УДК 343.985.7:343.7

ОСОБЕННОСТИ РАБОТЫ СЛЕДОВАТЕЛЯ С КОМПЬЮТЕРНОЙ ИНФОРМАЦИЕЙ ПРИ РАССЛЕДОВАНИИ МОШЕННИЧЕСТВ И ХИЩЕНИЙ ПУТЕМ ЗЛОУПОТРЕБЛЕНИЯ СЛУЖЕБНЫМИ ПОЛНОМОЧИЯМИ, СОВЕРШЕННЫХ ПРИ ЗАКАЗЕ И ПРИЕМКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Павел Александрович Капица
Институт повышения квалификации и переподготовки Следственного комитета Республики Беларусь, Минск, Республика Беларусь, pauluk1756@yandex.by

Аннотация. В публикации на основании анализа эмпирической базы (уголовные дела, рассмотренные судами Республики Беларусь, и материалы проверки по сообщению о совершенном преступлении) представлены основные виды компьютерной информации, формируемой в ходе подготовки и совершения мошенничеств и хищений путем злоупотребления служебными полномочиями при заказе и приемке программного обеспечения. Компьютерная информация разделена автором на непосредственно связанную с разработкой программного обеспечения и относящуюся к иным обстоятельствам совершенного хищения. Определены наиболее вероятные носители компьютерной информации по делам рассматриваемой категории. Описаны организационно-тактические особенности собирания доказательственной компьютерной информации, ее осмотра и анализа. Выделены основные этапы осмотра мобильного устройства, содержащего криминалистически значимую компьютерную информацию. Сформулированы вопросы для назначения компьютерно-технического экспертного исследования, в ходе производства которого должно быть оценено проверяемое программное обеспечение. Изучение материалов следственной и экспертной практики позволяет констатировать, что наиболее значимым является разрешение диагностических (соответствие программного обеспечения определенным критериям, условиям договора, техническому заданию и т. д.) и идентификационных (сравнение программного кода) задач.

Ключевые слова: компьютерная информация, хищения, мошенничество, программное обеспечение, расследование преступлений, тактика следственных действий

Для цитирования: Капица П. А. Особенности работы следователя с компьютерной информацией при расследовании мошенничеств и хищений путем злоупотребления служебными полномочиями, совершенных при заказе и приемке программного обеспечения // Вестник Волгоградской академии МВД России. 2025. № 2 (73). С. 103—110.

SPECIFICS OF THE INVESTIGATOR'S WORK WITH COMPUTERIZED INFORMATION WHILE INVESTIGATING FRAUDS AND THEFT BY OFFICIAL POWERS ABUSE, COMMITTED WHEN ORDERING AND ACCEPTING SOFTWARE

Pavel Aleksandrovich Kapitsa
Institute for Advanced Training and Retraining of the Investigative Committee of the Republic of Belarus, Minsk, Republic of Belarus, pauluk1756@yandex.by

Abstract. The article, based on the analysis of the empirical base (criminal cases considered by the courts of the Republic of Belarus and verification materials on crime reports), presents the main types of computerized information being created during the frauds and thefts preparation and commission by official powers abuse when ordering and accepting software. The author distinguishes computerized information directly related to software development and computerized information related to other theft circumstances. The most probable computer storage devices on cases of the category under consideration are determined. The organizational and tactical features of collecting evidentiary computerized information, its examining and analyzing are described.

The main stages of examining of a mobile device containing forensically significant computerized information are identified. Questions for the computer-technical examination appointment are formulated, during which the software being checked should be assessed. The study of the materials of investigative and forensic practice allows us to state that the solution of diagnostic (software compliance with certain criteria, terms of the contract, technical specifications, etc.) and identifying (program code comparison) problems are of the most significance.

Keywords: computerized information, theft, fraud, software, crime investigation, tactics of investigative actions

For citation: Kapitsa P. A. Specifics of the investigator's work with computerized information while investigating frauds and theft by official powers abuse, committed when ordering and accepting software. Journal of the Volgograd Academy of the Ministry of the Interior of Russia, 103—110, 2025. (In Russ.).

