Сүйіншалин Б. И., *магистрант Института послевузовского образования (Карагандинская академия МВД РК им. Б. Бейсенова, г. Караганда, Республика Казахстан)*

Меры противодействия уголовным правонарушениям в сфере информатизации и связи в Республике Казахстан

Аннотация. В статье рассматриваются меры противодействия уголовным правонарушениям в сфере информатизации и связи в Республике Казахстан. Развитие информационной сферы становится одним из ключевых моментов, влияющих на общественное и государственное развитие. От степени развитости информационного общества зависит эффективность функционирования государственных институтов, экономики и обороноспособности государств. Необходимым условием состоятельности государства в условиях современности выступает наличие соотносимого с потребностями граждан информационного общества. Однако технологическая эволюция одновременно с положительными моментами порождает новые проблемы и угрозы информационной безопасности государств, усугубляя существующие. Автор приходит к выводу, что в Казахстане складывается эффективная система противодействия информационным угрозам, которая осуществляется при полном взаимодействии всех государственных органов, негосударственных структур и граждан Республики Казахстан.

Ключевые слова: противодействие, правонарушение, киберпреступность, информатизация, связь, национальная безопасность, законодательство, развитие, информационная сфера.

В соответствии с п. 5 ст. 4 Закона Республики Казахстан «О национальной безопасности Республики Казахстан» от 6 января 2012 года № 527-IV информационная безопасность относится к видам национальной безопасности. Информационная безопасность — это состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны [1].

Развитие информационной сферы становится одним из ключевых моментов, влияющих на общественное и государственное развитие. От степени развитости информационного общества зависит эффективность функционирования государственных институтов, экономики и обороноспособности государства. Необходимым условием состоятельности государства в условиях современности выступает наличие соотносимого с потребностями граждан информационного общества. Однако технологическая эволюция одновременно с позитивом порождает новые проблемы и угрозы информационной безопасности государств, усугубляя существующие. В обстановке глобальной конкуренции информационное давление становится действенным и эффективным методом решения межгосударственных конфликтов. Возможности глобальных информационно-коммуникационных сетей все интенсивнее используются экстремистскими и террористическими организациями для пропаганды и популяризации своей идеологии, распространения радикальных идей, вовлечения все большего числа единомышленников, их обучения, поддержания контактов и финансирования. Информационные системы государств подвержены угрозе компьютерных атак, являющихся одним из способов террористической деятельности. Организованные транснациональные преступные группы все активнее используют современные информационно-коммуникационные технологии в криминальных целях. Меняется динамика уголовных правонарушений в сфере информатизации и связи, для нее характерна устойчивая тенденция роста. С 2008 по 2017 гг. в Казахстане зафиксировано 778 уголовных правонарушений в сфере информатизации и связи. С переходом на интернет-рельсы оплаты покупок и сервисов в геометрической прогрессии растет и количество кибер-преступлений. По данным Генпрокуратуры Республики Казахстан, в этом году количество правонарушений в IT-сфере выросло на 25 % [2].

При этом, несмотря на увеличение зарегистрированных уголовных правонарушений с использованием современных информационно-коммуникационных технологий, официальная статистика не отражает объективную картину распространения уголовных правонарушений в сфере информатизации и связи, показывая лишь незначительную часть реально совершенных. Особенность уголовных правонарушений с использованием современных информационно-коммуникационных технологий заключается в их высокой латентности, появлении новых, изощренных способов совершения уголовных правонарушений, доказательство которых сильно затруднено из-за отсутствия необходимых правовых, организационных и технических инструментов. Поэтому борьба с уголовными правонарушениями в сфере информатизации и связи обусловливает потребность соответствующего оперативного реагирования, совместных скоординированных действий спецслужб и правоохранительных органов государств. «Вопрос о создании новых органов и организаций, координирующих и осуществляющих борьбу с киберпреступностью, что, в свою очередь, требует подготовки национальных кадров, представителей которых можно было бы привлекать на службу в транснациональные органы и организации, направленные на борьбу с киберпреступностью», становиться наиболее актуальным [3, 28–33].

В этой связи, в системе МВД в Департаменте Криминальной полиции в 2003 г. было создано новое подразделение — Управление «К» (специальной оперативно-аналитической работы и раскрытия преступлений в сфере высоких технологий). Одним из основных направлений деятельности подразделений по борьбе с преступлениями в сфере высоких технологий является выявление и раскрытие преступлений в телекоммуникационных и информационных системах, а именно:

– борьба с преступлениями, связанными с незаконным доступом к компьютерной информации;

– борьба с незаконным оборотом радиоэлектронных и специальных технических средств;

– борьба с распространением предметов и информации, запрещенных в свободном обороте (порнографии, контрафактной продукции, вредоносных программ);

– борьба с преступлениями в сфере телекоммуникаций, а также организация работы по использованию возможностей информационно-телекоммуникационных и компьютерных технологий для раскрытия преступлений.

