Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность

Баранова Т.Ю., Озеров К.И., Кеменяш Ю.В.

ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ АКТАМ КИБЕРТЕРРОРИЗМА НА ОБЪЕКТАХ ТРАНСПОРТА

В данной статье рассмотрены различные аспекты проявления актов кибертерроризма на объектах транспорта, проанализировано законодательство в области обеспечения кибербезопасности объектов транспортного комплекса, а также определены основные направления совершенствования деятельности в данной области. На современном этапе данные вопросы имеют прикладную направленность в связи с возрастанием количества актов кибертерроризма. Повсеместное распространение информационно-телекоммуникационных технологий способствует повышению интереса отдельных категорий граждан к преступным деяниям в данной сфере.

Каждое 4 зарегистрированное в Российской Федерации преступление совершается с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Более половины всех преступлений экстремистской направленности совершены с использованием сети «Интернет» [1].

В первом квартале 2021 года в IT-сфере совершено на 33,7 % больше преступлений, чем год назад, в том числе с использованием сети Интернет – на 51,6 % и при помощи средств мобильной связи – на 31,6 %. В январе – марте 2020 года удельный вес таких деяний составлял 19,9 % от общего числа зарегистрированных преступлений, а за три месяца текущего года увеличился до 27,1 % [2].

20 октября 2020 года заместитель секретаря Совета Безопасности Российской Федерации Юрий Коков отметил, что количество преступлений, совершенных с использованием IT-технологий, увеличилось в 20 раз, а также обратил внимание на то, что информация, имеющаяся в киберпространстве, позволяет киберперступникам использовать интернет в качестве инструмента планирования и подготовки террористических актов [3].

1. В ряде стран киберпреступность стала объектом глобальных исследований, направленных на разработку методов, способов уличения преступников в содеянном. Россия не стала исключением, и нередко обращает внимание на опыт зарубежных стран. Киберпреступность – всемирная проблема, поэтому и бороться с ней следует совместными усилиями: перенимать опыт, давать советы, обращать внимание на развитие преступности в различных регионах стран, учитывать ошибки товарищей.

2. Так, за преступления, совершенные в сфере компьютерной информации, предусмотрена уголовная ответственность, но уголовное законодательство зарубежных стран значительно отличается от Уголовного Кодекса Российской Федерации [4]. Проанализировав историю развития киберпреступлений и развития зарубежного законодательства, можно сделать вывод, что первые шаги в защиту компьютерной информации были сделаны законодательством Швеции. В 1973 году в стране был принят «Закон о данных», который ввёл новое понятие «злоупотребление при помощи компьютера».

3. Киберугрозы не являются новостью для мира, так как одним из первых и широко известных преступлений в сфере информационных технологий признается преступление Роберта Морриса. Оно было совершено в ноябре 1988 года. 23-летний студент Роберт Моррис запустил вирус в сеть «Интернете». «Червь Морриса», как стало

известно позже, парализовал работу шести тысяч из 60 000 интернет-узлов в США. Многие корпорации и правительственные сайты отключились от Интернета, так как новости об инциденте распространились достаточно стремительно. Эпидемия показала, как опасно безоговорочно доверять компьютерным сетям [5].

Так, в России общественное внимание в большей степени содержится в таких материальных сферах жизнедеятельности, как сферах обслуживания, интернете и транспорта. Основываясь на вышеуказанных фактах, можно с уверенностью отметить, что сфера денежных переводов и платежей страдает от «хакерских» нападений почти ежедневно, принося огромный материальный ущерб всем ее пользователям.

Значимость противодействия киберпреступности на объектах транспорта обусловлена множеством факторов, которые можно проследить при изучении жизнедеятельности и средств жизнеобеспечения граждан [6].

Транспорт, как одна из основных материальных сфер жизнедеятельности граждан, является основным средством передвижения всех граждан по территории Российской Федерации и за ее рубежом. Он быстро развивается, создаются различные компьютерные системы, позволяющие управлять им без физического контакта, то есть с использованием возможностей виртуального пространства, искусственного интеллекта и наличием определенных программ. В связи с этим, следует констатировать, что транспортный комплекс находится под угрозой совершения актов незаконного вмешательства в вышеуказанные системы, которые не имеют должного образа защищенности [7].