Сфера разработки программного обеспечения (далее — РПО) является высоковостребованной индустрией, технологические достижения которой обеспечивают необходимый уровень цифровизации общества. Это обстоятельство обусловливает неизбежный интерес криминального сообщества к данной сфере, в том числе выражающийся в виде хищений и преступлений коррупционной направленности. Согласно законодательству Республики Беларусь общественно опасные деяния данного типа можно разделить:

1) на мошенничества (ст. 209 Уголовного кодекса Республики Беларусь (далее — УК РБ)). Получив денежные средства, недобросовестные разработчики компьютерных программ умышленно некачественно исполняют свои договорные обязанности либо не исполняют их вообще;

2) хищения путем злоупотребления служебными полномочиями (ст. 210 УК РБ). Должностные лица организаций-заказчиков либо органов, уполномоченных на принятие решений о расходовании денежных средств на РПО, подбирают «нужных» разработчиков и при их помощи завладевают денежными средствами заказчика или государственного бюджета, при этом заказчики получают некачественные программные продукты;

3) сопряженные с указанными хищениями преступления против интересов службы (гл. 35 УК РБ). Должностные лица органов и организаций, в деятельность которых внедряется программное обеспечение, из корыстной или иной личной заинтересованности содействуют расхитителям.

По нашему мнению, согласно российскому законодательству аналогичные противоправные деяния следовало бы квалифицировать прежде всего как мошенничества по ст. 159 Уголовного кодекса Российской Федерации от 13 июня 1996 г. № 63-ФЗ (далее — УК РФ) либо как злоупотребления должностными полномочиями по ст. 285 УК РФ и иные сопряженные коррупционные преступления.

Преступления рассматриваемого вида обладают значительной общественной опасностью, поскольку недобросовестные разработчики программного обеспечения и лица, им содействующие, могут завладеть большими объемами денежных средств, в том числе бюджетных, которые выделяются на информатизацию. В первую очередь данным обстоятельством определяется актуальность разработки рекомендаций по расследованию хищений в сфере РПО. При создании этих рекомендаций отдельное внимание следует уделить организации работы следователя с компьютерной информацией, поскольку она выступает важнейшим доказательством по такого рода делам.

Ряд белорусских и российских ученых-криминалистов на диссертационном уровне занимался разработкой рекомендаций по расследованию хищений различных видов: Н. В. Быкова (особенности выявления и расследования мошенничеств в сфере страхования) [1], Р. С. Гарбуз (методика расследования присвоения либо растраты, совершаемых в бюджетной сфере) [2], К. В. Гончаров (методика расследования злоупотреблений должностными полномочиями, совершаемых вопреки интересам службы в коммерческих и иных организациях субъектами, выполняющими управленческие функции) [3], А. В. Дешук (криминалистическое обеспечение расследования хищений в сфере строительства) [4], Ю. Ф. Каменецкий (методика первоначального этапа расследования хищений путем злоупотребления служебными полномочиями в бюджетной сфере) [5]. Следственным комитетом Республики Беларусь подготовлены методические рекомендации по расследованию мошенничеств и хищений путем злоупотребления служебными полномочиями [6; 7]. В перечисленных работах и методических рекомендациях можно найти положения, связанные с тактикой проведения следственных действий, в том числе осмотров, назначения экспертиз. Однако они готовились во времена, когда компьютерная информация не играла такой роли в уголовном процессе, как в настоящее время. Кроме того, указанные исследования и рекомендации разрабатывались без учета специфики расследования

мошенничеств и хищений путем злоупотребления служебными полномочиями в сфере РПО. Это определяет научную новизну и практическую значимость представленного в настоящей публикации исследования.

Эмпирической базой исследования выступили:

— уголовное дело № 2-15/6, рассмотренное Минским городским судом. Согласно материалам дела, четверо должностных лиц учреждения образования Б. в период с апреля 2008 г. по декабрь 2010 г., действуя в составе преступной группы, создали ряд временных научных коллективов и под видом исполнения заданий государственной программы научных исследований «Металлургия» выдали ранее разработанное для иного заказчика программное обеспечение за новый программный продукт, зарегистрировали права интеллектуальной собственности на данный продукт не на учреждение образования Б., а на физических лиц из числа преступной группы, что повлекло за собой тяжкие последствия в виде нецелевого использования выделенных государством денежных средств в особо крупном размере[1];

