conduct of the elections, as well as within one month from the voting day, must be considered within five days. The statement, received less than five days before the election, on the voting day and before the announcement of the election results –must be considered immediately. An application to appeal the decision of the election commission on the need for correction in the voter lists (electors) must be considered on the day of receipt.

To this end, the courts, prosecutors and election commissions organize their work during the electoral process, including weekends and elections day, in such a way as to ensure that complaints are received and considered within the time limits established by law. During the preparation and conduct of elections, shifts are organized in all local courts.

It should be noted that the norms of the new Civil Procedure Code, enacted on January 1, 2016, and the amendments to the Law "On Elections in the Republic of Kazakhstan", significantly changed the division of jurisdiction of cases, the establishment of the procedure and deadlines for appealing decisions on electoral cases.

By and large, the proceedings in the court regarding applications for the protection of the electoral rights of citizens and public associations participating in elections are governed by chapter 27 of Code of Civil Procedure (special action proceedings). Thus, in accordance with Art. 286 CCP, citizen, public association, member of the election commission, agents of candidates and political parties, representatives of political parties with an advisory vote, observers of political parties, other public associations, non-profit organizations, which consider that a decision, action (inaction) of a state body, body of local government, election commission, enterprise, organization or their officials violate the right to elect or to be elected, to participate in elections, a referendum, have the right to make a written application to the court of competent jurisdiction.

The application is considered by the court with the participation of an applicant, a representative of the relevant election commission or a state body, a body of local government, an enterprise, an organization, a prosecutor, but their non-appearance with proper notification is not an obstacle to the resolution of the case.

Bibliography:

1. The Constitutional Law On Elections in the Republic of Kazakhstan of September 28, 1995 // https://online.zakon.kz/document/?doc_id=1004029

2. Federal Law "On the Election of Deputies of the State Duma of the Federal Assembly of the Russian Federation" of February 22, 2014 // http://base.garant.ru/70595878/

3. The electoral system of the Republic of Kazakhstan. The official website of the Central Election Commission of the Republic of Kazakhstan // https://www.election.gov.kz/rus/izbiratelnaya-sistema-rk/kratkaya-informatsiya-ob-izbiratelnoy-sisteme-rk.php

ПРАВО НА ИНФОРМАЦИЮ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Старожилова Н.П., старший преподаватель КарГУ имени Е.А. Букетова
Аманбекова А., студент 1 курса юридического факультета

В середине XX в. возникла проблема конкурентной борьбы за владение и способы передачи информации, на первый план вышла необходимость защиты и охраны информации, предотвращение несанкционированного ее использования. Постепенное осознание самой информации как объекта обработки и потребления способствовало постановке вопроса о праве на информацию, введении права на информацию в состав прав человека и гражданина в международных правовых актах и в национальном законодательстве государств.

Право на информацию в современном обществе является одним из важных гражданских прав человека. Оно нашло закрепление в статье 19 Всеобщей декларации прав человека, в статье 19 Международного Пакта о гражданских и политических правах человека. В Конституции Республики Казахстан право на информацию закреплено и выражено в двух статьях: в статье 20 и в пункте 3 статьи 18[1]. Анализ указанных статей в названных документах позволяет выделить в содержании данного права следующие элементы: 1) свободно искать, получать и распространять информацию; 2) использовать любые формы и способы выражения по своему выбору;3) это право не зависит от

государственных границ; 3) если какая-либо информация затрагивает права и интересы гражданина, то государственные органы, должностные лица и СМИ обязаны предоставить ему возможность ознакомиться с документами, решениями и указать источники такой информации (при условии, что речь идет о законных правах и интересах человека); 4) допускается возможность законного ограничения этого права в целях недопущения нарушения прав, интересов и репутации других лиц, обеспечения государственной безопасности, охраны общественного порядка, здоровья и нравственности народа. Например, в решении Европейского суда по правам человека по этому поводу сказано, что «плюрализм и демократия основаны на компромиссе и требуют от людей и социальных групп различных уступок, чтобы гарантировать права всему обществу в целом»[2].

