УДК 343.98(476)

Н. Н. БЕЛОМЫТЦЕВ

ОСОБЕННОСТИ ОБСТАНОВКИ СОВЕРШЕНИЯ ХИЩЕНИЯ ПУТЕМ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Статья посвящена актуальным вопросам обстановки совершения хищений путем использования компьютерной техники. На основании изучения научных взглядов и эмпирических данных проводится анализ основных элементов и свойств обстановки рассматриваемого хищения, а также их отличительные особенности. В результате исследования установлена взаимосвязь межу обстановкой и иными элементами криминалистической характеристики преступления, а также возможности использования сведений о ней при проведении следственных и иных процессуальных действий.

БЕЛОМЫТЦЕВ
Николай Николаевич,

майор милиции,
адъюнкт научно-педагогического факультета
Академии Министерства внутренних дел Республики Беларусь

N. N. BELOMITSEV

FEATURES OF THE THEFT ENVIRONMENT THROUGH THE USE OF COMPUTER THECHNOLOGY

The article deals with topical issues of the situation of theft by using computer technology. Based on the study of scientific views and empirical data, the analysis of the main elements and properties of the situation of the theft under consideration, as well as their distinctive features, is carried out. As a result of the study, an interrelation has been established between the situation and other elements of the criminalistic characteristics of the crime, as well as the possibility of using information about it during investigative and other procedural actions.

Любое преступное деяние совершается в конкретных, реальных условиях существования человека, сочетание которых в окружающей действительности образует обстановку, в которой совершается преступление. Как справедливо отмечает В. П. Шиенок, одним из наиболее важных моментов любого расследования наряду с установлением лица, совершившего уголовно наказуемое деяние, является выяснение обстоятельств произошедшего события [1, с. 149].

Исходя из практики расследования конкретных преступлений, выявление его криминалистической сущности обычно начинается с восприятия и изучения обстановки, в которой оно совершалось. Уяснение обстановки помогает не только разобраться в обстоятельствах преступного деяния, но и получить некоторые сведения о мотиве, цели, способе, субъекте и механизме совершения преступления, а также указывает на закономерности образования следовой картины и ее носителей. С практической точки зрения обстановка позволяет выбрать порядок и алгоритм проведения необходимых процессуальных и следственных действий.

Вопросы обстановки совершения преступлений в целом и конкретных преступных деяний рассматривались в работах Н. П. Яблокова [2], Р. С. Белкина [3], В. Ф. Ермоловича [4], В. А. Образцова [5], А. М. Кустова [6], В. И. Куликова [7] и ряда других ученых, мнения которых в некоторых аспектах расходятся. На наш взгляд, наиболее точно и полно это понятие определено Н. П. Яблоковым, который под обстановкой совершения преступления понимает систему различного рода взаимодействующих между собой до и в момент преступления объектов, явлений и процессов, характеризующих место, время, вещественные, природно-климатические, производственные, бытовые и иные условия

окружающей среды, особенности поведения непрямых участников противоправного события, психологические связи между ними и другие факторы объективной реальности, определяющие возможность, условия и иные обстоятельства совершения преступления [8].

Анализ следственной практики, юридической литературы дает возможность говорить о том, что обстановка совершения хищений путем использования компьютерной техники до настоящего времени подвергалась научному исследованию лишь в рамках уголовно-правовой оценки деяния [9], а также некоторые ее элементы рассматривались в рамках изучения методики расследования информационных преступлений [10; 11] и мошенничества в сфере компьютерной информации [12; 13]. Таким образом, имеющиеся сведения требуют дополнений и актуализации. В связи с чем считаем необходимым изучить в первую очередь существенные стороны обстановки совершения указанных хищений и отражения взаимосвязей с иными элементами криминалистической характеристики, а также ее влияния на методику его расследования в целом.