— уголовное дело № 1-593/20, рассмотренное судом Фрунзенского района г. Минска. Согласно материалам дела, П. — директор УП «М.» — получил деньги из инновационного фонда Минского городского исполнительного комитета для создания гипобаракамеры и программного обеспечения блока управления к ней. По условиям выделения денежных средств итоги работ должны были сохраняться и использоваться непосредственно в УП «М.». Ни гипобаракамера, ни программное обеспечение фактически не создавались. Однако согласно документам, составленным и собственноручно подписанным П., к РПО привлекался программист — «подставное» лицо, не осведомленное о преступном характере деятельности П., от имени которого последний получал деньги[2];

— материалы проверки Московского РУВД г. Минска № 1780/21, решение об отказе в возбуждении уголовного дела по которым принято в 2021 г. Руководитель учреждения В. — заказчика программного обеспечения — обратился в правоохранительные органы, поскольку, по его мнению, в действиях должностных лиц исполнителя — учреждения образования Б. и субподрядчика ЗАО И., которые качественно не исполнили свои обязанности, — присутствовал состав преступления[3].

По тематике исследования проведено анкетирование 200 сотрудников правоохранительных органов и адвокатуры: 141 сотрудник Следственного комитета Республики Беларусь, 45 сотрудников подразделений по борьбе с экономическими преступлениями органов внутренних дел Республики Беларусь, 14 адвокатов. Большинство опрошенных — 110 (55 %) — владели значительным опытом правоприменительной деятельности: стаж работы составлял от 11 до 20 и более лет.

Под «компьютерной информацией» в рамках данной публикации следует понимать прежде всего информацию, хранящуюся в компьютерной системе, сети или на машинных носителях, обрабатываемую компьютерной системой либо передаваемую в пространстве с помощью любых программно-технических средств. Данная дефиниция закреплена в ст. 4 УК РБ. Она некоторым образом отличается от определения, закрепленного в уголовном законе Российской Федерации (сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи). Вместе с тем представляется, что для данного исследования различия в определениях не носят существенного характера.

Для решения задач расследования хищений в сфере РПО компьютерную информацию, с которой работает следователь, можно разделить на связанную непосредственно с РПО и связанную с иными обстоятельствами совершения хищения.

К первому виду компьютерной информации относится программный код (его фрагменты), который выдавался недобросовестными разработчиками за качественный, файлы различных форматов (.doc, .pdf, .jpg и др.), содержащие в электронном виде документы и изображения, связанные с РПО (инструкции по пользованию, фрагменты интерфейса и др.) и финансово-хозяйственной деятельностью по ней. О том, что программный код относится к наиболее типичным следам преступной деятельности при совершении хищений в сфере РПО, высказались 79 % (158 из 200) респондентов.

Компьютерной информацией, непосредственно не связанной с РПО, но содержащей сведения об иных обстоятельствах совершенного хищения, являются переписка представителей контрагентов

[1] Уголовное дело № 2-15/6 // Архив Минского городского суда за 2016 г.

[2] Уголовное дело № 1-593/20 // Архив суда Фрунзенского района г. Минска за 2020 г.

[3] Материалы проверки № 1780/21 // Архив Московского РУВД г. Минска за 2021 г.

по договорам о РПО, документы, изображения, содержащиеся на носителях компьютерной информации. Переписку в электронном виде к типовым следам хищений в сфере РПО отнесли 59 % (118 из 200) опрошенных практиков.

Наиболее вероятными материальными носителями компьютерной информации при расследовании хищений в сфере РПО будут выступать:

1) накопители на жестких магнитных дисках. Они могут быть изъяты в ходе осмотров и обысков из компьютеров, ноутбуков расхитителей и иных лиц, иногда вместе с самим системным блоком, ноутбуком. На данных материальных носителях следует искать компьютерную информацию первого и второго указанных видов;

2) внешние жесткие диски, USB-накопители. Данные носители служат для организации работы и передачи файлов с устройства на устройство (компьютерная информация первого вида, а также проекты документов, связанных с государственными закупками, финансово-хозяйственной деятельностью и т. п.). Их следует искать при осмотрах и обысках на рабочих местах, по месту жительства и при личных обысках расхитителей;

3) флеш-память, карты памяти. Это носители прежде всего компьютерной информации второго вида — файлов с документами, изображениями и др. Они содержатся в компьютерной технике (смартфонах, планшетах и др.);

4) оптические (лазерные) компакт-диски. Указанные носители в преступлениях рассматриваемой категории используются для хранения и передачи компьютерной информации первого типа — программного кода (якобы разработанного программного обеспечения);

5) мобильные устройства (мобильные телефоны, смартфоны). Содержат на внутренней встроенной памяти компьютерную информацию второго типа — электронную переписку. Могут также содержать файлы с документами и изображениями, связанными с совершенным преступлением;

6) аппаратные криптокошельки. Они могут использоваться для хранения криптовалюты и перечисления ее в качестве взяток лицам, способствовавшим расхитителям.

