УДК 34 **DOI: 10.34670/AR.2024.76.80.032**

Особенности производства отдельных следственных действий по преступлениям в сфере компьютерных и телекоммуникационных технологий

Долгаев Виктор Викторович

Кандидат юридических наук,
доцент кафедры уголовно-процессуального права,
Северо-Западный филиал,
Российский государственный университет правосудия,
197046, Российская Федерация, Санкт-Петербург,
Александровский парк, 5;
e-mail: dolgaevviktor@yandex.ru

Аннотация

В данной статье автор исследует особенности проведения отдельных следственных действий в контексте расследования преступлений в сфере компьютерных и телекоммуникационных технологий. На примере типичной следственной ситуации, когда лицо, совершившее преступное деяние, задержано, автор выделяет ряд следственных действий, направленных на сбор и закрепление доказательств по делам данной категории, а именно: осмотр места происшествия, допрос потерпевшего и подозреваемого (или обвиняемого), обыск, проведение следственного эксперимента, а также осмотр предметов и документов. Кроме того, автором приведены рекомендации по поиску цифровых следов преступления. Делается вывод, что все перечисленные в исследовании следственные действия не являются универсальными, однако для начального этапа расследования преступлений рассматриваемого типа, с точки зрения получения наиболее значимых сведений, проведение этих следственных действий представляется минимально необходимым. Кроме того, организация и проведение следственных действий по делам о преступлениях, совершенных с использованием компьютерных и телекоммуникационных технологий, целиком и полностью зависят от типичных ситуаций, которые складываются на начальном этапе расследования преступлений данного вида.

Для цитирования в научных исследованиях

Долгаев В.В. Особенности производства отдельных следственных действий по преступлениям в сфере компьютерных и телекоммуникационных технологий // Вопросы российского и международного права. 2023. Том 13. № 11А. С. 275-284. DOI: 10.34670/AR.2024.76.80.032

Ключевые слова

Информация, киберпреступность, информационная безопасность, компьютерные и телекоммуникационные технологии, цифровые следы.

Введение

В современном мире компьютерные и телекоммуникационные технологии играют огромную роль в повседневной жизни каждого человека. Они охватывают все сферы жизнедеятельности человека, включая образование, медицину, экономику и многое другое. Однако, с развитием технологий, возникают и новые виды преступлений, предусмотренных Уголовным кодексом Российской Федерации, которые требуют особого подхода к их расследованию. В частности, это касается преступлений в сфере компьютерных и телекоммуникационных технологий. О придании значимости проводимого в данной статье анализа преступлений данной категории говорят и статистические данным, приведенные Министерством внутренних дел России. Тенденция к увеличению количества преступлений в сфере информационно-телекоммуникационных технологий сохраняется – на 28,7% (с января по август 2023 года). Их удельный вес в числе всех преступных посягательств возрос до 32,9%, а по тяжким и особо тяжким – до 56,4%. Больше совершено дистанционных мошенничеств и краж. Раскрываемость киберпреступлений составила 29,9%, в том числе совершенных с использованием сети Интернет – 28,8%, расчетных (пластиковых) карт – 35,7% [Краткая характеристика состояния преступности…, www].

Основная часть

Основным способом закрепления доказательств является проведение следственных действий, которые могут осуществляться как на этапе «доследственной» проверки (их перечень регламентирован частью 1 статьи 144 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ), так и на стадии предварительного расследования.

Стоит отметить, что проведение следственных действий по уголовным делам полностью зависит от сложившихся типичных следственных ситуаций. В связи с чем, выделим наиболее распространенные следственные ситуации по преступлениям в сфере компьютерных и телекоммуникационных технологий:

Во-первых, стоит выделить следственную ситуацию, когда известны способ совершения преступления, обстоятельства, а также его последствия (преступление совершено в условиях очевидности), лицо, подозреваемое в совершении преступления, задержано;

Второй следственной ситуацией необходимо выделить, когда известны способ совершения преступления, а также его последствия, но не известен механизм совершенного преступления, а лицо, подозреваемое в совершении преступления, не установлено;

Третьей следственной ситуацией выделим, когда информация о способе совершения преступления отсутствует, известны только последствия совершенного преступления, а лицо, подозреваемое в совершении преступления, не установлено.

В связи с тем, что одним из наиболее вероятного сценария будет являться первая вышеприведенная ситуация (то есть, при которой лицо, совершившее преступление, задержано), нами будут рассмотрены ряд следственных действий, которые можно считать наиболее универсальными для следователей и дознавателей с точки зрения целесообразности их проведения.

