DOI 10.31489/2021 L3/15-27

УДК 341.21

М.С. Бисалиев*, К.Н. Шакиров

Казахский национальный университет им. аль-Фараби, Алматы, Казахстан
(E-mail: mbissaliyev@gmail.com, kshakirov1954@mail.ru)

Характеристика источников международного права в сфере кибербезопасности

Информационное право, включающее в себя в качестве основного компонента обеспечение кибербезопасности в международных отношениях, — относительно новая область юридических знаний, необходимый доктринальный уровень которой достигнут сегодня далеко не по всем поднимаемым ею вопросам. Авторы полагают, что наименование «правовое обеспечение кибербезопасности» вряд ли уместно, поскольку право регулирует вопросы любого обеспечения кибербезопасности (технического и технологического, организационного), а не только правового, хотя и исключительно правовыми средствами. В статье использованы общенаучные, частнонаучные и иные методы исследования: социологический, исторический, формально-логический, сравнительно-правовой. Нормативную правовую базу составили нормы международного права, опубликованные и неопубликованные материалы отечественной и международной юридической практики, авторские эмпирические исследования в области международного и информационного права. К выводу об обособленности и системной самостоятельности права кибербезопасности также можно прийти по итогам исследования основных элементов юридической технологии в сфере обеспечения кибербезопасности: стратегии и тактики, юридической техники (как совокупности средств) и ресурсообеспеченности, внешних и внутренних (процессуальных) форм и режимов. С учетом приведенных позиций вполне можно вести речь о праве кибербезопасности как о самостоятельном институте международного информационного права.

Ключевые слова: кибербезопасность, источники права кибербезопасности, информационная безопасность, информационное право, информатизация, цифровизация, электронная цифровая подпись, интернет, защита персональных данных.

Введение

Усилившаяся в XXI веке экономическая глобализация неизбежно повлекла за собой аналогичные политические, социальные, культурные и иные, в том числе правовые аспекты общественных отношений. Сегодня мы наблюдаем, что характер международных взаимосвязей уже перерос свои масштабные количественные характеристики и приобрел качественно новые черты. С развитием информационных технологий, постоянно растущим количеством пользователей сети Интернет возникли две тенденции: во-первых, существенно растет количество высококвалифицированных специалистов по всему миру, деятельность которых контролировать и идентифицировать практически невозможно, хотя среди профессиональных пользователей сети могут встречаются и достаточно слабо образованные люди. Во-вторых, покрытым сетью Интернет является практически весь мир со своими особенностями геолокации, создающей трудности региональной идентификации пользователей сети. Как правило, подобное огромное киберпространство пользователей с достаточно слабой возможностью отслеживания и контроля, создает условия для возникновения существенного и разнообразного количества процессов, нередко преследующих преступные цели. Эта ситуация затрагивает как отдельных лиц и организациий, так и целые государства. Обезличенность и возможность дистанционного влияния на юридические и физические лица с преступными намерениями является одной из самых актуальных проблем на уровне государств, требующих квалифицированного разрешения.

С одной стороны, появилось понимание того обстоятельства, что современные государства как субъекты международного права не только обязаны следовать неким «правилам равенства» на мировой арене в отношении к «себе подобными» публичными субъектами права, но и должны соблюдать эти правила внутри себя, на своей территории, в национальной правовой системе. В ином случае соблюдению данных правил поведения государство-нарушитель может быть принуждено мировым сообществом.

* Автор-корреспондент. E-mail: *mbissaliyev@gmail.com*

Основной ценностной категорией сегодня стали не государственные, а гуманистические начала. Положение о том, что человек, его права и свободы являются высшей ценностью мировой цивилизации в развитых странах мира уже вышли за пределы конституций и научных монографий в судебные инстанции и к иным правоприменителям. Следует отметить также, что права и свободы, признаваемые и гарантируемые согласно общепризнанным принципам и нормам международного права, являются неотъемлемой составной частью общего, отраслевого (специального) и индивидуального статуса личности, в силу чего участники правоотношений, использующие, соблюдающие и исполняющие нормы права во всех случаях, а не только в случаях коллизий и при отсылках вправе ссылаться на данные принципы и нормы, что не может не учитываться в ходе правоприменительной деятельности и должно находить отражение в правоприменительных актах.

Рассмотрение вопроса о правовом регулировании отношений в сфере обеспечения кибербезопасности невозможно без установления тех основных начал и принципов, а именно норм и иных руководящих положений о такого рода отношениях. Понятие «источник правового регулирования кибербезопасности» в данном контексте несколько шире, нежели «источник (форма) права». Источником правового регулирования здесь могут быть признаны как международные акты и соглашения (договоры), так и конституционные акты или же, например, модельные акты не правового, а, скорее, морального характера. Основными источниками правового регулирования остаются национальные нормативные акты в каждой национальной системе правопорядка. Например, в Республике Казахстан – Закон РК «Об информатизации», нормативные правовые акты и подзаконные акты, затрагивающие сферу информатизации.

В процессе построения отношений в сфере обеспечения кибербезопасности можно отметить, что фундаментальную основу для регулирования таких отношений должны, в числе прочего, составить общепризнанные нормы и принципы международного права, а также иные международные нормы, имплементированные в национальное право [1; 49–51]. С практической точки зрения из всего этого массива нормативного-правовых актов следует обратить внимание главным образом на принципы регулирования отношений в сфере обеспечения кибербезопасности, а также указание на формы и способы обеспечения кибербезопасности, принятые в международном сообществе.

Такого рода нормы и принципы можно подразделить на две группы: во-первых, это некие основополагающие начала (стратегемы), в основе которых лежат право человека на информацию, право человека на неприкосновенность частной жизни, на тайну переписки и т.п. Во-вторых, это так называемые нормы международного права, регулирующие отношения в сфере обеспечения кибербезопасности, которые не получили статуса общепризнанных и могут базироваться, в числе прочего, и на региональных источниках, а также на двусторонних договорах и соглашениях.

Методы и материалы

В данной работе использованы общенаучные, частнонаучные и иные методы исследования: социологический, исторический, формально-логический, сравнительно-правовой. Нормативную правовую базу составили нормы международного права, опубликованные и неопубликованные материалы отечественной и международной юридической практики, авторские эмпирические исследования в области международного и информационного права.

