УДК 343.98

Гусейнов Тофик Азерович
Волгоградский институт управления – Российская академия народного хозяйства и государственной службы при Президенте РФ
Юридический факультет
Россия, Волгоград
ta_guseynov@mail.ru
Huseynov Tofik
Volgograd Institute of Management Russian Presidential Academy of National Economy and Public Administration
Faculty of Law
Russia, Volgograd

ПРОБЛЕМЫ И ОСОБЕННОСТИ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация: в статье анализируются особенности киберпреступлений, проблемы их расследования, ставится вопрос о возможности изменения и переработки законодательства РФ в отношении расследования таких преступлений, затрагивается зарубежный опыт их расследования.

Ключевые слова: киберпреступления, информационные технологии, интернет, компьютер, компьютерно-технологическая экспертиза.

PROBLEMS AND PECULIARITIES OF THE INVESTIGATION OF CYBER CRIMES

Annotation: the article analyzes the features of cybercrime, the problems of their investigation, raises the question of the possibility of changing and processing the legislation of the Russian Federation in relation to the investigation of such crimes, touches upon the foreign experience of their investigation.

Key words: cybercrime, information technology, Internet, computer, computer-technological expertise.

Развитие информационных технологий, а также формирование виртуальной среды в обществе не могло не привести к появлению преступлений в данной сфере, следовательно, необходимости создания и совершенствования способов и методов их расследования.

По словам главы МВД Владимира Колокольцева число преступлений, связанных с информационными технологиями и телекоммуникациями по сравнению с 2018 годом увеличилось в 16 раз (на 92 %) [9].

Разница между совершенными данными видами преступных деяний, заключается прежде всего в том, что одна из данных групп предусмотрена соответствующей главой УК РФ [1] (гл. 28), а ответственность по другой группе деяний предусмотрена в иных, различных составах

Преступления, совершаемые посредством кибертехнологий - это преступления которые совершаются с помощью: компьютеров, а также иных информационных средств и вычислительно–программируемых устройств и т.д. Ряд ученых по разному подходит к определению киберпреступности и киберпреступлений.

К примеру Д.Н. Карпова считает, что «киберпреступления –это акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет» [6, с.47]. Как видно, данное определение хотя и не является привычным для науки криминалистики и уголовного процесса, однако оно по своему содержанию достаточно емкое и полное. В нем демонстрируется все наиболее важные факторы, определяющие киберпреступность.

Известный ученый-практик Д.М Берова в своей работе дает следующее определение исследуемого общественного явления: «Киберпреступность – это совокупность преступлений, совершаемая в киберпространстве с помощью или посредством компьютерных систем и компьютерных сетей, а также против компьютерных сетей, компьютерных систем и компьютерных данных» [5, с.

65]. Далее, ученый также отмечает, что на данный момент, наиболее распространенными преступлениями в данной сфере являются не только те, что предусмотрены в главе 28 УК РФ, но и такие, общие для уголовного права как кража, мошенничество, нарушение неприкосновенности частной жизни т.д. Разумеется, процесс расследования таких преступлений аналогичен общему процессу, изложенному в УПК РФ [2].

Например, в результате проверки информации о нелегальной деятельности клуба, связанной с махинациями в сфере финансовых и денежных средств, был установлено наличие факта противоправного использования специальных средств, предназначенных для извлечения прибыли в индустрии азартных игр, путем использования глобальной сети Internet вне игровой зоны предназначенной для проведения азартных игр [3, с. 246].

Также следует отметить, что основным видом киберпреступлений на данный момент является, т.н. «фишинг», то есть один из видов мошенничества, при котором злоумышленники ставят своей целью получить индивидуальные данные лица, которые помогут в совершении преступления против денежных средств гражданина (номер банковской карты, номер счета и т.д.) и, таким образом, обогатиться за счет жертвы [8, с. 99].

Исследуя эту категорию злодеяний нужно показать, собственно, что источниками подобных сведений могут быть всевозможные, которые предусмотренны законодательством.