Осмотр места происшествия *– это одно из ключевых следственных действий, которое проводится для сбора доказательств и информации, необходимой для расследования преступления. Какие же особенности осмотра места происшествия по преступлениям в сфере*

компьютерных и телекоммуникационных технологий?

1) Удалить с места проведения осмотра посторонних лиц, не имеющих отношения к проведению данного следственного действия;
2) Организовать охрану места проведения осмотра, руководить действиями участников осмотра — специалиста и эксперта-криминалиста, контролировать присутствующих при осмотре лиц. Охране должны подлежать: помещение или территория осмотра; задержанные лица (при их наличии); место установки компьютерной техники, в которой были обнаружены следы преступления; сервер локальной сети, содержащий базу данных обо всех проведенных операциях за последнее время; места отключения электропитания компьютеров, сервера и др. технических средств;
3) Принять необходимые меры по сохранению режима электропитания объекта, на котором производится осмотр;
4) Определить вид операционной системы и прикладные программы, используемые на компьютерных устройствах, а также обеспечить их сохранность и безопасную возможность копирования;
5) Своевременно и подробно фиксировать в протоколе всю значимую информацию в случае, если компьютер, смартфон, телефон либо другое устройство включены (не только описать само устройство, но и информацию, содержащуюся в нем, имеющую отношение к совершенному преступлению: например, указать время звонка, его продолжительность, номер абонента; содержание СМС-сообщения, время его отправления; описать информацию на сайте в сети «Интернет», его точный адрес; содержание информации; время получения сообщения, запроса, документа потерпевшему и т. д.);
6) Провести подробную криминалистическую фотосъемку или видео фиксацию осмотра;
7) Определить предметы, подлежащие изъятию, и правильно их упаковать.

Как правило, по данной категории уголовных дел имеется лицо, которому нанесен материальный ущерб. В связи с чем данное лицо подлежит допросу в качестве потерпевшего. Данный вид допроса проводится с целью получения информации от потерпевшего о совершенном в отношении него преступлении.

*При **допросе в качестве потерпевшего** по преступлениям, совершаемым с использованием компьютерных и телекоммуникационных технологий следователю (дознавателю) следует выяснить следующие обстоятельства:*

1) Точную информацию о том, когда, где и при каких обстоятельствах им было обнаружено преступное посягательство;
2) Предмет преступного посягательства: какие персональные компьютеры и какая именно информация, содержащаяся на данных компьютерах, были подвержены внешнему воздействию;
3) Степень причинения вреда, с обязательным приобщением к материалам дела документов, подтверждающих сумму ущерба, причиненного в результате несанкционированного воздействия на компьютерную систему, а также иные предметы, которые в дальнейшем могут подтвердить причинение вреда;
4) Круг лиц, имеющих доступ к использованию персональных компьютеров, а также наличие на компьютерах паролей — от этого напрямую будет зависеть круг подозреваемых, использовались ли данные персональные компьютеры не для профессиональной деятельности (установка программ, не предназначенных для

исполнения трудовых обязанностей);

5) Были ли установлены антивирусные программы, а также программы, предназначенные для ограничения доступа к содержащейся на персональных компьютерах информации, если да, где были приобретены и как часто обновлялись.

Допрос лица в качестве подозреваемого (обвиняемого) *по уголовным делам в сфере компьютерных и телекоммуникационных технологий.*

Процессуальные права и обязанности подозреваемого (обвиняемого) предусмотрены ст. ст. 46, 47 УПК РФ, в случае если по подозрению в совершении преступления задержан несовершеннолетний подозреваемый, правила производства допроса описаны в ст. 425 УПК РФ. В ходе проведения допроса необходимо выяснить:

– сведения о личности подозреваемого: особое внимание стоит обратить на уровень профессиональной подготовки: где и в какой период времени проходил обучение, по какой специальности; был ли официально трудоустроен, если да, указать в какой именно организации, его должностные обязанности в занимаемой должности; является сфера компьютерных или телекоммуникационных технологий его профессиональной, источники дохода, а также имущественное положение;

– сведения о способе совершения преступления: какие именно применялись технологии для достижения преступного умысла: точное наименование, предназначение, а также подробное описание работы технического устройства; местонахождение, источник приобретения технических устройств с подробным внешним описанием продавца и его контактных данных;