Обсуждение

Обратимся, первоначально, к нормам и принципам первой группы. Среди положений актов, содержащих такого рода общепризнанные нормы и принципы международного права, видимо, следует назвать в первую очередь нормы статьи 19 Всеобщей декларации прав человека 1948 г. [2], а также нормы статьей 19 и 20 Международного пакта о гражданских и политических правах [3]. Необходимо признать, что интересующие нас нормы правоположений сформулированы в достаточно общем виде. Их необходимая конкретизация сделана в иных международных документах, например, таком важнейшем акте, как Европейская конвенция о защите прав человека и основных свобод [4]. В частности, например, в статье 10 Конвенции провозглашено право свободно выражать свое мнение, которое (право) включает свободу получать и распространять информацию и идеи без какого-либо вмешательства со стороны публичных властей и независимо от государственных границ. Очевидно, что без реализации права на информацию не может быть речи и об ее защите. Между тем в п. 2 ст. 10 Конвенции установлены ограничения в материальном и формальном (процедурном) смысле этого слова для реализации этого права. Предпосылками «Конвенции о защите частных лиц в отношении

автоматизированной обработки данных личного характера» [5] служили вопросы о степени разработки европейского законодательства, которые обеспечивают адекватную защиту отдельных лиц, когда данные о них передаются через «границу». Компьютеры в сочетании с телекоммуникациями уже открывали новые перспективы для обработки данных в международном масштабе. Сетевые технологии позволили пользователям получить доступ в информационные системы в отдаленных странах. В некоторых секторах, например, в банковском, страховом деле, туризме такие приложения для трансграничной обработки данных уже стали обычным явлением. В принципе, в разных сферах должны применяться одни и те же фундаментальные правила независимо от того, где происходили операции обработки данных, а субъекты данных должны иметь одинаковые гарантии. Становится проблематично контролировать данные, когда они распределены в разных государствах: банковские данные в одной стране, персональные – во второй, медицинские данные – в третьей. Чтобы противостоять этим рискам, некоторые страны ввели в свое внутреннее законодательство специальные меры контроля, например, в виде требований и правил обработки данных. В казахстанском сегменте Интернет также существуют требования к размещению Интернет-ресурсов. Например, соответствии пп. 5 п. 16 о «Правилах регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента Интернета» от 13 марта 2018 г., приостанавливается пользование доменным именем KZ и .ҚАЗ в случае, если физическое размещение данных находится вне территории Республики Казахстан [6]. Однако такой контроль мешает свободному международному потоку информации, что является принципом фундаментальной важности как для отдельных людей, так и для государств.

При таких обстоятельствах нужно исходить из примата международных норм, закрепленных Конвенцией №108, и считать, что предусмотренные законодательством о персональных данных случаи запрета и ограничения трансграничной передачи персональных данных напрямую не касаются случаев раскрытия этих данных их субъектами непосредственно иностранным операторам. Оценка действий субъектов персональных данных в такой ситуации должна производиться, исходя из природы права гражданина на персональные данные. В Европейском союзе имеются единые кодифицированные акты, которые регламентируют вопросы такого рода более подробным образом. В частности, к ним относится Регламент Европейского парламента и совета 2016/679 «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46/ЕС (Общие правила защиты данных» (GDPR) от 27 апреля 2016 г. [7]. В силу п. 1 ст. 2 указанного документа, Регламент применяется к обработке персональных данных полностью или частично автоматизированными средствами и к обработке неавтоматизированными средствами, которые являются или предполагаются частью системы регистрации документов. Регламент предусматривает правила по защите физических лиц в отношении обработки персональных данных и правила свободного обращения персональных данных. При этом особо оговаривается, что свободное обращение персональных данных в Союзе не должно быть ни ограничено, ни запрещено по причинам, связанным с защитой физических лиц при обработке персональных данных (п. 3 ст.1 Регламента). Согласно ст. 3 Регламента, он применяется в отношении обработки персональных данных, в связи с действиями, осуществляемыми контроллером или оператором данных по месту предпринимательской деятельности в Союзе, независимо от того, проводится обработка в Союзе или нет. Также указано, что Регламент применяется в отношении обработки персональных, находящихся в Союзе субъектов данных, которую осуществляет контроллер или оператор данных, не ведущий предпринимательскую деятельность в Союзе, если действия по обработке связаны либо с предоставлением товаров и услуг такого рода субъектам данных в Союзе, независимо от того, требуется ли оплата от субъекта данных, либо с мониторингом их поведения, поскольку их поведение происходит в Союзе. Регламентом предусмотрены принципы обработки персональных данных (ст. 5 Регламента), среди которых основным является принцип законности обработки (ст. 6 Регламента). Регламент достаточно гибко подходит к условиям для согласия на обработку данных, отдельно выделяя даже условия, применяемые к согласию ребенка на такие действия (ст. 8 Регламента). Помимо обычных условий обработки персональных данных, Регламент предусматривает также особенности их обработки в трех случаях: когда эти персональные данные относятся к специальной категории, когда они связаны с приговорами или правонарушениями в целом, когда обработка не требует идентификации (ст. 9-11 Регламента). Право доступа к персональным данным увязывается Регламентом с возможностью действовать по двум алгоритмам: когда личные данные собираются от субъекта персональных данных, или были получены помимо указанного субъекта. В рамках процесса исправления и удаления данных Регламентом предусмотрены не только права, признаваемые в национальных правопорядках, вроде права на

исправление (ст. 16 Регламента) или на переносимость данных (ст. 20 Регламента), но и такие права, как «право на забвение» (ст. 17 Регламента), право на ограничение обработки (ст. 18 Регламента) и т.п. Основными фигурами процесса работы с персональными данными являются контроллер и оператор. Контроллер данных — это тот, кто взаимодействует с клиентом, собирает данные и определяет, каким образом их дальше обрабатывать. Оператор данных — получает персональные данные от контроллера, хранит их или каким-то образом обрабатывает, по указанию контроллера. Оператор не работает с физическими лицами, а только обрабатывает их персональные данные, строго по поручению контроллера. Согласно GDPR статус оператора можно потерять, если оператор начинает сам определять, каким образом обрабатывать данные, а не следовать указаниям контроллера. Регламентом предусмотрена ответственность контроллера, отдельные проверочные действия предусмотрены и в отношении оператора. Регламент устанавливает требования к безопасности обработке (ст. 32 Регламента). О взломе персональных данных, если таковой произойдет, уведомляется надзорный орган, а также сам субъект данных (ст. 33, 34 Регламента). Особую важность среди объектов критической инфраструктуры, нуждающихся в защите от киберугроз, приобрели в современных условиях медицинские учреждения. Основная (но не единственная) проблема здесь – обеспечение сохранности персональных данных. К сожалению, не все наиболее значимые вопросы этой области уже разрешены на международно-правовом уровне, однако законодательство Евросоюза о защите персональных данных может служить образцом для построения общемировой модели. В материальном смысле слова в Конвенции установлены «обязанности и ответственность» в рамках указанных взаимоотношений, которые сводятся по своей целевой характеристике к интересам демократического общества, а именно, решают задачи: а) национальной безопасности; б) территориальной целостности; в) общественного порядка; г) предотвращения беспорядков или преступлений; д) охраны здоровья и нравственности; е) защиты репутации или прав других лиц, ж) предотвращения разглашения информации, полученной конфиденциально и з) обеспечения авторитета и беспристрастности правосудия. Таким образом, уже на уровне международных норм права создаются условия для национального правового регулирования вопросов безопасности государства и личности (в части вредной информации) [8; 21–33]. Из указанного примера видно, что общепризнанные нормы и принципы международного права могут и должны служить значимым источником правового регулирования отношений в сфере обеспечения кибербезопасности.

