ, также возможно получить пароль при осмотре компьютерной техники подозреваемого, обвиняемого (здесь используется возможность большинства браузеров сохранять пароли используемых сайтов. Это дает возможность установить логины и пароли, используемые злоумышленником). Например, для просмотра сохраненных паролей в интернет-браузере «Hcrome» необходимо открыть меню браузера, войти в раздел «Настройки», далее перейти по ссылке «Показать дополнительные настройки», после чего выбрать ссылку «Настроить» в подразделе «Предлагать сохранять пароли для сайтов» раздела «Пароли и формы». После нажатия на сохраненный профиль появится ссылка «Показать», после нажатия на которую пароль станет виден.

Как мы уже отмечали, получение переписки с сервера без согласия пользователя и без получения судебного решения в любом случае является недопустимым, несмотря на это 11 % следователей считают данный способ законным.

По результатам анкетирования следователей УФСКН России по Красноярскому краю, 22 % участников отметили получение переписки путем осмотра при согласии подозреваемого как наиболее приемлемый, такая позиция обусловлена простотой получения информации, в связи с тем, что процедура не затягивается из-за получения судебного решения, при наличии логина и пароля злоумышленника следователь может незамедлительно провести следственное действие.

Сравнивая 2 способа, описанных выше, можно отметить различие в вопросах определения тайны связи, и если в целом первый вариант можно считать законным, при условии достаточности согласия одного лица, для получения информации находящейся в переписке

двух лиц, то второй подход в корне противоречит законодательству, хотя и является более приемлемым и простым в использовании для сотрудников правоохранительных органов.

Исходя из вышеперечисленного мы пришли к выводу о том, что согласие отправителя не обязательно для проведения осмотра страницы в сети Интернет, в связи с тем, что он уже реализовал свое право путем отправления письма получателем.

Два следующих способа процессуального закрепления переписки – это фиксация переписки в протоколе осмотра предметов и документов (осмотр сведений, расположенных в сети Интернет) по судебному решению и получение переписки посредством производства выемки носителей с необходимыми сведениями у представителя соответствующего Интернет-ресурса также при условии получения судебного решения.

Дистанционный осмотр сервера с перепиской пользователя по судебному решению законным считают 15 % следователей, при этом приемлемым – лишь 7 % (по вопросу приемлемости этот результат является самым низким из полученных, хотя фактически использовали его 19 % сотрудников). На наш взгляд низкий показатель приемлемости связан в первую очередь с необходимостью получения судебного решения. С другой стороны, в статье 29 УПК РФ не указано полномочие суда давать согласие на производство такого следственного действия как осмотр. Пункт 7 ч. 2 ст. 29 УПК РФ говорит лишь о даче судом разрешения на производство выемки предметов и документов, содержащих иную, охраняемую федеральным законом тайну, однако на наш взгляд при разрешении данного вопроса можно использовать допустимую в уголовном процессе аналогию закона.

Наряду с этим возникает проблема в удалении информации злоумышленником, восстановление которой возможно только при обращении к оператору связи, что делает процесс намного более длительным. В случае удаления переписки пользователем, посредством дистанционного осмотра ознакомиться с перепиской мы уже не сможем, и тогда останется единственный вариант – производить выемку непосредственно у представителя оператора связи.

Получение переписки посредством производства выемки носителей с необходимыми сведениями у представителя соответствующего Интернет-ресурса (с обязательным получением судебного решения на производство такой выемки) является одним из самых используемых способов. 33 % следователей указали в своих анкетах на его

применение, но при этом всего 7 % считают его приемлемым. На наш взгляд, вызвано это тем, что данный способ является хоть и законным, но наиболее затратным с точки зрения сил и средств. Трудности здесь заключаются в том, что серверы могут находиться:

1) На значительном удалении от места расследования уголовного дела, что делает этот процесс более длительным.

2) На территории иностранного государства, что влечет за собой необходимость направления запроса о правовой помощи, при этом исполнение таких запросов занимает значительное время (до нескольких месяцев), кроме того направление данного запроса затруднено необходимостью его согласования в различных инстанциях.

Также допустимым на наш взгляд является получение переписки, посредством направления поручения органу дознания на проведение соответствующего оперативно розыскного мероприятия[1], с последующим предоставлением материалов в качестве результатов оперативно-розыскной деятельности. Данным способом пользовалось наименьшее количество сотрудников – 14 %, хотя законным его считает 19 %, а наиболее приемлемым для следователя 26 %. Высокий процент приемлемости данного способа, на наш взгляд связан с тем, что посредством дачи поручения органу дознания, следователь частично освобождает себя от работы.

Таким образом, рассмотрев вопросы получения электронной переписки из сети Интернет можно сказать, что к этой проблеме нет единого подхода, однако в арсенале следователя имеется несколько возможных вариантов. Оценив их с точки рения законности следователь вправе самостоятельно принять решение о том, какое средство фиксации переписки применить в конкретном случае, исходя из обстоятельств совершенного преступления и особенностей доказывания по уголовному делу. Важным выводом работы является то, что УПК РФ не исключает возможность применения дистанционного осмотра, что по нашему мнению может значительно облегчить работу следователя, и способствовать быстрому и качественному установлению обстоятельств, подлежащих доказыванию.

[1] Об оперативно-розыскной деятельности: Федеральный закон от 12 авг.1995 г. № 144-ФЗ // Собрание законодательства РФ. 1995. №33. Ст. 3349.

Список использованной литературы

1. Карлов А.Л. Правовой режим использования в доказывании по уголовным делам электронной переписки, содержащейся в памяти технических средств коммуникации // Актуальные проблемы профилактики наркомании и противодействия правонарушениям в сфере легального и незаконного оборота наркотиков: национальный и международный уровни: материалы XVII международной научно-практической конференции (17-18 апреля 2014 года). Красноярск: СибЮИ ФСКН России, 2014.

2. Невирко Д.Д. Права и свободы человека и гражданина: проблемы соотношения, взаимодействия и иерархии: Монография. Красноярск, 2006.

3. Строгович М.С. Проблемы советского соцалистического государства в современный период. Некоторые теоретические вопросы. М., 1967.

4. Терехов М. Ю. Получение дознавателями и следователями органов внутренних дел сведений, составляющих государственную или иную охраняемую федеральным законом тайну: особенности уголовно-процессуальной формы: Автореферат. М., 2010.

5. Федотова Н. В. Уголовная ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений: Автореферат. М., 2009.

Информация об авторе

Пахорукова Юлия Евгеньевна – студентка, Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Сибирский юридический институт Федеральной службы Российской Федерации по контролю за оборотом наркотиков».

УДК 343.13

Е.Ю. Земзикова
Научный руководитель: В.Ф. Васюков

ОСОБЕННОСТИ ИЗЪЯТИЯ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ ПРИ ПРОИЗВОДСТВЕ ВЫЕМКИ

В настоящее время мы живем в мире, где научно-техническое развитие является непрерывным. Внедрение новых технологий в жизнь человека обусловлено тем, что информация стала таким же необходимым ресурсом для человека, как и драгоценные металлы, нефть, природный газ.

Каждый человек ежедневно пользуется техническими средствами, которые предназначены для обмена информацией, фиксации каких- либо событий, окружающего его мира. Внедрение достижений научно- технического прогресса во все сферы жизнедеятельности человека позитивно отразилось на возможностях информационного обмена, однако это порождает опасность использования информации в противоправных целях.

На сегодняшний день, преступлениям в сфере компьютерной информации уделено особое внимание, так как данная группа преступлений характеризуется особой сложностью в расследовании. Производство следственных действий в этой области невозможно без специальных познаний. Однако в настоящее время, алгоритм производства следственных действий при расследовании преступлений в сфере компьютерной информации еще недостаточно освещен в научной литературе.

Федеральным законом РФ от 28.07.2012 № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» в уголовный процесс вводится понятие «электронного носителя информации», устанавливаются особенности работы с ним при проведении ряда следственных действий, регулируется специфика правового режима. Внесение указанных изменений в УПК РФ нацелено на решение главным образом двух задач:

– обеспечение дополнительной защиты прав участников процесса;

– усиления требований к защите компьютерной информации.

Однако внедрение новых процессуальных требований возлагает на следственные органы ряд дополнительных обязанностей, повыша-

ет уровень занятости следователя. В настоящее время фактически по любой категории дел следователь сталкивается с необходимостью поиска, фиксации и изъятия электронных носителей информации.

В связи с этим в настоящем эссе мы постараемся охарактеризовать алгоритм обнаружения, фиксации и изъятия информации с электронных носителей.

Степень разработанности темы исследования. Современное состояние вопроса характеризуется, с одной стороны, недостаточной научной разработанностью, а с другой – большой реальной значимостью для практики борьбы с преступностью. Это нашло свое отражение в диссертационных исследованиях В.В. Крылова (1999), А.Н. Яковлева (2000), В.А. Мещерякова (2001), А.И. Усова (2002), А.А. Васильева (2003), Л.Н. Соловьева (2003), Г.В. Семенова (2003), И.Г. Иванова (2007), В.В. Полякова (2008), В.Б. Вехова (2008) и других ученных.

Объектом исследования являются общественные отношения, формирующиеся в рамках расследования преступлений в сфере информационных технологий.

Предметом исследования являются закономерности использования специальных познаний в сфере компьютерной информации и высоких технологий при производстве выемки по уголовному делу.

Целью исследования явилось рассмотрение теоретических и практических вопросов использования специальных познаний в области компьютерной информации и высоких технологий при расследовании преступлений, в частности, при производстве обыска, связанных с использованием средств компьютерной техники, разработка научно обоснованных рекомендаций и рациональных способов организации взаимодействия следователя со специалистами и экспертами при применении указанных специальных познаний.

Для достижения указанной цели сформулированы следующие основные задачи:

1. Провести анализ понятий и видов специальных познаний в сфере компьютерной информации и высоких технологий, используемых при выемке электронных носителей информации.

2. Определить и разработать наиболее эффективные и рациональные способы организации взаимодействия следователя с лицами, обладающими указанными специальными познаниями, при производстве выемки электронных носителей информации.

3. Рассмотреть комплекс организационных и практических мер, а также методические рекомендации, направленные на повышение эффективности оперативно-служебной деятельности и укрепление взаимодействия при проведении следственных действий.

Следует начать с того, что обыск является одним из ключевых следственных действий, основной целью которого является установление обстоятельств расследуемого события. Как известно, преступления данной категории сложны в расследовании, поэтому к обыску целесообразно привлекать одновременно несколько следственно-оперативных групп после установления лиц, совершивших преступление, а также соучастников.

Как известно, подготовительный этап проведения следственного действия включает в себя два этапа: проведение определенных действий до выезда на место происшествия и по приезду на место происшествия. До выезда на место проведения обыска следователю необходимо:

1. Выяснить сведения о вычислительной технике, которая имеется в обыскиваемом помещении и о ее количестве.

2. Выяснить, используются ли с вычислительной техникой устройства бесперебойного питания.

3. Пригласить специалиста (в соответствии с требованиями ч. 9.1 ст. 182 УПК).

4. Подготовить технические средства, с помощью которых будет считываться и храниться изъятая информация.

5. Целесообразно изучить личность владельца обыскиваемой компьютерной техники.

6. Определиться со временем производства обыска, так как наиболее благоприятным временем для производства данного следственного действия считаются утренние часы [9, с. 45].

Если компьютерная техника установлена в нескольких помещениях, то целесообразно проводить обыск одновременно во всех помещениях. При этом все участники следственного действия должны быть проинструктированы, специалистам должны быть разъяснены их процессуальные права. При подборке членов следственно-оперативной группы следователь должен учитывать их знания и опыт по проведению обыска по преступлениям в сфере компьютерной информации. В ходе проведения инструктажа следователь должен акцентировать внимания на особенностях расследуемого преступления, информации

о тех документах или предметах, которые необходимо отыскать и изъять, порядке обращения с компьютерной техникой и т.д.

