

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

**Федеральное государственное бюджетное образовательное
учреждение высшего образования**

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Юридический факультет

Кафедра

«Правоохранительная деятельность»

ДИПЛОМНАЯ РАБОТА

на тему

**Особенности расследования и раскрытия преступлений в сфере компьютерной
информации**

Студент

(подпись, дата)

(ФИО полностью)

Научный руководитель

(подпись, дата)

(фамилия, инициалы)

Нормоконтролер

(подпись, дата)

(фамилия, инициалы)

Рецензент

(должность, место работы)

(подпись, дата)

(фамилия, инициалы)

Работа допущена к защите (протокол заседания кафедры от _____ № ____).

Заведующий кафедрой

(подпись)

(фамилия, инициалы)

Работа защищена с оценкой _____ (протокол ГЭК от _____ № ____).

Секретарь ГЭК

(подпись)

(фамилия, инициалы)

Пенза

Оглавление

Введение.....	3
1. Характеристика преступлений в сфере компьютерной информации.....	6
1.1. История возникновения и развития компьютерных преступлений: отечественный и зарубежный анализ.....	6
1.2. История создания подразделения по борьбе с компьютерными преступлениями в структуре МВД России.....	14
1.3. Информация как основной элемент при раскрытии преступлений.....	16
2. Криминалистическая характеристика преступлений, совершаемых в сфере компьютерной информации.....	24
2.1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ)	24
2.2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)	29
2.3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-коммуникационных сетей (ст. 274 УК РФ).....	35
3. Особенности расследования и раскрытия преступлений в сфере компьютерной информации.....	38
4. Расследование и раскрытие компьютерных преступлений: проблемы и пути совершенствования	48
4.1. Структура и состояние компьютерной преступности в Российской Федерации.....	48
4.2. Современные проблемы расследования и раскрытия преступлений в сфере компьютерной информации и пути их решения.....	51
4.3. Международное сотрудничество как основной фактор совершенствования методик расследования и раскрытия компьютерных преступлений.....	63
Заключение	73
Список литературы	75

Введение

Актуальность темы исследования обусловлена практической и теоретической значимостью вопросов, связанных со становлением и развитием механизмов обеспечения информационной безопасности в России. Открытия в различных областях науки, развитие информационно-коммуникационных технологий, технологическое перевооружение промышленности привели к кардинальным переменам во всем мире, обусловили переход к новому типу общества – информационному. Основное содержание преобразований, происходящих и в настоящее время, обусловлено процессами создания, обработки, хранения и использования информации в различных сферах деятельности человека.

Компьютеризация ознаменовала современную эпоху научно-технического прогресса. Но, наряду, с бесспорными положительными сторонами компьютеризации, она имеет и негативные стороны, в частности, появление нового вида противоправных деяний, таких как преступления в сфере компьютерной информации. По своему механизму, способам совершения и сокрытия следов, эти преступления имеют свои особенности и характеризуются большой латентностью и низкой раскрываемостью.

Несмотря на многочисленные исследования, проведенные в данной области, многие вопросы на сегодняшний день остаются спорными, либо вовсе нерешенными. Кроме этого, вслед за постоянным внедрением новых технологии идет изменение способов и механизмов совершения преступлений в сфере компьютерной информации. Внедряются новые методы маскировки как самих противоправных деяний, так и следов, указывающих на лиц, их подготовивших и совершивших. Данные обстоятельства требуют постоянного научного внимания к проблеме выявления и расследования преступлений в сфере компьютерной информации, а также глубоких знаний в области информационных технологий у лиц, связанных с этой деятельностью.

Недостаточная изученность криминологической характеристики

неправомерного доступа к компьютерной информации, необходимость совершенствования уголовного законодательства, комплексный анализ правовых и организационно-технических мер предупреждения и противодействия рассматриваемому виду противоправных деяний, предопределили выбор темы дипломной работы.

Объектом исследования данной работы являются общественные отношения, в части правомерного и безопасного использования компьютерной информации и информационных ресурсов.

Предмет исследования включает в себя: преступность в сфере компьютерной информации, как объект уголовно-правового регулирования, ее состояние, структуру и динамику; методы, особенности расследования преступлений в сфере компьютерной информации; совокупность мер по предупреждению компьютерных преступлений.

Цель работы заключается в комплексном уголовно-правовом и криминологическом научном исследовании состояния, тенденций, характерных черт преступлений в сфере компьютерной информации в Российской Федерации.

Задачи исследования:

- проанализировать нормы права, устанавливающие уголовную ответственность за преступления в сфере компьютерной информации;
- исследовать проблемы квалификации преступления и проблемы привлечения к уголовной ответственности;
- раскрыть основные причины и условия, способствующие совершению преступления в сфере компьютерной информации;
- изучить особенности и проблемы в раскрытии и расследовании преступлений в сфере компьютерной информации;

Методологической основой исследования послужили общенаучные методы познания, а также частно-научные методы:

- историко-правовой - применительно к изучению истории компьютерных преступлений, уголовной ответственности за их совершение;

- формально-логический, заключающийся в детальном анализе уголовно-правовых и организационно-технических мер противостояния неправомерному доступу к компьютерной информации;

- статистический, включающий сбор и анализ статистических данных о неправомерном доступе к компьютерной информации.

Структура работы включает в себя введение, 4 главы и заключение. Отдельные главы посвящены истории компьютерных преступлений, методах и особенностях их расследования, включая отечественную и зарубежную практики, а также мерах по предупреждению данных преступлений.

1. Характеристика преступлений в сфере компьютерной информации

1.1. История возникновения и развития компьютерных преступлений: отечественный и зарубежный анализ

С момента зарождения человеческого общества люди испытывают потребность в общении друг с другом. Первоначально общение осуществлялось жестами, знаками, мимикой и нечленораздельными звуками, затем появились человеческая речь, письменность, книгопечатание. В XX столетии получили развитие такие средства коммуникации, как телеграф, телефон, радио, кино, телевидение. В последние десятилетия отмечается бурное развитие компьютерных технологий и их активное внедрение во все без исключения сферы жизни общества. Огромные массивы различных сведений, представлены в виде компьютерной информации, что существенно облегчает работу с ними.

Информационные сети локального характера, а также сеть Интернет, позволяют создать единое информационное пространство, мгновенно обмениваться информацией и оперативно координировать действия различных служб, органов, подразделений и организаций. Внедрение компьютерных технологий позволило автоматизировать различные производственные и управленческие процессы, что способствовало увеличению производительности труда.

В XXI веке с появлением коммуникаторов, смартфонов, «планшетов», компьютер из некогда дорогого, громоздкого стационарного устройства превратился в доступный подавляющему числу жителей планеты мобильный «гаджет», обладающий обширным функционалом.

Вместе с тем, появление ЭВМ и дальнейшее развитие компьютерных технологий привело к возникновению совершенно нового вида преступности - компьютерной.

Родиной термина «компьютерная преступность» считается США, где в 60-х годах прошлого века подобное словосочетание впервые появилось в СМИ в связи с выявлением первых преступлений, совершенных с использованием

ЭВМ. Так, в 1969 г. Альфонсе Конфессоре, получив незаконно доступ к информации в электронно-вычислительной сети, совершил налоговое преступление, ущерб от которого составил \$620000, а в 1970 году, также путем незаконного доступа к информации "Секюрити пасификбэнк" с одного из счетов банка было незаконно списано \$10,2 миллиона¹.

Первое преступление, совершенное с использованием ЭВМ в бывшем СССР, было зарегистрировано в 1979 году в Вильнюсе – это было хищение денежных средств оператором почтовой связи. Используя недостатки программного обеспечения автоматизированного комплекса «Онега», женщина в течение двух лет совершала хищения денежных средств, направляемых гражданам в качестве пенсий и пособий по старости. Общий ущерб от её деяний составил 78584 руб. Огромные деньги по тем временам.

В 1983 году в Париже группой экспертов Организации экономического сотрудничества и развития (ОЭСР) было дано криминологическое определение компьютерного преступления, под которым понималось любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку и (или) передачу данных.

Из года в год подобные преступления стали совершаться чаще, а их сложность и причиняемый ущерб возрастали.

Так, в 1988 г. студент Корнельского университета в городе Итака США Роберт Моррис создал компьютерную программу, названную позже «червь», предназначенную специально для атаки компьютеров через сеть Интернет. В отличие от компьютерных вирусов, которые автоматически присоединяются к той или иной программе, нарушая ее работу, созданная им программа, попав в компьютер – жертву, создавала свои копии и проникала во все системы компьютера, вызывая его сбой, главным образом, за счет «съедания» ресурсов оперативной памяти. До того, как данная программа была нейтрализована, она

¹ Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2001. С. 496.

вызвала сбои в работе примерно 6200 компьютеров в США и других странах, повлекла ущерб на сумму более 98 миллионов долларов США¹.

Что же касается России, то первое преступление с использованием компьютерной техники, было совершено на территории РСФСР в 1991 году, когда были похищены 125,5 тыс. долларов США во Внешэкономбанке СССР сотрудником вычислительного центра данного учреждения.

С появлением новой угрозы, на законодательном уровне неоднократно предпринимались попытки регламентации ответственности за совершение компьютерных преступлений. Так, 06 декабря 1991 года был представлен проект Закона РСФСР «Об ответственности за правонарушения при работе с информацией», который предусматривал введение в действующий Уголовный кодекс РСФСР норм, устанавливающих ответственность за совершение компьютерных преступлений. Постановлением Верховного Совета РФ от 23.09.92 № 3524-1 «О порядке введения в действие Закона Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» предполагалось внесение изменений и дополнений в Гражданский, Уголовный кодекс РСФСР и другие законодательные акты, связанные с вопросами правовой охраны программ для электронных вычислительных машин и баз данных. В 1994 году был разработан проект закона о внесении дополнений в УК РСФСР, которым устанавливалась ответственность за ряд противоправных действий в сфере компьютерной информации. В 1995 году был опубликован проект Уголовного кодекса Российской Федерации, в котором предусматривалась Глава 29 «Компьютерные Преступления», включавшая в себя следующие составы: самовольное проникновение в автоматизированную компьютерную систему (ст. 271); неправомерное завладение программами для ЭВМ, файлами или базами данных (ст. 272); самовольная модификация, повреждение, уничтожение баз данных или программ для ЭВМ (ст. 273); внесение или

¹ Батулин Ю.М. Проблемы компьютерного права / Ю.М. Батулин. М.: Юридическая литература, 1991. С. 272.

распространение вирусных программ для ЭВМ (ст. 274); нарушение правил, обеспечивающих безопасность информационной системы (ст. 275)¹.

1 января 1997 г. вступил в силу новый Уголовный кодекс Российской Федерации, в котором появилась Глава 28 «Преступления в сфере компьютерной информации», объединяющая ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ» и ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети», который с рядом изменений действует и по настоящее время².

Дальнейшее развитие информационных технологий, появление и активное внедрение сети Интернет, массовая компьютеризация привели к бурному развитию компьютерной преступности, как на уровне отдельных государств, в том числе, России, так и на международном уровне³.

С 1997 по 2005 г. произошло увеличение численности выявленных преступлений данного вида. В 1998 г. зарегистрировано 66 преступлений в сфере компьютерной информации, в том числе по ст. 272 УК РФ - 53, по ст. 273 - 12, по ст. 274 - 1. В 1999 г. зарегистрировано 294 преступления, из них по ст. 272 - 209, по ст. 273 - 85. В 2000 г. зарегистрировано 800 преступлений в сфере компьютерной информации, из них по ст. 272 - 584, по ст. 273 - 172, по ст. 274 - 44. В 2003 году в России было возбуждено 1602 уголовных дела по ст. 272 УК РФ («Неправомерный доступ к компьютерной информации»). В 2004 году в РФ было выявлено 8739 компьютерных преступлений, из которых было раскрыто 96%. В 2005 году выявлено 10214 преступлений.

Пик роста компьютерной преступности пришелся на 2009 год. Было зарегистрировано 11636 преступлений подобного рода. Далее наметилась тенденция к снижению количества зарегистрированных преступлений рассматриваемой направленности и, вместе с тем, рост их качественных

¹ Уголовный кодекс РСФСР (утв. ВС РСФСР 27.10.1960; ред. от 30.07.1996) // Ведомости ВС РСФСР. 1960. № 40. Ст. 591 (утратил силу).

² Уголовный кодекс Российской Федерации от 13.06.1996 №63 – ФЗ (ред. от 23.04.2018) // СЗ.1996. № 25. Ст. 2954

³ Сычев Ю.Н. Основы информационной безопасности : учебно-практическое пособие / Ю.Н. Сычев. Изд. центр ЕАОИ, 2007. С. 300.

показателей. Это было связано, в том числе, и с активизацией деятельности правоохранительных органов, повышением профессионального уровня сотрудников подразделений, занимающихся борьбой с компьютерной преступностью. Другой причиной стало повышение мастерства лиц, их совершающих.

Так в 2010 было зарегистрировано (выявлено) 7398 преступлений рассматриваемой категории, а в 2011 всего 2698.

На основании изложенного, можно сделать вывод о том, что компьютерная преступность представляет собой очень серьезную угрозу, как для отдельных государств, так и для всего мирового сообщества, в связи, с чем необходимо разработать и реализовать на практике действенные механизмы противодействия подобным явлениям.

Разработка таких механизмов невозможна без изучения зарубежного опыта борьбы с киберпреступностью, поэтому рассмотрим опыт законодательной регламентации уголовной ответственности за подобные деяния на примере США, Германии и Франции.

Как уже отмечалось ранее, первые компьютерные преступления были совершены на территории США, поэтому, не удивительно, что именно Америка одной из первых законодательно установила уголовную ответственность за их совершение.

Так, в 1977 г. в США был разработан законопроект о защите федеральных компьютерных систем. Он предусматривал уголовную ответственность за такие деяния, как введение заведомо ложных данных в компьютерную систему; незаконное использование компьютерных устройств; внесение изменений в процессы обработки информации или нарушение этих процессов; хищение денежных средств, ценных бумаг, имущества, услуг, ценной информации, совершенные с использованием возможностей компьютерных технологий или с использованием компьютерной информации. На основе данного законопроекта в октябре 1984 г. был принят «Закон о мошенничестве и злоупотреблении с использованием компьютеров» основной нормативно-правовой акт,

устанавливающий уголовную ответственность за преступления в сфере компьютерной информации. В последующем он неоднократно (в 1986, 1988, 1989, 1990, 1994 и 1996 гг.) изменялся и дополнялся, а в настоящее время он включен в виде §1030 в Титул 18 Свода законов США.