Компьютерная информация, непосредственно связанная с РПО, может быть осмотрена и проанализирована. Например, в ходе осмотра следователь может зафиксировать факт того, что компьютерная программа не запускается. В результате анкетирования 74 % (148 из 200) респондентов высказались, что на первоначальном этапе расследования целесообразно осмотреть материальный носитель программного кода. Следователь также может анализировать содержание имеющихся в электронном виде документов и их проектов.

Вместе с тем представляется, что в качестве достоверного доказательства некачественной работы программного обеспечения может выступить только заключение эксперта. Поэтому основным направлением работы следователя с компьютерной информацией, непосредственно связанной с РПО, выступит назначение экспертизы по оценке качества программного обеспечения [8]. Экспертное исследование назначалось по уголовному делу № 2-15/6[1]. По уголовному делу № 1-593/20 экспертиза не проводилась, поскольку программное обеспечение не разрабатывалось вообще[2]. В ходе проверки по заявлению руководителя учреждения В. сотрудники органа дознания анализировали материалы экспертиз, проведенных в рамках гражданского спора между заказчиком и разработчиком[3].

Исследования, направленные на оценку качества программного обеспечения, следует относить в первую очередь к компьютерно-техническому виду экспертного исследования. А. И. Швед отмечает, что предметом таких экспертиз являются «фактические сведения об обстоятельствах разработки и эксплуатации компьютерных средств и систем, обеспечивающих реализацию информационных процессов» [9, с. 155]. В то же время примеры из правоприменительной практики Республики Беларусь свидетельствуют о том, что при назначении экспертиз, связанных с оценкой качества программного обеспечения, они именовались по-разному («судебно-программно-компьютерная экспертиза», «комплексная экспертиза результатов научной деятельности»). Перед экспертами ставились вопросы, ответы на которые выходят за пределы компетенции компьютерно-технического исследования. Представляется, что подобный подход правоприменителя обусловлен нетипичностью экспертизы и нестандартностью задач, которые было необходимо решить в целях доказывания факта невыполнения разработчиком программного обеспечения своих договорных обязательств.

[1] Уголовное дело № 2-15/6 // Архив Минского городского суда за 2016 г.

[2] Уголовное дело № 1-593/20 // Архив суда Фрунзенского района г. Минска за 2020 г.

[3] Материалы проверки № 1780/21 // Архив Московского РУВД г. Минска за 2021 г.

Для разрешения вопросов, требующих привлечения специальных знаний по рассматриваемым видам преступлений, следователь выносит постановление о назначении экспертных исследований, содержащих вопросы диагностического и идентификационного характера. К вопросам диагностического характера относятся следующие:

1. Функционирует ли представленная на исследование компьютерная программа? Если да, то какие технические условия аппаратных устройств требуются для ее эксплуатации? Какие функции способна выполнять представленная на исследование программа?

Ответы на данные вопросы должны способствовать проверке выдвинутых версий относительно того, что договорные обязанности недобросовестным разработчиком не выполнены вообще, о чем и свидетельствует факт невозможности запуска программы. Кроме того, важно определить, для каких аппаратных устройств предназначено программное обеспечение и может ли оно функционировать на устройствах заказчика. Уточнение функционала компьютерной программы поможет решить дальнейшие вопросы о соответствии результатов РПО техническому заданию (иным документам).

2. Соответствует ли разработанное (указать субъект хозяйствования) по договору (указать дату и номер договора) программное обеспечение (указать название или иные характеристики) требованиям технического задания на разработку программного обеспечения?

В формулировку данного вопроса могут быть добавлены и иные документы, которые определяли задачи РПО (например, сам договор, приложения к нему).

3. Соответствует ли разработанное (указать субъект хозяйствования) по договору (указать дату и номер договора) программное обеспечение (указать название или иные характеристики) современному на момент заключения договора уровню компьютерных программ?

