ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ
Халықаралық қатынастар факультеті
Халықаралық құқық кафедрасы

Қазақстан Республикасы Тәуелсіздігінің 30 жылдығына арналған

«ТӘУЕЛСІЗ ҚАЗАҚСТАН: ТАРИХ ЖӘНЕ ҚАЗІРГІ ЗАМАН»
атты халықаралық студенттер мен жас ғалымдардың
ғылыми-практикалық конференциясының

МАТЕРИАЛДАРЫ

Алматы, 15 *желтоқсан 2021 ж.*

МАТЕРИАЛЫ

Международной научно-практической конференции
студентов и молодых ученых

«НЕЗАВИСИМЫЙ КАЗАХСТАН: ИСТОРИЯ И СОВРЕМЕННОСТЬ»

посвященной 30-летию Независимости Республики Казахстан

Алматы, 15 *декабря* 2021 г.

MATERIALS

International Scientific and Practical Conference
of Students and Young Scientists

«INDEPENDENT KAZAKHSTAN: HISTORY AND MODERNITY»

dedicated to the 30th anniversary of Independence
of the Republic of Kazakhstan.

Almaty, December 15, 2021

Алматы
2021

ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ
Халықаралық қатынастар факультеті
Халықаралық құқық кафедрасы

Қазақстан Республикасы Тәуелсіздігінің 30 жылдығына арналған

«ТӘУЕЛСІЗ ҚАЗАҚСТАН: ТАРИХ ЖӘНЕ ҚАЗІРГІ ЗАМАН»
атты халықаралық студенттер мен жас ғалымдардың ғылыми-практикалық конференциясының

МАТЕРИАЛДАРЫ

Алматы, 15 желтоқсан 2021 ж.

МАТЕРИАЛЫ

Международной научно-практической конференции студентов и молодых ученых

«НЕЗАВИСИМЫЙ КАЗАХСТАН: ИСТОРИЯ И СОВРЕМЕННОСТЬ»

посвященной 30-летию Независимости Республики Казахстан

Алматы, 15 декабря 2021 г.

MATERIALS

International Scientific and Practical Conference of Students and Young Scientists

«INDEPENDENT KAZAKHSTAN: HISTORY AND MODERNITY»

dedicated to the 30th anniversary of Independence
of the Republic of Kazakhstan.

Almaty, December 15, 2021

Алматы
«Қазақ университеті»

2021

«**Независимый Казахстан: история и современность**»: Материалы Международной научно- практической конференции студентов и молодых ученых, посвященной 30-летию Независимости Республики Казахстан 15 декабря 2021 г. / под общ. ред. к.ю.н., доцента Ж.Т. Сайрамбаевой. – Алматы:Изд-во LEM, 2021. – 272 с.

ISBN 978-601-04-5839-0

В настоящем сборнике представлены материалы Международной научно-практической конференции студентов и молодых ученых, посвященной 30-летию Независимости Республики Казахстан. В рамках конференции обсуждаются достижения Казахстана за годы независисмости и перспективы его дальнейшего развития.

Материалы конференции опубликованы в редакции авторов.

ISBN 978-601-04-5839-0

Бисалиев М.С.
докторант 1-го курса, специальность
«международное право» КазНУ им. аль-Фараби
Научный руководитель: Шакиров К.Н.
д.ю.н., профессор кафедры международного права,
КазНУ им. аль-Фараби.

КОНЦЕПЦИЯ КИБЕРБЕЗОПАСНОСТИ РЕСПУБЛИКИ КАЗАХСТАН КАК ПРИМЕР УСПЕШНОЙ МОДЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗА 30 ЛЕТ НЕЗАВИСИМОСТИ РЕСПУБЛИКИ КАЗАХСТАН.

Одной из важнейших предпосылок возникновения института защиты персональных данных в условиях информационного общества служит естественная потребность каждого индивида обеспечить неприкосновенность своей частной жизни и самостоятельно регулировать процессы движения информации личного характера, а также иметь возможности контролировать ее распространение.

В этом плане в нашей стране принята Концепция кибербезопасности Республики Казахстан «Киберщит Казахстана» от 30 июня 2017 года [1], которую возможно рассматривать в качестве типичного и удачного примера модели обеспечения информационной безопасности. При этом необходимо отметить, что принятая Концепция не является единственным и тем более самостоятельным нормативным документом. Формально она была принята на основании Послания Президента Республики Казахстан Н. Назарбаева «Третья модернизация Казахстана: Глобальная конкурентоспособность» от 31 января 2017 года [2]. В этом смысле цели Концепции достаточно широки, несмотря на то что именно обеспечение безопасности личной информации не указано в ее вводных положениях в качестве самостоятельной цели.

