**Содержание:**

# Введение

Компьютерная преступность (преступление с использованием компьютера) - представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных. При этом, компьютерная информация является предметом или средством совершения преступления. Структура и динамика компьютерной преступности в разных странах существенно отличается друг от друга. В юридическом понятии, компьютерных преступлений, как преступлений специфических не существует.

В настоящее время имеются все основания полагать, что значительная часть преступлений, совершенных с применением информационных компьютерных технологий, остается нераскрытой вследствие высокой эффективности оказанного расследованию информационно-технологического противодействия. Таким образом, «главной проблемой в борьбе с преступлениями в сфере компьютерной информации является то, что выявляется их правоохранительными органами гораздо меньше, чем совершается» [4, 5].

Это является справедливым не только по отношению к преступлениям в сфере компьютерной информации, но и ко всем преступлениям, при совершении которых используются компьютерные технологии. Одной из основных особенностей таких преступлений является то, что способ и механизм их совершения, как правило, уже на начальном этапе предполагает включение действий, направленных на сокрытие.

# Глава 1. Компьютерные преступления

## Способы сокрытия преступлений

В преступлениях, совершенных с применением информационных компьютерных технологий преступник стремится прежде всего к тому, чтобы совершенные им противоправные действия не были обнаружены. Для этих целей, как правило,

используются достаточно сложные, с технической точки зрения, средства, которые чаще всего представляют собой новейшее программное обеспечение. Сложность этих средств является залогом того, что преступление не будет замечено право-охранительными органами. Справедливо отмечается, что «наиболее частым способом инсценировки является то, что преступник использует технические возможности компьютерных сетей и специальные программы для того, чтобы при обнаружении преступления следы, оставленные в сети, указывали не на него (или, точнее, его компьютер), а на совершенно другое лицо, которое может и не подозревать о совершении этого преступления» [3, 7].

В этом случае преступник достигает прежде всего анонимности, что обеспечивает безнаказанность и возможность в последующем совершать аналогичные действия. Очевидно, что длительное их совершение ведет к тому, что преступники улучшают применяемые ими способы и средства. Таким образом, постепенно достигается настолько высокий уровень преступлений, что их обнаружение становится для правоохранительных органов более проблематичным.

Очевидно, именно в этом отчасти кроется причина высокой латентности преступлений, совершенных с применением информационных компьютерных технологий. Для того чтобы скрыть свою личность, преступник прибегает к специальным программам, созданным с учетом принципа так называемой «луковичной маршрутизации» (tor), используемой для передачи информации в глобальной сети Интернет.

Данная технология позволяет сохранять анонимность при посещении сайтов, публикации материалов, отправке сообщений благодаря созданию сети маршрутизаторов (серверов-«посредников»), через которые устанавливается соединение.

Учитывая, что таких «посредников» много и значительная их часть находится за пределами одного государства, то правоохранительным службам этого государства бывает сложно установить как потребителя информации с того или иного сайта, так и того, кто ее на нем оставил. Отметим, что устанавливаемая цепочка связи шифруется. Все это делает установление личности того, кто использует подобную программу, почти невозможным. Существует другие способы обеспечения анонимности в глобальной сети. Например, с помощью веб-прокси, суть которых состоит в том, что услуга анонимности предоставляется определенными веб-сайтами. Еще один способ предполагает заражение вирусом соответствующего сайта или адреса электронной почты конкретного пользователя

и позволяет добиться сразу двух целей: преступного результата и сохранения анонимности. Необходимо отметить, что действия, направленные на сокрытие преступлений с применением информационных компьютерных технологий, не ограничиваются названными способами. Информационные технологии постоянно развиваются, а вместе с ними совершенствуются способы сокрытия подобных преступлений.

Более того, бурное развитие этих технологий способствует появлению принципиально новых способов. Именно поэтому в настоящее время не представляется возможным составить их исчерпывающий перечень. Одним из распространенных методов сокрытия преступлений, совершенных с применением информационных компьютерных технологий, является имитация технического сбоя, который, как правило, связан с перебоями в энергоснабжении или несовместимостью программного обеспечения.

В последнем случае они могут приводить к завершению работы программ, «зависанию» компьютера и даже утрате части информации. Имитация такой несовместимости иногда используется преступниками для уничтожения определенных сведений или «взлома» защиты с целью совершения противоправных действий.

Существуют и другие виды сокрытия преступлений. Их выбор во многом зависит от особенностей совершенного деяния, или используемого программного обеспечения, или от особенностей (прежде всего интеллектуальных) того лица, которое планирует и организует сокрытие. Одной из разновидностей сокрытия преступлений является преступная инсценировка.

В. И. Фадеев определяет ее как «деятельность субъекта преступления по сокрытию (видоизменению) совершенного преступления (аморального поступка) и (или) совершению преступления, характеризующаяся умышленным созданием ложной субъектной, предметной, пространственной, временной, информационной, следовой обстановки, скрывающей умысел и цели преступника» [6, 9].