В качестве особенности предоставленной категории уголовных дел можно отметить недоступность на практике в ней явок с повинной. Этот говорит, о спланированном характере и предумышленности злодеяний, например то, что собственные действия злоумышленники не считают нелегальными или же считают, что останутся незамеченными и не понесут наказания. Во время проверки, сообщения о злодеянии подлежат установлению такие условия, как:

I) факт совершения преступления (является ли такое явление преступным);

II) предмет преступления (говоря о современном состоянии киберпреступности можно прийти к выводу, что он не включает в себя только преступления связанные с киберинформацией, а вбирает в себя намного больше особенностей);

III) место совершения криминальных действий, место наступления вредных последствий, время совершения преступлений;

IV) способ совершения преступления, в том числе роль компьютерных технологий;

V) следы, оставленные преступлением;

Обнаружение, фиксация и изъятие следов преступления является важным условием всестороннего и надлежащего расследования уголовного дела.

«Т., увидев на web-сайте объявление с предложением внести денежные средства под процент на счет 890****470*, открытый в Visa Qiwi Wallet, осуществила перевод денежных средств, после чего счет оказался заблокирован» [4, с. 230].

Во время проверки были установлены регистрационные данные web-сайта с сервера, а также транзакции по указанному счету, что в свою очередь способствовало установлению и привлечению к ответственности преступника.

VI) лицо пострадавшее от совершения преступления (физическое или же юридическое лицо) и лица, совершившего преступление;

В случае если лицо пострадавшего, как правило, становится известно незамедлительно, то установление лица, совершившего правонарушение, требует конкретных усилий, например для киберпреступлений, которые в большинстве своем, относятся к категории неочевидных деяний.

Установление данного факта, в основном, имеет профилактическую цель.

Оценку доказательств и достаточность данных, которые необходимы для идентификации конкретного состава преступления, оценивает следователь, учитывая сложившеюся практику.

Далее, применяются криминалистические средства и методы (например, методы компьютерного моделирования, анализ материалов уголовных дел

предшествующих лет и т. п.), с помощи которых проводится воссоздание преступного механизма.

Так, например компьютерное моделирование в настоящий момент происходит по трем направлениям, а именно:

Во-первых, с помощью кибертехнологий происходит создание моделей каких-либо отдельных объектов, так и механизма и процесса совершения противоправного деяния. Существуют различные программы, которые позволяют смоделировать лицо человека по черепу, сконструировать процесс столкновения и траекторию движения транспортного средства при ДТП.

Следующая направленность проявляется в применении программного обеспечения, дозволяющего имитировать реальное продвижение следствия в базе обобщающих, стандартных информативных модификаций определенного типа правонарушений. Форма является вариантом информативной концепции, которая формируется в итогах статистической обработки, а также подборки дел о правонарушениях этого типа. Выстроенная форма выражает логические взаимосвязи среди отличительных компонентов объективных действий правонарушения. В следствии подобного прогнозирования, возникают стандартные версии следствия, которые устанавливают базовые варианты развития технологии расследования правонарушений конкретного вида.

Особенностью третьего направления в использовании кибертехнологий при расследовании преступлений заключается в использовании различных учащих, а также адаптирующих игр и проектов. Невзирая в данном случае, то что в них никак не применяется реальное присутствие следователя при расследовании правонарушений, однако они представляют немаловажную значимость при подготовке, а также повышения квалификации, умений и способностей работников организаций защищающих правопорядок и безопасность граждан. Применение игр дает возможность гарантировать введение человека в процедуру работы следователя и дознавателя наилучшим способом.

Подчеркиваем кроме того, то что из числа подобных игр особенное роль имеют ситуационные вид игр. Сведения и обстановка в таких играх формируют как бы настоящую обстановку расследования правонарушения. Их основной характерной чертой считается незамедлительное действие и реагирование игрока в согласовании с определенными инструкциями в соответствии с этим либо другим видом преступлений. В данных компьютерных играх содержится информация как необходимая для расследования, так и избыточная, которая зачастую является ошибочной. Данные обстоятельства максимально приближают к условиям реальных обстоятельств раскрытия уголовных нарушений, то есть показывают трудность деятельности органов предварительного следствия при установлении важных и необходимых данных и фактов.

