Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Южно-Уральский государственный университет»
(национальный исследовательский университет)
Институт «Юридический»
Кафедра «Правоохранительная деятельность и национальная безопасность»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
д.ю.н., доцент
_____С. В. Зуев
_____2019 г.

Расследование преступлений, совершаемых с использованием информационных технологий сотрудниками органов внутренних дел

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
ФГАОУ ВО «ЮУрГУ» (НИУ) – 40.05.02.2019.516 ВКР

Руководитель работы,
Заведующий кафедры, д.ю.н.
_____ С.В. Зуев
_____2019 г.

Автор работы,
Студент группы Ю-516
_____ В.А. Сарлыбаев
_____2019 г.

Нормоконтролер,
доцент кафедры, к.ю.н.
_____ В.А. Задорожная
_____2019 г.

Челябинск 2019

АННОТАЦИЯ

Сарлыбаев В.А. Выпускная квалификационная работа «Расследование преступлений, совершаемых с использованием информационных технологий сотрудниками органов внутренних дел»: ФГАОУ ВО «ЮУрГУ» (НИУ), Ю-517, 67 с., библиогр. список – 45 наим., 1 приложение.

Целью исследования является всестороннее, полное и объективное исследование проблем, связанных с расследованием и предупреждением преступлений, совершаемых с использованием информационных технологий сотрудниками полиции.

В соответствии с поставленной целью были определены следующие задачи данного исследования:

1. Определиться с понятием, свойствами, видами и соотношением информации и информационных технологий.
2. Проанализировать правовые основы применения информационных технологий в расследовании преступлений.
3. Рассмотреть виды преступлений, совершаемых сотрудниками органов внутренних дел с использованием информационных технологий.
4. Провести анализ тактических особенностей расследования преступлений, совершаемых сотрудниками полиции.
5. Выяснить способы сокрытия средств, добытых преступным путем сотрудниками органов внутренних дел, с использованием информационных технологий.
6. Определиться с основными направлениями развития информационных технологий в расследовании преступлений, совершаемых сотрудниками органов внутренних дел.

7. Привести конкретные примеры из судебной практики, непосредственно относящиеся к предмету исследования.

В качестве объекта исследования выступают общественные отношения, регулирующие расследование преступлений, совершаемых с использованием информационных технологий сотрудниками полиции.

Предмет исследования – совокупность нормативных правовых положений, затрагивающих аспекты расследования преступлений, совершаемых с использованием информационных технологий сотрудниками органов внутренних дел.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования заключается в том, что в настоящее время роль развития и использования информационных технологий во всех сферах жизни резко возрастает. С одной стороны, наблюдается возрастающая роль информационных функций как характерной особенности деятельности органов внутренних дел. Взаимообмен служебно-справочной информацией происходит с помощью современной системы средств информационного обмена. Криминалистика также оказывает существенное воздействие на расследование и предупреждение преступлений путем внедрения и апробирования различных технологических средств и методов.

С другой стороны, достижения в области развития информационных и телекоммуникационных технологий используются сотрудниками органов внутренних дел и в преступных целях. К примеру, на практике возникают ситуации, когда в состав организованной преступной группы входят сотрудники полиции, служащие в информационных центрах МВД РФ и предоставляющие необходимую информацию преступникам. Кроме того, на практике наблюдаются такие способы получения взятки сотрудниками органов внутренних дел с использованием информационных технологий, как перевод на банковскую карту, зарегистрированную на третье лицо, перевод на счет в зарубежный банк или использование криптовалюты.

Следовательно, использование информационных технологий может выступать как способ совершения преступлений коррупционной направленности сотрудниками полиции. Так, согласно статистическим данным, размещенным на сайте Судебного департамента при Верховном Суде РФ, только за 2018 год в России к уголовной ответственности за совершение преступлений коррупционной направленности были привлечены

17 334 лица, из которых сотрудники органов внутренних дел занимают около 32 %[1].

В качестве важности решения проблем расследования данной категории преступлений можно привести данные, опубликованные «Трансперенси интернешнл». Так, в 2018 году Россия заняла 138 место из 180. Последние три года Россия набирала 29 баллов, а в этом году потеряла еще один балл и опустилась на три места. Столько же баллов набрали Папуа-Новая Гвинея, Ливан, Иран и Мексика.

В качестве объекта исследования выступают общественные отношения, регулирующие расследование преступлений, совершаемых с использованием информационных технологий сотрудниками полиции.

Предмет исследования – совокупность нормативных правовых положений, затрагивающих аспекты расследования преступлений, совершаемых с использованием информационных технологий сотрудниками органов внутренних дел.

Целью исследования является всестороннее, полное и объективное исследование проблем, связанных с расследованием и предупреждением преступлений, совершаемых с использованием информационных технологий сотрудниками полиции.

В соответствии с поставленной целью были определены следующие задачи данного исследования:

8. Определиться с понятием, свойствами, видами и соотношением информации и информационных технологий.

9. Проанализировать правовые основы применения информационных технологий в расследовании преступлений.

10. Рассмотреть виды преступлений, совершаемых сотрудниками органов внутренних дел с использованием информационных технологий.

[1] Сайт Судебного департамента при Верховном Суде Российской Федерации // URL: http://www.cdep.ru/index.php?id=150 (дата обращения 12.05.2019 г.).

11. Провести анализ тактических особенностей расследования преступлений, совершаемых сотрудниками полиции.

12. Выяснить способы сокрытия средств, добытых преступным путем сотрудниками органов внутренних дел, с использованием информационных технологий.

13. Определиться с основными направлениями развития информационных технологий в расследовании преступлений, совершаемых сотрудниками органов внутренних дел.

14. Привести конкретные примеры из судебной практики, непосредственно относящиеся к предмету исследования.

Нормативная основа данного исследования представлена следующими нормативными правовыми актами: Конституция РФ, Уголовный кодекс РФ, Кодекс об административных правонарушениях РФ, различные федеральные законы, подзаконные нормативные акты, тем или иным образом затрагивающие аспекты противодействия коррупции в органах внутренних дел. Несомненно, в качестве основных нормативных документов можно выделить: Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1], Федеральный закон Российской Федерации от 25.12.2008 г. № 273-ФЗ «О противодействии коррупции»[2], Федеральный закон Российской Федерации от 07.08.2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[3].

Методологическая основа данной работы представляет собой использование комплекса общенаучных и специальных методов познания.

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 г. № 149-ФЗ (с изм. и доп., вступ. в силу с 30.10.2018 г.) // СПС Консультант плюс.

[2] О противодействии коррупции: Федеральный закон от 25.12.2008 г № 273-ФЗ (с изм. и доп., вступ. в силу с 12.05.2018 г.) // СПС Консультант плюс.

[3] О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма: Федеральный закон от 07.08.2001 г. № 115-ФЗ (с изм. и доп., вступ. в силу с 27.12.2018 г.) // СПС Консультант плюс.

Особенно часто применялись такие методы, как обобщение, дедукция, метод правового моделирования, метод формализации и идеализации. Кроме того, в качестве специально-юридических методов применялись: сравнительно-правовой, метод толкования правовых норм, формально-юридический метод.

Практическую (эмпирическую) основу составляют материалы, конкретные примеры из судебной практики, непосредственно затрагивающие тему данного исследования.

Практическая значимость работы заключается в том, что выводы, научные положения, сформулированные в данном исследовании, могут быть использованы в научно-педагогической деятельности, в дальнейшем рассмотрении данного вопроса с целью совершенствования законодательства, регулирующего расследование преступлений, совершаемых с использованием информационных технологий сотрудниками органов внутренних дел.

Структура выпускной квалификационной работы соответствует логике исследования и состоит из введения, шести параграфов, заключения, списка использованной литературы. Структура отражает цель и задачи, поставленные в данной работе.

1 ТЕОРЕТИЧЕСКИЕ И ПРАВОВЫЕ ОСНОВЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1.1 Информация и информационные технологии: понятия, свойства, виды и соотношение

Термин «информация» происходит от латинского слова «information», что означает «ведения, разъяснения, изложение». Информация представляет собой настолько глубокое понятие, что его не представляется возможным раскрыть одной фразой. В данное понятие в науке, технике и житейских ситуациях вкладывается различный смысл. К примеру, в науке информацию принято считать как сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые воспринимают информационные системы (живые организмы, управляющие машины и др.) в процессе жизнедеятельности и работы.

Одно и то же информационное сообщение в виде статьи в газете, письма или радиопередачи может содержать разное количество информации для разных людей. Данный факт будет зависеть от количества накопленных знаний и уровня понимания каждого отдельного человека. Информация не является характеристикой самого сообщения, она представляет соотношение между сообщением и его потребителем. Следовательно, без наличия потребителя говорить об информации бессмысленно.

Если же говорить об информации применительно к компьютерной обработке данных, то информацию можно представить как «некоторую последовательность символических обозначений, несущих смысловую нагрузку и представленных в понятном компьютеру виде»[1]. Каждый новый

[1] Волевод А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М., 2012. – С. 73.

символ в такой последовательности увеличивает информационный объем сообщения.

Сущностное определение информации в правовом поле и, в частности, в уголовном процессе основывается на осознании субъектом познания требований, предъявляемых уголовно-процессуальным законом к содержанию доказательств и способам их получения, а также сведений о преступлении, и реализуется с момента восприятия субъектом информации, поступающей в устной, письменной, электронной и других формах передачи сигнала. Исследование информационно-сигнальной природы электронных доказательств в уголовном процессе позволяет различать физический уровень электронно-цифровых следов и информацию, определяемую субъектом уголовно-процессуального познания как имеющую значение для уголовного дела. Преобразование электронного сигнала в данные, пригодные для восприятия человеком, происходит с помощью специальных программ. Информация, полученная и проверенная в порядке, установленном уголовно-процессуальным законом, может стать доказательством.

Как и всякий объект, информация обладает определенными свойствами. Самой отличительной чертой является ее дуализм (на информацию влияют как исходные данные, так и методы, с помощью которых она фиксируется). С точки зрения информатики наиболее важными свойствами выступают: объективность, достоверность, полнота, актуальность, полезность, своевременность, понятность, доступность. Так, самой ценной информацией будет объективная, достоверная, полная и актуальная.

Классификация электронной информации достаточно условна. В литературе можно встретить классификации документов[1], электронных

[1] Иванов Н.А. Теоретические и методические основы судебной компьютерно-технической экспертизы документов: дисс… к.ю.н. – Москва, 2005. – С. 54-59; Лисиченко В.К. Криминалистическое исследование документов (правовые и методологические проблемы): дисс… д-ра юрид. наук. – Киев, 1973. – С. 105.

документов[1], документы на машинных магнитных носителях информации[2]. Ближе к настоящему исследованию классификация компьютерной информации, предложенная Н.А. Зигурой, которая делает это по таким основаниям:

1. По связи с событием преступления:

- компьютерная информация, которая служила орудием совершения преступления (вредоносные программы, программы – взломщики; программы подбора паролей);

- компьютерная информация, на которую были направлены преступления;

- иная компьютерная информация, которая может служить средством обнаружения преступления и установления обстоятельств уголовного дела (например, регистрация входа в локальную сеть в не рабочее время).

2. По происхождению:

- компьютерная информация, внесенная пользователем;

- компьютерная информация, созданная аппаратными и программными средствами.

3. По типу данных:

- текстовая информация;

- базы данных;

- графическая информация;

- анимация;

- мультимедийная;

- исполняемыми программами.

4. По типу носителя:

- компьютерная информация на энергозависимом носителе (ОЗУ);

[1] Кукарникова Т.Э. Электронный документ в уголовном процессе и криминалистике: дисс… к.ю.н. – Саратов, 2003. – С.67-74.

[2] Яковлев А.Н. Теоретические и методические основы экспертного исследования документов на машинных носителях информации: дисс.. к.ю.н. – Саратов, 2000. – С. 61.

- компьютерная информация на энергонезависимом носителе (жесткие диски, дискеты, лазерные диски, флэш-накопители).

Практическое значение имеет классификация сведений в электронной форме, предложенная В.Б. Веховым, который выделяет:

1) электронное сообщение – информацию, переданной или полученной пользователем информационно-телекоммуникационной сети, под которой понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

2) электронный документ – документированной информации, представленной в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационных сетям или обработки в информационных системах;

3) программы для ЭВМ – представленные в объективной форме совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения;

5) сайты в сети «Интернет» - совокупности программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается через сеть «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет»;

6) страницы сайта в сети «Интернет» (интернет-страницы) – части сайта в сети «Интернет», доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети «Интернет»[1].

