# ЭКСПЕРТИЗА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*К.А. Силуянова, А.А. Тебряев*
*Санкт-Петербургский политехнический университет имени Петра Великого,*
*г. Санкт-Петербург*

**Введение**

Исследование любого объекта, имеющего значение для разрешения административного, гражданского или уголовного дела, начинается с фиксации, изъятия, изучения и сопоставления полученной информации. Экспертная техника под влиянием технического прогресса претерпевает изменения в лучшую сторону и, в связи с этим в отдельных видах экспертизы появились методы, в основе которых лежат цифровые технологии, а большинство операций по обработке полученных данных выполняются при помощи электронно-вычислительной техники, компьютерных технологий, когда данные хранятся и сопоставляются в информационных базах и в информационно-справочных системах. Цифровые технические устройства очень многофункциональны, а их надежность подтверждена многими исследованиями и практикой, однако процесс оперативно-розыскных и следственных мероприятий является сложным с точки зрения как процессуального законодательства, так и специальных технических знаний, а следовательно исследование вопросов законодательства должны сопровождаться развитием взаимодействия закона и прогрессивных информационных технологий. Особенного внимания заслуживает вопрос экспертизы в сфере информационной безопасности, фиксации криминалистической информации, следов и объектов принципиально нового формата.

Объектом данного исследования являются общественные отношения, складывающиеся в процессе производства судебной экспертизы. Предметом исследования являются нормативно-правовые акты, регулирующие общественные отношения, а также, складывающиеся в процессе производства судебной экспертизы объектов и следов правонарушений и преступлений, связанных, в свою очередь, с нарушением информационной безопасности.

Цель исследования – рассмотрение проблемы применения и перспектив развития судебной экспертизы в области информационной безопасности.

Для обеспечения цели необходимо выполнить следующий ряд задач:

1. Определить понятие цифровой безопасности;
2. Исследовать носители информации как объекты экспертизы;
3. Рассмотреть соотношение понятий электронной и цифровой информации;
4. Исследовать проблемы экспертизы в сфере информационной безопасности.

Методология исследования. Проведенное исследование базируется на диалектическом методе познания объективной действительности. В нем использованы также системно-структурный, формально-юридический, сравнительно-правовой и другие частные методы научного познания.

Теоретическую основу исследования составили научные работы современных российских ученых в области экспертных исследований как Багмет А.М., Бессонов А.А., Жидко Е.А., Россинская Е.Р., Скобелин С.Ю. и других. При выполнении работы использовались достижения в области общей теории права, уголовного права, криминалистики, информатики, кибернетики и уголовно-процессуальной науки.

**Основная часть**

Для развития системы правосудия и охраны правопорядка появление цифровых технологий является существенным фактом, так как благодаря цифровизации процессуальной деятельности возможно существенно изменить скорость и объективность обработки информации по делу, повлиять на ход расследования и

вынесения объективного решения по результатам рассмотрения дела в судебном порядке. Методология раскрытия и предотвращения преступлений находится в зависимости от результатов научно-технической революции, в связи с чем вопрос технического оснащения, прежде всего, правоохранительных органов представляет для исследователей особый интерес. Рост киберпреступлений, терроризма и прогресс в области совершенствования методов сокрытия преступлений заставляет органы, осуществляющие действия по борьбе с преступностью усовершенствовать технические средства для оперативной работы. Тесное взаимодействие судебно-экспертных учреждений и правоохранительных органов может обеспечить полноту исследований различных следов и объектов, имеющих важное значение для доказательной базы по расследуемым уголовным делам. Методики судебной экспертизы в совокупности с высокотехнологичными средствами могут обеспечить рост раскрываемости преступлений. Необходимость постоянной интеграции новых технологий в деятельность экспертных учреждений, увеличению технических характеристик современного экспертного оборудования, а также установление и поддержание минимального порога соответствия технических средств являются одними из основных функций по обеспечению процессуальной деятельности [1].