В российском правовом пространстве проблематика применения международных правоположений достаточно подробно исследована в современной литературе, причем очевидно, что судами и иными органами правоприменения общепризнанные нормы и принципы международного права применяются (за исключением случаев, когда это происходит в связи с необходимостью исполнения решений Европейского суда по правам человека или иных международных судебных инстанций) при рассмотрении (разрешении) конкретных правовых споров лишь в двух случаях: в первом случае, в дополнение к существующей норме национального права при ее нечеткости или неопределенности – для лучшей правовой аргументации и мотивировки решения и, во втором случае, в связи с тем, что стоящая выше судебная инстанция уже сослалась на данную норму при разрешении схожей ситуации и нижестоящий суд попросту «переписывает» ее из решения стоящего выше суда в мотивировочную часть решения по рассматриваемому им делу. При этом применяются лишь общепризнанные нормы и принципы международного права, которые содержатся либо в международных договорах Российской Федерации, либо в международных нормативных правовых актах, то есть применяются, по сути, не сами общепризнанные принципы и нормы международного права, а указанные источники права, содержащие их [9; 45–60].

Вторая группа международно-правовых источников (нормы международного права, непосредственно регулирующие отношения в сфере обеспечения кибербезопасности) часто имеют технологический и организационный характер, что не снижает их значимости, однако отводит им некоторую вспомогательную роль. Например, Законом РК от 07 марта 2002 г. N 300 «О ратификации Устава и Конвенции Международного союза электросвязи» Республика Казахстан ратифицировала Устав и Конвенцию Международного союза электросвязи, подписанную в Женеве 22 декабря 1992 г. [10, 11]. В данных документах, в частности, предусмотрена обязанность государства по поддержанию передачи информации путем сети Интернет, что создало новый сложный объект для защиты информации, информационных прав и интересов граждан, государства и общества. Свободу передачи информации и соответствующие обязанности государств в названной сфере подтверждает и Окинавская хартия глобального информационного общества, принятая на совещании стран восьмерки 22 июля 2000 г.

[12]. Часть вопросов доступа к судебной информации рассматривается в Соглашении стран СНГ от 21.10.1994 г. «Об обмене правовой информацией» [13].

Странами ШОС (Шанхайское общество сотрудничества) также проводится работа в области обеспечения международной информационной безопасности. Шесть стран (Казахстан, Россия, Таджикистан, Узбекистан, Кыргызстан, Китай) в рамках ШОС подписали «Правила поведения в области обеспечения международной информационной безопасности». Правила обязывают государства-участников использовать приемлемое использование систем защиты информации, не имея средств к информационному оружию и источнику угрозы. Документ был подан в 2015 г. в ООН и ратифицирован шестью государствами [14]. В рамках Организации исламского сотрудничества (ОИС) странами-участницами принята Резолюция о «Сотрудничестве групп реагирования на компьютерные чрезвычайные ситуации (OIC-CERT) между странами-членами ОИС». Резолюция была одобрена на 35-й сессии Совета министров иностранных дел встречи ОИК в Кампале, Уганда, «18–20» июня 2008 г., Резолюция № 3/35-INF. OIC-CERT открыт для частного сектора и специалистов по информационной безопасности из стран-членов ОИС [15]. Цель состоит в том, чтобы способствовать беспрепятственному сотрудничеству и взаимодействию между группами реагирования и профессионалами в области информационной безопасности среди участников для достижения целей OIC-CERT, а именно:

– укрепление отношений между CERT в странах-членах ОИС;
– улучшение обмена информацией в области кибербезопасности;
– предотвращение или сокращение киберпреступлений;
– содействие образовательным и просветительским программам;
– содействие совместным исследованиям и разработкам технологий;
– предоставление кибернетических каналов связи между странами-членами.

В Стратегии Организации Договора о коллективной безопасности на период до 2025 г. (ОДКБ) от 2016 г. подчеркивается, что формирование безопасного информационного пространства государств-членов ОДКБ является основной стратегической целью информационной безопасности ОДКБ, что, несомненно, включает в себя также киберпространство [16]. При этом, согласно Стратегии, ОДКБ должна предпринять следующий комплекс действий для обеспечения комплексной информационной безопасности государств-членов:

– формирование системы информационной безопасности государств-членов ОДКБ;
– развитие межгосударственной и межгосударственной информационной безопасности;
– межведомственное сотрудничество в области информационной безопасности;
– модернизация механизмов противодействия угрозам в информационном пространстве;
– проведение совместных мероприятий по противодействию и нейтрализации угроз в информационно-коммуникационной сфере ОДКБ пространства;
– взаимодействие в вопросах обеспечения международной информационной безопасности;
– разработка согласованных правил поведения в информационном пространстве и продвижение их на международный уровень;
– разработка условий для создания основы для согласованной информационной политики.

Один из основных компонентов электронного обмена является наличие электронной подписи. В первую очередь, необходимо подчеркнуть, что значение термина «электронная подпись» в праве Англии и Уэльса отличается от значения этого понятия в иных национальных правопорядках, например, в Законе Республики Казахстан от 7 января 2003 г. № 370-II «Об электронном документе и электронной цифровой подписи» [17]. В казахстанских реалиях под электронной подписью обычно понимается способ криптографического преобразования информации. В то же время ч. 3 ст. 152 ГК РК позволяет совершать сделки при помощи электронного обмена. В английском же праве термин имеет более широкое значение и применяется по отношению к любому тексту, предназначенному играть роль подписи в конце письма в том числе. Таким образом, безопасность использования электронной подписи в Великобритании имеет куда большее значение для субъектов соответствующих правоотношений в рамках национального права. На практике, разумеется, не всегда та или иная сторона возникшего обязательства считает себя связанной. Зачастую электронная переписка воспринимается менее серьезно, чем, например, обмен бумажными документами, и в особенности тогда, когда к электронным сообщениям не прикрепляются никакие электронные файлы, что зачастую негативно сказывается на участниках такого обмена сообщениями.

Тем не менее электронные сообщения, если они составляют единую логическую цепочку и являются последовательными ответами одно на другое, могут представлять собой юридически обязывающий договор. Причем не имеет значения, было ли сообщение прочитано и прочитано достаточно внимательно, если на него был дан ответ. Так, в деле *Nicholas Prestige Homes v Neal (2010)* женщина отправила сообщение: «*Hi Mark, That's fine, look forward to some viewings. Sally*» в ответ на письмо, к которому был прикреплен типовой договор и которое содержало оферту [18]. В суде она утверждала, что ее слова были ответом на телефонный звонок, который ранее поступил ей от контрагента. Тем не менее в истории переписки видно, что ее сообщение является ответом на сообщение контрагента, содержащее оферту и типовой договор, и составляет с ним логическую цепочку, а не является заново и независимо отправленным сообщением. Более того, суд постановил, что только лишь имена, указанные в конце сообщений, являются подписью, и отправленные сообщения, таким образом, приравниваются к отправке бумажного подписанного письма. Английские судьи уделяют большое внимание формальной стороне вопроса, что подтверждает решение по указанному выше делу, где ответчица была признана стороной по договору, исходя из формального и фактического наличия цепочки сообщений, хотя она не имела намерения вступать в данный договор.

