мо наладить работу по мониторингу интернет-пространства с целью оперативного реагирования на размещаемые материалы, для признания их экстремистскими, разоблачения фейковой информации и, соответственно, привлечению лиц, разместивших данный контент, к установленной законом ответственности. Не следует забывать о необходимости информационно-просветительской работы с населением, в большей степени в среде подрастающего поколения, для популяризации патриотизма, уважения к истории своей страны, веротерпимости и законопослушности.

УДК 343.3

Д.К. Куаныш

ОСОБЕННОСТИ МОШЕННИЧЕСТВА В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Одним из современных явлений, которое коренным образом повлияло на развитие глобальных процессов в мировом сообществе, стало интенсивное совершенствование информационно-коммуникационных технологий. Масштаб культурных, социальных, экономических, политических, правовых изменений, вызванных распространением сетевых компьютерных коммуникаций, позволяет многим ученым считать их отражением начала нового этапа в истории человеческой цивилизации. Использование глобальной компьютерной сети Интернет выступает одной из важнейших предпосылок глобализации межгосударственных отношений и построения информационного общества.

Избрав цель занять достойное место среди ведущих стран мира в области развития информационного общества, Республика Казахстан активно развивает собственную информационную и телекоммуникационную инфраструктуру, формирует адекватную политику по обеспечению информационной безопасности.

Киберпреступление – это преступление, совершенное дистанционно в киберпространстве, направленное на причинение вреда охраняемым законом разнородным общественным отношениям, совершаемое с использованием информационно-телекоммуникационных сетей, средств и устройств с доступом в киберпространство. Киберпреступление обязательно обладает такими признаками, как противоправность, общественная опасность, виновность и наказуемость.

Исследование признаков и особенностей киберпреступлений нередко вызывает определенные сложности. Во-первых, это отсутствие в юридической науке и правоприменительной практике устоявшегося терминологического аппарата для данной группы противоправных деяний.

Общественная опасность рассматриваемых уголовных правонарушений заключается прежде всего в том, что они нарушают права и законные интересы граждан и организаций, охраняемые законом интересы общества и государства в информационной сфере, наносят вред конфиденциальности, целостности, сохранности и доступности информационных ресурсов, информационных систем и инфраструктуры связи [1].

Квалификация, раскрытие и расследование уголовных правонарушений в сфере информатизации и связи остается до сих пор нелегкой задачей для сотрудников правоохранительных и специальных органов Республики Казахстан. К причинам подобного рода можно отнести:

отсутствие обобщений следственной и судебной практики;

соответствующих научно обоснованных методических и криминалистических рекомендаций;

специального учебного курса, при подготовке в учебных заведениях системы МВД сотрудников следственно-криминалистической специализации, а также следователей, дознавателей, оперативных сотрудников на курсах повышения квалификации и переподготовки;

достаточной подготовленности сотрудников правоохранительных органов к работе со специфическим видом доказательственной информации, возникающей в результате совершения этих уголовных правонарушений, и рядом других факторов.

Для понимания и уточнения некоторых особенностей исследуемой нами киберпреступности необходимо остановиться на отдельных составах преступлений, где объектом выступают в первую очередь общественные интересы в сфере информационной безопасности.

Объектом уголовного правонарушения, предусмотренного ст. 205 Уголовного кодекса (УК) Республики Казахстан, являются права и законные интересы граждан и организаций на конфиденциальность информации, информационных систем и сетей телекоммуникаций. Предметом рассматриваемого уголовного правонарушения выступают: информация, охраняемая законом и содержащаяся на электронном носителе; информационная система, в том числе информационная система государственных органов; сеть телекоммуникаций; государственные электронные информационные ресурсы.

Объективная сторона рассматриваемого уголовного правонарушения выражается в неправомерном доступе к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или сеть телекоммуникаций. Неправомерный доступ к охраняемой

законом информации, содержащейся на электронном носителе, выражается в получении возможности непосредственного завладения этой информацией и может быть осуществлен как с преодолением мер защиты, установленных собственником (владельцем) электронного носителя, так и без такового. Неправомерный доступ к сетям телекоммуникаций выражается в получении возможности непосредственного взаимодействия с входящими в нее информационными системами и их составляющими и осуществляется, как правило, с преодолением мер защиты. Доступ осуществляется только программно-техническими средствами.

