При условии разработки и размещения в свободном доступе на специализированных онлайн-магазинах (Google Play, App Store и др.) данные приложения вызовут обоснованный интерес той категории молодежи, которая готовится к поступлению в учреждения образования юридического профиля и изучает учебную дисциплину «Криминалистика». В этой связи посредством мобильных приложений могут быть с успехом решены отдельные задачи профориентационной работы, информационно-пропагандистской деятельности и иные.

Таким образом, в указанных условиях разработка, использование информационно-коммуникативных технологий, в том числе в виде мобильных приложений, специализированных компьютерных игр (тестов), способствуют более качественной подготовке юридического специалиста, повышению авторитета юридического образования и решению иных, связанных с указанными, задач.

1. О программе патриотического воспитания населения Республики Беларусь на 2022–2025 годы [Электронный ресурс] : постановление Совета Министров Респ. Беларусь, 29 дек. 2021 г., № 773 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Концепция развития юридического образования в Республике Беларусь на период до 2025 года [Электронный ресурс] : Концепция М-ва образования Респ. Беларусь, 31 авг. 2017 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

3. Непрерывное дополнительное образование в государствах – участниках СНГ: опыт, приоритеты и перспективы развития : сб. ст. IV Междунар. науч.-практ. конф., посвящ. 20-летию ИПКиП, г. Могилев, 26–27 нояб. 2020 г. / под ред. В.А. Гайсенка, И.В. Шардыко. – Могилев : МГУ им. А.А. Кулешова, 2021. – 352 с.

УДК 343.985.7

А.А. Точилкина

ПРОБЛЕМНЫЕ АСПЕКТЫ ОРГАНИЗАЦИИ ПРОЦЕССА РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ В УСЛОВИЯХ СОВРЕМЕННЫХ СОЦИАЛЬНО-ПРАВОВЫХ РЕАЛИЙ

Развитие современных технологий привносит в нашу жизнь как колоссальные возможности, так и новые угрозы. Преступления, совершаемые с использованием сети Интернет, – одна из серьезнейших проблем современного общества.

В условиях стремительного развития информационных технологий, широкое распространение получает новый вид преступной деятельности – киберпреступность, которая, несомненно, носит трансграничный характер. Киберпреступление – это правонарушение, которое совершено в электронной сфере, направлено на незаконное проникновение в работу компьютерных сетей, программ, устройств, с целью видоизменения данных, их изъятия или добавления ложной информации. Понятия «киберпреступление» и «киберпреступность» будут использоваться в данной статье, так как имеют один и тот же смысл с понятиями «преступление, совершаемое с использованием сети Интернет» и «преступность в сети Интернет» [1].

При расследовании преступлений указанной категории правоохранительные органы сталкиваются с рядом проблем, отдельные из которых подлежат рассмотрению.

В связи с вышеизложенным в первую очередь справедливо отметить, что киберпространство принципиально трансгранично, здесь нет расстояния и часто верно определить местоположение источника кибератаки очень трудно, что приводит к активизации транснациональной киберпреступной деятельности. Из транснационального характера киберпреступлений вытекают трудности их расследования. Одна из трудностей заключается в том, что принцип суверенитета предполагает проведение расследований в определенном государстве только с согласия этого государства. Именно поэтому очень важно сотрудничество между государствами – от этого зависит раскрытие киберпреступлений. Другая трудность связана со временем – оно крайне ограничено (а для совершения киберпреступления часто достаточно нескольких секунд, и следы от киберпреступлений удаляются очень быстро). В связи с этим решающее значение имеет оперативное и своевременное взаимодействие между государствами.

Во-вторых, следует отметить, что в условиях современных социально-правовых реалий киберпреступления становятся все более совершенными, изощренными и скрытными, они наносят крупный экономический и политический ущерб. В связи с этим следует указать, что в киберпространстве действуют разнородные субъекты – и государства, и негосударственные субъекты, что вызывает сложности при разграничении преступной деятельности и политической деятельности государств в киберпространстве. Некоторые негосударственные субъекты могут превосходить кибервозможности государств и способны проводить кибероперации, которые глубоко затрагивают безопасность отдельных государств и международную безопасность. Следовательно, в киберпространстве сглаживаются различия между государством и негосударственными субъектами в отношении ресурсов и кибервозможностей. Распространено мнение, что лишь государства способны прово-

дить мощные кибератаки, однако данное предположение представляется необоснованным, так как информационные технологии широко доступны, и ключевым фактором успеха кибероперации является технический талант, которым потенциально могут обладать как государственные (в лице специалистов), так и негосударственные субъекты.

