УДК 342

Сергеев Сергей Александрович
магистр юриспруденции, Казахский гуманитарно-юридический инновационный университет, г.Семей
e-mail: sergeev-1955.18@mail.ru

ПРАВОВАЯ ПОЛИТИКА РЕСПУБЛИКИ КАЗАХСТАН ПО ПРЕОДОЛЕНИЮ ПРОБЛЕМ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Цифрлы технологиялардың дамуы және Ғаламтордың кеңеюі сарапшылардың айтуы бойынша екі бағытты болды. Бір жағынан ол қолданушыларға көп мүмкіндік берсе, екінші жағынан жаңа қылмыстық құқық бұзушылықтардың пайда болуына әкелді. Мақалада ақпарат және байланыс саласында, киберқылмыстармен күресті заңнамалық қамтамасыз ету саласында ақпараттық қауіпсіздікті қамтамасыз ету бойынша мемлекеттің қызметі талданады. Қазақстанның киберқауіпсіздік саласындағы проблемалар мен қауіптерге сипаттама беріледі және оларды шешу жолдары ұсынылады.

***Түйін сөздер**: киберқауіпсіздік, киберқылмыстар, концепция, мониторинг, алаяқтық, интернет, информация, телекоммуникация.*

Стремительное развитие цифровых технологий и постоянное расширение Всемирной сети обернулось, как и предсказывали эксперты, палкой о двух концах. С одной стороны, оно открыло новые возможности для пользователей, а с другой, породило новый вид уголовных правонарушений. В статье проведен анализ деятельности государства по обеспечению информационной безопасности в области информатизации и связи, законодательному обеспечению борьбы с киберпреступностью. Дается характеристика проблем и угроз в сфере кибербезопасности Казахстана, предложены пути их решения.

***Ключевые слова:** кибербезопасность, киберпреступность, концепция, мониторинг, мошенники, интернет, информация, телекоммуникация.*

The rapid development of digital technologies and the continuous expansion of the World Wide Web turned out, as experts predicted, a double-edged sword. On the one hand, it opened up new opportunities for users, and on the other, gave birth to a new type of criminal offense. The article analyzes the activities of the state to ensure information security in the field of information and communication, legislative support of the fight against cybercrime. The problems and threats in the sphere of cybersecurity of Kazakhstan are characterized, the ways of their solution are offered.

***Keywords:** cybersecurity, cybercrime, concept, monitoring, scammers, Internet, information, telecommunications.*

Стремительное развитие цифровых технологий и постоянное расширение Всемирной сети обернулось, как и предсказывали эксперты, палкой о двух концах. С одной стороны, оно открыло новые возможности для пользователей, а с другой, породило новый вид уголовных правонарушений, получивших приставку «кибер».

Сегодня уголовные правонарушения в сфере информационных технологий в нашей стране в процентном соотношении пока уступают общеуголовным (5 к 95), однако лиха беда начало: есть высокая вероятность, что в самом ближайшем будущем они увеличатся в разы. Ведь чем больше становится активных пользователей Всемирной сети, тем сильнее разгорается аппетит у киберпреступников. Количество онлайн-покупок увеличивается в геометрической прогрессии, что привлекает повышенное внимание хакеров к содержимому чужих электронных кошельков. Да и в целом сама интернет-ниша в Казахстане ещё полностью не освоена, поэтому на неё нацелены виртуальные мошенники и воры буквально со всех стран мира.

В Казахстане атакам со стороны киберпреступников подвержены Алматы, Караганда и Астана. Это именно те города, в которых больше всего банковских и финансовых центров, учебных заведений, а также промышленных предприятий и государственных учреждений.

Основные виды уголовных правонарушений в сфере информационных технологий включают как распространение вредоносных вирусов, взлом паролей, кражу номеров кредитных карточек и других банковских реквизитов (фишинг), так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) через Интернет, коммунальные объекты.

Способы и методы совершения уголовных правонарушений становятся более изощренными. К примеру, участились мошеннические действия, связанные с кредитными карточками, не редко становятся

случаи с использованием платежной системы «QIWI кошелек» для взаиморасчета по сбыту героина.