Рассмотрим понятие электронной подписи, а также вопрос о намерении лица поставить подпись. Согласно Акту «Об электронных сообщениях 2000 года» (Electronic Communications Act 2000), электронная подпись является действительной, если она включена в электронное сообщение или логически связана с ним [19]. Споры возникают относительно того, что именно считать электронной подписью. Сложности имеют место, когда речь идет не о подписях, вставленных в электронный документ с помощью специальных программ, а о подписях, содержащихся в тексте электронного сообщения просто в виде напечатанного имени лица. Чтобы иметь юридическую силу, электронное сообщение должно содержать наименование лица, которое отправляет сообщение. Такое наименование будет являться электронной подписью. Большое значение при заключении письменного договора имеет намерение лица поставить именно подпись, данное правило применяется и к электронным сообщениям. Электронный адрес, с которого отправлено сообщение, вставленный в письмо автоматически, не является электронной подписью лица, которому этот адрес принадлежит. Также электронной подписью не является просто наименование лица или ссылка на лицо в тексте сообщения. Лицо должно указать свое имя с намерением поставить именно подпись и таким образом подтвердить подлинность отправляемого электронного письма, то есть, например, указать его в конце сообщения. Благодаря предпринятым законодательным мерам, в Великобритании сегодня не имеется каких-либо проблем с возможностью заключения с помощью обмена электронными сообщениями договоров, относящихся к категории устных сделок при соблюдении, разумеется, требований, обращенных законом к устной форме сделки. Вне зависимости от способа (вида, типа, формы) обмена такими сообщениями речь идет об опосредованном электронными устройствами непосредственном общении физических лиц, где важными остаются наличие воли на заключение договора и ее изъявление. Однако современное гражданское законодательство романо-германской правовой семьи, в том числе российское, в случае его расширительного толкования позволяет осуществлять заключение гражданско-правовых договоров путем обмена электронными сообщениями в самых разнообразных формах, по крайней мере, прямые запреты на это отсутствуют.

Как отмечалось выше, среди отдельных актов следует выделить Закон о неправомерном использовании компьютерных технологий 1990 г. (Computer Misuse Act, 1990) [20]. Этим актом предусмотрены уголовно-правовые меры в области борьбы с киберпреступностью. Помимо ожидаемых для такого закона вопросов, формулировки признаков состава преступления, установления уголовно-правовых санкций и т.п., Закон содержит и важные принципиальные положения. Например, в его рамках в качестве основного нарушения рассматривается попытка получения доступа или доступ к компьютеру или данным, которые он хранит, путем принуждения компьютера к выполнению любой функции с намерением обеспечить безопасный доступ. Таким образом, хакеры, которые программируют свои компьютеры на поиск перестановок паролей, несут ответственность, даже если их попытки войти в систему отклоняются целевым компьютером. Единственным предварительным условием ответственности является то, что хакер должен знать, что попытка доступа неавторизована. Таким образом, использование имени пользователя или идентификатора (ID) и пароля другого лица без надлежащих полномочий для доступа к данным или программе, или для изменения, удаления, копирования или перемещения программы или данных, или просто для вывода программы или данных на экран или принтер, или выдавать себя за другое лицо с помощью электронной почты, онлайн-чата, Ин-

тернета или других служб, является правонарушением. Даже если первоначальный доступ разрешен, последующее исследование, если в системе существует иерархия привилегий, может привести к входу в те части системы, для которых отсутствуют необходимые привилегии, и нарушение будет совершено. Интересно, что «взгляд через плечо пользователя», или использование сложного электронного оборудования для отслеживания электромагнитного излучения, излучаемого дисплеями («электронное подслушивание»), не входит в сферу действия данного правонарушения. Аналогичным образом использование методов фишинга или троянского коня для получения идентификационных данных или любых других данных из неавторизованного источника, или изменение файлов операционной системы или некоторых аспектов функций компьютера, чтобы помешать его работе или предотвратить доступ к любым данным, включая уничтожение файлов или преднамеренное создание кода, вызывающего полную неисправность системы, являются преступными «модификациями».

В Законе о защите данных 1998 г. (Data Protection Act, 1998) разрешаются вопросы уголовной за незаконное разглашение персональных данных, в том числе с использованием компьютерных технологий [21]. Следует отметить, что по данному акту уголовная ответственность наступает за незаконное разглашение персональных данных, если эти действия причинили или могли причинить существенный вред человеку, персональные данные которого разглашены или причинили существенный вред его правам и свободам. Одной из актуальных проблем британский законодатель считает спам, рассматривая его как способ кибератаки через внедрение вредоносного или шпионского программного обеспечения. В целях борьбы со спамом (нежелательной компьютерной информацией) в Великобритании в 2003 г. были приняты положения «Правила о конфиденциальности и электронных коммуникациях (Директива ЕС) 2003 г.» (The Privacy and Electronic Communications (EC Directive) Regulations 2003) [22]. Данным Положением выстроена интересная схема защиты прав: компании обязаны получить разрешение физического лица, прежде чем посылать ему сообщения по электронной почте или СМС-сообщений (положения закона относятся также к телефонным звонкам и факсам). Между тем юридические лица по данному закону не защищены от спама: его положения применимы только к сообщениям, отправляемым на адреса физических лиц, хотя, очевидно, что в реальности это отследить сложно. Более того, в современных условиях юридические лица нуждаются в явно не меньшей защите от спама, чем физические.

В работе Дж. Козефа структурирована проблема регламентации кибербезопасности США на несколько уровней: оценка текущего состояния законодательства и разъединенность между структурами национальной безопасности и корпоративным правам. К вопросам национальной безопасности отнесены вопросы о персональных данных физических и юридических лиц. Более того, директивным органам следует рассмотреть возможность предоставления компаниям экономических стимулов для принятия мер кибербезопасности [23; 985]. И. Киловаты описывает глобальную роль таких технических гигантов, как Microsoft, Google и Facebook, и их роль в «Приватизации законодательства в области кибербезопасности» [24; 1181]. В статье представлен анализ того, как технологические компании эффективно становятся регуляторами глобальной кибербезопасности, основываясь на неспособности государств преодолеть геополитические разногласия в отношении того, как киберпространство должно регулироваться на глобальном уровне. Основное назначение такого рода актов – зафиксировать требования к деятельности государств (в том числе в межгосударственном общении) в части обеспечения свободного и безопасного обмена информацией в виде организационной обязанности способствовать претворению в жизнь общепризнанных норм и принципов международного права, регулирующих право граждан на свободный информационный обмен, одновременно, информационный обмен, соответствующий требованиям кибербезопасности.