Как указывалось выше, следователь должен определиться со временем производства обыска, так как в нерабочее время компьютерные системы отключены от сети и производство обыска будет более эффективным. Так же отсутствие рабочего персонала будет способствовать получению всей необходимой документации.

Также необходимо помнить, что следователю на этапе подготовки проведения обыска нужно определить вид компьютерной среды, который можно разделить на автономный и сетевой. В автономной среде компьютер работает независимо от других компьютеров, обладает самостоятельной операционной системой, поэтому он рассчитан на индивидуального пользователя. Обыск проводится в пределах одного компьютера, а если в помещении есть несколько таких компьютеров, то обыску подвергается каждый из них.

Что касается сетевой среды, то в ней компьютеры имеют общий канал обмена данными. Сложность в том, что необходимо отследить все соединенные компьютеры, определить место нахождения запоминающегося устройства.

По прибытии необходимо оперативно войти в помещение, чтобы предотвратить уничтожение информации, пригласить понятых до предъявления постановления о производстве обыска, так как начинать обыск можно только после приглашения понятых.

Следователь может поручить членам следственно-оперативной группы охрану компьютеров тем самым отрезать доступ персонала, лиц, присутствующих в помещении.

На обзорной стадии необходимо выполнить действия аналогичные рекомендациям по прибытии на место происшествия.

Что касается производства обыска, то необходимо помнить, что:

1.Нужно определить тип и предназначение обыскиваемого компьютера.

2. Осмотреть соединения с другими компьютерами.

3. Установить текущее состояние обыскиваемого компьютера и задачи, которые он выполняет на момент производства обыска.

4. Принять решения о последующих действиях с данным устройством.

5. Принять меры, которые необходимы для транспортировки технического средства.

Следователю так же необходимо фиксировать в протоколе все произведенные действия и их результаты, а так же реакцию операционной системы на них. После выполнения всех действий с техническим средством можно приступать к подготовке к его транспортировке.

Что касается изъятия компьютерной информации, то существует два основных способа: изъятие информации вместе с носителем и без него.

Изъятие информации вместе с носителем предполагает изъятие собственно носителя информации или системы устройств. Этот способ наиболее приемлем, так как он позволяет обнаружить новые доказательства, доступен в осуществлении.

Что касается второго способа, то он является более сложным, так как изъятие информации с отрывом от общей информационной среды способствует утере данных или неполному их изъятию. Однако этот способ так же применяется на практике в случаях, когда работа сети не может быть прервана.

При изъятии необходимо:

1. Изъять все компьютеры и магнитные носители.

2. Обратить внимание на коды доступа и пароли при осмотре документов.

3. Изъять все материалы, находящиеся на столах, опечатать столы и приложить информацию о владельце и месте изъятия технического средства.

При изъятии технических средств можно не производить изъятие мониторов.

Следователю необходимо помнить, что все предметы обнаруженные в ходе обыска и выемки должны быть изъяты в соответствии с требованиями законодательства. Все необходимые сведение должны быть точно отражены в протоколе следственного действия.

В настоящее время в следственной практике стали распространенными случаи производства обыска и выемки до возбуждения уголовного дела.

Поскольку предварительная проверка проводится в сроки, регламентированные действующим уголовно-процессуальным законом, целесообразно составить план ее проведения. Федеральный закон от 4 марта 2013 г. № 23-ФЗ «О внесении изменений в статьи 62 и 303 Уголовного кодекса Российской Федерации и Уголовно-процессуального кодекса Российской Федерации» значительно расширил процессуальные возможности сотрудников органов предвари-

тельного расследования[1]. С учетом законодательных изменений представляется возможным предложить следующие позиции, которые должны быть отражены в плане доследственной проверки по делам о преступлениях в сфере компьютерной информации:

1) получение письменного объяснения от заявителя;

2) осмотр места происшествия – места обнаружения следов преступления с обязательным осмотром ЭВМ или иного компьютерного устройства, электронных носителей и содержащейся на них компьютерной информации. В ходе производства данного следственного действия должны быть получены данные, подтверждающие факты, изложенные заявителем;

3) получение письменных объяснений у лиц, на которых ссылается заявитель или имеются данные о них как о возможных свидетелях происшедшего события;

4) ознакомление с технологией использования документированной компьютерной информации в конкретном технологическом процессе или операции;

5) изучение правовой основы операции, итогом которой явилось событие, изложенное в сообщении о преступлении;

6) консультации со специалистами;

7) истребование необходимых материалов, свидетельствующих о противоправности события либо отражающих незаконность проведения операции в сфере обработки компьютерной информации;

8) осмотр полученных предметов и документов;

9) анализ имеющейся информации и решение вопроса о необходимости получения письменного заключения специалиста, назначения экспертиз, например судебной компьютерной экспертизы, проведения ревизий, документальных или иных проверок;

10) проверка подлинности и действительности документов, имеющихся в материалах доследственной проверки;

11) изучение полноты комплекта и содержания документов, подтверждающих противоправность исследуемого деяния [5].

Однако, по мнению К.Б. Калиновского, практика производства обысков и выемок до возбуждения уголовного дела противоречит уголовно-процессуальному кодексу. В соответствии с ч.1 ст.144 УПК

[1] О внесении изменений в статьи 62 и 303 Уголовного кодекса Российской Федерации и Уголовно-процессуального кодекса Российской Федерации: Федеральный закон от 4 марта 2013 г. № 23-ФЗ» [Электронный ресурс] // СПС КонсультантПлюс (дата обращения 05.03.2015 г.)

РФ при проверке сообщения о преступлении возможно получение объяснения, образцов для сравнительного исследования, истребование предметов и документов, их изъятие и производство судебной экспертизы [6, с. 9].

Мы придерживаемся аналогичного мнения, так как проведение обыска и выемки до возбуждения уголовного дела в отношении лица способствует ограничению конституционных прав граждан.

Все изъятые электронные носители информации должны быть упакованы и опечатаны, при их упаковке необходимо использовать такие материал и инструменты, которые не могут оказывать на носитель негативное воздействие, приводящее к потере информации. Более того, упаковочный материал должен предохранять электронные носители информации от негативных воздействий различного рода. Например, оптические дисковые носители информации (CD, DVD) должны быть уложены в футляры, исключающие механическое воздействие на информационноносящую отражающую поверхность диска.

При транспортировке электронных носителей информации необходимо исключить их механические повреждения и взаимодействие с химически активными веществами. Следует экранировать от воздействия магнитного поля изъятые электронные носители информации. Такое воздействие может привести к порче или уничтожению информации путем размагничивания, кроме того, надо оградить изъятые объекты от воздействия широко используемых криминалистических средств (например, магнитных подъемников, металлоискателей, магнитных кисточек для выявления следов рук и др.). При размещении изъятых объектов на хранение следует соблюдать установленные правила хранения и складирования электронных технических средств.

Некоторые ученые выражают мнение, что при изъятии компьютеров системный блок должен опечатываться листом бумаги с подписями следователя, собственника и понятых, который прикрепляется на лицевую и заднюю панель компьютера и захлестывается на боковые стенки, чтобы исключить возможность разукомплектования, физического повреждения, изменения, удаления содержащейся в нем информации [4, с. 3-4]. Мы полагаем, что это не совсем верно, так как остается доступ к различным портам и разъемам на лицевой или задней панели системного блока, что позволяет подключить различные периферийные или другие электронные устройства и с их помощью произвести удаление или изменение содержащейся в данном электронном носителе информации. При этом все опечатывающие бирки

останутся целы. Нарушение порядка изъятия и упаковки электронных носителей информации на практике приводит к признанию данных предметов недопустимыми доказательствами и потере криминалистически важной доказательственной информации, а в последующем и освобождению виновников от уголовной ответственности.

Дискуссионным вопросом является участие специалиста при производстве изъятия электронных носителей информации. В соответствии со ст.ст.182, 183 УПК РФ изъятие электронных носителей в ходе обыска и выемки производится с обязательным участием специалиста. По требованию законного владельца или обладателя изымаемых электронных носителей осуществляется копирование информации на представленные им носители, если это не препятствует расследованию преступления, но может быть отказано по заявлению специалиста, если это может повлечь утрату или изменение информации.

С одной стороны, законодатель справедливо принял во внимание то обстоятельство, что изъятие электронного носителя информации в ходе обыска и выемки может представлять собой задачу, требующую достаточных знаний в области информатики [3, с. 5]. Участие специалиста в данном случае служит обеспечению права законного владельца или обладателя на получение копии сведений, содержащихся на изымаемом носителе. Внимание законодателя к этой проблеме оправдано. Вместе с тем привлечение сотрудников экспертно-криминалистических подразделений затруднительно из-за высокой нагрузки и небольшой численности отделов, проводящих компьютерные экспертизы. С учетом изложенного возникает вопрос о законности изъятия электронных носителей информации без участия специалиста, будут ли в последующем данные электронные средства признаны недопустимыми доказательствами.

Полностью поддерживаем мнение некоторых ученых [8], которое подтверждается решениями судов [1, 2], о том, что при изъятии электронных носителей информации, проводимых без участия специалиста, хотя и нарушаются требования ч. 9^1 ст.182 УПК РФ, но в соответствии с положениями ст. 38 УПК РФ следователь является процессуально самостоятельным лицом, имеющим право по делу, находящемуся у него в производстве, самостоятельно направлять ход расследования, принимать решения о производстве следственных и иных процессуальных действий, само изъятие в ходе следственных действий указанных предметов осуществляется в рамках требований уголовно-процессуального закона следователем, хотя и без участия

специалиста. Суды, на наш взгляд, обоснованно считают, что формальное нарушение процедуры не связано с нарушением прав и законных интересов участников уголовного процесса и не дает оснований для признания производства следственного действия незаконным. Соответственно, отсутствие специалиста не влечет признания изъятых электронных носителей недопустимыми доказательствами.

Рассмотренные нами особенности изъятия электронных носителей информации лишь подтверждают тот факт, что преступления в сфере компьютерной информации сложны в расследовании [7]. Борьба с преступлениями в сфере компьютерной информации должна оставаться одной из приоритетных задач для правоохранительных органов, обеспечивающих общественную безопасность Российской Федерации. В противном случае нарастание негативных процессов, протекающих в общественной среде нашего государства, создаст угрозу национальной безопасности России.

В современных условиях подготовки сотрудников следственных подразделений наиболее эффективным считается внедрение практико-ориентированных технологий обучения, способствующих формированию у обучающихся значимых для будущей профессиональной деятельности качеств личности, а также знаний, умений и навыков, обеспечивающих качественное выполнение функциональных обязанностей по избранной специальности.

В связи с этим, нами был подготовлен учебный фильм, который содержит производство выемки электронных носителей информации, раскрывает основные ее особенности (ссылка передана в электронном сообщении вместе с работой).

Проведенное нами исследование обосновывает необходимость дальнейшей теоретической и практической разработки вопросов их применения. Особое внимание автором уделяется теоретическим и практическим аспектам особенностям изъятия электронных носителей информации при производстве выемки, а также тактике оперативно-розыскных и следственных действий при расследовании преступлений, совершаемых с применением высоких технологий. Ведь только квалифицированно проведенная стадия оперативно-следственных мероприятий позволяет собрать процессуально-корректные материалы для дальнейшего экспертного исследования, отвечающие принципам относимости, допустимости и достоверности.

Расследование компьютерных преступлений, использование в качестве доказательства информации, полученной с помощью

средств компьютерной техники и иных высоких технологий, требует специальной технической подготовки и во многом зависит от лиц, обладающих специальными познаниями в этой области.