Мошенники переправляют пользователей на интернет ресурсы, которые блокируют работу браузера, и появляется текст от имени правоохранительных органов, в частности, от министерства внутренних дел РК, сообщающий о нарушении закона просмотра, или копирования запрещенного контента. Для разблокировки мошенники вынуждают пользователей интернета оплатить через платежные терминалы определенный штраф [1].

В Казахстане специально создано управление «К», криминальной полиции, которое специализируется на этих видах уголовных правонарушений.

Киберпреступность угрожает не только отдельным лицам или организациям, но потенциально – национальной безопасности любой страны, достигшей значительного уровня компьютеризации жизненно важных отраслей экономики.

В целях борьбы с киберпреступностью вводятся законодательные акты, которые будут заслоном от совершения подобных уголовных правонарушений.

В действующем Уголовном кодексе РК от 03.07.2014 года впервые в истории отечественной юриспруденции, появилась целая глава 7, посвящённая киберпреступлениям – «Уголовные правонарушения в сфере информатизации и связи».

С учетом квалифицирующих обстоятельств в ней содержится 38 составов уголовных правонарушений против электронных информационных ресурсов и систем или сетей телекоммуникаций, за которые предусмотрена уголовная ответственность [2].

Основным непосредственным объектом рассматриваемых уголовных правонарушений является состояние защищенности охраняемой законом информации, находящейся на электронных носителях информационной системы или сети телекоммуникаций.

Дополнительным непосредственным объектом могут выступать права человека на личную тайну, тайну усыновления и т.п. Предметом данных уголовных правонарушений выступают электронные носители, информационная система или сеть коммуникаций, содержащие охраняемую законом информацию [3].

Предыдущая редакция Уголовного кодекса не содержала аналогичных составов.

Кодекс Республики Казахстан об административных правонарушениях также содержит ряд составов административных правонарушений, за совершение которых предусмотрены меры административной ответственности, в том числе на должностных лиц, не выполняющих обязанности по обеспечению информационной безопасности в виде нарушения требований по эксплуатации средств защиты электронных информационных ресурсов, невыполнения Единых требований, неосуществления или ненадлежащего осуществления собственником или владельцем информационных систем, содержащих персональные данные, мер по их защите [4].

Для обеспечения государственных органов полной, достоверной и своевременной информацией требуется принятие обоснованных решений, в том числе для защиты государственных информационных ресурсов, разработка средств защиты информации, совершенствования нормативной правовой базы в данной сфере.

Начиная с 1998 года, когда было принято постановление Правительства Республики Казахстан от 31 декабря 1998 года № 1384 «О координации работ по формированию и развитию национальной информационной инфраструктуры, процессов информатизации и обеспечению информационной безопасности», было принято 3 новых редакции законов Республики Казахстан «Об информатизации» (2003, 2007, 2015 годы) и несколько специализированных законов Республики Казахстан о внесении в них соответствующих изменений по вопросам электронных форматов представления информации (данных) в том числе по вопросам информационно-коммуникационных сетей, «электронного правительства».

За прошедший период электронные информационные ресурсы и информационные системы введены в хозяйственный оборот наряду с другими видами имущественных активов, расширена сфера их рыночного использования.

Характерная для последних десятилетий общемировая тенденция внедрения достижений информационно-коммуникационных технологий с темпами, существенно опережающими формирование культуры их использования, и укоренения общественных и производственных отношений, характерных для «информационного общества», в первую очередь, в вопросах обеспечения кибербезопасности, в Казахстане также находит свое подтверждение.

С этапа становления вопросов информационной безопасности с учетом

характера содержащейся информации дифференцированы правовые режимы общедоступных и конфиденциальных электронных информационных ресурсов и систем, установлены права и обязанности собственников, владельцев и пользователей по их защите.

Деятельность государственных органов и других субъектов по обеспечению информационной безопасности в области информатизации и связи осуществляется в соответствии с их отраслевой компетенцией, а также целями и задачами в предметных областях, связанных с использованием ИКТ (регулирование связи и информационных технологий, защита персональных данных, защита государственных секретов, противодействие деятельности иностранных технических разведок, оперативно-розыскная деятельность на сетях связи, расследование уголовных правонарушений, совершаемых с использованием ИКТ и другие).