Немаловажную роль в расследовании и раскрытии преступлений играет техническое оснащение правоохранительных органов. Высокотехнологическое материальное оснащение органов охраны правопорядка, отвечающее современным техническим характеристикам, является залогом успешности выполнения поставленных перед ними задач. Чем изощрённей становятся методы совершения преступлений, тем больше технических средств и научных знаний применяются для их раскрытия. Криминалистическая наука при этом наиболее востребована практикой борьбы с преступностью. Одной из важнейших задач экспертов в процессе предварительного следствия по уголовным делам является их активное участие в формировании доказательственной базы на всех этапах расследования. Однако методы криминалистической экспертизы, а также процессуальные действия требуют постоянного развития и совершенствования с целью не только выявить технологии совершения преступности, но и обеспечить достойный уровень подготовки специалистов для раскрытия принципиально новых видов преступлений.

В современном цифровизированном обществе особо возрастает уровень преступности, связанной с кибернетическим пространством и посягательством на информационную безопасность субъектов права Российской Федерации. В связи с этим законодательство нацелено на совершенствование правового регулирования по вопросам обеспечения информационной безопасности. Уголовное законодательство предусматривает ответственность за преступления в сфере компьютерной безопасности, в том числе за неправомерный доступ к охраняемой законом компьютерной информации, однако в рамках статьи 272 Уголовного кодекса Российской Федерации общественно опасные последствия неправомерного доступа к компьютерной информации должны выражаться в уничтожении, блокировке, модификации и копировании компьютерной информации [2]. В связи с этим появляется вопрос о соотношении компьютерной информаций и информационной безопасности, а также взаимосвязи компьютерной информации с определённым персональным компьютером.

Информационную безопасность, как правило ассоциируют с защитой конфиденциальности, целостности и доступности информации, однако стоит обратить внимание, что сама информация как предмет в совокупности внешних структурных признаков и внутренним свойствам, формирующим целостность элементов безопасности [3]. Многими исследователями подчёркивается тот факт, что понятие безопасности невозможно определить только по внешним и внутренним свойствам его носителя, так как составляющими безопасности являются такие

факторы как, во-первых, конфиденциальность информации, как ограниченность доступности информации до определённого круга субъектов. Во-вторых, целостность информации как ограниченный режим доступа и блокировки действий по несанкционированному изменению исходных данных. В-третьих, доступность информации как система, позволяющая получить доступ к информации определённым субъектам, тем самым ограничивая доступ к информации для несанкционированных пользователей, но сохраняя режим доступа для правообладателей [4].

Однако исходя из терминологии Уголовного кодекса Российской Федерации законодатель ограничивает доступ не информационной безопасности в целом, а информации, содержащейся непосредственно на устройстве, квалифицированном как «компьютерное» технологическое устройство [5]. Иными словами, законодательство не использует широкое и не до конца определенное понятие «информационная безопасность», которое постоянно видоизменяется за счёт прогрессивности технологических исследований, так как его использование может вызвать множество проблем применения данной нормы Уголовного и права и соответственно повлиять на разрешение уголовного дела. В данном контексте соединение безопасности информации с её носителем предполагается наиболее логичным, так как именно носители информации такие как персональный компьютер, смартфоны и иные цифровые и энергоёмкие записывающие устройства (как флеш-накопители) сохраняют следы нарушенного права на доступность, сохранность и тайну охраняемой законом информации в электронном виде.

Именно носители информации в данном случае и выступают в качестве объектов экспертизы, при этом они содержат в себе не только первоначальную защищаемую законом информацию, но и информацию криминалистического направления, которая и является целью судебно-экспертного исследования [6]. Однако компьютерная экспертиза и её отдельные действия, связанные с исследованием информационной безопасности, сталкивается с определёнными проблемами. В первую очередь это связано с недостатком требований к электронным следам информационного преступления. Иными словами, необходимо проведение исследований для определения требований протокола допустимых информационных электронных следов компьютерных преступлений. В связи с этим появляется необходимость в создании технической регламентации протокола допустимой информации, который одновременно будет включать в себя информационно-справочные элементы о технических требованиях к цифровым и электронным файлам и следам преступления, а также обеспечивает сохранность искаженных файлов информации от случайного уничтожения. Любой объект экспертизы, в том числе и информация, имеет свои свойства. Если для обеспечения объективности экспертного исследования некого материального объекта производят выборку образцов, объем которых определяет возможность применения разрушающих и частично-разрушающих методов исследования, то для проведения экспертизы компьютерной информации выборку сделать не представляется возможным, её может заменить копирование электронного файла с сохранением его свойств. Однако технические устройства сложны в эксплуатации и не всегда защищены от технических ошибок и искажений электронных файлов, как правило данная проблема встречается у энергозависимых накопителей памяти и энергоёмких записывающих устройств, которые используются не по назначению или с существенными нарушениями правил эксплуатации технически сложных средств и устройств. Тем самым файл может быть как намеренно, так и в результате нарушения техники эксплуатации испорчен и недоступен для исследования, а любые действия в процессе экспертизы, целью которых является обеспечить доступ к файлу или изъятию из него какой-либо полезной для исследования информации, могут повлечь полное уничтожение файла и