В Германии уголовная ответственность за компьютерные преступления была установлена в 1986 году, когда были внесены соответствующие изменения в УК ФРГ. К преступлениям в сфере компьютерной информации согласно УК Германии отнесены:

- действия лиц, неправомочно приобретающих для себя или иного лица непосредственно не воспринимаемые сведения, которые могут быть воспроизведены или переданы электронным, магнитным или иным способом (§ 202a);

- умышленные деяния лиц с намерением получить для себя или третьих лиц имущественную выгоду, заключающееся в причинении вреда чужому имуществу путем воздействия на результат обработки данных путем неправильного создания программ, использования неправильных или данных, неправомочного использования данных или иного воздействия на результат обработки данных (§ 263a);

- подделка или использование поддельных технических записей, под которыми, в числе иного, понимаются данные, полностью или частично регистрируемые автоматическими устройствами (§ 268);

- аналогичная подделка данных, имеющих доказательственное значение (§ 269);

- уничтожение, изменение или утаивание технических записей (§ 274);

- противоправное аннулирование, уничтожение, приведение в негодность или изменение данных (§ 303a);

- нарушение обработки данных путем разрушения, повреждения, приведения в негодность либо приведения в негодность установки для обработки данных или носителей информации (§ 303b).

Уголовный кодекс Франции, вступивший в силу весной 1994 г., также предусматривает уголовную ответственность за ряд компьютерных преступлений. В сфере компьютерной информации УК Франции устанавливает ответственность за совершение следующих преступлений:

- перехват, хищение, использование или предание огласке сообщений, передаваемых средствами дальней связи (ст. 226-15);
- незаконный доступ к автоматизированной системе обработки данных или незаконное пребывание в ней (ст. 323-1);
- воспрепятствование работе или нарушение работы компьютерной системы (ст. 323-2);
- ввод обманным путем в систему информации, а также изменение или уничтожение, содержащихся в автоматизированной системе данных (ст. 323-3);
- ввод или хранение в памяти ЭВМ запрещенных законом данных (ст. 226-19).

К преступлениям в информационном компьютерном пространстве, в соответствии с УК Франции, могут быть также отнесены:

- осуществление или отдача указания об осуществлении автоматизированной обработки поименных данных без осуществления предусмотренных в законе формальностей (ст. 226-16);
- осуществление или отдача указания об осуществлении обработки этих данных без принятия всех мер предосторожностей, необходимых для того, чтобы обеспечить безопасность данных (ст. 226-17);
- сбор и обработка данных незаконным способом (ст. 226-18);
- хранение определенных данных сверх установленного законом срока (ст. 226-20);
- и другие.

За рассматриваемые выше деяния УК Франции предусматривает уголовную ответственность, как для физических, так и для юридических лиц.

Не может обратить на себя внимание тот факт, что законодатели США, ГДР и, особенно, Франции изложили более четкие диспозиции и квалификацию

компьютерных преступлений, что, несомненно, благоприятно отразилось на эффективности их выявления и расследования.

Безусловно, на момент принятия Уголовного кодекса 1997 года Россия существенно отставала от стран Европы по количеству средств вычислительной техники, используемых как организациями различных форм собственности, так и непосредственно гражданами. Но, по моему мнению, ограниченная трактовка противоправных деяний, изложенных в Главе 28 УК РФ, зачастую не способствует их исчерпывающей и правильной квалификации.

С развитием общественно-экономических отношений объемы перерабатываемой информации постоянно увеличиваются, и если XX век многие ученые называли веком энергетики, то XXI - веком информатики.

Высказывание Натана Ротшильда: «Кто владеет информацией, тот владеет миром» в наши дни приобретает все большую актуальность.

Информация обрела реальную цену и с развитием информационных технологий становится все более ценным товаром. Это подтверждает и возникновение виртуальных средств платежей, так называемых «криптовалют», которых по данным различных Интернет ресурсов в мире насчитывается от 1,5 до 1,8 тысяч наименований! И все они имеют свою котировку по отношению к мировым валютам.

Но, новые технологии стимулируют развитие и новых форм преступности. В последние годы отмечается тенденция стремительного роста компьютерных преступлений, совершенных посредством глобальной сети передачи данных «Интернет». Кроме этого, акцент смещается в сторону атак на различные мобильные устройства, так как они получили колоссальное распространение среди жителей планеты, а большая часть их пользователей в силу разных причин пренебрегает элементарными мерами безопасности. Сети же крупных организаций имеют, как правило, несколько степеней защиты, обеспечиваемых как аппаратными устройствами, так и специализированными программными продуктами.

На основании изложенного, можно сделать вывод о том, что компьютерная преступность является одной из самых специфических, сложно устроенных и динамично развивающихся видов преступности. Она является серьезной угрозой, как для отдельных государств, так и для всего мирового сообщества. Ущерб от действий киберпреступников огромен и исчисляется миллиардами долларов. Для эффективной борьбы с данным явлением необходимо совершенствование законодательства, регламентирующего уголовную ответственность за совершение компьютерных преступлений, в том числе и с использованием положительного опыта зарубежных стран. Да и сам термин «Компьютерные преступления» уже потерял свою актуальность. Считаю более правильным обозначить данные деяния как «Преступления, совершаемые в информационно-телекоммуникационной сфере».

1.2. История создания подразделения по борьбе с компьютерными преступлениями в структуре МВД России.

Необходимость создания в структуре МВД России подразделения, занимающегося раскрытием преступлений с использованием информационных технологий, возникла в начале 80-х годов прошлого века. Революционное развитие науки и техники привнесли в общество не только неоспоримые преимущества, но и проблемы, связанные с проникновением преступности в информационное пространство.

В 1986 году для обеспечения радиоэлектронной безопасности органов внутренних дел, выявления специальных технических устройств, предназначенных для негласного съема информации, пресечения попыток проникновения в компьютерные сети и других противоправных действий в сфере компьютерной информации, в структуре МВД СССР было создано Управление радиоэлектронной борьбы (или Управление «Р»).

7 октября 1998 года Управление «Р» было преобразовано в Управление по борьбе с преступлениями в сфере высоких технологий (УБПСВТ). В его

структуре были выделены три направления деятельности:

1. Борьба с преступлениями в сфере компьютерной информации.
2. Борьба с преступлениями в сфере телекоммуникаций.
3. Борьба с незаконным оборотом радиоэлектронных и специальных технических средств.

В территориальных подразделениях МВД Республик, УВД, ГУВД областей до 1999 года были созданы аналогичные структурные подразделения – отделы БПСВТ (ОБПСВТ).

В 2002 году Управление БПСВТ было упразднено, а его штатная численность была передана Главному Управлению Специальных Технических мероприятий МВД России.¹

После серии преобразований название подразделения приобрело свой современный вид – Управление «К» БСТМ МВД России в структуре МВД и отделы «К» в структуре территориальных подразделений МВД.

Основными направлениями оперативно-служебной деятельности отделов «К» в настоящее время являются:

1. Борьба с неправомерным доступом к компьютерной информации.
2. Борьба с преступлениями, связанными с созданием и использованием вредоносного программного обеспечения.
3. Борьба с нарушениями авторских и смежных прав в сфере информационных технологий.
4. Борьба с преступлениями в электронных платежных системах и системах дистанционного банковского обслуживания.
5. Борьба с мошенничеством в сети Интернет.
6. Борьба с преступлениями в сетях связи общего пользования.
7. Борьба с преступлениями, связанными с изготовлением и распространением порнографических материалов, в том числе с изображением несовершеннолетних.

¹ Отдел «К» УМВД России по Тульской области. URL: https://71.xn--b1aew.xn--p1ai/Dejatelnost/Borba_s_kiberprestupnostju (Дата обращения: 23.04.18).

8. Борьба с незаконным оборотом специальных технических средств для негласного получения информации¹.

Со времен создания подразделения злоумышленники придумали множество новых способов реализации своих противоправных намерений, преступления стали более изощренными и циничными. Граждане, организации и государство в целом несут огромные финансовые потери. Все это требует от сотрудников отдела «К» постоянного совершенствования своих профессиональных навыков и разработки новых методов борьбы с киберпреступностью.

За годы своего существования подразделение претерпело немало изменений, целью которых было соответствие современному уровню технического прогресса. Результаты работы отделов по борьбе с «киберпреступностью» используются при раскрытии самого широкого круга преступлений.

Залог успеха заключается в привлечении высококвалифицированных специалистов, создании системы подготовки и повышения квалификации кадров, использовании современных программных средств и передовых методик, а также тесном взаимодействии с поставщиками информационно-телекоммуникационных услуг.

На сегодняшний день Управление «К» БСТМ МВД России эффективно взаимодействуют с различными организациями, функционирующими в сфере высоких технологий, с целью реализации совместных программ, направленных на профилактику преступлений².

1.3. Информация как основной элемент при раскрытии преступлений

Компьютеризация всех слоев населения представляет собой социально значимое явление, ее достижения могут быть использованы не только в

¹ Управление «К» МВД России. URL:

https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (Дата обращения: 23.04.18).

² 19 октября - 25 лет со дня образования БСТМ МВД России. URL: <https://xn--b1aew.xn--p1ai/news/item/11374675> (Дата обращения: 23.04.18).

хороших намерениях, но и при совершении преступлений компьютерной направленности. Компьютерные преступления носят специфичный характер, так как способы их совершения настолько многогранны, что сотрудникам подразделений «К» при документировании и раскрытии данного вида преступлений приходится сталкиваться с определенными трудностями. Для их преодоления разрабатываются и внедряются новые формы и методы оперативно-розыскной деятельности.

Действующий уголовный закон в настоящее время защищает не только документированную информацию, но и ее разновидности, что расширяет возможности своевременно изобличать лиц, совершающих преступления данной направленности. Из проведенного анализа Уголовного кодекса Российской Федерации следует отметить, что отношения, возникающие в области компьютерной информации, в настоящее время подлежат специальной охране.

В главу 28 УК РФ о преступлениях в сфере компьютерной информации введены термины и понятия, которых ранее не было не только в уголовно-правовой терминологии, но и в законодательстве, регулировавшем информационные отношения.

Проанализировав нормы из различных отраслей права, можно сделать ряд выводов¹:

1. Информация - сведения (сообщения, данные) независимо от формы их представления².
2. Правовой защите подлежит любая документированная информация, т.е. информация, облеченная в форму, позволяющую ее идентифицировать.
3. Документированная информация является объектом гражданских прав и имеет собственника.

¹ Сычев Е.А., Алексеров В.И., Колокольчикова О.Н. Преступления, совершаемые в телекоммуникационных сетях, как разновидность преступлений в сфере компьютерной информации // Е.А. Сычев, В.И. Алексеров, О.Н. Колокольчикова. Историческая и социально-образовательная мысль. 2014. № 4. С. 350–355.

² Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ // СЗ. 2006. № 31. Ст. 3448.

4. Информация может быть конфиденциальной, ознакомление с которой ограничивается ее собственником или нормами закона, и массовой, предназначенной для широкого круга лиц.

5. Ограничения использования информации устанавливаются законом или собственником информации, которые объявляют уровень ее конфиденциальности.

Конфиденциальными в соответствии с законом являются, в частности, такие виды информации, как:

- содержащая государственную тайну;
- передаваемая путем переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений¹;
- содержащая служебную тайну, коммерческую тайну, банковскую тайну, личную тайну и семейную тайну, информация, являющаяся объектом авторских и смежных прав;
- непосредственно затрагивающая права и свободы гражданина или персональные данные и др.

6. Любая форма завладения и пользования конфиденциальной документированной информацией без прямо выраженного согласия ее собственника является нарушением его прав, т.е. неправомерным деянием.

Уголовно-правовой анализ преступлений в сфере компьютерной информации невозможно провести без предварительного уяснения родового понятия «информации». Информация как таковая выступает в качестве сравнительно нового предмета исследования и особого объекта правового регулирования. Именно поэтому необходимо обратиться не только к законодательным понятиям информации, но и к научным ее толкованиям.

Понятие «информация» имеет как минимум четыре основных значения:

- как сведения, передаваемые людьми любым способом;
- как общенаучное понятие;
- как обмен сигналами в животном и растительном мире;

¹ Российская Федерация. Конституция (1993) // СЗ. 2014. № 31. Ст. 4398.

- информация как кибернетический термин.

Само слово «информация» происходит от латинского «information» и означает «разъяснение» или «осведомленность». Начальные шаги в теории информации были сделаны еще в первой половине XX в. В 1928 г. американский инженер Ральф Хартли впервые дал количественное определение информации, а в 1948 г. вышла знаменитая книга его соотечественника Клода Шеннона «Математическая теория связи», где информация и дается уже как статистическое определение.

Таким образом, информация с точки зрения кибернетики представляется не как общественный феномен, то есть информация, производимая и потребляемая обществом, а в более узком, техническом аспекте – как информация, циркулирующая по электронным каналам связи. Кибернетика доказала, что информация имеет непосредственное отношение к процессам управления и развития, обеспечивающим функционирование любых систем¹.

Информационная сфера сегодня – это одна из наиболее динамичных и быстро развивающихся сфер общественных отношений, нуждающаяся в адекватном правовом регулировании. С этой целью создается «информационное» законодательство, а также система мер уголовно-правовой защиты данной группы отношений.

Основное различие правового режима информации состоит в степени ее доступности для пользователей. Так, в зависимости от категории доступа к ней, информация подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)².

В соответствии со ст. 5 ФЗ № 149 от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации», информация в зависимости от порядка ее предоставления или распространения подразделяется на:

¹ Вестник Всероссийского института повышения квалификации сотрудников МВД России // 2013. №2. С. 32–37.

² Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации: учеб. пособие / А.А. Фатьянов. М.: Юрист, 2001. С. 10.

- 1) информацию, свободно распространяемую;
- 2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- 3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- 4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Основополагающие принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации заложены в ст. 3 рассматриваемого Федерального закона и основываются на принципах:

- 1) свободы поиска, получения, передачи, производства и распространения информации любым законным способом;
- 2) установления ограничений доступа к информации только федеральными законами;
- 3) открытости информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- 4) равноправия языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- 5) обеспечения безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- 6) достоверности информации и своевременности ее предоставления;
- 7) неприкосновенности частной жизни, недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- 8) недопустимости установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных

информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами¹.