Между тем, очевидно, что такая цель подразумевается, поскольку речь в документе идет о формировании государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, а также обеспечения безопасного использования информационно-коммуникационных технологий. Такой подход отразился и на используемой в Концепции терминологии. Например, Концепция кибербезопасности предлагает считать «состояние защищенности информации в электронной форме и среды ее обработки, хранения, передачи (электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры) от внешних и внутренних угроз, то есть информационная безопасность в сфере информатизации». Хотя само по себе изложение приведённой терминологии вполне полноценно, тем не менее она не совсем правильно определяет неизвестное через неизвестное. Концепция указывает лишь на некие «атрибуты модели информационной безопасности», хотя, скорее всего, речь идет о требованиях и характеристиках. В качестве одного из таких атрибутов названа конфиденциальность.

По мнению разработчиков Концепции, «конфиденциальность информации означает, что с ней может ознакомиться только строго ограниченный круг лиц, определенный ее владельцем», а вот «если доступ к информации получает неуполномоченное лицо, происходят

несанкционированный доступ или нарушение конфиденциальности». Разумеется, точнее было бы прописать, что конфиденциальность — это право обладателей информации определять ее судьбу в виде недоступности или доступности третьим лицам, а полученное от обладателя информации право каких-либо лиц на ознакомление с этой информацией — уже право ее нового обладателя устанавливать доступ к информационному ресурсу.

Тем не менее, в Концепции верно отмечается, что требование о конфиденциальности информации — одно из наиболее важных для персональных данных ограниченного доступа, например, сведения о бенефициарах банковской, страховой и медицинской деятельности.

Помимо конфиденциальности в отношении персональных данных, также важна и доступность такого рода информации, которую Концепция достаточно смело определяет «способностью информационной системы предоставлять своевременный беспрепятственный доступ к информации субъектам, обладающим соответствующими полномочиями». Однако, в данном случае, на мой взгляд, речь можно вести о качестве, скорости и иных характеристиках доступа к персональным данным, а не об их доступности.

Необходимое внимание в Концепции также уделено аутентичности и апеллируемости, хотя это явно не самые значимые свойства для информации в виде персональных данных. Концепция рассматривает угрозу информационной безопасности достаточно широко – как любое потенциально возможное: 1) событие, 2) процесс или 3) явление, которые посредством воздействия на информацию или компоненты информационной системы или ресурса могут прямо или косвенно привести к нанесению ущерба интересам владельцев и пользователей. Такого рода определение представляется нам слишком широким. В нем угроза, по существу, сводится к категории риска. Также непонятно, почему на информацию (наверное, все-таки, на информационный ресурс или информационную систему) воздействуют именно события, процессы и явления. Скорее мы видим, что на информацию воздействуют люди, их действия (правомерные или неправомерные волевые акты), а также операции как совокупности таких действий.

Концепция среди наиболее распространенных угроз информационной безопасности выделяет как технические векторы (программные и программно-аппаратные), так и векторы со стороны человеческих ресурсов (как внутренних, так и внешних), причем как неумышленные, так и преднамеренные. Интересным моментом является признание того факта, что у собственников (так называет обладателей информации Концепция), владельцев и пользователей не только права, но и обязанности по соблюдению по их защите.

Защита персональных данных отмечается как особая, самостоятельная задача (цель) государственных органов и других субъектов по обеспечению информационной безопасности в области информатизации. Разработчики Концепции увязывают такого рода деятельность также с исполнением норм Закона Республики Казахстан № 527-IV от 06.01.2012 года «О национальной безопасности» [3] и Законом Республики Казахстан № 94-V от 21.05.2013 года «О персональных данных и их защите» [4].

Вместе с тем, в Концепции, к сожалению, основное внимание по линии государственного мониторинга вопросов информационной безопасности уделяется лишь вопросам безопасности деятельности критически важных объектов инфраструктуры, но не защите личной информации. Также не затронуты вопросы защиты персональных данных юридических лиц, где требуется четкое разграничение данных, относящиеся непосредственно к юридическим лицам, и данные о бенефициарах и акционерах юридических лиц. Требования по безопасности финансовых информационных систем обеспечиваются лишь подзаконными правовыми актами Национального Банка Республики Казахстан [5] и Агентства Республики Казахстан по регулированию и развитию финансового рынка с учетом отраслевых и международных требований по обеспечению безопасности информационных систем [6-7].

