УДК 343.1

**Нуров Мурад Абдусамадович,**
преподаватель кафедры уголовного процесса
Уфимского юридического института МВД России

# К ВОПРОСУ ОБ АКТУАЛЬНЫХ ПРОБЛЕМАХ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

**Аннотация:** в статье автором рассмотрены проблемы, связанные с раскрытием и расследованием тяжких преступлений в сфере информационно-телекоммуникационных технологий, профессиональный уровень следователей.

**Ключевые слова:** киберпреступления, информационно-телекоммуникационные технологии, правоохранительные органы, следователь.

В наше время информационно-телекоммуникационные технологии проникают во все сферы нашей жизни, от общения и работы до развлечений и управления финансами. Цифровая среда создает уникальные возможности для совершения преступлений, таких как кибермошенничество, кибершпионаж, хакерские атаки, а также злоупотребление личной информацией и дезинформация. Расследование уголовных дел представляет собой сложную задачу, требующую высокой квалификации, технических знаний и специализированных инструментов.

Ключевые аспекты, такие как кибербезопасность, защита личных данных, а также проблемы, связанные с глобальными масштабами киберпреступности, порождают новые вызовы в расследовании следственных подразделений.

В данной статье мы рассматриваем актуальные проблемы, их влияние на современное общество и возможные пути их решения. Рассмотрение данных проблем поможет нам лучше понять всю сложность, с которой сталкиваются правоохранительные органы по борьбе с цифровой преступностью, и обратить внимание на важные аспекты развития информационной безопасности и этического использования технологий в наше время.

Актуальность темы, связанной с раскрытием и расследованием преступлений, совершенных с использованием информационно-телекоммуникационных технологий, трудно переоценить. В современном цифровом мире киберпреступность и другие аспекты цифровой безопасности стали одними из наиболее острых проблем для органов власти, бизнеса и общества в целом.

С каждым днем масштабы и сложности киберпреступлений распространяются, а это означает, что проблемы, связанные с ними, становятся все более актуальными. Рост цифр кибератак, утечек данных, кибершпионажа и других киберугроз требует пристального внимания и разработки новых подходов к борьбе с ними.

Таким образом, разговор о раскрытии и расследовании преступлений, связанных с информационными технологиями, является весьма актуальным и необходимым в современном мире.

Проблемы, связанные с раскрытием и расследованием преступлений, возникающих при использовании информационно-телекоммуникационных технологий, являются многообразными и включают в себя следующие аспекты:

1. Анонимность и близость к обнаружению окружающих объектов в окружающей среде, что затрудняет их обнаружение и привлечение к установленной законом ответственности.

2. Быстрое развитие технологий, включая шифрование, анонимные сети и новые методы нападения, требует привлечения органов, поскольку им необходимо постоянно совершенствовать методы и инструменты.

3. Недостаток специалистов по кибербезопасности и цифровому расследованию, что приводит к нехватке опытных кадров, способных эффективно бороться с киберпреступностью.

4. Технические проблемы и проблемы правового регулирования, такие как такие различия в законодательстве различных стран и наличие действующего международного правового стандарта для регулирования киберпреступности, что затрудняет сотрудничество и эффективное пресечение преступной деятельности в современной цифровой среде.

Исследование и решение этих проблем являются важнейшими требованиями для обеспечения безопасности в цифровом пространстве, защиты прав граждан и предотвращения серьезных угроз, которые могут возникнуть из-за киберпреступности.

В виду постоянного совершенствования современных цифровых технологий, быстрого внедрения их в повседневную деятельность, которые охватывают все сферы жизнедеятельности в том числе и преступную деятельность, вопросы противодействия преступлениям с использованием цифровых технологий, совершенствования уголовно-процессуального закона, в данном направлении, особенно актуальны. Очевидно, что проводимые профилактические мероприятия на надлежащем уровне, но требуют применения новых норм и методов распространения информации о способах и методах совершения ИТТ – преступлений среди населения.