Кроме того, отметим, что у массива норм права, регулирующих вопросы обеспечения кибербезопасности, имеет место наличие признаков относительной однородности и системности. Специфика предмета правового регулирования (отношения в сфере обеспечения кибербезопасности) и особенности правового подхода к регулированию общественных отношений, в котором преобладают императивные нормы права, запреты и предписания, позволяют большинству авторов говорить об обособленности указанных норм в институт или подотрасль права. Вместе с тем единства позиций по данному вопросу в литературе не наблюдается. В частности, многие авторы просто презюмируют обозначение системы норм в сфере обеспечения кибербезопасности как институт информационного права, поскольку это им представляется очевидным. А.К. Костылев обосновывает институциональность норм права об обеспечении кибербезопасности их обособленностью и стоящими перед ними специфическими задачами, однако прямо право информационной безопасности институтом (подот-

раслью) информационного права и не именует [25; 147]. Т.А. Полякова выделяет в качестве самостоятельной подотрасли информационного законодательства законодательство в области обеспечения кибербезопасности с учетом определения самостоятельности предмета и комплексности применяемых методов правового регулирования, но не указывает на обособленность права кибербезопасности как самостоятельного института (подотрасли) самого информационного права, хотя в самом тексте диссертационного исследования автор признает право кибербезопасности все-таки подотраслью информационного права, причем такой подотраслью, которая в свою очередь подразделяется на институты [26; 118]. Анализ же начальных работ указанного автора позволяет нам полагать, что это далеко не просто оговорка: ученый не считает, что право кибербезопасности «не доросло» пока еще в процессе своей институализации до такой обособленной совокупности правовых норм, как институт (подотрасль) права, однако законодательство о кибербезопасности уже может быть выделено в отдельную, обособленную систему. В.Н. Лопатин также указывает право в сфере обеспечения кибербезопасности как подотрасль информационного права, представляющую совокупность правовых норм, регулирующих общественные отношения по защите национальных интересов в информационной сфере. По его мнению, предметом здесь выступает кибербезопасность, а объектом – общественные отношения, связанные с ее обеспечением [27; 141]. И.Л. Бачило также относит институт кибербезопасности к общим правовым институтам информационного права [28; 126]. Схожую позицию и аргументацию несколько ранее представлял и В.А. Копылов [29; 219]. Множество субинститутов и суботраслей выделяет в рамках информационного права и П.У. Кузнецов [30; 115]. В то же время существуют и достаточно оригинальные позиции. Например, П.Г. Андреев предлагает говорить о кибербезопасности как о новом правовом образовании, именуя его при этом «правовым обеспечением кибербезопасности», как подотраслью информационного права. Среди признаков правового обеспечения кибербезопасности как подотрасли информационного права он выделяет: обособленный предмет правового регулирования, логически связанную структуру, особый правовой режим, комплексное использование отраслевых методов правового регулирования, высокую степень специализации и интеграции входящих в его состав правовых институтов, каждый из которых в свою очередь также имеет структуру (субинституты), единство цели правового регулирования (обеспечение кибербезопасности), единством комплексной природы подотрасли правового обеспечения информационной безопасности и комплексной природы информационного права, включенность правоотношений, связанных с обеспечением кибербезопасности, в состав отраслевых информационных правоотношений [31; 91].

Результаты

Мы полагаем, что наименование «правовое обеспечение кибербезопасности» вряд ли уместно, поскольку право регулирует вопросы любого обеспечения кибербезопасности (технического и технологического, организационного), а не только правового, хотя и исключительно правовыми средствами. С точки же зрения выделения указанных П.Г.Андреевым оснований для обособления норм права кибербезопасности в системе информационного права, то здесь автор приводит как и достаточно верные, так и весьма спорные для этого критерии. Наша позиция в указанной части сводится к следующим основным соображениям. Прежде всего, вопрос о степени институализации указанных норм (выступает ли право кибербезопасности в качестве подотрасли или же института информационного права) очень оценочен: он зависит от множества выделяемых авторами критериев и свидетельствует не о целевой, методологической и предметной самостоятельности указанных норм, сколько о степени их развитости в обособленной системе, их месте в самом информационном праве. Поэтому данный вопрос достаточно субъективен и не слишком важен. Интересно и то обстоятельство, что авторами не дискутируется, как это нередко бывает, вопрос о возможности признания кибербезопасности комплексным институтом права (например, во взаимосвязи с административным правом в части доступа к государственной тайне или лицензионным разрешением на ту или иную деятельность по защите информации, с гражданским правом в связи с правовым регулированием вопросов защиты прав на информационные продукты как на результаты интеллектуальной деятельности, уголовным и уголовно-процессуальным правом в части киберпреступности и пр.). Все-таки о комплексности здесь вряд ли можно вести речь, хотя теоретически такое правопонимание и не исключается. В частности, А.А. Стрельцов полагает, что правовое обеспечение кибербезопасности базируется на совокупности институтов и норм информационного, конституционного, гражданского, административного и уголовного права, регулирующих отношения в области противодействия угрозам безопасности объектов

национальных интересов в информационной сфере [32; 105], причем его позицию активно поддерживают представители отраслевых наук, включая ученых-криминологов [33; 21]. Более принципиален сам вопрос о том, является ли право кибербезопасности самостоятельной системой обособленных норм права в рамках информационного права или же нет. Решению такого вопроса должны предшествовать выводы об: 1) относительной обособленности указанных правовых норм; 2) об их однородности. К такого рода выводам можно прийти на основании совокупности субъективных и объективных факторов. К субъективным факторам мы относим относительно развитое законодательство, наличие некоторой практики его применения, существование развитой доктрины по данным вопросам, логическая связанность и структурность системы таких норм, их собственный функционал и целевые установки (единство цели правового регулирования (обеспечение кибербезопасности). По нашему мнению, в той или иной степени указанные субъективные критерии в нашем случае присутствуют, однако приоритет все-таки должен быть отдан наличию двух объективных факторов, а именно, собственному предмету правового регулирования, обособленному от других предметов в данной отрасли права и особой методологии правового регулирования выделяемых общественных отношений. Очевидно, что собственный предмет правового регулирования здесь присутствует: информационные отношения в сфере обеспечения кибербезопасности явно выделяются среди других видов информационных отношений по своему субъектно-объектному составу, фактическим и юридическим действиям, особенностям возникновения, изменения и прекращения, целям и результатам среди других общественных отношений, регулируемых информационным правом. Авторы отмечают, что законодательство в сфере кибербезопасности образует два блока, первый из которых включает нормы, устанавливающие правовой режим информации, права, обязанности, ответственность субъектов информационных отношений, меры по созданию и обеспечению состояния информационной защищенности тех или иных объектов, а второй – нормы, устанавливающие требования к техническим средствам, сетям связи, условия передачи информации и ко всему тому, что формирует их свойство обеспечивать защищенность информации и, в конечном счете, защищенность самих объектов [34; 100]. Несколько сложнее обстоит дело со спецификой метода правового регулирования. Помимо обычных запретов и предписаний, в целом характерных для информационного права, здесь можно говорить, например, о санкционирующем методе правового регулирования. который И.М. Рассолов определяет как такой способ, при котором законодатель предоставляет тому или иному участнику информационных отношений право самому принимать решения по интересующим его проблемам, но эти решения в то же время должны быть санкционированы в установленном законом порядке [35; 79].