В Концепции провозглашена приверженность международно-правовому принципу неприкосновенности частной жизни в том числе в сфере персональной информации, хотя, одновременно и указывается, что сам по себе термин «кибербезопасность» и его производные (киберпространство, киберзащита, кибератаки, кибернападение и другие) не имеют единого

общепризнанного юридического определения на международном уровне. Наибольшее внимание разработчиками Концепции было уделено исследованию зарубежного опыта в области обеспечения согласованных действий органов власти, уполномоченных на соответствующее правовое регулирование или правоприменение.

Надо отметить, что принятый в ряде государств «информационный» подход к формированию системы защиты личной информации не всегда и не в полной мере соответствует нормам международного права; постулируя защиту, главным образом, не частного, а государственного (публичного) интереса. Такой подход не обладает необходимой универсальностью; в ряде случаев нормативные акты не конкретны и декларативны; характеризуется отсутствием процессуальных и процедурных норм в целях своей реализации; как правило, не устанавливает персональные данные в виде особого предмета и объекта правовой охраны. Вместе с тем, такой рода подход отличается разработанностью отдельных норм и институтов; представляет собой относительно стройную систему инструментов правового регулирования, начиная с концепций и заканчивая проблематикой защиты личной информации в конкретной среде; разрешает многие вопросы взаимодействия в сфере защиты персональной информации между субъектами публичного права [8].

Необходимо отметить, что цели и задачи Концепции определены в достаточно общем виде и сводятся к повышению уровня защищенности информационных систем и ресурсов как правовыми, так и технологическими средствами. При этом совершенно четко указаны ожидаемые от реализации Концепции результаты, в том числе, выраженные в однозначной количественной форме. Одним из примеров является глобальный индекс кибербезопасности Казахстана. Индекс кибербезопасности был разработан Международным союзом электросвязи в 2015 году и объединяет 82 вопроса об обязательствах государств-членов в области кибербезопасности по пяти основным направлениям: 1) правовые меры, 2) технические меры, 3) организационные меры, 4) меры по развитию потенциала, 5) меры сотрудничества. Так, согласно отчету Международного союза электросвязи о глобальном индексе кибербезопасности 2017 года, Республика Казахстан была на 83 месте [9], а в отчете 2020 года индекс Республики поднялся до 31 места [10].

Защита прав и охраняемых законом интересов субъекта персональных данных, учет потребностей иных участников исследуемых правоотношений при сборе и накоплении, хранении и обработке, передаче и предоставлении персональных данных требует работы с большим массивом самой разнообразной информации, что невозможно без широкого применения технических и правовых средств. Однако, с учетом требований по обеспечению безопасности такого особого информационного продукта как персональные данные, находящиеся в обороте в киберпространства, можно выделить средства, так или иначе связанные с техническими, математическими или иными физическими характеристиками как объекта а, так и средства защиты.

Административный порядок предусматривает создание национальной системы органов, в задачи которых входят вопросы охраны персональных данных в сети Интернет, либо выделение специально на то уполномоченного органа. Так, в большинстве государств обычно имеется «общий» надзорный орган (как правило, это институт прокуратуры) и специально на то уполномоченные органы (например, Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан) [11]. Эти органы обладают возможностью принимать как административные меры (меры прокурорского реагирования у органов прокуратуры, запреты и привлечение к административной ответственности у иных контролирующих органов и проч.), так и обращаться в суд в защиту прав субъекта персональных данных.

Нельзя не учитывать, что совершенствование информационных технологий и потребности современного общества делают необходимой автоматизированную обработку значительных по объему массивов персональных данных. Формируемые государственными органами и коммерческими организациями базы персональных данных становятся специфическим объектом преступных посягательств в сфере информационной безопасности

личности. В связи с развитием цифровизации и усилением законодательства в области защиты персональных данных увеличивается и количество прецедентов их нарушения.

(см. График 1).