Неправомерный доступ без преодоления защиты может осуществляться через компьютер, на котором открыт доступ (сеанс) лицом, имеющим право на это (администратор, пользователь системы и сети). Неправомерный доступ может осуществляться удаленно, в том числе через сеть Интернет.

Рассматриваемое уголовное правонарушение по конструкции относится к материальному составу. Оно признается оконченным с момента наступления вредных последствий. Рассматриваемое уголовное правонарушение по конструкции относится к материальному составу. Оно признается оконченным с момента наступления вредных последствий. Вредные последствия выражаются в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства. Согласно п. 14 ст. 3 УК Республики Казахстан, в котором дано понятие существенного вреда, здесь следует понимать, в частности:

нарушение конституционных прав и свобод человека и гражданина, прав и законных интересов организаций, охраняемых законом интересов общества и государства;

причинение значительного ущерба (т. е. ущерба на сумму, в сто раз превышающую месячный расчетный показатель);

нарушение нормальной работы организаций или государственных органов [2].

Между неправомерным доступом и наступившими общественно опасными последствиями должна быть установлена причинная связь.

С субъективной стороны рассматриваемое уголовное правонарушение может быть совершено только умышленно (прямой и косвенный умысел): виновный сознает, что он совершает неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или сеть телекоммуникации, предвидит возможность или неизбежность наступления общественно опасных последствий и желает их наступления.

По отношению к причинению существенного вреда в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства возможен косвенный умысел, когда виновное лицо сознательно допускает эти последствия либо относится к их наступлению безразлично.

Мотивы и цели данного уголовного правонарушения разнообразны и на квалификацию не влияют, но они должны учитываться при индивидуализации наказания. В большинстве случаев это корыстный мотив.

В ч. 2 ст. 205 УК Республики Казахстан установлена ответственность за неправомерный доступ к национальному электронному информационному ресурсу или национальной информационной системе.

Национальными признаются информационные системы, состоящие из государственных электронных информационных ресурсов, имеющих важное стратегическое значение для экономики и безопасности государства. В ч. 3 ст. 205 УК Республики Казахстан предусмотрен особо квалифицирующий признак – тяжкие последствия. С учетом положений п. 4 ст. 3 УК Республики Казахстан к тяжким последствиям необходимо относить, в частности: самоубийство потерпевшего (потерпевшей) или его (ее) близкого (близких); причинение крупного или особо крупного ущерба. Эти последствия должны находиться в причинной связи с умышленным неправомерным доступом.

Проведя небольшой анализ ст. 205 УК Республики Казахстан, непосредственно к рассматриваемой нами области исследования, мы отнесли именно совершение неправомерного доступа к информации, в информационную систему или сеть телекоммуникаций именно удаленно, с компьютерного устройства через сеть Интернет, образующим киберпространство.

Во-вторых, затрудняет исследование киберпреступности отсутствие статистического учета преступлений, совершенных в киберпространстве, официальная статистика располагает данными только по перечисленным выше уголовным правонарушениям. Учитывая наш подход к определению киберпреступлений, значительный круг уголовных правонарушений находится в различных главах Особенной части УК Республики Казахстан. Использование информационно-телекоммуникационных сетей, средств и устройств с доступом в киберпространство является квалифицирующим признаком некоторых уголовных правонарушений в разрезе объектов посягательства [1].

Необходимо отметить, что с развитием высоких технологий и расширением сферы их использования, перечень уголовных киберправонарушений может постоянно расширяться, и не всегда уголовное законодательство будет своевременно реагировать на новые угрозы в киберпространстве.

Как правило, киберпреступления различают по своим целям, объектам воздействия, способам и средствам совершения преступного деяния.

