УДК 343.85

ПРОФИЛАКТИКА УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ В РЕСПУБЛИКЕ КАЗАХСТАН

Г. Р. Рустемова
доктор юридических наук, профессор,
профессор кафедры уголовного права и криминологии
Алматинской академии МВД Республики Казахстан
имени Макана Есбулатова

Статья посвящена профилактике уголовных правонарушений в сфере информатизации и связи в Республике Казахстан. Использование сети Интернет, других средств информатизации и связи предполагает защиту от незаконного проникновения в базы данных. В Казахстане принят ряд законов в этой сфере, в том числе новая глава VII Уголовного кодекса Республики Казахстан «Уголовные правонарушения в сфере информации и связи». Рассматриваются меры правового, организационного и технического характера в рамках действующего уголовного законодательства и законодательства в сфере информатизации и связи. По мнению автора, данные меры должны рассматриваться в каждом конкретном случае самостоятельно для реализации задач общих и специальных мер профилактики уголовных правонарушений в указанной сфере.

Ключевые слова: *Республика Казахстан, уголовные правонарушения в сфере информатизации и связи, профилактика, правовые, организационные, технические меры.*

Одной из эффективных мер противодействия всем правонарушениям является профилактика. Идея о необходимости профилактики правонарушений высказывалась со времен Античности.

Профилактика правонарушений — комплекс правовых, экономических, социальных и организационных мер, осуществляемых субъектами профилактики правонарушений, направленных на сохранение и укрепление правопорядка путем выявления, изучения, устранения причин и условий, способствующих совершению правонарушений [1].

Все виды уголовных правонарушений в сфере информатизации и связи можно так или иначе предотвратить. Имеющийся зарубежный опыт свидетельствует о том, что для решения этой задачи необходимо использовать различные профилактические меры. В данном случае профилактические меры следует понимать как деятельность, направленную на выявление и устранение причин, порождающих правонарушения, и условий, способствующих их совершению.

Каких-либо особенных методов, применяемых в Республике Казахстан для противодействия правонарушений в сфере информатизации и связи, не имеется. Используются те же методы, что и во всем мире. В мире в борьбе с киберпреступлениями применяются в совокупности различные меры, в том числе правовые, организационные и технические методы.

К правовым мерам профилактики правонарушений в первую очередь относятся нормы законодательства — нормы, устанавливающие ответственность за правонарушения, совершенствование уголовного и иного законодательства, заключение и исполнение международных договоров в данной сфере.

В Республике Казахстан принят ряд законов, направленных на профилактику уголовных правонарушений в сфере информатизации и связи.

Вопросы профилактики отражены в Законе Республики Казахстан от 29 апреля 2010 г. № 271-IV «О профилактике правонарушений», который определяет основные и общие правовые, экономические, социальные и организационные основы деятельности государственных органов, органов местного самоуправления, организаций и граждан Республики Казахстан по профилактике правонарушений [1].

Отметим также специальные законы: Закон Республики Казахстан от 24 ноября 2015 г. № 418-V «Об информатизации», регулирующий общественные отношения в сфере информатизации, возникающие на территории Республики Казахстан между государственными органами, физическими и юридическими лицами при создании, развитии и эксплуатации объектов информатизации; Закон Республики Казахстан от 5 июля 2004 г. № 567 «О связи», устанавливающий правовые основы деятельности в области связи на территории Республики Казахстан, определяющий полномочия государственных органов по регулированию данной деятельности, права и обязанности физических и юридических лиц, оказывающих или пользующихся услугами связи [2; 3]. Кроме того, вопросы информационной безопасности в сфере информатизации и связи содержатся в Законах Республики Казахстан: «О государственных секретах» от 15 марта 1999 г. № 349-I, «О персональных данных и их защите» от 21 мая 2013 г. № 94-V, «Об электронном документе и электронной цифровой подписи» от 7 января 2003 г. № 370-II [4; 5].

Принят целый ряд подзаконных актов, разработанных в целях реализации Закона Республики Казахстан «Об информатизации», вступившего в силу с 1 января 2016 г. Так, Правительством Республики Казахстан утверждена «Концепция кибербезопасности («Киберщит Казахстана»)» от 30 июня 2017 года № 407 [6]. Концепция определяет основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий, предлагает ввести в правовое поле понятие «кибергигиена».