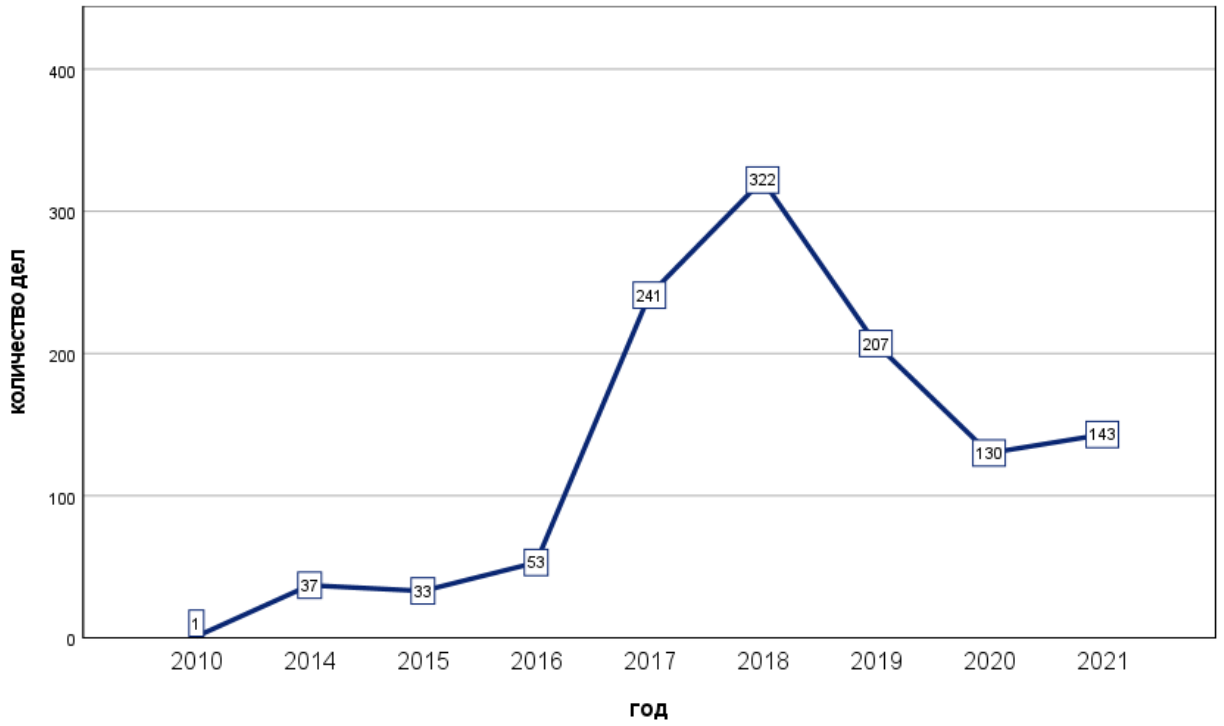

График 1 — Тенденция роста и спада количества гражданских дел по Республике Казахста по запросу о защите персональных данных в период 2010 по 2021 гг.

По состоянию на декабрь 2021 года в Банке судебных актов [12] содержится 1 167 судебных дел по запросу «персональные данные» по гражданским делам, фабулы дел которых содержат нарушения и признаки нарушений законодательства Республики Казахстан о персональных данных и их защите, более того, некоторые дела квалифицированы как уголовные преступления. Среднее количество процессов в год составляет 130 единиц, однако, с 2017 года тренд начинает быть отрицательным. Это может быть обусловлено усилением законодательства в области регулирования сбора и обработки персональных данных.

Заключение

Государственный подход к стратегическому обеспечению кибербезопасности Казахстана должен стать определяющим в условиях обсуждения проблем становления цифрового общества. Естественно, что разработке собственной Стратегии должна предшествовать выработка Концепции стратегической безопасности с учётом определение основных приоритетов государства и граждан в данной области. Всё, что необходимо для решение этих задач это обоснованное определение предмета и объекта научного исследования, приобретение требуемого технологического обеспечения, выбор надлежащей методологии обеспечения кибербезопасности, подбор профессиональных управленческих и экспертных кадров. Все эти составляющие в целом почти достигнуты в стране, а другие, пока ещё недоработанные на законодательном уровне, вполне достижимы при условии более чёткого выбора государством приоритета в столь важном для страны направлении. В этом плане более внимательный подход государства к защите персональных данных в нормативном регулировании правоотношений, в том числе и при принятии Концепции кибербезопасности страны, позволит на должном уровне обеспечить законные права и интересы граждан с учётом внедрения в стране современных информационных технологий.