– сведения об источнике финансирования приобретения средств (личные средства или внешнее финансирование), предназначенных для покупки оборудования и иных сопутствующих совершению преступления технических устройств, использованных в качестве орудия преступления. Если источником финансирования являются внешние источники, необходимо уточнить сведения о процедуре передачи денежных средств за оказанные услуги: процедура передачи денежных средств осуществлена с использованием безналичного платежа либо наличными, в этом случае уточнить место передачи. Адрес места жительства, абонентские номера телефонов и т. д., по возможности необходимо составить фоторобот лиц, с которыми подозреваемый поддерживал связь;

– сведения о действиях лица по реализации преступного умысла: какие именно программы применялись им с целью достижения преступной цели, какие были им осуществлены умышленные действия, направленные к изменениям в работе пользователей персональных компьютеров, какая информация стала доступна в результате осуществления несанкционированного доступа в систему, передавалась ли данная информация третьим лица, если нет, то где данная информация находится в момент допроса лица.

Весьма важным следственным действием по преступлениям, совершаемым в сфере компьютерных и телекоммуникационных технологий, является ***обыск.***

Места, в которых может быть проведен обыск, могут находиться на значительном расстоянии друг от друга. Так, например, создание вредоносных компьютерных программ может быть совершено в одном месте, их распространение в сети «Интернет» – в другом. Соответственно, при получении оперативной информации о том, что местами преступлений являются несколько точек, расположенных по разным адресам, во избежание уничтожения

вещественных доказательств, а также утечки информации, целесообразно создание следственной группы. В этом случае проведение обысков целесообразно начинать одновременно сразу по нескольким адресам.

К проведению обыска необходимо привлечь оперативных сотрудников, так как может быть оказано силовое сопротивление. С целью изъятия следов пальцев рук и иных объектов обыск необходимо проводить с участием специалиста-криминалиста, а также специалиста в сфере компьютерного и программного обеспечения.

В первую очередь в ходе обыска необходимо установить способы соединений компьютеров: одноранговая сеть [Свободная энциклопедия, www] – оверлейная компьютерная сеть, основанная на равноправии участников; компьютеры для работы администраторов (англ. system administrator, разг. сисадмин) – лица, обязанностью которых является обеспечение штатной работы компьютерной техники, сети и программного обеспечения; а также пользовательские компьютеры. Далее в ходе обыска необходимо установить способы объединения компьютеров (локальная сеть и др. виды), а также зафиксировать способы выхода в Интернет: проводное соединение, оптоволоконный кабель, телефонный провод, беспроводное соединение, использование в качестве модема мобильного устройства смартфона, планшета, с вставленной СИМ-картой и т. д.

Дальнейшее проведение обыска целесообразно начинать с компьютера, принадлежащего системному администратору, так как именно с него поступают команды об операциях, проводимых на других компьютерах. Если компьютер находится в рабочем режиме, необходимо обратить внимание на изображение на мониторе, которое необходимо зафиксировать в протоколе следственного действия, а также произвести фотосъемку монитора компьютера. В протоколе необходимо отразить программы, которые на момент обыска включены, после фиксации их необходимо отключить, о чем сделать в протоколе соответствующую запись. Также необходимо проверить использование на осматриваемом персональном компьютере установку программ-мессенджеров: «WhatsUpp», «Viber», «Telegram» и др., которые предусматривают десктопную версию приложений.

Проверяется электронная почта, в случае обнаружения информации, представляющей интерес, данные переписки необходимо распечатать при помощи принтера, подключенного к компьютеру. Также на осматриваемом компьютере необходимо проверить наличие в интернет-браузере закладок с различными социальными сетями. Все логины и пароли, указанные при входе в социальные сети, фиксируются в протоколе.

С участием специалиста описываются все внешние устройства, подключенные на момент обыска к персональному компьютеру: USB-флеш-накопители, накопители на жестких магнитных дисках, портативные устройства в виде внешних жестких дисков, принтеры, сканеры, вэб-камеры и т. д., осуществляется проверка наличия дисков в дисководе.

Перед самой процедурой изъятия компьютера необходимо решить вопрос о полном изъятии техники, включающей в себя системный блок, монитор, и другие устройства. В случае, если специалистом будет установлен факт возможности работы накопителя жесткого диска отдельно от всей системы компьютера без ввода пароля для системы BIOS (англ. basic input/output system – «базовая система ввода-вывода), такая необходимость отсутствует и всю информацию, содержащуюся на компьютере, можно скопировать на внешний жесткий диск. Если для входа в систему BIOS потребуется введение пароля, изымать необходимо весь системный блок.