К элементам обстановки совершения преступлений в сфере информационной безопасности, оказывающим влияние на механизм совершения преступлений, как правило, исследователи относят организационные, пространственно-временные, технические, программные, социально-психологические факторы их подготовки, совершения и сокрытия, наличие либо отсутствие системы защиты информации [14, с. 63–67]. Данные элементы являются актуальными в том числе и для хищений с помощью компьютерной техники, так как данные преступления совершаются лишь путем изменения информации либо путем введения в компьютерную систему ложной информации. Вместе с тем особенностью данного рода преступлений является то, что на их совершение практически не оказывают влияние природно-климатические факторы [15; 16], за исключением ситуаций, препятствующих функционированию компьютерной техники и сетей (путей) передачи данных (отключение или перебои с подачей электроэнергии, а также разрыв и повреждение сетей передачи данных, вызванных стихийными бедствиями и катаклизмами). Отличительной особенностью выступает и наличие обязательного юридического факта завладения имуществом, а также функционирование программно-технического оборудования, осуществляющего управление финансовыми средствами потерпевшей стороны, что само по себе вытекает из объективной стороны рассматриваемого преступления [9, с. 83].

Рассмотрим вышеуказанные основные элементы обстановки хищения путем использования компьютерной техники более подробно.

Пространственно-временные факторы. Подготовка, совершение и сокрытие указанных хищений, как правило, разнесены в пространстве и во времени. Этим определяется особенность данных преступлений, в том числе связанных с созданием, использованием и распространением вредоносных программ: место непосредственного совершения противоправного деяния (место, где выполнялись действия объективной стороны состава преступления) и место наступления вредных последствий (место, где наступил результат противоправного деяния) не совпадают. Данная закономерность проявляется независимо от разновидности рассматриваемого преступного деяния. Исключением могут являться хищения путем использования компьютерной техники работниками финансовых учреждений.

Следует указать и на то, что время достижения преступной цели (завладение имуществом) после совершения некоторых противоправных действий может исчисляться долями секунды, но может существовать более значительный временной разрыв между ними. Одним из примеров последнего является тот случай, когда активация вредоносной программы установлена на определенную дату и время, отличающиеся от времени ее создания и внедрения, а также в тех случаях, когда срок ее существования определен конкретным временным промежутком, после которого она самостоятельно удаляется или не функционирует. Так, время активации вредоносного программного обеспечения при осуществлении хищения из банкоматов белорусского ЗАО «Альфа-Банк» было строго определено ее разработчиками. В процессе функционирования программа получала данные о системном времени банкомата (его программно-технической составляющей) и в случае, если оно не соответствует указанному в коде программы, завершала свою работу. Если же время совпадало, продолжала свое действие до операции выдачи наличных, и при успешном завершении банкомат выдавал купюры так называемому обнальщику (мулу) по заданным параметрам [17].

Местом подготовки данного преступления могут являться жилые и служебные помещения, которые оборудованы компьютерной и иной техникой или аппаратурой, в том числе для приобретения, разработки, модификации и распространения вредоносных программ, сбора компрометирующей информации, создания и направления во всевозможные финансовые учреждения подложных электронных расчетных документов, создания скиммингового и иного оборудования для совершения хищения, а также других подготовительных действий. При этом перечисленное даже по одному факту хищения, как правило, разнесено по разным местам (помещениям),

в том числе значительно удаленным друг от друга и расположенным как в разных регионах страны, так и за рубежом. Также местами подготовительных действий могут быть точки размещения банкоматов или POS-терминалов в случае предварительного их оборудования скимминговыми и иными устройствами.

Кроме того, к местам подготовки рассматриваемых хищений относятся помещения, в которых расположены серверы, в том числе в зарубежных странах. Данное обстоятельство подтверждается выявлением фактов совершения преступлений с использованием PROXY-серверов с IP-адресами других государств.

Местом совершения данных хищений, с одной стороны, могут быть как компьютерная система, или машинные носители информации, или сети передачи данных, в которых происходит изменение (ввод, удаление, блокирование, модификация) информации, либо в которые осуществляется введение ложной информации. С другой стороны, местом совершения преступного деяния является также местонахождение конкретного программно-технического средства (ПК, ноутбук, смартфон и др.), с которого осуществляется неправомерный доступ, где в основном и находится основной объем информации, характеризующий механизм совершения преступления (способ, орудия и средства, следы и т. п.).

В подавляющем большинстве (98,1 % от количества изученных уголовных дел; эмпирические данные были получены в ходе изучения 118 уголовных дел, возбужденных по ч. 2–4 ст. 212 УК Республики Беларусь) хищение путем использования компьютерной техники осуществляется со счетов клиентов финансовых учреждений, сведения и информация о наличии и движении денежных средств хранятся именно в данных учреждениях (за исключением хищений криптовалют). Закономерно, что местом, где наступил преступный результат, являются финансово-кредитная организация (например, банк) или платежная система, где открыты счета, с которых незаконно списываются денежные средства, а также точки размещения банкоматов (при хищении находящихся в них денежных средств с использованием программно-технических устройств).