Заключение

Одним из важнейших методов в праве кибербезопасности выступает метод ограничений, который обладает определенной универсальностью, например, в части ограничения доступа к той или иной информации. Итоги анализа субъектно-объектного состава правоотношений в сфере обеспечения кибербезопасности, основания возникновения данных отношений и их результаты, фактические и юридически значимые действия сторон отношений позволяют сделать вывод о том, что правоотношение в сфере кибербезопасности явно следует считать самостоятельным типом информационных отношений.

К выводу об обособленности и системной самостоятельности права кибербезопасности также можно прийти по итогам исследования основных элементов юридической технологии в сфере обеспечения кибербезопасности: стратегии и тактики, юридической техники (как совокупности средств) и ресурсообеспеченности, внешних и внутренних (процессуальных) форм и режимов. С учетом приведенных позиций вполне можно вести речь о праве кибербезопасности как о самостоятельном институте международного информационного права.

Таким образом, в международном праве в настоящее время происходит обособление норм, регулирующих вопросы обеспечения кибербезопасности. Данное обособление является системным и отвечает обычным требованиям, предъявляемым к институтам международного права. Данная ситуация предполагает усиление внимания учёных к рассмотренной формирующейся отрасли (подотрасли) знания и требует более серьёзного подхода в связи с многочисленными противоречиями, встречающимися в оценке не только её предметно-объектной и методологической составляющей, но и в связи с недооценкой влияния киберправонарушений не только в практике международных отношений, но и в региональном и национальном контексте правового развития государств.

Список литературы

1 Максуров А.А. Соотношение общепризнанных принципов международного права и общепризнанных норм международного права / А.А. Максуров и др. // Ростов н/Д.: Вестн. Южн. федер. ун-та, 2019. — Т. 6. — № 3. — С. 49–51.

2 Всеобщая декларация прав человека от 10 декабря 1948 года [Электронный ресурс]. — Режим доступа: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml

3 Международный пакт о гражданских и политических правах от 16 декабря 1966 года [Электронный ресурс]. — Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

4 Европейская конвенция о защите прав человека и основных свобод от 4 ноября 1950 года [Электронный ресурс]. — Режим доступа: https://www.coe.int/ru/web/compass/the-european-convention-on-human-rights-and-its-protocols

5 Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года [Электронный ресурс]. — Режим доступа: https://pd.rkn.gov.ru/law/document170.htm

6 Приказ министра оборонной и аэрокосмической промышленности Республики Казахстан от 13 марта 2018 года № 38/НК «Об утверждении Правил регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента Интернета» [Электронный ресурс]. — Режим доступа: https://online.zakon.kz/document/? doc_id=35205534

7 Общие правила защиты данных от 27 апреля 2016 года [Электронный ресурс]. — Режим доступа: https://gdpr-info.eu/

8 Микеле де Сальвиа. Европейская конвенция по правам человека / Микеле де Сальвиа. — СПб.: Юрид. центр «Пресс», 2004. — 310 с.

9 Максуров А.А. Общепризнанные принципы и нормы международного права: понятие и проблемы применения в Российской Федерации / А.А. Максуров. — М.: ИНФРА-М, 2020. — 189 с.

10 Закон Республики Казахстан от 7 марта 2002 года N 300 «О ратификации Поправочных документов к Уставу и Конвенции Международного союза электросвязи» [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/Z020000300_

11 Устав Международного союза электросвязи 1994 года [Электронный ресурс]. Режим доступа: https://www.itu.int/en/council/2019/Documents/basic-texts/Constitution-R.pdf.

12 Окинавская хартия глобального информационного общества от 22 июля 2000 года [Электронный ресурс]. — Режим доступа: https://docs.cntd.ru/document/901770887

13 Соглашение стран СНГ от 21 ноября 1994 «Об обмене правовой информацией» [Электронный ресурс]. — Режим доступа: https://normativ.kontur.ru/document? moduleId=1&documentId=13378

14 Правила поведения в области обеспечения международной информационной безопасности от 14 сентября 2011 года [Электронный ресурс]. — Режим доступа: https://digitallibrary.un.org/record/786846/files/A_69_723-RU.pdf? version=1

15 Resolutions on Information Affairs. 35th Session of the Council of Foreign Ministers [Электронный ресурс]. — Режим доступа: https://www.oic-oci.org/docdown/? docID=427&refID=30

16 Стратегия коллективной безопасности организации договора о коллективной безопасности на период до 2025 года от 18 октября 2016 года [Электронный ресурс]. — Режим доступа: https://odkb-csto.org/documents/statements/strategiya_kollektivnoy_bezopasnosti_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_na_period_do_/

17 Закон Республики Казахстан от 7 января 2003 года № 370 «Об электронном документе и электронной цифровой подписи» [Электронный ресурс]. — Режим доступа: https://online.zakon.kz/document/? doc_id=1035484

18 Case: Nicholas Prestige Homes v Neal (2010) [Электронный ресурс]. — Режим доступа: https://www.casemine.com/judgement/uk/5a8ff70660d03e7f57ea603b

19 Electronic Communications Act 2000 [Электронный ресурс]. — Режим доступа: https://www.legislation.gov.uk/ukpga/2000/7/pdfs/ukpga_20000007_en.pdf

20 Computer Misuse Act 1990 [Электронный ресурс]. — Режим доступа: https://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf

21 Data Protection Act 1998 [Электронный ресурс]. — Режим доступа: https://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf

22 The Privacy and Electronic Communications (EC Directive) Regulations 2003 [Электронный ресурс]. — Режим доступа: https://www.legislation.gov.uk/uksi/2003/2426/pdfs/uksi_20032426_en.pdf

23 Kosseff Jeff. Defining Cybersecurity Law /Kosseff Jeff. — Iowa: Iowa Law Review, 2017. — V. 103. — C. 985.

24 Kilovaty Ido. Privatized Cybersecurity Law / Kilovaty Ido // California: UC Irvine Law Review — 2019. — P. 1181.

25 Костылев А.К. Информационное право / А.К. Костылев. — Тюмень: Изд-во Тюмен. гос. ун-та, 2010. — 244 с.

26 Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. ... д-ра юрид. наук / Т.А. Полякова. — М., 2008. — С. 118–122.

27 Лопатин В.Н. Информационная безопасность: дис. ... д-ра юрид. наук / В.Н. Лопатин. — СПб., 2000. — С. 141–150.

28 Бачило И.Л. Информационное право / И.Л. Бачило. — М.: Юрайт, 2019. — 419 с.