Постановка именно данного вопроса необходима потому, что недобросовестные исполнители могут находиться в сговоре с представителями заказчика от самого начала процедуры государственных органов и оказывать влияние на разработку «нужного» технического задания. Поэтому указанный документ может содержать требования под конкретную, уже созданную или иным образом приобретенную разработчиком компьютерную программу. Она, в свою очередь, может не относиться к категории эффективных и качественных и может не соответствовать современному на момент заключения договора состоянию развития электронно-вычислительной техники, компьютерных программ.

4. Соответствуют ли заданные в представленной на исследование компьютерной программе параметры реальным параметрам технологического процесса, для информатизации которого разрабатывалось программное обеспечение?

Решение данной экспертной задачи требует комплексного подхода — применения знаний не только в сфере программирования, но и в соответствующей отрасли, для упрощения технологических (организационных) процессов в которой осуществлялась РПО. Поэтому к проведению исследований следует привлекать квалифицированных лиц из разных сфер знаний. Так, если речь идет о создании компьютерной программы для управления оборудованием на производстве, в целях оценки результатов РПО следователю в качестве эксперта необходимо привлечь специалиста, который работает с таким оборудованием и знаком с организацией производственных процессов.

5. Какова рыночная стоимость разработки программного обеспечения на момент заключения договора (при выполнении условий договора, технического задания, иных документов)?

Поставленный вопрос предусматривает назначение товароведческого исследования (в том числе комплексно с компьютерно-техническим), в ходе производства которого должна быть определена стоимость продукции. Данная задача может ставиться следователем в случаях, если за выполнение незначительного объема работ исполнитель потребовал несоразмерную оплату.

Идентификационные задачи компьютерно-технической экспертизы, связанной с оценкой качества программного обеспечения, призваны обеспечить решение следующих вопросов:

1. Имеются ли отличия в представленных на исследование программном коде, который содержится (указать носитель), и программном коде, содержащемся (указать носитель)? Если есть, то какие?

Данный вопрос может быть поставлен, если у следователя есть дополнительные основания полагать, что заказчику представлен целиком устаревший продукт или программа, права на которую уже принадлежат иному заказчику.

2. Содержатся ли в представленном на исследование программном коде, расположенном (указать носитель), элементы программного кода,

расположенного (указать носитель)? Если содержатся, то какие?

Вопрос такого типа следует ставить, если есть основание полагать, что недобросовестный разработчик использовал (целиком или частично) чужие наработки (например, работников заказчика).

В связи с нетипичностью компьютерно-технического исследования, предусматривающего решение вопросов по оценке качества программного обеспечения, перед экспертом могут ставиться и иные вопросы, обусловленные спецификой способа совершения конкретного преступления, особенностями сферы, для информатизации которой осуществлялась РПО. Не исключается также постановка вопросов о научной значимости результатов РПО (если компьютерная программа разрабатывалась в рамках бюджетной научно-исследовательской деятельности), денежной оценке стоимости выполненных работ (если за незначительный объем работ была умышленно расходована несоразмерная значительная сумма) и др.

Для анализа компьютерной информации, непосредственно не связанной с РПО, но относящейся к иным обстоятельствам совершения хищения, достаточно произвести ее осмотр.

В рамках данной публикации следует охарактеризовать особенности осмотра мобильных устройств, поскольку в настоящее время они имеются практически у каждого, что в полной мере относится и к подозреваемым, и свидетелям по делам о хищениях в сфере РПО.

Белорусскими исследователями М. В. Савич и Г. Р. Пянтковским предложены общие правила производства осмотра мобильных устройств. Они выделили особенности осмотра на подготовительном, рабочем и заключительном этапах [10]. Данные правила можно адаптировать для расследования хищений в сфере РПО.

На подготовительном этапе осмотра следователь:

1. Изучает материалы уголовного дела и определяет:

— обстоятельства изъятия мобильного устройства и его комплектность;

— содержание показаний участников уголовного процесса относительно обстоятельств совершенного преступления, предмета осмотра — мобильного устройства. Так, если представители заказчика свидетельствовали о том, что договаривались с представителями недобросовестных разработчиков при помощи электронной переписки, то при осмотре следователю необходимо обращать внимание прежде всего на содержание SMS-сообщений, мессенджеров, электронной почты;

— принадлежность мобильного устройства конкретному лицу, наличие аутентификационных данных и возможность получения доступа к компьютерной информации. Информация о владельце и пользователях мобильного устройства позволяет определить направление тактики его осмотра. Так, файлы с личными фотографиями свидетеля, если он явно не имеет отношения к подозреваемым (подчиненные, субподрядчики по договорам в сфере РПО), не представляют интереса для следствия. В то же время личные фотографии расхитителей могут нести дополнительную информацию об их связях, имущественном положении.