Необходимо отметить, что криминальные методы «удаленного» хищения денежных средств постоянно эволюционируют, при этом преступниками активно используются современные ИТТ, которые зачастую просты в использовании и доступны неограниченному числу пользователей глобальной сети. Уже сейчас правонарушители взламывают личные аккаунты людей на портале «Госуслуг», тем самым получая доступ к информации, которую используют при разговоре с потенциальными потерпевшими. К основным схемам обмана граждан остаются звонки «службы безопасности банка». К данному способу обмана добавился звонок от мошенников, представляющихся сотрудниками различных правоохранительных органов, в том числе путем подменных номеров дежурных частей правоохранительных органов, при этом, ссылаясь на проверку телефонных номеров на официальном сайте правоохранительных органов. Такая схема призвана убедить жертву в достоверности излагаемой информации и оказать на неё давление. Подставные правоохранители подтверждают «правомерность» действий «банковских сотрудников», предлагающих перевести деньги клиента на «безопасные счета».

Также мошенники используют иные способы обмана людей в интернете: от спама до создания сайтов-двойников, руководствуясь прежде всего необходимостью в получении персональных данных пользователя (потерпевшего), номера банковских карт, CVC кода на оборотной стороне банковской карты, паспортных данных, логинов и паролей. У потерпевших похищаются денежные средства под предлогом совершения каких-либо банковских операций, (либо на предотвращение таких операций), направленных на восстановление якобы поврежденных данных об их банковских вкладах, либо путем введения их в заблуждение. При этом, в подавляющем большинстве случаев злоумышленники представляются либо банковскими работниками, либо работниками правоохранительных органов.

Ведомственный нормативный правовой акт утвердил Алгоритм по раскрытию и расследованию хищений, совершенных с использованием ИТТ [1].

Основными действиями в указанном алгоритме заключено, что следователям необходимо своевременно направить запросы и соответственно истребовать ответы на запросы операторов сотовой связи, банковских учреждений в рамках расследуемого уголовного дела, в получении информации которой, необходимо проверить на причастность пользователей абонентский номеров и банковских счетов, используемые при совершении

преступлений. Банковские учреждения предоставляют информацию о движении денежных средств по счетам потерпевшего, о принадлежности счетов, на которые переводились денежные средства. При получении указанной информации, во исполнение приоритетной задачи органов внутренних дел по обеспечению возмещения ущерба, в том числе причиненного преступлениями, совершенными с использованием ИТТ, применяется норма процессуального принуждения в виде наложения ареста счета, позволяющая обеспечить защиту граждан от неправомерных посягательств.

При совершении преступлений, с использованием ИТТ, следователь по согласованию с руководителем следственного органа направляет в суд ходатайство в порядке ст.186.1 УПК РФ об истребовании информации о соединениях между абонентами и абонентскими средствами связи, которые позволяют своевременно получить информацию, имеющую значение для раскрытия преступления, а также выявить факты использованиям злоумышленниками технологий подмены абонентских номеров, использования динамических, нераспознаваемых IP – адресов или их подмен.

В целях предотвращения использования преступниками теневого трафика при совершении преступлений, операторы связи обязаны осуществлять построение сетей связи с учетом требований обеспечения устойчивости и безопасности их функционирования [2].

На более широком уровне обеспечение цифровой безопасности и борьба с киберпреступностью требуют не только технических и правовых решений, но также изменений в культуре использования информационных технологий и осведомленности пользователей. Это включает в себя необходимость обучения людей цифровой грамотности, осведомленности в области кибербезопасности и ответственного использования технологий. Также сотрудникам банка предлагается распространение информации о мошенничестве, их видах и формах совершении, в том числе установления обстоятельств заключения кредитного договора, особенностей поведения и эмоционального состояния человека. Так как сотрудники банковских и кредитных учреждений могут установить обстоятельства мошеннических действий и предотвращать противоправные деяния.

Кроме того, в настоящее время важно развитие новых технологий, таких как искусственный интеллект, машинное обучение и квантовые вычисления, для более эффективного обнаружения и предотвращения киберпреступности.

Проблемы цифровой безопасности, включая раскрытие и расследование киберпреступлений, являются сложными и многогранными, и их решение требует всестороннего подхода со стороны общества, правоохранительных органов, правительства и технологических компаний.

*Список литературы:*

1. Приказ Министерства внутренних дел по Республике Башкортостан №278 от 28.04.2022 «Об утверждении алгоритма действий сотрудников ОВД при раскрытии и расследовании мошенничеств и хищений, совершенных с использованием ИТТ».
2. Федеральный закон от 07.07.2003 №126 ФЗ «О связи».

«Материал не содержит сведений ограниченного распространения, неправомерного заимствования; вычитан; цифры, факты, цитаты сверены с первоисточником».

Нуров М.А.