Сопоставление данного определения с практикой расследования преступлений, совершенных с применением информационных компьютерных технологий, заставляет усомниться в возможности распространения данного определения на рассматриваемую область. Прежде всего, возникает сомнение, что преступная инсценировка является результатом деятельности только субъекта преступления. Анализ практики расследования позволяет утверждать, что не только субъекты

преступления участвуют в преступных инсценировках; к ним могут привлекаться лица, не подозревающие о том, что было совершено преступление.

Так, преступник (преступники) может привлекать программистов к тому, чтобы модернизировать то или иное программное обеспечение, согласно конкретным нуждам потребителя. При этом перед специалистами могут быть поставлены такие задачи по улучшению программного обеспечения, выполнение которых позволит не только успешно совершить преступление, но и инсценировать его.

Например, известно, что программное обеспечение анонимности в настоящее время используется для того, чтобы преодолевать цензуру в Интернете. Отметим, что оно способно не только обеспечить анонимность, но и преодолеть блокировку отдельных сайтов. Умелая модификация соответствующих программ способна привести к тому, что они смогут преодолевать защиту отдельных сайтов, банковских счетов и т. д.

При этом такое преодоление, как правило, инсценирует источник, из которого была произведена атака. Очевидно, что программист в данном случае не является субъектом преступления, однако именно благодаря его участию преступная инсценировка стала возможной, поэтому его деятельность по модификации программного обеспечения также следует рассматривать причастной к преступлению. Не менее распространенными в последнее время стали отвлекающие хакерские атаки. Как правило, они проводятся достаточно организованно, но при этом многие их участники не знают истинных целей организаторов этих атак и руководствуются не стремлением добиться какого-либо преступного результата, а своего рода «спортивным» интересом, возможностью продемонстрировать силу своего интеллекта.

Однако именно они способствуют преступной инсценировке. В последнее время достаточно распространенными стали преступления по хищению средств с банковских счетов. Достаточно часто их скрывают именно с помощью хакерской атаки. Существуют и другие случаи, когда то или иное лицо, не являясь субъектом преступления, участвует (часто не осознавая этого) в совершении преступной инсценировки. Так, учитывая, что социальная среда благоволит киберпреступникам, находится немало пользователей компьютерных сетей, которые готовы бескорыстно содействовать этим преступникам в инсценировке или любом другом способе сокрытия совершенного ими преступления.

Отчасти это объясняется тем, что внутри различных категорий компьютерных пользователей наблюдается солидарность, проявляющаяся в готовности помочь другому такому же пользователю в трудную для него минуту, не разбираясь при этом в сути тех причин, по которым эти трудности возникли.

Главным для них в этом случае является осознание того, что киберпреступник – пользователь, относящийся к аналогичной категории. При этом такие лица могут не иметь личного знакомства с преступником и, соответственно, не знать о его преступных намерениях.

Очевидно, что они также не являются субъектами преступления, однако их роль в инсценировке может быть значительной. Все виды преступной инсценировки во многом обусловлены спецификой отношений, возникающих между пользователями глобальных сетей и далеко не всегда основанных на корысти. К сожалению, такая среда часто используется как для совершения преступлений с применением высоких технологий, так и для их сокрытия. По этой причине нельзя ограничивать круг лиц, которые могут быть причастными к инсценировке только субъектами преступления.

В связи с этим мы считаем, что определение инсценировки, данное Р. С. Белкиным, в большей мере отображает реалии совершения преступлений с применением информационных компьютерных технологий. Так, он писал, что инсценировка преступлений – это «создание обстановки, не соответствующей фактически происшедшему на этом месте событию; может дополняться ложным поведением и ложными сообщениями» [1, 4]. При этом ученый отмечал, что все инсцинировки классифицируются «по субъекту – совершаемые преступником(ами) или иными лицами». Очевидно, Р. С. Белкин не считал правильным ограничивать понятие инсценировок только теми из них, которые совершены субъектами преступления.

Такой подход считается наиболее целесообразным. Р. С. Белкин также полагал, что инсценировка относится к смешанным способам сокрытия преступлений: «Смешанные способы сокрытия преступления представлены в следственной практике различными инсценировками или, по старой терминологии, различными видами симуляции обстоятельств преступления» [2, 5].

При этом справедливо замечание о том, что в «инсценировках могут присутствовать элементы и фальсификации, и утаивания, и уничтожения, и маскировки» [5, 7]. Применение конкретного способа сокрытия зависит от вида соответствующего преступления. Таким образом, совершение определенного вида

преступления позволяет с высокой степенью вероятности предположить примененным способ его сокрытия, то есть в какой-то степени способ сокрытия и конкретный вид преступления идентифицируют друг друга. Следует отметить, что среди способов сокрытия преступлений, совершенных с применением информационных компьютерных технологий, наиболее распространенным является преступная инсценировка, поскольку эффективность других не настолько высока.

Так, например, утаивание, уничтожение или маскировку информации достаточно легко обнаружить с помощью соответствующих программ. Кроме того, преступления, при совершении которых применяются информационные компьютерные технологии, в силу своих особенностей предполагают преимущественное использование преступных инсценировок, поскольку они позволяют как сохранить анонимность, так и достигнуть преступного результата.

