МРНТИ 04.11.91

Н.Е. Хамитова,
А.Е. Белялова
Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
*(E-mail: khamitovanaz@gmail.com, aigerim.belyalova@*kaznu*.edu.kz)*

Южнокорейские национальные подходы к управлению информационными данными

Аннотация. *В этой статье рассматривается основная политика Южной Кореи, связанная с онлайн-аутентификацией и контролем доступа к данным. Анализируются движущие силы этой политики, такие, как политика Южной Кореи в области информационно-коммуникационных технологий, инциденты в области кибербезопасности, политика в области кибербезопасности. Представлены особенности развития процесса онлайн-аутентификации и затронуты проблемы контроля доступа к данным. Рассматриваются цифровые новые проекты Южной Кореи, направленные на развитие цифрового общества.*

Цифровая среда Южной Кореи - одна из передовых в мире. Цифровизация общества еще более усилилась с разделением общества на до и после пандемии Covid-19, которая показала уровень развития каждого государства в сфере цифровых технологий. Элементом успешного продвижения политики цифровизации Южной Кореи стали национальные подходы и кибербезопасность.

В заключение излагается важность развития цифровой среды по определенной специфичной для страны модели, и она рассматривается как важный современный инструмент в процессе реализации развития цифровой среды.

Ключевые слова: *цифровое пространство, цифровые технологии, информатизация общества, Южная Корея, кибербезопастность, цифровые данные, интернет.*

DOI: https://doi.org/10.32523/2616-6887/2023-143-2-232-240
Поступила: 11.11. 2022 / Одобрена к опубликованию: 10.02.2023

Введение

На сегодняшний день мир настолько сильно быстро меняется, что человек не успевает за всеми этими переменами преуспевать и добиться успеха. Этот эффект является результатом развития информационно-коммуникационных технологий и создания цифровой среды мирового масштаба.

Возникновение глубоко укоренившегося, многоаспектного соперничества между США и Китаем заставил многих утверждать, что мир раскалывается на две сферы – китаецентричный порядок и американо-ориентированный. Предполагается, что одним из результатов этого может быть то, что Пекин устанавливает условия управления данными и Интернетом не только в пределах своей территории, а также технологические стандарты в азиатских странах и за их пределами. Однако факт заключается в том, что Соединенные Штаты и Китай – не единственные крупные цифровые игроки в мире [1].

Республика Корея является потенциальной целью для хакерских атак в силу высокого уровня информатизации общества, большого количества объектов интеллектуальной собственности и широкого использования мобильных устройств. По данным Мировой статистики интернета (англ.

Internet World Stats), количество интернет-пользователей в Южной Корее составляет около 47 млн (92,7% от общего населения страны), а число зарегистрированных пользователей социальной сети Facebook достигло 17 млн в 2017 г. Кроме того, Южная Корея является мировым лидером по скорости интернет-соединения, будучи единственным государством, средняя скорость интернета в котором превысила порог в 25 Мбит/с. и составляет 26,1 Мбит/с. Несмотря на то, что Южная Корея обладает высокоразвитыми информационными технологиями и активно осваивает интернет-пространство (став в 2005 г. первым в мире государством, полностью осуществившим переход от коммутируемого удаленного доступа в глобальную сеть к широкополосному), информационная инфраструктура страны остается весьма уязвимой перед кибератаками [2].

Кроме того, посредством применения цифровых коммуникационных технологий осуществляется целенаправленный подрыв социально-политической стабильности государств, выступающих в качестве геополитических оппонентов. Ведущие технологические площадки (Google, Facebook, Twitter, YouTube, Instagram и др.) при этом осуществляют, по сути, монополизацию цифрового пространства, предлагая миллиардам пользователей по всему миру достаточно ограниченный набор моделей социально-политической реальности, осуществляя при этом активную блокировку альтернатив (блокировка аккаунтов политиков, средств массовой информации и др. в Facebook, Instagram и Twitter, блокировка каналов на видеохостинге YouTube, блокировка доступа к информации по поисковым запросам Google и т.д.) [3].