Примерами таких компьютерных программ являются «Убийство» и «Следователь», в них игроку предлагается самому провести расследование, попутно принимая те или иные решения, а в конце игры посмотреть какие из них были правильными, а какие нет.

Оправданной, на наш взгляд, является необходимость упомянуть в данной статье, что подобные программы (хотя и немного иной направленности). Данные программы направлены для формирования у обучающихся ВУЗов умений и навыков необходимых им для профессиональной деятельности. Например «Криминалистическая техника» и «Судебная фотография».

Специалист, проводящее расследование по уголовному делу, на основе имеющихся данных, выстраивает логическую цепочку связей, корреляций и выводов, собирает доказательства, приводящие к злоумышленникам, что в дальнейшем позволяет доказать их вину и привлечь к ответственности.

Оперативно-розыскные мероприятия, следственные и иные процессуальные действия, которые проводятся по данной категории преступлений, различны и не ограничены чем-либо, кроме установленных

законом. Залог их успешности заключается в компетентности следователя, который и расследует это уголовное делу.

Также одной из проблем расследований таких преступлений является на наш взгляд то, обстоятельство, что часто работники органов предварительного следствия не имеют помимо юридического дополнительно какого-то образования связанного с компьютерными технологиями. Данная проблема выражается в том, что следователи часто не могут оперативно и в полной степени осознать вышеуказанные факторы необходимые для формирования полного и всестороннего представления о совершившемся преступлении.

Можно полностью согласиться с тем, что следующей проблемой как отмечает С.А. Нестерович [7, с. 46], является сложность расследования таких преступлений сама по себе. Так, часто сама жертва преступления не понимает, что преступление совершенно. Это происходит ввиду того, что жертва может попросту не заметить совершенного преступления (не обратить внимания на исчезновение денежной суммы, особенно если она незначительна; не заметить исчезновения или нарушения работы в какой-либо программе или файле). В последнем случае все осложняется тем, что зачастую системные неполадки и сбои часто списываются на плохую работу компьютера либо на занесение вредоносных программ по вине самого пользователя. Отсюда вытекает вторая проблема – несвоевременное сообщение о преступлении, часто жертва осознает, что против неё совершено противоправное деяние слишком поздно (более 10 дней) и только тогда сообщает об этом в правоохранительные органы. За столь продолжительный срок многие важные обстоятельства (да и сам преступник) могут бесследно исчезнуть. Также негативным обстоятельством в данном случае является сложность и длительность проведения необходимых экспертиз.

Именно компьютерно-техническая экспертиза на наш взгляд является основным и наиболее эффективным способом в расследовании преступлений. Отметим, что, к сожалению, ввиду своей дороговизны и сложности данные

экспертизы не так часто применяются в расследовании данных преступлений, в связи с этим обратимся к зарубежному опыту.

Однако, на сегодняшний день многие компании, финансовые организации и другие фирмы, осуществляющие оборот денежных средств в информационной сфере, заключают соглашения (договоры) об оказание услуг на совершение действий, направленных на предотвращение и расследование киберпреступлений. Такие договоры заключаются с известными в сфере борьбы с киберпреступностью организациями, такими как, например, Group-IB [11] или LETA IT-company [12], которые работают не только в России, но и в других странах. В данных организациях, разумеется, работают высококвалифицированные специалисты, профессионалы своего дела. Также данные компании широко сотрудничают с правоохранительными органами, как на внутригосударственном, так и на международном уровнях. Разумеется, что такая взаимопомощь, обмен опытом и флагманскими технологиями и разработками в данной сфере делает расследование таких преступлений намного эффективнее.