Обладая специальными познаниями в сфере компьютерной техники и иных высоких технологий, специалисты (эксперты) способны внести неоценимый вклад в деятельность следователя по установлению истины при расследовании преступлений. Причем специальные познания могут применяться не только при расследовании «компьютерных преступлений», так как при совершении «традиционных» преступлений компьютер может быть использован для проектирования и изготовления фальсифицированных документов, денежных знаков, для создания и хранения базы данных, содержащей информацию о преступлении и в других целях. Таким образом, несмотря на то, что обязанность поиска и закрепления доказательств лежит на следователе, эффективность производства таких следственных действий как выемка.

Список использованной литературы

1. Апелляционное определение Московского городского суда от 30.09.2013 №10-9507 // СПС «КонсультантПлюс».

2. Апелляционное постановление Московского городского суда от 07.10.2013 №10-9861 // СПС «КонсультантПлюс».
Апелляционное постановление Московского городского суда от 30.06.2014 №10-8300 // СПС «КонсультантПлюс».

3. Белкин А.Р. Новеллы уголовно-процессуального законодательства – шаги вперед или возврат на проверенные позиции? // Уголовное судопроизводство. 2013. № 3.

4. Васюков В.Ф., Булыжкин А.В. Некоторые особенности осмотра средств сотовой связи при расследовании уголовных дел // Российский следователь. 2014. № 2.

5. Вехов В.Б. Особенности проведения доследственной проверки по делам о преступлениях в сфере компьютерной информации [Электронный ресурс] СПС КонсультантПлюс (дата обращения 06.03.2015 г.).

6. Калиновский С.Б. «Доследственный» обыск – незаконное ноу-хау // Уголовный процесс. 2015. №1.

7. Клевцов В.В. Проблемные аспекты изъятия электронных носителей информации при расследовании распространения «дизайнер-

ских» наркотиков с использованием сети интернет // Российский следователь. 2015. №6.

8. Козловский П.В., Седельников П.В. Участие специалиста в изъятии электронных носителей // Научный вестник Омской академии МВД Рос-сии. 2014. № 1 (52). С. 17-19.

9. Худяков А.А. Особенности производства следственных действий при расследовании преступлений в сфере компьютерной информации. М., 2013. С. 45.

Информация об авторе

Земзикова Екатерина Юрьевна – курсант факультета подготовки следователей Орловского юридического института МВД России имени В.В. Лукьянова

УДК 343.13

Е.А. Брагина
Научный руководитель: С.И. Земцова

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ АСПЕКТЫ ПРОИЗВОДСТВА ОСМОТРА СОТОВОГО ТЕЛЕФОНА

В последние годы при совершении значительного количества преступлений для оперативного контактирования используется сотовая связь. Общение преступников при этом происходит с использованием сотового или мобильного телефона. Несмотря на то, что данный предмет стал неотъемлемой частью повседневной жизни, производство его осмотра в случае изъятия представляет некоторые сложности. Связано это с тем, что фактически отсутствуют рекомендации, направленные на правильный алгоритмированный порядок действий следователя (дознавателя). Практически не освещены эти вопросы и в криминалистической литературе. Имеются лишь единичные работы, посвященные данному вопросу [1,2,4].

Однако, прежде чем попытаться исследовать указанный вопрос на основе анализа литературы и судебно-следственной практики, рассмотрим кратко, что же понимается в целом под сотовым телефоном,

чем он отличается от мобильного телефона и какое устройство он имеет.

Мобильный телефон – переносное средство связи, предназначенное преимущественно для голосового общения. В настоящее время сотовая связь – самая распространенная из всех видов мобильной радиосвязи, поэтому чаще всего мобильным телефоном называют сотовый телефон. В то же время, наряду с сотовыми телефонами, мобильными являются также спутниковые телефоны, радиотелефоны и аппараты магистральной связи [5].

Виды мобильных телефонов:

– Сотовый телефон;
– Спутниковый телефон;
– Аппарат транковой связи;
– Автомобильный радиотелефон;
– Радиотелефон дальнего действия;
– Радиотелефон ближнего действия.

Сотовый телефон – мобильный телефон, предназначенный для работы в сетях сотовой связи; использует приемопередатчик радиодиапазона и традиционную телефонную коммутацию для осуществления телефонной связи на территории зоны покрытия сотовой сети [3].

Выделяют несколько типов сотовых телефонов, такие как:

1) По функциональности:

– Камерофон – мобильные телефоны с функцией фотоаппарата и/или видеокамеры. В настоящее время данное название практически вышло из обихода в первоначальном понимании, поскольку большинство современных аппаратов оснащено встроенными фото/видеокамерами. Тем не менее, так часто называют мультимедийные телефоны с расширенными фотовозможностями (в частности, телефоны с высоким качеством камеры).

– Мультимедийный телефон (плеерфон, мьюзикфон, музыкальный телефон) – специализированные мобильные телефоны с расширенными возможностями воспроизведения аудио- и видеофайлов и т. п. Этот термин, как и «камерофон», выходит из употребления, поскольку большая часть современных средних по цене аппаратов может проигрывать цифровые фонограммы и оснащается разъемом для карты памяти. Тем не менее, в ряде мультимедийных телефонов упор делается именно на аудиовозможностях (например, Sony Ericsson серии W (Walkman) со встроенным плеером, Motorola серии W, являющиеся в основном бюджетными телефонами, за некоторыми исключениями).

– Смартфон – мобильный телефон с полноценной операционной системой (Symbian OS, Windows Mobile, Palm OS, GNU/Linux, Android, Apple iOS, MeeGo и др.). Такие телефоны позволяют устанавливать любые новые программы, поддерживаемые данной операционной системой и расширяющие их функциональность: IM-клиенты, офисные пакеты, органайзеры, аудио и видеопроигрыватели, программы управления звонками, браузеры и т. д. Для смартфонов существуют и вирусы (в то время как возможность внедрения в обычные телефоны деструктивного кода весьма затруднительна, в силу закрытости ОС). С появлением таких телефонов, в русском языке, за телефонами, не обладающими такими функциями, закрепился жаргонный термин «звонилка».

– Коммуникатор – карманный персональный компьютер (КПК) с функциями мобильного телефона. Иная ветвь мобильных устройств, по отношению к смартфонам, но имеющая тенденцию к сближению между ними (в настоящее время функциональность и тех, и других в целом сходится). Как и смартфоны, работают под управлением операционных систем, открытых для разработки сторонних приложений. Возможности смартфонов и коммуникаторов, как и любых «старших» компьютеров, зависят от установленных программ и «железа».

– Бизнес-телефон – телефон со специализированными функциями для корпоративных пользователей. Такие телефоны позволяют просматривать текстовые документы и электронные таблицы, работать с электронной почтой, синхронизировать данные органайзера с корпоративным сервером и т. п. Значительная часть бизнес-телефонов является смартфонами или коммуникаторами, часто встречаются устройства с QWERTY-клавиатурой. Иногда такие телефоны, обладая значительной функциональностью, лишены фотокамеры (для организаций с повышенными требованиями безопасности).

– Имиджевый телефон – телефоны, главная особенность которых – стильный внешний вид и броская функциональность (в частности – автоматизированное раскрытие). В имиджевых телефонах часто применяются необычные форм-факторы и стильные (и дорогостоящие) материалы – при изготовлении таких телефонов для отделки корпуса нередко используются благородные металлы и драгоценные камни. Функциональность таких устройств обычно невысока, хотя, в виде исключения, среди них встречаются смартфоны и коммуникаторы. Примером имиджевых телефонов являются модели от Vertu, хотя таковые обычно имеются и в линейках моделей у многих производителей.

– Одноразовый телефон – телефон, обладающий базовой функциональностью (зачастую без дисплея и даже SIM-карты, некоторые в формате кредитной карты), предназначенный для звонков до исчерпания баланса или до окончания заряда батарей, далее выбрасываемый или утилизируемый.

– Телефон для пожилых людей (бабушкофон, дедушкофон) – телефон, обладающий базовой функциональностью, кнопкой SOS, большими кнопками, крупным шрифтом на дисплее (зачастую монохромном).

– По форм-фактору корпуса

– Моноблок;

– Раскладной;

– Слайдер;

– Ротатор – корпус с поворотным механизмом.

– Помимо основной своей функции, а именно телефонной связи, современные сотовые телефоны имеют множество дополнительных:

– Базовые:

– телефонный справочник;

– голосовое управление;

– вибровызов («виброзвонок») – полезен в зашумленных местах, или же там, где нельзя нарушать тишину;

– сменные мелодии звонков (чаще всего форматов MIDI, MMF, WAV, MP3 и AAC);

– подключение гарнитуры (Hands Free) (наушники + микрофон);

– громкоговорящая связь («громкая связь»);

– часы;

– будильник;

– секундомер;

– таймер;

– календарь;

– калькулятор;

– хранение данных (встроенная флэш-память, поддержка сменных карт флэш-памяти (MMC, RS MMC, SD, Memory Stick, MicroSD, Memory Stick Micro, Mini SD и др.), также жесткий диск);

– игры и приложения (на Java (J2ME), Brew, Android, Windows Mobile);

– Деловые:

– инженерный калькулятор;

– конвертер валют;

– диктофон;

– органайзер;

– конференц-связь – в этом режиме могут разговаривать несколько человек (для работы функции необходима поддержка функции оператора);

– Органайзер паролей – возможность записать несколько паролей и скрыть их под единым паролем;

– Мультимедийные:

– Радиоприемник;

– цифровой проигрыватель;

– видеопроигрыватель;

– ТВ-тюнер;

– караоке (LG F1200);

– цифровой фотоаппарат, цифровая видеокамера (см. камерафон);

– простые графические и видеоредакторы;

– TrackID – сервис, встроенный в телефоны Sony Ericsson (серия Walkman (начиная с W810), K-серия), позволяющий узнать название и исполнителя музыкального произведения;

– Функция получения некоторой информации от радиостанции (RDS);

– Обмен сообщениями:

– SMS – служба коротких сообщений SMS (Short Message Service);

– EMS – служба расширенных сообщений EMS (Enhanced Message Service – расширение SMS, позволяющее форматировать текст, добавлять смайлик, черно-белые (а иногда и цветные) изображения, звуки и простые мелодии);

– MMS – служба мультимедийных сообщений MMS (Multimedia Messaging Service) позволяет добавлять в сообщения звук, изображение (например, фотографию) или небольшой видеоролик;

– Встроенный или дополнительно устанавливаемый IM-клиент;

– CB (Cell Broadcast) – прием информационных сообщений от оператора;

– Обмен данными:

– через факс;

– через модем (в том числе доступ в Интернет, по протоколам CSD, GPRS, EDGE, HSDPA, EV-DO, Wi-Fi, WiMAX и др.);

– через встроенный WAP-браузер;

– через встроенный или дополнительно устанавливаемый Веб-браузер;

– через средства для работы с электронной почтой;

– через дата-кабель;

– через ИК порт;

– через Bluetooth;

– через WiFi;

– через NFC;

– Прочие функции:

– GPS;

– Push-to-talk (PTT) – в этом режиме телефон имитирует портативную рацию;

– Фонарик;

– фотокамера (присутствует во всех новых телефонах);

– принтер (Polaroid HS-RSS);

– сканер изображений;

– компас;

– сканер отпечатков пальцев (Pantech GI100, iPhone 5s);

– преобразование речи в текст и наоборот (некоторые аппараты Samsung и Nokia);

– видеокамера (присутствует во всех новых телефонах);

– Location-based services;

– Солнечная панель (Samsung S7550 Blue Earth) (позволяет заряжать телефон от солнца, 1 час = 10 мин разговора);

– Шагометр (Samsung S7550 Blue Earth) (количество сохраненных деревьев, потраченной энергии, уменьшение выброса CO2);

– ТВ-тюнер (аналоговый или цифровой) (многие китайские модели);

– Проектор встроенный в телефон (многие китайские модели, а также фирменные);

– Телефон-Часы (многие китайские модели);

– iFan зарядка iPhone силой ветра (крепится на руль велосипеда);

– Тепло-генератор встроенный в телефон Nokia E-Cu (концепт).