Актуальность данной темы в том, что сейчас наблюдается распространение различных моделей политики и регулирования интернетом, и международное управление над ним становится все более востребованным, поскольку страны начинают экспериментировать, внедрять инновации и делиться своим политическим опытом и практикой, успехами и неудачами. Управление информационными цифровыми данными является одной из важнейших спорных областей, поскольку оно становится все более важным для следующего поколения, и многим экономическим и политическим областям в мире. Такие страны, как Южная Корея, Япония, Китай разработали отличительные национальные подходы к управлению данными в цифровом мире. Ни одна из стран не стремится подражать или перенимать полностью американскую, а тем более китайскую политику и практику в области обработки данных. Следовательно, каждая страна пытается изо всех сил быть не только просто лидером этой сферы, но и хотят иметь уникальную своеобразную систему цифрового пространства.

Методология исследования

Методологическую основу статьи составляют, во-первых, дескриптивный метод исследования: анализ зарубежной литературы и источников по концепции «цифровая среда», «цифровое правительство», «цифровые данные»; во-вторых, изучение литературы с применением этнокультурного подхода и анализа; в-третьих, путем диахронного метода и метода актуализации объясняются реальные возможности цифровых технологий и их риски.

В статье используются социологические, политологические, экономические и культурологические работы, которые опубликованы по теме данной статьи, а также книги и материалы периодических печатей. На основе анализа литературы дается заключение важности и актуальности темы цифрового пространства в мире. Цель данной статьи заключается в выявлении роли и особенностей национальных подходов к цифровым данным в Южной Корее и показать актуальность ее изучения сейчас.

Обсуждение

Цифровая «девификация» потребительской культуры, ситуация, когда все больше и больше форм действий опосредуются цифровыми устройствами, делает акцент на динамичном и материальном, но все же недетерминированном влиянии цифровых технологий на потребление и потребительское поведение [4].

Южная Корея является самым развитым в области цифрового пространства страной в мире. Южнокорейские имеющиеся подходы в силу своей инновационности могут сформировать многообещающее цифровое будущее. Однако все же перед цифровым развитым южнокорейским правительством стоит решение таких важные задач, как:

- Создать уникальную экосистему онлайн-аутентификации.
- Интенсивная цифровизация всех отраслей общества, которая имеет возможность противостоять киберопасностям.
- Необходимость нормативно-правовых баз данных, которые согласуются с нормативно-правовой базой основных экономических партнеров страны.

В южнокорейском обществе существуют разногласия по поводу процесса развития киберпространства, относительно того, как наилучшим образом разрабатывать политику для интернета и цифровых технологий. Следовательно, это может вызвать то, что можно назвать "расстройством множественной политики", которая приводит к путанице как среди технологических компаний, так и среди пользователей технологий.

Процесс проб и ошибок не является единственной причиной цифрового успеха Южной Кореи. Страна также преуспела во внедрении конкретных технологий. Одним из примеров является внедрение широкополосного интернета в Южной Корее за последние тридцать лет. Сегодня южнокорейские компании входят в число мировых лидеров в области беспроводной широкополосной связи 5G. Информационно-коммуникационные технологии (ИКТ), особенно интернет и другие технологии становятся основой экономики и общества. Они позволяют отдельным лицам и организациям по всему миру подключаться, обмениваться информацией и сотрудничать. Они оказали сильное влияние на промышленность, политику и средства массовой информации. Пандемия коронавируса только ускорила переход бизнеса, образования, правительства и других основных видов деятельности в онлайн-мир, что потенциально имеет долгосрочные последствия. И именно пандемия ускорила процесс цифровизации на мировом масштабе.