В эпоху глобализации обеспечение информационной безопасности приобретает все более важное значение для системы обеспечения национальной безопасности. Это обусловлено значительным прогрессом в развитии информационно-коммуникационных технологий и средств, а также огромным масштабом информационного пространства.Информационная безопасность осознается как социально значимая проблема по мере развития общества, смены технологической основы связи, передачи и использования информации. Приобретение опыта, знаний, передача их новым поколениям, охрана от соперников и врагов в борьбе за жизнь сопровождают всю историю человека и разных форм его ассоциаций (род, племя, семья; секреты производства, обмена, торговли, различных видов государственной власти). Информация сегодня является важнейшим ресурсом, имеющим такаю же большую ценность, как природные финансовые, трудовые и иные ресурсы. Информация стала товаром, который продается и покупается. Информация превратилась в оружие, возникают и прекращаются информационные войны.

Международная информационная безопасность является одним из элементов системы международной безопасности. Однако, в современном информационном законодательстве Казахстана определения термина «информация» нет. Недостатки в терминологии отражаются на качестве законодательной техники. Отсутствует определение понятия «информация» и в Законе РК «О средствах массовой информации» [3]. Используется термин «данные» применительно к персональным данным как к виду электронных информационных ресурсов (статья 36). Анализ действующего законодательства Республики Казахстан позволяет выделить следующие виды. Массовая информация — «предназначенные для неограниченного круга лиц печатные, аудио-сообщения, аудиовизуальные и иные сообщения и материалы» (Закон РК «О средствах массовой информации»); информация о гражданах (персональные данные) — «сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе» (ст. 1 Закона РК «О персональных данных и их защите» [4]), «информация об управлении правами - информация, которая идентифицирует произведение, автора произведения, исполнителя, исполнение исполнителя, производителя фонограммы, фонограмму, обладателя какого-либо права на произведение, исполнение или фонограмму либо информацию об условиях использования произведения, исполнения или фонограммы. Под информацией об управлении правами также понимаются любые цифры или коды, в которых предоставлена такая информация, когда любой из этих элементов информации приложен к экземпляру произведения, записанного исполнения или фонограммы либо появляется в связи с сообщением произведения или сообщением и (или) доведением записанного исполнения или фонограммы для всеобщего сведения» (ст. 1 Закона РК «Об авторском праве и смежных правах»); электронные информационные ресурсы ограниченного доступа (конфиденциальная информация) - электронные информационные ресурсы, содержащие сведения, доступ к которым ограничен законами Республики Казахстан либо их собственником или владельцем (ст. 32 Закона РК «Об информатизации») [5]; государственная тайна — «защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права» (ст. 1 Закона РК «О государственных секретах»); реклама — «реклама - распространяемая и размещаемая в любой форме с помощью любых средств информация, предназначенная для неопределенного круга лиц и призванная формировать или поддерживать интерес к физическому или юридическому лицу, товарам, товарным знакам, работам, услугам и способствовать их реализации» (ст. 1 Закона РК «О рекламе»).

Сравнительный анализ законодательства об информатизации и о национальной безопасности показал, что действующие законы не содержат положений о соотношении угроз информационной

безопасности и их источников. В Законе «Об информатизации» отсутствуют нормы, перечисляющие виды угроз и источников информационной безопасности. Из содержания рассмотренных правовых актов не ясно в чем различие между угрозами и источниками угроз. Считаем, что при подготовке проекта Кодекса об информатизации в части определения угроз и их источников для информационной безопасности можно имплементировать положения Соглашения ШОС.

Информация о личной, индивидуальной или семейной жизни человека также обладает особой ценностью. В соответствии со статьей 18 Конституции Республики Казахстан закреплено, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства. Из содержания этой статьи следует, что к такой информации относятся следующие данные: личная и семейная тайна, сведения о личных вкладах и сбережениях, переписка, телефонные переговоры, почтовые, телеграфные и иные сообщения.

Копылов В.А. выделяет три основных направления правового обеспечения информационной безопасности:

1. защита чести, достоинства, деловой репутации от угроз воздействия вредной, опасной, недоброкачественной, недостоверной информации, нарушение порядка распространения информации;

2. защита информации и информационных ресурсов ограниченного доступа от угроз несанкционированного и неправомерного воздействия посторонних лиц;

3. защита информационных прав и свобод личности на передачу и использование информации в условиях информатизации [6 с.240]