4. Современные методы и способы противодействия киберпреступноти в сфере информационных технологий, зародившиеся в США, активно используются компетентными уполномоченными подразделениями в сфере безопасности в различных странах, в том числе в России.

5. На сегодняшний день, проблему проявления киберпреступности можно считать комплексной. В связи с этим, необходимо наличие усовершенствованной, соответствующей современным реалиям нормативной базы, которая смогла бы в должной мере, при правильном расчете угроз, их масштабов и приемов, используемых преступными субъектами, выработать тактику противодействия и предупреждения преступлений в данной области. С учетом развития угроз совершения актов киберпреступности на объектах транспорта, необходимо отметить важность принятия новых нормативно-правовых актов, либо внесений изменений в уже существующие, основываясь на том, что объекты транспортной инфраструктуры являются неотъемлемым элементом жизнедеятельности граждан и совершение актов киберпреступности на таковых объектах может привести к непоправимым последствиям.

6. Также, необходимо отметить, что киберпреступность на объектах транспорта представляет собой целый ряд важнейших вызовов, связанных с различными обстоятельствами [8].

7. Во-первых, важно отметить невозможность прогнозирования кибератак из-за их скрытого, внутреннего характера, характеризующегося отсутствием явных подготовительных действий, анонимностью субъектов, зашифровкой каналов выхода в сеть, постоянной сменой местонахождения ip-адресов с помощью специально подготовленных программ, что в свою очередь затрудняет возможность поиска самих субъектов и фиксации их преступной деятельности.

8. Во-вторых, из-за неурегулированности вопросов в области киберпреступности, включающих отсутствие законодательно закрепленного самого понятия киберпреступность, ответственности лиц их совершивших, а также поиск, захват и выдача отдельных лиц представляются проблематичными.

Вопрос совершенствования деятельности территориальных органов МВД России на транспорте на региональном уровне при проведении мероприятий по противодействию кибертерроризму на объектах транспорта должен рассматриваться комплексно всеми ведомствами, так или иначе имеющими полномочия влиять на законодательную и исполнительную базу в целях ее улучшения и оптимизации.

При рассмотрении основных законов, нормативных актов, и приказов государственных служб и ведомств, регулирующих состояние безопасности на транспорте Российской Федерации, обнаруживается ряд недостатков. Неоспоримо, что уже предпринято множество мер, для предотвращения и устранения угрозы совершения актов незаконного кибервмешательства на объектах транспорта, но в комплексе выработать единую законодательную и исполнительную систему крайне сложно [9].

Этому факту есть вполне объяснимые причины. Во-первых, протяженность транспортных маршрутов очень велика, во-вторых, сложность обуславливается большим количеством пассажиров и грузов, в-третьих, все транспортные объекты относятся к разным формам собственности, что усложняет применение к ним единой системы контроля и надзора, в-четвертых, наличие огромного количества систем, позволяющих надлежащим образом функционировать различным видам транспорта.

Анализ действующего законодательства в сфере обеспечения безопасности на объектах транспорта, позволяет сделать вывод о том, что несмотря на наличие отдельных проектов в области обеспечения кибербезопасности на объектах транспорта, деятельность линейных подразделений в области обеспечения кибербезопасности объектов транспортной инфраструктуры в должной мере не определена. Также, важно отметить, что не существует четких понятий, касаемых границ полномочий по противодействию актам кибертерроризма на объектах транспортного комплекса.