Различные области в Южной Корее, включая ИКТ и кибербезопасность, изменились из-за пандемии коронавируса, которая разразилась в 2020 году. С бурным ростом дистанционной работы и онлайн-услуг, таких, как телемедицина (которую некоторые корейцы называют "untact" - новое слово, объединяющее "un" и "contact"). Зависимость страны от технологий ИКТ растет быстрее, чем когда-либо прежде. Правительство объявило о новом курсе в июле 2020 года, направленном на преодоление экономического спада после пандемии и изменение парадигмы всей экономики и общества. Корейский новый курс распространяется как на государственный (за исключением военных), так и на частный секторы и состоит из трех проектов: Цифровой новый курс, «Зеленый новый курс» и прочная система социальной защиты [5].

Несмотря на многие возможности цифровых технологий, они также способствуют преступности: дезинформации, краже личной информации, конфиденциальной деловой информации и кибератакам. ИКТ-компании стремятся устранить такие киберпреступления в своем программном обеспечении и пытаются сопротивляться злоумышленникам, которые постоянно находят новые способы использования эти уязвимости. Установить личность и доверие в интернете гораздо сложнее, чем при личном общении, в результате чего в мошенничестве с личными данными пользователь может потерять многое. Пользователи цифровых технологий требуют лучших и более простых методов онлайн-аутентификации и контроля доступа к данным. Подход южнокорейского правительства к онлайн-аутентификации и контролю доступа к данным показывает несколько уникальных характеристик всех сфер развития страны. Страна инвестировала значительные средства в инфраструктуру ИКТ в качестве национального приоритета, создавая широкополосные сети и расширяя их охват практически в каждом южнокорейском доме. При средней скорости фиксированной широкополосной связи более 200 мегабит в секунду, широкополосные сети страны создали мощную платформу для инноваций. Южная Корея не является единственной страной, которая сталкивается с враждебной внешней средой. Другие страны, такие, как Эстония, Тайвань, США, Китай также сталкиваются с острой киберугрозой со стороны угрожающих соседей, также вложили значительные средства в кибербезопасность. Однако масштабы киберпреступности и безопасности имеют свои отличия в силу политико-экономической ситуации страны.

Процесс развития ИКТ Южной Кореи опирается на исторический опыт и практику, которые являются уникальными для траектории развития страны с 1960-х годов. В

течение этого десятилетия страна приступила к стремительной индустриализации, которая включала систему идентификации личности на национальном уровне, ставшая особенно важной, поскольку экономика страны начала переходить в онлайн в последующие десятилетия. Более того, Южная Корея создала и внедрила инфраструктуру аутентификации национального уровня под названием Авторизованный сертификат на основе инфраструктуры национальных открытых ключей (АС на основе NPKI), превосходящую многие другие сертификаты. К сожалению, с сертификатом возникло несколько проблем, поскольку он сложен в использовании и зависит от единой технологической платформы. В результате использование этих средств идентификации и аутентификации методы были ограничены, и правительству пришлось ввести альтернативные методы [1].

В основном подход Южной Кореи к доступности данных был консервативным. Однако сегодня ситуация меняется, благодаря четкому признанию государственными чиновниками, руководителями корпораций и гражданами необходимости более гибкой, открытой политики, отражающей социальные требования и изменения в деловой современной среде.

В дополнение к быстрому экономическому росту Южной Кореи и так называемой культуре “ппалли ппалли” (быстрее, быстрее), географические и демографические преимущества и проводимая правительством политика были основными факторами в его развитии в области ИКТ. В 1970-х годах национальная инициатива в области государственного управления привела к созданию системы регистрации резидентов и компьютеризации административной информации. В 1980-х годах была проведена политика распространения и расширения телекоммуникационных сетей. В 1990-х годах были разработаны сверхскоростные информационно-коммуникационные сети. И в 2000-х годах переход к информационному обществу привел к развитию и распространению интернет-технологий, заложив основу для электронных государственных услуг и улучшив информационную безопасность. Наиболее сложной проблемой, касающейся доступа к данным в частном секторе, является использование личной информации. Следовательно южнокорейскому правительству пришлось найти и принять путь, отражающий ее национальные условия. Сегодня корейские правила, касающиеся персональных данных, похожи на правила европейского образца, в которых подчеркивается защита в виде подробных положений, ограничивающих сбор и несанкционированное использование личной информации, позволяющей установить личность. На заре развития ИКТ в стране не было нормативных актов, касающихся личной информации. Всерьез эта проблема была решена только в 2001 году путем пересмотра Закона о содействии развитию ИКТ, который теперь называется Законом о содействии использованию информационно-коммуникационных сетей и защите информации [1].