[1] Вехов В.Б. Электронные доказательства: новеллы уголовно-процессуального законодательства: материалы международной научно-практической конференции

Считаем необходимым остановиться на некоторых видах информации поподробнее. Так, электронное сообщение это самый распространенный вид компьютерной и иной информации, используемый электронно-цифровую передачи данных. По закону, электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети. Согласно ГОСТ Р 53898-2010 от 26.10.2010 электронное сообщение – это XML документ, а также, при необходимости, дополнительные файлы, передаваемые (получаемые) из одной системы управления документами в другую систему управления документами.

Как весьма точно указывает Т.А. Боннер, «существенным недостатком электронного обмена документами через каналы Интернет, равно как и недостатком электронного документа вообще, является легкость внесения в него изменений и, как следствие, отсутствие уверенности в достоверности»[1] полученного документа.

Электронное сообщение хранится в памяти компьютера, с которого оно было отправлено (при использовании почтовых программ типа Microsoft Office Outlook), либо на сервере почтовой службы, если использовалась бесплатная онлайн-почта (Yandex, Google, Mail). Таким образом, подтвердить отправку письма с определенного компьютера или IP-адреса вполне возможно. Боле сложным представляется установление автора отправки сообщения, т.к. возникает вопрос о доступности компьютера и кто им мог воспользоваться.

В настоящее время в современном международном праве, в юридической и технической литературе достаточно широко используется термин «электронный документ». Однако, несмотря на это, данный термин как принятое официальное определение является относительно новым международным понятием и на национальном законодательном уровне

«Актуальные проблемы применения уголовно-процессуального законодательства при расследовании преступлений». – М., 2012. – С. 91-92.

[1] Боннер А.Т. Проблемы установления истины в гражданском процессе: монография. СПб., 2009. – С. 470.

легализован недавно. В Российской Федерации ни законодатель, ни современная доктрина до настоящего времени не разработали общепринятого определения электронного документа: в научной литературе имеется свыше 40 таких определений. Их анализ показал, что при всем разнообразии подходов можно выделить три основные группы определений электронного документа:

1) это машиночитаемый документ на машинном носителе;

2) это особый тип документа;

3) это электронная форма документа.

Следующим важным понятием, которое необходимо раскрыть в ходе данного исследования являются информационные технологии (от англ. information technology) – это широкий класс дисциплин и областей деятельности, относящихся к технологиям управления и обработки данных, в том числе, с применением вычислительной техники[1]. В последнее время под информационными технологиями все чаще понимают компьютерные технологии. В частности, информационные технологии имеют дело с использованием компьютеров и программного обеспечения для хранения, преобразования, защиты, обработки, передачи и получения информации.

Слово «технология», прежде всего, означает метод или способ выполнения определенных операций и процессов, связанных с изменением качества или первоначального состояния материала, объекта и т.п. К примеру, технология материального производства подразумевает процесс, заключающийся в изготовлении, обработке, изменении состояния, свойств и формы сырья материала.

Особенностью информационных технологий является то, что они связаны не с одним, а сразу с несколькими информационными процессами: создание, получение, сбор, хранение, обработка, передача и распространение

[1] Осипенко А.Л. Особенности расследования сетевых компьютерных преступлений // Российский юридический журнал. – 2010. – № 2. – С. 121-126.

информации. Кроме того, они не могут рассматриваться изолировано (вне материальной сферы).

Информационные технологии, во многом, ориентированы на решение определенных индустриальных задач, умножая возможности человека. Однако данный инструмент можно использовать и в качестве методологической платформы, обладающей универсальными моделями, языками для представления, формализации, моделирования, систематизации и обработки прикладных знаний. Также не стоит забывать о непосредственном или опосредованном участии человека в технологических процессах. Любой автоматизированный и даже автоматический процесс связан с необходимостью представления или получения информации в форме, удобной для человека.

Необходимо поговорить о различных проявлениях информационных технологий. Некоторые исследователи употребляют другие термины для обозначения подобных актов: «машинный документ» (Э. Мурадьян), «цифровой документ» (И.Ю. Богдановская), «документ на машинном носителе» (В. Вехов), «виртуальный документ» (А.А. Васильев, Т.Н. Абдурагимова). Однако приведенные понятия представляются не совсем точными ввиду того, что являются слишком широкими и не содержат указания на форму документа, которая и определяет особенности использования таких документов в гражданском и публичном обороте, а также в других сферах деятельности.

По мнению других ученых более обоснованно употребление термина «электронный документ»[1]. С такой позицией можно согласиться. Однако, по нашему, мнению электронные документы могут быть двух видов. В широком смысле это любая электронная информация, которая, может приравниваться к компьютерной информации, и электронный документ, заверенный электронной подписью. Поэтому все определения можно сгруппировать по

[1] Федосеева Н.Н., Шилова Д.А. Понятие и сущность электронного документа // Юрист. – 2008. – № 5. – С. 58.

данному основанию: в широком и узком смысле. Общее для них является то, что особой формы этого документа является электронной, т.е. связанной с электронами или основанной на свойствах электронов.

В широком смысле электронный документ представлен в правовых актах, в позициях ученых, в общественном сознании.

В Федеральном законе от 10 января 2002 г. «Об электронной цифровой подписи» он определяется как «документ, в котором информация представлена в электронно-цифровой форме»[1].

А.В. Рыбин под электронным документом как источником судебного доказательства предлагает понимать сведения об обстоятельствах, подлежащих установлению по делу, записанные на перфокарту, перфоленту, магнитный, оптический, магнитооптический накопитель, карту флэш-памяти или иной подобный носитель, полученные с соблюдением процессуального порядка их собирания[2].

Другое понимание электронного документа, в более узком смысле, основано на некоторых его признаках. Так, например, Л.Б. Краснова, считает, что электронный документ – один или несколько взаимосвязанных по установленному правилу файлов, содержащих совокупность электронно-цифровых объектов:

- отражающих сведения о лицах, предметах, фактах, событиях, явлениях и процессах;

- отражающих реквизиты, позволяющие подтвердить их подлинность и целостность;

[1] Об электронной подписи: Федеральный закон от 06.04. г. № 1-ФЗ (с изм. и доп., вступ. в силу с 28.07.2018 г.) // СПС Консультант плюс.

[2] Рыбин А.В. Электронный документ как вещественное доказательство по делам о преступлениях в сфере компьютерной информации: процессуальные и криминалистические аспекты / А.В. Рыбин : автореф. дисс. … канд. юрид. наук. – Краснодар, 2005. – С. 56.

- имеющих возможность представления в форме, пригодной для восприятия человеком[1].

Подлинность документа здесь является очень важным элементом. А.В. Нарижный также акцентирует на этом свое внимание. По его мнению, «электронный документ» – это сведения (сообщения, данные) в электронно-цифровой форме, зафиксированные на материальном носителе посредством электромагнитных взаимодействий либо передающиеся по каналам электросвязи посредством электромагнитных сигналов с реквизитами, позволяющими идентифицировать данные сведения (выделено авт. – Д.О.)[2].

Федеральный закон от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» уравнял правовой режим электронных документов и форм их употребления и оборота с режимом употребления традиционных документов на бумажном носителе во всех сферах коммерческой деятельности (ст. 6). Однако, как справедливо заметил Ю.П. Гармаев, науки антикриминального цикла пока не демонстрируют большого интереса к перспективным новинкам: работают, как говорится, по старинке – через традиционную «бумажную» продукцию[3].

Что касается электронных документов, то в практике хозяйствующих субъектов в целях экономии времени и финансовых средств широко распространена электронная переписка между контрагентами по различным вопросам: согласованию условий будущих взаимоотношений, пересылке тех или иных документов и т.п. Например, в договоре стороны могут предусмотреть, что все приложения, спецификации, протоколы согласования

---

[1] Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике: дисс. … канд. юрид. наук. – Воронеж, 2005. – С. 25.

[2] Нарижный А.В. Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий: дисс. … канд. юрид. наук. – Краснодар. 2009. – С. 53.

[3] Гармаев Ю.П. Мультимедийные криминалистические и межотраслевые средства противодействия преступности: перспективы разработки и внедрения / Дружественные к ребенку правосудие и проблемы ювенальной уголовной политики : материалы IV международной научно-практической конференции (г. Улан-Уде, 3-4 октября 2013). – Улан-Уде. 2013. – С. 43.

цен и иные документы, переданные электронной почтой, являются неотъемлемой частью этого договора и имеют юридическую силу.

Программа для ЭВМ – это совокупность данных и команд, которая предназначена для функционирования компьютерных устройств, в том числе электронно-вычислительных машин, в целях получения материалов, необходимых для разработки программ и самих программ для ЭВМ, а также порождаемые аудиовизуальные отображения.

Развитие компьютерных технологий порождает все новые компьютерные программы для разного назначения и применения. Безусловно, следователю, дознавателю и суду сложно ориентироваться во всём многообразии существующих программ, но им необходимо иметь достаточное представление о них, чтобы руководить расследованием или рассмотрением дела в суде. Такое представление может дать классификация компьютерных программ.

Программные продукты можно классифицировать по разным критериям. Основным из них является их назначение. Так, компьютерные программы разделяют на системные, инструментальные и прикладные.

Системные программы – это комплекс программ, осуществляющих управление внутренними компонентами компьютера и обеспечивающий их взаимодействие с прикладными программами. К системным программам можно отнести: операционные системы, драйверы, программные оболочки, утилиты.

Операционная система – это комплекс взаимосвязанных системных программ, контролирующий использование и распределение ресурсов вычислительной системы и организующий взаимодействие пользователя с компьютером. В зависимости от количества одновременно обрабатываемых задач и числа пользователей, различают четыре основных класса операционных систем: однопользовательские однозадачные – поддерживают одну клавиатуру и могут работать только с одной (в данный момент) задачей; однопользовательские однозадачные с фоновой печатью – позволяют помимо

основной задачи запускать одну дополнительную задачу, ориентированную на вывод информации на печать; однопользовательские многозадачные – обеспечивают одному пользователю параллельную обработку нескольких задач; многопользовательские многозадачные – позволяющие на одном компьютере запускать несколько задач несколькими пользователями. Известны операционные системы: MS-DOS, Windows NT, Windows 95, Windows 98, Windows 2000, Windows Me, Windows XP, Windows Vista, Windows 7, Windows 8, Linux и др.

Драйверы – программы расширяющие возможности операционной системы по управлению устройствами ввода-вывода, оперативной памятью и т.д. С помощью драйверов возможно подключение к компьютеру новых устройств или нестандартное использование имеющихся (драйверы клавиатуры, принтера, видеоконтроллера и др.). Драйверы устройств можно разделить на два основных вида: пользовательского режима и режима ядра. Драйверы пользовательского режима делятся на драйверы виртуальных устройств, использующиеся для поддержки программ (*MS-DOS*), и драйверы принтеров. Драйверы режима ядра подразделяются на драйверы файловой системы (реализующие ввод/вывод на локальные и сетевые диски), драйверы потоковых устройств (реализующие ввод/вывод видео и звука), драйверы видеоадаптеров (реализующие графические операции), *WDM*-драйверы (предназначенные в общем для расширения стандартных возможностей основного драйвера). Также, драйверы разделяют на одноуровневые и многоуровневые. Большинство драйверов, управляющих физическими устройствами, является многоуровневыми.

Программы оболочки – программы, созданные для упрощения работы со сложными программными системами. Оболочки предоставляют пользователю удобный доступ к файлам и обширные сервисные услуги. Примерами программ оболочек являются: Norton Commander, Total Commander, Volkov Commander, FAR Managerи т.п.

Утилиты – вспомогательные компьютерные программы, расширяющие и дополняющие соответствующие возможности операционной системы. Их подразделяют на антивирусные программы, программы архиваторы, программы русификаторы, программы для оптимизации дисков. Антивирусные программы предназначены для предотвращения заражения компьютерными вирусами и ликвидации последствий заражения вирусами. Различают следующие виды антивирусных программ: детекторы – сканируют файлы для поиска известных вирусов, соответствующих определению в словаре вирусов; доктора – находят и удаляют зараженные вирусом файлы; ревизоры – запоминают исходное состояние программ, каталогов и системных областей, а затем периодически сравнивают текущее состояние с исходным.