29 Копылов В.А. Информационное право / В.А. Копылов. — М.: Юристъ, 2002. — 512 с.

30 Кузнецов П.У. Теоретические основания информационного права: дис. ... д-ра юрид. наук / П.А. Кузнецов. — СПб., 2005. — С. 321.

31 Андреев П.Г. Институциональное развитие правового обеспечения информационной безопасности в российском информационном праве: дис. ... д-ра юрид. наук / П.Г. Андреев. — Екатеринбург, 2012. — С. 247.

32 Стрельцов А.А. Теоретические и методологические основы правового обеспечения информационной безопасности России: дис. ... д-ра юрид. наук / А.А. Стрельцов. — М., 2004. — С. 146.

33 Ефремова М.А. Информационная безопасность как объект уголовно-правовой охраны / М.А. Ефремова. — М.: Информационное право, 2014. — № 5. — С. 21–25.

34 Терещенко Л.К. Информационная безопасность органов исполнительной власти на современном этапе / Л.К. Терещенко // Журн. рос. права. — 2015. — 8. — № 224. — С. 100–109.

35 Рассолов И.М. Информационное право: учеб. и практ. для академического бакалавриата / И.М. Рассолов. — М.: Юрайт, 2017. — 347 с.

М.С. Бисәлиев, К.Н. Шәкіров

Киберқауіпсіздік саласындағы халықаралық құқық қайнаркөздерінің сипаты

Халықаралық қарым-қатынастағы киберқауіпсіздікті қамтамасыз ететін негізгі құрамдас бөлігі болып табылатын ақпараттық құқық – заң білімдерінің салыстырмалы жаңа саласы, бүгінгі күнде ағымға қойылатын сұрақтардың барлығын аса қамти бермейтін, қажетті жаңа доктриналық деңгей болып табылады. Авторлар "киберқауіпсіздікті құқықтық қамтамасыз ету" атауын қолайсыздау деп санайды, өйткені құқық құқықтық құралдар арқылы тек құқықтық ғана емес, кез келген киберқауіпсіздікті (техникалық, технологиялық және ұйымдастырушылық) қамтамасыз ету мәселелерін де реттеп отырады. Мақалада жалпы ғылыми, жеке ғылыми және басқа да: әлеуметтану, тарихи, формальды-логикалық, салыстырмалы-құқықтық зерттеу әдістері қолданылды. Нормативтік құқықтық базаны халықаралық құқық нормалары, отандық және халықаралық заң тәжірибелерінің жарияланған және жарияланбаған материалдары, халықаралық және ақпараттық құқық саласындағы авторлық эмпирикалық зерттеулер құрады. Киберқауіпсіздікті қамтамасыз ету саласындағы заң технологиясының негізгі элементтерін: стратегия мен тактиканы, заң техникасын (құралдар жиынтығы ретінде) және ресурстармен қамтамасыз етуді, сыртқы және ішкі (іс жүргізудегі) нысандары мен режимдерін зерттеу қорытындылары бойынша киберқауіпсіздік құқығының ерекшеленуі және жүйелі дербестігі туралы қорытынды жасауға болады. Қарастырылған ұстанымдарды ескере отырып, халықаралық ақпараттық құқықтың тәуелсіз институты ретінде киберқауіпсіздік құқығы туралы айтуға болады.

Кілт сөздер: киберқауіпсіздік, киберқауіпсіздік заңының қайнар көздері, ақпараттық қауіпсіздік, ақпараттық заң, ақпараттандыру, цифрландыру, электрондық цифрлық қолтаңба, интернет, жеке деректерді қорғау.

M.S. Bissaliyev, K.N. Shakirov

Characteristic of the sources of international law in cybersecurity

Information law, which includes cybersecurity in international relations as its main component, is a relatively new area of legal research, the required doctrinal level of which has not been achieved today on all the issues it raised. We believe that the name “legal support of cybersecurity” is hardly appropriate, since the law regulates the issues of any provision of cybersecurity (technical, technological and organizational), and not only legal, albeit exclusively by legal means. In this work general scientific, specific scientific and other research methods were used, such as sociological, historical, formal logical, comparative legal. The normative legal base was formed by the norms of international law, published and unpublished materials of domestic and international legal practice, author's empirical research in the field of international and information law. The conclusion about the isolation and systemic independence of cybersecurity law can also be reached based on the results of the study of the main elements of legal technology in the field of cybersecurity: strategy and tactics, legal framework and resource availability, external and internal (procedural) forms and types. Taking into account the above positions, it is quite possible to talk about the law of cybersecurity as an independent institution of international information law.

Keywords: cybersecurity, sources of cybersecurity law, information security, information law, informatization, digitalization, electronic digital signature, Internet, personal data protection.

References

1 Maksurov, A.A. (2019). Sootnoshenie obshchepriznannykh printsipov mezhdunarodnogo prava i obshchepriznannykh norm mezhdunarodnogo prava [Correlation between generally recognized principles of international law and generally recognized norms of international law]. *Vestnik Yuzhnogo federalnogo universiteta — Bulletin of the Faculty of Law of the Southern Federal University, 3, 49–51*. Rostov-na-Donu [in Russian].

2 Vseobshchaia deklaratsiia prav cheloveka ot 10 dekabria 1948 goda [Universal Declaration of Human Rights of 10 December, 1948]. *un.org.* Retrieved from https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml [in Russian].

3 Mezhdunarodnyi pakt o grazhdanskikh i politicheskikh pravakh ot 16 dekabria 1966 goda [International Covenant on Civil and Political Rights of 16 December, 1966.] *un.org.* Retrieved from https://www.un.org/ru/documents/decl_conv /conventions/pactpol.shtml [in Russian].

4 Evropeiskaia konventsiia o zashchite prav cheloveka i osnovnykh svobod ot 4 noiabria 1950 goda [European Convention on Human Rights of 4 November, 1950]. *coe.int.* Retrieved from https://www.coe.int/ru/web/compass/the-european-convention-on-human-rights-and-its-protocols [in Russian].

5 Konventsiia o zashchite fizicheskikh lits pri avtomatizirovannoi obrabotke personalnykh dannykh ot 28 yanvaria 1981 goda [Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January, 1981]. *pd.rkn.gov.ru.* Retrieved from https://pd.rkn.gov.ru/law/document170.htm [in Russian].

6 Prikaz ministra oboronnoi i aierokosmicheskoi promyshlennosti Respubliki Kazakhstan ot 13 marta 2018 goda № 38 / NK «Ob utverzhdenii Pravil registratsii, polzovaniia i raspredeleniia domennykh imen v prostranstve kazakhstanskogo segmenta Interneta» [Order of the Minister of Defense and Aerospace Industry of the Republic of Kazakhstan dated March 13, 2018 No. 38 / NK «On approval of the Rules for registration, use and distribution of domain names in the space of the Kazakhstani segment of the Internet»]. *online.zakon.kz.* Retrieved from https://online.zakon.kz/document/? doc_id=35205534 [in Russian].