В прошлом публичные данные в Южной Корее обрабатывались и управлялись правительством, которое гарантировало право общественности знать посредством запросов о раскрытии информации. В 1996 году был принят Закон о раскрытии информации общественными организациями для определения прав и форм публичных запросов о раскрытии информации, находящейся в распоряжении государственных учреждений. Этот закон направлен на обеспечение права общественности на информацию, участия граждан в национальных делах и прозрачности правительства. Запросы о раскрытии информации в государственных учреждениях были обработаны Национальным архивом Записи, начиная с 2004 года, и запросы на раскрытие информации увеличивались с каждым годом, демонстрируя устойчивый рост со 104 024 в 2004 году до 756 342 в 2016 году. В среднем уровень принятия раскрытия информации поддерживается на уровне около 95 % каждый год [1].

Для осуществления контроля за доступом к публичным данным правительство предприняло различные усилия, такие, как создание системы управления, управление доступностью и обеспечение доступности. В 2002 году был создан Специальный комитет по электронному правительству, который ввел политику внедрения и создания услуг электронного правительства. Южнокорейское правительство старается формировать определенные агентства и организации по недопущению ущерба политики развития цифрового общества, что строго контролирует соблюдение всех норм и правил использования ИКТ.

Одной из первых организаций в сфере защиты информационного пространства в публичном секторе является центр интернет-безопасности KrCERT, созданный в конце 1990-х годов при Агентстве информационной безопасности Республики Корея (ныне — Агентство интернет-безопасности Республики Корея) и начавший активную деятельность в начале 2000-х годов. Основная сфера ответственности KrCERT — это противодействие DDoSатакам: центр проводит круглосуточный мониторинг DDoS-угроз и предотвращает распространение вредоносного кода [6].

Таким образом, несмотря на то, что Интернет в 1990-е годы только начал набирать обороты, государство было сильно заинтересовано в правильности реализации политики построения цифрового пространства в стране.

В 2004 году был подготовлен план создания и продвижения проекта ISP, связанного с интегрированной вычислительной средой. В 2005 году в Тэджоне при Министерстве информации и коммуникаций (MIC) был создан Правительственный интегрированный вычислительный центр. Правительство интегрировало вычислительную технику. Центр был переименован в Национальную службу управления информационными ресурсами в 2017 году [1].

В целом правительственная политика начинала набирать активные обороты по защите цифровых данных с помощью принятия и формирования специальных агентств, которые, в свою очередь, имели главную цель в создании прочного фундамента защиты цифровых данных страны.

В 2008 г. было расформировано Министерство информации и связи, и его функции в области информационной безопасности были распределены между Комиссией по связи, Министерством общественной администрации и безопасности (ныне – Министерство внутренних дел и безопасности). В июле 2013 г. были приняты «Меры по обеспечению государственной кибербезопасности» – последний на сегодняшний день документ, в котором предпринимается попытка комплексно отразить государственную политику по кибербезопасности, направленную на построение продвинутой системы защиты информационного пространства страны [2].

В 2004 году корейское правительство инициирует переход к новому этапу цифровой революции, предполагающему доступ к информации в любое время и любом месте. Этот этап связывают с проектом «u-Korea vision». Для поддержания проекта корейское правительство разрабатывает новую национальную стратегию в области информационно-коммуникационных технологий – IT839 (восемь услуг, три инфраструктуры и девять технологий) [7].