В целом, в Республике Казахстан организационно-правовые и технические основы системы мер по обеспечению информационной безопасности в области информатизации и связи (кибербезопасности) формировались и законодательно закреплялись как составляющие информационной безопасности и обеспечения безопасности информационного пространства и инфраструктуры связи в соответствии с Законом Республики Казахстан «О национальной безопасности».

В последние годы различные взаимоувязанные аспекты обеспечения информационной безопасности в области информатизации и связи нашли свое отражение и развитие в Уголовном кодексе Республики Казахстан, Кодексе Республики Казахстан «Об административных правонарушениях», законах Республики Казахстан «О государственных секретах», «О персональных данных и их защите», «Об электронном документе и электронной цифровой подписи», «О связи», и целом ряде подзаконных актов, разработанных в реализацию новой редакции Закона Республики Казахстан «Об информатизации», вступившего в силу с 1 января 2016 года [5].

Ряд подзаконных актов, принятых в последнее время, еще не получил развернутой правоприменительной практики. В частности, постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности», представляющих собой кодификацию правовых и технических норм из национальных и гармонизированных стандартов. Документ подробно описывает процедуры и правила по использованию информационно-коммуникационных технологий при обработке защищаемых законом видов информации, содержит важные нормы по обеспечению технологической безопасности информационной инфраструктуры, информационных систем и ресурсов, программного обеспечения, технических средств на всех этапах их жизненного цикла [6].

На законодательном уровне регламентировано функционирование системы мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства», включающих в себя как государственные, так и негосударственные информационные системы, интегрируемые с государственными.

В Правилах проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации «электронного правительства», утвержденных приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 66, заложены основные принципы взаимодействия между заинтересованными сторонами при технологических сбоях или признаках компьютерных атак, а также алгоритмы реагирования на возникающие события и инциденты информационной безопасности [7].

Центр мониторинга безопасности «электронного правительства» ежедневно выявляет не устраненные уязвимости, о чем для принятия мер направляет уведомления владельцам информационных систем, являющиеся его компонентами. Имеется положительная динамика выявляемых уязвимостей и принимаемых в отношении них мер. Так в 2014 году было выявлена 1241 не устранённая уязвимость, в 2015 – 469, в 2016 – 355.

Также постановлением Правительства Республики Казахстан от 8 сентября 2016 года № 529 утверждены Правила и критерии отнесения объектов к критически важным объектам информационно-коммуникационной инфраструктуры из числа особо важных государственных и стратегических объектов, а также объектов отраслей экономики, имеющих стратегическое значение.

На подобные объекты, вошедшие в перечень критически важных объектов информационно-коммуникационной инфраструктуры, распространяются Единые требования, а также необходимость участия в предусмотренных законодательством совместных мероприятиях по обеспечению мониторинга их информационной безопасности, защиты и безопасного функционирования, включая обязанность информирования об инцидентах информационной безопасности.

Совершенствуются процедуры введения информационных систем в промышленную эксплуатацию. В этой связи, законодательно дифференцированы меры безопасности к информационным системам в зависимости от их отнесения к определенному классу, ограничен срок нахождения информационной системы в режиме опытной эксплуатации.

Требования по безопасности банковских информационных систем обеспечиваются нормативно-правовыми актами Национального Банка Республики Казахстан с учетом отраслевых и международных требований по обеспечению безопасности информационных систем.

Транснациональный и трансграничный характер многих продуктов ИКТ и международная связанность сетей телекоммуникаций общего пользования используются преступностью в целях совершения противоправных действий в отношении пользователей и операторов ИКТ-услуг и владельцев Интернет-ресурсов, размещенных в национальном сегменте, а также информационных систем, взаимодействующих с Интернетом.

Высокая латентность и зачастую международный характер таких уголовных правонарушений повышают их общественную опасность. Ситуация усугубляется укоренившимися в обществе стереотипами о безнаказанности так называемой «киберпреступности», ненужности принимаемых государством мер по укреплению сферы безопасного использования ИКТ, ограниченными возможностями органов правопорядка по привлечению к ответственности виновных в совершении высокотехнологичных преступлений, несмотря на развитые уголовно-правовые институты информационной безопасности.