В настоящее время, как нами уже отмечалось, все чаще используются сотовые телефоны в приготовлении, совершении преступлений, сокрытии его следов. Поэтому актуальным стал вопрос, связанный с изъятием, фиксацией и исследованием информации, которая содержится в данных устройствах. И конечно эта информация является ценной для выявления, раскрытия и расследования преступле-

ний, идентификации неопознанных трупов и др. Так как данная информация может помочь следователю определить местонахождение субъекта преступления, его соучастников, ознакомиться с журналом звонков, содержанием СМС-переписок, чатов и т.д.

Примером может служить заключение эксперта № – 660 от 31.05.2013 года, согласно выводам которого, представленный на экспертизу сотовый телефон «Soni Ericsson XPERIA» содержит информацию, имеющую значение для дела, а также заключение эксперта № 661 от 03.06.2013 года, согласно выводам которого, представленные на экспертизу сотовый телефон «Sony XPERIA» с сим-картой «Мегафон» и сотовый телефон «Nokia» с сим-картой «Билайн» содержат информацию, имеющую значение для дела, в отношении Кандыба В.А., который выполнял роль курьера, распространяющего наркотические средства через систему тайников, место нахождения которых сообщалось посредством использования службы мгновенного обмена сообщениями в сети интернет «ICQ»[1].

Федеральным законом от 28 июля 2012 г. № 143-ФЗ электронные носители информации включены в уголовно-процессуальный закон России как новый вид вещественных доказательств[2]. Однако, чтобы полученная информация и сами устройства стали таковыми и были допустимыми доказательствами, требуется корректная работа с ними, исключающая возможность потери либо, наоборот, привнесения внешней информации в их память. Электронные носители информации высокотехнологичны, и для работы с ними необходимо участие специалиста, так как внешнего осмотра и получения той или иной информации недостаточно, такая информация может быть тщательно завуалирована либо удалена.

Анализ действующего законодательства и правоприменительной практики позволяет сделать вывод о том, что на сегодняшний день извлечение информации из сотовых телефонов наиболее часто производится в рамках такого следственного действия, как осмотр предметов (ст. 176 УПК РФ).

---

[1] Обвинительное заключение по уголовному делу № 201326299/78 в отношении Кандыба Виталия Анатольевича по обвинению в совершении преступлений, предусмотренных ч.1 ст. 30 УК РФ, ч.5 ст. 228.1 УК РФ, направлено прокурору г. Тюмени 26 сентября 2012 г. // Архив кафедры криминалистики СибЮИ ФСКН России.

[2] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 28 июля 2012 г. № 143-ФЗ // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 25.04.2015).

Например, согласно содержащейся информации сотового телефона «Sony Ericsson Xperia» с sim- картой, изъятого 07 марта 2013 года, в ходе осмотра комнаты, в которой был задержан Старчиков В.В. (который получал от Шилко Д.М. расфасованные мелким оптом партии наркотического средства героин, хранил и выполнял функции «закладчика»), была обнаружена информация о текстовой переписке между Старчиковым В.В., Шилко Д.М. (который искал других членов преступной группы и распределял между ними обязанности, получал и хранил у себя дома крупные партии наркотического средства героин, расфасовывал его на более мелкие партии и передавал другому члену преступной группы – Старчикову В.В.) и неустановленным в ходе следствия лицом, осуществляющейся при помощи ICQ и электронной почты с использованием имен «vasiagold34», «Радость счастье», «Сумасшедшее золото» и «Воздух любви», а именно тайников с адресами, в которых находилось наркотическое средство героин, что послужило одним из доказательств по делу[1].

Осмотр сотового телефона можно разделить на 3 этапа [2]:

1. Внешний осмотр. На данной стадии происходит непосредственное изучение и фиксация наружного строения и состояния аппарата, в рамках которого в протоколе указываются марка, модель, тип, форма аппарата, цвет корпуса, размер; наличие объективов тыльной и (или) лицевой фото/видеокамеры (вспышки), фирменных наименований, логотипа, обозначений; количество и расположение функциональных, встроенных, сенсорных клавиш (джойстика); разъемов Mini(Micro)USB, зарядного устройства, стереонаушников; наличие отверстий для динамика, микрофона, датчика расстояния, внешней освещенности. Отдельно указываются особые приметы наружного строения: повреждения – сколы, царапины, потертости, отсутствие должных элементов; наличие дополнительных атрибутов и технических составляющих – чехла, шнурка, брелока, гарнитуры, полимерных наклеек, графических вставок, надписей, инкрустации драгоценными металлами и др. В ходе внешнего осмотра проводится детальная фотосъемка внешней, оборотной и боковых панелей мобильного

[1] Обвинительное заключение по уголовному делу № 851110 в отношении Шилко Дмитрия Михайловича по обвинению в совершении преступлений, предусмотренных ч. 3 ст. 30 УК РФ, п «г» ч. 4 ст. 228.1 УК РФ; ч. 3 ст. 30 УК РФ, п «г» ч. 4 ст. 228.1 УК РФ, Старчикова Владислава Владимировича по обвинению в совершении преступлений, предусмотренных ч. 3 ст. 30 УК РФ, п «г» ч. 4 ст. 228.1 УК РФ, направлено прокурору г. Волжского Волгоградской области 12 августа 2013 г.// Архив кафедры криминалистики СибЮИ ФСКН России за 2013 г.

телефона. В случае если осматриваемый телефон раскладного («бабочка») или раздвижного типа («слайдер»), то телефон фотографируется в первоначальном и раскладном/раздвижном состоянии.

2. Конструктивный осмотр. На данной стадии производится осмотр конструкции телефона по частям – задней крышки телефона и (или) аккумуляторной батареи (в определенных моделях аппаратов сотовой связи батарея встроена в корпус либо в заднюю крышку), флеш-карты, SIM-карт(ы). При осмотре аккумуляторной батареи в протоколе следует указать ее идентификационный номер, тип, марку, модель, мощность, иную информацию, указанную на корпусе. Также в протоколе указывается цвет и родовой материал, из которого изготовлена батарея. При осмотре флеш-карты (MiniSD) необходимо обратить внимание на ее идентификационный номер, объем, цвет и родовой материал корпуса. SIM-карта, обнаруженная в телефоне, осматривается аналогичным образом. Как правило, на корпусе SIM-карты имеется логотип оператора сотовой связи, описание которого также обязательно в протоколе.

В ходе конструктивного осмотра проводится детальная фотосъемка внешней и оборотной стороны батареи, флеш-карты, SIM-карты, а также тыльной стороны корпуса мобильного телефона (без задней крышки) так, чтобы на снимке был виден IMEI-номер аппарата.

3. Осмотр информационной среды. Осмотр информационной среды телефона включает изучение и фиксацию сведений, которые содержатся в:

1) списке контактов и журнале звонков;

2) СМС сообщениях;

3) приложениях – для изучения переписки между участниками преступной группы посредством интернет мессенджеров, установленных на телефоне (Isq, watsapp, skype др.);

4) файлах в памяти телефона и других объектах (например, фотографии мест закладок наркотиков, имущества подозреваемых, участников группы, записи мест закладок и др).

В случае если в ходе осмотра следователю удалось включить мобильный телефон и получен доступ к сведениям, которые в нем находятся, в протоколе в хронологическом порядке фиксируются все производимые в дальнейшем с аппаратом манипуляции.

В следственной практике нередко возникают ситуации, в которых в ходе производства первоначальных следственных действий изымается сразу несколько аппаратов сотовой связи во включенном

состоянии. Выключать в таких случаях мобильные телефоны до осмотра нецелесообразно (отключение может произойти при извлечении батареи, SIM-карты, просмотре IMEI-кода на наклейке, расположенной во внутренней части панели телефона и т.д.), т.к. при последующем включении потребуются коды блокировки (PIN-код), которые могут быть известны только его последнему пользователю (подозреваемому, свидетелю или потерпевшему). Отказ последнего в предоставлении информации по разблокировке телефона может исключить возможность незамедлительного полноценного исследования его информационного содержимого (электронной записной книжки, входящих и исходящих соединений, SMS-, MMS-сообщений, E-mail, голосовой почты, фото-, видеофайлов, диктофонных записей, органайзера и др., в зависимости от модели телефона). Поэтому важно подчеркнуть, что если к моменту осмотра телефон был включен, то конструктивный осмотр следует проводить только после изучения его информационной среды [2].

Не стоит забывать о том, что если для уголовного дела имеют значение данные из СМС, переписки в социальных сетях, Skaip и по электронной почте и законный владелец мобильного телефона не дает согласие, то следователь может осматривать подобного рода информацию только по решению суда. Обязательность исполнения этого положения закрепляется позицией Конституционного Суда Российской Федерации, выраженной в Определении от 2 октября 2003 г. N 345-О: «...информацией, составляющей охраняемую Конституцией Российской Федерации и действующими на территории Российской Федерации законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи; для доступа к указанным сведениям органам, осуществляющим оперативно-розыскную деятельность, необходимо получение судебного решения. Иное означало бы несоблюдение требования статьи 23 (часть 2) Конституции Российской Федерации о возможности ограничения права на тайну телефонных переговоров только на основании судебного решения»[1].

[1] Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 года «О связи»: Определение Конституционного Суда Российской Федерации от 2 октября 2003 г. № 345-О // ВКС РФ. 2004. № 1. С. 50–52.

Но, в случае извлечения информации о входящих-исходящих звонках, данных записной книжки, заметок в календаре решение суда получать не нужно[1].

В случаях, не терпящих отлагательства осмотр средств связи может производиться следователем в соответствии с требованиями ч. 5 ст. 165 УПК РФ.

Электронные носители информации высокотехнологичны и иногда необходимая информация может быть тщательно завуалирована либо удалена, в таких ситуациях рекомендуется использовать криминалистическую технику, позволяющую извлекать полную информацию (включая удаленную) из памяти мобильных устройств, а также электронных накопителей (карт памяти, сим-карт и др.) , такую как универсальное устройство извлечения судебной информации (UFED – Universal Forensic Extraction Device), мобильный криминалист, XRY, MOBILedit, Тарантула и др.). При этом данная криминалистическая техника позволяет работать практически с любой моделью мобильных устройств, в том числе с поврежденными устройствами на основе любой операционной системы. Осмотр с использованием криминалистической техники осуществляется с участием специалиста.

Список использованной литературы

1. Багмет А.М., Скобелин С.Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность.. 2013. № 2.

2. Васюков В.Ф., Булыжкин А.В. Некоторые особенности осмотра средств сотовой связи при расследовании уголовных дел // Российский следователь. 2014. № 2.

3. ВикипедиЯ. https://ru.wikipedia.org/wiki/Сотовый_телефон (обращение 15.04.2015 г.)

4. Суров О.А., Земцова С.И., Галушин П.В., Судницын А.Б. Методика расследования преступлений, связанных с незаконным оборотом наркотиков, совершаемых с использованием информационно- телекоммуникационных сетей (включая сеть Интернет): отчет о научно исследовательской работе. Красноярск. СибЮИ ФСКН России, 2014 г.

[1] Надзорное определение Судебной коллегии по уголовным делам Верховного Суда РФ от 2 июня 2006 г. № 9-ДП06-10 // Бюллетень Верховного Суда РФ. 2006. № 12.

5. Циклопедия. http://cyclowiki.org/wiki/Мобильный_телефон (обращение 15.04.2015 г.).

Информация об авторе

Брагина Екатерина Анатольевна – студент, Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Сибирский юридический институт Федеральной службы Российской Федерации по контролю за оборотом наркотиков».