Представители антивирусного семейства программ – Microsoft Security Essentials, Kaspersky Antivirus, DrWeb, Norton Antivirus. Программы-упаковщики (архиваторы), позволяют сжимать информацию на дисках, а также объединять копии нескольких файлов в один архивный файл, для удобного хранения информации. Представители данных программ –WinZip и WinRar. Программы для оптимизации дисков, создания резервных копий информации (например, APBackUp, Acronis True Image) – позволяют периодически копировать информацию, находящуюся на жёстком диске компьютера, на дополнительные носители.

Инструментальные программы – программы, которые используются в ходе разработки, корректировки или развития других прикладных или системных программ. К инструментальным программам можно отнести трансляторы, редакторы текстов программ, вспомогательные программы, библиотеки подпрограмм. Трансляторы реализуются в виде компиляторов или интерпретаторов, выполняют преобразование с одного языка программирования на другой. Компилятор читает всю программу целиком, делает её перевод и создает законченный вариант программы на машинном языке, который затем и выполняется. Интерпретатор переводит и выполняет

программу строка за строкой. Редакторы обеспечивают редактирование текстов программ и цветовое выделение на экране синтаксических конструкций языка программирования. Вспомогательные программы – это отладчики, программы для получения перекрёстных ссылок и т. п. Библиотеки подпрограмм содержат заранее подготовленные подпрограммы, которые могут использовать программисты. Большое количество программ написано с использованием языков программирования: Java, *C*, *C++*, *PHP*, MathLab,Visual Basic/Basic, FoxPro, Assembler, Pascal.

Прикладные программы – способствующие решению какой-либо задачи в пределах данной проблемной области и обеспечивающие выполнение необходимых пользователям работ: редактирование текстов, рисование картинок, обработка информационных массивов и т.д. Их разделяют на программы общего назначения, методо-ориентированные, проблемно-ориентированные и профессионального уровня.

Программы общего назначения – программы, ориентированные на широкий круг пользователей в различных проблемных областях, позволяющие автоматизировать наиболее часто используемые функции и работы.

Методо-ориентированные программы предназначены для решения задач числового анализа, статистических задач. К ним относятся программы: математических методов (для решения дифференциальных уравнений и имитационного моделирования, к примеру, Mathematica, SMathStudio, EquPixy, Matrix и др.), статистики (например, Calc *3*D Pro), экономического назначения (бухгалтерские – 1С8, Галактика, Парус и т. п., финансового анализа – Project Expert, Pick Soft, Budget Manager *и* др., правовые базы данных – Гарант, Консультант, Кодекс и т.п.), обучающие программы (например, RocketReader), компьютерные вирусы.

Компьютерные вирусы можно условно классифицировать по следующим признакам: по среде обитания вируса (сетевые, файловые, загрузочные); по способу заражения среды обитания; по деструктивным

возможностям; по особенностям алгоритма вируса. По способу заражения среды обитания вирусы бывают резидентные (при инфицировании компьютера находятся в оперативной памяти и являются активными вплоть до его выключения) и нерезидентные (не заражают память компьютера и являются активными ограниченное время). По деструктивным возможностям их разделяют на очень опасные (уничтожают данные на компьютере), опасные (приводят к сбою в работе компьютера), неопасные (уменьшают память и создают различные эффекты) и безвредные (уменьшают свободную память). По особенностям алгоритма вируса различают программы: троянские программы, вирусы-черви, компаньон-вирусы, паразитические, стелс-вирус, полиморфик-вирусы и макровирусы. Проблемно-ориентированные компьютерные программы – программы для решения задач планирования, оперативного управления, материально-технического снабжения и т.д. Они включают в себя программы: комплексные для предприятий, комплексные для не промышленной сферы и для отдельных предметных областей.

Программы АРМ – помогают решать задачи в рамках деятельности этого специалиста (например, АРМ диспетчера, АРМ конструктора, АРМ технолога и т. п.).

Представляют интерес также сайты. Сайт (произошло от англ. website: web – «паутина, сеть» и site – «место», буквально «место, сегмент, часть в сети») – система электронных документов (файлов данных и кода) физического или юридического лица в компьютерной сети под общим адресом (доменным именем или IP-адресом). Все сайты вместе составляют Всемирную паутину, где коммуникация (паутина) объединяет сегменты информации мирового сообщества в единое целое – базу данных и коммуникации планетарного масштаба. Для прямого доступа клиентов к сайтам на серверах был специально разработан протокол HTTP.

Соотношение категорий «информация» и «информационные технологии можно рассматривать с нескольких аспектов. Так, информация не

существует сама по себе, она проявляется в информационных процессах. Информационные процессы могут быть целенаправленными или стихийными, организованными или хаотичными, детерминированными или вероятностными. Следует обратить внимание, что информационный процесс всегда протекает в какой-либо информационной системе. Наиболее общими информационными процессами являются три процесса: сбор, преобразование, использование информации.

То есть, информационные технологии представляют собой определенный порядок выполнения операций, действий по переработке первоначальной информации с целью предоставления ее для пользователя в определенном виде. Следовательно, информационные технологии взаимодействуют с информационными системами, которые, в свою очередь, включают в себя информационные процессы (сбор, преобразование и использование информации).

Таким образом, на данный момент возникла проблема, когда наиболее отчетливо проявился разрыв между объемом информации в обществе и возможностями отдельного человека в ее освоении. Впервые в истории человечества большинство социальных процессов приобрели ярко выраженную особенность информационных, то есть не просто связанных с операциями извлечения информации, ее трансляции в пространстве и времени, а в большой степени – с избирательным отношением человека к информации, с потребностью в специальных инструментах, которую будут способствовать получению и обработке информации.

В данном контексте не стали исключением и правоохранительные органы. Преступники все чаще стали использовать информационные технологии как средство и орудие совершения преступлений. Кроме того, и сами сотрудники органов внутренних дел используют их для сокрытия средств, добытых преступным путем. В связи с этим возникает потребность в разработке тактики и методов раскрытия подобных преступлений.

1.2 Правовые основы применения информационных технологий в расследовании преступлений

В первую очередь следует упомянуть международные правовые акты, регулирующие применение информационных технологий в расследовании преступлений. 10-17 апреля 2000 года на X Конгрессе ООН по предупреждению преступности и обращению с правонарушителями в Вене была принята Декларация о преступности и правосудии: ответы на вызовы XXI века[1], где было принято решение разработать ориентированные на конкретные действия программные рекомендации в отношении предупреждения преступлений, связанных с использованием компьютеров, и борьбы с ними, и предложено Комиссии по предупреждению преступности и уголовному правосудию приступить к работе в этом направлении, принимая во внимание работу, которая ведется в других форумах. Также было принято решение работать в направлении укрепления наших возможностей по предупреждению, расследованию и преследованию преступлений, связанных с использованием высоких технологий и компьютеров.

01 июня 2001 года в г. Минске принято Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. Россия ратифицировала Соглашение с оговоркой (Федеральный закон от 01.10.2008 № 164-ФЗ). Соглашение вступило в силу для России 17.10.2008[2]. Согласно данной оговорки, Российская Федерация оставляет за собой право отказать в исполнении запроса полностью или частично, если исполнение запроса может нанести ущерб ее суверенитету или безопасности[3].

[1] Декларация о преступности и правосудии: ответы на вызовы XXI века. // URL: http://www.un.org/ru/documents/decl_conv/declarations/vendec.shtml.
[2] Бюллетень международных договоров. – 2009. – № 6. – С. 12-17
[3] Российская газета. – 2008. – 03 октября.

23 ноября 2001 года в г. Будапешт Совет Европы принял Конвенцию о преступности в сфере компьютерной информации[1]. В этом документе в стремлении к единству между его членами признается необходимость в приоритетном порядке общей политики в сфере уголовного права, нацеленной на защиту общества от преступности в сфере компьютерной информации, в том числе путем принятия соответствующих законодательных актов и укрепления международного сотрудничества.

Обращено внимание на Рекомендации Комитета министров NR (85) 10 относительно практического применения Европейской конвенции о взаимной правовой помощи по уголовным делам в том, что касается судебных поручений о перехвате телекоммуникационных сообщений, NR (88) 2 о борьбе с пиратством в области авторского права и смежных прав , NR (87) 15 о порядке использования персональных данных полицией, NR (95) 4 о защите персональных данных в сфере телекоммуникационных услуг, в особенности телефонных услуг. Аналогичного внимания подвергнута Резолюция № 1, принятая на 21-ой Конференции министров юстиции стран Европы (Прага, 10 и 11 июня 1997 г.), в которой Комитету министров было рекомендовано поддержать проводимую Европейским комитетом по проблемам преступности (ЕКПП) работу по преступности в сфере компьютерной информации, чтобы обеспечить большую согласованность положений внутреннего уголовного права и сделать возможным использование эффективных средств расследования таких правонарушений.

Проблема, с которой столкнулись страны, связана с ограничением информационной свободы. С одной стороны, пользование всемирной компьютерной сетью предоставляет свободный обмен информацией; с другой стороны, государственным службам безопасности должна быть предоставлена возможность поиска и перехвата информации в Интернете, а также затребование ее в случае необходимости. Так, ст. 20 Конвенции

[1] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 года) // СПС Консультант плюс.

предоставляет возможность сбора в режиме реального времени данных о потоках информации. Согласно ее положениям каждая Сторона принимает законодательные и иные меры, необходимые для предоставления ее компетентным органам полномочий по сбору или записыванию с применением технических средств на территории этой Стороны; обязать поставщиков услуг в пределах имеющихся у них технических возможностей по сбору или записыванию с применением технических средств на территории этой Стороны.

Кроме того, ст. 21 определяет перехват данных о содержании и требует, что каждая Сторона принимает законодательные и иные меры в отношении ряда серьезных правонарушений, подлежащих квалификации в соответствии с нормами внутригосударственного права, необходимые для того, чтобы наделить ее компетентные органы полномочиями: собирать или записывать с применением технических средств на территории этой Стороны; обязать поставщика услуг в пределах имеющихся у него технических возможностей собирать или записывать с использованием технических средств на территории этой Стороны, сотрудничать с компетентными органами и помогать им в сборе или записи в режиме реального времени данных о содержании указанных сообщений на ее территории, передаваемых с помощью компьютерных систем.

Все это достаточно серьезно ограничивает свободу общения между людьми и затрагивает суверенитет государств. А.Н. Гулемин считает, что в международных документах необходимо удержание равновесия между задачами правоохранительных органов и потребностями общества, государства и личности[1].

[1] Гулемин А.Н. Конвенция о киберпреступности: проблемы интеграции в национальное законодательстве / Проблемы профилактики и противодействия компьютерным преступлениям: материалы международной научно-практической конференции (г. Челябинск, 30 мая 2007 г.) и круглого стола (г. Челябинск, 18 мая 2007 г.) отв. ред. А.В. Минбалеев / Челябинский центр по исследованию проблем противодействия организованной преступности и коррупции. – Челябинск, 2007. – С. 66-69.

Такое равновесие добиться достаточно сложно. Возможно, поэтому далеко не все государства присоединились к данной Конвенции, в том числе и Россия. Присоединение к Конвенции неизбежно потребует либо принятия оговорок относительно юридического действия целого ряда положений Конвенции относительно их применения в Российской Федерации, либо внесения изменений в российское уголовное законодательство.

Хотелось бы заметить, что текущая позиция мирового сообщества относительно правового регулирования электронного документооборота включает в себя главным образом разработку единообразных законов в независимых государствах с очень различающимися правовыми системами и традициями. Поэтому главная цель состоит в гармонизации и унификации законодательства. Наиболее важным законодательным инструментом, используемым для достижения этих целей, в частности Европейским союзом, являются директивы. В них содержится обязательный результат, который государства-члены должны достигнуть в течение указанного срока, но формы и методы достижения результата оставлены на рассмотрение государств.