Разнообразие субъектов злонамеренной деятельности в киберпространстве способствует возникновению такой проблемы, как сложности разграничения преступной деятельности и политической деятельности государств в киберпространстве. Грань между государственными кибероперациями и кибероперациями отдельных преступных группировок может быть крайне размытой. При этом критерий преследования политических целей не позволяет однозначно отделить государства от негосударственных субъектов в киберпространстве, потому как, во-первых, существуют такие негосударственные субъекты, как «хактивисты» – они продвигают политические идеи через несанкционированный доступ к компьютерным системам или осуществление иных кибероперациий (например, масштабными DDos-атаками), а во-вторых, потому что мотивы злоумышленников могут быть в принципе непонятны [2].

Проблема разграничения государства от негосударственных субъектов в киберпространстве также связана со способом совершения указанных преступлений:

для подготовки кибератаки не требуется, например, никаких материалов, которые доступны только государствам, нужен лишь компьютер и знания, потому как сети, образующие киберпространство, не являются монополией правительства и во многих случаях принадлежат частному сектору и управляются им. К тому же первые компьютерные взломы совершали именно негосударственные субъекты – «скучающие» компьютерщики хотели продемонстрировать свое мастерство. Кроме того, разнородность субъектов в киберпространстве усугубляется сложностью их идентификации, т. е. сложно установить действительный источник кибератаки с технической точки зрения, потому что киберпреступники умело заметают следы (очищают историю, стирают коды, могут запустить кибератаку из точки, которая не является местом их нахождения, и т. д.) [3].

доступность киберинструментов, которые могут быть приобретены в сети «Даркнет». «Покупка кибервозможностей» создает непредсказуемость и асимметрию среди субъектов совершения преступного деяния. Следует отметить, что использование в качестве способа совершения преступного деяния незащищенной сети передачи данных, связанных с внедрением злоумышленников в локальные сети при отсутствии защищенного с помощью сертифицированных программных средств сегмента сети и несоблюдении требований информационной

безопасности, свидетельствует о практически нулевой возможности раскрытия таких преступлений [4].

Следующий проблемный аспект при расследовании киберпреступлений – низкий уровень квалификации самих сотрудников правоохранительной системы, которые часто не относят многие правонарушения в сфере компьютерных технологий к категории преступлений и, как следствие, отказывают в возбуждении уголовного дела. Значительное число допускаемых в ходе расследования ошибок объясняется, как правило, недостаточной подготовленностью следователей в вопросах, связанных с функционированием глобальных компьютерных сетей.

Резюмируя вышеизложенное, приходим к выводу, что в деятельности правоохранительных органов по расследованию преступлений указанной категории необходимо идентифицировать источник кибератаки, а также разграничить преступную деятельность и политическую деятельность субъектов киберпространства. Проблему составляет и то, что нужно не просто установить источник запуска кибератаки, но и разобраться, управляли ли или нет компьютером удаленно при помощи вредоносного ПО и кто управлял кибератакой.

Успех в достоверном и оперативном установлении источника кибератак возможен только при эффективном взаимодействии правоохранительных органов государств и международной кооперации в расследовании.

При расследовании киберпреступлений возникают проблемы, порождаемые уникальными свойствами киберпространства (информационного пространства) глобальных компьютерных сетей. При этом специфика новых видов преступлений слабо учитывается практическими работниками при проведении следствия [5].

В связи с этим возрастает роль криминалистических средств и методов в раскрытии и расследовании киберпреступлений. Кроме того, помимо совершенствования материально-технического обеспечения деятельности следственных подразделений, необходимо расширить возможности привлечения к расследованию киберпреступлений специалистов/экспертов в области глобальных компьютерных сетей. Указанные меры позволят сотрудникам правоохранительных органов выявлять и правильно осуществлять осмотр, изъятие и исследование виртуальных следов, сбор, проверку и оценку доказательств, которые в конечном итоге будут признаны таковыми в силу своей достоверности и допустимости, что впоследствии повысит эффективность всего процесса расследования преступлений в киберпространстве.

1. Гончарова, С.В. Киберпреступления и преступления по телефону / С.В. Гончарова, Е.Н. Полунина // Балт. гуманитар. журн. – 2020. – № 3 (32). – С. 359–363.

2. Ресненко, А.В. Современный анализ киберпреступлений / А.В. Ресненко // Новые вопросы современной науки : материалы Междунар. (заоч.) науч.-практ. конф. – М., 2019. – С. 151–153.

