УДК 34

Бакурова С.С.
студент
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева»
Научный руководитель: Баженов О.Н., к.ю.н., доцент
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева»

СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ПО ЭЛЕКТРОННЫМ СЛЕДАМ

Аннотация: В статье рассматривается современное состояние преступности в цифровом пространстве. Выявляются новые возможности в раскрытии и расследовании преступлений по электронным следам, определяется их правовая природа, рассматривается процессуальное и криминалистическое значение. Помимо этого, формулируются меры по совершенствованию механизма расследования преступлений в сфере современных технологий.

Ключевые слова: цифровые технологии, преступления с использованием IT-технологий, киберпреступность, персональные данные, преступность.

Bakurova S.S.
student
Federal State Budgetary Educational Institution of Higher Education Oryol State University named after I.S. Turgenev"
Scientific adviser: Bazhenov O.N., candidate of juridical sciences, associate professor
Federal State Budgetary Educational Institution of Higher Education Oryol State University named after I.S. Turgenev"

MODERN POSSIBILITIES OF DISCOVERING AND INVESTIGATION OF CRIMES ON ELECTRONIC TRAILS

Annotation: The article deals with the current state of crime in the digital space. New opportunities are revealed in the disclosure and investigation of crimes on electronic traces, their legal nature is determined, and the procedural and forensic significance is considered. In addition, measures are being formulated to improve the mechanism for investigating crimes in the field of modern technologies.

Key words: digital technologies, crimes using IT technologies, cybercrime, personal data, crime.

Цифровые технологии активно используются в современной криминалистике, причем совершенно в разнообразном качестве. Особую роль они играют при раскрытии преступных деяний, в частности совершенных в цифровом пространстве. Внедрение цифровых атрибутов в преступную деятельность обусловлено в том числе и активной государственной деятельностью по цифровизации государственных и общественных функций. Области внедрения цифровых технологий не ограничены – к ним относятся и экономика, и здравоохранение, и государственное управление. Цифровая революция не только принесла пользу экономике и социуму, но и открыла для криминалитета новые способы совершения преступлений – с использованием IT-технологий.

Согласно данным официальной статистики, за прошедший год зарегистрировано более 294 тысяч преступлений, совершенных с использованием информационно-телекоммуникационных технологий – на 70 % больше, чем в 2020 году[1]. При этом рост статистического трафика налицо – за январь-сентябрь текущего года с применением IT-технологий совершено на 77 % больше деяний – по сравнению с аналогичным периодом 2021 года.

[1] Министерство внутренних дел Российской Федерации : Официальный сайт [Электронный ресурс] // Режим доступа: https://мвд.рф/ (дата обращения 03.10.2022).

Криминальный IT-скачок не мог остаться без внимания со стороны правоохранительных органов. Так, в структуре Главного следственного управления Следственного комитета РФ и в системе Министерства внутренних дел РФ созданы подразделения по расследованию киберпреступлений и преступлений в сфере высоких технологий[2].

Формирование специализированных структур – необходимый шаг для борьбы с киберпреступлениями, характеризующимися трансграничностью и неочевидностью.

В условиях коронавирусной пандемии поле деятельности для злоумышленников расширилось – продажа фейковых цифровых пропусков, направление несуществующих штрафов и т. д. Традиционные для новой эры способы дистанционных хищений – фишинг и вишинг – также активно используются преступниками. При квалификации конкретных фактических обстоятельств необходимо провести четкую линию демаркации между различными формами посягательств против собственности.

Исходя из рекомендаций высшей судебной инстанции, следует заключить, что при мошенничестве виновный воздействует на психику потерпевшего – с целью получения имущества или приобретения права на имущество. Вместе с тем, с точки зрения юридической техники, законодательные положения не всегда отвечают приведенной аксиоме.

В 2012 году УК РФ дополнен новым видом мошенничества в сфере компьютерной информации (ст. 159.6). Думается, что с позиций теории уголовного права и рекомендаций высшей судебной инстанции данное преступление не является мошенничеством, поскольку хищение совершается не путем воздействия на психику потерпевшего, а посредством «вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей». Данное преступление – самостоятельная

[2] Федеральный закон от 29.11.2012 № 207-ФЗ (ред. от 03.07.2016) «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ, 03.12.2012, № 49, ст. 6752.

форма хищений с использованием IT-технологий. Следует заметить, что для совершения хищений в режиме «онлайн» у злоумышленников должен быть минимальный пакет информации о предполагаемой жертве. В этих целях преступники нередко пользуются услугами «пробива» (если самостоятельно не являются их поставщиками). Суть «пробива» заключается в деятельности по сбору и анализу информации о конкретной личности или организации – как из открытых источников, так и посредством неправомерного доступа к персональным данным или иной охраняемой законом тайне.

Сейчас на просторах Telegram существует большое количество каналов, где интересанты могут приобрести полный комплект информации о персоне – от паспортных данных и номера сотового телефона до сведений о банковских счетах. После прохождения «информационной стадии» хищения и непосредственного его совершения злоумышленники занимаются сокрытием преступно полученных доходов.

Широкой популярностью у криминалитета пользуются электронные кошельки, которые дают возможность «отмыть» похищенные денежные средства. Кроме того, электронные кошельки, в частности биткоин-платформы, стали дистанционной площадкой для совершения иных преступлений, в том числе связанных с незаконным оборотом наркотиков.

Вышеуказанные проблемы предполагают скорейшее развитие цифровой криминалистики, которая способна обеспечить эффективное расследование и раскрытие преступлений в компьютерной области. В целом современная уголовно-правовая база для противодействия киберпреступности отвечает потребностям времени и сложившейся правоприменительной практике[3]. Однако следует признать, что специфика такого рода криминальных деяний состоит в их латентности, неочевидности и трансграничности, в связи с чем, необходимо применение комплекса мер по предупреждению и ликвидации последствий преступлений в сфере IT, в

[3] Фролова Е.Ю. Современные возможности раскрытия и расследования преступлений по электронным следам / Е. Ю. Фролова, Н. С. Шовин. // Молодой ученый. 2021. № 15 (357). С. 272-274.

частности: выработка стратегий кибербезопасности на всех уровнях, активное международное сотрудничество и приведение специального законодательства в соответствие с новейшими тенденциями в сфере информационных технологий.

Сейчас цифровые следы — инструмент установления обстоятельств по уголовному делу. Они остаются как на смартфонах, так в сетях Интернет. При этом существует комплекс механизмов, которые способны не только изъять информацию с электронных устройств, но и проникнуть в глубину цифровых взаимоотношений.

Таким образом, цифровые следы — эффективный механизм расследования и раскрытия преступлений. В этих целях важно развивать цифровые технологии и стремиться к повышению эффективности инструментов форензик-расследования в ходе производства по уголовному делу, а также проведения оперативных мероприятий. При этом классические инструменты криминалистики уже не справляются с существующими проблемами в области преступности в области информационных технологий.

Использованные источники:

1. Федеральный закон от 29.11.2012 № 207-ФЗ (ред. от 03.07.2016) «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ, 03.12.2012, № 49, ст. 6752.

2. Министерство внутренних дел Российской Федерации : Официальный сайт [Электронный ресурс] // Режим доступа: https://мвд.рф/ (дата обращения 03.10.2022).

3. Фролова Е.Ю. Современные возможности раскрытия и расследования преступлений по электронным следам / Е. Ю. Фролова, Н. С. Шовин. // Молодой ученый. 2021. № 15 (357). С. 272-274.