28 мая 2004 года на Межпарламентской Ассамблее Евразийского Сообщества в Астане (Республика Казахстан) принято постановление №5-20, О типовых проектах законодательных актов МПА ЕврАзЭС в сфере информационных технологий («Об информатизации», «Об информационной безопасности», «Основные принципы электронной торговли»)». Согласно ст. 1 типового проекта «Основные принципы электронной торговли» одной из целей его разработки является «признание электронных документов в качестве судебных доказательств» [1].

На XI Конгрессе ООН по предупреждению преступности и уголовному правосудию, который состоялся в Бангкоке 25 апреля 2005 г., большое внимание было уделено преступности, связанной с использованием

[1] О типовых проектах законодательных актов МПА ЕврАзЭС в сфере информационных технологий: постановление от 24.05.2008 г. №5-20 // СПС Консультант плюс.

компьютеров. Было отмечено, что «для решения проблем киберпреступности необходимо применять широкие, комплексные подходы, выходящие за рамки уголовного и уголовно-процессуального законодательства, а также правоприменения. Помимо необходимости предотвращения преступлений, связанных с использованием компьютеров, и судебного преследования за их совершение, появляется глобальная задача – создание глобальной культуры кибербезопасности, в рамках которой учитывались бы потребности всех стран, включая развивающиеся, структуры информационных технологий в которых находятся в процессе становления и пока еще весьма уязвимы».

Законодательство зарубежных стран готово к электронному обмену документов. В настоящее время в ряде государств - участников Содружества Независимых Государств действуют законы об электронном документе - в Республике Армения, Республике Беларусь, Кыргызской Республике, Республике Молдова, Республике Узбекистан, Азербайджанской Республике, Республике Казахстан и других.

Так, Законом Республики Беларусь от 28 декабря 2009 г. N 113-З «Об электронном документе и электронной цифровой подписи» введены в действие такие понятия, как «копия электронного документа», «подлинность электронного документа», «целостность электронного документа».

Электронный документ, согласно ст. 17 указанного Закона, состоит из двух неотъемлемых частей – общей и особенной. Общая часть электронного документа состоит из информации, составляющей содержание документа. Особенная часть электронного документа состоит из одной или нескольких электронных цифровых подписей, а также может содержать дополнительные данные, необходимые для проверки электронной цифровой подписи (электронных цифровых подписей) и идентификации электронного документа, понятной для восприятия человеком.

В Латвии с 1 июля 2010 г. вступил в силу Закон от 19 мая 2010 г. № 78 (4270) «О юридической силе документов», которым устанавливаются требования к обеспечению юридической силы оригиналов, копий и выписок

документов. К электронным документам применяются также требования Закона от 31 октября 2002 г. № 169 (2744) «Об электронных документах», которым установлено, что в электронном документообороте между государственными учреждениями и учреждениями самоуправления или между этими учреждениями и физическими лицами электронный документ считается подписанным, если у него имеется безопасная электронная подпись и временная печать или электронная подпись, если стороны письменно договорились о подписании электронного документа электронной подписью.

В Германии принят Закон об административном производстве от 25 мая 1976 г., который не только устанавливает принципиальную возможность использования электронных документов, но и регулирует порядок их передачи, подписания электронной подписью, перевода документов из одного вида в другой, порядок свидетельствования документов административными органами, издание административного акта в электронной форме. В частности, в соответствии с § 33 указанного Закона административными органами свидетельствуются копии документов, распечатки электронных документов, а также электронных документов, изготовленных в виде иллюстрации письменных документов. Свидетельствование осуществляется путем надписи, содержащей: точное наименование документа; подтверждение соответствия копии представленному документу; указание на то, в какой орган представляется копия, место и дату свидетельствования, подпись правомочного сотрудника и оттиск служебной печати[1].

Для Соединенного Королевства характерен подход ограничения вмешательства государства в частные дела. Соответственно и электронный

[1] Бергманн В. Административно-процессуальное право Германии = Verwaltungsrechtsschutz in Deutschland: Закон об административном производстве; Закон об административно-судебном процессе; Законодательство об исполнении административных решений / Пер. с нем.; введ., сост. В. Бергманн. М.: Волтерс Клувер, 2007. Кн. 4 (серия «Германские и европейские законы»).

документооборот не должен быть объектом жесткого регулирования. Для Германии же характерен государственный подход к регулированию многих сфер деятельности, вследствие чего и электронный документооборот оказался под жестким контролем государства.

Например, в Германии решили, что электронный документооборот, а в особенности электронные подписи, – самостоятельная сфера деятельности в области телекоммуникаций (наряду с телевещанием, предоставлением доступа в Интернет), а, следовательно, должны быть поставлены под жесткий контроль государства. Во Франции, наоборот, намного более свободный подход к регулированию электронного документооборота, что проявляется в предоставлении сторонам свободы выбора технологии электронного документооборота при осуществлении предпринимательской и других видов деятельности – электронный документ и электронная подпись закреплены в нормах ГК[1]. Причем рекомендуется также обязать провайдеров сохранять полную конфиденциальность о фактах сотрудничества с правоохранительными органами[2]. Например, в Германии (как и во многих других европейских странах) в отношении провайдеров действует обязательное требование о предоставлении информации в соответствии с § 89 абз. 6 Закона о телекоммуникациях (TKG)[3].

Представляется, что зарубежный опыт может быть полезен при совершенствовании законодательства Российской Федерации в сфере обеспечения юридической значимости электронных документов[4].

---

[1] Дутов М.М. Сравнительный анализ европейского законодательства в области электронного документооборота // URL: fecha@skif.net.

[2] Дашян М. Обзор Конвенции Совета Европы о киберпреступности // Современное право. – 2002. – № 11. – С. 23.

[3] Юрген П.Г. Преступления в Интернете. Полномочия и границы органов расследования // Переводы материалов о практике деятельности правоохранительных органов зарубежных стран. М., 2003. – С. 49.

[4] Семизорова Е.В. Актуальные вопросы правового регулирования обеспечения юридической значимости электронных документов // Российская юстиция. – 2011. – № 2. – С. 46.

Что касается отечественного правового регулирования данного вопроса, то законодатель обратил внимание к информационное сфере еще в 1991 году, когда был разработан проект закона РСФСР «Об ответственности за правонарушения при работе с информацией», предусматривающий дисциплинарную, гражданско-правовую, административную и уголовную ответственность за подобные деяния, однако он так и не был принят[1]. Затем было принято множество нормативных правовых актов, так или иначе регулирующих данную сферу. Например: Федеральный закон от 20 февраля 1995 г. «Об информации, информатизации и о защите информации»; Федеральный закон от 27.07.2006 г. № 149-ФЗ; Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной цифровой подписи»[2]. Уголовный кодекс РФ объединил в главу 28 преступления, за которые предусмотрена ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ), нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ).

Федеральный закон «Об информации, информационных технологиях и о защите информации» определяет такие важные понятия, как информация, информационные технологии; информационная система; информационно-телекоммуникационная сеть; электронное сообщение; электронный документ; сайт в сети «Интернет»; страница сайта в сети «Интернет». К примеру, согласно п. 10 ч. 2 приведенного закона электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети. При этом под последним понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

---

[1] О концепции правовой информатизации России: указ Президента РФ от 28.061993 г. № 966 // Российские вести. – 1993. – 13 июля.

[2] Об электронной подписи: Федеральный закон от 06.04.2011 г. № 63-ФЗ (с изм. и доп., вступ. в силу с 23.06.2016 г.) // СПС Консультант плюс.

Уголовный процесс, как отдельная отрасль российского права, по нашему мнению, отстает в информационно-технологическом плане от остальных отраслей. Так, в гражданском судопроизводстве происходит вытеснение письменных документов электронными, юридические факты устанавливаются электронными средствами доказывания. В сфере государственного управления происходит аналогичная ситуация по замене письменного документооборота электронным. Несомненно, в нормах УПК РФ содержатся положения по применению современных технологий. Так, ч. 6 ст. 164 гласит, что «при производстве следственных действий могут применяться технические средства и способы обнаружения, фиксации и изъятия следов преступления и вещественных доказательств».

В настоящее время правовая основа раскрытия и расследования преступлений, совершаемых с использованием информационных технологий, отстает от уровня развития общественных отношений. В целях совершенствования регулирования раскрытия и расследования данной категории преступлений предлагается внести ряд изменений в УПК РФ, в частности п. 2.1 статьи 37 УПК РФ изложить следующим образом: «2.1. По мотивированному письменному (электронному) запросу прокурора ему предоставляется возможность ознакомиться с материалами находящего в производстве уголовного дела. В случае электронного запроса необходимо использование электронно-цифровой подписи». Также дополнить ст. 5 п. 63 следующего содержания: «63) электронно-цифровая подпись (электронная подпись) – это информация в электронной форме, совмещенная с подписываемой информацией и (или) иным образом связанная с ней, используемая для идентификации лица, подписывающего информацию». Кроме того, считаем необходимым дополнить главу 10 ст. 84.1 УПК РФ «Электронная информация» (Приложение 1).

1.3 Виды преступлений, совершаемых сотрудниками органов внутренних дел с использованием информационных технологий.

Говоря о преступлениях, которые могут совершать сотрудники органов внутренних дел, используя информационные технологии, необходимо обратиться к Уголовному кодексу РФ (далее УК РФ) и перечислить конкретные виды преступлений. В качестве первого состава выступает ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». Данная норма была внесена в УК РФ Федеральным законом от 7 декабря 2011 года № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»[1].

Такие законодательные изменения были вызваны бурным развитием информационно-коммуникационных технологий, что, в конечном счете, приводит к существенным модификациям понятийного аппарата, который должен содержаться в уголовном законодательстве. Увеличение количества и разновидностей противоправных деяний в этой сфере требует их уточнения в объективной стороне конкретных составов преступления. Так, П. М. Чернышев по этому поводу пишет: «внедрение автоматизированных информационных систем и технологий управления и обработки информации, придание юридической силы актам, осуществляемым с помощью компьютерных программ, создали предпосылки использования этих процессов для совершения преступных актов, а следовательно, и необходимость усиления их защиты, в том числе, уголовно-правовыми методами»[2].

Общественная опасность данного состава преступления обусловлена тем, что изменение, блокировка или уничтожение компьютерной

[1] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 07.12.2011 г. № 420-ФЗ // Российская газета. – 2011. – 8 декабря.
[2] Чернышев П.М. Информационные технологии в юридической деятельности // Марийский юридический вестник. – 2016. – № 2. – С. 63.

информации могут повлечь серьезные последствия, включая серьезные финансовые потери, причинение вреда здоровью и даже гибель людей. Не случайно законодатель отнес гл. «преступления в сфере компьютерной информации» к разделу IX УК РФ «Преступления против общественной безопасности и общественного порядка».

Объективная сторона ст. 272 УК РФ представлена в виде неправомерного доступа к охраняемой законом компьютерной информации. Доступом к информации является получение возможности ознакомиться и (или) воспользоваться компьютерной информацией. Данный процесс может выражаться в виде определенных действий: «проникновение в компьютерную систему путем использования специальных технических или программных средств, позволяющих преодолеть установленные системы защиты, незаконное использование действующих паролей или кодов для проникновения в компьютер, либо совершение иных действий в целях проникновения в систему или сеть под видом законного пользователя».

Объектом данного состава преступления выступает компьютерная информация. Субъективная сторона характеризуется умышленной формой вины по отношению к совершаемым действиям, однако в отношении последствий возможно и неосторожная форма вины. Состав преступления является материальным и требует наступления одного из следующих последствий: уничтожение, блокирование, модификация или копирование информации. Субъект – общий, в том числе им может быть и сотрудник органов внутренних дел.

Не обходят стороной сотрудников органов внутренних дел и преступления коррупционной направленности. Так, согласно данным, размещенным на сайте Судебного департамента при Верховном Суде РФ, в России за 2018 год было рассмотрено 476 уголовных дел, в которых сотрудники правоохранительных органов были осуждены по ст. 290 УК РФ

«Получение взятки»[1]. В рамках данного исследования нас интересуют способы получения взятки с использованием информационных технологий. К таковым можно отнести:

1) путем перевода на банковскую карту, зарегистрированную на третье лицо;

2) путем перевода на счет в зарубежный банк;

3) используя криптовалюту.

Следует отметить, что пока не только в России, но и в мире не существует законодательно зафиксированного прецедента получения взятки именно в криптовалюте и, тем более, последовавшего затем наказания. Однако в средствах массовой информации периодически появляется информация, связанная с попытками совершения таких преступлений.