Что касается самого процесса проведения экспертизы, то эксперту предстоит провести достаточно кропотливую работу, так, в случае заражения носителя эксперту предстоит самостоятельно отыскать вредоносную программу (вирус) путем декомпиляции всех установленных программ и файлов, что потребует затраты достаточно большого количества времени. Так, например, при заражении телефона с предустановленной операционной системой «Android» будут изучаться подозрительные приложения и программы (файлы расширения .apk формата). При исследовании вредоносного вируса эксперт обнаружит в части кода IP-адрес, на который без ведома владельца вирус отправляет компрометирующую информацию. С помощью дальнейших оперативно-розыскных мероприятий (действий) необходимо обнаружить местонахождение предполагаемого правонарушителя и произвести его задержание (арест). Следователю по месту жительства лица необходимо организовать и провести обыск (выемку), благодаря которой будет собрана

доказательственная база, которая будет положена в основу обвинительного акта, также необходимо провести иные следственные действия. Данные действия, в дальнейшем, предоставляют в определенных рамках возможность выбора варианта и стратегии поведения следователя.

В нашей работе стоит также упомянуть проблему совершения киберпреступлений в военной сфере. Данное упоминание на наш взгляд полностью оправданно, так как, несмотря на то, что армия хоть и не является типичным местом для совершения киберпреступлений в том смысле, в котором мы их рассматривали ранее, однако Вооруженные силы РФ, её важнейшие информационные данные и разработки являются «лакомым кусочком» для злоумышленников. Так, например в 2017 году на инфраструктуру Минобороны РФ была совершена кибератака вирусом WannaCry, однако, как указывает ТАСС [10], данные атаки были повсеместно успешно отражены.

Что касается, к примеру, атаки на полевые банки Вооруженных сил РФ, то в данном случае каких-либо открытые статистические данные найти сложно. Вероятнее всего, доступ к такой информации ограничен для соблюдения интересов государства и общества. Но все же, если такие атаки и происходили, то очевидно, что информационная безопасность наших вооруженных сил не позволяет таким преступлениям нанести значительный ущерб.

Таким образом, можно сделать вывод, что расследование киберпреступлений весьма слабо разработано на данный момент, однако обсуждения этой проблемы активно ведутся в науке, в связи с чем полагаем, что в скором времени на законодательном уровне будет:

1) более подробно описаны составы киберпреступлений, ужесточены санкции за их совершение;

2) следователи, которые будут заниматься данной категорией дел, будут проходить более тщательный отбор, связанный с навыками владения и знания компьютерных технологий, а также иметь образование в IT-сфере.

3) будет перенят опыт зарубежных методов расследования таких преступлений, а также создание, развитие и дальнейшее совершенствование таких методов.

Список литературы:

1. Уголовный кодекс Российской Федерации: федер. закон от 13.06.1996 № 63-ФЗ. // Доступ из СПС «Консультант Плюс».

2. Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18.12.2001 г. №177-ФЗ. // Доступ из СПС «Консультант Плюс».

3. Материал КУСП №455 от 24.03.2017 г. // Архив ОП (Прикубанский округ) УМВД России по г. Краснодару.

4. Уголовное дело № 16100707 по ч. 2 ст. 159 УК РФ // СУ УМВД России по г. Краснодару, 2017.

5. Берова Д.М. Расследование киберпреступлений // Пробелы в российском законодательстве. №2. 2018. С. 173-175.

6. Карпова Д.Н. Киберпреступность: глобальная проблема и её решение. // Власть. №8. 2014. С. 46-50

7. Нестерович С.А. Проблемы расследования преступлений, которые стоят пред сотрудниками следственных органов. // Вестник науки и образования. №8. 2018. С. 46-49.

8. Хачатурова СС. Киберпреступления в информационном обществе. // Проблемы современной науки и образования. 2016. №11 (53). С. 99-100.

9. Российская газета // URL: https://rg.ru/2019/03/25/kolokolcev-chislo-kiberprestuplenij-v-rossii-uvelichilos-v-16-raz.html.

10. ТАСС // URL: https://tass.ru/armiya-i-opk/4256146.

11. Group IB // URL: https://www.group-ib.ru/.

12. LETA IT-company // URL: https://www.leta.ru/.