Проблемы в правоприменительной практике связаны с тем, что на законодательном уровне определение «компьютерной информации» появилось относительно недавно. Однако в специальной и учебной литературе предложено множество определений рассматриваемого термина. Одними из первых, понятие «компьютерной информации» дали: в 1998 году Т.Г. Смирнова, определив в своей диссертации компьютерную информацию как «совокупность сведений, представляющих особую ценность для государства, общества и отдельных граждан, производство, хранение и использование которых осуществляется посредством компьютерной техники», и в 2000г. А.А. Петров, предложивший понимать в своей книге «Компьютерная безопасность» под данным термином «информацию, содержащую сведения, составляющие государственную или коммерческую тайну, сведения конфиденциального характера и общего пользования».

Следует отметить, что предложенные определения не лишены недостатков. Из определения Т.Г. Смирновой следует, что информация и ее материальный носитель («компьютерная техника») неотделимы друг от друга, а исходя из такого подхода, компьютерная информация, циркулирующая в сетях передачи данных, либо записанная на каком-либо носителе, не будет являться предметом данной категории преступлений. Из понятия данного А.А. Петровым вообще невозможно выделить отличительные признаки компьютерной информации как таковой.

Более корректными представляются определения, предложенные в постатейных комментариях к Уголовному кодексу В.С. Комиссаровым в 1997 году и С.А. Пашиным в комментариях от 2001 года. Первый автор считает, что «компьютерная информация может находиться или на машинном носителе (магнитном диске, магнитной ленте, дискете, магнитно-оптическом диске или

¹ Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ // СЗ. 2006. № 31. Ст. 3448.

непосредственно в ЭВМ (в постоянном или оперативном запоминающих устройствах)), либо в системе ЭВМ или их сети». Второй определил, что «компьютерная информация - это информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ».

На мой взгляд, оба понятия более четко отражают критерии предмета преступления в сфере компьютерной информации.

Нельзя не согласиться и с определением «компьютерного преступления», предложенным авторами В.А. Дуленко, Р.Р. Мамлеевым, В.А. Пестриковым, где сказано, что компьютерное преступление как уголовно-правовое понятие – это предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства¹.

С учетом представленных позиций вышеуказанных авторов, на сегодняшний день в действующей редакции Уголовного кодекса РФ под компьютерной информацией понимаются «сведения (сообщения, данные), представленные в форме электрических сигналов независимо от средств их хранения, обработки и передачи».

Уголовно-правовой защите должны подлежать любые сведения, неправомерное обращение с которыми может нанести ущерб их собственнику (владельцу, пользователю).

Исходя из вышеизложенного, можно сделать вывод, что на начальном этапе раскрытия преступлений в сфере компьютерной информации немаловажное значение имеет своевременное получение сведений о факте совершенного или подготавливаемого преступлении, объекте преступного посягательства и последствиях, наступивших в результате его совершения. Полученная информация позволит избрать правильную линию поведения

¹ Дуленко В.А., Мамлеев Р.Р., Пестриков В.А. Преступления в сфере высоких технологий: учеб. пособие / В.А. Дуленко, Р.Р. Мамлеев, В.А. Пестриков. М.: ЦОКР МВД России, 2010. С. 67.

оперативным сотрудникам подразделений «К» с целью определения необходимого комплекса неотложных оперативно-розыскных, специальных технических мероприятий и следственных действий.

Это поможет с наименьшей затратой времени выйти на более точное оперативное сопровождение по установлению конкретных лиц, причастных к совершенному преступлению, и, как положительный результат, приведет к изобличению фигурантов с закреплением полученных в ходе документирования доказательств¹.

¹ Вестник Всероссийского института повышения квалификации сотрудников МВД России // 2013. №2. С. 32–37.

2. Криминалистическая характеристика преступлений, совершаемых в сфере компьютерной информации

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

Статья 272 УК РФ предусматривает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации. Современное понятие компьютерной информации было введено Федеральным законом от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации».

Общим объектом преступления, предусмотренного ст. 272 УК РФ, выступают общественные отношения, обеспечивающие правомерный доступ, создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление ее иными пользователями. В ч. 3 ст. 272 УК РФ указан дополнительный объект преступления – общественные отношения, обеспечивающие интересы службы.

Диспозиция ч. 1 ст. 272 УК РФ в предыдущей редакции от 07.03.2011 была изложена следующим образом: «Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети». В действующей редакции ч. 1 ст. 272 УК РФ изложена следующим образом: «Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации».

Законодатель внес данные изменения, чтобы решить ряд проблем, возникающих в правоприменительной практике. Например, при рассмотрении дел указанной категории суды зачастую сталкивались с трудностями, когда

неправомерный доступ осуществлялся к устройству, не подпадающему под определение ЭВМ, но по своим свойствам и функциям фактически не уступающему ЭВМ по возможности хранения и обработки информации (мобильные телефоны, смартфоны, карманные персональные компьютеры).

Неправомерный доступ к компьютерной информации осуществляется, как правило, с использованием чужого имени, подменой физических идентификаторов технических устройств, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных, либо интерфейсам периферийных устройств ввода-вывода..

Хакеры или компьютерные пираты - так называют компьютерных правонарушителей, осуществляющих противоправный несанкционированный доступ в чужие информационные сети.

Несанкционированный противоправный доступ к файлам и информации законного пользователя осуществляется также нахождением слабых мест в компьютерной защите системы. Однажды обнаружив их, преступник может неспешно исследовать содержащуюся в системе информацию, копировать ее, внедрять вредоносное программное обеспечение (ПО) в операционную систему.

Разработчики программного обеспечения иногда допускают ошибки (так называемые «баги» или «дыры») в программах, которые не удается обнаружить в процессе отладки. Условно это можно представить какой-либо определенной последовательностью действий (команд, операций) пользователя, которые приводят к неадекватному реагированию системы. Например, нештатному отключению, либо «зависанию» служб безопасности, перезагрузке ПО с небезопасными параметрами и т.д.

Уязвимые места обнаруживаются и в электронных сетях. Все эти небрежности, ошибки приводят к появлению у злоумышленника возможности совершения противоправного деяния.

Еще одним способом проникновения правонарушителя в компьютерную систему является маскировка себя под легитимного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам, по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т.п.), оказываются без защиты против этого способа совершения преступления. Самый простейший путь его осуществления – это получить коды и другие идентифицирующие реквизиты законных пользователей. Это возможно путем:

- приобретения (обычно подкупом персонала) списка пользователей со всей необходимой информацией;
- обнаружения такого документа в организациях, где не налажен достаточный контроль за их хранением;
- незаконного, несанкционированного подслушивания через телефонные линии;
- внедрения программных и аппаратных перехватчиков (снифферов) трафика.

Объективная сторона состава преступления включает в себя действие, состоящее в неправомерном доступе к охраняемой законом компьютерной информации (информации ограниченного доступа) и его последствия в виде уничтожения, блокирования, модификации, копирования компьютерной информации, а также возможную причинно-следственную связь между указанным действием и любым из названных последствий.

Законодателем не уточнено понятие доступа к информации. Указанное понятие содержится в п. 6 статьи 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», согласно которому: «доступ к информации – возможность получения информации и ее использования». Под охраняемой законом понимается информация, для которой законом установлен специальный режим ее правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные и т.д.).

Неправомерным считается доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты. Другими словами, неправомерный доступ к компьютерной информации – это незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации. При этом под доступом понимается проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники, позволяющее использовать полученную информацию (копировать, модифицировать, блокировать либо уничтожать ее).

Состав данного преступления носит материальный характер и предполагает обязательное наступление одного из последствий:

а) уничтожение информации – это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое «вытеснение» старых версий файлов последними по времени;

б) блокирование информации – результат воздействия на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, то есть совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением;

в) модификация информации – внесение изменений в компьютерную информацию (или ее параметры). Законом установлены случаи легальной модификации программ (баз данных) лицами, правомерно владеющими этой информацией, а именно: модификация в виде исправления явных ошибок;

модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя; модификация в виде частной декомпиляции программы для достижения способности к взаимодействию с другими программами;

г) копирование информации – создание копии имеющейся информации на другом носителе, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме – от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации и т.п.

Однако, если в силу настроек компьютерной программы при работе с ней, пусть даже и в результате неправомерного доступа, автоматически создается резервная копия компьютерной информации, то данное действие не будет иметь уголовно-правовых последствий, поскольку оно осуществляется независимо от волеизъявления лица и, соответственно, в прямой причинной связи с его действиями не состоит. Преступление окончено с момента наступления любого из указанных последствий. Устанавливая причинную связь между несанкционированным доступом и наступлением вредных последствий, следует иметь в виду, что в компьютерных системах возможны уничтожение, блокирование и модификация компьютерной информации в результате технических неисправностей или ошибок при функционировании операционной среды или иных программ. В этих случаях лицо, совершившее неправомерный доступ к компьютерной информации, не подлежит ответственности по данной статье ввиду отсутствия причинной связи между его действиями и наступившими последствиями.

Еще одной особенностью диспозиции данной статьи, по моему мнению, является отсутствие такого последствия незаконного доступа к информации как ознакомление с ней. Возможны случаи, когда злоумышленнику будет достаточно просто запомнить те или иные сведения, неправомерное

использование которых, приведет к нежелательным последствиям для правообладателя.

Субъективная сторона рассматриваемого преступления характеризуется виной в форме умысла (прямого или косвенного).

Субъект преступления общий – вменяемое лицо, достигшее шестнадцати лет. Вместе с тем ч. 3 ст. 272 УК РФ предусматривает наличие специального субъекта, совершившего данное преступление с использованием своего служебного положения. Под использованием служебного положения, предусмотренного в диспозиции ч. 3 ст. 272 УК РФ, понимается использование возможности доступа к компьютерной информации, возникшей в результате выполняемой работы (по трудовому, гражданско-правовому договору) или влияния по службе на лиц, имеющих такой доступ (в данном случае субъектом преступления не обязательно является должностное лицо), то есть тех, кто на законных основаниях использует компьютерную информацию и средства ее обращения (программисты, сотрудники, вводящие информацию в память компьютера, другие пользователи, а также администраторы баз данных, инженерно-технический персонал, специалисты по эксплуатации электронно-вычислительной техники и прочие).

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

Понятие компьютерной программы достаточно многогранно. Необходимо разделить два основных толкования термина «программа». В качестве первого, может выступать исходный набор команд, инструкций и правил, присущих конкретному языку программирования, оформленный в соответствии с определенными синтаксическими правилами. Это является так называемым «исходным кодом» или текстом программы. Текст может содержаться на листе бумаги, размещен в текстовом файле, представлен в

любом ином формате, позволяющем модифицировать себя средствами текстовых редакторов или оболочкой языка программирования.

После преобразования, или на языке разработчиков - компиляции исходного текста программы в исполняемый файл, мы получаем исполняемый код, который понятен операционной системе и аппаратной части ЭВМ. Исполняемый код невозможно модифицировать стандартными редакторами, да и с применением специальных средств, эта задача будет под силу лишь узкому кругу специалистов.

В статье 273 УК РФ термин «компьютерная программа» подразумевает свою трактовку именно как исполняемый код, т.е. комбинация инструкций и данных определенного языка программирования, позволяющая аппаратному обеспечению вычислительной системы выполнять вычисления или функции управления.

Любой корректно исполняемый код будет восприниматься аппаратной частью ЭВМ как набор команд и функций, реализующих определенные задачи.

В общих случаях вычислительная система не может разделить исполняемые ей программы на вредные и полезные.

Вредоносность программы определяется ее конечными задачами, в качестве которых, как правило, выступают несанкционированное уничтожение, блокирование, модификация, копирование информации, нейтрализация средств защиты, нарушение функционирования ЭВМ и сетей передачи данных.

Таким образом, по моему мнению, верное определение вредоносной компьютерной программы может быть изложено как исполняемый машинный код, задачами которого являются несанкционированное скрытое уничтожение, блокирование, повреждение, копирование, модификация информации пользователя, нарушение нормального функционирования ЭВМ и сетей передачи данных.

Еще одной задачей вредоносной компьютерной программы является воспроизводство самой себя на сторонних ресурсах, доступ к которым получен в результате осуществления вышеуказанных неправомерных действий.

Эта особенность характерна для выделенных в отдельный класс вредоносных программ, называемых «компьютерными вирусами».

Компьютерный вирус – это специально написанная, как правило, небольшая по размерам программа, которая может записывать (внедрять) свои копии (возможно, изменённые) в компьютерные программы, расположенные в исполняемых файлах, системных областях дисков, драйверах, документах и т.д., причём эти копии сохраняют возможность к «размножению». Процесс внедрения вирусом своей копии в другую программу (системную область диска и т.д.) называется заражением, а программа или иной объект, содержащий вирус, – заражённым.

Использование в названии рассматриваемой статьи термина «вредоносные программы» не случайно. Если бы средством совершения данного преступления были только «компьютерные вирусы», это существенно ограничило бы применение рассматриваемой уголовно-правовой нормы. Например, компьютерный вирус может быть безвредным, следовательно подвергать его создателя уголовному преследованию будет необоснованно.

Создание вредоносной программы – написание ее алгоритма и преобразование его в исполняемый машинный код. Соответственно, внесение изменений в программу означает исключение её отдельных частей, внесение новых фрагментов или изменение алгоритма.

Вредоносность или полезность соответствующих программ для ЭВМ определяется не в зависимости от их назначения, способности уничтожать, блокировать, модифицировать, копировать информацию (это вполне типичные функции абсолютно легальных программ), а в связи с тем, предполагает ли их действие, во-первых, предварительное уведомление собственника компьютерной информации или другого добросовестного пользователя о характере действия программы, а во-вторых, получение его согласия (санкции) на реализацию программой своего назначения. Нарушение одного из этих требований делает программу для ЭВМ вредоносной.

Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Известны случаи, когда вирусы блокировали работу организаций и предприятий. Более того, несколько лет назад был зафиксирован случай, когда компьютерный вирус стал причиной гибели человека. В одном из госпиталей Нидерландов пациент получил летальную дозу морфия по той причине, что компьютер был заражен вирусом и выдавал неверную информацию (вирус произвёл модификацию).

Следует отметить, что вредоносные программы могут быть хорошо замаскированы и до поры до времени ни как себя не проявлять. Как правило, их код встраивается в уже имеющееся ПО, причем не нарушая штатное функционирование последнего. Свои действия эти программы могут начать при наличии определенных условий в системе («логическая бомба»), либо достижении определенного периода времени («временная бомба»).

Логическая бомба, например, может начать работу при подключении отдельной ПЭВМ в сеть конкретного предприятия. Временная бомба может проявлять активность при наступлении периода зачисления денежных средств на расчетные счета сотрудников предприятия.