К примеру, довольно мощный скандал случился в 2017 году в США, когда партнер юридической фирмы «Akin Gump Strauss» Джеффри Верткин был арестован при попытке продать конфиденциальную информацию за 310 000 $. Изначально адвокат требовал за нее средства в бикоинах – ведь транзакции сложно отследить. Однако уже при совершении взяточничества участвовали «настоящие» деньги, а потенциальный покупатель компромата начал сотрудничать с властями[2].

Кроме того, у должностных лиц в России появилось больше возможностей получать взятки. Так, Министерство труда в начале 2019 года выпустило новые методические рекомендации для чиновников «по вопросам представления сведений о доходах, расходах, об имуществе и обязательствах имущественного характера и заполнения соответствующей формы справки в

[1] Сайт Судебного департамента при Верховном Суде Российской Федерации // URL: http://www.cdep.ru/index.php?id=79&item=4572 (дата обращения 24.03.2019 г.).
[2] Деловой журнал «Инвест-Форсайт» // URL: https://www.if24.ru/vojdut-li-v-modu-kriptovzyatki/ (дата обращения 24.03.2019 г.).

2019 году[1]. Данный документ ведомство разрабатывает ежегодно при участии администрации президента и Генпрокуратуры.

По данному вопросу высказался председатель национального анстикоррупционного комитета России К. А. Кабанов: «Привлекательность криптовалют для сомнительных, с точки зрения буквы закона операций, объяснима, конечно же, отсутствием для цифровых денег правового поля. Криптовалюты изначально использовались для незаконных денежных операций, и сегодня человека практически невозможно привлечь, скажем, за получение или дачу взятки в биткоинах. Доказать это будет столь же сложно, как обосновать стоимость воздуха. Можно попробовать доказать, что биткоины были кем-то приобретены за реальные деньги и являются ценным активом, но это крайне затруднительно»[2].

Еще одним способом получения взятки является перевод денежных средств на банковскую карту третьего лица. В качестве яркого примера механизма получения взятки таким способом может служить следующий случай из судебной практики.

Так, 27 июня 2017 года, в 19 часов 35 минут, в дежурную часть ОМВД России «Котельниковский» в книгу учета сообщений и преступлений было зарегистрировано сообщение о том, что на контрольно-пропускном пункте Гремячинского горно-обогатительного комбината задержан рабочий, который пытался незаконно пронести фрагмент медного кабеля. Сразу после получения данного сообщения был организован выезд следственно-оперативной группы, в состав которой входил подозреваемый следователь П., на место происшествия.

Следователь П., достоверно зная, что за свое противоправное действие рабочий будет привлечен к административной ответственности за мелкое хищение, а также достоверно зная, о том, что данный материал будет передан

[1] Официальный сайт Министерства труда и социальной защиты Российской Федерации // URL: https://rosmintrud.ru/docs (дата обращения 03.04.2019 г.).
[2] Официальный сайт Национального Антикоррупционного Совета Российской Федерации // URL: http://www.korupcii.net/index.php?s=3 (дата обращения 03.04.2019 г.).

должностному лицу, уполномоченному составлять протоколы об административных правонарушениях отдела полиции и он не сможет в силу своих должностных полномочий, ведомственных нормативных актов, действующего уголовно-процессуального законодательства, влиять на принятие по материалу процессуального решения, в том числе и принимать решение о возбуждении уголовного дела, имея умысел, направленный на хищение чужого имущества, путем обмана, используя свое служебное положение, действуя из корыстных побуждений, сообщил рабочему, что за совершенные противоправные деяния он может быть привлечен к уголовной ответственности, тем самым заведомо создал условия, при которых у рабочего с учетом имевшейся у него непогашенной судимости имелись основания опасаться осуществления этого.

После чего следователь П. в продолжение реализации своих преступных намерений предложил рабочему передать ему денежные средства в сумме 50 000 рублей за оказание содействия в освобождении от уголовного наказания. Рабочий, введенный следователем П. в заблуждение, согласился передать ему денежные средства в сумме 50 000 рублей. Следователь П., в свою очередь, определил порядок передачи денежных средств путем их перевода на банковскую карту, номер которой он пообещал сообщить позднее.

Уже 29 июня 2017 года, в 18 часов 46 минут, следователь П., продолжая реализацию своего преступного умысла, направил на абонентский номер рабочего смс-сообщение с указанием в нем номера банковской карты ПАО «Сбербанк России», зарегистрированную на его знакомого, которого о своих преступных намерениях незаконного обогащения не поставил, ограничившись только предоставлением информации о переводе ему денежных средств должником в качестве исполнения долговых обязательств, которые знакомый должен будет снять со своего счета и передать ему.

Затем районным судом данный рабочий был признан виновным в совершении административного правонарушения, предусмотренного ч.1 ст.

7.27 КоАП РФ. Однако следователь П. в телефонном разговоре с рабочим высказал ему, что в случае нарушения им ранее достигнутой договоренности о передаче ему денежных средств в сумме 50 000 рублей, он приобщит к материалам административного дела справку с завышенной суммой ущерба, что приведет к возбуждению уголовного дела. В последующем рабочий уже под контролем сотрудников СБ ГУ МВД России по Волгоградской области, несколькими частями перевел оговоренную сумму знакомому следователя П. Затем данный следователь принял 50 000 рублей наличными от своего знакомого и был задержан сотрудниками органов внутренних дел[1].

Кроме того, на практике возникают ситуации, когда в состав организованной преступной группы входят сотрудники органов внутренних дел, служащих в информационных центрах МВД РФ и предоставляющие необходимую информацию преступникам. Ярким примером может служить следующий случай из судебной практики.

Так, на территории Российской Федерации Е. занимался деятельностью, связанной со сбором, обобщением и систематизацией информации, поступающей от различных кредитно-финансовых, банковских и иных организаций. Указанная информация содержала сведения о, так называемых, «проблемных» клиентах последних и представляла интерес в деятельности таких хозяйствующих субъектов. Обобщенную и систематизированную под его руководством информацию Е. в виде компьютерных баз данных за денежное вознаграждение реализовывал представителям таких организаций, получая тем самым стабильный доход.

Затем Е., желая обеспечить наибольший спрос реализовываемых им компьютерных данных, решил усовершенствовать последние путем внесения в них охраняемой законом компьютерной информации, содержащей сведения о персональных данных неопределенного числа граждан, сведения

[1] Приговор Кательниковского районного суда № 1-11/2018 от 23 мая 2018 г. по делу № 1-122/2017 [Электронный ресурс]: Судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/uYUyZdOitVJ3/?regular/ (дата обращения 12.04.2019 г.).

о которых имелись в базах данных Информационного центра УМВД России по Курганской области. Осознавая, что реализовать задуманное ему не под силу, он решил создать подчиненную ему организованную группу.

Для реализации своих преступных намерений Е. привлек в качестве члена организованной преступной группы Д., которому как бывшему начальнику ИЦ УМВД России по Курганской области, имеющему знакомых среди сотрудников данного структурного подразделения органа внутренних дел, за денежное вознаграждение предложил подыскать среди последних соучастника, который с использованием своего служебного положения осуществит неправомерный доступ к базам данных ИЦ УМВД по Курганской области, содержащим информацию о персональных данных неопределенного числа граждан, их копирование на внешний накопитель информации, и передачу последнего Е. через Д. также за денежное вознаграждение.

После этого Д. подобрал в качестве непосредственного исполнителя преступления и члена указанной преступной группы ранее знакомого ему П., который в соответствии с приказом начальника УМВД России по Курганской области занимал соответствующую должность в ИЦ УМВД России по Курганской области. Затем в один из периодов П. осуществил неправомерный доступ к базам данных и копирование интересующей компьютерной информации на твердотельный накопитель и за денежное вознаграждение передал Д[1].

Таким образом, на основе всего вышеизложенного в настоящей главе можно сделать следующий вывод. Соотношение категорий «информация» и «информационные технологии можно рассматривать с нескольких аспектов. Так, информация не существует сама по себе, она проявляется в информационных процессах. Информационные процессы могут быть

[1] Приговор Кетовского районного суда № 1-730/2017 от 29 мая 2017 г. по делу № 1-730/2017 [Электронный ресурс]: Судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/Z7ltwZeNI9bC/?regular/ (дата обращения 12.04.2019 г.).

целенаправленными или стихийными, организованными или хаотичными, детерминированными или вероятностными. Следует обратить внимание, что информационный процесс всегда протекает в какой-либо информационной системе. Наиболее общими информационными процессами являются три процесса: сбор, преобразование, использование информации.

То есть, информационные технологии представляют собой определенный порядок выполнения операций, действий по переработке первоначальной информации с целью предоставления ее для пользователя в определенном виде. Следовательно, информационные технологии взаимодействуют с информационными системами, которые, в свою очередь, включают в себя информационные процессы (сбор, преобразование и использование информации).

На данный момент возникла проблема, когда наиболее отчетливо проявился разрыв между объемом информации в обществе и возможностями отдельного человека в ее освоении. Впервые в истории человечества большинство социальных процессов приобрели ярко выраженную особенность информационных, то есть не просто связанных с операциями извлечения информации, ее трансляции в пространстве и времени, а в большой степени – с избирательным отношением человека к информации, с потребностью в специальных инструментах, которую будут способствовать получению и обработке информации.

В данном контексте не стали исключением и правоохранительные органы. Преступники все чаще стали использовать информационные технологии как средство и орудие совершения преступлений. Кроме того, и сами сотрудники органов внутренних дел используют их для сокрытия средств, добытых преступным путем. В связи с этим возникает потребность в разработке тактики и методов раскрытия подобных преступлений.

2 ВЫЯВЛЕНИЕ И РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕНОЛОГИЙ СОТРУДНИКАМИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

2.1 Особенности расследования преступлений, совершаемых сотрудниками органов внутренних дел

Существенное значение в структуре криминалистической методики расследования преступлений, совершаемых сотрудниками органов внутренних дел, имеет криминалистическая характеристика предварительного расследования. Так, А.А. Бессонов данное понятие определяет как «систему обобщенных сведений, отражающих закономерности механизма раскрытия и расследования преступлений данной категории, а именно: деятельности правоохранительных органов на различных этапах предварительного следствия по доказыванию факта совершения сотрудником ОВД преступлений, по взаимодействию субъектов доказывания в ходе совместного решения задач уголовного судопроизводства»[1].

Криминалистическую характеристику предварительного расследования по данной категории преступлений можно представить как систему, состоящую из следующих элементов:

– криминалистические ситуации и версии;

– направления раскрытия и расследования, складывающиеся на этапе проверки сообщения о преступлении, на первоначальном и последующем этапах;

– совокупность следственных действий и оперативно-розыскных мероприятий;

– система организационно-технических и тактических операций.

[1] Бессонов А.А. О сущности криминалистической характеристика преступлений // Правовое регулирование в современной России. – 2014. – № 1. – С. 46.

Так, версии расследования фактов совершения сотрудниками полиции преступлений строятся, основываясь на юридических, фактических обстоятельствах и данных криминалистической характеристики данных преступлений, личности преступника.

Рассмотрение криминалистических ситуаций является важным компонентом расследования данной категории преступлений, так как это деятельность позволяет дифференцировать все многообразие ситуаций, возникающих в процессе преступной и правоприменительной деятельности, и составить практические рекомендации, способные оптимизировать процесс расследования. В зависимости от источника информации о факте совершения сотрудников полиции преступлений можно выделить следующие криминалистические ситуации:

1) информация о готовящемся или совершенном преступлении была получена оперативным путем;

2) информация о коррупционной деятельности сотрудника полиции получена от лица, в отношении которого планируется, или совершено преступление коррупционной направленности и которое готово оказать помощь правоохранительным органам в изобличении коррумпированного сотрудника органов внутренних дел;

3) есть факт совершения преступления, и задержан подозреваемый в совершении данного преступного деяния.

Определившись с версиями и криминалистическими ситуациями необходимо определить общее направление раскрытия и расследования преступного деяния.

Проверка сообщения о готовящемся или совершенном преступлении данной категории весьма затруднительна, что связано с несколькими причинами. Зачастую правоохранительные органы обладают недостаточной информацией, также возникает дефицит времени, в течение которого должно быть принято решение, каким путем получить и закрепить доказательства преступной деятельности.