В связи с этим имеющиеся проблемы в сфере обеспечения кибербезопасности не могут быть полноценно решены традиционными методами и средствами. Они требуют системного подхода при создании комплексного механизма безопасности, способной противостоять многочисленным киберугрозам. Во-первых, это координация усилий в данном направлении государственных органов, негосударственных структур, бизнеса и общества в целом. Во-вторых, это разработка адекватной системы противодействия киберпреступности, которая включает в себя широкий спектр мероприятий по анализу объективных условий и субъективных обстоятельств, порождающих киберпреступления, механизмов их совершения, способов выявления, пресечения, расследования, опыт судебного рассмотрения.

Список использованных источников

1. Борчашвили, И.Ш. Комментарий к Уголовному кодексу Республики Казахстан. Особенная часть (т. 2) / И.Ш. Борчашвили / под общ. ред. Генер. прокурора Респ. Казахстан, Гос. советника юстиции I класса А.К. Даулбаева. – Алматы : Жеті Жарғы, 2015. – С. 1120.

2. Уголовный кодекс Республики Казахстан [Электронный ресурс]. – Режим доступа: http://www.zakon.kz. – Дата доступа: 15.08.2022.

УДК 343

С.В. Кузьменкова

О ПРОТИВОДЕЙСТВИИ ВЫСОКОТЕХНОЛОГИЧНОЙ ПРЕСТУПНОСТИ В СЕТИ ИНТЕРНЕТ

Общественная деятельность современного мира характеризуется преобладанием информационных отношений, которые сложно представить без использования современных информационных технологий. Глобальная компьютеризация современного общества приводит к увеличению числа интернет-пользователей, которые не всегда способны удовлетворить свои потребности в силу ряда причин, в том числе и экономического характера, что приводит к увеличению преступности в сети Интернет. Совершение преступлений с использованием цифровых технологий является весьма актуальной проблемой белорусского государства, так как влечет не только появление новых рисков, но и огромную угрозу национальной безопасности. Соответственно, эффективность противостояния данному вызову оказывает непосредственное воздействие не только на защиту прав и интересов граждан, но и на обеспечение информационной безопасности общества и государства в целом.

Несмотря на меры, принимаемые на протяжении последних лет, в Республике Беларусь наблюдается рост количества регистрируемых преступлений в сфере информационных технологий. Так, в 2015 г. было зарегистрировано 2 440 преступлений, 2016 г. – 2 471, 2017 г. – 3 099, 2018 г. – 4 741, 2019 г. – 10 539, в 2020 г. – 25 561. Начиная же с 2021 г. отмечается относительное снижение числа рассматриваемых преступлений (за прошедший год было зарегистрировано 15 503 таких преступлений).

Международный опыт показывает, что для большинства стран мира также свойственно увеличение числа преступлений, совершенных с использованием информационных технологий. Например, на территории Российской Федерации только за последние годы число таких уголовно наказуемых деяний выросло на 73,4 %, а их удельный вес в структуре преступности составил 25 %.

В настоящее время в Республике Беларусь наиболее распространенными в числе рассматриваемых преступлений являются следующие: несанкционированный доступ к компьютерной информации (ст. 349 Уголовного кодекса Республики Беларусь (УК)); разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств (ст. 354 УК), а также хищение путем модификации компьютерной информации (ст. 212 УК).

Целесообразно отметить, что известные методы оплаты в сети Интернет позволяют совершать платежи с помощью введения в компьютерную систему сведений о банковской платежной карточке, а при завладении персональными данными клиента – разрешают открывать и использовать счета. Механизмы завладения указанной информацией весьма разнообразны, что способствует злоумышленникам совершать различные платежи в сети Интернет, а также пользоваться счетами без ведома их владельцев. С целью завладения денежными средствами пользователей злоумышленники также создают и используют всевозможные учетные записи (аккаунт) в социальных сетях и различных мессенджерах.

В свою очередь, совершенно очевидно, что совершение рассматриваемых преступлений обусловливается множеством факторов. Так, несовершенство уголовного законодательства в сфере борьбы с высокотехнологичной преступностью приводит к тому, что до настоящего времени окончательно так и не решен вопрос оценки ущерба от данных преступных посягательств. Кроме этого, в следственно-судебной практике отсутствует единая точка зрения в понимании и применении уголовно-правовых норм правоохранительными органами, что приводит к назначению наказаний, не связанных с лишением свободы, либо прекращению уголовного производства по делу в связи с