Имеется еще одна разновидность вредоносных программ. Ее особенность заключается в том, что в обычную часть программы вставляются команды, формирующие другие команды и после выполнения уничтожающие их. В этом случае программисту, пытающемуся найти вредоносную программу, необходимо искать не ее саму, а команды, ее формирующие. Развивая эту идею, можно представить себе вредоносные команды, которые создают команды и т.д. (сколь угодно большое число раз), создающие вредоносную программу по типу «троянского коня».

Объектом рассматриваемого преступления являются общественные отношения в сфере обеспечения безопасности компьютерной информации.

Субъектом - лицо, достигшее 16 лет. Квалифицирующим обстоятельством данного преступления является наступление тяжких

последствий (ч. 2 ст. 273 УК). При фиксации последствий в данном составе преступления законодатель использует оценочное понятие.

Следовательно, их тяжесть должна определяться с учетом конкретных обстоятельств дела: имущественный ущерб, сопряженный с восстановлением информации; упущенная выгода при срыве заключения крупного контракта или соглашения; дезорганизация работы предприятий или учреждений и т.п. Форма вины по отношению к тяжким последствиям может быть только неосторожной.

Объективная сторона выражается в совершении одного из следующих действий:

- создание вредоносной программы, приводящей к несанкционированному уничтожению, блокированию, модификации либо копированию информации, а также к нейтрализации средств защиты компьютерной информации;
- внесение изменений в существующие программы, заведомо приводящие к указанным последствиям;
- использование вредоносной программы или машинного носителя с такой программой;
- распространение вредоносной программы или машинного носителя с такой программой.

Субъективная сторона преступления, содержащегося в ч. 1 ст. 273 УК РФ, выражается только в прямом умысле, то есть лицо осознает общественную опасность своих деяний, предвидит возможность наступления общественно-опасных последствий и желает их наступления. Для данного преступления характерен признак заведомости – очевидность для виновного того, что созданная им программа может причинить указанные в законе общественно-опасные последствия. Если же лицо не знало об опасности распространяемых им программ, то лицо не должно быть подвергнуто уголовному преследованию.

Распространение программы для ЭВМ возможно как в активной (внедрение вредоносной программы в ЭВМ, их систему или сеть любым способом, предоставляющим свободный доступ к ней), так и пассивной

(невоспрепятствование самораспространению вредоносной программы или распространению ее третьими лицами) формах.

Распространение машинного носителя с программой для ЭВМ – это передача его третьим лицам в любой форме.

Непосредственным объектом данного преступления является неприкосновенность и стабильность компьютерной информации и ее материального носителя – ЭВМ.

Рассмотрим примеры выявленных преступлений, раскрытых в тесном взаимодействии сотрудников Управления «К» со службой безопасности ОАО «Сбербанка России» и ЦИБ ФСБ России, взятые из практики.

В результате проделанной работы сотрудниками Управления «К» БСТМ МВД России во взаимодействии со Службой безопасности ОАО «Сбербанка России» была пресечена противоправная деятельность членов организованной преступной группы, причастных к более чем 200 хищениям, совершенным с использованием вредоносной программы «Stels APK», нацеленной на компрометацию профессиональных данных, размещенных на планшетах и телефонах под управлением оперативной системы Android. Данная вредоносная программа после успешного внедрения на устройство пользователя скрытно осуществляла отправку СМС - сообщения на номер «900» (технический номер ОАО «Сбербанка России») с затребованием баланса счета пользователя, после чего пересылала полученный ответ на сервер злоумышленников, в последующем осуществляла переводы денежных средств с банковского счета на заранее подготовленные счета мобильных телефонов и банковских карт, подконтрольные преступникам.

В октябре-ноябре 2015 года Управлением «К» совместно с ЦИБ ФСБ России в целях декриминализации сетей связи был осуществлен комплекс организационных, оперативно-розыскных и оперативно-технических мероприятий по результатам которых был установлен и задержан житель г. Ярославля гражданин «Е», 1980 года рождения. Фигурант организовал преступную деятельность в различных регионах Российской Федерации и

Украины, связанную с разработкой, распространением и использованием вредоносных программ для операционной системы «Андроид» с целью последующего хищения денежных средств, привязанных к абонентским номерам сотовых телефонов банковских карт ОАО «Сбербанк России».

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

Объектом преступления являются отношения в сфере обеспечения безопасности.

Субъект данного преступления – специальные. Им может являться лицо, имеющее законный доступ к эксплуатации упомянутых технических средств, достигшее 16 лет. Это могут быть программисты, операторы ЭВМ, системные администраторы, техники-наладчики и другие лица, имеющие доступ к ним в соответствии с возложенными служебными обязанностями. Квалифицирующим признаком ч. 2 ст. 274 УК является наступление тяжких последствий, а субъективная сторона характеризуется неосторожной формой вины по отношению к этим последствиям.

Объективную сторону преступления образует нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это причинило существенный вред.

Субъективную сторону характеризует преступление, которое может быть совершено как умышленно, так и по неосторожности в виде, как небрежности, так и легкомыслия. При установлении умысла на нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации, информационно-телекоммуникационных сетей, деяние

предусмотренное ст. 274 УК, становится лишь способом совершения иного преступления.

Данное преступное деяние в этом случае подлежит квалификации по наступившим последствиям, которые предвидел виновный, по совокупности с преступлением, предусмотренным данной статьей УК.

Под охраняемой законом информацией следует понимать информацию, изъятую из публичного (открытого) оборота на основании закона, других нормативных (включая ведомственные) актов, а также правил внутреннего распорядка, основанных на упомянутых нормативных документах. По общему правилу такая информация имеет гриф ограниченного пользования.

Правила эксплуатации компьютерной системы – это правила одной из перечисленных ниже разновидностей:

- правила, содержащиеся в общих требованиях по технике безопасности и эксплуатации компьютерного оборудования;
- правила, установленные изготовителями компьютерного оборудования;
- правила, установленные разработчиками программного обеспечения;
- правила внутреннего распорядка, установленные владельцами компьютерной системы или сети и т.д.

Нарушение этих правил (несоблюдение, ненадлежащее соблюдение, либо прямое несоблюдение) может быть осуществлено как путем активного действия, так и бездействия. Состав ч. 1 ст. 274 УК РФ сформулирован как материальный. При этом общественно опасные последствия заключаются в одновременном наличии двух факторов:

- уничтожении, блокировании или модификации охраняемой законом информации в ЭВМ;
- вызванного этим существенного вреда.

Нарушения правил эксплуатации могут выражаться в блокировке системы защиты от несанкционированного доступа, нарушении правил электро- и противопожарной безопасности, отключении сигнализации, длительном оставлении без присмотра, нарушении температурного режима в

помещении, неправильном подключении ЭВМ к источникам питания, нерегулярном техническом обслуживании, несвоевременном обновлении антивирусного ПО, нарушении порядка ведения диалога с компьютером и т.д.

Из рассмотренного следует, что если преступления, квалифицируемые статьей 272 УК РФ «Неправомерный доступ к компьютерной информации», а также статьей 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ», осуществляются только путём совершения действий, то преступления, квалифицируемые статьей 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» – путём как действий, так и бездействием.

Неправомерный доступ к компьютерной информации и нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей сформулированы как преступления с материальным составом, а создание либо использование вредоносных программ для ЭВМ – с формальным. В качестве последствий в статье 272 и 274 УК указываются: уничтожение, модификация, блокирование либо копирование информации, нарушение работы ЭВМ или системы ЭВМ, причинение существенного вреда и т. п.¹.

¹ Алексеров В.И., Колокольчикова О.Н. Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации: учеб. пособие / В.И. Алексеров, О.Н. Колокольчикова. М.: ВИПК МВД России, 2016. С. 52–67.

3. Особенности расследования и раскрытия преступлений в сфере компьютерной информации

В динамичных условиях нашего времени общество постоянно сталкивается с проблемами различного характера, порождение которых зачастую вызвано стремлением к созданию более совершенных и эффективных моделей существования. Это в полной мере относится и к такой специфической сфере, которая все более быстрыми темпами внедряется в современную жизнь мирового сообщества, – как область применения электронной техники и информационных технологий.

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы способны вызвать тяжелые и необратимые последствия.

Одним из важнейших составляющих элементов криминалистической характеристики методики раскрытия компьютерных преступлений является субъективная особенность личности преступника, которая на начальном этапе раскрытия преступлений зачастую характеризуется лишь скудной информацией, а порой и отсутствует вовсе. Для успешного расследования преступления необходимо учитывать такие составляющие личности подозреваемого лица, как пол, возраст, социальное происхождение, уровень образования, род занятий, семейное положение, социальный статус, уровень материальной обеспеченности, место жительства, а также места проведения досуга и возможная принадлежность к определенной субкультуре¹.

Иными словами, немаловажное значение в раскрытии любого вида компьютерного преступления играет своевременно полученная информация,

¹ Ворошилова Т.В. Социальная и психологическая характеристика личности компьютерного преступника: практ. пособие. М.: ВНИИ МВД России. 2009. С. 5.

раскрывающая характерологическую особенность психологии личности преступника. Данная информация позволит определить правильную линию поведения оперативных сотрудников подразделений «К», сузить круг подозреваемых лиц, установить мотив преступления, способ его совершения, а также выдвинуть конкретные версии, отработка которых точно сориентирует и приблизит оперативных сотрудников и следователей к проведению оперативно-розыскных, специальных технических мероприятий и следственных действий, способствующих раскрытию данного вида преступлений. Это позволит с наименьшей затратой времени выйти на более точное оперативное сопровождение по установлению конкретных лиц, причастных к совершенному преступлению, и приведет к изобличению фигурантов с закреплением полученных в ходе документирования доказательств. В качестве примера, можно указать, что в отношении лица, находящегося в местах лишения свободы и рассылающего со смартфона стандартные вредоносные ссылки лицам, разместившим объявления на различных торговых площадках, будет проведен иной комплекс ОРМ, нежели в отношении инженера-программиста, окончившего престижный технический ВУЗ и разработавшего уникальную вредоносную программу.

Выявление лица, причастного к совершению компьютерного преступления – сложный комплекс оперативно-розыскных, технических мероприятий и криминалистических исследований, подробный анализ которого выходит за рамки тематики данной работы.

Рассмотрим механизм раскрытия компьютерного преступления когда подозреваемое лицо (круг лиц) выявлено, либо известно.

В этом случае первоначальная задача оперативных сотрудников и следствия заключается в полном установлении обстоятельств дела, сборе с помощью собственника информационной системы и процессуальной фиксации доказательств:

а) нарушения целостности или конфиденциальности информации в системе;

б) размера ущерба, причиненного нарушением целостности или конфиденциальности информации;

в) механизма совершения преступления, а именно: причинной связи между действиями, образующими способ совершения, и наступившими последствиями путем детализации способа нарушения целостности или конфиденциальности информации в системе и характера совершенных виновным лицом действий;

г) отношение виновного лица к совершенным действиям и наступившим последствиям.

Если подозреваемые задержаны сразу после совершения преступления, для данной ситуации характерны следующие первоначальные следственные действия:

а) личный обыск задержанных;

б) допрос задержанных;

в) обыск по месту жительства, месту работы и месту задержания.

Осмотр и обыск (выемка) по делам данной категории являются важнейшими инструментами установления обстоятельств расследуемого преступления.

Известно, что главными процессуальными способами изъятия вещественных доказательств являются осмотр, обыск и выемка.

Следует напомнить, что осмотр – это непосредственное обнаружение, восприятие и исследование следователем (оперативным сотрудником по отдельному поручению следователя) материальных объектов, имеющих отношение к исследуемому событию. Обыск – следственное действие, в процессе которого производится поисковые действия и принудительное изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства. Выемка – следственное действие, в процессе которого производится изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства, в тех случаях, когда их

местонахождение точно известно следователю и изъятие прямо или косвенно не нарушает прав личности¹.

Носители информации, имеющие отношение к расследуемому преступлению, могут быть с соблюдением установленного УПК РФ порядка изъяты и приобщены к уголовному делу в качестве вещественных доказательств.

Для участия в обыске и выемке целесообразно приглашать специалиста в области телекоммуникаций и компьютерной информации (техники).

Видится целесообразным отметить определенные особенности производства осмотров и обысков.

Если компьютер работает, ситуация для следователя, производящего следственное действие без помощи специалиста, существенно осложняется, однако и в этом случае не следует отказываться от оперативного изъятия интересующих данных.

В этой ситуации необходимо:

а) определить, какая программа выполняется. Для этого необходимо изучить изображение на экране дисплея и, по возможности, детально описать его.

Используя «Диспетчер файлов» (одновременное нажатие клавиш Ctrl-Alt-Del), можно посмотреть, какие процессы на данном компьютере запущены (за исключением скрытых). Необходимо помнить, что программы, имеющие функцию экстренного уничтожения информации, могут работать и в скрытом режиме.

После остановки программы и выхода в операционную систему иногда при нажатии функциональной клавиши «F3» можно восстановить наименование вызывавшейся последний раз программы.

Можно осуществить фотографирование или видеозапись изображения;

¹ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 23.04.2018)
// Российская газета. 2001. № 2861.

б) остановить исполнение программы. Остановку можно осуществить также с использованием «Диспетчера файлов», либо одновременным нажатием клавиш Ctrl-C или Ctrl-Break;

в) зафиксировать (отразить в протоколе) результаты своих действий и реакции компьютера на них;

г) определить наличие у компьютера внешних устройств, накопителей информации на жестких магнитных дисках и картах памяти, виртуального диска;

д) определить наличие у компьютера внешних устройств удаленного доступа к системе и определить их состояние (отразить в протоколе), после чего разъединить сетевые кабели так, чтобы никто не мог изменить или уничтожить информацию в ходе обыска (например, отключить телефонный шнур из модема);

е) скопировать программы и файлы данных. Копирование осуществляется стандартными средствами операционной системы;

ж) выключить подачу энергии в компьютер и далее действовать по схеме «компьютер не работает».

Если компьютер не работает, следует:

а) точно отразить в протоколе следственного действия и на прилагаемой к нему схеме местонахождение компьютера и его периферийных устройств;

б) точно описать порядок соединения между собой этих устройств с указанием особенностей (цвет, количество соединительных разъемов, их спецификация) соединительных проводов и кабелей; перед разъединением полезно осуществить видеозапись или фотографирование мест соединения;

в) с соблюдением всех мер предосторожности разъединить устройства компьютера, предварительно обесточив его;

г) упаковать отдельно носители (диски, карты памяти и др.) и поместить их в оболочки, не несущие заряда статического электричества;

д) упаковать каждое устройство и соединительные кабели, провода;

е) особой осторожности требует транспортировка жесткого диска.