УДК 343.148.6

М.И. Денежкин
Научный руководитель: С.И. Земцова

К ВОПРОСУ ПРИМЕНЕНИЯ КРИМИНАЛИСТИЧЕСКОЙ ТЕХНИКИ ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В МОБИЛЬНЫХ ЭЛЕКТРОННЫХ УСТРОЙСТВАХ

Каждый день, привносит в наш мир, все большие изменения. Так как общество не стоит на месте и постоянно развивается, это затрагивает все сферы общественной жизни. Но наиболее быстро развивается наука и техника, уже невозможно представить те дисковые домашние телефоны, которые еще пятнадцать-двадцать лет назад казались роскошью. Персональный компьютер в семье обычное дело, хотя еще в 70-х годах двадцатого века, такие электронные машины занимали по площади целые этажи и были не доступны обычным гражданам. В связи с этим, изменился характер деятельности человека, она стала более компактной, то на что раньше требовалось большое количество времени, теперь можно сделать за пару минут. Все эти масштабные изменения не обошли стороной и правоохранительную деятельность. На данный момент с помощью технических средств можно обнаружить большое количество следовой информации на тех предметах, на которых лет 20–30 назад ни кто и не подумал бы искать информацию, которая может стать криминалистически важной для предварительного следствия. В связи с данными явле-

ниями актуальность набирает проблема, возможности применения криминалистических технических средств, для получения информации содержащейся в электронных средствах коммуникации, во время его осмотра, в соответствии со ст. 164, 165 УПК РФ.

Достаточно очевидно, что информация, содержащаяся в памяти мобильных электронных устройств, может иметь для следственных органов важное доказательственное или ориентирующее значение. В настоящее время органы правоохраны Российской Федерации обеспечены криминалистической техникой программами (устройство извлечения судебной информации (UFED), Мобильный криминалист, XRY, MOBILedit), позволяющей извлекать информацию (включая удаленную) из памяти мобильных электронных устройств, а также электронных накопителей (карт памяти, сим-карт и др.) участников уголовного судопроизводства, как в ходе проверки сообщений о преступлениях, так и на протяжении всего их расследования. «На основе исследования практической деятельностипо применению универсального технического средства извлечения судебной информации (UFED), проведенной сотрудниками Института повышении квалификации Следственного комитета Российской Федерации в территориальных следственных подразделениях Следственного Комитета России, показало очень высокую эффективность использования данных устройства в получении информации (87 %). Однако отсутствие единого подхода при процессуальном оформлении порождает вопросы, связанные с пределами ограничения конституционных прав граждан Российской Федерации на тайну переписки, личной жизни, телефонных и иных переговоров при раскрытии и расследовании преступлений. Поскольку ограничение данных прав должно наступать только на основании судебного решения» [1].

В основном исследуются: мобильные телефоны, сим-карты, планшетные компьютеры. В единичных случаях информация извлекается из навигаторов, видео-регистраторов и цифровых фотокамер. Практика изъятия мобильных электронных устройств для извлечения из них криминалистически значимой информации для расследования и рассмотрения материалов проверки сообщения о преступлении, несмотря на появление ч. 3.1. ст. 183 УПК РФ, происходит достаточно однообразно. Мобильные электронные устройства изымаются в ходе осмотра места происшествия, обыска, выемки, личного обыска при задержании, о чем делается отметка в протоколе производимого следственного действия. Встречаются ситуации, когда следователи

изымают мобильное электронное устройство не в ходе определенного следственного действия, а сразу производят его осмотр.Примером могут послужить ситуации, потерпевший в ходе допроса предъявляет свой мобильный телефон с определенной интересующей следователя информацией или когда телефон обнаружен на месте происшествия. В 92 % случаев извлечение криминалистически важной информации из мобильных электронных устройств, производится в порядке осмотра предметов (мобильных устройств) с применением технических средств (UFED).

В некоторых субъектах Российской Федерации сложилась практика, что для извлечения удаленной информации и работы с некоторыми моделями сотовых телефонов китайского производства также выносилось постановление о назначении компьютерно-технической экспертизы мобильных устройств. При этом чаще всего ставились вопросы о возможности эксперта изъять полные сведения из мобильного электронного устройства. Извлечение криминалистически важной информации, процессуально оформляется протоколом осмотра предмета (мобильного устройства) с приложением отчета в бумажном и электронном (на CD-диске) носителе, с предлагающимися к ним заключением эксперта либо справкой специалиста. В ряде регионов криминалистическую технику(UFED, Мобильный криминалист, XRY, MOBILedit) используют только в целях ускорения получения возможных внешних данных и построения отчета, тогда как данные технические средства имеют куда более широкие возможности. При производстве следствия по ряду уголовных дел применение данных технических устройств и программ позволило изобличить виновных в совершении особо тяжких резонансных преступлений.

Следует заметить, что ходатайства перед судом на производство осмотра мобильных устройств и извлечениякриминалистически важной информации, имеющей значение дня раскрытия органами предварительного следствия возбужденного уголовногодела, следователями не возбуждались, соответствующие постановления не выносились. Однако при данном противоречии в судебно-следственной практике не отмечено, случаев признания судами недопустимыми доказательств, полученных с использованием даннойкриминалистической техники(UFED, Мобильный криминалист, XRY, MOBILedit). В единичных случаях, при полном физическом извлечении дампа памяти (пароли, СМС-сообщения, сообщения электронной почты, чаты) следователи Следственного Управления Следственного Комитета

России Якутии и Ярославской области подавали ходатайство на получение судебного решения [1]. Однако в ответ на поданное ходатайство следователя Ярославской области о разрешении провести осмотр мобильного устройства с использованием UFED судья подчеркнул, что необходимости ходатайства равно как и получение разрешения суда на проведение подобного следственного действия нет. При этом руководители целого ряда СУ СК России обратили внимание на то, что получаемая криминалистически важная информация с помощью криминалистической техники относятся к охраняемой законом «тайне личной жизни, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений»[1]. Вследствие чего получение данной информации возможно только на основании судебного решения. Для устранения данной проблемы возможно внесения соответствующих изменений (дополнений) в ст. 165 УПК РФ.

Ряд руководителей считают более правильным способом извлечения криминалистически важной информации из мобильных электронных устройств с помощью криминалистической техники находящейся в пользовании правоохранительных органов Российской Федерации при получении согласия собственника мобильного электронного устройства. Если такое согласие отсутствует, то аналогично ч.5 ст. 177 УПК РФ (Осмотр жилища) и ч.2 ст. 186 УПК РФ (Контроль и запись переговоров) требуется получение решения суда. Практические сотрудники СК России не видят препятствий в использовании криминалистической техники применяемой для получения информации их мобильных электронных устройств на основе действующего законодательства Российской Федерации. Так в соответствии со ст. 23 Конституции России каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение данного права возможно только на основании полученного судебного решения. Однако в судебной практике границы тайны очень противоречивы.

Важное практическое значение имеет Определение Конституционного Суда РФ от 8 апреля 2010 г. №433-О-ООб отказе в принятии к рассмотрению жалобы гражданина Тарасова Н. А. на нарушение его конституционных прав частью первой статьи 176 и частью первой

[1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Собрание законодательства РФ. 04.08.2014. № 31. Ст. 4398.

статьи 285 УПК РФ»[1]. В данной жалобе на органы предварительного расследования гр. Тарасов Н.А. указывает на то, что из его мобильного телефона, (он был признан подозреваемым по уголовному делу) без получения решения суда, были получены сведения, находящиеся в электронной памяти СМС-сообщения и оглашены в судебном заседании. Конституционный Суд РФ, отказал гр. Тарасову в принятии к рассмотрению его жалобы, не усмотрел нарушений его конституционных прав в нормах уголовно-процессуального закона (ч. 1 ст. 176 и ч. 1 ст. 285 УПК РФ). Суд подчеркнул, что в указанных нормах представлены основания для производства следственных действий в виде осмотра материальных объектов (данных сотового теле-она) и правила оглашения в судебном разбирательстве протоколов следственных действий (протокола осмотра сотового телефона), целью которых является установление обстоятельств, имеющихважное значение для рассмотрения уголовного дела.

В связи с этим, важно разработать практически применимое методическое пособие, по производству изъятия мобильных электронных устройств в ходе таких следственных действий как обыск и осмотр места происшествия, как для следователя, так и для специалиста криминалиста который может быть привлечен к участию в данных следственных действиях. Для ускорения раскрытия преступлений, возможного задержания по горячим следам, а так же более полного сбора всей возможно интересующей следовой базой, которая может иметь доказательственное значение.

Список использованной литературы

1. Багмет А.М., Скобелин С.Ю. Актуальные вопросы применения криминалистической техники для получения информации содержащейся в мобильных устройствах // Вестник криминалистики. 2013. № 4.

Информация об авторе

Денежкин Максим Игоревич – курсант, Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Сибирский юридический институт Федеральной службы Российской Федерации по контролю за оборотом наркотиков».

[1] Определение Конституционного Суда Российской Федерации от 8 апреля 2010 года №443-О-О [Электронный ресурс] // Режим доступа: Консультант Плюс

УДК 343.148.6

Р.Д. Брагин
Научный руководитель: С.И. Земцова

К ВОПРОСУ О ЗНАЧЕНИИ СУДЕБНЫХ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ЭКСПЕРТИЗ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Судебные компьютерно-технические экспертизы (СКТЭ) производятся в целях определения статуса объекта как компьютерного средства, выявления и изучения его роли в расследуемом преступлении, а также получения доступа к информации на носителях данных с последующим всесторонним ее исследованием. Специальные знания СКТЭ составляют электроника, электротехника, информационные системы и процессы, радиотехника и связь, вычислительная техника и автоматизация. Общим предметом СКТЭ являются факты и обстоятельства, устанавливаемые на основе исследования закономерностей разработки и эксплуатации компьютерных средств, обеспечивающих реализацию информационных процессов, которые зафиксированы в материалах уголовного дела. Необходимость в СКТЭ обуславливается широким внедрением компьютерных технологий практически во все сферы человеческой деятельности [см., например, 1, 2,3].

Родовая классификация СКТЭ организована на основе обеспечивающих компонентов любого компьютерного средства (аппаратного, или технического, программного и информационного обеспечения). Соответственно этому в СКТЭ выделяются:

1) аппаратно-компьютерная экспертиза;
2) программно-компьютерная экспертиза;
3) информационно-компьютерная экспертиза;
4) компьютерно-сетевая экспертиза.

Данная классификация может быть эффективно использована при назначении комплексных экспертиз и решения большого перечня задач.

Сущность судебной аппаратно-компьютерной экспертизы заключается в проведении исследования технических средств компьютерной системы. Предметом данного вида СКТЭ являются факты и обстоятельства, устанавливаемые на основе исследования закономерностей эксплуатации аппаратных средств компьютерной системы – материальных носителей информации о факте или событии уголовного дела.

Для осуществления экспертного исследования программного обеспечения предназначена судебная программно-компьютерная экспертиза. Ее предметом являются закономерности разработки (создания) и применения (использования) программного обеспечения компьютерной системы, представленной на исследование в целях установления истины по уголовному делу. Основной целью программно-компьютерной экспертизы является установление причастности исследуемого программного комплекса к расследуемому преступному деянию. Также в результате анализа могут быть обнаружены следы совершенных противоправных действий. Предметом исследования данной экспертизы являются особенности разработки и применения программных средств компьютерной системы [5].

Судебная информационно-компьютерная экспертиза является ключевым видом СКТЭ, так как позволяет завершить целостное построение доказательственной базы путем окончательного разрешения большинства вопросов, связанных с компьютерной информацией. Целью этого вида является поиск, обнаружение, анализ и оценка информации, подготовленной пользователем или порожденной (созданной) программами для организации информационных процессов в компьютерной системе.