2. Определяет место, время и способ производства осмотра, обеспечивает наличие заряда аккумуляторной батареи мобильного устройства, подбирает научно-технические средства производства осмотра.

3. Приглашает в необходимых случаях для производства осмотра участников уголовного процесса. Например, добросовестный представитель заказчика может оказать содействие следователю в копировании электронной переписки, которая велась между ним и расхитителем.

На рабочем этапе осмотра решаются две основные задачи: осмотр самого мобильного устройства и осмотр компьютерной информации, которая в нем содержится.

При осмотре компьютерной информации, содержащейся на мобильном устройстве, следует зафиксировать группы приложений, виджеты и иные сведения в общем виде, которые отражаются на дисплее (путем фотографирования, исполнения скриншотов), после чего детально изучается следующее:

1) список контактов, содержащихся в телефонной книге устройства, и журнал вызовов (не только позволяет увидеть, с кем контактировало лицо, но и может свидетельствовать о характере взаимоотношений между подозреваемыми и свидетелями (как подписано лицо в контактах, сколько раз и кто кому звонил и т. д.));

2) SMS-сообщения (могут содержать не только переписку, но и иную значимую информацию (сведения о перечислении денег со счета на счет));

3) сведения браузера об истории посещений интернет-сайтов, прежде всего о посещении социальных сетей, содержащих переписку и фотоизображения;

4) сведения приложений. В качестве значимых источников для определения обстоятельств, подлежащих доказыванию, выступает информация из мессенджеров, при изучении которых можно получить следующую информацию относительно совершенного хищения:

— о контактах лица, в том числе не содержащихся непосредственно в телефонной книге мобильного устройства;

— фотоснимках и видеофайлах. В расследовании хищений в сфере РПО играют ту же роль, что и обнаруженные непосредственно на мобильном устройстве. Кроме того, фотоснимки в мессенджерах могут содержать отражения документов и проектов документов, относящихся к совершению преступления;

— сведениях о месторасположении и маршруте перемещений лица (например, если надо подтвердить факт встречи расхитителей между собой или с представителями заказчика);

— перемещении денежных средств (криптовалют). Данные сведения могут представлять интерес, если есть информация о распределении похищенных денежных средств между расхитителями, лицами, им содействовавшими, от дачи взятки должностным лицам, принимавшим положительное решение при проведении государственной закупки в сфере информатизации и др.;

5) сведения средств синхронизации. Их изучение позволит получить возможную скопированную информацию, которая была удалена пользователем.

Заключительный этап осмотра мобильного устройства и компьютерной информации, в нем содержащейся, предусматривает действия следователя по обеспечению сохранности полученной информации, оформлению протокола осмотра предметов и компьютерной информации, фиксирующего ход и результаты следственного действия, упаковке мобильного устройства в соответствующем порядке [10].

Подводя итоги исследования, сформулируем следующие выводы.

1. По делам о хищениях в сфере РПО компьютерную информацию можно разделить на два основных вида: непосредственно связанную с РПО и связанную с иными обстоятельствами совершения преступления.

2. Вероятными носителями компьютерной информации по делам о хищениях в сфере РПО могут выступать: накопители на жестких магнитных дисках, внешние жесткие диски, USB-накопители, флеш-память, карты памяти, оптические (лазерные) компакт-диски, мобильные устройства (мобильные телефоны, смартфоны), аппаратные криптокошельки.

3. Компьютерная информация, непосредственно связанная с РПО, может быть осмотрена и проанализирована следователем. Вместе с тем для решения вопроса о качестве программного кода, его соответствии определенным требованиям, установленным договорами и техническими заданиями, и иным параметрам необходимо назначать экспертизу оценки качества программного обеспечения. В ходе назначения экспертизы могут быть поставлены вопросы, направленные на решение диагностических и идентификационных задач.

4. Компьютерная информация, непосредственно не связанная с РПО, однако содержащая значимые для расследования хищений сведения, подлежит осмотру. В ходе осмотра мобильных устройств при расследовании хищений в сфере РПО выделяются определенные этапы и особенности, которые должны быть учтены следователем.