Согласно плавному переходу страны на цифровые технологии, южнокорейское правительство было одним из первых стран, которое приняло проект «электронного правительства» в 1999 году. И на сегодняшний день результатом этого служат широкие удобства во многих сферах социальных услуг, начиная с банковских и заканчивая школьной системой.

На современном этапе изучения вопроса развития сервисной экономики заслуживает внимания достаточно масштабная работа M. Barrett, E. Davidson, J. Prabhu и S.L. Vargo, опубликованная в 2015 году. В статье проведен подробный структурированный обзор исследований по инновациям в сфере услуг в условиях развития информационно-коммуникационных технологий [8].

Защита и контроль являются необходимыми не только в сфере цифровых технологий, но и также в любой другой сфере. А в цифровых технологиях основной целью и уязвимым местом являются личные, секретные информации, данные, которые являются козырем злоумышленников. Следовательно, очень важно сформировать свою цифровую модель, которая поможет контролировать доступы к цифровым данным.

С принятием Закона о защите личной информации (PIPA) в 2011 году в Южной Корее была создана система регулирования личной информации. PIPA - это общий закон, регулирующий общие темы и защиту личной информации в Южной Корее, а Закон об ИКТ и безопасности конкретно регулирует OSP. Закон о защите кредитной информации конкретно регулирует деятельность финансовых учреждений. PIPA в широком смысле определяет личную информацию как информацию, которая сама по себе или в сочетании с другими информациями может быть использована для идентификации лица, связанного с этой информацией. В рамках

подготовки к Четвертой промышленной революции были выдвинуты требования об улучшении южнокорейских правил конфиденциальности. Соответственно, в январе 2020 года правительство пересмотрело поправки к так называемым трем законам о данных, чтобы улучшить защиту личной информации. Пересмотрев эти три закона, правительство ввело возможность использования неидентифицирующих персональных информаций и обеспечило социальный доступ к данным в расчете на то, что будут созданы новые коммерческие сервисы, такие, как MyData. Это универсальный сервис, основанный на переносимости данных, который был создан консорциумом промышленности и университетов для предоставления различной информации, связанной с финансами [1].

Один из исследователей цифрового пространства Расмус Эриксон отмечает, что Сеулу следует рассмотреть вопрос о ратификации Будапештской конвенции о киберпреступности в качестве первой меры по включению кибербезопасности в их продолжающийся диалог с ЕС. [9].

Представления об общественной информации также резко изменились в связи с появлением смартфонов и вызванным этим потоком данных и новых приложений. Ограничения на публичную информацию стали проблемой из-за увеличения числа приложений, получающих доступ к информации на смартфоне. Например, простое приложение для определения местоположения автобуса требовало правительственных данных в режиме реального времени. Для того, чтобы справиться с подобными проблемами, Южная Корея создала план содействия частному использованию публичной информации в 2010 году. В 2011 году были разработаны руководящие принципы предоставления услуг портала общественной информации и публичных данных, что привело к созданию проекта Government 3.0. – Базовый план и Закон о предоставлении и использовании общедоступных данных в 2013 году.

В 2016 году правительство разработало Базовый план электронного правительства до 2020 года, а также пять стратегий, отражающих социальные потребности, связанные с гиперактивностью использования Интернета обществом. Улучшение доступа к общедоступным данным стало возможным благодаря увеличению финансирования государственных ИТ-систем и переходу на облачные административные системы. В феврале 2021 года правительство учредило проект Data 119 и объявило о стратегии в области данных, направленной на оживление цифровой экономики путем поощрения использования открытых данных. Стратегия предусматривала внесение поправок и актуализацию так называемых поправок к трем законам о данных и запуск девяти новых служб передачи данных, а также обозначила одиннадцать практических задач, включая создание специального комитета по данным. Поправки к трем законам о данных относятся к поправкам к Закону о защите личной информации [1].