В Великобритании, например, проблемам правового обеспечения безопасности персональных данных стали уделять внимание еще в восьмидесятых годах прошлого века. В этой стране правовое регулирование неприкосновенности частной жизни и персональных данных осуществляется на национальном и универсальном уровнях. Великобритания ратифицировала Конвенцию «О защите частных лиц в отношении автоматизированной обработки персональных данных» 1981 года. Эта страна также выполняет требования Директивы ОЭСР «О защите неприкосновенности частной жизни и международных обменов персональными данными» от 23 сентября 1980 года. К основным правовым актам национального характера относятся Закон о защите данных 1998 года [7], Закон о свободе информации 2000 года. Под «данными» в Законе о защите данных понимается информация, которая обрабатывается и записывается с помощью автоматизированного оборудования и является частью системы или записью, находящегося в распоряжении государственного органа. Стоит отметить один недостаток этой формулировки. Данные могут находиться не только в распоряжении и пользовании государственного органа [8 с.72]. Очень часто такими данными обладают частные лица и организации, которые предоставляют какие-либо услуги, например, коммунальные, услуги связи. Этот же закон, например, делает различия между понятиями «конфиденциальные персональные данные» и «персональные данные». К конфиденциальным персональным данным относится информация о расовом иди этническом происхождении субъекта данных, о политических взглядах, о религиозных убеждениях, о членстве в профсоюзах, о физическом или психическом здоровье человека, о совершенных правонарушениях. Основным субъектом обеспечения конфиденциальности персональных данных является контролер данных – лицо, которое определяет цели и средства обработки персональных данных. Персональные данные могут обрабатываться и использоваться только в законных целях, которые определил контролер.

Согласно классическому определению, которое дается в международном стандарте ISO/IEC 27001 и которое применяется в специализированной научной литературе, информационная безопасность включает в себя три части:

- конфиденциальность – обеспечение доступности информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи);

- целостность – обеспечение точности и полноты информации, а также методов ее обработки;

- доступность – обеспечение доступа к информации авторизированным пользователям, когда это необходимо (по требованию).

В Концепции информационной безопасности Республики Казахстан сформулировано определение: «Информационная безопасность страны рассматривается в двух взаимосвязанных аспектах: техническом и социально-политическом. Технический аспект подразумевает обеспечение защиты национальных информационных ресурсов, информационных систем, информационно-телекоммуникационной инфраструктуры от неавторизованного доступа, использования, раскрытия, нарушения, изменения, прочтения, проверки, записи или уничтожения для обеспечения целостности, конфиденциальности и доступности информации. Социально-политический аспект заключается в

защите национального информационного пространства и систем распространения массовой информации от целенаправленного негативного информационного и организационного воздействия, могущего причинить ущерб национальным интересам Республики Казахстан».

Нарушениями информационной безопасности, согласно положениям Конвенции «Об обеспечении международной информационной безопасности», являются: неправомерное использование информационных ресурсов, несанкционированное вмешательство в информационные ресурсы, терроризм в информационном пространстве, использование информационных технологий и средств для осуществления враждебных действий и актов агрессии, целенаправленное деструктивное воздействие в информационном пространстве на критически важные структуры другого государства, неправомерное использование информационных ресурсов другого государства без согласования с государством, винформационном пространстве которого располагаются эти ресурсы, действия в информационном пространстве с целью подрыва политической, экономической и социальной систем другого государства, психологическая обработка населения, дестабилизирующая общество, использование международного информационного пространства государственными и негосударственными структурами, организациями, группами и отдельными лицами в террористических, экстремистских и иных преступных целях, трансграничное распространение информации, противоречащей принципам и нормам международного права, а также национальным законодательствам государств, использование информационной инфраструктуры для распространения информации, разжигающей межнациональную, межрасовую и межконфессиональную вражду, расистских и ксенофобских письменных материалов, изображений или любого другого представления идей или теорий, которые пропагандируют, способствуют или подстрекают к ненависти, дискриминации или насилиюпротив любой личности или группы лиц, если в качестве предлога к этому используются факторы, основанные на расе, цвете кожи, национальном или этническом происхождении, а также религии, манипулирование информационными потоками в информационном пространстве других государств, дезинформация и сокрытие информации с целью искажения психологической и духовной среды общества, эрозия традиционных культурных, нравственных, этических и эстетических ценностей, использование информационно-коммуникационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационном пространстве, противодействие доступу к новейшим информационно-коммуникационным технологиям, создание условий технологической зависимости в сфере информатизации в ущерб другим государствам, информационная экспансия, приобретения контроля над национальными информационными ресурсами другого государства.