Отдельного внимания заслуживают особенности поиска и изъятия информации, следов воздействия на нее в компьютере и его устройствах.

В компьютере информация может находиться непосредственно в оперативном запоминающем устройстве (ОЗУ) при выполнении программы, в ОЗУ периферийных устройств и на внешних запоминающих устройствах (ВЗУ).

Наиболее эффективным и простым способом фиксации данных из ОЗУ является распечатка на бумагу информации, появляющейся на мониторе. Также можно использовать специализированное программное обеспечение для сохранения и последующей визуализации дампа памяти.

Дамп памяти – это копия содержимого оперативной памяти, находящаяся на жёстком диске или другом энергонезависимом устройстве памяти. Естественно, дампом может быть не вся оперативная память, а только какая-то определённая её часть, которая, так сказать, интересует в данный момент ту программу, которая делает этот дамп.

Ниже приводится один из способов получения дампа памяти:

1. Правой кнопкой мышки щелкнуть по значку «Мой компьютер».
 2. Щелкнуть по пункту меню «Свойства». Появится окно «Свойства системы».
 3. Перейти на вкладку «Дополнительно» и щелкнуть по кнопке «Параметры».
 4. Снять галочку с «Выполнить автоматическую перезагрузку».
- Указать путь, по которому будет создан дамп.
5. В секции «Запись отладочной информации» выбрать «Дамп памяти ядра».
- Для этого необходимо щелкнуть по выпадающему списку.
6. Нажать кнопку ОК. По указанному адресу будет записан дамп памяти.

Если Вы указали дамп памяти ядра, то дамп будет находиться в каталоге Windows с именем Memory.dmp.

Если компьютер не работает, информация может находиться в ВЗУ и других компьютерах информационной системы или в «почтовых ящиках» электронной почты или сети ЭВМ.

Необходимо произвести детальный осмотр файлов и структур их расположения, лучше это осуществить с участием специалиста в лабораторных условиях или на рабочем месте следователя.

Следует обращать внимание на поиск так называемых «скрытых» файлов и архивов, где может храниться важная информация.

Периферийные устройства ввода-вывода могут также некоторое время сохранять фрагменты программного обеспечения и информации, однако для вывода этой информации необходимы глубокие специальные познания.

Осмотр компьютеров и изъятие информации производится в присутствии понятых, которые расписываются на распечатках информации, изготовленных в ходе осмотра.

В ходе осмотров по делам данной категории могут быть обнаружены и изъяты следующие виды важных документов, которые могут стать вещественными доказательствами по делу:

- а) документы, носящие следы совершенного преступления, – телефонные счета, пароли и коды доступа, дневники связи и пр.;
- б) документы со следами действия аппаратуры. Всегда следует искать в устройствах вывода (например, в принтерах) бумажные носители информации, которые могли остаться внутри их в результате сбоя в работе устройства;
- в) документы, описывающие аппаратуру и программное обеспечение;
- г) документы, устанавливающие правила работы с ЭВМ, нормативные акты, регламентирующие правила работы с данной ЭВМ, системой, сетью, доказывающие, что злоумышленник их знал и умышленно нарушал;
- д) личные документы подозреваемого или обвиняемого¹.

Комплекс неотложных следственных действий обязательных для первоначального этапа расследования также включает:

1. Проведение обыска в служебном помещении, на рабочем месте подозреваемого с целью обнаружения и изъятия физических носителей

¹ Филиппов А.Г. Криминалистика: учеб. пособие / А.Г. Филиппов. М.: Высшее образование, 2007. С. 154–156.

компьютерной информации и других документов, имеющих или возможно имеющих отношение к несанкционированному использованию программного обеспечения или носящих иные следы подготовки к преступлению.

2. Назначение и производство компьютерно-технических экспертиз, которые, в свою очередь, подразделяются на следующие виды:

- аппаратно-компьютерные, где предметом исследования являются факты и обстоятельства, устанавливаемые на основе исследования закономерностей эксплуатации аппаратных средств компьютерной системы – материальных носителей информации о факте или событии гражданского либо уголовного дела;

- программно-компьютерные, где предметом исследования являются закономерности разработки и применения программного обеспечения компьютерной системы;

- информационно-компьютерная (экспертиза данных), она является ключевым видом судебных компьютерно-технических экспертиз, которая позволяет осуществить поиск, обнаружение, анализ и оценку информации, подготовленной пользователем или созданной программами для организации информационных процессов в компьютерной системе;

- компьютерно-сетевая экспертиза. Она позволяет исследовать функциональное предназначение компьютерных средств, реализующих какую-либо сетевую информационную технологию¹.

Вышеперечисленные виды экспертиз целесообразно производить с привлечением специалистов правоохранительных органов, специалистов в области средств компьютерной техники, специалистов по обеспечению безопасности информации в сфере телекоммуникаций и компьютерных системах.

Результаты компьютерно-технической экспертизы должны быть оформлены в виде заключения эксперта, которые в дальнейшем можно

¹ Россинская Е.Р. Судебная экспертиза в гражданском, административном и уголовном процессе. М.: Норма, 2005. С. 458–467.

использовать в виде доказательств в ходе предварительного расследования и судебного исследования, и разрешения уголовных дел по существу. В настоящее время с помощью таких экспертиз могут решаться задачи идентификационного и диагностического характера, например:

1. Относится ли изъятое устройство к аппаратным компьютерным средствам.

2. Восстановление информации, ранее содержавшейся на физических носителях и впоследствии стертой или измененной по различным причинам.

3. Установление времени ввода, изменения, уничтожения либо копирования той или иной информации.

4. Расшифровка закодированной информации, подбор паролей и раскрытие систем защиты.

5. Установление авторства, места, средств подготовки и способа изготовления документов (файлов, программ).

6. Выяснение возможных каналов утечки информации из компьютерной сети и помещений.

7. Установление уровня профессиональной подготовки отдельных лиц, проходящих по делу в области программирования и в качестве пользователя.

8. Наличие какой-либо информации о проведении электронных платежей и использовании кодов кредитных карт.

9. Воспроизведение и распечатка всей или части информации, содержащейся на физических носителях. В том числе, находящейся в нетекстовой форме.

Таким образом, рассматривая типичные следственные ситуации, встречающиеся в ходе расследования преступлений в сфере телекоммуникаций и компьютерной информации, наиболее часто приходится проводить следующие следственные действия:

- контроль и запись переговоров
- следственный осмотр;
- допрос (свидетеля, потерпевшего, обвиняемого, подозреваемого,

эксперта, специалиста);

- обыск;

- выемка;

- назначение и производство судебных информационно-технических экспертиз;

- следственный эксперимент.

Для выявления противоправности действий преступника и поиска следов преступлений, совершаемых в сфере телекоммуникаций и компьютерной информации требуется эксперт, обладающий опытом и знаниями в области электронной техники и информационных технологий никак не меньшими, чем сам преступник. Без грамотного экспертного заключения привлечение лица к уголовной ответственности, даже при наличии признаков состава преступления, становится проблематичным.

4. Расследование и раскрытие компьютерных преступлений: проблемы и пути совершенствования

4.1. Структура и состояние компьютерной преступности в Российской Федерации

В настоящее время одной из проблем развития Российского государства и общества является существование компьютерной преступности, причиняющей колоссальный вред политическим, социально-экономическим, научно-техническим, культурным и информационным отношениям. В связи с этим все более актуальным становится вопрос о защите физических и юридических лиц от неправомерного доступа к компьютерной информации, вредоносных компьютерных программ и иных угроз.

Анализ нормативных, научных и иных источников показывает, что для иллюстрации структуры компьютерной преступности в России лучше использовать классификацию и статистику совершенных преступлений, формируемую информационными центрами правоохранительных органов (МВД России). Это связано с тем, что существующая методика учета зарегистрированных преступлений, расследованных, приостановленных и прекращенных уголовных дел уже проверена временем и складывается из ежедневно поступающих данных от территориальных органов ФСБ России, СК России, МВД России, а также из служебных отчетов, докладных записок, информационных писем, обзоров (квартальных, полугодовых, годовых).

Правоохранительные органы обладают большим объемом аналитической информации о структуре и масштабе компьютерной преступности в России, чем экспертное или научное сообщество, что не умаляет значение последних в исследовании данного криминального явления.

Исследуя официальную статистику МВД России, а также аналитические материалы компаний, занимающихся информационной безопасностью и разработкой антивирусного программного обеспечения, можно увидеть

следующую картину российской компьютерной преступности, характеризующую ее состояние.

В 2015 году на территории Российской Федерации были возбуждены следующие уголовные дела по выявленным фактам совершения компьютерных преступлений:

- за неправомерный доступ к компьютерной информации (ст. 272 УК РФ) – 1 396;
- создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) – 974;
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) – 12.

Согласно официальной статистике, динамика выявления преступлений в сфере компьютерной информации носит регрессивный характер, т.е. количество зарегистрированных, и следовательно, расследованных и направленных в суд уголовных дел из года в год неуклонно снижается.

По данным ГИАЦ МВД России, общее количество выявленных преступлений в сфере компьютерной информации, предусмотренных ст. 272, ст. 273 и ст. 274 УК РФ составило:

- в 2009 г. соответственно 9 489, 2097 и 4;
- в 2010 г. – 6 132, 1 010 и 0;
- в 2011 г. – 2 005, 693 и 0;
- в 2012 г. – 1 930, 889 и 1;
- в 2013 г. – 1 799, 764 и 0;
- в 2014 г. – 1 151, 585 и 3;
- в 2015 г. – 1396, 974 и 12.

Таким образом, за анализируемый период количество выявленных преступлений в сфере компьютерной информации сократилось почти в 5 с (11 590 до 2 382). Количество преступлений, квалифицируемых по ст. 274 УК РФ,

как мы видим, является незначительным и в целом не влияет на общую картину компьютерной преступности в России¹.

При этом необходимо отметить серьезные проблемы не только в выявлении преступлений в сфере компьютерной информации, но и в деятельности органов дознания и предварительного следствия при расследовании данной категории дел. Например, статистика расследованных уголовных дел, возбужденных по признакам преступлений, предусмотренных ст. 273 УК РФ, показывает, что по реабилитирующим основаниям прекращены: в 2009 г. – 50, в 2010 г. – 35, в 2011 г. – 78, в 2012 г. – 163 уголовных дела; «приостановлены за нерозыском лица либо в случае неустановления лица, совершившего преступление»: в 2010 г. – 58, в 2011 г. – 75, в 2012 г. – 108, в 2013 г. – 106, в 2014 г. – 119, в 2015 г. – 193 уголовных дела.

В 2010 году из находившихся в производстве по ст. 273 УК РФ 1 066 уголовных дел в суд направлено 914, в 2011 году из 754 уголовных дел в суд направлено 558, в 2012 году из 953 уголовных дел в суд направлено только 664, в 2013 году из 860 уголовных дел в суд направлено 575, в 2014 году из 665 уголовных дел в суд направлено 344, в 2015 году из 974 уголовных дел в суд направлено 369.

Около 20% зарегистрированных уголовных дел прекращается либо приостанавливается на стадии предварительного следствия (дознания), в суд направляется немногим более 50% уголовных дел².

В частности, профессор В.Б. Вехов еще 2004 году указывал, что «...с определенной долей успеха расследуется лишь около 49% выявленных «компьютерных» преступлений, обвинительные приговоры выносятся в 25,5 % случаев от общего числа возбужденных уголовных дел, а средний показатель количества уголовных дел, по которым производство приостановлено, составляет 43,5%. Все это закономерные последствия явно недостаточного уровня профессионализма сотрудников правоохранительных органов в

¹ Платов А.А. Состояние преступности в сфере компьютерной информации // Центральный научный вестник. 2018. № 3. С. 23–24.

² Номоконов В.А., Тропина Т.Л. Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. 2013. № 5. С. 148–160.

деятельности по раскрытию, расследованию и предупреждению преступлений указанного вида».

Можно сделать вывод о том, что в ближайшие годы мы сможем наблюдать рост количества зарегистрированных преступлений, предусмотренных ст.ст. 272 и 273 УК РФ, но процент их раскрываемости, и соответственно количество лиц, привлеченных к уголовной ответственности, будет снижаться. Этому способствует несовершенство уголовного законодательства, недостатки и ошибки в судебно-следственной практике, отсутствие в правоохранительных органах необходимого количества высококвалифицированных специалистов для раскрытия компьютерных преступлений.

4.2. Современные проблемы расследования и раскрытия преступлений в сфере компьютерной информации и пути их решения

Для нашей страны рассматриваемый вид противоправных деяний является сравнительно новым, о чем может свидетельствовать сравнительно-правовой анализ действующих в этой сфере нормативно-правовых актов. Если в США на сегодняшний день действует более 2000 законов и подзаконных актов, касающихся компьютерных преступлений и связанных с ними явлений (аналогичные нормы действуют в ФРГ, Великобритании и Франции), то в России их число крайне невелико.

Вызывает озабоченность тот факт, что в последнее время противоправная деятельность в сфере информационных технологий стала глобальной международной проблемой, о чём свидетельствуют практически ежедневные сообщения СМИ на данную тему. Среди недавних, наиболее известных информационных инцидентов можно выделить: в мае 2017 г. - компьютерные системы в более чем 150 странах мира поразил вирус-шифровальщик под названием WannaCry. На экране зараженных компьютеров появлялось сообщение о том, что все файлы зашифрованы, а за расшифровку пользователю

предлагалось выплатить эквивалент \$300 в биткоинах. По некоторым оценкам кибератака с использованием вируса WannaCry привела ущербу свыше миллиарда долларов; в июне 2017 г. - компьютерные системы по всему миру были атакованы вирусом Petya. Сильнее всего пострадала Украина, там кибератака парализовала работу сайтов правительства, банков, энергетических и транспортных компаний. В России вирус атаковал компьютерные системы «Роснефти» и «Башнефти». В конце июня вирус-шифровальщик Petya, распространился на компьютерные системы в Европе, США, стран Азии¹.

Формирование полноценной методики расследования преступлений в сфере компьютерной информации является важнейшей задачей криминалистической науки на современном этапе ее развития. В настоящее время перед правоохранительными органами при расследовании компьютерных преступлений возникает ряд серьезных проблем таких как: сложность в установлении факта совершения компьютерного преступления и решения вопроса о возбуждении уголовного дела; сложность в подготовке и проведении отдельных следственных действий; особенности выбора и назначения необходимых судебных экспертиз; несовершенство методики расследования компьютерных преступлений.