Судебная компьютерно-сетевая экспертиза, в отличие от предыдущих, основывается, прежде всего, на функциональном предназначении компьютерных средств, реализующих какую-либо сетевую информационную технологию. Она выделена в отдельный вид в связи с тем, что лишь использование специальных знаний в области сетевых технологий позволяет соединить воедино полученные объекты, сведения о них и эффективно решить поставленные экспертные задачи. Особое место в компьютерно-сетевой экспертизе занимают экспертные исследования, связанные с интернет-технологиями.

Весьма показательным является пример проведения судебной компьютерно-сетевой экспертизы так называемых программных закладок, предоставляющих возможность несанкционированного доступа по сети к данным чужих компьютеров. Суть экспертного исследования программных закладок заключается в установлении признаков несанкционированных действий (т.е. возможности выполнения своих действий с информацией на ЭВМ без уведомления и согласия ее законного пользователя), а также выявление адресов, по которым производится несанкционированная пересылка тех или иных данных с ЭВМ.

В связи со стремительным развитием современных телекоммуникаций и связи в судебной компьютерно-сетевой экспертизе можно выделить судебную телематическую экспертизу, предметом которой являются фактические данные, устанавливаемые на основе применения специальных знаний при исследовании средств телекоммуникаций и подвижной связи как материальных носителей информации о факте или событии, имеющем отношение к уголовному делу.

Практика показывает, что рассмотренные выше основные виды СКТЭ при производстве большинства экспертных исследований применяются комплексно и, чаще всего, последовательно. Поэтому в настоящее время в постановлении на производство судебной экспертизы целесообразно указывать не родовое наименование экспертизы, а назначать судебную компьютерно-техническую экспертизу.

При проведении компьютерно-технических экспертиз возникает целый ряд проблем, например, такие как:

1) Отсутствие в штате экспертных подразделений правоохранительных органов и Министерства юстиции достаточно квалифицированных специалистов в области компьютерной информации.

2) Недостаточная подготовка в области программного обеспечения и компьютерной техники, не позволяющая правильно сформулировать вопросы для эксперта (особенно по общеуголовным составам). Постановка перед экспертами вопросов, выходящих за рамки их компетенции.

3) Трудности в интерпретации результатов экспертизы.

В настоящее время ведомственные эксперты, за очень редким исключением, разбираются в компьютерных системах на уровне «пользователя», то есть в принципе не имеют возможности проводить сложные экспертизы. Известны случаи, когда недостаточно квалифицированные эксперты полностью уничтожали существенную информацию на изъятой компьютерной технике (например, по делу гр. С., которое расследовалось СЧ СУ при УВД Кировской области в 2006–2007 гг.) [4].

Технико-криминалистические экспертизы компьютерных систем проводятся не во всех регионах РФ и занимают значительное время, в связи с тем, что недостаточно соответствующих специалистов, тогда как ведомственная инструкция отводит на проведение экспертизы 15 суток[1]. Сроки же предварительного следствия жестко ограничены Уго-

[1] Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации:

ловно-процессуальным кодексом. В соответствии со ст. 162 УПК, «предварительное следствие по уголовному делу должно быть закончено в срок, не превышающий 2 месяцев со дня возбуждения уголовного дела». Срок предварительного следствия может быть продлен, но по обычным уголовным делам экономической направленности продление крайне редко оформляется на срок свыше 1 месяца. В результате заключение экспертов, поступившее в последние дни перед окончанием срока следствия, просто подшивается в дело как одно из доказательств. Использовать предоставленную экспертом информацию для новых следственных действий у следователя просто не остается времени. Следствием всего изложенного является формальность результатов экспертизы для следователя. В большинстве случаев заключение эксперта не просматривается полностью, а только его резолютивная часть, где следователь убеждается, что на поставленные им вопросы дан положительный ответ. А в суде может выясниться, например, что экспертом обнаружены признаки и других составов преступлений, которые были благополучно проигнорированы следователем.

Данная проблема усугубляется тем, что следователи и судьи при назначении экспертизы компьютерных систем неправильно ставят перед экспертом вопросы, в связи с тем, что имеют недостаточные знания в данной сфере. Наиболее характерна ошибка, когда перед экспертом ставятся вопросы, которые должны решаться не экспертом, а исключительно следствием и судом. К таким относятся вопросы о нарушении законодательства, а также о целях и мотивах каких-либо действий. Характерный пример – вопрос: «Являются ли программы на изъятом компьютере контрафактными?»

Ведомственные эксперты, как правило, некритически относятся к подобным вопросам, и их заключения оказываются либо неконкретными, малоинформативными для следствия, либо же оспариваются в суде адвокатом стороны защиты. В самом деле, когда эксперт указывает в заключении, что на таком-то компьютере им обнаружено контрафактное программное обеспечение, он по сути присваивает себе полномочия суда, поскольку устанавливать наличие состава преступления в России может только суд. Тем не менее эксперт, не дожидаясь судебного приговора, сам объявляет преступление доказанным. Разумеется, к такому заключению суд обязан отнестись критически.

Приказ МВД России от 29 июня 2005г. № 511 (ред. от 15.10.2012) [Электронный ресурс] // Режим доступа: Консультант Плюс.

Часто выводы экспертов ставятся под сомнение в суде. Подсудимый находит высококвалифицированного специалиста в области программного обеспечения и приводит его в суд в качестве свидетеля защиты. В этом случае, суд должен, обязан допросить такого специалиста. Но и судьи понимают, что допрос квалифицированного специалиста в суде несомненно может поставить под сомнение результаты экспертизы и нередко просто отказывают в его допросе, мотивируя тем, что сомневаться в квалификации эксперта не приходится.

При другом развитии событий, суд может только назначить повторную экспертизу, как правило, в том же самом учреждении. При этом зачастую оказывается, что в ходе первой экспертизы исследуемые системы изменены до такой степени, что новый эксперт руководствуется в большей степени корпоративной солидарностью и «перепечатывает» прежнее заключение, меняя только даты производства экспертизы и ФИО эксперта. Многие юристы в такой ситуации настаивают на «независимой» экспертизе, приглашая собственных экспертов. Но независимость этих экспертов весьма сомнительна, поскольку их услуги оплачены стороной защиты. И в заключениях этих экспертов будет преобладать явно выраженный «оправдательный уклон», в противовес «обвинительному уклону» экспертов государственных экспертных учреждений.

Большинство экспертов нарушают требования УПК РФ в самом начале исследования – как только включают исследуемый компьютер. Дело в том, что пункт 3 части четвертой статьи 57 УПК РФ прямо запрещает эксперту производить действия, вызывающие изменения основных свойств исследуемого объекта. Применительно к компьютерной технике, эксперт обязан обеспечить неизменность содержимого жестких дисков и иных носителей информации в исследуемых компьютерах. Только при соблюдении этого условия выводы эксперта могут быть проверены при необходимости повторной экспертизой.

Эксперт может достичь цели сохранения всех исследуемых носителей информации в неизменном состоянии как технологическими, так и физическими методами. Основной технологический прием – загрузка на исследуемом компьютере с внешнего носителя, так называемой, доверенной операционной системы, которая заведомо не производит несанкционированной записи на жесткий диск. Характерным примером такой системы может служить MS DOS 6.22 (без менеджеров памяти типа QEMM), а также некоторые усеченные версии UNIX. Допустимо также изъятие жесткого диска из исследуемого

компьютера и подключение его к собственному компьютеру с загруженной там доверенной операционной системой.

Физически жесткий диск исследуемого компьютера может быть защищен от записи путем подключения его через специальное устройство. Например, устройство FastBloc производства Guidance Software обеспечивает аппаратную блокировку записи на жесткие диски с интерфейсами IDE и SCSI при сохранении скорости обмена с диском.

В любом случае невозможность записи на жесткий диск исследуемого компьютера существенно затрудняет процесс поиска нужной информации. Оказывается невозможным, к примеру, восстановить стертые файлы, работать с текстовыми процессорами и даже просто осуществлять расширенный поиск информации. Поэтому для того, чтобы произвести экспертизу за приемлемое время, эксперт должен создать файл-образ исследуемого жесткого диска на своем компьютере либо попросту скопировать исследуемый жесткий диск на другой. При этом недопустимо стандартное копирование файлов, поскольку не меньший интерес для эксперта представляет пространство диска, считающееся свободным. Следует использовать специальное программное обеспечение, например, Symantec Ghost, которое осуществляет посекторное копирование носителей информации.

Слабым местом такого подхода является финансирование. Для того, чтобы создать на своем компьютере (или компьютерах) образ или копию исследуемого жесткого диска, эксперт должен располагать носителем информации как минимум такой же емкости. А если на экспертизу направлено несколько компьютеров, да еще сервер с RAID-массивом… Вот тут-то государственный эксперт и вспоминает, что проверить его заключение сможет разве что коллега из соседнего кабинета. И 57-я статья УПК РФ приносится в жертву целесообразности. Раз такого объема свободного места просто нет, эксперт начинает работать непосредственно с жестким диском исследуемого компьютера. При этом могут быть восстановлены файлы, распакованы архивы, снят пароль с базы данных, то есть, в ходе исследования происходит то самое «изменение внешнего вида или основных свойств» исследуемого объекта. Аналогичные ошибки зачастую допускают и «независимые» эксперты, приглашенные сторонами процесса либо правоохранительными органами.

В тоже время, имеются очень серьезные нюансы при изготовлении заключения эксперта: сотрудники государственных экспертных учреждений в совершенстве знают процессуальную сторону дела и

имеют весьма ценный опыт защиты своих выводов непосредственно в судебном заседании. Специалисты же из негосударственных структур, хотя и обладают более высокой квалификацией в области компьютерных систем, не уделяют достаточного внимания ни процессуальному оформлению своих заключений, ни выступлению в суде.

В ходе допроса суд имеет возможность как проверить квалификацию эксперта, так и получить дополнительную информацию, не вошедшую в заключение. Однако, неготовые к допросам в суде частные эксперты зачастую становятся легкой добычей адвокатов стороны защиты. Опытному адвокату с большим стажем выступлений в суде обычно не составляет труда запутать и подавить человека, никогда в суде не выступавшего.

На современном этапе развития целесообразно не только организовать качественную экспертизу компьютерных систем как по уголовным, так и по гражданским делам на базе негосударственных учреждений, специализирующихся в области информационной безопасности, но и вернуться к вопросам специализации следователей и судей (предварительное и судебное следствие должно проводиться лицами, имеющими опыт в области программного обеспечения и компьютерных систем). Разумеется, такой подход предполагает усиление внимания к правовой стороне вопроса, в частности обязательное сертифицирование экспертной деятельности и обучением специалистов.

Несмотря на существующие проблемы, судебная компьютерно-техническая экспертиза приносит результаты необходимые для расследования преступлений в сфере незаконного оборота наркотиков. Так, например, заключение эксперта № 2/585 от 27.02.2012 о проведении компьютерно-технической экспертизы по уголовному делу № 1-53/201 возбужденному в отношении гр. С., 1985 г.р. позволило доказать вину С. в совершении незаконного перемещения через Государственную границу РФ, а также незаконной пересылки в целях сбыта, а также незаконного сбыта сильнодействующих веществ, не являющихся наркотическими или психотропными веществами, группой лиц по предварительному сговору, в крупном размере[1].

По уголовному делу № 5603523, представленные в качестве доказательств заключения эксперта: № 26-с от 19.03.2013 года о прове-

[1] Обвинительное заключение по уголовному делу № 1-53/201 по обвинению С. в совершении преступлений, предусмотренных ч.1 ст. 226.1 УК РФ, ч.3 ст. 234 УК РФ, ч. 1 ст. 226.1 УК РФ, ч.3 ст. 234 УК РФ направлено прокурору г. Сухой Лог Свердловской области. // Архив кафедры криминалистики СибЮИ ФСКН России.