При этом совершение преступной инсценировки предполагается преступниками уже на стадии планирования преступления. Отдельные действия, составляющие преступление, могут быть не только элементами данного преступления, но и одновременно являться частью системы, составляющей инсценировку.

Особенностью в этом случае является то, что если нет возможности создания инсценировки, то преступник может отказаться от совершения соответствующего преступления. Таким образом, возможность создания преступной инсценировки является одним из условий совершения преступлений, в которых применяются информационные компьютерные технологии.

- 1. **Средства совершения компьютерных преступлений**

Быстрое развитие компьютерных технологий сопровождается ростом компьютерной преступности и, что еще более важно, ее качественным изменением. Преступления совершаются более изощренными способами с применением специальных программно-аппаратных средств и сетевых технологий. Способы совершения компьютерных преступлений становятся высокотехнологичными за счет применения нетривиальных технических решений, а также принципиально новых или модифицированных программ [1]. Преступники творчески используют и модифицируют компьютерную технику и программное обеспечение. Результатом таких действий становится исключительно высокая латентность компьютерных преступлений [2]. Вопрос о средствах совершения компьютерных преступлений, рассматриваемых с криминалистических позиций,

является малоизученным. От современной криминалистики требуется изучение причин, благодаря которым компьютерные преступления становятся возможными, анализ применяемых преступниками технологий, аппаратных и программных средств подготовки, совершения и сокрытия преступлений.

Эти вопросы входят в криминалистическую характеристику компьютерных преступлений и являются предметом доказывания по данной категории уголовных дел.

Преступления в сфере компьютерной информации всегда совершаются с помощью средств компьютерной техники. Понятие этих средства является комплексным, включающим в себя компьютеры в различных вариантах их исполнения (ноутбуки, планшеты, смартфоны, и т.д.), компьютерные технологии (беспроводные Wi-Fi, Bluetooth, 3G, WiMAX и др.), а также компьютерное программное обеспечение, находящееся в открытом, запрещенном или ограниченном обороте и имеющее различное назначение (разрешенные и бесплатно распространяемые программы, например, Opera, Mozilla Firefox, вредоносные программы, например, SpyEye, Zeus, Carberp и т.д.). Следует отметить, что в настоящее время главную роль при совершении компьютерных преступлений выполняет программное обеспечение, а не аппаратные средства, которые сами по себе обычно не представляют опасности. Как показывает современная практика, в большинстве случаев компьютерные преступления совершаются путем удаленного доступа по телекоммуникационным сетям с помощью обычной компьютерной техники, на которую устанавливается специальное программное обеспечение [3].

Это принципиальное обстоятельство имеет следствия, исключительно важные как для расследования, так и для предотвращения компьютерных преступлений. Так, в непосредственных (бессетевых) способах совершения преступлений аппаратные средства, например аппаратные кейлогеры или скиммеры для негласного съема информации, действуют лишь в отношении конкретного компьютерного устройства. Преступники хорошо знают, что при совершении преступления непосредственным образом остаются традиционные (материальные) следы, по которым можно будет их идентифицировать. Использование вредоносного программного обеспечения при удаленном доступе по информационным сетям позволяет осуществить преступление одновременно в отношении многих компьютеров.

При таком доступе преступникам не нужно проникать в помещение, в котором находится объект посягательства, при этом остаются не персонифицируемыми их

электронно-цифровые следы. Электронно-цифровые следы всегда образуются и модифицируются в результате опосредованного воздействия компьютерных программ. Специфика этих следов проявляется в том, что они не имеют геометрической формы, цвета, запаха и иных характеристик, традиционно рассматриваемых криминалистикой, в которых могли бы отразиться отельные черты преступника, например его ДНК, запах, папиллярный узор и т.д.

Таким образом, в механизме следообразования нет непосредственного следового контакта с преступником, его физическими и иными особенностями, так как компьютерная программа не несет на себе отпечатка конкретного человека, одни и те же электронно-цифровые следы-последствия могут быть образованы кем угодно.

Несмотря на эту специфику, основным источником информации о средствах, применяемых в компьютерном преступлении, остаются именно конкретные следы и вся следовая картина в целом. В настоящее время для совершения большинства компьютерных преступлений не требуется наличия средств преступления в виде дорогостоящей компьютерной техники.

Практически каждый может найти в сети Интернет бесплатные вредоносные программы, включающие в себя необходимый для совершения преступления алгоритм действий. К таким программам могут прикладываться наглядные инструкции по их использованию. Эти обстоятельства в значительной степени способствуют росту числа совершаемых преступлений в сфере компьютерной информации [4]. Более того, помимо количества преступлений, меняется типичный портрет преступника в сторону лиц, не имеющих специального или высшего образования и постоянной работы [5, 8]. Следственные органы, особенно на первоначальном этапе расследования компьютерных преступлений, редко располагают сведениями о средствах, используемых в преступлении.