Для системной борьбы с уголовными правонарушениям в сфере информатизации и связи в 2006 г. был создан также Национальный контактный пункт по борьбе с преступлениями в сфере информационных технологий, который осуществляет постоянный обмен информацией со странами СНГ и дальним зарубежьем.

Обеспеченность сферы информационной безопасности квалифицированными кадрами является одним из основных факторов, влияющих на результативность борьбы с уголовными правонарушениями в сфере информатизации и связи. Помимо этого необходимо совершенствование процессов и методики обучения, повышения квалификации специалистов, занятых в сфере обеспечения информационной безопасности и борьбы с уголовными правонарушениями в сфере информатизации и связи.

Для эффективной работы по противодействию уголовным правонарушениям в сфере информатизации и связи требуется правовое обеспечение информационной сферы на государственном уровне, в связи с чем следует обратить особое внимание на правовые механизмы, регулирующие:

1) информационные правоотношения, возникающие при поиске, получении, потреблении различной категории информации, информационных ресурсов, информационных продуктов, информационных услуг;

2) процессы производства, передачи и распространения информации, информационных ресурсов, информационных продуктов, информационных услуг;

3) информационные правоотношения, возникающие при создании и применении информационных систем, их сетей, средств обеспечения, телекоммуникационной инфраструктуры.

Для обеспечения государственных органов полной, достоверной и своевременной информацией требуются: принятие обоснованных решений, в том числе для защиты государственных информационных ресурсов; разработка отечественных средств защиты информации и системы подтверждения соответствия импортируемых технических средств установленным требованиям, а также дальнейшая проработка вопросов противодействия техническим разведкам, защиты от информационного оружия и совершенствования нормативной правовой базы в данной сфере. Необходима комплексная координация мер по защите информации в общегосударственном масштабе и на ведомственном уровне для обеспечения целостности и конфиденциальности информации [4, 47].

По мнению Д. А. Вечеринского, И. И. Шалькевича, меры противодействия компьютерным преступлениям можно подразделить на технические, организационные и правовые [5, 69].

К техническим мерам можно отнести: защиту от несанкционированного доступа к системе; резервирование особо важных компьютерных подсистем; организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев; установку оборудования для тушения пожара, для обнаружения воды; принятия конструкционных мер защиты от хищений, саботажа, диверсий; оснащение помещений замками; установку сигнализации и многое другое.

К организационным мерам относятся: охрана вычислительного центра; тщательный подбор персонала; исключение случаев ведения особо важных работ только одним человеком; наличие плана восстановления работоспособности центра после выхода его из строя; организация обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра; универсальность средств защиты от всех пользователей, включая высшее руководство; возложение ответственности на лиц, которые должны обеспечить безопасность центра; выбор места его расположения и т. п.

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства, вопросы общественного контроля за разработчиками компьютерных систем и принятие международных договоров об их ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашения.

В уголовном законодательстве Казахстана сегодня сложилась ситуация, когда отношения в сфере информационной безопасности потребовали криминализации ряда общественно опасных деяний и самостоятельной охраны названных отношений в отдельной главе Особенной части Уголовного кодекса, вследствие чего законодатель предусмотрел данную ситуацию и в новом Уголовном кодексе Республики Казахстан от 3 июля 2014 г. и объединил уголовные правонарушения в сфере информатизации и связи в одну 7 главу, включающую 9 основных составов уголовных правонарушений, за которые предусмотрена уголовная ответственность за совершение уголовных правонарушений в сфере информатизации и связи [6].

Таким образом, в Казахстане принимаются меры противодействия уголовным правонарушениям в сфере информатизации и связи на техническом, организационном и правовом уровне, а также складывается эффективная система противодействия информационным угрозам, которая осуществляется при полном взаимодействии всех государственных органов, негосударственных структур и граждан Республики Казахстан.

Түйін

Мақалада Қазақстан Республикасында ақпараттық және коммуникациялық саласындағы қылмыстық құқық бұзушылықтарға қарсы іс-қимыл шаралары қарастырылады.

Resume

In the article the author considers measures of counteraction to criminal offenses in the field of information and communication in the Republic of Kazakhstan.

Список использованной литературы:

1. Закон Республики Казахстан «О национальной безопасности Республики Казахстан» от 6 января 2012 г. № 527-IV // http://online.zakon.kz/Document/?doc_id=31106860

2 Статистические сведения о состоянии преступности в Республике Казахстан // http://service.pravstat.kz

3. Протасевич А. А., Зверянская П. П. Борьба с киберпреступностью как актуальная задача современной науки // Криминологический журнал Байкальск. гос. ун-та экономики и права. — 2011. — № 3.

4. Ахметов Е. Киберпреступность в Казахстане // Законность и правовая статистика. — 2009. — № 2 (11).

5. Вечерский Д. А., Шалькевич И. И. Расследование компьютерных преступлений. — Минск, 2001.

6. Уголовный кодекс Республики Казахстан: Практ. пос. — Алматы, 2018.