В Уголовном кодексе Республики Казахстан от 3 июля 2014 г. № 226-V (с изменениями и дополнениями по состоянию на 11.01.2020 г.) выделена отдельная глава № VII с девятью статьями, именуемая «Уголовные правонарушения в сфере информации и связи», в которой содержатся нормы, регламентирующие уголовную ответственность за правонарушения в сфере информации и связи:

«Статья 205. Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций.

Статья 206. Неправомерные уничтожение или модификация информации.

Статья 207. Нарушение работы информационной системы или сетей телекоммуникаций.

Статья 208. Неправомерное завладение информацией.

Статья 209. Принуждение к передаче информации.

Статья 210. Создание, использование или распространение вредоносных компьютерных программ и программных продуктов.

Статья 211. Неправомерное распространение электронных информационных ресурсов ограниченного доступа.

Статья 212. Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели.

Статья 213. Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства [7].

Уголовно-правовая характеристика правонарушений подробно изложена в литературе [8].

В Кодексе Республики Казахстан об административных правонарушениях от 5 июля 2014 г. № 235-V также содержится глава 31 «Административные правонарушения в области информатизации и связи», состоящая из 5 статей [9]. Между тем, одними правовыми мерами не удается достичь должных результатов профилактической деятельности.

Далее рассмотрим применение мер организационного характера. Организационные меры направлены на исключение возникновения ситуаций, угрожающих инфор-

мационной безопасности. К ним относятся документы, регламентирующие процессы функционирования информационно-коммуникационной инфраструктуры, политика информационной безопасности, утвержденная для каждой структуры отдельно, различные методики оценки рисков информационной безопасности и наличие нижеперечисленных правил:

– идентификация, классификация и маркировка активов, связанных со средствами обработки информации;

– обеспечение непрерывной работы активов, связанных со средствами обработки информации;

– инвентаризация и паспортизация средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения;

– проведение внутреннего аудита информационной безопасности;

– использование средств криптографической защиты информации;

– разграничение прав доступа к электронным информационным ресурсам;

– использование Интернета и электронной почты;

– организация процедуры аутентификации;

– организация антивирусного контроля;

– использование мобильных устройств и носителей информации;

– «организация физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов» [10].

К организационным мерам также относится кадровая политика. В заключаемых трудовых договорах отражаются в обязательном порядке условия конфиденциальности, как на весь период работы, так и на определенный срок после расторжения трудового договора. Кроме того, осуществляется создание службы информационной безопасности с непосредственным подчинением первому руководителю, обучение персонала правилам и средствам защиты информации с учетом последних нововведений.

Согласно Концепции кибербезопасности Республики Казахстан, в целях «реализации задачи по формированию необходимых условий для повышения осведомленности об угрозах, развития человеческого капитала и потенциала отечественной отрасли информационно-коммуникационных технологий, устойчивой к вредоносному программно-техническому воздействию, предлагается формирование в обществе устойчивых представлений о «кибергигиене» [6]. В ситуации стремительного перехода информации в цифровую форму крайне важно соблюдать определенный набор правил безопасности работы в мире информационных технологий.

Кибергигиена подразумевает соблюдение элементарных основ цифровой безопасности при работе в информационно-коммуникационной среде, ставшей неотъемлемой частью нашей жизни.

В понятие «кибергигиена» входят такие рекомендации, как использование только лицензионного программного обеспечения и своевременная установка всех выходящих обновлений:

отказ от установки на вычислительные устройства (компьютеры, ноутбуки, планшеты, телефоны и т. д.) программного обеспечения, производитель которого неизвестен, а источник скачивания не проверен, шифрование пользовательских данных;

отказ от открытия и перехода по ссылкам в электронных письмах, полученных от неизвестных источников;

использование сложных и разных паролей на всех интернет-ресурсах (электронная почта, социальные сети и т. д.), так как утечка пароля на одном из таких ресурсов сделает уязвимым профиль на других ресурсах;

полный отказ от передачи пароля третьим лицам и пересылки ПИН-кодов от банковских карт;

удаление профилей на интернет-ресурсах, если больше он не используется;

избегание посещения неизвестных сайтов, размещаемый контент которых не соответствует общепринятым нормам нравственности, морали либо ограничен к размещению законодательством;

использование антивирусных средств, которые в свою очередь позволят блокировать известные уязвимости:

удаление в социальных сетях подробной информации (ФИО, дата рождения, точное место проживания) о себе и своих близких, а если такие данные имеются — немедленно скрыть.