дении компьютерно-технической экспертизы, согласно которой установлена информация, имеющаяся в ноутбуке «ASUS», который принадлежал К., а именно: наличие электронной переписки на Форуме LegalRC о курительных смесях, о задержке посылки от 22.01.2013 года, herbalopt.com о продаже легальной химии, свидетельствующие о заинтересованности К. к нелегальным курительным смесям, их приобретении и реализации; № 28-с от 21.03.2013 года о проведении компьютерно-технической экспертизы, согласно которой установлена информация, имеющаяся в системном блоке «IN WIN», который принадлежал К.., обнаруженные текстовые файлы и история посещения интернет страниц, содержащих сведения о переписке по электронной почте на Форуме LegalRC о получении курительных смесей, психоделических поллсов и легального аналога бутирата от 27.01.2013 г., сведений о приобретении качественного спайса, надежных закладок, качественного сервиса, свидетельствующие о прямой заинтересованности К. к нелегальным курительным смесям, их приобретении и реализации изобличили гр. К. в том, что он, действуя умышленно, из корыстных побуждений, с целью незаконного обогащения, осознавая, что посягает на здоровье населения РФ, совершил приготовление к незаконному сбыту смеси, содержащей наркотическое средство метилендиоксипировалерон, в крупном размере[1].

Список использованной литературы

1. Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике: автореф. дис. ... канд. юрид. наук. Воронеж, 2005.

2. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: Изд-во Воронеж. гос. ун-та, 2002.

3. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: автореф. дис. ... канд. юрид. наук. Омск, 2008.

4. Проблемы при проведении компьютерно-технических экспертиз. http://pravo-zakon.jimdo.com/2014/07/22/проблемы-при-проведении-компьютерно-технических-экспертиз/ (дата обращения 20.04.2015 г.).

[1] Обвинительное заключение по уголовному делу № 5603523 по обвинению К. в совершении преступления, предусмотренного ч.1 ст. 30 УК РФ, п. «г», ч.4 ст. 228.1 УК РФ, направлено прокурору г. Челябинск // Архив кафедры криминалистики СибЮИ ФСКН России.

5. Центр по проведению судебных экспертиз и исследований автономная некоммерческая организация «Судебный Эксперт». http://sudexpa.ru/expertises/computers/software/ (дата обращения: 18.04.2015 г.).

Информация об авторе

Брагин Роман Дмитриевич – курсант, Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Сибирский юридический институт Федеральной службы Российской Федерации по контролю за оборотом наркотиков».

УДК 343.148.6
ББК 67.53

Е.В. Демидов
Научный руководитель: С.И. Земцова

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ СПЕЦИАЛИСТА ПРИ ИЗЪЯТИИ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ ПРИ ПРОИЗВОДСТВЕ ОБЫСКА

В течение последнего десятилетия наблюдается стабильный рост преступлений. В связи с этим возникает необходимость в повышении качественного уровня расследования уголовных дел, таким образом, это является одной из важнейших задач. В большинстве случаев как показывает практика следователи и оперативные сотрудники не умеют самостоятельно правильно применять технико-криминалистические средства, в ходе поиска, обнаружения, фиксации и изъятия материальных следов преступления. При этом такое применение специальных знаний приводит к порче или уничтожению материальных следов преступления. Сложившаяся ситуация требует постоянного совершенствования процесса использования специальных знаний в ходе предварительного расследования преступлений. Данное обстоятельство вызывает необходимость в разработке мер по практической реализации концепции постоянного технико-криминалистического обеспечения про-

цесса раскрытия, расследования и предупреждения преступлений, одной из задач которой является повышение роли специалистов в использовании ими специальных знаний в ходе проведения отдельных следственных действий и оперативно-розыскных мероприятий. Действующее уголовно-процессуальное законодательство не определяет какие именно знания являются «специальными». Отсутствует единое мнение об этом и среди ученых, что создает трудности в их использовании. Между тем, четкое определение понятия «специальные знания» необходимо для наиболее эффективного их использования в процессе раскрытия и расследования преступлений в соответствии с требованиями закона. Проанализировав мнения ряда ученых на определение ими понятия «специальные знания» (Р.С. Белкин, П.П. Ищенко, Е.В. Карнаухов, В.Н. Махов, Е.Р. Россинская, А.В. Кудрявцев, и др). Специальные знания – это навыки и умения, приобретенные субъектом их применения путем специальной подготовки или профессионального опыта и используемые на основе современных достижений в соответствующей области науки, техники, искусства или ремесла, применяемые при раскрытии и расследовании преступлений в целях установления обстоятельств, подлежащих доказыванию, в случаях и порядке, определенных действующим законодательством. Пределы компетенции специалиста и сама необходимость его участия в деле зависят от содержания этого понятия.

Действующее уголовно-процессуальное законодательство дает четкое определение такому понятию, как «специалист», а именно в части первой статьи 58 (Специалист) Уголовно-процессуального кодекса РФ говорится, что специалистом является лицо, обладающее специальными знаниями, привлекаемое к участию в процессуальных действиях в порядке, установленном настоящим Кодексом, для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, для постановки вопросов эксперту, а также для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию. Из этого понятия следует функция специалиста, а именно – оказание содействия в обнаружении, закреплении и изъятии предметов и документов. Данная функция была дополнена после внесения изменений в Уголовно-процессуальный кодекс РФ в статью 182 (Основания и порядок производства обыска) посредством введения части 9.1 Федеральным законом от 28.07.2012 г. № 143-ФЗ, в редакции Федерального закона от 29.11.2012 г. № 207-ФЗ. При про-

изводстве обыска электронные носители информации изымаются с участием специалиста. По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в обыске, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации. Таким образом можно сделать вывод о том, что обязательное участие специалиста при изъятии электронных носителей обеспечит правильное и в то же время безопасное изъятие электронного носителя информации, а также копирование информации.

Прежде чем перейти к процедуре изъятия электронных носителей информации, нам необходимо обозначить, что подразумевается под понятием электронный носитель информации. Согласно ГОСТу 2.051 2006 ЕСКД «Электронные документы. Общие положения» п. 3.1.15 под электронным носителем понимается материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемых с помощью средств вычислительной техники [1]. К электронным носителям информации относят носители для однократной или многократной цифровой записи электрическим способом: оптические диски (CD, DVD, Blu-ray) [2], гибкие магнитные диски (дискета), жесткие магнитные диски (жесткий диск), носители на основе флэш-памяти: карта памяти (флэш-карта); USB флэш-накопитель (флэшка) [3]. Существуют так называемые объекты-носители электронного носителя информации, к ним относятся: мобильные телефоны (смартфоны), ноутбуки, системные блоки, серверы и др.

Список использованной литературы

1. http://vsegost.com/Catalog/42/4288.shtml Все ГОСТы.
2. https://ru.wikipedia.org/wiki/Носитель_информации Википедия.
3. http://juranalytic.ru/ Юридические вести.

Информация об авторе

Демидов Евгений Васильевич – курсант, Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Сибирский юридический институт Федеральной службы Российской Федерации по контролю за оборотом наркотиков».

УДК 434.985
ББК 67.523.14

Е.Н. Стельмах
Научный руководитель: Е.А. Ерахтина

СПЕЦИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Внедрения новых информационных технологий необходимо для эффективной борьбы с преступностью, современные реалии требуют постоянного поиска новых технических решений и методического обеспечения оперативно-розыскной работы. Качественно новым, развивающимся информационным пространством для эффективного осуществления оперативно-розыскной деятельности являются глобальные компьютерные информационные сети. Идет стремительная криминализация компьютерного информационного пространства, в нем нашли свое место наркомания, проституция, распространение порнографии, терроризм, грубые нарушения национального и расового равноправия.

Комплекс ОРМ по раскрытию преступлений может применяться в информационной сфере (Интернет). В силу этого в арсенале технических средств особое место заняла специальная техника поисково-разведывательного назначения. Она выступает эффективным инструментом ОРД, обладают мощными тактическими возможностями. Наиболее перспективны направлением из многообразия технических средств выступает СОРМ, а перспективы его развития могут вывести ОРД на качественно новый уровень. Необходимо отметить, что в мире существуют аналоги данной системы, и по своим показателем некоторые из них опережают нашу отечественную систему на целое поколение, поэтому будет целесообразно проанализировать подобные системы и выделить на основе этого вектор развития Российского СОРМ.

В мире существует классификация подобных систем, они называются, системы законного перехвата сообщений LI (Lawful Interception) в терминах Европейского института стандартизации ETSI. Под законным перехватом сообщений понимают процесс передачи правоохранительным органам (LEA – Law Enforcement Agency) информации соединений определенных пользователей телекоммуни-

кационной сети. Законный перехват является санкционированным действием и не дает пользователю возможности его определить. В различных странах под правоохранительными органами подразумевается одна или несколько организаций. Программы компьютерного слежения и радиоэлектронной разведки, реализованных или реализуемых в настоящее время правительствами стран мира, а также международные проекты в данной сфере:

– NarusInsight – система шпионажа кластерного класса, предназначенная для прослушивания и анализа данных сетевого трафика в интернете. В качестве вспомогательных узлов поставки данных использует систему Carnivore. Оператором системы в США является ФБР, пользователями – все федеральные агентства США.

– Terrorist Finance Tracking Program – совместная программа ЦРУ и Министерства финансов США по получению доступа к базе транзакций SWIFT.

– Tempora (Великобритания) – секретная программа компьютерного слежения, созданная и используемая Центром правительственной связи Великобритании (GCHQ) совместно с Агентством национальной безопасности США.

– Эшелон – глобальная система радиоэлектронной разведки, действующая в рамках соглашения о радиотехнической и разведывательной безопасности Австралии, Канады, Новой Зеландии, Великобритании и США, также известного под названиями UKUSA Agreement, AUSCANNZUKUS. Эшелон имеет возможность перехвата и анализа телефонных переговоров, факсов, электронных писем и других информационных потоков по всему миру путем подключения к каналам связи, таким как спутниковая связь, телефонная сеть общего пользования, СВЧ-соединения.

– Carnivore (США) – автоматическая система для прослушивания информации, поступающей и уходящей с Web-сайтов, анализа баз данных, а также для вскрытия и анализа электронной почты, аналог российского СОРМ-2. Carnivore является системным компонентом NarusInsight.

– PRISM (Program for Robotics, Intelligents Sensing and Mechatronics) – государственная программа США – комплекс мероприятий, осуществляемых с целью массового негласного сбора информации, передаваемой по сетям электросвязи, формально классифицированная как совершенно секретная. Действует на основании закона о контроле за деятельностью иностранных разведок (FISA) и за-

кона Protect America Act (PAA), который позволяет вести слежение за пределами США без судебного решения. Кодовое название программы слежения PRISM – 984XN. Включена в состав внутренних и внешних специальных разведывательных операций АНБ. Система PRISM включает в себя: несколько приложений слежения за компьютерами; компьютерные системы; базы данных.

XKeyscore создана в дополнение к PRISM. XKeyscore – инструмент для поиска и анализа информации о конкретных пользователях или людях с заданными характеристиками.

Большинство этих систем построены в соответствии с законами о мониторинге пользователей и международными стандартами в области электронного слежения CALEA и ETSI. Комплекс возможностей которыми обладают эти программы в совокупности: Масштабирование для анализа больших и сверхбольших IP сетей (таких как Интернет); Глубокая обработка данных искусственным интеллектом: нормализация, корреляция, агрегация и анализ, создание информационной модели пользователей, элементов информационных систем, анализа этих моделей; Отслеживание индивидуальных пользователей и мониторинг программам их пользования, сайты посещения, связь пользователей друг с другом, электронной почты, включая запись: электронных текстовых сообщений; голосовых сообщений; видео файлов; фотографий; файлами обмена; Отслеживание сервисов: Microsoft, Yahoo, Google, Facebook, Paltalk, YouTube, AOL, Skype, Apple. Fairview, Blarney, Oakstar и Stormbrew; Поиск и анализ информации о конкретных пользователях или людях с заданными характеристиками.