По нашему мнению, конституционной основой правового обеспечения информационной безопасности является пункт 3 статьи 20 Конституции РК, который гласит: «Не допускается пропаганда или агитация насильственного изменения конституционного строя, нарушения целостности Республики, подрыва безопасности государства, войны, социального, расового, национального, религиозного, сословного и родового превосходства, а также культа жестокости и насилия»[1].

Одним из важнейших нормативных правовых актов, направленных на реализацию информационной безопасности, является Закон РК «О средствах массовой информации» от 23 июля 1999 г. Новым пунктом дополнен перечень оснований, по которым можно приостановить деятельность СМИ, закрепленный в пункте 3 статьи 13 Закона. Теперь факты нарушения авторских и смежных прав в сети Интернет могут стать основаниями для вынесения решения о приостановлении деятельности СМИ. К ряду других оснований относятся: разглашение сведений, составляющих государственные секреты или иную охраняемую законом тайну, распространение информации, раскрывающей технические приемы и тактику антитеррористических операций в период их проведения, пропаганда наркотических средств, психотропных веществ и прекурсоров, пропаганда и агитация культа жестокости и насилия, социального, расового, национального, религиозного, сословного и родового превосходства, распространение радио-, телепрограмм, а также демонстрация вино- и видеопродукции порнографического и специального сексуально-эротического характера, использование средства массовой информации в целях нарушения условий проведения предвыборной агитации, осуществления иностранцами, лицами без гражданства, иностранными юридическими лицами и международными организациями деятельности, препятствующей и (или) способствующей выдвижению и избранию кандидатов, политических партий, выдвинувших партийный список, достижению определенного результата на выборах, проведения агитации в период ее запрещения, принуждения к участию или отказу от участия в забастовке, нарушения

законодательства Республики Казахстан о порядке организации и проведения мирных собраний, митингов, шествий, пикетов и демонстраций.

Кроме этого статья 7 перечисляет виды ненадлежащей рекламы, к которым отнесены недобросовестная реклама, недостоверная реклама, неэтичная реклама. Статья 15 особо посвящена защите интересов несовершеннолетних при размещении рекламы от злоупотребления их доверием и отсутствием у них опыта. Поэтому в такой рекламе не допускаются: дискредитация авторитета родителей, подрыв доверия к ним несовершеннолетних; приуменьшение необходимого уровня навыков использования продукции у несовершеннолетних, за исключением случаев, когда результаты использования продукции показаны или описаны; создание у несовершеннолетних нереального (искаженного) представления о стоимости (цене) продукции для несовершеннолетних, а также прямое или косвенное указание на то, что рекламируемая продукция доступна для любого семейного бюджета.

Информация, содержащая данные о личной, индивидуальной или семейной жизни человека, также обладает большой ценностью. Однако, в условиях Интернета часто совершаются правонарушения, связанные с использованием персональных данных, не соответствующим целям операторами данных. Например, поисковые системы собирают информацию обо всех действиях своих пользователей, осуществляемых в Интернете, без их согласия, и в дальнейшем эту информацию используют для рассылки рекламы или предоставления дополнительных услуг. Свои действия поисковые системы объясняют тем, что информация о совершаемых действиях пользователей не относится к персональным данным. Такие действия операторами поисковых систем совершаются практически во всех странах. Поэтому актуальным становится вопрос о понятии персональных данных. Так, Закон Великобритании о защите данных 1998 года определяет их как «любые данные, которые относятся к живому человеку и на основании которых этот человек может быть идентифицирован, или информацию, которая находится в распоряжении контролера данных или может поступать к нему для обработки, в том числе любые выражения мнения об индивидуальных особенностях человека или его личности (ч.1 статьи 1) [7]. Закон о свободе информации 2000 года к персональным данным причисляет также любой запрос информационного характера, в котором содержится информация о субъекте персональных данных (п.40 ч.2). Аналогичные признаки персональных данных содержит и Закон РФ «О персональных данных» от 27 июля 2006 года.