Помимо изъятия компьютерной техники, в ходе обыска необходимо заострить внимание на имеющемся документообороте, который, как правило, на постоянной основе ведется системным

администратором. Изъятие данных записей может содержать в себе информацию о дополнительных пользователях, подключенных к данной локальной сети, расположенных удаленно от места обыска, информацию об иных лицах, причастных к совершению данных преступлений, а также о лицах, в отношении которых было совершено либо только планируются противоправные деяния.

В протоколе обыска следователь должен подробно описать ход всего следственного действия, идентификационные признаки каждого изъятого устройства: марка, модель, цвет, серийный номер, если осмотр места происшествия (обыск) производится в офисе какой-либо из организаций, обратить внимание на инвентарный номер. В ходе обыска необходимо тщательно проверить все помещения, так как съемные носители, имеющие значение для расследования уголовного дела, могут быть запрятаны в тайники. В дополнение к вышеперечисленному, стоит также сделать акцент и на изъятии цифровых следов преступления, которые подробно были описаны в 1 параграфе настоящей главы.

В протоколе обыска должен быть детально описан порядок следственного действия, а также идентификационные характеристики каждого изъятого объекта, включая марку, модель, цвет и серийный номер изымаемого устройства. Если обыск проводится в помещении организации, следует обратить внимание на наличие инвентарного номера. В процессе обыска необходимо провести тщательный осмотр всех помещений, поскольку съемные носители информации, имеющие значение для уголовного расследования, могут быть спрятаны в тайниках.

Итак, при производстве обыска обязательно необходимо учитывать следующее:

1) Обеспечить контроль всех помещений, в которых установлена компьютерная техника, а также узел электропитания;
2) Обеспечить надлежащую охрану компьютерной техники с целью недопущения осуществления с ней каких-либо манипуляций; отключить сетевые соединения компьютерной техники;
3) Не допускать включения ранее выключенных устройств;
4) Произвести фото— и видеосъемку всей компьютерной техники и описать ее в протоколе обыска.
5) Если компьютерное устройство на момент проведения обыска включено, в протоколе обыска необходимо зафиксировать и описать изображение на мониторе.
6) Обнаружить и изъять все бумажные записи, на которых могут быть записаны пароли, сетевые адреса и другие значимые данные о совершенном преступлении.
7) В процессе проведения обыска необходимо получить от администратора сведения о паролях, имеющих значение к изъятой компьютерной технике.

Следственный эксперимент *по уголовным делам в сфере компьютерных и телекоммуникационных технологий.*

По общим правилам данное следственное действие осуществляется в порядке ст. 181 УПК РФ. Основной задачей проведения данного следственного действия является воспроизведение лицом действий, а также обстановки или иных обстоятельств определенного события. Особенностью данного следственного действия по преступлениям в сфере компьютерных или телекоммуникационных технологий является то, что в ходе его производства может быть установлена компетентность подозреваемого, его квалификационные навыки, например по использованию программ-шпионов за пользователями сети «Интернет», созданию фишинговых интернет-сайтов, создание вредоносных программ, получение дистанционного доступа к использованию банковских карт пользователей и т. д. Одной из сложностей производства

следственного эксперимента по данной категории уголовных дел является необходимость предоставления подозреваемому аналогичного технического оборудования для повторного воспроизведения действий.

Следующее следственное действие, которое нами будет рассмотрено – ***осмотр предметов и документов.***

По общим правилам, осмотр предметов производится в соответствии со статьей 177 УПК РФ. Данное следственное действие служит для детального изучения признаков доказательств путем осмотра представленных объектов, которые были изъяты при предшествующих следственных действиях (осмотре места происшествия, обыске, выемке). Например, в ходе осмотра был изъят системный блок системного администратора, который должен быть изучен на предмет наличия в нем значимой информации. После чего принимается решение о необходимости признания данного системного блока в качестве вещественного доказательства. Аналогичная процедура будет происходить со всеми предметами, изъятыми в ходе любых процессуальных действий, допустим, в ходе обыска был обнаружен блокнот подозреваемого, с имеющимися в нем записями о движении денежных средств по счетам пользователей. Указанный блокнот также необходимо осмотреть в установленном законом порядке с указанием его отличительных признаков, а также иных сведений, указав в протоколе осмотра предметов всю информацию, имеющую значение для расследования уголовного дела. Похожая ситуация будет обстоять и с документами бухгалтерской отчетности, в ходе осмотра которых необходимо обязательно указывать все реквизиты, печати/штампы, подписи и др. сведения. Кроме того, для установления подлинности подписей, выполненных в документах, а также принадлежности конкретных записей лицу, подозреваемому в совершении преступления, необходимо проведение почерковедческой судебной экспертизы, по результатам которой принимается окончательное решение о признании данных документов вещественными доказательствами по делу.