Тем самым подчеркивается, с одной стороны, элементарность правил кибергигиены, с другой — необходимость соблюдения этих правил на уровне повседневной привычки.

Помимо организационных мер, существенную профилактическую роль играют меры технического характера. Технические меры предназначены для защиты от нежелательного воздействия на информационные системы и сети телекоммуникации, «закрытия возможных каналов утечки конфиденциальной информации за счет применения лазерных, радиотехнических и других способов перехвата, а также средств визуального наблюдения и средств связи, других технических приспособлений» [11].

Применение этих методов осуществляется путем использования различных технических разработок, устройств, специального оборудования, программного и аппаратно-программного обеспечения.

Условно технические меры, в зависимости от характера и специфики защищаемого объекта, можно разделить на две основные группы: аппаратные и программные. Аппаратные методы применяются для защиты аппаратных средств и средств связи компьютерной техники от нежелательных физических воздействий на них сторонних сил, а также для блокирования возможных каналов утечки конфиденциальной информации и имеющихся данных. Практическая реализация данных методов осуществляется через применение различных технических устройств, к ним относятся:

– различные устройства и сооружения, препятствующие проникновению к защищаемой информации;

– источники бесперебойного питания, предохраняющие от скачкообразных перепадов напряжения и обеспечивающие электропитание в экстренных случаях и при авариях;

– устройства экранирования аппаратуры, линий проводной связи и защищаемых помещений;

– устройства, обеспечивающие санкционированный физический доступ пользователя в защищаемое помещение (замки, система управления контролем доступа, устройства идентификации личности и т. п.);

– устройства идентификации и фиксации используемых терминалов и пользователей при попытках несанкционированного доступа к информационно-коммуникационной инфраструктуре;

– средства охранно-пожарной сигнализации;

– средства защиты портов компьютерной техники;

– средства визуального контроля за внутренним и внешним периметром.

Программные же методы защиты предназначаются для непосредственной защиты информации. В частности, используются различные методы шифрования данных, применение паролей и средств антивирусного контроля. Последние являются в настоящее время одним из действенных способов борьбы с компьютерными вирусами, вызывающими различные нежелательные последствия в виде неправомерного доступа третьих лиц к информационно-коммуникационной инфраструктуре, уничтожения, блокирования, модификации или копирования информации, нарушения работы информационной системы.

В настоящее время идеальной всеохватывающей системы противодействия правонарушениям в сфере информатизации и связи не существует. Только комплексный

подход к рассматриваемой проблеме и сочетание различных правовых, организационных и технических мер противодействия позволят добиться уменьшения общественно опасных деяний в отношении личности, общества и государства.

На современном этапе развития нашего общества проблема совершаемых преступлений и правонарушений в рассматриваемой сфере пока не является существенной, в отличие от развитых стран. В государстве происходит процесс освоения рынка новых информационных технологий, интеграции в международные компьютерные сети, решение вопросов компьютерной оснащенности и интеграции государственных органов и организаций, остается низким кадровый потенциал сотрудников, специализирующихся на создании отечественных современных информационных технологий.

Однако указанные факторы, на наш взгляд, носят временный характер. Увеличивающиеся темпы интеграции Республики Казахстан в мировое информационное пространство, заполнение рынка доступными средствами информационных технологий и их внедрение в повседневную жизнь граждан, выявление отдельных фактов совершения уголовных правонарушений в рассматриваемой сфере свидетельствуют о том, что в ближайшем будущем эта проблема может стоять остро.

Поэтому вопросы совершенствования эффективности мер профилактики преступлений и правонарушений в сфере информатизации и связи являются актуальными, призваны содействовать нейтрализации и минимизации негативных последствий преступной деятельности, предупреждению возникновения таких угроз.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. О профилактике правонарушений [Электронный ресурс] : Закон Респ. Казахстан, 29 апр. 2010 г., № 271-IV // Сайт информационно-правовой системы НПА РК. — Режим доступа: http://adilet.zan.kz/rus/docs/Z100000271_. — Дата доступа: 11.03.2020.