Статья 1 Закона РК «О персональных данных» определяет их как сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе. Полагаем, что данная формулировка требует уточнения и дополнения применительно к целевому использованию персональных данных, а именно: сведения, на основании которых физическое лицо может быть идентифицировано, в том числе любые выражения мнения об индивидуальных особенностях субъекта».С января 2016 г. вступили в силу изменения в Закон «О персональных данных», предусматривающие, что запись, накопление и хранение персональных данных казахстанцев разрешаются только на территории Республики Казахстан. Принятие указанных актов свидетельствует об особом внимании к качеству программного обеспечения парка ИКТ Казахстана с учетом того, что Интернет-среда все более насыщается информацией, опасной для человека и используемой в целях массового поражения. Жатканбаева А.Е. отмечает, что «проблема обеспечения конфиденциальности сведений о личности является очень актуальной и болезненной. Так, например, в МВД РК создана единая компьютерная база со всей необходимой информацией о всех гражданах Республики Казахстан, ставится задача всеобщей дактилоскопии… Минздрав готов создать свою базу данных о здоровье всех и каждого в Казахстане…, но «наибольших успехов» добилось министерство финансов, присвоив каждому гражданину ИНН, зная который можно получить практически любую информацию о человеке» [9 с.144].

Планирование и реализация внешних информационных угроз продолжаются и сегодня. Достаточно просмотра новостей в Интернете. Планируется деятельность в таких социальных сетях, как Facebook, Twitter, «В контакте» и «Одноклассники». США увеличивают расходы на информационную пропаганду. Как заявил заместитель помощника Госсекретаря США по делам Европы и Евразии Зифф на слушаниях в Сенатском комитете по иностранным делам Конгресса США, расход на эти цели предусматривает рост на 86 млн долларов. Как отмечает Мовкебаева Г.А., военные операции в кибепространстве, доктринальные разработки ведения информационной войны в США начались после ведения войны в Персидском заливе [10 с.238]. Для этого в США создано Командование совместных информационных операций. Информационная операция – это комплекс

мероприятий по манипулированию информацией в целях достижения и удержания всеобъемлющего превосходства над противником посредством воздействия на информационные процессы, происходящие в системах управления.

В настоящее время особенно важной является проблема защиты интересов детей в Интернете. Причиной этому стали с участившиеся случаи интернет-мошенничества, вовлечения подростков в совершение преступлений и склонения их к суицидам. Это явление уже получило свое название, которое пришло из английского языка – кибербуллинг. Так называется одна из форм психологического воздействия, травли, запугивания, насилия подростков и младших детей при помощи информационно-коммуникационных технологий, а именно Интернета и мобильных телефонов. Этот вид терроризма в виртуальном пространстве имеет разные формы проявления. Первая стадия воздействия – шутки, насмешки. На более тяжелых стадиях – сильное психологическое влияние, приводящее к суицидам и смертям. Сегодня по всей территории СНГ активно распространяются интернет-игры «Синий кит» и «Тихий дом», в которые втягивают подростков. Участники групп в социальной сети «ВКонтакте» ведут игру на протяжении 50 дней, всего 50 этапов. По утверждениям экспертов на конечной стадии игры - суицид - игрок (подросток) должен покончить жизнь самоубийством. По данным СМИ, с ноября 2015-го по апрель 2016-го года покончили с собой более 120 подростков, которые почти все были участниками одних и тех же групп смерти в социальных сетях [11 с.41; 12].

В связи с нарастающим глобальным процессом активного формирования и широкомасштабного использования информационных ресурсов особое значение приобретает информационная безопасность детей. Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию. Обеспечение государством информационной безопасности детей, защита физического, умственного и нравственного развития несовершеннолетних, а также человеческого достоинства во всех аудиовизуальных медиа-услугах и электронных СМИ – требование международного права. Международные стандарты в области информационной безопасности детей пока не нашли отражение в казахстанском законодательстве.

Кроме этого, появился новый вид бизнеса – так называемые информационные брокеры, лица, которые ведут сбор и обобщение информации о пользователях, которую они оставляют в общем свободном доступе. Эта информация продается компаниями, которые ее используют по своему усмотрению. Все мы сталкиваемся с такой практикой в условиях Интернета, когда сайтами совершаются действия, связанные с обработкой наших персональных данных, не соответствующих целям, заявленным оператором персональных данных, законодательству. Например, поисковые системы собирают информацию обо всех действиях своих пользователей в Интернете без их согласия (какие сайты посещаются чаще всего, чем интересуется пользователь). В дальнейшем эта информация используется для рассылки рекламы или предоставления дополнительных платных услуг.