7 General Data Protection Regulation of April 27, 2016 [General Data Protection Regulation of 27 April, 2016]. *gdpr-info.eugdpr-info.eu.* Retrieved from https://gdpr-info.eu/.

8 Mikele de Salvia. (2004). *Evropeiskaia konventsiia po pravam cheloveka [European Convention on Human Rights]*. Saint-Petersburg: Yuridicheskii tsentr «Press» [in Russian].

9 Maksurov, A.A. (2020). *Obshchepriznannye printsipy i normy mezhdunarodnogo prava: poniatie i problemy primeneniia v Rossiiskoi Federatsii [Generally recognized principles and norms of international law: the concept and problems of application in the Russian Federation]*. Moscow: INFRA-M [in Russian].

10 Zakon Respubliki Kazakhstan ot 7 marta 2002 goda N 300 «O ratifikatsii popravochnykh dokumentov k Ustavu i Konventsii Mezhdunarodnogo soiuza elektrosviazi» [Law of the Republic of Kazakhstan dated March 7, 2002 No. 300 «On ratification of the Amendment documents to the Charter and Convention of the International Telecommunication Union"]. *adilet.zan.kz.* Retrieved from https://adilet.zan.kz/rus/docs/Z020000300_ [in Russian].

11 Ustav Mezhdunarodnogo soiuza yelektrosviazi 1994 goda [Statute of the International Telecommunication Union of 1994]. *itu.int.* Retrieved from https://www.itu.int/en/council/2019/Documents/basic-texts/Constitution-R.pdf [in Russian].

12 Okinawa Charter of the Global Information Society of 22 June, 2000. *docs.cntd.ru.* Retrieved from https://docs.cntd.ru/document/901770887.

13 Soglashenie stran SNG ot 21 noiabria 1994 goda «Ob obmene pravovoi informatsiei» [Agreement of the CIS countries of November 21, 1994 «On the exchange of legal information"]. *normativ.kontur.ru.* Retrieved from https://normativ.kontur.ru/document? moduleId=1&documentId=13378 [in Russian].

14 Pravila povedeniia v oblasti obespecheniia mezhdunarodnoi informatsionnoi bezopasnosti ot 14 sentiabiia 2011 goda [Rules of Conduct in the Field of International Information Security of September 14, 2011]. *digitallibrary.un.org.* Retrieved from https://digitallibrary.un.org/record/786846/files/A_69_723-RU.pdf? version=1 [in Russian].

15 Resolutions on Information Affairs. 35th Session of the Council of Foreign Ministers. *oic-oci.org.* Retrieved from https://www.oic-oci.org/docdown/? docID=427&refID=30

16 Strategiia Kollektivnoi bezopasnosti organizatsii dogovora o kollektivnoi bezopasnosti na period do 2025 goda ot 18 oktiabria 2016 goda [The Collective Security Strategy of the Collective Security Treaty Organization for the period up to 2025 dated October 18, 2016]. *odkb-csto.org.* Retrieved from https://odkb-csto.org/documents/statements/strategiya_kollektivnoy_ bezopasnosti_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_na_period_do_/ [in Russian].

17 Zakon Respubliki Kazakhstan ot 7 yanvaria 2003 goda N 370 «Ob elektronnom dokumente i elektronnoi tsifrovoi podpisi» [Law of the Republic of Kazakhstan dated January 7, 2003 N 370 «On electronic document and electronic digital signature"]. *online.zakon.kz.* Retrieved from https://online.zakon.kz/document/? doc_id=1035484 [in Russian].

18 Case: Nicholas Prestige Homes v Neal (2010). *casemine.com.* Retrieved from https://www.casemine.com/judgement/uk /5a8ff70660d03e7f57ea603b

19 Electronic Communications Act 2000. *legislation.gov.uk.* Retrieved from https://www.legislation.gov.uk/ukpga/2000/7/pdfs /ukpga_20000007_en.pdf

20 Computer Misuse Act 1990. *legislation.gov.uk*. Retrieved from https://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_ 19900018_en.pdf

21 Data Protection Act 1998. Retrieved from https://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf

22 The Privacy and Electronic Communications (EC Directive) Regulations 2003. *legislation.gov.uk.* Retrieved from https://www.legislation.gov.uk/uksi/2003/2426/pdfs/uksi_20032426_en.pdf

23 Kosseff, Jeff. (2017). Defining Cybersecurity Law. *Iowa: Iowa Law Review, 103, 985*.

24 Kilovaty Ido Privatized Cybersecurity Law. (2019). California: UC Irvine Law Review, 1181.

25 Kostylev, A.K. (2010). *Informatsionnoe pravo [Information Law]*. Tiumen: Izdatelstvo Tiumenskogo gosudarstvennogo universiteta [in Russian].

26 Poljakova, T.A. (2008). Pravovoe obespechenie informatsionnoi bezopasnosti pri postroenii informatsionnogo obshchestva v Rossii [Legal support of information security when building an information society in Russia]. *Doctor's thesis.* Moscow [in Russian].

27 Lopatin, V.N. (2000). Informatsionnaia bezopasnost Rossii [Information security of Russia]. *Doctor's thesis.* Saint-Petersburg [in Russian].

28 Bachilo, I.L. (2019). *Informatsionnoe pravo [Information Law]*. Moscow: Yurait [in Russian].

29 Kopylov, V.A. (2002). *Informatsionnoe pravo [Information Law]*. Moscow: Yurait [in Russian].

30 Kuznecov, P.A. (2005). Teoreticheskie osnovaniia informatsionnogo prava [Theoretical foundations of information law]. *Doctor's thesis.* Saint-Petersburg [in Russian].

31 Andreev, P.G. (2012). Institutsionalnoe razvitie pravovogo obespecheniia informatsionnoi bezopasnosti v rossiiskom informatsionnom prave [Institutional development of legal support for information security in Russian information law]. *Doctor's thesis*. Ekaterinburg [in Russian].

32 Strelcov, A.A. (2004). Teoreticheskie i metodologicheskie osnovy pravovogo obespecheniia informatsionnoi bezopasnosti Rossii [Theoretical and methodological foundations of legal support of information security in Russia]. *Doctor's thesis.* Moscow [in Russian].

33 Efremova, M.A. (2014). Informatsionnaia bezopasnost kak obekt ugolovno-pravovoi okhrany [Information security as an object of criminal law protection]. *Informatsionnoe pravo — Information Law, 5, 21–25* [in Russian].

34 Tereshhenko, L.K. & Tiunov, I.T. (2015). Informatsionnaia bezopasnost organov ispolnitelnoi vlasti na sovremennom etape [Information security of executive authorities at the present stage]. *Zhurnal rossiiskogo prava — Journal of Russian Law, 8, 224,* 100–109 [in Russian].

35 Rassolov, I.M. (2017). *Informatsionnoe pravo [Information Law]*. Moscow: Yurait [in Russian].