3. Зайцев, А.А. Следы киберпреступлений / А.А. Зайцев, А.В. Смолин // Проблемы правовой и техн. защиты информ. – 2020. – № 8. – С. 61–65.

4. Садыкова, К.А. Некоторые проблемы раскрытия и расследования преступлений в сфере информационных технологий / К.А. Садыкова, Д.Е. Жонина // Междунар. журн. гуманитар. и естеств. наук. – 2021. – № 12-4 (63). – С. 171–173.

5. Шевченко, Е.С. Тактика отдельных следственных действий при расследовании киберпреступлений / Е.С. Шевченко // Закон и право. – 2015. – № 8. – С. 128–138.

УДК 343.985

А.М. Трофименко

ПОДГОТОВКА К ДОПРОСУ ПОДОЗРЕВАЕМОГО (ОБВИНЯЕМОГО) ПРИ РАССЛЕДОВАНИИ НЕНАДЛЕЖАЩЕГО ИСПОЛНЕНИЯ МЕДИЦИНСКИМ РАБОТНИКОМ ПРОФЕССИОНАЛЬНЫХ ОБЯЗАННОСТЕЙ

Общие правила проведения допроса закреплены в ст. 217 Уголовно-процессуального кодекса Республики Беларусь. При расследовании уголовных дел о преступлениях, предусмотренных ст. 162 Уголовного кодекса Республики Беларусь, указанное следственное действие является одним из наиболее значимых источников получения важной информации доказательственного характера. При этом с учетом сложности рассматриваемой категории уголовных дел, наличия специального субъекта преступления, корпоративной солидарности медицинских работников допрос имеет ряд специфических особенностей и требует тщательной, планомерной подготовки.

Обязательным условием является предварительное глубокое изучение личности медицинского работника, которое фактически должно быть начато с момента поступления заявления (сообщения) о совершенном ятрогенном преступлении. Кроме стандартной процедуры сбора характеризующих сведений различного рода (в том числе при допросе коллег по работе), запрашивается информация об образовании, повышении квалификации, наличии поощрений и фактов привлечения к ответственности за ненадлежащее исполнение своих обязанностей, жалоб со стороны пациентов и их родственников.

Следователю важно четко определить объем возложенных на подозреваемого (обвиняемого) профессиональных обязанностей. В этой связи в полном объеме, по возможности в оригиналах, изымается вся

соответствующая документация (должностные инструкции, контракты, приказы о назначении на должность, возложении дополнительных обязанностей, замещении). В случае совмещения с исполнением непосредственных обязанностей еще и административных функций (руководство работой отделения больницы) изъятию и последующему анализу подлежат обе должностные инструкции.

Во избежание использования подозреваемым (обвиняемым) некомпетентности следователя в области медицинских знаний в качестве проработки методической базы предстоящего допроса следователем отбираются и изучаются нормативные правовые акты, определяющие организационные основы оказания медицинской помощи, особенности диагностики и лечения определенного заболевания (законы Республики Беларусь, клинические протоколы Министерства здравоохранения Республики Беларусь и др.).

Применительно к конкретной следственной ситуации с целью оперирования необходимой медицинской терминологией, получения базовых сведений об отдельных медицинских манипуляциях изучается медицинская литература, в том числе справочного характера. При необходимости соответствующие сведения могут быть получены также у квалифицированных узких специалистов-медиков путем проведения устной консультации, допроса в качестве свидетеля по интересующему кругу вопросов либо посредством истребования по официальному запросу следователя в профильном учреждении здравоохранения либо Министерстве здравоохранения Республики Беларусь.

Анализируются уже содержащиеся в материалах уголовного дела сведения об обстоятельствах оказания ненадлежащей медицинской помощи (протокол осмотра места происшествия, медицинская карта, протокол операции, заключение судебно-медицинской экспертизы либо результаты патологоанатомического исследования, видеозаписи врачебных манипуляций, справки служебных проверок Министерства здравоохранения и его структурных подразделений, сведения о результатах разбирательств на уровне учреждения здравоохранения). В данном случае медицинские документы выступают одним из главных и наиболее информативных источников доказательств причастности врача или врачей к ненадлежащему оказанию медицинской помощи.

После обработки полученной информации составляется план предстоящего допроса, формулируется перечень подлежащих выяснению вопросов. В плане допроса целесообразно предусмотреть возможные варианты защиты. С целью преодоления возможного противодействия со стороны подозреваемого (обвиняемого) готовятся материалы, подлежащие предъявлению ему на обозрение в ходе следственного действия, планируется тактика очередности их предъявления. Психологически