в результате замедлить ход действия расследования. Значимость вопроса о экспертном исследовании необходимой информации без её модификации и уничтожения весьма велика, что подтверждает необходимость создания специальных процессуальных норм и технических регламентаций по использованию электронной криминалистической информации. При работе с носителями и записывающими устройствами электронной информации судебному эксперту необходимо использовать программные обеспечения, которые позволяют получить доступ к имеющимся на них данным без их модификации, в том числе и данными, которые искажены, при этом, в зависимости от цели экспертного исследования, необходима возможность обеспечить как восстановление повреждённого файла, так и сохранность искажений файла в неизменном виде[7].

Экспертное исследование также может быть осложнено неоднозначностью терминов, применяемых в процессе экспертизы компьютерной информации различными экспертами, экспертными учреждениями и терминами, содержащимися в методологических рекомендациях проведения экспертного исследования данного вида. Тем самым возможно выделить сразу несколько терминов схожих между собой: компьютерная информация, электронная информация и цифровая информация. Также эти термины применительно к следам правонарушения, например, следам, оставляемым вредоносными вирусными операционными системами [8]. Однако исследователями нередко поднимается вопрос о различии терминов компьютерные, электронные, цифровые следы правонарушения. Как уже говорилось выше, мы предполагаем, что законодатель в главе 28 использует термин компьютерная информация так как сознательно уходит от неопределённости термина и связывает информацию и следы преступления с определённым персональным компьютером или другим схожим технологичным устройством, на котором эта информация содержится (записана). В таком случае термины электронной и цифровой информации возможно исследовать как термины, связанные с тем, где эта информация существует – в цифровом или электронном пространстве. Соответственно появляется вопрос о различии цифрового и электронного. Эти два термина неразрывно связаны между собой, а большинство исследователей используют их как синонимы. Однако, возможно предположить границы различия этих терминов между собой. Электронная информация как правило характеризуется как образ существующие действительности, переданный в символичной форме посредством искусственно созданного языка кодирования и воспроизведённая технически сложным электронно-вычислительным устройством. А цифровая информация — это дискретные данные, то есть информация, переданная посредством переменных, которые способны принимать значения только из определённого списка допустимых значений. Например, двоичная система, где использованы значения 0 и 1, которые передают соответственный сигнал «ложь» и «истина». Таким образом мы предполагаем, что электронная информация — это общее понятие, включающее в себя цифровую информацию, но на данный момент цифровые дискретные данные обеспечивают существование электронной информации, так как все языки кодирования так или иначе связаны с понятием цифровой информации. Следовательно, использование данных терминов как синонимов допускается, однако в случае каких-либо изменений в этой сфере возможно возникновения проблем в соотношении этих определений и соответственно это отразится на процессуальных действиях и судебно-экспертных исследованиях. При этом изъятие информации при этом необходимо рассматривать как отдельное следственное действие, которое при этом должно быть запротоколировано [9]. Так, например, данные, содержащиеся в памяти мобильных устройств, не обладают признаками документа, однако также являются информацией, и поэтому изъять их в рамках таких следственных действий, как обыск или выемка, наведение справок или исследование документов, не представляется возможным [10].