Важно отметить, что сведения о некоторых программах стали известны только благодаря, утечки секретной информации. Возможности которые предоставляют данные программы по истине колоссальны, в связи с чем в обществе идет жаркая дискуссия о возможных нарушениях основополагающих прав человека которые могут нарушаться, поэтому необходимо учитывать опыт их внедрения и эксплуатирования. Необходимо осознавать, что одной из целей подобных программ является разведка, что может создавать угрозу национальной безопасности страны.

Для предотвращения и раскрытия преступлений самого различного уровня была разработана Система Оперативно Розыскных Мероприятий (СОРМ). Принцип работы которой заключается в перехвате пользовательской и статистической информации на сетях связи для ее дальнейшего использования в правоохранительных целях. СОРМ

(Система технических средств для обеспечения функций оперативно-розыскных мероприятий) – комплекс технических средств и мер, предназначенных для проведения оперативно-розыскных мероприятий в сетях телефонной, подвижной и беспроводной связи и радиосвязи[1]. СОРМ действует на основе Федерального закона «Об оперативно-розыскной деятельности» от 12 августа 1995 г. и Федерального закона «О связи» от 16 февраля 1995 г. и предназначена для технического обеспечения проведения указанных мероприятий на сетях (службах) документальной электросвязи (СДЭС), используемых для предоставления услуг передачи данных и телематических служб, включая сеть Интернет. Данные требования распространяются на все СДЭС, которые создаются или были созданы ранее на основании лицензий Госкомсвязи (Минсвязи) России на деятельность по предоставлению услуг передачи данных и/или телематических служб.[2] Эта система обеспечивает возможность съема информации, передаваемой и принимаемой любым пользователем (юридическим, физическим, техническим ресурсом, пользующимся услугами сети документальной электросвязи).

Комплекс АПС СОРМ, устанавливаемый на узлах СДЭС, обеспечивает возможность съема с линий СДЭС и передачу на удаленный ПУ информации, передаваемой и принимаемой любым конкретным пользователем в процессе предоставления любых услуг СДЭС. Принцип функционирования систем законного перехвата сообщений СОРМ заключается в обнаружении в реальном времени попыток контролируемого объекта получить доступ к услугам своего интернет-провайдера и последующем перехвате этой информации. Перехваченная таким образом информация форматируется и передается правоохранительным органам. При постановке абонентов на контроль им присваивается одна из двух его категорий: полный или статистический контроль. При полном контроле передается информация о фазах установления соединений, данные о контролируемых вызовах, а также осуществляться съем и трансляция информации, передаваемой в разговорном тракте контролируемого пользователя. При статисти-

[1] О связи: Федеральный закон от 7 июля 2003 г. № 126-ФЗ ред. от 21.07.2014// Справочная правовая система «Консультант плюс».

[2] Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность: Постановление Правительства Российской Федерации от 27 августа 2005 г. № 538 // Российская газета. 2005. № 3864.

ческом контроле на ПУ в реальном масштабе времени передается только информация о фазах установления соединений и данные о контролируемых вызовах. Предусмотрена возможность изменения параметров контроля объекта наблюдения. Предусмотрена защита технических средств СОРМ от несанкционированного вмешательства в ее работу [1].

С достаточно большой долей уверенности можно утверждать, что законный перехват IP-контента с годами будет только усложняться. В сложившейся ситуации необходимость создания и внедрения соответствующей нормативно-технологической базы для существующей сетевой инфраструктуры, с учетом наиболее вероятных сценариев ее развития, является основной задачей. Расширение возможностей отечественной системы законного перехвата связано с предполагаемыми поправками в законодательную базу, приказ «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий». Часть III. Который предусматривает технические требования записывать все поступающие данные и хранить их не менее 12 часов, так же детализирует, какая информация будет перехватываться. Это, в частности, телефонный номер, IP-адрес, имя учетной записи пользователя, адреса электронной почты, номер ICQ, (IMEI), идентификаторы абонентов интернет-телефонии, информация о местоположении абонентов интернет-телефонии (Google Talk, Skype и др.).

Таким образом, получается, что СОРМ стоит на пороге внедрения функций, которые уже почти десятилетие используется зарубежными программами, и безнадежно от них отстает.

Сегодня дополнительную сложность законному перехвату добавляет повсеместное увлечение криптографической защитой информации. Обстановка в мире превратила СОРМ из весьма сомнительного требования в бесспорную и абсолютно необходимую функцию узлов коммутации современных сетей связи. При детальном анализе, СОРМ по многим параметрам уступает своим зарубежным аналогам, более того, ее даже нельзя включить в класс программ типа PRISM, у этих программ разное назначение, которое определяется их техническими возможностями. СОРМ по основным параметрам схожа с американской системой Carnivore, которая, в свою очередь, всего лишь, является системным компонентом NarusInsight, исходя из возмозностей NarusInsight, и вышеизложенного следует, что мы без-

надежно отстаем в этом направлении ОРД. Для обеспечения национальной и информационной безопасности государства, нашей стране необходимы программы класса PRISM. Эти факторы требуют расширения функциональности систем СОРМ, анализа и обсуждения спецификаций и инженерных решений. По моему мнению, дальнейшие развитие системы должно быть направленно на создание и внедрение системы, включающей создание единого информационного центра, в который бы стекалась информация из разных источников: СОРМ-1 прослушивание телефонных переговоров, СОРМ-2 снятие информации с электронных каналов, а также системы мониторинга уличного видеонаблюдения, базы данных ЖРЭУ, налоговых органов, банковских и муниципальных учреждений.

Выделение СОРМ в отдельную категорию технических средств «Технические средства поддержки ОРД», создания нормативной базы этого понятия, а так же системы судебного санкционирования ОРМ в сети интернет.

Список использованной литературы

1. Законный перехват сообщений: подходы ETSI, CALEA и СОРМ // Вестник связи. 2007. № 3.

Информация об авторе

Стельмах Ефим Николаевич – магистрант, ФГБОУ ВПО «КрасГАУ», Юридический институт.

ПЕРСОНАЛИИ

Абенова Кымбат Есмуханбетовна – студентка, юридический факультет, Карагандинский государственный университет им. Е.А. Букетова, г. Караганда, Республика Казахстан

Агаева Арзу Гусейновна – студентка, факультет государственного права и национальной безопасности, Байкальский государственный университет экономики и права, г. Иркутск, Российская Федерация

Агапов Даниил Александрович – курсант, факультета по подготовке следователей, Краснодарский университет МВД России, г. Краснодар, Российская Федерация

Бардаханов Михаил Рубенович – студент, факультет государственного права и национальной безопасности, Байкальский государственный университет экономики и права, г. Иркутск, Российская Федерация

Брагина Екатерина Анатольевна – студентка, Сибирский юридический институт Федеральной службы Российской Федерации по контролю за оборотом наркотиков, г. Красноярск, Российская Федерация

Брагин Роман Дмитриевич – курсант, Сибирский юридический институт Федеральной службы Российской Федерации по контролю за оборотом наркотиков, г. Красноярск, Российская Федерация

Демидов Евгений Васильевич – курсант, Сибирский юридический институт Федеральной службы Российской Федерации по контролю за оборотом наркотиков, г. Красноярск, Российская Федерация

Денежкин Максим Игоревич – курсант, Сибирский юридический институт Федеральной службы Российской Федерации по контролю за оборотом наркотиков, г. Красноярск, Российская Федерация

Долсонова Лиана Зориктоевна – студент, факультет государственного права и национальной безопасности, Байкальский государственный университет экономики и права, г. Иркутск, Российская Федерация

Дресвянская Кристина Владимировна – студентка, факультета государственного права и национальной безопасности, Байкальский государственный университет экономики и права, г. Иркутск, Российская Федерация

Завгородняя Евгения Сергеевна – студентка, судебно-следственный факультет, Байкальский государственный университет экономики и права, г. Иркутск, Российская Федерация

Земзикова Екатерина Юрьевна – курсант, факультет подготовки следователей Орловского юридического института МВД России имени В.В. Лукьянова, г. Орел, Российская Федерация

Измайлов Алексей Викторович – студент, Институт правоохранительной деятельности, Саратовская государственная юридическая академия, г. Саратов, Российская Федерация

Караульская Олеся Владимировна – студентка, факультет государственного права и национальной безопасности, Байкальский государственный университет экономики и права, г. Иркутск, Российская Федерация

Козленко Виктория Витальевна – студентка, Сибирский юридический институт Федеральной службы по контролю за оборотом наркотиков, г. Красноярск, Российская Федерация

Лашина Дарья Александровна – студентка, юридический факультет, Белорусский государственный университет, г. Минск, Республика Беларусь

Макушев Дмитрий Иванович – студент, Иркутский юридический институт (филиал), Академия Генеральной прокуратуры Российской Федерации, г. Иркутск, Российская Федерация

Мананников Антон Сергеевич – студент, юридический факультет, Алтайский государственный университет, г. Барнаул, Российская Федерация

Махазагдаева Алена Дагбасамбуевна – студентка, факультет государственного права и национальной безопасности, Байкальский государственный университет экономики и права, г. Иркутск**,** Российская Федерация

Нуроян Кристина Львовна – студентка, судебно-следственный факультет, Байкальский государственный университет экономики и права, г. Иркутск, Российская Федерация

Пахорукова Юлия Евгеньевна – студентка, Сибирский юридический институт Федеральной службы Российской Федерации по контролю за оборотом наркотиков, г. Красноярск, Российская Федерация

Санок Елена Эдуардовна – студентка, юридический факультет Белорусский государственный университет, г. Минск, Республика Беларусь

Скуратовский Алексей Юрьевич – студент, Иркутский юридический институт (филиал), Академия Генеральной прокуратуры Российской Федерации, г. Иркутск, Российская Федерация

Смолякова Алена – студентка, Сибирский юридический институт Федеральной службы Российской Федерации по контролю за оборотом наркотиков, г. Красноярск, Российская Федерация

Стельмах Ефим Николаевич – магистрант, юридический институт, Красноярский государственный аграрный университет, г. Красноярск, Российская Федерация

Хлыстова Дарья Станиславовна – студентка, Иркутский юридический институт (филиал), Академия Генеральной прокуратуры Российской Федерации, г. Иркутск, Российская Федерация

Цынгеева Бимбасо Солбоновна – студентка, факультет подготовки специалистов для судебной системы (юридический факультет), Российский государственный университет правосудия (Восточно-Сибирский филиал), г. Иркутск, Российская Федерация

Шагеев Равиль – студент, Сибирский юридический институт Федеральной службы Российской Федерации по контролю за оборотом наркотиков, г. Красноярск, Российская Федерация

Черных Анастасия Юрьевна – студентка, Иркутский юридический институт (филиал), Российская правовая академия Министерства юстиции Российской Федерации, г. Иркутск, Российская Федерация

Научное издание

АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ РАЗВИТИЯ ЮРИДИЧЕСКОГО ОБРАЗОВАНИЯ: ПРОБЛЕМЫ, ТЕНДЕНЦИИ, ПЕРСПЕКТИВЫ

Сборник статей и эссе студентов

Издается в авторской редакции

Технический редактор
А.С. Ларионова

ИД № 06318 от 26.11.01.
Подписано в печать 03.09.15. Формат 60х90 1/16. Бумага офсетная. Печать трафаретная. Усл. печ. л. 11,8. Тираж 100 экз. Заказ .

Издательство Байкальского государственного университета
экономики и права.
664003, г. Иркутск, ул. Ленина, 11.
Отпечатано в ИПО БГУЭП.