Террористические преступления также совершаются с использованием информационных технологий. Сегодня все новые угрозы несут в себе возможности использования киберпространства террористическими организациями и различными экстремистскими группировками, осуществляющими через Всемирную сеть вербовку новых членов, в том числе в молодежной среде. Так, в Нормативном постановлении Верховного Суда Республики Казахстан от 8 декабря 2017 года №11 «О некоторых вопросах судебной практики по применению законодательства о террористических и экстремистских преступлениях» сказано, способ распространения не имеет значения для квалификации данных преступлений, что под пропагандой терроризма следует понимать распространение любым способом материалов или информации, содержащих идеологию насилия и практику терроризма, посредством воздействия на сознание и волю человека (людей) с целью возбуждения в нем (них) стремления к осуществлению террористической деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности. Публичные призывы к осуществлению акта терроризма включают в себя использование средств массовой информации или сетей телекоммуникаций (периодического печатного издания, теле-радиоканала, интернет-ресурсов и других средств) [13].

Рост уровня доступности глобальной сети Интернет неизбежно приводит к увеличению числа инцидентов информационной безопасности. Лаборатория KasperskySecurityNetwork сообщает сведения, что 85% интернет атак в Центральной Азии приходится на Казахстан. Для сравнения: на Узбекистан приходится 8%, на Кыргызстан 4%, на Туркменистан 2%, на Таджикистан 1%[3]. Если

раньше крупным кибеаратакам подвергались в основном правительственные сайты, причем их рост шел одновременно с ростом цифровизации управления. То в последнее время значительно выросла угроза со стороны кибератак в отношении крупного бизнеса. Источником угрозы информационной безопасности для систем государственного управления и социальной стабильности в стране является также утрата данных национальных и государственных информационных систем.

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, использование форм общественного контроля деятельности центральных органов государственной власти и местных органов государственной власти Республики Казахстан.

1 В Конституции Республики Казахстан право на информацию имеет различную субъектную принадлежность. При формулировке права на поиск, получение и распространение информации используется слово «каждый» (и гражданин РК, и иностранец). Требовать от государственных органов и должностных лиц предоставления информации, затрагивающей права и интересы, могут только граждане. В редакцию п.3 статьи 18 Конституции необходимо внести изменения и заменить слово «гражданин» на слово «каждый».

2 Накопленный массив нормативных правовых актов в сфере информационного права, возросшая в современном обществе роль информационных ресурсов, необходимость защиты информации и обеспечения информационной безопасности государства требуют систематизации и качественного правового обеспечения. Все это обусловливает необходимость принятия Кодекса Республики Казахстан «Об информатизации».

3 Сравнительный анализ законодательства об информатизации и о национальной безопасности показал, что действующие законы не содержат положений о соотношении угроз информационной безопасности и их источников. В Законе «Об информатизации» отсутствуют нормы, перечисляющие виды угроз и источников информационной безопасности. Из содержания рассмотренных правовых актов не ясно в чем различие между угрозами и источниками угроз. Считаем, что при подготовке проекта Кодекса об информатизации в части определения угроз и их источников для информационной безопасности можно имплементировать положения Соглашения между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности (2010).

4 Для защиты нравственного здоровья несовершеннолетних от негативного влияния информации установить законодательный запрет на регистрацию в социальных сетях Facebook, В Контакте, Twitter для лиц младше 18 лет без согласия родителей. Компании должны разработать специальный механизм запрашивания согласия родителей на регистрацию в той или иной сети.

5 Дополнить Главу 2 «Уголовные правонарушения против семьи и несовершеннолетних» Уголовного кодекса Республики Казахстан статьей, предусматривающей уголовную ответственность за преступления против несовершеннолетних с использованием информационно-коммуникативных технологий (вовлечение в преступные игры, доведение до самоубийства и др.).

Список литературы:

1 Конституция Республики Казахстан от 30 августа 1995 года (с изм. и доп. по сост. на 10.03.2017) - Электронный ресурс – Режим доступа -https://online.zakon.kz/Document/?doc_id=1021546

2 The Welfare Party and others v. Turkey, Judgment of 13 February 2003 // [Электронныйресурс] – Режимдоступа - http://europeancourt.ru/uploads/ The Welfare Party and others v. Turkey.pdf

3 Закон Республики Казахстан от 23 июля 1999 года № 451-I «О средствах массовой информации» (с изменениями и дополнениями по состоянию на 28.12.2017 г.).) – Электронный ресурс – [Режим доступа] -https://online.zakon.kz/document/?doc_id=31396226

4 Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 28.12.2017 г.) – Электронный ресурс – [Режим доступа] -https://online.zakon.kz/document/?doc_id=31396226

5 Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» (с изменениями и дополнениями по состоянию на 28.12.2017 г.) – Электронный ресурс – [Режим доступа] - https://online.zakon.kz/document/

6 Копылов В.А. Информационное право. –М.: Юрист, 2002. – 612с.