Нагнетаемая отдельными странами милитаризация сферы ИКТ, трудности в доказывании причастности государств к использованию ИКТ в нарушение принципов международного права, вызванные в значительной степени стихийно сложившимся характером существующей международной системы управления Интернетом, сохраняющийся цифровой разрыв между странами препятствует формированию в мировом сообществе надежных международно-правовых инструментов предотвращения военного использования достижений в сфере информатизации и телекоммуникаций.

При этом по своей сути арсенал, используемый в военных целях, не отличается от арсенала программно-технических средств, используемых киберпреступностью, о чем свидетельствуют массовые случаи использования ИКТ в разведывательных, подрывных и иных целях, угрожающих поддержанию международного мира и безопасности.

Международные террористические группировки используют Интернет и социальные сети для распространения своих посланий и привлечения недовольных, предупреждают эксперты. Опасные тенденции набирает такое явление, как кибертерроризм.

Уголовные правонарушения, совершаемые экстремистами и другими преступниками, включают в себя взлом и кражу данных, а также распространение и пропаганду экстремистов.

Вербовка через Интернет тоже относится к киберпреступности.

Таким образом, Казахстан в сфере кибербезопасности испытывает такие серьезные угрозы как:

- низкая правовая грамотность населения, работников сферы ИКТ и руководителей организаций по вопросам информационной безопасности;

- нарушение государственными и негосударственными субъектами информатизации и пользователями услуг в сфере ИКТ установленных требований, технических стандартов и регламентов сбора, обработки, хранения и передачи информации в электронной форме;

- непреднамеренные ошибки персонала и технологические сбои, оказывающие негативное воздействие на информационные системы, программное обеспечение и другие элементы информационно-коммуникационной инфраструктуры;

- действия международных преступных групп, сообществ и отдельных лиц по осуществлению хищений в финансово-банковской сфере, вредоносного воздействия в целях нарушения работы автоматизированных систем управления технологическими процессами промышленности, энергетики, связи

и в сфере информационно-коммуникационных услуг;

- деятельность политических, экономических, террористических структур, разведывательных и специальных служб иностранных государств, направленная против интересов Республики Казахстан, путем оказания разведывательного и подрывного воздействия на информационно-коммуникационную инфраструктуру.

Низкая правовая грамотность по вопросам информационной безопасности и отсутствие сформировавшихся потребностей в её повышении у населения, работников сферы ИКТ и руководителей организаций создают питательную почву для развития правонарушений и преступлений в информационной сфере.

Отсутствие знаний о правовых ограничениях создает иллюзию дозволенности действий, нарушающих права и свободы других граждан, права обладателей авторских и смежных прав на программное обеспечение и влияющих на функционирование информационных ресурсов.

Таким образом, низкий уровень цифровой грамотности конечных пользователей в вопросах защиты персональных данных при отсутствии базовых знаний по общим методам распространения вредоносных компьютерных программ и программных продуктов (особенно «фишинговые» страницы поддельных интернет-магазинов и банков, распространение вирусных и «троянских» программ через «взломанные» сайты, скачивание нелицензионного («пиратского») программного обеспечения) приводят к тысячам случаев, когда граждане Республики Казахстан становятся жертвами, а принадлежащие им технические средства орудиями противоправного использования ИКТ.

В рамках правительственной программы борьбы с терроризмом на 2017-2020 г.г. Правительством Республики Казахстан утверждена Концепция кибербезопасности («Киберщит Казахстана»)[8].

Концепция основана на оценке текущей ситуации в сфере информатизации государственных органов, автоматизации государственных услуг, перспектив развития «цифровой» экономики и технологической модернизации производственных процессов в промышленности, расширения сферы оказания информационно-коммуникационных услуг.

Она определяет основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий.

Данная Концепция призвана обеспечить единство подходов к мониторингу обеспечения информационной безопасности государственных органов, физических и юридических лиц, а также выработку механизмов предупреждения и оперативного реагирования на инциденты информационной безопасности, в том числе в условиях чрезвычайных ситуаций социального, природного и техногенного характера, введения чрезвычайного или военного положения.