При анализе полученных нами в ходе изучения уголовных дел сведений установлено, что в 88,7 % от общего числа случаев осуществления противоправных действий место фактического похищения имущества не совпадает с местом совершения действий по завладению имуществом.

Своеобразной средой, в которой совершается хищение путем использования компьютерной техники, может также являться киберпространство, частью его выступает глобальная сеть Интернет, представляющая, по предположению Д. А. Илюшина, международную информационно-телекоммуникационную сеть ЭВМ с отсутствием единого центра управления и организации, при этом доступ к которой осуществляется через соединения по сети передачи данных (сеанса связи) [18, с. 14].

Однако следует уточнить, что одной только сетью Интернет система обмена электронно-цифровой информацией не ограничивается.

По мнению В. А. Мещерякова, в состав кибернетического пространства также входят:

- отдельные помещения или их комплекс, где расположены автоматизированные информационно-вычислительные системы с техническим комплексом обеспечения их деятельности (системы связи, электропитания, заземления и т. п.);
- различные каналы передачи данных (в том числе звуковые волны и электромагнитные поля);
- машинные носители информации, обеспечивающие хранение информации в виде, пригодном для ее автоматизированной обработки;
- непосредственно сама информация, представленная в виде, пригодном для ее автоматизированной обработки (данные в соответствующих форматах, управляющие программы и т. п.);
- принятые порядок и последовательность (протоколы) автоматизированной обработки информации, а также установленные правила и распределение обязанностей между должностными лицами автоматизированной информационной системы [19, с. 15–16].

Несомненно, данное пространство, состоящее из вышеперечисленных элементов, является средой, где могут происходить подготовка, непосредственно совершение либо осуществляется сокрытие рассматриваемого преступления.

Очевидно, что указанные пространственно-временные обстоятельства определяют специфику процесса расследования хищений путем использования компьютерной техники и обуславливают необходимость обязательного международного сотрудничества в деятельности правоохранительных органов, что далее будет показано на примере практики взаимодействия правоохранительных органов Беларуси с Российской Федерацией, Украиной, США и другими странами при расследованиях такой категории уголовных дел.

Так, в Главном следственном управлении СК Республики Беларусь в 2013–2014 гг. расследовалось уголовное дело по обвинению граждан Республики Беларусь З., С., Б. и Г. в совершении преступлений, предусмотренных ч. 4 ст. 212, ст. 18 и ч. 2 ст. 351, ст. 18 и ч. 1 ст. 354 УК Республики Беларусь. Первичная информация, предоставленная из ФБР США, помогла выявить организованную преступную группу, состоящую в большинстве своем

из граждан Беларуси, Украины и России (предположительное число членов преступной группы — около 150 человек).

При подготовке преступной деятельности был создан вебсайт (размещен на вебсервере Федеративной Республики Германия) для объединения организованной преступной группы и управления ее деятельностью. На протяжении всего периода активности группы осуществлялось привлечение ее новых участников. Далее было создано вредоносное программное обеспечение (псевдоантивирус, так называемый Scareware, причем с платной подпиской). Членами организованной преступной группы — распространителями вредоносного программного обеспечения в глобальной сети Интернет — осуществлялись регистрация и администрирование серверов для размещения установочных файлов фальшивого антивируса, загрузка таких файлов на серверы для их последующей выгрузки. Указанный «антивирус» использовался с целью получения реквизитов банковских платежных карточек (далее — БПК) потерпевших лиц, ее пользователей, последующего их использования для хищения денежных средств с картсчетов граждан. Далее создавались биллинговые вебсайты (биллинг — возможность получать денежные средства от клиентов прямо через сайт) для обработки информации о платежах в счет приобретения фальшивого антивируса и аккумулирования реквизитов БПК пользователей зараженных компьютеров, с использованием которых совершались платежи без ведома их владельцев. Преступной организацией были заключены соглашения с процессинговыми компаниями приема платежей, банкамиэквайерами. Было установлено, что в период с января по апрель 2010 г. организованная группа с использованием незаконно полученных реквизитов БПК совершила более 260 000 эпизодов хищений денежных средств с картсчетов на сумму более 18 000 000 долларов США. Пострадавшими от описанной преступной деятельности стали более 267 000 граждан, проживающих в 123 государствах. Тем самым подготовка, осуществление и маскировка хищения происходили непосредственно через глобальную сеть Интернет и указанные составляющие киберпространства [20, с. 259–267].