Важной особенностью выступает характеристика личности преступника: наличие юридических знаний, служебное положение, опыт, связанный с расследованием подобных преступлений, а также связи с иными сотрудниками правоохранительных органов. В связи с этим, сотрудник органов внутренних дел имеет возможность тщательно подготовить и спланировать совершение преступления, а также принять все необходимые меры к маскировке и сокрытию следов своих преступных действий. Кроме того, при изобличении преступников в структуре полиции может возникать существенное сопротивление как со стороны самого подозреваемого, так и со стороны его сослуживцев и коллег.

Все перечисленные особенности свидетельствуют о том, что при расследовании данной категории преступлений важным фактором выступает сбор первоначальной информации, а также тщательная ее проверка. Как пишет в своей работе А.Н. Калюжный: «анализ судебно-следственной практики показывает, что именно на этапе проверки информации о подготавливаемом или совершенном сотрудником органов внутренних дел преступлений, проводимой преимущественно в условиях строгой конспирации и заключающейся в документировании деятельности подозреваемого лица, происходит сбор базовой доказательственной информации, определяющей судебную перспективу уголовного дела»[1].

Представляет интерес информация, размещенная в работе В.Ф. Луговик. Так, согласно опросу оперативных сотрудников СБ ОВД РФ при расследовании преступлений, совершаемых сотрудниками органов внутренних дел наиболее часто проводятся следующие оперативно-розыскные мероприятия:

– наведение справок (67, 3%);

– наблюдение (86,8%);

– опрос (78,8%);

[1] Калюжный А.Н. Предварительная проверка сообщений о преступлениях: понятие и этапы производства // Юридическая наука. – 2013. – № 1. – С. 61.

– прослушивание телефонных переговоров (67,3%);

– оперативный эксперимент (88,2%);

– обследование помещений, зданий, сооружений, участков местности и транспортных средств (76,4%);

– снятие информации с технических каналов связи (59,2%);

– контроль почтовых отправлений, телеграфных и иных сообщений (68,8%)[1].

Проведение оперативно-розыскных мероприятий и следственных действий по преступлениям, совершаемых сотрудниками органов внутренних дел, также имеет некоторые особенности. Так, если речь идет о ситуации, при которой расследование производит сотрудник СБ ОВД, то, скорее всего, подозреваемый будет настроен враждебно. Следовательно сотруднику СБ ОВД следует перебороть у своего оппонента предубеждение к своей личности путем обнаружения им сходства общих жизненных принципов, потребностей и т.д.

В качестве еще одной особенности можно считать особый психологический климат в коллективе сотрудников органов внутренних дел. Речь, прежде всего, идет о некотором страхе подчиненных перед руководителем, что обусловлено каждодневной субординацией и повышенным конформизмом. Следовательно, при привлечении к ответственности руководителя определенного подразделения мала вероятность того, что кто-либо из сотрудников будет сотрудничать при расследовании такого преступления[2].

Проанализировав изложенное выше, можем сделать вывод, что первостепенное значение имеет первоначальный этап расследования преступлений, совершаемых сотрудниками органов внутренних дел,

[1] Луговик В.Ф. Оперативно-розыскная деятельность органов внутренних дел: перспективы совершенствования правового регулирования // Вестник Воронежского института МВД России. – 2015. – № 4. – С. 8

[2] Покозий В.В. Отдельные вопросы привлечения сотрудников органов внутренних дел к ответственности // Вестник Московского университета МВД России. – 2017. – № 2. – С. 196.

поскольку именно на данной стадии происходит закрепление доказательств, которые впоследствии составят базу обвинения. Последующий этап расследования преступлений данной категории характеризуется проведением следственных действий уточняющего и дополняющего характера, позволяющих устранить имеющиеся противоречия между отдельными доказательствами. По результатам последующего этапа расследования должна быть создана цельная система доказательств вины сотрудника полиции, на основании которой суд сможет вынести законное, справедливое и обоснованное решение.

2.2 Способы сокрытия средств, добытых преступным путем сотрудниками органов внутренних дел, с использованием информационных технологий

Борьбе с сокрытием средств, добытых преступным путем, уделяется большое внимание не только в России, но и во всем мире. Каждое государство разрабатывает собственную законодательную и социально-экономическую основу по противодействию легализации преступных доходов.

Основным нормативным правовым актом в данной сфере является Федеральный закон от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[1]. Согласно данному нормативному правовому акту в качестве доходов, полученных преступным путем, выступают денежные средства или иное имущество, полученные в результате совершения преступления. Легализацией доходов, полученных преступным путем, признается придание правомерного вида владению, пользованию или

[1] О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: Федеральный закон от 07.08.2001 г. № 115-ФЗ (с изм. и доп., вступ. в силу с 30.10.2018 г.) // СПС Консультант плюс.

распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления.

Легализация преступных доходов является сложным и многоэтапным процессом, состоящим из множества финансовых операций. С этой целью используются различные техники, средства, приемы и способы, которые призваны исказить информацию об источниках денежных средств и имущества, ввести их в легальную сферу экономики.

Преступные доходы, как правило, образуются одним из следующих способов:

– путем создания или приобретения в результате свершения преступления вне легального хозяйственного оборота, то есть в криминальном секторе теневой экономики;

– путем выведения из легального хозяйственного оборота в криминальный сектор теневой экономики в результате совершения противоправного деяния, а затем введения вновь легальный хозяйственный оборот.

В качестве способа легализации средств, добытых преступным путем сотрудниками органов внутренних дел с использованием информационных технологий, выступает перемещение за границу, преимущественно в оффшорные зоны, и инвестирование в экономику зарубежных государств.

Определение оффшорной зоны можно найти в работе П.В. Палова: «оффшорная зона – территория, на которой юридически закреплены низкие налоги, либо полностью отсутствующее налогообложение для компаний определенного типа, а также существует упрощенная система регистрации юридических лиц и, как правило, созданы условия для относительно анонимного ведения бизнеса»[1].

[1] Павлов П.В. Оффшорная зона как особая территория осуществления финансово-экономической деятельности: некоторые вопросы правового регулирования // Известия вузов. Северо-Кавказский регион. – 2010. – № 1. – С. 104.

Использование оффшорных зон для сокрытия преступных доходов обусловлено несколькими обстоятельствами:

– возможность использования номинальных акционеров и директоров, что позволяет скрыть лицо истинного владельца акций;

– возможность дополнительной защиты прав акционеров;

– возможность снижать налоговые затраты либо вовсе избегать их.

Отмывание денежных средств, полученных преступным путем сотрудниками органов внутренних дел в оффшорных юрисдикциях осуществляется с помощью финансовых или нефинансовых институтов при помощи различных схем с использованием для обналичивания денег оффшорных «технологических» компаний, фирм-посредников, сети Интернет, небанковских систем перевода денежных средств, совершением различных трансграничных сделок. Глобализация финансовых рынков позволяет модифицировать схемы по отмыванию доходов, облегчает сам процесс легализации, поскольку нивелируются границы между внутренними и внешними источниками незаконного капитала.

Примером сокрытия денежных средств, добытых преступным путем сотрудниками органов внутренних дел, с использованием информационных технологий может служить создание бизнеса в оффшорной зоне через сеть Интернет. Для конфиденциальности бизнеса приобретается номинальный сервис – номинальный директор и номинальный акционер. Эти люди, как правило, резиденты соответствующей оффшорной юрисдикции, являются номинальными лицами в бизнесе, прикрывая собой имена реальных владельцев и директоров компании. Это всегда проверенные люди, работающие на профессиональной основе и берущие за этого деньги.

Реальный владелец бизнеса (в нашем случае – сотрудник органов внутренних дел, совершивший преступление) защищен от возможных незаконных действий номинального директора документом «Declaration of Trust», которые подписывает последний, отказываясь от права реального управления компанией и обязуясь не подписывать никакие документы без

ведома бенефициара (владельца) компании. Номинальный акционер подписывает документ «Share Transfer», по которому отказывается от номинального права владения долей бизнеса в пользу владельца.

При этом также не выезжая за границу, через интернет возможно открыть мерчант-аккаунт – особый торговый счет, который позволяет принимать платежи банковских карт и банковских счетов клиентов через интернет. Преимущества данного счета заключается в том, что отсутствует валютный контроль и финансовый мониторинг, нет требований по оформлению паспорта сделки, оптимизация налогообложения. Открытие мерчант-аккаунта на оффшорную компанию позволяет вести бесконтрольный и безналоговый бизнес по всему миру.

Полагается, что эффективной мерой по борьбе с легализацией преступных доходов, полученных сотрудниками органов внутренних дел с использованием информационных технологий, является улучшение условий для привлечения независимого финансирования журналистских расследований в данной сфере.

2.3 Развитие информационных технологий, и их использование в расследовании и предупреждении преступлений, совершаемых сотрудниками органов внутренних дел

Применение информационных средств и компьютерной техники в раскрытии и расследовании преступлений представляет собой систему повседневной деятельности следователей, специалистов-криминалистов, сотрудников органов дознания, связанную с применением автоматизированных систем, специализированных программ. Организация этой деятельности должна основываться на четких и последовательных комплексах действий сотрудников, направленных на планирование следственных действий и оперативно-розыскных мероприятий с применением компьютерных средств и информационных компонентов этих

действий и мероприятий. Применение информационных технологий должно быть нацелено на получение, накопление и обработку значимой информации.

Следователь в процессе осуществления своих полномочий сталкивается с большим объемом информации, из которой необходимо выделять сведения, значимые для конкретного расследуемого уголовного дела. Данная деятельность осложняется трудностями, возникающими при получении данных из различных источников при дефиците времени. Особенно ярко это проявляется при расследовании многоэпизодных уголовных дел, в которых фигурируют члены организованных преступных групп и сообществ в сфере экономической деятельности, когда следователю необходимо выявлять межрегиональных и международные преступные связи. Такие задачи не могут быть решены без отлаженного информационно-аналитического обеспечения.

Так, в настоящее время компьютерные технологии позволяют сформировать образ подозреваемого или обвиняемого. К примеру, с помощью компьютерной программы «Формер» возможно обеспечить высокую информативность сбора криминалистических данных при расследований убийств.[1] Данная программа способна сформировать круг лиц, подлежащих проверке на причастность к конкретному совершенному преступлению, сформировать криминалистические версии, что позволяет оперативно сформулировать задания сотрудникам органа дознания.

Такие операции производятся путем анализа аналогичных преступлений в компьютерной базе данных. То есть следователь путем применения метода аналогии может просмотреть уголовные дела как находящиеся в производстве, так и занесенные в архив. Поиск производится путем простой сортировки уголовных дел по признакам пола, возраста жертвы, способу убийства, сокрытия следов преступления.

[1] Толстолуцкий В.Ю. Использование информационных технологий в раскрытии и расследовании убийств: учебное пособие. – Нижний Новогород, 2015. – С. 151.

Особенно перспективным является использование информационных технологий при расследовании и предупреждении преступлений коррупционной направленности, совершаемых сотрудниками органов внутренних дел. Зарубежная практика борьбы с коррупций в системе исполнительных органов государственной власти показывает, что использование информационных технологий обеспечивает существенную экономию финансовых средств[1].

Так, на федеральном и региональном уровне для усиления роли информационных технологий в антикоррупционной практике в системе органов внутренних дел целесообразно улучшать условия для привлечения независимого финансирования журналистских расследований. К примеру, государство может предоставлять определенные налоговые льготы и финансовую поддержку независимым редакциям и организациям, осуществляющим расследования коррупционных схем и преступлений среди сотрудников правоохранительных органов, используя Интернет.

Возможно создание онлайн платформ, на которых простые граждане могут как лично, так и анонимно размещать информацию, представлять доказательства и свидетельства коррупционных действия со стороны сотрудников полиции. Кроме того, важным направлением может стать мониторинг доходов сотрудников органов внутренних дел и их членов семьи путем выявления аномального поведения в электронных операциях и анализа социальных сетей.

Представляет интерес также привлечение общественности в решении вопросов привлечения сотрудников полиции к ответственности за коррупцию. Так, обсуждение в социальных сетях фактов совершения взяточничества, систематическая публикация информации в сети Интернет о фактах коррупции, а также о расхождении в доходах и расходах будет

[1] Булгакова Е.В. Механизмы электронного государства по противодействию коррупции // Правовая информатика. – 2016. – № 1. – С. 23.