1. Быкова Н. В. Выявление и раскрытие мошенничества в сфере страхования: автореф. дис. ... канд. юрид. наук. Москва, 2009. 31 с.

2. Гарбуз Г. С. Методика по расследованию присвоения или растраты, совершаемых в бюджетной сфере: автореф. дис. ... канд. юрид. наук. Иркутск, 2007. 24 с.

3. Гончаров К. В. Совершенствование методики расследования злоупотреблений полномочиями, совершенных вопреки интересам службы в коммерческих и иных организациях субъектами, осуществляющими управленческие функции: автореф. дис. ... канд. юрид. наук. Ростов-на-Дону, 2018. 27 с.

1. Bykova N. V. Detection and solution of fraud in the sphere of insurance. Abstract of dissertation of candidate of juridical sciences. Moscow; 2009: 28. (In Russ.).

2. Garbuz G. S. Methodology for investigating embezzlement or misappropriation committed in the public sector. Abstract of dissertation of candidate of juridical sciences. Irkutsk; 2007: 24. (In Russ.).

3. Goncharov K. V. Improving the methodology for investigating powers abuse committed contrary to the service interests in commercial and other organizations by persons exercising managerial functions. Abstract of dissertation of candidate of

4. Дешук А. В. Криминалистическое обеспечение расследования хищений в сфере строительства: дис. ... канд. юрид. наук. Минск, 2016. 199 с.

5. Каменецкий Ю. Ф. Методика первоначального этапа расследования хищений путем злоупотребления служебными полномочиями в бюджетной сфере: дис. ... канд. юрид. наук. Минск, 2016. 196 с.

6. Методические рекомендации по расследованию мошенничества / Следств. комитет Респ. Беларусь. Минск, 2024. 44 с.

7. Методические рекомендации по расследованию хищений путем злоупотребления служебными полномочиями / Следств. комитет Респ. Беларусь. Минск, 2014. 31 с.

8. Капіца П. А. Асаблівасці прызначэння экспертных даследаванняў з мэтай вызначэння якасці распрацаванага праграмнага забеспячэння // Право.by. 2024. № 2 (88). С. 102—109.

9. Швед А. И. Судебная экспертиза: пособие. Минск: Форум, 2022. 296 с.

10. Компьютерная информация в следственной деятельности: собирание, оценка, использование: учеб. пособие / Ю. Ф. Каменецкий [и др.]; под общ. ред. Ю. Ф. Каменецкого. Минск: СтройМедиаПроект, 2022. 376 с.

juridical sciences. Rostov-on-Don; 2018: 27. (In Russ.).

4. Deshuk A. V. Forensic support for investigating embezzlement in the construction sector. Abstract of dissertation of candidate of juridical sciences. Minsk; 2016: 199. (In Russ.).

5. Kamenetsky Yu. F. Methodology of the initial stage of investigating theft by official powers abuse in the public sector. Dissertation of candidate of juridical sciences. Minsk; 2016: 196. (In Russ.).

6. Methodological recommendations for the fraud investigation. Investigative Committee of the Republic of Belarus. Minsk; 2024: 44. (In Russ.).

7. Methodological recommendations for the theft investigation by official powers abuse. Investigative Committee of the Republic of Belarus. Minsk; 2014: 31. (In Russ.).

8. Kapitsa P. A. Peculiarities of the purpose of expert studies for the purpose of determining the quality of developed software. Pravo.by, 102—109, 2024. (In Belaruss).

9. Shved A. I. Forensic examination. Manual. Minsk: Forum; 2022: 296. (In Russ.).

10. Computerized information in investigative activities: collection, evaluation, use. Manual. Red. by Yu. F. Kamenetsky. Minsk: StroyMediaProekt; 2022: 376. (In Russ.).

Капица Павел Александрович,
начальник учебного отдела
Института повышения
квалификации и переподготовки
Следственного комитета
Республики Беларусь;
pauluk1756@yandex.by

Kapitsa Pavel Aleksandrovich,
head of the educational department
of the Institute for Advanced Training
and Retraining
of the Investigative Committee
of the Republic of Belarus;
pauluk1756@yandex.by

Статья поступила в редакцию 27.03.2025; одобрена после рецензирования 03.04.2025; принята к публикации 15.05.2025.

The article was submitted 27.03.2025; approved after reviewing 03.04.2025; accepted for publication 15.05.2025.

***