Немаловажным аспектом для понимания способа и механизма совершения хищения является само отношение лиц к совершенному хищению, а именно к месту фактического расположения похищаемого. Весьма сомнительно, что средой и местом совершения преступления указанные лица воспринимают какой-то конкретный участок района города и страны, на котором размещен тот или иной финансовый орган либо проживает конкретное лицо. Зачастую преступникам все равно, где фактически находятся потерпевшая сторона и финансовый орган, а точнее непосредственно программно-техническое оборудование, обслуживающее тот или иной счет, либо финансовый сервис. В силу специфики совершения преступления для успешного похищения эти сведения не имеют большого значения, чему служит приведенный выше пример.

Как правило, юридический факт — хищение путем использования компьютерной техники — во многих случаях является самим фактом завладения имуществом, который измеряется долями секунды. При этом время подготовки к такому хищению и его сокрытию чаще всего имеет продолжительный период (до нескольких месяцев). Данное обстоятельство в большинстве случаев играет решающую роль для успешного завладения чужим имуществом. Примером может служить довольно распространенное хищение денежных средств с банковского счета с использованием реквизитов БПК (либо данных доступа к интернет-банкингу и иных платежных сервисов компаний), когда данные сведения становятся известными преступникам, в переписке с потерпевшим выдающим себя за знакомого или родственника. Так, неустановленное в ходе следствия лицо, не являясь держателем БПК ЗАО «МТБанк», эмитированной на имя Ш., имея умысел хищения имущества путем введения в компьютерную систему ложной информации, сопряженного с несанкционированным доступом к компьютерной информации, при использовании скомпрометированного доступа к странице «ВКонтакте» знакомого потерпевшей под предлогом перевода денег на счет Ш., узнав у последней реквизиты ее БПК, похитило принадлежащие Ш. денежные средства в размере 269 рублей 36 копеек, осуществив моментальную покупку в интернет-магазине, домен которого зарегистрирован в Украине. При этом преступником использовались указанные реквизиты БПК, а само завладение имуществом производилось моментально, как если бы это делала потерпевшая самостоятельно. Свидетельство этого — приобщенные к материалам уголовного дела переписка и сведения по картсчету из ЗАО «МТБанк», где время сообщения о списании денег со счета и время последнего сообщения потерпевшей с кодом подтверждения операции совпадают [21].

В данном случае хищение путем использования компьютерной техники следует считать оконченным с момента перевода денежных средств на счет преступника или подконтрольные ему счета других лиц, поскольку после этого он получает реальную возможность распоряжаться указанными деньгами по своему усмотрению [22, с. 463].

Технический фактор. К нему следует отнести особенности программно-технических устройств и сетей, используемых потерпевшей стороной, а также преступником(-ами). Как свидетельствует практика расследования преступных деяний, при наличии в них под-

готовительного этапа лица, совершающие киберхищения (в частности, хищения с использованием кибератак), в обязательном порядке изучают именно техническое оснащение объекта будущего посягательства. Так, результаты изучения уголовных дел показали, что в 72,4 % случаев осуществлялись подготовительные мероприятия, в том числе в форме изучения технических факторов. Исследование технической оснащенности потерпевшей стороны обусловлено, с одной стороны, более тщательной подготовкой к совершению преступления с целью самой возможности осуществления хищения, а также последующего уничтожения следов криминального деяния.

Как правило, выясняется, какое именно программно-техническое оборудование используется (тип, количество и т. д.), тип операционной системы, ее версия и наличие либо отсутствие обновлений, какое программное обеспечение установлено, имеется ли доступ к сети (локальной, глобальной), а также какое именно программно-техническое средство выходит в Интернет, связано ли оно с иными программно-техническими средствами на объекте нападения, имеющиеся недостатки в программном обеспечении (наличие либо отсутствие защитного программного обеспечения, необходимые обновления) и т. д.