сдерживать сотрудников органов внутренних дел от коррупционных действий.

Примером широкого применения информационных технологий при предупреждении совершения коррупционных преступлений сотрудниками правоохранительных органов может служить опыт Индии. Так, в 2009 году был создан правительственный департамент «Центральная наблюдательная Комиссия», в обязанность которой входил прием и обработка жалоб, связанных с коррупцией. Произведя проверку таких сообщений граждан, данный департамент опубликовал на своей сайте список коррумпированных чиновников и сотрудников полиции. До публикации этого списка многие рекомендации правительственной комиссии со стороны коррупционеров просто игнорировались. Однако получив подобное общественное порицание, от чиновников и сотрудников полиции были получении многочисленные просьбы снять их фамилии под обещание того, что они исправятся[1].

Широкое использование информационных технологий в расследовании преступлений наиболее полно может реализоваться при создании специализированных отделов компьютерного обеспечения в системе правоохранительных органов. Так, к примеру, И.Н. Яковенко в своих трудах предлагает следующее: «необходима реализация концепции построения системы управления, контроля, организации процесса расследования по вертикальному принципу, что означает контроль процессуальных документов нижестоящих органов вышестоящими»[2]. Данные отделы полиции смогут обеспечивать систему моделирования нестандартных ситуаций, учитывать альтернативные решения сотрудников полиции на основе диагностики предложенных вариантов, а также предоставлять информацию в удобной для восприятия форме.

[1] Слонская М.С. Коррупция в Индии: масштабы и методы борьбы с ней // Азия и Африка. – 2015. – № 7. – С. 33.
[2] Яковенко И.Н. Современное состояние и перспективы использования информационных технологий в расследовании преступлений // Наука и право. – 2014. – № 2. – С. 61.

Развитие информационных технологий в расследовании и предупреждении преступлений возможно также путем технологизации криминалистической подготовки сотрудников правоохранительных органов. В данном направлении наше государство в некоторой степени отстает от развитых зарубежных стран, однако обладает значительным творческим и научным потенциалом. Так, Н.Н. Федотов пишет: «особенности советской системы высшего образования, особенно ее исследовательский уклон в подготовке кадров привели к тому, что российские специалисты отличаются от западных креативностью, способностью быстро осваивать новые знания, критичностью мышления – это как раз то, что требуется для успешного совершения компьютерных преступлений и их раскрытия»[1].

Успешным примером может служить следующий практический случай. Так, в Волгоградской академии МВД России зарекомендовала себя с положительной стороны и доказала эффективность работа лабораторий учебно-научных комплексов экспертно-криминалистической деятельности узкоспециализированных лабораторий кафедр экспертного профиля. Слушатели и курсанты данного заведения с неподдельным интересом посещают данные занятия, принимая в их проведении активное участие, так как понимают важность такого обучения в будущей профессиональной деятельности. На основе разработанного учебного комплекса курсанты и слушатели индивидуально и коллективно выполняют научно-исследовательские работы, решая при этом научные проблемы. Кроме того, важным стимулом выступает возможность подавать заявки для получения патентов на полезные изобретения и внедрять результаты своих исследований в экспертную практику.

Не стоит забывать и о подготовке специалистов в области судебной компьютерно-технической экспертизы. Нельзя не отметить ценность приобретаемых ими в процессе обучения специальных познаний, так как их заключение можно использовать в качестве доказательства по уголовному

[1] Федотов Н.Н. Форензика – компьютерная криминалистика. – М., 2013. – С. 26.

делу. Криминалистика на данной этапе развития должна уделять большое внимание исследованию иных следов, связанных с информационными технологиями.

Таким образом, с целью совершенствования использования информационных технологий в расследовании и предупреждении преступлений, совершаемых сотрудниками органов внутренних дел, предлагаются следующие организационные меры:

– разработка универсальной концепции развития информационных технологий в криминалистике;

– своевременная переподготовка и повышение квалификации действующих сотрудников в сфере расследования преступления, связанных с использованием информационных технологий;

– качественное мотивирование сотрудников правоохранительных органов к эффективному использованию новых технологий на практике;

– создание онлайн платформ, на которых простые граждане как лично, так и анонимно могли бы оставлять жалобы на действующих сотрудников органов внутренних дел;

– создание специализированных отделов компьютерного обеспечения в полиции, в компетенцию которых входит обеспечение системы моделирования нестандартных ситуаций, оценивание решений сотрудников, основываясь на диагностике предложенных вариантов, предоставление информации в удобной для восприятия форме;

– улучшение условий для привлечения независимого финансирования журналистских расследований, связанных с раскрытием путей и каналов легализации денежных средств с использованием информационных технологий, добытых преступным путем сотрудниками полиции.

ЗАКЛЮЧЕНИЕ

Проведенное исследование проблем расследования преступлений, совершаемых с использованием информационных технологий сотрудниками органов внутренних дел, позволяет сделать некоторые выводы:

1. Соотношение категорий «информация» и «информационные технологии можно рассматривать с нескольких аспектов. Так, информация не существует сама по себе, она проявляется в информационных процессах. Информационные процессы могут быть целенаправленными или стихийными, организованными или хаотичными, детерминированными или вероятностными. Следует обратить внимание, что информационный процесс всегда протекает в какой-либо информационной системе. Наиболее общими информационными процессами являются три процесса: сбор, преобразование, использование информации. То есть, информационные технологии представляют собой определенный порядок выполнения операций, действий по переработке первоначальной информации с целью предоставления ее для пользователя в определенном виде. Следовательно, информационные технологии взаимодействуют с информационными системами, которые, в свою очередь, включают в себя информационные процессы (сбор, преобразование и использование информации).

2. На данный момент возникла проблема, когда наиболее отчетливо проявился разрыв между объемом информации в обществе и возможностями отдельного человека в ее освоении. Впервые в истории человечества большинство социальных процессов приобрели ярко выраженную особенность информационных, то есть не просто связанных с операциями извлечения информации, ее трансляции в пространстве и времени, а в большой степени – с избирательным отношением человека к информации, с потребностью в специальных инструментах, которую будут способствовать получению и обработке информации. В данном контексте не стали исключением и правоохранительные органы. Преступники все чаще стали

использовать информационные технологии как средство и орудие совершения преступлений. Кроме того, и сами сотрудники органов внутренних дел используют их для сокрытия средств, добытых преступным путем. В связи с этим возникает потребность в разработке тактики и методов раскрытия подобных преступлений.

3. В настоящее время правовая основа раскрытия и расследования преступлений, совершаемых с использованием информационных технологий, отстает от уровня развития общественных отношений. В целях совершенствования регулирования раскрытия и расследования данной категории преступлений предлагается внести ряд изменений в УПК РФ, в частности п. 2.1 статьи 37 УПК РФ изложить следующим образом: «2.1. По мотивированному письменному (электронному) запросу прокурора ему предоставляется возможность ознакомиться с материалами находящего в производстве уголовного дела. В случае электронного запроса необходимо использование электронно-цифровой подписи». Также дополнить ст. 5 п. 63 следующего содержания: «63) электронно-цифровая подпись (электронная подпись) – это информация в электронной форме, совмещенная с подписываемой информацией и (или) иным образом связанная с ней, используемая для идентификации лица, подписывающего информацию». Кроме того, считаем необходимым дополнить главу 10 ст. 84.1 УПК РФ «Электронная информация» (Приложение 1).

4. Раскрытие и расследование преступлений, совершаемых сотрудниками полиции, обладает некоторыми особенностями. К примеру, проведение оперативно-розыскных мероприятий и следственных действий по преступлениям. Так, если речь идет о ситуации, при которой расследование производит сотрудник СБ ОВД, то, скорее всего, подозреваемый будет настроен враждебно. Следовательно сотруднику СБ ОВД следует перебороть у своего оппонента предубеждение к своей личности путем обнаружения им сходства общих жизненных принципов, потребностей и т.д.

Психологический климат в коллективе сотрудников органов внутренних дел также влияет на ход расследования. Речь, прежде всего, идет о некотором страхе подчиненных перед руководителем, что обусловлено каждодневной субординацией и повышенным конформизмом. Следовательно, при привлечении к ответственности руководителя определенного подразделения мала вероятность того, что кто-либо из сотрудников будет сотрудничать при расследовании такого преступления.

5. В качестве основного способа легализации преступных средств с применением информационных технологий является использование оффшорных зон. Основным нормативным правовым актом, регулирующим данные вопросы, выступает Федеральный закон Российской Федерации от 07.08.2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Полагается, что эффективной мерой по борьбе с легализацией преступных доходов данным способом может являться улучшение условий для привлечения независимого финансирования журналистских расследований .

6. с целью совершенствования использования информационных технологий в расследовании и предупреждении преступлений, совершаемых сотрудниками органов внутренних дел, предлагаются следующие организационные меры:

– разработка универсальной концепции развития информационных технологий в криминалистике;

– своевременная переподготовка и повышение квалификации действующих сотрудников в сфере расследования преступления, связанных с использованием информационных технологий;

– качественное мотивирование сотрудников правоохранительных органов к эффективному использованию новых технологий на практике;

– создание онлайн платформ, на которых простые граждане как лично, так и анонимно могли бы оставлять жалобы на действующих сотрудников органов внутренних дел;

– создание специализированных отделов компьютерного обеспечения в полиции, в компетенцию которых входит обеспечение системы моделирования нестандартных ситуаций, оценивание решений сотрудников, основываясь на диагностике предложенных вариантов, предоставление информации в удобной для восприятия форме;

– улучшение условий для привлечения независимого финансирования журналистских расследований, связанных с раскрытием путей и каналов легализации денежных средств с использованием информационных технологий, добытых преступным путем сотрудниками полиции.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

РАЗДЕЛ I. НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ И ИНЫЕ ОФИЦИАЛЬНЫЕ АКТЫ

1. Конвенция Организации Объединенных наций против коррупции. // URL: http://www.un.org/ru/documents/decl_conv/conventions/corruption.shtml.
2. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 года) // СПС Консультант плюс.
3. Кодекс поведения должностных лиц по поддержанию правопорядка. // URL: http://www.un.org/ru/documents/decl_conv/conventions/code_of_conduct.shtml.
4. Декларация о преступности и правосудии: ответы на вызовы XXI века. // URL: http://www.un.org/ru/documents/decl_conv/declarations/vendec.shtml.
5. О типовых проектах законодательных актов МПА ЕврАзЭС в сфере информационных технологий: постановление от 24.05.2008 г. №5-20 // СПС Консультант плюс.
6. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 года // Российская газета. – 1993. – 25 декабря.
7. О полиции: Федеральный закон от 07.02.2011 г. № 3-ФЗ (с изм. и доп., вступ. в силу с 01.04.2019 г.) // СПС Консультант плюс.
8. О противодействии коррупции: Федеральный закон от 25.12.2008 г № 273-ФЗ (с изм. и доп., вступ. в силу с 30.10.2018 г.) // СПС Консультант плюс.
9. Об антикоррупционной экспертизе нормативных правовых актов и проектов нормативных правовых актов: Федеральный закон от 17.07.2009 г. № 172-ФЗ (с изм. и доп., вступ. в силу с 11.10.2018 г.) // СПС Консультант плюс.

10. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 г. № 149-ФЗ (с изм. и доп., вступ. в силу с 30.10.2018 г.) // СПС Консультант плюс.
11. О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма: Федеральный закон от 07.08.2001 г. № 115-ФЗ (с изм. и доп., вступ. в силу с 27.12.2018 г.) // СПС Консультант плюс.
12. Об электронной подписи: Федеральный закон от 06.04. г. № 1-ФЗ (с изм. и доп., вступ. в силу с 28.07.2018 г.) // СПС Консультант плюс.
13. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 07.12.2011 г. № 420-ФЗ // Российская газета. – 2011. – 8 декабря.
14. О концепции правовой информатизации России: указ Президента РФ от 28.061993 г. № 966 // Российские вести. – 1993. – 13 июля.