В отсутствие такой информации имеет важную роль для проведения расследования криминалистическая характеристика аналогичных преступлений. Ее практическое значение, проявляющееся в корреляционной взаимосвязи между структурными элементами преступления, дает основания строить следственные версии на основе использования имеющихся неполных данных.

В компьютерных преступлениях выбор средств для их совершения обычно зависит от целого ряда факторов: объекта посягательства, принятого на нем режима охраны, применяемых технических и организационных средств охраны,

программно-аппаратной защиты информации. Так как в большинстве случаев поводом для возбуждения уголовных дел являются заявления потерпевших, то следствию становится известен объект посягательства. Его исследование может пролить свет на способ совершения преступления или примененные преступником программно-аппаратные средства. Анализ судебно-следственной практики показывает, что типичные (относительно простые) или, наоборот, высокотехнологичные способы совершения преступлений могут осуществляться характерными для них программно-аппаратными средствами.

Возможна также обратная ситуация, когда данные о средствах преступления известны и помогают строить следственные версии о других искомых элементах преступления. Например, конкретные средства совершения преступления могут указывать на применяемый преступниками способ совершения преступления, а также время и место его осуществления. Средства, которые используются при совершении преступлений в сфере компьютерной информации, достаточно разнообразны.

Важно также, что с криминалистических позиций их можно классифицировать по существенно различным критериям:

по законности происхождения;

по созданию;

по техническому содержанию;

по технологии использования;

по стадии в преступлении и др.

Это обусловливает необходимость разработки системы криминалистической классификации. В целях повышения эффективности расследования компьютерных преступлений разнообразные средства их совершения следует классифицировать, учитывая их основные особенности.

Преступниками может применяться не только широкий перечень готового программно-аппаратного обеспечения, в том числе модифицированного, но и собственные уникальные разработки. Это наиболее характерно для высокотехнологичных способов совершения компьютерных преступлений, при которых используются компьютерные программы, созданные членами преступной группы или посторонними специалистами по заказу преступников.

В этом случае речь идет прежде всего о так называемых шеллах (shell), которые позволяют преступнику выполнять ограниченный круг команд по управлению автоматизированным рабочим местом (например, выполнить какое-либо действие командной оболочки операционной системы и т.п.).

По техническому содержанию рассматриваемые средства могут быть условно разделены на аппаратные, программные и программно-аппаратные. При незаконном доступе к объекту посягательства использование чисто аппаратных средств мало распространено, так как современные компьютерные устройства обычно обладают каким-либо собственным программным обеспечением.

Как показывает судебно-следственная практика, примерами программно-аппаратных устройств выступают скиммеры и кейлогеры. Скиммеры используют для кражи реквизитов банковских карт. Как правило, скиммер состоит из двух компонентов – устройства для считывания данных хранящейся на магнитной полосе банковской карты и устройства, позволяющего скопировать пин-код.

Некоторые скиммеры оснащены инструментами беспроводной связи, с помощью которой злоумышленники получают информацию в реальном времени, а не хранят ее непосредственно на скиммере. Кейлогеры представляют собой устройства, которые позволяют перехватывать данные, вводимые с клавиатуры. Они выполняются в различных вариантах и могут хранить полученную информацию в собственной памяти или быть оснащены средствами беспроводной связи. Программное обеспечение, используемое для незаконного доступа к компьютерной информации, может быть признано вредоносным только судом. Отметим, что четкого определения вредоносного программного обеспечения в ст. 273 УК РФ не дается, что требует отдельного рассмотрения.

При проведении расследовании целесообразно учитывать, что конкретные средства совершения компьютерных преступлений могут использоваться только на определенных стадиях – подготовки к преступлению, непосредственно при его совершении, при сокрытии преступления, при противодействии следствию в условиях оперативно-розыскных мероприятий или следственных действий.

Так, на стадии подготовки преступники изучают обстановку объекта посягательства, физический режим его охраны (замки, контроль сотрудниками, видеонаблюдение, сигнализацию), пытаются собрать информацию о действующих устройствах и программах информационной безопасности (системах идентификации и аутентификации), готовят хранилища для переноса охраняемой

информации (flash носители, облачные хранилища и пр.), средства сокрытия и уничтожения следов своей деятельности (например, размагничивание жесткого диска).

На этой стадии могут применяться специальные программы, исследующие и оценивающие объект посягательства с точки зрения его защищенности внешним угрозам (например, программы-шпионы типа Zeus).

Непосредственно на этапе совершения преступления соответствующие средства направлены на получение преступником возможности управлять автоматизированным рабочим местом потерпевшего. Для получения неправомерного доступа преступники могут использовать программы, предназначенные для администраторов (TeamViewer, Radmin, TightVNC и т.п.), специализированные клиенты сетевых протоколов RDP (Remote Desktop Protocol) или VNC (Virtual Network Computing), имеющие собственный web-интерфейс для администрирования и управления, либо модификации вредоносного программного обеспечения, например Zeus, Carberp и т.п.

Опасной разновидностью вредоносного программного обеспечения, позволяющего получить неправомерный доступ к автоматизированному рабочему месту, являются эксплойты, под которыми понимается программный код или его фрагмент, который через ошибки в каком-либо программном обеспечении, работающем на объекте посягательства, приводит к выполнению этим программным обеспечением действия, непредусмотренного разработчиками.

При попытке массового заражения рабочих мест через использование web-сервисов применяются инструменты, которые включают в себя наборы эксплойтов, нацеленные на эксплуатацию ошибок в web-браузерах и различного рода расширений к ним (Adobe Flash, ActiveX и т.п.). Сокрытие преступления, отдельных следов-последствий и участия в нем преступника может реализовываться во время совершения преступления и после него.

Для этой цели могут применяться различные элементы маскировки, например: программно-аппаратный сбой, противоправные действия иных лиц и многое другое. Отметим, что для сокрытия электронно-цифровых следов может применяться не только вредоносное, но и законное программное обеспечение, например, позволяющее безвозвратно удалять информацию с носителя путем многократной ее перезаписи. Как правило, сокрытие сводится к попытке затруднить определение местонахождения преступников. Подобная цель может

достигаться путем использования сервисов, позволяющих осуществить подмену реального IP-адреса на другой. Популярностью у преступников пользуются услуги предоставления доступа к сети, работающей по протоколу VPN. Современные VPN-сервисы предоставляют доступ к сети путем использования цепочки промежуточных серверов (Double/Triple-VPN), что значитель- но затрудняет определение реального IP-адреса преступника. В случаях, когда не требуется высокая пропускная способность канала связи, преступник может отдать предпочтение таким технологиям, как Tor, ввиду бесплатного предоставления анонимности при работе в телекоммуникационных сетях. Исследование средств совершения компьютерных преступлений с позиций криминалистики, их типизация и классификация позволяют установить корреляционные связи между обстоятельствами, подлежащими установлению и доказыванию по уголовным делам, что способно повысить эффективность расследования подобных преступлений.

# Глава 2 Проблемы оптимизации российского уголовного законодательства, регламентирующего ответственность за преступления, совершаемые с использованием компьютерных технологий

## 2.1. Особенности российского уголовного законодательства, регламентирующего ответственность за преступления, совершаемые с использованием компьютерных технологий

Развитие технологий в современном обществе достаточно динамично. Технические новинки делают нашу жизнь проще, удобнее и безопасней.

К сожалению, параллельно происходит и обратный процесс – современные технические разработки все чаще применяются и для облегчения совершения различных противоправных деяний. До недавнего времени законодатель обходил

своим вниманием необходимость модернизации норм об ответственности за совершение преступлений с использованием компьютерных технологий.

Позитивные изменения в данном вопросе наметились только в конце 2011 – начале 2012 г., в связи с принятием Федерального закона от 07 декабря 2011 г. № 420 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [2], в соответствии с которым были внесены изменения в главу 28 УК «Преступления в сфере компьютерной информации», а также Федерального закона от 29 февраля 2012 г. № 14 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации в целях усиления ответственности за преступления сексуального характера, совершенные в отношении несовершеннолетних» [4], который привнес в статью 242.1 УК РФ квалифицирующий признак - совершение преступления с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть «Интернет»).

Очередным шагом законодателя на пути модернизации современного российского уголовного законодательства в соответствии с требованиями, предъявляемыми информационным сообществом, явилось принятие Федерального закона от 29 ноября 2012 г. № 207 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [3].

В соответствии с этим законом в Уголовный кодекс России введены специальные составы мошенничества, в том числе и мошенничество с использованием платежных карт (статья 159.3 УК РФ). Высокие технологии позволяют лицам, владеющим ими, совершать преступления со все возрастающей эффективностью и с легкостью избегать наказания. Не обошла эта тенденция и сферу мошеннических операций.

Современный мошенник не только и не столько сидящий в переходе метро наперсточник и не улыбчивый зазывала, предлагающий всего за сто рублей попытать счастье и выиграть телевизор. Современные мошенники активно используют технические новинки для совершения преступлений. Одним из самых распространенных видов высокотехнологичного мошенничества является мошенничество с использованием платежных карт. Это обусловлено несколькими факторами.

Среди них как обширное распространение платежных карт среди населения, так и низкая культура обращения с этими картами; как сравнительная легкость получения данных карты жертвы, так и сложность идентификации мошенника и сбора доказательств его вины. В соответствии с этим законодатель посчитал совершение мошенничества с использованием платежных карт настолько серьезной разновидностью мошенничества, что ввел в Уголовный кодекс отдельную статью, предусматривающую уголовную ответственность за совершение данного деяния.

Введение в Уголовный кодекс Российской Федерации статьи, предусматривающей ответственность за совершение мошенничества с использованием платежных карт, - это абсолютная новелла для российского права. Хотя теоретики изучения киберпреступлений давно указывали на необходимость введения такого состава в российское уголовное право [1].

Подобные составы давно включены в уголовное законодательство многих зарубежных государств. К сожалению, примененная законодателем конструкция статьи и использованные формулировки несовершенны и, на наш взгляд, нуждаются в доработке. Диспозиция части 1 статьи 159.3 УК сформулирована следующим образом: мошенничество с использованием платежных карт, то есть хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации.

Непосредственным объектом указанного преступления, как видно из диспозиции, является собственность, то есть общественные отношения, связанные с владением, пользованием и распоряжением имуществом. Объективную сторону составляет определенный вид противоправного поведения, а именно: мошенничество с использованием платежных карт, то есть хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации.

При этом сущность мошенничества как хищения чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием сохраняется и в рамках данного состава преступления. Под хищением, в соответствии с примечанием 1 к статье 158 УК, понимается совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение

чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества.

При этом законодателем допущена некорректная формулировка предусмотренного статьей 159.3 УК со- става преступления. Исходя из буквального прочтения диспозиции, объективная сторона преступления не- обоснованно урезана: из нее исключено приобретение права на чужое имущество. Также при буквальном толковании исчезает один из способов совершения мошенничества: путем злоупотребления доверием. Мошенничество с использованием платежных карт возможно только с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты.

При этом законодательное закрепление формулировки термина «платежная карта» отсутствует, что может привести к разночтениям при применении указанной нормы. Существует термин банковская платежная карта, под которой понимается пластиковая карта, привязанная к одному или нескольким расчетным счетам в банке [5]. Кроме того, используется термин «банковская карта», по своему смыслу эквивалентный предыдущему.

Таким образом, критерием отнесения карты к банковской платежной является ее привязка к банковскому счету. Но «банковская платежная карта» и «платежная карта» - это не одно и то же, так как существуют определенные сервисы (например: Qiwi, WebMoney, Яндекс.Деньги и т.д.), не являющиеся банками, но оказывающие содействие в оплате товаров и услуг.

Кроме того, некоторые сервисы оказывают услуги по созданию «виртуальной платежной карты», которая обладает всеми признаками банковской карты, кроме одного: она не существует на материальном носителе. Попадает ли мошенничество с использованием карт таких сервисов под признаки состава преступления, предусмотренного статьей 159.3 УК, покажут только разъяснения законодателя и судебная практика. Однако уже сейчас можно сказать, что, помимо платежных карт, существуют бонусные, подарочные, накопительные и иные карты, действия с которыми, видимо, не образуют состава указанного преступления.

Мошенничество с использованием банковских карт возможно только путем обмана уполномоченного работника кредитной, торговой или иной организации. Как уже было сказано выше, законодатель необоснованно исключает из состава такой способ мошенничества, как «злоупотребление доверием», а кроме того, вводит абсолютно бесполезный здесь ограничитель «уполномоченного работника».

Непонятно, кто является таким лицом. Исходя из буквального толкования статьи, можно заключить, что лицо, осуществившее действия с картой через «неуполномоченного работника», ответственности не несет.

Равно, не несет ответственности лицо, использующее злоупотребление доверием или использующее карту путем обмана не работника, а например, собственника карты. Формулировка в диспозиции статьи «другому лицу» подразумевает только физическое лицо. Однако существуют так называемые корпоративные банковские карты, которые выпускаются на организацию или индивидуального предпринимателя (юридическое лицо).

Субъект преступления общий - вменяемое физическое лицо, достигшее возраста наступления уголовной ответственности (16 лет). Субъективная сторона преступления характеризуется прямым умыслом. Злоумышленник осознает общественную опасность мошеннических операций с использованием платежных карт, предвидит наступление общественно опасных последствий и желает их наступления. Части вторая-четвертая указанной статьи содержат квалифицирующие признаки преступления, полностью совпадающие с закрепленными в статье 159 УК.

Указанные признаки не нуждаются в дополнительном толковании. Ответственность за совершение мошенничества с использованием платежных карт, закрепленная в санкциях частей статьи 159.3 УК, дословно соответствует формулировкам статьи 159.6 УК, анализ которой про- изведен выше. Здесь следует отметить, что отнесение состава статьи 159.3 УК к привилегированным, а не квалифицированным, и, как следствие, установление более мягкой санкции по сравнению с общим составом мошенничества (статья 159 УК РФ), является нелогичным законодательным решением, поскольку степень общественной опасности данного деяния гораздо выше, чем деяния, ответственность за совершение которого предусмотрена статьей 159 УК.

В целом, подводя итог анализу статьи 159.3 УК, можно заключить, что нормы, содержащиеся в данной статье, достаточно непроработаны. Попытка законодателя регламентировать ответственность за особую разновидность мошенничества с использованием законодательно не закрепленных терминов, в правоприменительной практике может привести к возникновению серьезных сложностей в толковании закона. Кроме того, необоснованное исключение из диспозиции статьи признаков обычного состава мошенничества ограничивает сферу ее применения. И, наконец, смягчение санкции за совершение

мошенничества с использованием платежных карт недопустимо, поскольку данное деяние имеет большую степень общественной опасности, чем обычное мошенничество.

## 2.2. Некоторые аспекты раскрытия преступлений, совершаемых в сфере высоких технологий

В доктрину информационной безопасности входит «охрана информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем как функционирующих, так и создаваемых на территории России» [1, 8]. Преступления в сфере высоких технологий предусмотрены главой 28 Уголовного кодекса Российской Федерации и представляют собой общественно опасные деяния, направленные против безопасности компьютерной информации и причиняющие вред охраняемым законом благам и интересам: ст. 272 «Неправомерный доступ к компьютерной информации»; ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ»; ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» [2, 9].

Высокая общественная опасность преступлений, совершенных с использованием глобальной сети Интернет, напрямую зависит от транснационального характера их совершения, т.к. количество преступников может быть достаточно велико и нередко они проживают в разных странах. При совершении преступлений в рассматриваемой сфере, в отличие от других видов преступлений, предусмотренных Уголовным кодексом РФ, преступник на- прямую не контактирует с потерпевшим, что также не позволяет своевременно принять меры для раскрытия преступления. Наличие компьютерной информации напрямую связано с ее утечкой, разрушением, риском противоправного использования, изъятием или дополнением необъективной информацией. При совершении преступлений преступники посягают на права и интересы граждан, предприятий и др. категорий пользователей, непосредственно связанных с хранением информации.

В законодательстве Российской Федерации, которое так или иначе регулирует сферу высоких технологий, выделить ряд действий, связанных с информацией и подпадающих под защиту, к таковым относятся:

создание и обработка информации;

сбор и поиск информации (в т.ч. доступ к ней);

накопление и хранение информации; защита информации;

распространение и предоставление информации; непредставление информации;

копирование информации;

уничтожение информации; изменение (модификация) информации;

хищение, изъятие и утрата информации;

блокирование информации [3, 11].

Практика деятельности органов внутренних дел позволяет выделить наиболее распространенные характерные черты преступлений, совершаемых в сфере высоких технологий, к данным особенностям относятся:

1) общественная опасность;

2) устойчивость;

3) латентность;

4) достаточно высокий профессионализм преступников и др.

Немаловажным фактором, влияющим на распространение преступлений, совершаемых в компьютерной сфере является появление и внедрение новейших технологий, происходящих в различных секторах рассматриваемой сферы.

Также фактором, препятствующим выявлению преступлений в сфере компьютерных технологий, является то, что между этапом совершения преступления и устранением следов его совершения могут проходить незначительные промежутки времени, после чего следы или улики могут быть обнаружены только у нарушителя.

Но многие лица, причастные к совершению подобных деяний, прибегают к ряду способов избавления от таких следов, т.е. лишают возможности выполнить работу по раскрытию и расследованию преступления.

При совершении преступлений в сфере компьютерных технологий преступники стремятся обеспечить безопасность получения похищенных материальных ценностей.

Для этого привлекаются соучастники, на чье имя могут отправляться товары из электронных интернет - магазинов или переводятся денежные средства на банковские счета.

В настоящее время уровень технической оснащенности оперативных подразделений органов внутренних дел остается на весьма низком уровне (по сравнению с различными преступными формированиями), помимо этого недостаточная квалификация специалистов оказывает свое негативное влияние на уровень и качество раскрытия преступлений в сфере высоких технологий.

Поэтому для осуществления оперативно-розыскной деятельности в области информационных технологий целесообразно привлекать преподавателей и специалистов, прошедших углубленную подготовку по компьютерным наукам. Получение информации, значимой для органов внутренних дел, непосредственно на объектах глобальной сети Интернет является наиболее эффективным в результате применения отдельных приемов, установления контакта, изучения документов, направления запросов или проведения отдельных оперативно-розыскных мероприятий, предусмотренных Федеральным законом от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности ОВД» [14].

Так, согласно ст. 7 Федерального закона от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности ОВД» основаниями для проведения оперативно-розыскных мероприятий являются:

1. Наличие возбужденного уголовного дела.

2. Ставшие известными органам, осуществляющим оперативно-розыскную деятельность, сведения о:

1) признаках подготавливаемого, совершаемого или совершенного противоправного деяния, а также о лицах, его подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела;

2) событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации;

3) Поручения следователя, руководителя следственного органа, дознавателя, органа дознания или определения суда по уголовным делам и материалам

проверки сообщений о преступлении, находящимся в их производстве;

4) Запросы других органов, осуществляющих оперативно-розыскную деятельность, по основаниям, указанным в настоящей статье;

5) Постановление о применении мер безопасности в отношении защищаемых лиц, осуществляемых уполномоченными на то государственными органами в порядке, предусмотренном законодательством Российской Федерации;

6) Запросы международных правоохранительных организаций и правоохранительных органов иностранных государств в соответствии с международными договорами Российской Федерации [4].

При выявлении и раскрытии преступлений, совершенных с использованием компьютеров, вычислительных систем или иной электронной техники, оперативный сотрудник сталкивается с нетрадиционными следами преступной деятельности или вещественными доказательствами.

Поэтому для успешного осуществления оперативно-розыскной деятельности сотрудникам необходимо хорошее знание действий хакера, его тактики проведения атак на компьютерные системы, повышать уровень своих знаний и находить возможность их пополнения. Преподаватели высших технических заведений, обучающие студентов современным компьютерным технологиям, могут помочь сотрудникам спрогнозировать поведения преступных элементов, подсказать возможные пути пресечения преступных действий.

## Заключение

В настоящее время происходит рост количества компьютерных преступлений. По относительно немногим из них возбуждаются и доходят до судебного разбирательства уголовные дела, лишь малая часть которых заканчивается обвинительным приговором.

По возбужденным уголовным делам возникают серьезные проблемы доказывания. Анализ судебно-следственной практики показывает, что эти проблемы обусловлены недостатками процессуального и криминалистического регламентирования производства следственных действий по данному виду преступлений.

Многочисленные спорные вопросы относимости, допустимости и достоверности доказательств, полученных на стадии предварительного следствия, обрушиваются на суд.

Обобщение практики компьютерных преступлений позволяет отметить, что детерминанты их раскрытия заложены в личности самих преступников. Практически любой пользователь с минимальным набором знаний в области компьютерной техники может совершить подобное преступление.

Преступники, обладающие профессиональными знаниями в области компьютерных технологий, как правило, не занимаются подобного рода деятельностью, осознавая низкую вероятность ухода от уголовной ответственности и предпочитая не оставлять следов, которые способны их идентифицировать.

Самую немногочисленную долю раскрытых преступлений в сфере компьютерных технологий составляют наиболее опасные преступления, совершаемые высококвалифицированными специалистами в области высоких технологий. Эти преступления зачастую совершаются в составе организованных преступных групп.

Высококвалифицированные преступники прилагают много усилий не только для обеспечения несанкционированного доступа, но и для сокрытия своей личности, для чего в их арсенале присутствует немало средств – от дистанционного удаления файловой системы после взлома до использования компьютеров сторонних пользователей в качестве базы для доступа к ЭВМ жертвы.

Безусловно, в мировой и российской практике присутствуют раскрытые дела этой группы, но их процент весьма невелик по сравнению с теми, которые так и не были раскрыты. Специфика способов совершения таких преступлений приводит к высокой латентности, несмотря на то, что, по-видимому, практическая численность их совершения достаточно велика. Это говорит о значительных правовых и технических пробелах в области компьютерной безопасности, а также о недостаточности методик расследования и необходимости про- ведения масштабных исследований в этом направлении.

## Список литературы

1. Добрынин Ю. Классификация преступлений, совершаемых в сфере компьютерной информации [Электронный ресурс]. URL:

http://www.russianlaw.net/law/computer_crime/a158/ (дата обращения: 04.02.2012).
2. Косынкин, А. А. Преодоление противодействия расследованию преступлений в сфере компьютерной информации / А. А. Косынкин. – Москва : Юрлитинформ, 2013. – С. 90.
3. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 07 декабря 2011 г. № 420-ФЗ // Российская газета. 2011. 9 декабря.
4. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 29 ноября 2012 г. № 207-ФЗ // Российская газета. 2012. 3 декабря.
5. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации в целях усиления ответственности за преступления сексуального характера, совершенные в отношении несовершеннолетних: Федеральный закон от 29 февраля 2012 г. № 14-ФЗ // Российская газета. 2012. 2 марта.
6. Подольный, Н. А. Проблемы оптимизации расследования преступлений в сфере компьютерной информации / Н. А. Подольный // Раскрытие и расследование преступлений, сопряженных с использованием средств вычислительной техники, проблемы, тенденции, перспективы. – Москва : МАКС Пресс, 2005. – С. 172.
7. Подольный, Н. А. Теоретические и практические основы раскрытия и расследования преступлений, совершенных молодежными организованными группировками : дис. на соиск. учен. степ. д-ра юрид. наук / Н. А. Подольный. – Москва, 2007. – С. 374.
8. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. – 2013. – № 2. – С. 114–116.
9. Поляков В.В. Характеристика высокотехнологичных способов совершения преступлений в сфере компьютерной информации: матер. ежег. Всерос. науч.-практ. конф., посвященной 50-летию юридического факультета и 40-летию Алтайского государственного университета «Уголовно- процессуальные и криминалистические чтения на Алтае». – Барнаул: Изд-во Алт. ун-та, 2012. – Вып. 11–12. – С. 123–126.
10. Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. – 2012. – № 24. – С. 43–46.
11. Уголовное дело № 1-179/06 // Архив суда г. Алейска. – 2006.

12. Уголовное дело № 1-337/2011 // Архив суда г. Новоалтайска. – 2011.
13. Уголовное дело № 2-23/2011 // Архив суда г. Камень-на-Оби. – 2011
14. Уголовное дело № 706/09 // Архив Железнодорожного районного суда г. Барнаула. – 2009.
15. Фадеев, В. И. Расследование криминальных инсценировок / В. И. Фадеев. – Москва : Норма, 2007. – С. 26.