Следующей проблемой экспертизы в сфере информационной безопасности является возможность использования электронных протоколов изъятия или исследования информации. Осмотр носителя информации или непосредственное открытие файла, содержащего в себе как охраняемую законом информацию, так и информацию о совершённом правонарушении в отношении данного объекта информации является процессуальным действием и соответственно должно быть отображено в протоколе. Однако отображение в письменном протоколе электронной информации представляется нелогичным, иными словами, любые искажения информации должны быть записаны должностным лицом с описанием характерных свойств исследуемого объекта, в том числе и искажения в коде или общий вид экрана с отображением критической системной ошибки в операционной системе. В то время как электронный протокол процессуального действия может отобразить эти данные непосредственно путём копирования данной информации без лишнего описания [11]. Однако в данном случае необходимо проработать ряд процессуальных требований к такому виду доказательств как электронный протокол следственного или иного процессуального действия, в том числе и рассмотреть вопрос шифрования информации на компьютерной технике должностного лица, производящего процессуальное протоколируемое действие. Протокол как известно должен быть подписан участниками процессуального действия и понятыми в установленном законом порядке, для обеспечения объективности протокола.

В данном случае электронный протокол может быть подписан электронной подписью или же его объективность, достоверность и допустимость должны подтверждаться иными способами. Электронный протокол при этом может быть изменён в результате несанкционированного доступа. Для предотвращения несанкционированного доступа соответственно необходимы меры защиты электронных процессуальных документов, такие как шифрование и кодировка. При этом любые действия с электронным протоколом не должны повреждать имеющуюся в нём информацию или же приложенные к нему электронные файлы и документы.

**Вывод**

Обеспечение судебной экспертизы в сфере информационной безопасности постоянно будет сталкиваться с проблемами соотношения материальных и процессуальных норм с техническими возможностями обеспечения изъятия, фиксации и исследования электронных объектов экспертизы. Исследования данного вопроса необходимо в первую очередь для создания специальных процессуальных норм и технических регламентаций по использованию электронной криминалистической информации, которые могут быть использованы как для проведения экспертного исследования, так и для обеспечения объективности, достоверности и допустимости процессуальных документов, создаваемых при производстве процессуальных действий по уголовным делам, связанным с посягательствами на безопасность и конфиденциальность информации. А также обеспечения программным контентом для работы эксперта с носителями и записывающими устройствами электронной информации, которые позволяют получить доступ к имеющимся на них данным без их модификации, в том числе и данным, которые повреждены.

**Библиографический список**

1. Силуянова К.А. Использование портативных приборов экспертом-криминалистом в процессе осмотра места преступления // Российское право онлайн. – 2018. – №4. – С. 63-70.
2. Уголовный кодекс Российской Федерации от 13 июня 1996г. № 63-ФЗ // Собрание законодательства Российской Федерации. – 1996 г. – № 25. – ст. 2954.

3. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. – 2014. – №. 5(8). – С.39-42.
4. Владимирова Т.В. К социальной природе понятия «информационная безопасность» // Вопросы безопасности. – 2013. – №. 4. – С. 78-95.
5. Степанов-Егиянц В.Г. Содержание термина «неправомерный доступ к компьютерной информации» в Уголовном Кодексе Российской Федерации // Право и экономика. – 2014. – №. 8. – С. 42-45.
6. Жидко Е.А. Методология формирования единого алгоритма исследований информационной безопасности // Вестник Воронежского института МВД России. – 2015. – №. 1. – С.62-69.
7. Бессонов А.А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета имени О.Е. Кутафина. – 2019. – №. 3 (55). – С.46-52.
8. Вехов В.Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения. – 2015. – №. 2. – С. 43-46.
9. Пропастин С.В. Осмотр или судебная экспертиза: выбор в пограничных ситуациях (на примере обнаружения и исследования компьютерной информации) // Современное право. – 2013. – №. 6. – С. 129-132.
10. Багмет А.М., Скобелин С.Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность. – 2013. – №. 2. – С. 24.
11. Гарифуллина А. Х., Сухарева О. С. Электронный протокол как новый вид доказательства и новый элемент удостоверительного аспекта уголовного судопроизводства //Вестник Казанского юридического института МВД России. – 2012. – №. 9. – С.111-117.