2. Об информатизации [Электронный ресурс] : Закон Респ. Казахстан, 24 нояб. 2015 г., № 418-V ЗРК // Сайт информационно-правовой системы НПА Р. — Режим доступа: http://adilet.zan.kz/rus/docs/Z1500000418. — Дата доступа: 11.03.2020.

3. О связи [Электронный ресурс] : Закон Респ. Казахстан, 5 июля 2004 г., № 567. — Режим доступа: https://online.zakon.kz/document/?doc_id=1049207. — Дата доступа: 10.03.2020.

4. О государственных секретах [Электронный ресурс] : Закон Респ. Казахстан, 15 марта 1999 г., № 349-1 // Сайт информационно-правовой системы НПА РК. — Режим доступа: http://adilet.zan.kz/rus/docs/Z990000349. — Дата доступа: 10.03.2020.

5. О персональных данных и их защите [Электронный ресурс] : Закон Респ. Казахстан, 21 мая 2013 г., № 94-V. — Режим доступа: https://online.zakon.kz/document/?doc_id=31396226. — Дата доступа: 22.04.2020.

6. Об утверждении Концепции кибербезопасности (Киберщит Казахстана) [Электронный ресурс] : постановление Правительства РК, 30 июня 2017 г., № 407 // Сайт информационно-правовой системы НПА РК. — Режим доступа: http://adilet.zan.kz/rus/docs/Z1700000407. — Дата доступа: 13.05.2019.

7. Уголовный кодекс Республики Казахстан [Электронный ресурс] : 3 июля 2014 г., № 226-V : с изм. и доп. по сост. на 11.01.2020 г. — Режим доступа: https://zakon.uchet.kz/rus/docs/K1400000226. — Дата доступа: 21.04.2020.

8. Уголовное право Республики Казахстан. Особенная часть : учебник. Т. 1. — Алматы : Жеті Жарғы, 2016. — 500 с.

9. Кодекс Республики Казахстан об административных правонарушениях [Электронный ресурс] : 5 июля 2014 г., № 235-V : с изм. и доп. по сост. на 16.01.2020 г. — Режим доступа: https://online.zakon.kz/document/?doc_id=31577399#pos=9088;-5. — Дата доступа: 21.04.2020.

10. Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры [Электронный ресурс] : постановление Правительства Респ. Казахстан, 8 сент.2016 г., № 529 : с изм. и доп. по сост. на 31.12.2019 г. — Режим доступа: https://online.zakon.kz/Document/?doc_id=36572190#pos=1;-98. — Дата обращения 21.04.2020.

11. Абраменкова, В. С. Технические средства — одна из мер предупреждения компьютерных преступлений [Электронный ресурс] / В. С. Абраменкова // Сибирский юрид. вестник. — 1999. — № 4. — Режим доступа: http://www.law.edu.ru/doc/document.asp?docID=1117307. — Дата обращения: 21.04.2020.

Поступила в редакцию 18.05.2020 г.
Контакты: g.rustemova@mail.ru (Рустемова Гаухар Рустембековна)

Rustemova G. R.

PREVENTION OF CRIMINAL OFFENSES IN INFORMATIZATION AND COMMUNICATIONS IN THE REPUBLIC OF KAZAKHSTAN

The article is devoted to the prevention of criminal offenses in the field of informatization and communicationservice in the Republic of Kazakhstan. The use of the Internet, other means of hardware and software and communication implies protection against unlawful entryinto databases. Kazakhstan is not an exception. Therefore, the state has adopted a number of laws regulating a number of laws in this area, including the new chapter VII of the Criminal Code of the Republic of Kazakhstan «Criminal offenses in the field of information and communications». Measures of legal, organizational and technical nature are considered within the framework of the current criminal law and legislation in the field of informatization and communications. They are discussed generally without details. However, each of them should be considered independently to implement tasks of general and special measures for the prevention of criminal offenses in this area.

Keywords: *Republic of Kazakhstan, criminal offenses in the field of informatization and communications, prevention, legal, organizational, technical measures.*