Перечень технических факторов достаточно многообразен и включает как отдельные элементы, так и в целом автоматизированную информационную систему финансовой организации и ее возможности, в том числе способ подтверждения платежа (по SMS, 3D-Secure и др.), средства защиты компьютерной информации, правовые основы реализации компьютерной техники и т. п.

Использование тех или иных программно-технических средств преступником(-ами) может указывать на уровень подготовки, количественный состав преступной группы, их качественный уровень подготовки, а также предмет преступного посягательства. В некоторых случаях определяет способ совершения преступления, а также дальнейшие преступные действия по совершению и сокрытию преступной деятельности и подготовке к новым преступлениям.

Социально-психологические факторы. Профессиональные и личные качества как потерпевшей стороны, так и лиц, совершающих и причастных к рассматриваемому хищению, имеют немаловажное значение для обеспечения информационной безопасности. Чем выше уровень профессиональной подготовки специалиста, обеспечивающего защиту информации, тем более информативной будет «следовая картина», обусловленная особенностями обстановки совершения преступления [10, с. 60]. В свою очередь, чем выше данный уровень у виновного лица, тем сложнее будет установить его причастность к совершенному преступлению, о чем свидетельствует статистика раскрываемости преступлений. По данным управления по раскрытию преступлений в сфере высоких технологий, этот показатель в период с 2017 по 2018 г. составляет 43,95 % и имеется тенденция к понижению [23]. Кроме того, особенности поведения злоумышленника могут указывать на стремление адаптироваться к создавшейся ситуации, каким-либо образом изменить ее либо абсолютно пренебрегать ею, что в конечном счете отображается в предметах-носителях следовой картины (в том числе электронно-цифровой) преступления. Указанные обстоятельства также влияют на способ совершения преступления, ее предмет, а также следовую картину.

Завершая рассмотрение вопроса об особенностях обстановки хищений путем использования компьютерной техники, можно сделать следующие выводы:

• обстановка совершения преступления выступает систематизирующим элементом в рамках криминалистической характеристики рассматриваемого хищения. Ее изучение позволяет получить некоторые сведения об иных элементах криминалистической характеристики и эффективнее планировать и проводить следственные и иные процессуальные действия;

• отличительной особенностью обстановки совершения рассматриваемых хищений является наличие обязательного юридического факта — завладения имуществом, а также функционирование программно-технических средств как злоумышленников, так и потерпевшей стороны;

• зачастую местами совершения преступлений одновременно являются место осуществления подготовительных действий, реализации и сокрытия хищения, места обработки и хранения информации о наличии и движении денежных средств потерпевшей стороны, а также непосредственно места нахождения программно-технических средств, через которые осуществля-лось управление потерпевшей стороной своим имуществом, без какой-либо зависимости от государственного территориального расположения. Для удобства восприятия и понимания взаимодействия указанных программно-технических средств в пространстве логичным видится говорить о наличии киберпространства, в котором совершается полностью либо часть преступного деяния;

• время совершения рассматриваемого хищения в зависимости от способа и иных элементов складывающейся обстановки может исчисляться как долями секунд, так и месяцами. Также возможен разрыв во времени между совершением противоправных действий и достижением преступной цели. Хищение считается оконченным с момента перевода денежных средств на счет

преступника или подконтрольные счета других лиц;

• выяснение, установление и анализ принципа функционирования программно-технических средств сторон преступления зачастую указывают на их количественный и качественный состав, уровень подготовки и предмет преступного посягательства. В некоторых случаях определяются способ совершения преступления, дальнейшие преступные действия, а также подготовка к новым преступлениям.