По оценке отечественных и зарубежных исследователей, решение проблем раскрытия и расследования данного вида преступлений представляет собой задачу более сложную, чем задачи, связанные с их предупреждением. О формировании полноценных методик по раскрытию, расследованию и предупреждению преступлений в сфере компьютерной информации всерьез заговорили в 2013 г., когда в г. Москве состоялся 15-й Национальный форум информационной безопасности «Инфофорум».

Данное мероприятие традиционно проводилось при поддержке Совета Безопасности РФ, Комитета по безопасности и противодействию коррупции Государственной Думы РФ, МИД России, ФСБ России и многих других

¹ Гончар В.В. Совершенствование расследования преступлений в сфере информационных технологий // Эпоха науки. 2017. № 1. С. 28.

федеральных, региональных ведомств и является площадкой для обсуждения широкого спектра проблем обеспечения информационной безопасности, на которой вырабатываются предложения по формированию государственной политики в этой сфере и анализируется практика правоприменения. Ежегодно в ходе работы данного форума особое внимание уделяется статистическим данным, связанным с выявлением и предотвращением компьютерных преступлений.¹

В связи с развитием компьютерной техники, информационных сетей и технологий перед отечественными правоохранительными органами все острее стоит вопрос о выработке наиболее эффективной практической методики расследования преступлений в сфере компьютерной информации.

Раскрытие компьютерных преступлений – это в основном нетрадиционная и порой дискуссионная проблема – как по причине сложности самого факта доказывания, так и в силу несовершенства действующего законодательства. Определенные проблемы в борьбе с преступлениями в сфере высоких технологий вызывают следующие обстоятельства.

В первую очередь это высокий уровень латентности указанной группы преступлений. Здесь основной причиной является отсутствие видимых материальных следов приготовления и совершения преступлений.

Следующее обстоятельство – разнообразие способов совершения данных преступлений. Вызывают также определенные трудности определение самого события преступления, включающего в себя место и время его совершения. Здесь мест совершения преступлений может быть несколько, при этом располагаться они могут, на разных территориях. Их границы, в свою очередь, могут находиться на значительном расстоянии друг от друга.

С учетом специфики средств совершения данных преступлений (то есть, компьютерной техники) их следы представляют собой совокупность материально фиксированных, или классических «трассологических», следов

¹ Зверьянская Л.П., Протасевич А.А. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2013. № 11. С. 45–47.

(отпечатки пальцев на клавиатуре, элементах системного блока, модеме, всевозможные микроследы на этих же объектах и т.д.) и, так называемых, виртуальных следов, то есть следов на магнитных носителях, указывающих на время работы подозреваемого с ЭВМ, на время осуществления удаленного доступа (работы в сети «Интернет», например), на объем полученной информации с других компьютеров и серверов, и, непосредственно, сама полученная информация и прочее¹.

В литературе под виртуальными следами понимают любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации. Данные следы занимают условно промежуточную позицию между материальными и идеальными следами. Особенную сложность для сотрудников правоохранительных органов представляет работа именно со второй группой следов. «Виртуальные следы», по сути дела, это компьютерная информация, которая находится в файлах. При расследовании компьютерных преступлений всегда важно учитывать, что следы, указывающие на то, что подозреваемый работал на каком-то конкретном компьютере, не имеют практически никакой ценности. Причиной этому служит тот факт, что нередко орудием рассматриваемых преступлений является домашний или служебный компьютер подозреваемого, который используется им постоянно. Более важными являются те особенности обнаруженных следов, которые могут дать информацию о времени работы подозреваемого с компьютером. Необходимо соотнести полученные данные с информацией из виртуальных следов².

На практике серьезные проблемы может вызывать обнаружение, изъятие и фиксация материально фиксированных следов. Это связано с тем, что в большинстве случаев одним персональным компьютером может пользоваться неограниченное число пользователей. Это обстоятельство является причиной

¹ Мошкин С.В. Типичные следственные ситуации на первоначальном этапе расследования преступлений в сфере компьютерной информации // Ретроспективы и перспективы права. 2013. № 5. С. 48–50.

² Нагорный А.А. Криминологические особенности преступлений в сфере компьютерной информации // Законность и правопорядок в современном обществе: сборник материалов XV Международной научно-практической конференции. Новосибирск. 2013. С. 216–223.

того, что на различных частях компьютера можно обнаружить большое количество отпечатков пальцев, принадлежащих нескольким людям. Как правило, они нечеткие из-за неоднократного нажатия одних и тех же клавиш на клавиатуре, кнопок на системном блоке, постоянного использования манипуляторов («мышей», «трэк-болов» и т.д.). Следовоспринимающими объектами для материально фиксированных следов обычно являются:

1) клавиатура (устройство для ввода текстовой и цифровой информации): на ней обследованию подлежат клавиши (для выявления потожировых отпечатков пальцев), четкие отдельные отпечатки возможно обнаружить на редко используемых клавишах («Num Lock», «Caps Lock», «Scroll Lock», F1 – F12, специальных клавишах на последних моделях клавиатур: «Search», «Files» и т.д.; помимо клавиш необходимо обратить внимание на подставку под ладони (если таковая имеется) на предмет выявления четких потожировых отпечатков ладоней, на разъем, вставляемый в соответствующий порт системного блока; немаловажно обратить внимание на слой пыли на клавиатуре; некоторые микроследы возможно обнаружить под клавишами;

2) манипулятор «мышь»: осматривается на предмет обнаружения отпечатков пальцев и ладоней, также следует обратить внимание на разъем;

3) монитор: потожировые следы на кнопках управления монитором, в иных местах;

4) системный блок: необходимо осмотреть все кнопки, включая кнопки дисководов и CD (DVD)-ROM привода; обратить внимание на отпечатки пальцев в районе задней панели со «входами» («портами»), на наличие скрепляющих системный блок с наружным кожухом болтов;

5) отдельные элементы системного блока: внутри системного блока необходимо обратить внимание на внутренний модем (если он там присутствует), выявить: не подключался ли к данному компьютеру в недавнее время дополнительный «винчестер», о чем может говорить неподключенный к шлейфу CD(DVD)-ROM привод или свежие отпечатки на дополнительном

разъеме шлейфа (если он есть), к которому мог быть подключен дополнительный «винчестер».

б) принтер, сканер, модем, «хаб» и т.д.: на этих устройствах также могут быть обнаружены отпечатки пальцев, микроследы, в принтере могут быть обнаружены так называемые «зажеванные» листы бумаги с текстом, который так или иначе может касаться обстоятельств дела¹.

Также вызывает затруднение определения времени совершения преступлений. Например, вредоносная программа может начать действовать, пока не наступит определенное в ее алгоритме событие. Негативным обстоятельством для данных преступлений является легкость уничтожения следов подготовки и совершения преступлений. Компьютерная информация может выступать как носитель следов преступления, либо быть следами совершенных преступлений.

Характеризуя следы рассматриваемых, сравнительно новых в практике криминалистики преступлений, необходимо отметить, что в настоящее время среди ученых не сложилось единого мнения в определении их понятия и сущности. Традиционно, в частной криминалистической теории следообразования, считается, что следами преступления являются любые изменения среды, возникшие в результате совершения в этой среде преступления. При этом все следы преступления, согласно данной теории, классифицируются на материальные и идеальные. К первым, обычно относятся «отпечатки» события на любых материальных объектах: предметах, документах, теле потерпевшего и т. д. Под идеальными следами понимают отпечатки события в сознании, памяти преступника, потерпевшего, свидетелей и других людей. Анализ особенностей формирования следовой картины при совершении преступления в сфере компьютерной информации показывает, что данные следы не вписываются в вышеуказанную классификацию следов.

¹ Алымов Д.В., Шереметова А.А. Методика расследования преступления в сфере компьютерной информации: сравнительный анализ отечественного и зарубежного опыта // Конф. УПК РФ 15 лет правоприменения. Курск. 2016. С. 182–186.

В настоящее время ряд ученых (В. А. Мещеряков и др.), пришли к выводу, о необходимости введения понятия «виртуальные следы», как промежуточных в классификации между материальными и идеальными следами.

В связи с изложенным, следует констатировать, что в настоящее время возникла необходимости пересмотра в этом отношении, частной криминалистической теории следообразования. При раскрытии и расследовании преступлений в сфере компьютерной информации данные следы имеют решающее значение, поскольку зачастую являются единственными и играют важную роль в диагностических исследованиях, позволяющих восстановить механизм совершения преступления.

Как показывает практика, наиболее сложные преступления в сфере компьютерной информации совершаются с использованием возможностей, предоставляемых глобальными сетями передачи данных. Поэтому при раскрытии и расследовании этих преступлений исследуются следы, которые создаются не только в технических (оконечных) устройствах пользователя, но формируются в результате прохождения информации по самим техническим каналам связи. Информация передается, как правило, пакетами, каждый из которых состоит из двух частей: заголовка (служебная информация, определяющая в том числе маршрут передачи) и непосредственно передаваемых данных (содержательная часть).

Для решения задач раскрытия и расследования преступлений основной интерес, несомненно, представляет доступ к содержательной части сообщений, передаваемых с определенного адреса и потенциально включающих сведения о преступной деятельности, однако часто большую ценность может представлять служебная часть сообщений, несущая в себе информацию о месте нахождения преступника. Если рассматривать следы, образуемые в технических каналах связи, то обычно они представляют собой сведения о сообщениях, передаваемых по данным сетям, которые содержатся в техническом оборудовании оператора связи, и аккумулируются в специальных файлах

регистрации, так называемых «Log-файлах». Например, в этих Log-файлах могут находиться данные о том, кто инициировал данное сообщение, когда и в какое время оно произошло и какие файлы затронуло. По существу в них протоколируется техническая информация, содержащая данные об информационно-технологических процессах обработки информации и представления ее потребителю.

При этом обычно выделяют две основных категории «служебных данных»: данные о пользователе и сведения о сообщении. Их анализ показывает, что они зачастую имеют разное доказательственное значение в раскрытии и расследовании рассматриваемых преступлений. Например, данные о пользователе могут включать в себя сведения о имени, адресе, дате рождения, номере телефона, адресе поставщика услуг в Интернет, адресе электронной почты, о номере или счете, используемого для осуществления платежных операций по расчетам за услуги провайдера, справочных данных, данных юридического лица, перечне предоставляемых услуг, на которые подписался клиент, IP-адресе, предыдущем IP-адресе пользователя, дополнительном адресе электронной почты и т. д. Тогда как сведения о сообщении содержат уже качественно иную информацию. Это могут быть данные первоначального номера телефона, используемого при регистрации; даты сеанса связи; информации о времени связи; статических или динамических IP-адресах и соответствующих телефонных номерах; скорости передачи сообщения; исходящих журналов сеансов связи, включающих тип использованных протоколов, самих протоколов и т. д.

Как указывалось ранее, для решения задач раскрытия и расследования преступлений, кроме следов оставляемых служебной частью сообщений, рассмотренных выше, особое значение представляют следы преступлений, имеющиеся в содержательной части этих сообщений. Например, файлы, содержащие тексты документов, фотоизображения, видео- и аудио-фрагменты, программное обеспечение и т. п.

Все рассмотренные объекты в свою очередь могут:

- а) быть орудиями преступлений (программное обеспечение);
- б) сохранять следы преступления (журналы регистрации событий в компьютерной системе);
- в) содержать информацию, запрещенную законом к распространению;
- г) относиться к иным объектам, имеющим доказательственное значение (файлы электронной переписки, интернет-адреса посещенных сайтов и т. д.).

Так как до настоящего времени на законодательном уровне вопросы хранения провайдерами вышеуказанных объектов компьютерной информации были не закреплены, то каждый из них регулировал эту деятельность самостоятельно. Практика показывает, что операторы, являющиеся собственниками указанных сведений, обычно оптимизируют их по своему усмотрению и сохраняют лишь для обеспечения контроля поступающих за эти услуги платежей. Из-за разнообразия услуг, предоставляемых компаниями, и связанных с ними разнообразных данных, которые могут быть доступными для сохранения, весьма трудно выделить те из них, которые каждое частное лицо или поставщик услуг должны сохранять. При этом форматы и объемы этих данных в регистрационных файлах напрямую зависят от технических возможностей самого оператора связи. Высокая конкуренция и сложная экономическая обстановка заставляет их сокращать свои расходы, в частности, и на хранение вышеуказанных данных, что неблагоприятно влияет на раскрытие и расследование преступлений в сфере компьютерной информации.

Как указывалось выше, уголовные дела по данным преступлениям в основном возбуждаются либо по сведениям, полученным в ходе осуществления ОРД, либо по факту уже совершенного преступления.

Так как расследование преступления по факту его совершения носит ретроспективный характер и в основном производится через сравнительно длительное время после его совершения, то возможность восстановления следователем механизма его совершения и получения при этом доказательств, ввиду не сохранения провайдером вышеуказанных следов, является ничтожной.

Аналогичные сложности возникают у следователя и при расследовании преступлений, возбужденных по данным, полученным в ходе осуществления ОРД. Например, оперативные сотрудники, работая в реальном времени, задокументировали преступную деятельность разрабатываемых лиц, но так как по сложным преступлениям их оперативная разработка осуществляется достаточно продолжительный период времени, то эти данные могут быть не сохранены провайдером и поэтому в ходе проведения уже процессуальных следственных действий не могут быть получены в качестве доказательств по уголовному делу.

Относительно данных случаев судебная практика показывает, что суды в качестве доказательств по уголовным делам не всегда признают копию, даже соответствующим образом документированной компьютерной информации, в данном случае оперативными подразделениями.

В настоящее время предпринята попытка разрешения данной проблемы в связи с принятием дополнений в Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (в ред. Федерального закона от 06.07.2016 № 374-ФЗ), где в ст. 64 «Обязанности операторов связи и ограничение прав пользователей услугами связи при проведении оперативно-розыскных мероприятий, мероприятий по обеспечению безопасности Российской Федерации и осуществлении следственных действий» введена новелла о том, что операторы связи, обязаны хранить информацию о фактах приема, передачи, доставки и обработки голосовой информации, текстовых сообщений, изображений, звуков, видео - или иных сообщений пользователей услугами связи – в течение трех лет¹.

Из содержания данной нормы следует предположить, что «информация о фактах» – это, по сути, так называемые Log-файлы, рассматриваемые выше и характеризующие следы, оставляемые служебной частью сообщений образуемых в технических каналах связи. В отношении информации, находящейся в содержательной части этих сообщений – текстовых сообщений, голосовой информации, изображений, звуков, видео-, иных сообщений

¹ О связи: федер. закон от 07.07.2003 № 126-ФЗ // Российская газета. 2003. № 3249.

пользователей услугами связи – законодателем установлен срок их хранения до шести месяцев.