Также проводятся различного вида экспертизы, иные следственные и процессуальные действия, направляются запросы с целью установления IP-адреса злоумышленника следователем (дознавателем) провайдеру; запросы операторам сотовой связи для получения сведений об абонентах; запросы в банк и кредитные организации о получении данных о совершенных денежных операциях (сумма, дата и место проведения операции, № счета, с которого проводилось списание или зачисление похищенных денежных средств, кем открыты счета и др. данные); принимаются меры к возмещению вреда, причиненного преступлением.

Учитывая постоянный рост количества данных видов преступлений, органам предварительного расследования на первоначальном этапе расследования преступлений в сфере компьютерных и телекоммуникационных технологий стоит обратить внимание на качественное проведение следственных действий, формирующих доказательственную базу по уголовным делам, а также уяснить определенный алгоритм проведения отдельных следственных действий, в ходе которых происходит поиск, а также дальнейшее закрепление цифровых следов преступления. В то же время сотрудникам правоохранительных органов в процессе производства следственных действий, проводимых с целью изъятия и фиксации цифровых следов особое внимание необходимо уделить:

– снятию образов дисков рабочих станций, при помощи «FTK Imager», «UNIX утилита», «dd-dataset definition» — инструменты, используемые для получения дампов системы, подлежащей криминалистическому судебному анализу;
– анализу дисков, проводимом при помощи таких инструментов как: «The Sleuth

KIT(TSK)», «AutoPsy» или «Belkasoft» — предназначенных для проведения криминалистического анализа файловых систем, которые относятся к категории приложений «Судебного анализа данных»;

– поиску и сбору индикаторов компрометации IOCs (пакет аналитических программ «Sysinternals», «SCCM», «GRRRapidResponse» «Osquery»), данное действие заключается в наблюдении с целью обеспечения компьютерной безопасности в сети или на конкретном устройстве объекта (или активность), который с большой долей вероятности указывает на несанкционированный доступ к системе, то есть ее компрометацию. Такие индикаторы используются для обнаружения вредоносной активности на ранней стадии, а также для предотвращения известных угроз [Энциклопедия Касперского, www];
– дампам оперативной памяти рабочих станций, иными словами, содержимому рабочей памяти одного процесса, ядра или всей операционной системы. Данный анализ производится на основе программных платформ: «FTK Imager», «DumpIt»);
– анализу дампов памяти, которые осуществляются при помощи таких программ как: «Rekall», «Volatility», «FireEyeRedline»;
– определению источника заражения, в которое входит исследование почтового сервера, в частности журналы корпоративной почты, а также журналы прокси-сервера (файрволла, шлюза безопасности UTM или других устройств);
– исследованию журналов системных событий и событий информационной безопасности как в операционных системах, так и в различных средствах защиты информации;
– просмотру сетевых соединений;
– поиску скомпрометированных хостов, просмотр логов сетевых устройств («DNS (англ. domain name system) активность» — система, обеспечивающая работу привычных доменных имен сайтов, стоит помнить, что связь между устройствами в сети «Интернет» осуществляется по IP-адресам, о которых было подробно указано в первой главе; «Netflow-потоки» предназначены для учета сетевого трафика).

Заключение

Таким образом, вышеперечисленные следственные действия не являются универсальными, однако для начального этапа расследования преступлений рассматриваемого типа, с точки зрения получения наиболее значимых сведений, проведение этих следственных действий представляется минимально необходимым. Кроме того, организация и проведение следственных действий по делам о преступлениях, совершенных с использованием компьютерных и телекоммуникационных технологий, целиком и полностью зависят от типичных ситуаций, которые складываются на начальном этапе расследования преступлений данного вида.

