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

деятельным раскаянием лица, примирением сторон и возмещением причиненного ущерба, что в последующем приводит к росту рецидива преступлений.

Полагается, что ряд проблемных вопросов противодействия цифровой преступности в глобальной компьютерной сети Интернет заключается в следующем: недостаточное поступление в правоохранительные органы количества заявлений потерпевших о совершении рассматриваемого вида преступлений; уровень квалификации сотрудников и финансирование подразделений в сфере борьбы с цифровой преступностью требует определенного повышения; отсутствие на законодательном уровне положений, всесторонне рассматривающих порядок расследования данных преступлений и пр.

Таким образом, сегодня перед государством стоит стратегически важная задача, заключающаяся в разработке эффективных способов противодействия высокотехнологичной преступности в сети Интернет.

Применительно к Республике Беларусь особое внимание целесообразно уделять тщательной предварительной подготовке при проведении осмотра места происшествия, обыска или выемки, использованию специальных технических устройств и программного обеспечения, а также принятию мер по обеспечению сохранности компьютерной информации. Например, проведение такого следственного действия, как прослушивание и запись переговоров (ст. 214 Уголовно-процессуального кодекса Республики Беларусь) по уголовным делам, если имеются достаточные основания полагать, что эти переговоры содержат сведения о преступлении, либо имеющие значение для дела, может способствовать установлению мест нахождения используемой компьютерной техники, иных незаконных предметов, документов (в частности электронных).

Кроме того, весьма важно предусмотреть и специальные меры предупреждения преступлений, совершенных с использованием информационных технологий в сети Интернет. К числу данных мер относятся: повсеместное введение и обеспечение достаточной и обязательной идентификации личности пользователя (включая места общественного пользования интернетом); разработка для каждого пользователя сети Интернет программы предоставления электронного сертификата, в котором будут содержаться все сведения, идентифицирующие личность пользователя; введение процедуры заключения в письменном виде договора с провайдером, способствующее предотвращению регистрации неподписанных электронных ящиков.

Однако противодействовать рассматриваемому роду преступности лишь на национальном уровне малоэффективно, так как принцип территориальности практически неприменим к глобальной компьютерной

сети Интернет. В этой связи одним из важнейших вопросов в сфере противодействия преступлениям, совершаемым с использованием цифровых технологий в сети Интернет, является совершенствование международного взаимодействия в сторону его упрощения, что, в свою очередь, окажет положительное влияние, например, на оперативность исполнения запроса о правовой помощи, а соответственно, и на эффективность противодействия вышеуказанной преступности.

Резюмируя изложенное, очевидно, что противодействие высокотехнологичной преступности в сети Интернет является одним из наиболее злободневных вопросов, стоящих перед современным обществом и государством. Совершенствование порядка расследования, сбора и оценки доказательств, повышение уровня научно-методического обеспечения, а также развитие международного сотрудничества является основой противодействия рассматриваемой преступности.

УДК 343.92

В.В. Лавренов, М.А. Лохницкий

НЕКОТОРЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ПРИ ПОСТРОЕНИИ ЭФФЕКТИВНОЙ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ

На нынешнем этапе мирового развития информационная сфера приобретает ключевое значение для современного человека, общества, государства и оказывает всеобъемлющее влияние на происходящие экономические, политические и социальные процессы в странах и регионах.

Наблюдается рост преступности с использованием информационно-коммуникационных технологий. Появился новый вид преступности – киберпреступность. Киберпреступность – это любая преступная деятельность, нацеленная на компьютер, компьютерную сеть или подключенное устройство или использующая ее.

Математическое моделирование является одним из новых направлений в борьбе с преступностью, и за последнее время был предложен ряд моделей, в которых используются различные подходы. Они варьируются от моделей на основе метода когнитивного моделирования до дифференциального моделирования.

При применении метода моделирования выделяют пять этапов:

1) создание репрезентативной среды;

2) тестирование, исследование и оценка;