7 DataProtectionAct 1998– Электронный ресурс – [Режим доступа] - https://www.legislation.gov.uk/ukpga/1998/36/contents

8 Жарова А.К. Опыт правового обеспечения безопасности персональных данных в Великобритании // Государство и право. – 2017. -№6. –С.70-79

9 Приоритеты национальной безопасности в условиях глобализации. / Жатканбаев Е.Б. и др.- Алматы: Қазақ университеті, 2006. -329с.

10 Мовкебаева К.А., Карманов А. Информационные операции США в контексте обеспечения кибербезопасности //Вестник КазНУ. Серия м.о. и м.п. -2016.-№2. –С.236-242

11 Строева Ю. О. Информационная безопасность детей в телекоммуникационных сетях // Молодой ученый. — 2017. — №50.1. — С. 41-43. — URL https://moluch.ru/archive/184/47336/ (дата обращения: 17.04.2018).

12Танекова М.О. К вопросу о распространении порнографических материалов в социальных сетях // Вестник КазНУ. Серия м.о. и м.п.- 2016. - №4. –С.158-154

13Нормативное постановление Верховного Суда Республики Казахстан от 8 декабря 2017 года №11 «О некоторых вопросах судебной практики по применению законодательства о террористических и экстремистских преступлениях» – Электронный ресурс – [Режим доступа]- https://online.zakon.kz/Document/?doc_id=355366

EURASIAN ECONOMIC UNIONLAW: APPROACHES TO CONCEPTUAL UNDERSTANDING

AmirbekK.S., PhD the doctoral candidate, Master of law, Ye.A. Buketov Karaganda State University

The beginning of the legal framework of integration EAEU founding members can be regarded in 1991 the formation of the Commonwealth of Independent States (CIS) – association that is very soft in legal essence (according to the opinions of some researchers, «at the initial period of CIS creation of and activities integration aspirations were declared more than fulfilled in reality» [1; 94]), but wider in scope of participants.

In 2000 a number of member states of the CIS (Russia, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan) established the «second floor» of post-Soviet integration – the Eurasian Economic Community (hereinafter - EurAsEC). It was more effective: in its framework nearly 200 international treaties were adopted; States participants were able to unify the domestic legal systems in part of trade and the economy in general. At the same time there was a definite imbalance in their rights and obligations: some states have not ratified certain treaties, haven't satisfied them [2; 127].

The problem was in the method of making and implementing decisions, so Russia, Belarus and Kazakhstan as the states more prepared decided to change the method - to transfer some part of the competences to the supranational level. In 2010, the Customs Union of three countries has been established, and as its main body - the Commission of the Customs Union with supranational powers was. Later, the Customs Union was amended by draft of the Common Economic Space; Eurasian Economic Commission was established instead of the Customs Union Commission (hereinafter – EEC).

In 2014, three countries signed the Treaty establishing the Eurasian Economic Union - the next «level» of integration. EurAsEC, which has performed its task, has been abolished. An optimization of the integration of the control system by means of international legal instruments, «multiplicity» of integration structures was eliminated, which are drawn to the attention of experts [3].

For a more complete understanding of the concept of the «EAEU law», which is formulated in Article 6 of the EAEU Founding agreement should apply to the formation of its origins and evolution within the Customs Union and Common Economic Space, which were the forerunners of the Union.

The foundations of the Customs Union between Belarus, Republic of Kazakhstan and the Russian Federation have been formulated January 6, 1995, when the Heads of this States signed in Minsk Agreement on the Customs Union between the Russian Federation and Belarus, and on January 20 of the same year Kazakhstan acceded to this Agreement. In 1996 the Kyrgyz Republic joined to this agreement, and in 1999 – Republic of Tadzhikistan.

In the future, the legal framework of the Customs Union has been supplemented by such agreements as the Treaty on the deepening of integration in economic and humanitarian spheres (1996), the Treaty on the Customs Union and the Common Economic Space (1999) and a number of others.

October 10, 2000 the Agreement on the Establishment of the Eurasian Economic Community (EurAsEC) was signed in Astana, an international organization, which has put in Article 2 the own aim the