Библиография

1. Елагина А.С. Интерпретация трендов уровня преступности: нормальные и шоковые изменения // Вопросы российского и международного права. 2018. Том 8. № 11А. С. 144-152.
2. Елагина А.С. Подходы к совершенствованию международного уголовного права // Вопросы российского и международного права. 2018. Том 8. № 10А. С. 96-101.
3. Краткая характеристика состояния преступности в Российской Федерации за январь – август 2023 года. URL: https://мвд.рф/reports/item/41741442
4. Свободная энциклопедия. URL: https://ru.wikipedia.org

5. Уголовно-процессуальный кодекс от 18.12.2001 № 174-ФЗ (ред. от 27.11.2023).
6. Уголовный кодекс от 13.06.2006 № 63-ФЗ (ред. от 04.08.2023).
7. Энциклопедия Касперского. URL: https://encyclopedia.kaspersky.ru/glossary/indicator-of-compromise-ioc/
8. Anderson R. et al. Measuring the cost of cybercrime //The economics of information security and privacy. – 2013. – C. 265-300.
9. Gordon S., Ford R. On the definition and classification of cybercrime //Journal in computer virology. – 2006. – T. 2. – C. 13-20.
10. Holt T., Bossler A. Cybercrime in progress: Theory and prevention of technology-enabled offenses. – Routledge, 2015.

Features of individual investigative actions for crimes in the field of computer and telecommunication technologies

Viktor V. Dolgaev

PhD in Law,
Associate Professor of the Departmentof Criminal Procedure Law,
North-West Branch of Russian State University of Justice,
197046, 5, Aleksandrovskii Park, Saint Petersburg, Russian Federation;
e-mail: dolgaevviktor@yandex.ru

Abstract

In this article, the author examines the features of conducting individual investigative actions in the context of investigating crimes in the field of computer and telecommunication technologies. Using the example of a typical investigative situation, when a person who committed a criminal act is detained, the author identifies a number of investigative actions aimed at collecting and securing evidence in cases of this category, namely: inspection of the scene of the incident, interrogation of the victim and suspect (or accused), search, conducting an investigative experiment, as well as examining objects and documents. In addition, the author of the paper provides some recommendations for searching for digital traces of a crime. It is finally concluded that all the investigative actions listed in the study are not universal, however, for the initial stage of the investigation of crimes of the type under consideration, from the point of view of obtaining the most significant information, carrying out these investigative actions seems to be minimally necessary. In addition, the organization and conduct of investigative actions in cases of crimes committed using computer and telecommunication technologies depend entirely on typical situations that arise at the initial stage of the investigation of crimes of this type.

For citation

Dolgaev V.V. (2023) Osobennosti proizvodstva otdel'nykh sledstvennykh deistvii po prestupleniyam v sfere komp'yuternykh i telekommunikatsionnykh tekhnologii [Features of individual investigative actions for crimes in the field of computer and telecommunication technologies]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 13 (11A), pp. 275-284. DOI: 10.34670/AR.2024.76.80.032

Keywords

Information, cybercrime, information security, computer and telecommunication technologies, digital traces.

References

1. Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. The economics of information security and privacy, 265-300.
2. Elagina A.S. (2018) Interpretatsiya trendov urovnya prestupnosti: normal'nye i shokovye izmeneniya [Interpretation of crime trends: normal and shock changes]. Voprosy rossiiskogo i mezhdunarodnogo prava [Matters of Russian and International Law], 8 (11A), pp. 144-152.
3. Elagina A.S. (2018) Podkhody k sovershenstvovaniyu mezhdunarodnogo ugolovnogo prava [Approaches to the improvement of international criminal law]. Voprosy rossiiskogo i mezhdunarodnogo prava [Matters of Russian and International Law], 8 (10A), pp. 96-101.
4. *Entsiklopediya Kasperskogo* [Kaspersky Encyclopedia]. Available at: https://encyclopedia.kaspersky.ru/glossary/indicator-of-compromise-ioc/ [Accessed 11/11/2023]
5. Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in computer virology, 2, 13-20.
6. Holt, T., & Bossler, A. (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.
7. *Kratkaya kharakteristika sostoyaniya prestupnosti v Rossiiskoi Federatsii za yanvar' – avgust 2023 goda* [Brief description of the state of crime in the Russian Federation for January – August 2023]. Available at: https://mvd.rf/reports/item/41741442 [Accessed 11/11/2023]
8. *Svobodnaya entsiklopediya* [Free encyclopedia]. Available at: https://ru.wikipedia.org [Accessed 11/11/2023]
9. *Ugolovno-protsessual'nyi kodeks ot 18.12.2001 № 174-FZ (red. ot 27.11.2023)* [Criminal Procedure Code of December 18, 2001 No. 174-FZ (as amended on November 27, 2023)].
10. *Ugolovnyi kodeks ot 13.06.2006 № 63-FZ (red. ot 04.08.2023)* [Criminal Code of June 13, 2006 No. 63-FZ (as amended on August 4, 2023)].