Необходимо отметить, что на проблему недостаточного правового регулирования в деятельности по защите объектов возможных антитеррористических посягательств и мест массового пребывания граждан и исследователи по вопросам антитеррористической безопасности обращались неоднократно. В частности, Н.С. Рязанов акцентировал внимание на существенные различия объектов по виду деятельности, специфике их работы, что усложняет задачу разработки общих унифицированных требований и подходов к организации их защищенности [10]. В.Б. Вехов, С.А. Ковалев отмечают особенности совершаемых преступных посягательств и выделяют причины, которые препятствуют эффективной борьбе с преступлениями данного вида: специфика данной сферы, высокая динамика, развитие и изменение, недостаточное урегулирование общественных отношений в данной сфере и другие [11]. В связи с чем, данный вопрос остается актуальным и обсуждаемым среди научных деятелей и практическими сотрудниками правоохранительных органов.

Важно обратить внимание на необходимость обсуждения проблем правовой неурегулированности в рамках заседаний антитеррористической комиссии в части осуществления антитеррористической деятельности уполномоченными субъектами, а именно при проведении мероприятий, направленных на защищенность объектов транспорта от киберугроз, а также внесения предложений в Национальный антитеррористический комитет для устранения пробелов в данном вопросе на законодательном уровне.

Также, проанализировав нормативно-правовые акты в области обеспечения кибербезопасности на объектах транспорта, предлагаем осуществлять разработку региональных и типовых муниципальных программ противодействия идеологии кибертерроризма исключительно на уровне антитеррористических комиссий субъектов Российской Федерации, что в свою очередь поспособствует качественному решению вопросов в области системности всей работы и четкой координации всех мероприятий по обеспечению кибербезопасности транспортных комплексов России.

Важно отметить, что Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [12] является одним из основополагающих источников по обеспечению транспортной безопасности от киберугроз.

В его статьях излагаются основные понятия, такие как: автоматизированная система управления, безопасность критической инфраструктуры, информационной инфраструктуры, компьютерная атака, компьютерный инцидент, критическая информационная инфраструктура и другие. Однако понятие «киберпреступность» отсутствует,

что указывает на неполное соответствие Федерального закона современным угрозам. Предлагаем законодательным органам внести изменение в ст. 2 данного закона, добавив понятие «киберпреступность», сформулировав его следующим образом: «киберпреступность – это совокупность явлений и процессов, возникающих в сфере информационно-телекоммуникационных технологий, образующих преступную деятельность, целью которой является осуществление неправомерного доступа к охраняемой законом компьютерной информации, создание, использование и распространение вредоносных программ, допущение нарушений в области эксплуатации средств хранения, обработки или передачи компьютерной информации и воздействия незаконным путем на критическую информационную структуру Российской Федерации».

Необходимость совершенствования способов противодействия таким противоправным деяниям со стороны усовершенствования нормативного урегулирования вопросов киберпреступности на транспорте, а именно внесения корректировки в Приказ Министерства транспорта Российской Федерации, Федеральной службы безопасности Российской Федерации и Министерства внутренних дел Российской Федерации от 5 марта 2010 г. № 52/112/134 «Об утверждении Перечня потенциальных угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры и транспортных средств» [13] в связи с проблемами противодействия киберпреступности на транспорте, как насущной и перспективной угрозе.

Необходимо отметить, что непосредственной задачей сотрудников правоохранительных органов является информирование граждан о фактах увеличения числа совершаемых киберпреступлений, совершенных с использованием сети Интернет, иначе киберпреступники, будут продолжать осуществлять свою деятельность по обогащению своего капитала за счет незнания людей о данных преступлениях.

Помимо информирования граждан перед сотрудниками правоохранительных органов стоит нелегкая задача, состоящая в совершенствовании навыков и знаний в сфере IT- технологий, им необходимо знать, какие угрозы существуют в настоящее время.

Эффективность противодействия киберпреступности на объектах транспорта возможно повысить путем повышения уровня квалификации у сотрудников территориальных органов МВД России на транспорте, а также путем устранения следующих причин, служащих для кибертеррористов благоприятными условиями:

- несоответствие программного обеспечения и операционных систем заявленным требованиям современных киберугроз;
- отсутствие кадров, специализирующихся на кибербзопасности и на защите от киберугроз;
- дефицит, связанный с проведением профилактических мероприятий и непризнание слабой защищенности в области кибербезопасности;
- отсутствие знаний сотрудников правоохранительных структур о возможных неблагоприятных последствиях от преступлений в киберсреде;
- сложная структурированная система сферы информационно-телеком-муникационных технологий.