Целями Концепции являются достижение и поддержание уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, обеспечивающего устойчивое развитие Республики Казахстан в условиях глобальной конкуренции.

К задачам Концепции относятся:

- формирование необходимых условий для повышения осведомленности об угрозах, развития человеческого капитала и потенциала отечественной отрасли ИКТ по созданию программных продуктов и систем кибербезопасности, направленных на блокирование и подавление вредоносного программно-технического воздействия и защищённого телекоммуникационного оборудования;

- совершенствование правоприменительной практики, методологической базы, нормативно-правового и организационно-технического обеспечения безопасного использования ИКТ в национальной системе защиты информации и безопасности автоматизированных систем управления технологическими процессами;

- создание высоко адаптивной и интегрированной системы государственного управления информационной безопасностью в сфере информатизации и связи в отношении всей национальной информационно-коммуникационной инфраструктуры.

Выполнение данной Концепции послужит дальнейшей модернизации казахстанского общества и будет способствовать реализации Стратегии «Казахстан-2050» по вхождению Казахстана в число 30-ти самых развитых государств мира, а также станет вкладом Казахстана в реализацию Глобальной программы кибербезопасности ООН.

Скоординированная реализация Концепции «Киберщит Казахстана» позволит существенно повысить место Казахстана в Глобальном

индексе кибербезопасности и достигнуть к 2022 году индекса 0,600.

На реализацию Концепции в 2017-2022 годах будут направлены средства государственного бюджета в рамках бюджетных программ заинтересованных государственных органов и предусмотренных в Плане реализации Государственной программы «Цифровой Казахстан 2020».

Список использованной литературы

1. Нормативное постановление Верховного Суда Республики Казахстан от 29 июня 2017 года № 6 «О судебной практике по делам о мошенничестве».
2. Уголовный кодекс Республики Казахстан от 3 июля 2014 года *(с* изменениями и дополнениями *по состоянию на 09.01.2018 г.)*
3. Комментарий к Уголовному кодексу Республики Казахстан /Под. ред. д.ю.н., профессора С.М. Рахметова, д.ю.н., профессора И.И. Рогова. – Алматы: ТОО «Издательство «Норма-К», 2016. – 752 с.
4. Кодекс Республики Казахстан об административных правонарушениях от 5 июля 2014 года (*с* изменениями и дополнениями *по состоянию на 09.01.2018 г.*).
5. Закон Республики Казахстан от 24 ноября 2015 года «Об информатизации».
6. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».
7. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 66 «Об утверждении Правил проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов
информатизации «электронного правительства».
8. Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»).

Сергеев Сергей Александрович
Лауазымы: құқықтану магистрі, Қазақ инновациялық гуманитарлық-заң университеті қылмыстық-құқықтық пәндер кафедрасының аға оқытушысы
Пошталық мекен-жайы: 071400, Қазақстан Республикасы, Семей қ., Қозбағаров, 7 үй, 28 пәтер
Байланыс тел: + 7 777 997 29 36
Кибер қауіпсіздікті қамтамасыз ету мәселелерін алдын алу бойынша Қазақстан Республикасының құқықтық саясаты

Сергеев Сергей Александрович
Должность: магистр юриспруденции, старший преподаватель кафедры уголовно-правовых дисциплин Казахского гуманитарно-юридического инновационного университета
Почтовый адрес: 071400, Республика Казахстан, г. Семей, ул. Козбагарова, д.7 кв.28
сот. тел: + 7 777 997 29 36
Правовая политика Республики Казахстан по преодолению проблем обеспечения кибербезопасности

Sergeyev Sergey Aleksandrovich
Position: Master of law, Senior Lecturer Chair of Criminal Law Disciplines of the Kazakh Humanitarian Juridical Innovative University
Mailing address: 071400, Republic of Kazakhstan, Semey, st. Kozbagarova 7, f.28
Mob.phone: + 7 777 997 29 36
Legal policy of the Republic of Kazakhstan to overcome the problems of cybersecurity