Список использованных источников

1. Шиенок, В. П. Очерки гуманистической методологии национальной юриспруденции : монография / В. П. Шиенок. — 2-е изд., испр. и доп. — Минск : Междунар. ун-т «МИТСО», 2017. — 238 с.
2. Яблоков, Н. П. Обстановка совершения преступления как элемент его криминалистической характеристики / Н. П. Яблоков // Криминалистическая характеристика преступлений : сб. науч. тр. — М., 1984. — 165 с.
3. Белкин, Р. С. Курс криминалистики = Course of criminalistics : учеб. пособие / Р. С. Белкин. — 3-е изд., доп. — М. : Юнити-ДАНА, 2001. — 837 с.
4. Ермолович, В. Ф. Криминалистическая характеристика преступлений / В. Ф. Ермолович. — Минск : Амалфея, 2001. — 304 с.
5. Образцов, В. А. Характеристика элементно-компонентного состава объекта практического познания в уголовном судопроизводстве / В. А. Образцов // Криминалистика / под ред. В. А. Образцова. — М., 1997. — С. 47.
6. Кустов, А. М. Механизм преступления и его криминалистическое значение / А. М. Кустов // Криминалистика : учебник для студентов вузов / под ред. А. Ф. Волынского, В. П. Лаврова. — 2-е изд., перераб. и доп. — М., 2008. — С. 27–28.
7. Куликов, В. И. Обстановка совершения преступлений и ее криминалистическое значение : автореф. дис. ... д-ра юрид. наук : 12.00.09 / В. И. Куликов, — М., 1983. — 23 с.
8. Криминалистика : учебник / отв. ред. Н. П. Яблоков. — 3-е изд., перераб. и доп.— М. : Юристъ, 2005. — 781 с.
9. Макаревич, А. В. Парадигма уголовно-правовой оценки хищений с использованием информационных систем : дис. ... канд. юрид. наук : 12.00.08 / А. В. Макаревич. — Минск, 2014. — 120 с.
10. IT-справочник следователя / С. В. Зуев [и др.] ; под. общ. ред. С. В. Зуева. — М. : Юрлитинформ, 2019. — 232 с.
11. Лепехин, А. Н. Криминалистическое обеспечение расследования преступлений против информационной безопасности : дис. ... канд. юрид. наук : 12.00.09 / А. Н. Лепехин. — Минск, 2007. — 201 с.
12. Атаманов, Р. С. Основы методики расследования мошенничества в сети интернет : автореф. дис. ... канд. юрид. наук : 12.00.12 / Р. С. Атаманов. — М., 2012. — 28 с.
13. Коломинов, В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа : дис. ... канд. юрид. наук : 12.00.12 / В. В. Коломинов. — Иркутск, 2017. — 230 с.
14. Судебно-экспертное исследование компьютерных средств и систем: основы методического обеспечения : учеб. пособие / А. И. Усов / под ред. Е. Р. Россинской. — М. : Изд-во «Экзамен», изд-во «Право и закон», 2003. — 368 с.
15. Крылов, В. В. Расследование преступлений в сфере информации / В. В. Крылов. — М. : Городец, 1998. — 264 с.
16. Преступления в сфере информационной безопасности: квалификация и доказывание : учеб. пособие / под ред. Ю. В. Гаврилина. — М. : Юрид. ин-т МВД Рос. Федерации, 2003. — 245 с.
17. Cobalt: эволюция и совместные операции [Электронный ресурс]. — Режим доступа: https://www.group-ib.ru/resources/threat-research/cobalt-evolution.html. — Дата доступа: 26.04.2019.
18. Илюшин, Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет : автореф. дис. ... канд. юрид. наук : 12.00.09 / Д. А. Илюшин. — Волгоград, 2008. — 26 с.
19. Мещеряков, В. А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис. ... д-ра юрид. наук : 12.00.09 / В. А. Мещеряков. — Воронеж, 2001. — 22 с.
20. Положительный опыт главного следственного управления центрального аппарата Следственного комитета по расследованию преступлений управления центрального аппарата в сфере высоких технологий / под общ. ред. В. А. Гайдучёнока // Инф. бюл. Сл-го ком. / Сл. ком. Респ. Беларусь. — Минск, 2018. — Вып. 2 (10): Расследование уголовных дел о преступлениях в сфере информационных технологий. — С. 258–269.
21. Архив Советского (г. Минска) РОСК за 2018 г. — Уголовное дело № 1008.
22. Научно-практический комментарий к Уголовному кодексу Республики Беларусь / Н. Ф. Ахраменка [и др.] ; под ред. А. В. Баркова, В. М. Хомича. — 2-е изд., с изм. и доп. — Минск : Гос. ин-т упр. и соц. технологий Белорус. гос. ун-та, 2010. — 1064 с.
23. Управление по раскрытию преступлений в сфере высоких технологий (Управление «К») Статистические данные [Электронный ресурс]. — Режим доступа: https://www.mvd.gov.by/ru/page/upravlenie-po-raskrytiyu-prestuplenij-v-sfere-vysokih-tehnologij-upravlenie-k/stastistika-urpsvt. — Дата доступа: 23.08.2019.

19.09.2019