ЛИТЕРАТУРА

1. Генеральная прокуратура Российской Федерации: портал правовой статистики [Электронный ресурс]. URL: genproc.gov.ru (дата обращения: 24.12.2020).

2. Министерство внутренних дел Российской Федерации [Электронный ресурс] // мвд.рф. URL: https://мвд.рф/reports/item/23816756/ (дата обращения: 01.05.2021).

3. Тасс [Электронный ресурс] // tass.ru. URL: https://tass.ru/proisshestviya/9767825 (дата обращения: 14.12.2020).

4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ: ред. от 5 апреля 2021 г.: с изм. от 8 апреля 2021 г. // Рос. газ. 18 июня № 113, 1996 г.; № 114. 19 июня1996 г.; № 115. 20 июня 1996 г. № 118. 25 июня 1996 г.

5. Чекунов И.Г. Понятие и отличительные особенности киберпреступности // Российский следователь. 2014. № 18. С. 53–56.

6. Меняйло Д.В., Колесников А.Г., Баранова Т.Ю. Кибертерроризм как угроза транспортному комплексу современной России // Эволюция государства и права: проблемы и перспективы. 2020. С. 461-465.

7. Рязанов Н.С. К вопросу о соотношении понятий «безопасность» и «транспортная безопасность» // Вестник Омской юридической академии. 2017. № 3. С. 89-94.

8. Агеев А.С. Право на доступ к информации, находящейся в распоряжении государственных органов (особенности конституционно-правового регулирования в России и в Германии): дис. … канд. юрид. наук. М., 2016. 162 с.

9. Чекунов И.Г. Понятие и отличительные особенности киберпреступности // Российский следователь. 2014. № 18. С. 53-56.

10. Рязанов Н.С. Проблемы соотношения институтов уголовно-правовой охраны интересов государства в сфере транспортной безопасности и административной ответственности // Транспортное право. 2017. № 3. С. 29-32.

11. Вехов В.Б., Ковалев С.А. Проблемы борьбы с кибертерроризмом // Правопорядок: история, теория, практика. 2018. № 1 (16). С. 89-93.

12. О безопасности критической информационной инфраструктуры Российской Федерации: Федер. закон Рос. Федерации от 26 июля 2017 г. № 187. Доступ из справ.-правовой системы «КонсультантПлюс».

13. Об утверждении Перечня потенциальных угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры и транспортных средств: приказ Министерства транспорта Российской Федерации, Федеральной службы безопасности Российской Федерации и Министерства внутренних дел Российской Федерации от 5 марта 2010 г. № 52/112/134. Доступ из справ.-правовой системы «КонсультантПлюс».

СВЕДЕНИЯ ОБ АВТОРАХ

Баранова Таисия Юрьевна. Инспектор специализированного отдела по обеспечению общественного порядка (в перевозочном и технологическом секторах объектов транспортной инфраструктуры).

Линейный отдел МВД России в аэропорту Внуково (г. Москва).

Служебный адрес: 119027, Российская Федерация, г. Москва, ул. 2-я Рейсовая, д. 2 А.

Озеров Кирилл Игоревич. Адъюнкт факультета подготовки научно-педагогических и научных кадров.

Московский Университет МВД России имени В.Я. Кикотя.

Служебный адрес: 117997, Российская Федерация, г. Москва, ул. Академика Волгина, д. 12.

Кеменяш Юлия Витальевна. Научный сотрудник отделения организации научно-исследовательской работы научно-исследовательского отдела.

Белгородский юридический институт МВД России имени И.Д. Путилина.

Служебный адрес: 308024, Российская Федерация, г. Белгород, ул. Горького, д. 71.

Ключевые слова: кибертерроризм; кибербезопасность; транспортный комплекс; транспортная безопасность.

УДК 343.9