Представляется, что в данном правовом акте заинтересованным компетентным органам необходимо разрешить следующие проблемные вопросы, рассмотренные выше:

- о единых стандартах сведений о сообщениях, подлежащих хранению, передаваемых по техническим каналам связи;
- разработать единые требования к объему и номенклатуре, подлежащей обязательному сохранению компьютерной информации;
- определить окончательный срок ее хранения;
- установить порядок ее документирования и передачи правоохранительным органам;
- разработать правила и порядок их уничтожения при отсутствии надобности¹.

Также, проблема расследования преступлений в сфере компьютерной информации связана с потребностью дополнительной квалификации специалистов, ведущих расследование по делам данной категории. Это объясняется отсутствием традиции обучения юристов высокотехнологичным дисциплинам. Здесь усматривается необходимость решения вопроса о специализации тех, кто желает заниматься расследованиями компьютерных преступлений, а также повышать квалификацию работающих специалистов либо отправлять их на дополнительное техническое обучение. Можно отметить и отсутствие разработанных методик по проведению тех или иных компьютерных экспертиз, а также нехватки высококвалифицированных специалистов.

Это, безусловно, связано, в–первую очередь, с отставанием более консервативной юриспруденции от стремительно развивающейся инженерии. Специалисты не появятся сами по себе, их необходимо готовить, а для

¹ Потапов С.А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические процессы и явления. 2016. № 10. С. 91–94.

правовой сферы специально и постоянно. Кроме того, необходимо совершенствовать квалификацию уже работающих специалистов. Только тогда, когда компьютер будет рассматриваться как заурядный бытовой прибор, понятный каждому, острота проблемы будет частично снята.

Правильно отмечается особая сложность обнаружения, фиксации и изъятия компьютерной информации при производстве следственных действий.

По вопросу обучения и повышения квалификации специалистов можно предложить следующее. Необходимо организовать постоянное (ежегодное) обучение специалистов, работающих по направлениям, связанным с расследованием преступлений, совершаемых с применением высоких информационных технологий. Требования к знаниям, изложенные в государственном образовательном стандарте (современные информационные технологии; аппаратные и программные средства персональной ЭВМ в локальных и глобальных вычислительных сетях; операционные системы, их функциональные возможности и области применения в юриспруденции; Интернет; операции с базами данных законодательства; основные принципы алгоритмизации, программирования и моделирования юридических ситуаций; роль математических методов и вычислительной техники в различных видах юридической деятельности и в функционировании правовых систем различных регионов мира; управление в социальных и экономических системах; символическая логика; правовое регулирование общих вопросов реализации государственных программ, управления в социальной и экономической сферах в правовых системах различных регионов мира), вполне соответствуют представлениям о специалистах процитированных авторов и являются достаточными для увеличения самостоятельности следователя в ходе расследования преступлений в сфере компьютерной информации¹.

Такой уровень подготовки будет способствовать развитию научных исследований, решению методических и терминологических вопросов. Также

¹ Вехов В. Б. Основные направления использования компьютерных технологий для обучения сотрудников правоохранительных органов // Вестник Волгоградской академии МВД России. 2009. № 2. С. 114–117.

для решения отдельных процессуальных вопросов в ходе расследования компьютерных преступлений рекомендуется доработать методики подготовки специалистов по предметам «Уголовный процесс» и «Криминалистика».

Таким образом, были проанализированы лишь некоторые проблемы, связанные с раскрытием, расследованием и предупреждением компьютерных преступлений. Для эффективной борьбы с киберпреступностью необходимо создать полноценную криминалистическую методику, отвечающую современным достижениям науки и техники. Безусловно, ученые и практические работники еще не раз столкнутся с трудностями теоретико-практического характера, поскольку киберпреступность в нашей стране и зарубежных странах растет очень быстрыми темпами. Существенно видоизменяется и характер преступных действий, появляются новые объекты криминалистического исследования, а также используются новейшие технические средства, применяемые для получения криминалистически значимой информации о преступлении рассматриваемого вида. Необходимо объединить отечественный и зарубежный опыт борьбы с киберпреступностью, выработав общую линию поведения и научно-практические рекомендации по противодействию исследуемым социально-опасным явлениям¹.

4.3. Международное сотрудничество как основной фактор совершенствования методик расследования и раскрытия компьютерных преступлений

Развитие информационных и коммуникационных технологий (ИКТ) играет важнейшую роль для экономического и социально-политического развития как каждой страны в отдельности, так и человечества в целом. Однако развитие ИКТ не только создает возможности для роста и развития, но и порождает угрозы международной и национальной безопасности.

¹ Ефремов К.А. О некоторых аспектах расследования преступлений в сфере компьютерной информации // Вестник Волгоградской Академии МВД России. 2015. № 2. С. 83 – 84.

Межгосударственное противоборство, перешедшее в информационную сферу, чревато конфликтами, крайней формой проявления которых могут стать информационные войны. В последние годы существенно увеличилось количество деструктивных информационных атак, совершаемых с использованием современных информационно-коммуникационных технологий, причем подобные атаки становятся все сложнее. В ближайшей перспективе объектами их воздействия будут не только информационные ресурсы в сети Интернет, но и критически важные объекты инфраструктуры государств, обеспечивающие функционирование промышленности, транспорта, энергетики и других сфер жизнедеятельности¹.

Актуальные проблемы организации международного сотрудничества стран СНГ в борьбе с киберпреступностью, преступностью в сфере информационно-коммуникационных технологий, включая компьютерную информацию, возникают по мере реализации планов расширения возможностей и границ цифрового пространства СНГ.

Стратегия сотрудничества государств - участников СНГ в построении и развитии информационного общества на период до 2025 г. и План действий по ее реализации, которые были утверждены на заседании Совета Глав Правительств СНГ в Минске 28.10.2016 г., являются новыми векторами интеграционного сотрудничества стран СНГ. Эти векторы идут в контексте международных тенденций развития и обеспечения безопасности информационно-коммуникационных технологий в ЕС, США, КНР и других странах².

Основы противодействия преступности в сфере ИКТ стран СНГ заложены Соглашением о сотрудничестве государств - участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 г. Это Соглашение до сих пор является базовым документом для разработки и реализации совместных программ и планов противодействия преступлениям,

¹ Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности // Право и управление. XXI век. 2014. № 4. С. 44.

² Булай Ю.Г., Булай Р.И. Профилактика и противодействие киберпреступности, а также международным киберугрозам // Академическая мысль. 2017. № 1. С. 31–35.

совершаемым с использованием информационных технологий, для сотрудничества с международными организациями в борьбе с преступлениями, совершаемыми с использованием информационных технологий.

После того, как были приняты Стратегия сотрудничества государств - участников СНГ в построении и развитии информационного общества на период до 2025 г. и План действий по ее реализации, которые были утверждены на заседании Совета Глав Правительств СНГ в Минске 28.10.2016 г., появилась система мер межгосударственной защиты безопасности ИКТ для стран СНГ. Однако в определенной степени опасности и риски совершения преступлений в сфере компьютерных технологий усилились, поскольку нормативно-правовая база предупреждения, выявления и борьбы с преступлениями в этой сфере не успевает за развитием новых форм кибератак.

ООН и региональными международными организациями рост транснациональной преступности в сфере компьютерных технологий рассматривается в качестве угрозы информационной безопасности для всех стран мира. В связи с этим анализ существующих правовых и институциональных инструментов, которыми располагает СНГ в рассматриваемой области, является актуальным¹.

Стратегия 2016 г. дополнена Планом действий по ее реализации, содержащим более 50 мероприятий, направленных на создание благоприятной среды для развития и укрепления сотрудничества в области ИКТ, гармонизацию законодательства и нормативно-технической базы, развитие цифровой экономики и «промышленного интернета», разработку и внедрение конкретных проектов в рамках актуальных направлений ИКТ (электронное правительство, электронная торговля, электронная наука, электронное здравоохранение, электронное обучение, электронная культура).

В последние годы возросло количество правонарушений в сфере информационных технологий и компьютерной информации, что повлекло

¹ Демидов О.В. Обеспечение международной информационной безопасности и российский национальные интересы // Индекс безопасности. 2013. №1. С. 129–168

создание в рамках СНГ правовых и организационных механизмов противодействия преступлениям в этой сфере.

В рамках СНГ был принят ряд соглашений по усилению межгосударственного сотрудничества в борьбе с преступлениями в сфере информационных цифровых технологий. Договорно-правовое сотрудничество в борьбе с преступностью в сфере информационных технологий в рамках СНГ базируется на ранее принятой международно-правовой базе и на новых документах межгосударственного сотрудничества. Между государствами - участниками Евразийского экономического союза, странами СНГ, другими государствами заключены двусторонние соглашения о полицейском сотрудничестве в целом или по отдельным направлениям оперативно-служебной деятельности, а также о сотрудничестве органов внутренних дел приграничных государств. И здесь хочется отметить положительный опыт сотрудничества, как в рамках СНГ, так и применительно к сотрудничеству с отдельными государствами. Например, Российской Федерации с Азербайджанской Республикой, Республикой Армения, Республикой Беларусь, Республикой Казахстан, Кыргызской Республикой, Республикой Таджикистан и др¹.

Западные страны – партнеры по НАТО также обеспокоены ростом киберпреступности в глобальном масштабе. На Мюнхенской конференции по безопасности стран – членов НАТО 17–19 февраля 2017 г. одним из ключевых вопросов был вопрос о борьбе с международной киберпреступностью в информационном пространстве. Россия неоднократно предлагала в рамках ООН выстраивать сотрудничество государств в сфере обеспечения международной информационной безопасности и борьбы с киберпреступностью. Инициативы России заложили основу соответствующих резолюций к вопросам кибербезопасности в профессиональном, техническом и технологическом смыслах.

¹ Ступаков В.И. Перспективы сотрудничества евразийских государств в развитии информационного общества: новые векторы сотрудничества стран СНГ, БРИКС в сфере информационных и коммуникационных технологий (ИКТ) // Международное сотрудничество евразийских государств: политика, экономика, право. 2016. № 3. С. 57–69.

Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 г. устанавливает основные определения, а также юридические основания привлечения к уголовно-правовой ответственности в регулируемой сфере, включая:

1) основания применения уголовного наказания за преступления в сфере компьютерной информации, предметом которых являются неправомерные посягательства на компьютерную информацию;

2) определение компьютерной информации как предмета посягательства, выраженного информацией, находящейся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающейся по каналам связи;

3) понятие вредоносной программы как одного из способов совершения преступления, означающей созданную или существующую программу со специально внесенными изменениями, заведомо приводящими к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети;

4) определение неправомерного доступа как способа совершения преступления через несанкционированное обращение к компьютерной информации.

Содержание международного сотрудничества по борьбе с преступностью представляет собой целенаправленную активную деятельность различных государств, субъектов международных отношений и уголовной политики, которые объединяют усилия, ресурсы для защиты интересов от международной и национальной преступности. Эта деятельность осуществляется путем совместной разработки и реализации обозначенных межгосударственными документами целей и задач сотрудничества правоохранительных органов государств в борьбе с национальной и транснациональной преступностью.

Статья 3 «Соглашения о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации» от 01.06.2001 г. определяет, что государства – участники СНГ признают в соответствии с национальным законодательством в качестве уголовно наказуемых следующие деяния, если они совершены умышленно:

а) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред или тяжкие последствия;

г) незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб. Определения понятий «существенный вред», «тяжкие последствия» и «существенный ущерб» относятся к компетенции государств СНГ¹.

Концепция и Программа сотрудничества государств – участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий Решением Совета глав государств Содружества Независимых Государств от 25.10.2013 г. в Минске одобрена Концепция сотрудничества государств – участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий. Основными направлениями сотрудничества государств – участников СНГ в борьбе с

¹ Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (заключено в г. Минске 01.06.2001) // URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=9210#09638639701102296> (Дата обращения 10.05.18).

преступлениями, совершаемыми с использованием информационных технологий, являются:

1) совершенствование договорно-правовой базы сотрудничества в борьбе с преступлениями, совершаемыми с использованием информационных технологий;

2) осуществление согласованных мер для выполнения положений международных нормативных правовых документов, направленных на борьбу с преступлениями, совершаемыми с использованием информационных технологий;

3) оказание взаимной консультативной помощи в разработке национальной системы мер противодействия преступлениям, совершаемым с использованием информационных технологий;

4) оказание содействия при осуществлении следственных действий, оперативно-разыскных и иных мероприятий, в том числе по взаимодействию с операторами электрической связи на территориях государств – участников СНГ;

5) обмен опытом работы по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений, совершаемых с использованием информационных технологий, проведение совместных семинаров, учений, сборов, консультаций и совещаний;

6) оценка эффективности совместных усилий, предпринимаемых компетентными органами государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий, внедрение положительного опыта в практику их деятельности;

7) подготовка, переподготовка и повышение квалификации кадров, участвующих в противодействии преступлениям, совершаемым с использованием информационных технологий;

8) проведение совместных научных исследований, разработка, производство, поставка, оказание помощи компетентным органам государств – участников СНГ во внедрении специальных программно-технических средств,

необходимых для обнаружения, фиксации, изъятия и исследования следов преступлений, совершаемых с использованием информационных технологий и другие меры¹.

На процессы гармонизации и унификации законодательства государств - участников СНГ о борьбе с транснациональными преступлениями, совершаемыми с использованием информационных технологий, влияют унифицированные международные нормы, принятые в рамках ООН. Особое место занимает Конвенция ООН против транснациональной организованной преступности, принятая Резолюцией 55/25 Генеральной Ассамблеи от 15.11.2000 г.

Конвенция ратифицирована в Российской Федерации Федеральным законом от 26.04.2004 г. № 26-ФЗ «О ратификации Конвенции ООН против транснациональной организованной преступности от 15 ноября 2000 г». Цель конвенции заключается в содействии сотрудничеству в деле более эффективного предупреждения транснациональной организованной преступности и борьбы с ней².

Основные формы сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий, предусматривают:

1) обмен оперативной, статистической, научно-методической и иной информацией о состоянии преступности в сфере информационных технологий, информацией для пополнения банка данных о транснациональных преступных группах и преступных организациях, совершающих преступления с использованием информационных технологий;

2) проведение согласованных следственных действий, комплексных совместных и/или согласованных профилактических оперативно-разыскных мероприятий и специальных операций, создание и укрепление

¹ О Концепции сотрудничества государств — участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий: решение Совета глав государств СНГ от 25.10.2013. // URL: <http://www.e-cis.info/page.php?id=23808> (Дата обращения: 15.05.18).