Заключение

Таким образом, южнокорейские меры, направленные на динамичное развитие цифровых технологий, имеют свои уникальности в том плане, что именно в сфере защиты и конфиденциальности хранения цифровых данных есть чему научиться многим мировым цифровым державам. Согласно анализу особенностей южнокорейской модели развития цифровых технологий можно выделить:

- Создание мощной цифровой инновационной платформы;
- Исторический южнокорейский опыт развития;
- Гибкий подход к новым инновационным изменениям;
- Географические и демографические особенности;
- Агентства по защите цифрового пространства, которые стали основным фундаментом цифровизации страны;
- Новые коммерческие цифровые сервисы;
- Ежегодное финансирование ИТ-систем южнокорейским правительством.

В 2022 году Южная Корея провела учения о кибербезопастности в онлайн-формате, которые охватили более 10 стран мира. К 2023 году планируется уже оффлайновые очные учения о кибербезопастности. Главной целью таких учений является сокращение технологического разрыва между странами и дать вместе отпор киберпреступности, происходящей в цифровом мире.

Список литературы

1. Jang Gye Hyun, Lim Jong In. Technologies of Trust: Online Authentication and Data Access Control in Korea. // Carnegie Endowment for International Peace. – 2021. – P. 11-39.
2. Волощак В.И. Проблемы развития национальной системы кибербезопасности Республики Корея // Проблемы Дальнего Востока. – 2018. – № 3. – С.117-125.
3. Володенков С.В. Феномен цифрового суверенитета современного государства в условиях глобальных технологических трансформаций: содержание и особенности // Политические исследования. – 2020. – С. 3-11.
4. Franck Cochoy, Christian Licoppe, Magdalena Petersson McIntyre & Niklas Sörum. Digitalizing consumer society: equipment and devices of digital consumption. // Journal of Cultural Economy. – 2020. – № 13. – P. 1-11
5. So Jeong Kim, Sunha Bae. Korean Policies of Cybersecurity and Data Resilience. // Carnegie Endowment for International Peace. – 2021. – P. 39-61
6. Шилинцева Е.В., Гарусова Л. Н. Кибербезопастность как основной фактор национальной безопасности в России и Республике Корея //Синергия наук. – 2020. –№ 46. – С. 220-230.
7. Койбаев Б.Г., Золоева З.Т. Правовые аспекты информатизации в Республике Корея // Гуманитарные и юридические исследования. – 2015. № 1. – С. 96-101.
8. Восколович Н.А. Особенности развития электронных услуг в цифровом обществе // Государственное управление. Электронный вестник. – 2018. − № 68. − С. 410–425.
9. Rasmus Eriksson. South Korea's Cybersecurity and International Cooperation. // Policy brief. – 2019. – № 8. – P. 1-3.

Н.Е. Хамитова, А.Е. Белялова
Әл-Фараби атындағы қазақ ұлттық университеті, Алматы, Қазақстан

Ақпараттық деректерді басқарудағы Оңтүстік Кореяның ұлттық ұстанымдары

Аңдатпа. Бұл мақалада Оңтүстік Кореяның онлайн аутентификация мен цифрлық деректерге қол жеткізуді бақылауға қатысты негізгі саясаты, олардың негізгі өзгерістері мен себептері қарастырылады. Оңтүстік Кореяның ақпараттық-коммуникациялық технология саясаты, киберқауіпсіздік саясаты сияқты қозғаушы күштері талданады. Онлайн аутентификация процесінің даму ерекшеліктері ұсынылған және цифрлық деректерге қол жеткізуді бақылау мәселелері қозғалған. Оңтүстік Кореяның цифрлық қоғамды дамытуға бағытталған цифрлық жаңа жобалары қарастырылады.

Оңтүстік Кореяның цифрлық ортасы әлемдегі ең озық орталардың бірі болып табылады. