Impact Factor: 9.9 ISSN-L: 2544-980X

Роль Эксперта –Криминалиста В Профилактике Преступлений В Сфере Компьютерной Информации И Киберпреступности

Тураббаев Хусанбек Абдусаламович [1]

Аннотация: В статье автором формируется происхождение киберпреступности — и совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных.

Ключевые слова: киберпреступность; компьютерная преступность; Интернет.

Процессы глобализации, в том числе глобализации информационных технологий, предоставляют неограниченные возможности для оказания воздействия на личность и общество. Одним из негативных последствий развития информационных технологий является появление и развитие новой формы преступности — преступности в сфере высоких технологий, когда компьютеры или компьютерные сети выступают в качестве объекта преступных посягательств, а также средства или способа совершения преступлений. Проблема киберпреступности актуализировалась в эпоху информационного общества, когда компьютеры и телекоммуникационные системы охватили все сферы жизнедеятельности человека и государства, а глобальная сеть Интернет является одной из наиболее быстрых областей развития телекоммуникационных технологий.

Киберпреступность основывается на взломе интернет-страниц, распространении вредоносных программ и противоправной информации людьми, осуществляющими преступную деятельность в виртуальном пространстве с помощью информационных технологий. Немаловажную роль для осуществления подобного рода противозаконной деятельности играет компьютер. Он является техническим средством, инструментом, позволяющим злоумышленникам не только похищать информацию, уничтожать или повреждать её, но и размещать вредоносные сайты, на которых содержатся компьютерные вирусы.

Данный вид преступления, как, впрочем, и все другие, таит в себе угрозу информационной безопасности общества. Помимо кражи денежных средств с банковских карт киберпреступники научились похищать персональные данные человека, что может нанести непоправимый урон его репутации в случае опубликования этой информации в сети. Киберпреступность является проблемой не только каждого отдельного взятого интернет-пользователя, - её следует рассматривать в более широком, социальном и даже международном ключе. От роста киберпреступности страдают не только физические, но и юридические лица; жертвами хакерских атак в нашей современности становятся целые страны, государства.

Киберпреступность — это преступность в так называемом киберпространстве. Для того чтобы дать определение киберпреступности, необходимо прежде всего осмыслить такое понятие, как «киберпространство».

[1]доцент кафедры Юридических дисциплин Института повышения квалификации МВД Республики Узбекистан, подполковник

Киберпреступность — это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных. Это определение соответствует рекомендациям экспертов ООН. По их мнению, термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершённое в электронной среде.[2]

Компьютерное преступление — это только такое преступление, которое посягает на безопасное функционирование компьютеров и компьютерных сетей, а также на обрабатываемые ими данные. Таким образом, компьютерное преступление — разновидность киберпреступления.[3]

Сегодня жертвами преступников, орудующих в виртуальном пространстве, могут стать не только люди, но и целые государства. При этом безопасность тысяч пользователей может оказаться в зависимости от нескольких преступников. Количество преступлений, совершаемых в киберпространстве, растёт пропорционально числу пользователей компьютерных сетей. Растущий профессионализм киберпреступников и постоянное совершенствование информационных технологий, и, как следствие, постоянная эволюция возможностей для совершения преступлений, создают новые угрозы для пользователей глобальных информационных сетей.

Стремительное развитие компьютерных сетей и проникновение их в различные сферы человеческой деятельности, как уже было сказано, изменило характер преступных посягательств и породило новые их формы.

Интернет и всё большее совершенствование устройств доступа к сети, в том числе «портативных» мобильных телефонов, коммуникаторов, создаёт новые возможности для злоупотребления информационными технологиями.

Термин «киберпреступность» в настоящее время часто употребляется наряду с термином «компьютерная преступность», причём нередко эти понятия используются как синонимы. Действительно, эти термины очень близки друг другу, но всё-таки не синонимичны. На наш взгляд, понятие «киберпреступность» (в англоязычном варианте — cybercrime) шире, чем «компьютерная преступность» (computer crime), и более точно отражает природу такого явления, как преступность в информационном пространстве.

В результате интенсивного развития и внедрения современных информационных технологий в мире активизировались процессы формирования глобального информационного пространства, повлекшие за собой и появление новых вызовов и угроз.[4]

Блага современной цивилизации, к которым, безусловно, относится цифровизация всех сфер жизни государства, общества, семьи и личности, к сожалению, приводят и к тому, что экономическая компьютерная преступность может затронуть практически каждого, живущего в современном мире.[5]

В быстро меняющихся условиях современного высокотехноло-гического мира широкое использование получила компьютерная техника, машинные информационные носители, используемые в Интернете и в других социальных сетях. Это позволило создать принципиально новую виртуальную проекцию реального мира, в которую стали вовлекаться в практически все

[2] Преступления, связанные с использованием компьютерной сети [Электронный ресурс] // Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями
[3] См. подробнее: Тропина Т.Л. Киберпреступность. — Владивосток, 2009.
[4] Илинич Е.В. Мошеннические операции с банковскими пластиковыми картами как угроза экономической безопасности в сфере банковской деятельности // Экономика, Статистика и Информатика. – 2013. – N 6. – С.41.
[5] Там же

стороны нашей жизни. А это, в свою очередь создали беспрецедентные условия для обмена информацией, совершенствованию информационно-коммуникационных технологий (ИКТ) в инновационном виртуальном пространстве. Наряду с положительными сторонами применения созданной ИКТ имеются и негативные последствия данной реальности, а именно возникновению возможностей незаконного проникновения в созданную информационно-телекоммуникационную сеть с целью криминального обогащения («киберпреступления»). Под данными преступлениями понимается правонарушения совершенные посредством применения высокотехнологичных средств компьютерной техники.

В сущности киберпреступность представляет собой общественно-опасное деяние в виртуальном пространстве, которое можно обозначить как киберпреступность моделируемое с помощью компьютерной техники и иных информационных, телекоммуникационных средств. Киберпреступность включает в себя любое преступление, которое может совершаться с помощью информационно-коммуникационных технологий в рамках компьютерной системы или сети. В сущности, данное преступление, совершенное в киберпространстве представляет собой противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством ИКТ, компьютерных сетей и программ.

Криминалистическое исследование компьютерной информации – достаточно новое явление в криминалистической технике. Появилось оно, в первую очередь, благодаря высокому уровню цифровизации общества. Все больше общественных процессов перетекает в цифровую среду. Наряду с положительными аспектами развития информационной индустрии, общество сталкивается с негативными особенностями указанного процесса, трансформирующихся в преступления, совершаемые посредством виртуального пространства, где используются такие средства, как: компьютерные вирусы, вредоносные программы, различные модификации гаджетов, персональные компьютеры, цифровые технологии, которые направлены на несанкционированный доступ к техническим средствам, личным данным и денежным ресурсам. Сложность раскрытия указанной категории преступлений заключается в опосредованности их совершения, что влечет определенные трудности в отыскании, фиксации, изъятии и исследовании объектов его совершения.

Большой охват потерпевших, использование возможностей современных технологий с минимизацией визуального контакта с потерпевшими, а также возможностью удаленного доступа к их денежным средствам привели к увеличению количества цифрового мошенничества.

Данное явление связано: во-первых, с отсутствием специальных знаний в сфере информационно-телекоммуникационных технологий (далее – ИТТ) у лица, проводящего расследование, во-вторых, с непониманием последним информационно-технических процессов совершения преступления, для комплексного решения данной задачи необходимо обеспечить взаимодействие следователя и лица, обладающего специальными познаниями в области компьютерных технологий, не только на этапе обнаружения следов, но и на последующих этапах их исследования (осмотре, назначении компьютерных экспертиз и т. д.). Одним из наиболее важных инструментов, позволяющих восстановить весь процесс совершенного преступного деяния в сфере цифровых технологий, является проведение судебной компьютерно-технической экспертизы.

В настоящее время криминалистическое исследование цифровой информации проводится по многим категориям преступлений. В частности, данный процесс актуален для расследования преступлений в сфере компьютерной информации, экономической направленности, терроризма и экстремизма, распространения порнографической продукции, нарушений авторских и смежных прав. Объектом криминалистического исследования указанных категорий преступлений является непосредственно информация, содержащаяся на различных

электронных носителях, виртуальных пространствах и обладающая определенной специфичностью.

Современное судопроизводство невозможно представить без применения специальных знаний. Эффективность отправления правосудия зависит от достоверности установления фактов и обстоятельств, подлежащих доказыванию, что зачастую возможно только при участии специалиста. Выводы заключения эксперта во многом предопределяют исход процесса. Действующии процессуальные законодательства позволяют использовать экспертные исследования по уголовным, гражданским, арбитражным и делам об административных правонарушениях.

В настоящее время судами используются многие виды экспертиз, такие, как строительная, товароведческая, бухгалтерская, почерковедческая, судебно-техническая экспертиза документов, экологическая, техническая, медико-социальная, оценочная, экспертиза ценности документов и многие другие.

Об этом свидетельствует не только рост числа экспертиз и исследований, выполняемых в государственных судебно-экспертных организациях различных министерств и ведомств, но и бурно развивающаяся негосударственная судебно экспертная деятельность, в рамках которой нередко реализуется законодательный принцип состязательности и равноправия сторон в судебном разбирательстве.

Киберпреступность в современном мире объявлена глобальной международной проблемой, о чём свидетельствуют принятые международные договорённости, предусматривающие совместные шаги по борьбе с этим высокотехнологичным злом.[6] Опасность киберпреступности для мирового сообщества в целом, признают и государственные правоохранительные органы. Средства информационно-телекоммуникационных технологий стали часто использоваться в совершении преступлений, которые получили обозначение как киберпреступление. Сталкиваясь с киберпреступлениями, сотрудники правоохранительных органов нуждаются в помощи высококвалифицированных специалистов в сфере программирования, в которых по-прежнему испытывается нехватка. Успешному расследованию данного вида преступлений препятствует ряд немаловажных факторов, среди которых, одним из важных является отсутствие действенного механизма привлечения специалистов в области информационных технологий для успешного раскрытия киберпреступлений. Эти специалисты облеченные полномочиями экспертов могли был оказать существенную помощь в раскрытии киберпреступлений.

Немало трудностей возникает и с определением самого факта совершения данного преступления. Ввиду отсутствия возможности проведения квалифицированной экспертизы, зачастую бывает сложно доказать, что за то или иное действие предусмотрено наказание.[7]

Решение той или иной экспертной задачи при проведении криминалистических экспертиз в полном объеме связано с расследованием киберпреступлений, начиная от процесса собирания доказательств и заканчивая их исследованием. Основной формой использования специальных знаний по киберпреступлениям является судебная экспертиза. В зависимости от обстоятельств дела могут быть назначены следующие виды компьютерно-технической экспертизы: аппаратно-компьютерная; программно-компьютерная; информационно-компьютерная; компьютерно-сетевая экспертиза. Так, например, качество и ценность экспертиз в сфере информационно-коммуникационных технологий в полной мере зависят от качества и

[6] «Конвенция о компьютерных преступлениях" (ETS N 185) [рус., англ.] (заключена в г. Будапеште 23.11.2001) с изм. от 28.01.2003 // http://www.coe.int/ru/web/conventions/full-list// conventions/treaty/185 (дата обращ.: 15.10.2014); "Окинавская хартия глобального информационного сообщества" (принята на о. Окинава 22.07.2000) // Дипломатический вестник. 2000. № 8. С. 51 – 56; Бангкокская декларация “Партнёрство во имя будущего” (принята в г. Бангкоке 21.10.2003) // Дипломатический вестник и другие.

[7] Волынская О. В Развитие юридической мысли и перспективы в борьбе с киберпреступностью в сфере уголовного судопроизводства // Вестник Московского университета МВД России. 2020. № 3. С. 72-74.

профессионализма работы специалиста в данной области на месте происшествия, направленной на отыскание и изъятие доказательственной информации. Как правило, от качества обнаруженных и зафиксированных следов, изымаемых с места происшествия, зависит доказательственная база по конкретному преступлению.

Небольшой процент идентификационных экспертиз при проведении экспертиз в сфере информационно-коммуникационных технологий и значительное количество экспертиз классификационного и диагностического характера в большинстве случаев объясняются отсутствием подозреваемого в начале расследования. Проблема актуальна, имеет научный и практический интерес, поскольку сегодня современные компьютерные технологии затрагивают практически все области жизнедеятельности человека.

В последние годы информация, становясь одним из определяющих факторов развития современного общества, активно внедряется во все социальные сферы и приобретает все большее значение. Закономерно, что при расширении сферы использования информационных технологий возрастает и количество экспертиз в сфере информационно-коммуникационных технологий. Однако при этом, отечественная практика расследования таких преступлений пока невелика. На стадии возбуждения уголовного дела экспертиза назначенная в сфере информационно-коммуникационных технологий может служить основанием принятия решений по возбуждению уголовного дела и основанием для возникновения уголовно-процессуальных отношений в целом. Информационно-коммуникационные технологии и их носители могут рассматриваться в качестве сведений и источников соответственно в структуре уголовно-процессуального доказательства, но лишь в таких видах, как вещественные доказательства и иные документы.

Расследование преступлений в сфере компьютерных технологий существенно отличаются от расследования других «традиционных» преступлений. Так как прослеживается существенная интенсивность хакерских атак на критически важные объекты инфраструктуры Государства и по данным уголовных дел чаще всего допускаются ошибки, зачастую объясняемые отсутствием надлежащего уровня теоретической и практической подготовки специалистов, которых следователь привлекает как экспертов. Кроме этого сами следователи имеющие только гуманитарное образование (юристы) плохо разбираются в сфере информационных технологий и затрудняются в расследовании киберпреступлений.

Изучение уголовных дел этой категории дает основание полагать, что одной из существенных причин низкого качества следствия является не привлечение соответствующих специалистов в области ИКТ отсутствие систематизированных и апробированных методик расследования компьютерных преступлений, а также ошибки, совершаемые при проведении следственных действий в отношении информационных технологий.

Обладая специальными знаниями в сфере компьютерной техники, специалисты (эксперты) способны внести вклад в деятельность следователя по установлению истины при расследовании киберпреступлений. Причем специальные знания могут применяться не только при расследовании преступлений в сфере компьютерных технологий, т.к. при совершении «традиционных» преступлений ИКТ может быть использован для проектирования и изготовления фальсифицированных документов, денежных знаков, для создания и хранения базы данных, содержащей информацию о преступлении и в других целях. При данных обстоятельствах, следователь не может эффективно работать в одиночку, опираясь только на собственные знания и навыки пользователя персонального компьютера. Может оказаться недостаточно даже знаний, привлекаемого эксперта или специалиста, т.к., в зависимости от обстоятельств дела, могут потребоваться знания в различных областях компьютерных технологий.

Несмотря на то, что обязанность поиска и закрепления доказательств лежит на следователе, эффективность производства таких следственных действий как осмотр места происшествия (места преступления), обыск, выемка и др., при расследовании преступлений, связанных с

использованием компьютерной техники, приобретает все большую зависимость от организации взаимодействия следователя и специалистов, вовлеченных в проведение данных мероприятий.

Данное обстоятельство влечет за собой необходимость активной разработки и применения общих организационных и тактических приемов использования помощи лиц, обладающих специальными знаниями в расследовании киберпреступлений, проведения исследования указанных объектов, а также организации взаимодействия следователя и специалистов в области нано-технологий при расследовании киберпреступлений и др.[8]

В литературе, посвященной расследованию киберпреступлений, разными авторами сформирована криминалистическая характеристика неправомерного доступа к компьютерной информации, классификация следов неправомерного доступа к компьютерной информации, классификация способов совершения данного преступления, представлены данные о способах его сокрытия, орудиях и средствах совершения, разработана методика исследования и обыска средств компьютерной техники.[9]

В связи с новизной методики расследования киберпреступлений, исследования особенностей использования специальных знаний в области компьютерной информации носят отрывочный, фрагментарный характер и чаще всего сводятся к отдельным, частным рекомендациям. Почти во всех работах, посвященных расследованию преступлений в сфере компьютерной информации, указывается на целесообразность привлечения специалистов, в той или иной мере, но не раскрывается содержание их помощи. Также организация и тактика использования экспертов в сфере ИКТ если и анализировались, то редко, фрагментарно.

В связи с этим, актуальным является исследование проблем привлечения экспертов в области компьютерных технологий, установление взаимодействия между ними и органами осуществляющими расследование.

Таким образом, в настоящее время во всем мире, вопросам назначения и производства экспертизы в сфере информационных технологий, при расследовании киберпреступлений уделяется особое внимание. Однако, механизм привлечения необходимых специалистов и экспертов в данной сфере для проведения необходимых экспертиз находится на не достаточном уровне и требует своего решения. Необходимо провести научное исследования криминалистических аспектов привлечения экспертов в области информационных технологий и разработать эффективную методику и тактику взаимодействия экспертов и специалистов с органами следствия, дознания и осуществляющими доследственную проверку. Следует разработать действующий эффективный механизм расследования именно киберпреступлений.

Список использованной литературы:

1. Илинич Е.В. Мошеннические операции с банковскими пластиковыми картами как угроза экономической безопасности в сфере банковской деятельности // Экономика, Статистика и Информатика. – 2013. – No6. – С.41.
2. «Конвенция о компьютерных преступлениях" (ETS N 185) [рус., англ.] (заключена в г. Будапеште 23.11.2001) с изм. от 28.01.2003 // http://www.coe.int/ru/web/conventions/full-list//conventions/treaty/185 (дата обращ.: 15.10.2014); "Окинавская хартия глобального информационного сообщества" (принята на о. Окинава 22.07.2000) // Дипломатический вестник. 2000. № 8. С. 51 – 56; Бангкокская декларация “Партнёрство во имя будущего” (принята в г. Бангкоке 21.10.2003) // Дипломатический вестник и другие.

[8] Полещук Д.Г. Уголовно-правовая охрана информационной безопасности (на примере отдельных аспектов охраны кибербезопасности и защиты информации ограниченного распространения): Автореф… дис. канд. юрид. наук. - Минск, 2020. –32 с.
[9] Анорбоев А.У. Кибержиноятларнинг жиноий-ҳуқуқий жиҳатлари: Юрид. фан. бўйича фалс. док-ри. (PhD). дис. – Т., 2020. – 290 б

3. Полещук Д.Г. Уголовно-правовая охрана информационной безопасности (на примере отдельных аспектов охраны кибербезопасности и защиты информации ограниченного распространения): Автореф… дис. канд. юрид. наук. - Минск, 2020. –32 с.
4. Анорбоев А.У. Кибержиноятларнинг жиноий-ҳуқуқий жиҳатлари: Юрид. фан. бўйича фалс. док-ри. (PhD). дис. – Т., 2020. – 290 б.
5. Расулев А.К. Совершенствование уголовно-правовых и криминологических мер борьбы с преступлениями в сфере информационных технологий и безопасности: Автореф. дис. …д-ра юрид. наук (DSc). – Т., 2018. – 74 с.
6. Астанов И. Р. Процессуальные и криминалистические аспекты использования специальных знаний по уголовным делам: Автореф. дис. …д-ра юрид. наук (DSc). – Т., 2018. – 75 с.
7. Анорбоев А.У. Уголовно-правовые аспекты киберпреступлений: Автореф. дис. …д-ра философии (PhD). – Т., 2020. –54 с.
8. Бахтеев Д.В. О некоторых современных способах совершения мошенничества в отношении имущества физических лиц //Российское право. –2016. – No3. – С.25.
9. Юрочкин Н.С.Кибермошенничество: характеристика, приемы и методы его совершения // Таврический научный обозреватель. – 2016. – No12 (17). – С. 158 www.tavr.science
10. Нугаева Э. Д., Чаплыгина В. Н. Роль цифровых технологий в оптимизации криминалистической деятельности //Актуальные проблемы уголовно-процессуального права, криминалистики и оперативно-розыскной деятельности: сборник статей. – 2022. – С. 60–63.
11. Харисова З.И., Филиппов О.А., Нугаева Э.Д. Изъятие криминалистически важной информации с мобильных средств связи в рамках расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Вестник института права Башкирского государственного университета. – 2023. – No 1. – С. 57–64.
12. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: Учебное пособие для вузов / С.В. Зуев. – М., 2023. – 243 с.
13. Россинская Е. Р., Шамаев Г. П. Новый раздел криминалистики: криминалистическое исследование компьютерных средств и систем // BaikalResearchJournal. Т.6. – 2015. – No 1. – С. 317–325