² Против транснациональной организованной преступности: конвенция ООН, принятая Резолюцией 55/25 Генеральной Ассамблеи от 15.11.2000 // Бюллетень международных договоров, заключенных Российской Федерацией. 2004. № 3.

специализированных подразделений по противодействию преступлениям, совершаемым с использованием информационных технологий, оснащение их современными аппаратно-программными научно-техническими средствами;

3) выполнение запросов, поступающих от компетентных органов других государств – участников СНГ, по вопросам противодействия преступлениям, совершаемым с использованием информационных технологий;

4) совместное использование высоких технологий в сфере противодействия преступлениям, совершаемым с использованием информационных технологий;

5) взаимообмен нормативными правовыми актами, научными, учебными и методическими пособиями по проблемным вопросам противодействия преступлениям, совершаемым с использованием информационных технологий.

Программа сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий была одобрена 04.12.2015 г. Исполнительным комитетом СНГ в Минске. С учетом замечаний и предложений, поступивших от Азербайджана, Беларуси, Казахстана, России, Совета командующих пограничными войсками, секретариата Координационного совета генеральных прокуроров государств СНГ, эксперты доработали и согласовали проекты документов и предложили Исполнительному комитету направить их в страны СНГ.

Основными задачами Программы сотрудничества стран СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий, на 2016 – 2020 гг. являются: дальнейшее развитие международно - правовой базы взаимодействия; совершенствование и сближение национального законодательства; проведение комплексных совместных, согласованных межведомственных профилактических, оперативно-розыскных мероприятий и специальных операций; информационное и научное обеспечение сотрудничества; осуществление сотрудничества в подготовке

кадров, повышении квалификации специалистов; развитие сотрудничества с международными организациями¹.

Таким образом, сдержать распространение угроз в сфере информационной безопасности, сократить их уровень возможно лишь путем осуществления масштабной научно-обоснованной программы предупреждения, к разработке и реализации которой должны быть привлечены самые различные органы, организации и специалисты всех развитых стран.

Наиболее эффективной будет работа в следующих направлениях:

- дальнейшее развитие международного сотрудничества в сфере информационной безопасности;
- разработка глобальных международных нормативно-правовых актов, регулирующих различные аспекты использования информационного пространства;
- имплементация международно-правовых норм в сфере информационной безопасности в национальное законодательство нашей страны;
- объединение усилий международного научного сообщества в целях создания безопасных информационных технологий;
- разработка эффективных методов и механизмов по противодействию и устранению информационных угроз².

¹ Ревин В.П. Актуальные проблемы сотрудничества государств – участников Содружества Независимых Государств в борьбе с преступлениями, совершаемых с использованием информационных технологий // Международное сотрудничество евразийских государств: политика, экономика, право. 2017. №10. С. 84–90.

² Маслакова Е.А., Жилкин М.Г., Качалов В.В. К вопросу о международном сотрудничестве в сфере обеспечения информационной безопасности // Вестник Московского Университета МВД России. 2015. № 9. С. 75–77.

Заключение

С повышением роли информации во всех сферах деятельности повышается роль и значение компьютерной информации как одной из самых популярных форм создания, использования, передачи информации. А с повышением роли компьютерной информации требуется повышать уровень ее защиты с помощью технических, организационных и особенно правовых мер.

Одной из причин возникновения компьютерной преступности явилось информационно-технологическое перевооружение предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных.

Анализируя материал данной дипломной работы можно сделать вывод о необходимости внесения значительного массива дополнений и изменений в действующее законодательство Российской Федерации. Кроме того, требуется издание новых законов вносящих правовое регулирование в информационные отношения.

Недостаток комплексных мер противодействия, их противоречивость и фрагментарность, высокая латентность преступности в сфере компьютерной информации приводят к неэффективности выработанных мер ее предупреждения, обуславливая трудности в противодействии и борьбе с данным видом общественно опасных деяний.

Снижению латентности преступлений в сфере компьютерной информации будет способствовать как международное, так и внутреннее сотрудничество между государством и правоохранительными органами. Разъяснительная работа по поводу необходимости защиты законных интересов в сфере использования и развития информационных технологий; повышение уровня технического оснащения и развитие специальных навыков у сотрудников правоохранительных органов для эффективного выявления подобных преступлений.

Так же необходимо осуществить следующие организационные и правовые меры:

- увеличение штатной численности подразделений, специализирующихся на выявлении и раскрытии преступлений в сфере компьютерной информации;

- подбор в указанные подразделения специалистов, имеющих исчерпывающие знания в области информационно-телекоммуникационных технологий и дальнейшее постоянное и динамичное совершенствование их квалификации;

- постоянное совершенствование научных методик, программных средств и технических устройств для получения и закрепления доказательств совершения компьютерного преступления в ответ на внедрение новых механизмов и средств передачи данных;

- законодательное ограничение использования пользователями сетей передачи данных различных «анонимайзеров», предоставляющих услуги по маскировке реальных идентификаторов (например, IP-адресов) их окончного оборудования;

- обязать компании, предоставляющие информационно - телекоммуникационные услуги, разработать реальный механизм идентификации конкретных пользователей в сетях передачи данных, исключив факты присвоения одинаковых динамических IP-адресов массиву окончных устройств в ограниченный период времени. Ввести обязательный учет уникальных идентификаторов сетевого оборудования (IMEI, MAC-адресов), используемого конечными пользователями;

- ужесточить ответственность за отсутствие либо внесение заведомо недостоверных сведений о пользователях информационно - телекоммуникационными услугами и услугами связи, предоставляемыми на территории Российской Федерации.

Список литературы

Нормативно-правовые акты

1. Против транснациональной организованной преступности: конвенция ООН, принятая Резолюцией 55/25 Генеральной Ассамблеи от 15.11.2000 // Бюллетень международных договоров, заключенных Российской Федерацией. – 2004. – №4.
2. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (заключено в г. Минске 01.06.2001) // URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=9210#09638639701102296> (Дата обращения: 10.05.18).
3. О Концепции сотрудничества государств - участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий: решение Совета глав государств СНГ от 25.10.2013 // URL: <http://www.e-cis.info/page.php?id=23808> (Дата обращения: 15.05.18).
4. Российская Федерация. Конституция (1993) // СЗ. – 2014. – № 31. – Ст. 4398.
5. Уголовный кодекс РСФСР (утв. ВС РСФСР 27.10.1960; ред. от 30.07.1996) // Ведомости ВС РСФСР. – 1960. – № 40. – Ст. 591 (утратил силу).
6. Уголовный кодекс Российской Федерации от 13.06.1996 №63 – ФЗ (ред. от 23.04.2018) // СЗ. – 1996. – № 25. – Ст. 2954.
7. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 23.04.2018) // Российская газета. – 2001. – № 2861.
8. О связи: федер. закон от 07.07.2003 № 126-ФЗ // Российская газета. – 2003. – № 3249.
9. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ // СЗ. – 2006. – № 31. – Ст. 3448.

10. О ратификации Конвенции Организации Объединенных Наций против транснациональной организованной преступности и дополняющих ее Протокола против незаконного ввоза мигрантов по суше, морю и воздуху и Протокола о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее: федер. закон от 26.04.2004 г. № 26-ФЗ // Российская газета. – 2004. – № 3467.

Учебная литература

11. Алексеров, В.И., Колокольчикова, О.Н. Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации: учеб. пособие / М.: ВИПК МВД России, 2016. – 166 с.

12. Батурин, Ю.М. Проблемы компьютерного права / Ю.М. Батурин. – М.: Юридическая литература, 1991. – 272 с.

13. Вехов, В.Б., Голубев, В.А. Расследование компьютерных преступлений в странах СНГ: монография / Волгоград: ВА МВД России, 2004. – 304 с.

14. Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М.: Юрлитинформ, 2001. – 496 с.

15. Ворошилова, Т.В. Социальная и психологическая характеристика личности компьютерного преступника: практ. пособие / Т.В. Ворошилова. – М.: ВНИИ МВД России, 2009. – 45 с.

16. Дуленко, В.А., Мамлеев, Р.Р., Пестриков, В.А. Преступления в сфере высоких технологий: учеб. пособие / – М.: ЦОКР МВД России, 2010. – 196 с.

17. Комисаров, В.С. Уголовное право Российской Федерации / М., 2006. – 307 с.

18. Россинская, Е.Р. Судебная экспертиза в гражданском, административном и уголовном процессе / Е.Р. Россинская. – М.: Норма, 2006. – 656 с.

19. Сычев, Ю.Н. Основы информационной безопасности: учебно-практическое пособие / Ю.Н. Сычев. – М.: Изд. центр ЕАОИ, 2007. – 300 с.

20. Фатьянов, А.А. Правовое обеспечение безопасности информации в РФ: учеб. пособие / А.А. Фатьянов. – М.: Юрист, 2001. – 412 с.

21. Филиппов, А.Г. Криминалистика: учеб. пособие / А.Г. Филиппов. – М.: Высшее образование, 2007. – 441 с.

Научная литература

22. Алымов, Д.В., Шереметова, А.А. Методика расследования преступления в сфере компьютерной информации: сравнительный анализ отечественного и зарубежного опыта // Конф. УПК РФ 15 лет правоприменения. Курск. – 2016. –

С. 181–186. URL: <https://elibrary.ru/item.asp?id=27237083>.

23. Бессонов, С.А. История и зарубежный опыт правовой регламентации компьютерной преступности // Теория науки. – 2013. – № 2. – С. 231–237. URL: <https://elibrary.ru/item.asp?id=25077489>.

24. Булай, Ю.Г., Булай, Р.И. Профилактика и противодействие киберпреступности, а также международным киберугрозам // Академическая мысль. – 2017. – № 1. – С. 31–35. URL: <https://elibrary.ru/item.asp?id=32446721>.

25. Вехов, В. Б. Основные направления использования компьютерных технологий для обучения сотрудников правоохранительных органов // Вестник Волгоградской академии МВД России. – 2009. – № 2. – С. 114–117.

26. Вестник Всероссийского института повышения квалификации сотрудников МВД России. – 2013. – № 4.

27. Вестник Всероссийского института повышения квалификации сотрудников МВД России. – 2013. – № 2. – С. 32–37

28. Гончар, В.В. Совершенствование расследования преступлений в сфере информационных технологий // Эпоха науки. – 2017. – № 11. – С. 28. URL: <https://elibrary.ru/item.asp?id=30043161>.

29. Демидов, О.В. Обеспечение международной информационной безопасности и российский национальные интересы // Индекс безопасности. – 2013. – № 1. – С. 129–168. URL: <https://elibrary.ru/item.asp?id=18207786>.

30. Евдокимов, К.Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. – 2016. – № 1. – С. 86–94. URL: <https://elibrary.ru/item.asp?id=27386975>.

31. Ефремов, К.А. О некоторых аспектах расследования преступлений в сфере компьютерной информации // Вестник Волгоградской Академии МВД России. – 2015. – № 2. – С. 83–84. URL: <https://elibrary.ru/item.asp?id=24387080>.

32. Зверьянская, Л.П., Протасевич, А.А. Криминалистическая характеристика компьютерных преступлений // Российский следователь. – 2013. – № 11. – С. 45–47.

33. Зиновьева, Е.С. Международное сотрудничество по обеспечению информационной безопасности // Право и управление. XXI век. – 2014. – № 4. – С. 44–52. URL: <https://elibrary.ru/item.asp?id=23299139>.

34. Маслакова, Е.А., Жилкин, М.Г., Качалов, В.В. К вопросу о международном сотрудничестве в сфере обеспечения информационной безопасности // Вестник Московского Университета МВД России. – 2015. – № 9. – С. 75–77. URL: <https://elibrary.ru/item.asp?id=24306749>.

35. Мошкин, С.В. Типичные следственные ситуации на первоначальном этапе расследования преступлений в сфере компьютерной информации // Ретроспективы и перспективы права. – 2013. – № 5. – С. 48–50.

36. Нагорный, А.А. Криминологические особенности преступлений в сфере компьютерной информации // Законность и правопорядок в современном обществе: сборник материалов XV Международной научно-практической конференции. Новосибирск. – 2013. – С. 216–223.

37. Номоконов, В.А., Тропина, Т.Л. Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. – 2013. – № 5. – С. 148–160.

38. Платов, А.А. Состояние преступности в сфере компьютерной информации // Центральный научный вестник. – 2018. – № 3. – С. 23–24. URL: <https://elibrary.ru/item.asp?id=32402014>.

39. Потапов, С.А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические

процессы и явления. – 2016. – № 10. – С. 90–96. URL: <https://elibrary.ru/item.asp?id=27337509>.

40. Ревин, В.П. Актуальные проблемы сотрудничества государств-участников Содружества Независимых Государств в борьбе с преступлениями, совершаемых с использованием информационных технологий // Международное сотрудничество евразийских государств: политика, экономика, право. – 2017. – № 10. – С. 84–90. URL: <https://elibrary.ru/item.asp?id=29810088>.

41. Ступаков, В.И. Перспективы сотрудничества евразийских государств в развитии информационного общества: новые векторы сотрудничества стран СНГ, БРИКС в сфере информационных и коммуникационных технологий (ИКТ) // Международное сотрудничество евразийских государств: политика, экономика, право. – 2016. – № 3. – С. 57–69.

42. Сычев, Е.А., Алексеров, В.И., Колокольчикова, О.Н. Преступления, совершаемые в телекоммуникационных сетях, как разновидность преступлений в сфере компьютерной информации // Историческая и социально-образовательная мысль. – 2014. – № 4. – С. 350–355.

Иные источники

43. 19 октября - 25 лет со дня образования БСТМ МВД России. – URL: <https://xn--b1aew.xn--p1ai/news/item/11374675/> (Дата обращения: 23.04.18).

44. День образования Управления «К» Кибербезопасности Подразделений Специальных технических мероприятий МВД. – URL: <https://ruspekh.ru/events/item/den-obrazovaniya-upravleniya-k-kiberbezopasnosti-podrazdelenij-spetsialnykh-tekhnicheskikh-meropriyatij-mvd> (Дата обращения: 23.04.18).

45. История компьютерных преступлений. – URL: <https://sites.google.com/site/komputernyeprestuplenia/home/istoria-komputernyh-prestuplenij> (Дата обращения: 23.04.18).

46. Отдел «К» УМВД России по Тульской области. – URL: https://71.xn--b1aew.xn--p1ai/Dejatelnost/Borba_s_kiberprestupnostju (Дата обращения: 23.04.18).

47. Управление «К» МВД России. – URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (Дата обращения: 23.04.18).