РАЗДЕЛ II. МОНОГРАФИИ, УЧЕБНИКИ, УЧЕБНЫЕ ПОСОБИЯ

15. Боннер, А.Т. Проблемы установления истины в гражданском процессе: монография. / А.Т. Боннер. – СПб., 2009. – С. 470.
16. Волевод А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волевод. – М., 2012. – С. 73.
17. Иванов, Н.А. Теоретические и методические основы судебной компьютерно-технической экспертизы документов: дисс… к.ю.н. / Н.А. Иванов. – Москва, 2005. – С. 54.
18. Кукарникова, Т.Э. Электронный документ в уголовном процессе и криминалистике: дисс… к.ю.н. / Т.Э. Кукарникова. – Саратов, 2003. – С.67.
19. Латышев, Д.С. Краткий обзор информационных технологий, используемых в юридической деятельности / Д.С. Латышев //

Международный научный журнал «Инновационная наука». – 2016. – № 4. – С. 55-58.

20. Лисиченко, В.К. Криминалистическое исследование документов: (правовые и методологические проблемы): дисс… д-ра юрид. наук. / В.К. Лисиченко. – Киев, 1973. – С. 105.

21. Нарижный, А.В. Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий: дисс. … канд. юрид. наук. / А.В. Нарижный. – Краснодар. 2009. – С. 53.

22. Толстолуцкий, В.Ю. Использование информационных технологий в раскрытии и расследовании убийств: учебное пособие / В.Ю. Толстолуцкий. – Нижний Новогород, 2015. – С. 151.

23. Федотов, Н.Н. Форензика – компьютерная криминалистика / Н.Н. Федотов. – М., 2013. – С. 26.

24. Юрген, П.Г. Преступления в Интернете. Полномочия и границы органов расследования // Переводы материалов о практике деятельности правоохранительных органов зарубежных стран / П.Г. Юрген. – М., 2013. – С. 49.

25. Яковлев, А.Н. Теоретические и методические основы экспертного исследования документов на машинных носителях информации: дисс.. к.ю.н. / А.Н. Яковлев. – Саратов, 2000. – С. 61.

РАЗДЕЛ III. КОММЕНТАРИИ К ЗАКОНОДАТЕЛЬСТВУ, НАУЧНЫЕ ПУБЛИКАЦИИ

26. Бессонов, А.А. О сущности криминалистической характеристика преступлений / А.А.Бессонов // Правовое регулирование в современной России. – 2014. – № 1. – С. 46.

27. Булгакова, Е.В. Механизмы электронного государства по противодействию коррупции / Е.В. Булгакова // Правовая информатика. – 2016. – № 1. – С. 23.

28. Дашян, М.А. Обзор Конвенции Совета Европы о киберпреступности / М.А. Дашян // Современное право. – 2002. – № 11. – С. 23.

29. Калюжный, А.Н. Предварительная проверка сообщений о преступлениях: понятие и этапы производства / А.Н. Калюжный // Юридическая наука. – 2013. – № 1. – С. 61.

30. Луговик, В.Ф. Оперативно-розыскная деятельность органов внутренних дел: перспективы совершенствования правового регулирования / В.Ф. Луговик // Вестник Воронежского института МВД России. – 2015. – № 4. – С. 8

31. Осипенко, А.Л. Особенности расследования сетевых компьютерных преступлений / А.Л. Осипенко // Российский юридический журнал. – 2010. – № 2. – С. 121-126.

32. Павлов, П.В. Оффшорная зона как особая территория осуществления финансово-экономической деятельности: некоторые вопросы правового регулирования / П.В. Павлов // Известия вузов. Северо-Кавказский регион. – 2010. – № 1. – С. 104.

33. Покозий, В.В. Отдельные вопросы привлечения сотрудников органов внутренних дел к ответственности / В.В. Покозий // Вестник Московского университета МВД России. – 2017. – № 2. – С. 196.

34. Семизорова, Е.В. Актуальные вопросы правового регулирования обеспечения юридической значимости электронных документов Е.В. Семизорова // Российская юстиция. – 2011. – № 2. – С. 46.

35. Слонская, М.С. Коррупция в Индии: масштабы и методы борьбы с ней / М.С. Слонская // Азия и Африка. – 2015. – № 7. – С. 33.

36. Федосеева, Н.Н., Шилова, Д.А. Понятие и сущность электронного документа / Н.Н. Федосеева, Д.А. Шилова // Юрист. – 2008. – № 5. – С. 58.

37. Чернышев, П.М. Информационные технологии в юридической деятельности / П.М. Чернышев // Марийский юридический вестник. – 2016. – № 2. – С. 63.
38. Яковенко, И.Н. Современное состояние и перспективы использования информационных технологий в расследовании преступлений / И.Н. Яковенко // Наука и право. – 2014. – № 2. – С. 61.

РАЗДЕЛ IV. СУДЕБНАЯ ПРАКТИКА

39. Бюллетень международных договоров. – 2009. – № 6. – С. 12-17
40. Приговор Кательниковского районного суда № 1-11/2018 от 23 мая 2018 г. по делу № 1-122/2017 [Электронный ресурс]: Судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/uYUyZdOitVJ3/?regular/ (дата обращения 12.04.2019 г.).
41. Приговор Кетовского районного суда № 1-730/2017 от 29 мая 2017 г. по делу № 1-730/2017 [Электронный ресурс]: Судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/Z7ltwZeNI9bC/?regular/ (дата обращения 12.04.2019 г.).

РАЗДЕЛ V: ЭЛЕКТРОННЫЕ РЕСУРСЫ

42. Сайт Судебного департамента при Верховном Суде Российской Федерации [Электронный ресурс] // URL: http://www.cdep.ru/index.php?id=150 (дата обращения 12.05.2019 г.).
43. Деловой журнал «Инвест-Форсайт» [Электронный ресурс] // URL: https://www.if24.ru/vojdut-li-v-modu-kriptovzyatki/ (дата обращения 24.03.2019 г.).

44. Официальный сайт Министерства труда и социальной защиты Российской Федерации [Электронный ресурс] // URL: https://rosmintrud.ru/docs (дата обращения 03.04.2019 г.).
45. Официальный сайт Национального Антикоррупционного Совета Российской Федерации [Электронный ресурс] // URL: http://www.korupcii.net/index.php?s=3 (дата обращения 03.04.2019 г.).

ПРИЛОЖЕНИЕ 1

Проект Федерального закона

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙЗАКОН

О ВНЕСЕНИИ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ В УГОЛОВНО-ПРОЦЕССУАЛЬНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 1. Внести в Уголовно-процессуальный кодекс Российской Федерации (Собрание законодательства Российской Федерации, 2006, № 23, ст. 2379, № 31, ст.34522007, № 1, ст. 46; № 16, ст. 1827; № 18, ст. 2118; 2008, № 12, ст. 1074; № 24, ст. 2798; № 49, ст. 5724; 2009, № 1, ст. 29; № 11, ст. 1267; № 18, 2010, № 1, ст. 4; № 8, ст. 780; № 11, ст. 1168; № 11, ст. 1169; № 15, ст. 1756; № 17, ст. 1985; 2011, № 1, ст. 16; № 1, ст. 39; № 1, ст. 45; № 1, ст. 46; № 7, ст. 901; № 45, ст. 6322; 2012, № 44, ст. 5641; 2014, № 19, ст. 2303, 2335; № 30, ст. 4228, 4259; № 48, ст. 6651; 2015, № 27, ст. 3983) следующие изменения и дополнения:

1. Изложить п. 2.1 статьи 37 следующим образом: «2.1. По мотивированному письменному (электронному) запросу прокурора ему предоставляется возможность ознакомиться с материалами находящего в производстве уголовного дела. В случае электронного запроса необходимо использование электронно-цифровой подписи».

2. Дополнить ст. 5 п. 63 следующего содержания: «63) электронно-цифровая подпись (электронная подпись) – это информация в электронной форме, совмещенная с подписываемой информацией и (или) иным образом связанная с ней, используемая для идентификации лица, подписывающего информацию».

3. В ч. 2 ст. 74 внести пункт 8 следующего содержания:

«электронная информация»

4. Дополнить Главу 10 ст. 84.1 УПК РФ и изложить ее так:

«Статья 84.1 Электронная информация

1. Электронная информация допускаются в качестве доказательств, если изложенные в них сведения имеют значение для установления обстоятельств, указанных в статье 73 настоящего Кодекса.

2. Электронная информация может содержать сведения, зафиксированные на фото-, аудио- и видео- и иных электронных носителях информации, полученных, истребованных или представленных в порядке, установленном статьей 86 настоящего Кодекса.

3. Электронная информация признается доказательством, о чем выносится соответствующее постановление.

4. Электронная информация приобщается к материалам уголовного дела и содержится на электронных носителях в течение всего срока его хранения. Порядок хранения электронных носителей информации устанавливается настоящей статьей и статьей 82 настоящего Кодекса. Электронные носители информации, содержащие скопированную информацию, возвращаются их законному владельцу изъятых электронных носителей информации или обладателю содержащейся на них информации».

Статья 2. Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

ПРИЛОЖЕНИЕ 2

ОБРАЗЕЦ АНКЕТЫ № 1

АНКЕТИРОВАНИЕ СОТРУДНИКОВ ПОЛИЦИИ

Уважаемые сотрудники полиции!

В целях получения беспристрастной информации для написания дипломной работы ***«Расследование преступлений, совершаемых с использованием информационных технологий сотрудниками органов внутренних дел» кафедра «Правоохранительной деятельности и национальной безопасности Юридического Института Южно-Уральского государственного университета (Национальный исследовательский университет)*** *проводит анкетирование. Для получения объективных результатов просим Вас ответить на ниже приведенные вопросы, выбрав один или несколько правильных, по Вашему мнению, ответов или предоставив свой вариант ответа.*

Заранее благодарим.

1. В каком отделе полиции Вы работаете?

□ следственный отдел;

□ отдел уголовного розыска;

□ Ваш вариант _____

2. Что Вы вкладываете в понятие «информационные технологии»?

□ компьютерная техника;

□ сеть Интернет;

□ социальные сети;

□ информационная безопасность;

□ телекоммуникационная сеть;

□ базы данных, информационные центры

□ Ваш вариант ответа_____

3. Считаете ли Вы, что информационные технологии полностью пронизывают социальные процессы в обществе?

□ да;

□ нет.

4. По Вашему мнению, представители каких профессий наиболее коррумпированы?

□ врачи, медицинские работники;

□ сотрудники ГИБДД;

□ работники прокуратуры;

□ судьи;

□ преподаватели ВУЗов;

□ Ваш вариант ответа_____

5. На Ваш взгляд, возможно ли применение информационных технологий сотрудником полиции с целью получения взятки?

□ да;

□ нет.

6. Считаете ли Вы, что своевременная переподготовка и повышение квалификации действующих сотрудников в сфере расследования преступлений, связанных с использованием информационных технологий, поможет качественно улучшить эффективность деятельности полиции?

□ да;

□ нет.

ПРИЛОЖЕНИЕ 3

РЕЗУЛЬТАТЫ АНКЕТИРОВАНИЯ

Результаты анкетирования

Опрошено: сотрудников ОМВД России по Кизильскому району Челябинской области – 10 чел.

№	Вопрос	Варианты ответов	Результаты, (%)
1	В каком отделе полиции Вы работаете?	а) следственный отдел; б) отдел уголовного розыска; в) ваш вариант	40 60 0
2	Что Вы вкладываете в понятие «информационные технологии»?	а) компьютерная техника; б) социальные сети; в) информационная безопасность; г) телекоммуникационная сесть ; д) базы данных, информационные центры	10 0 20 0 70
3	Считаете ли Вы, что информационные технологии полностью пронизывают социальные процессы в обществе?	а) да; б) нет	100 0
4	По Вашему мнению, представители каких профессий наиболее коррумпированы?	а) врачи, медицинские работники; б) сотрудники ГИБДД; в) работники прокуратуры; г) судьи; д) преподаватели ВУЗов; е) Ваш вариант	10 20 50 20 0 0
5	На Ваш взгляд, возможно ли применение информационных технологий сотрудником полиции с целью получения взятки?	а) да; б) нет	70 30

6	Считаете ли Вы, что своевременная переподготовка и повышение квалификации действующих сотрудников в сфере расследования преступлений, связанных с использованием информационных технологий, поможет качественно улучшить эффективность деятельности полиции?	а) да; б) нет	80 20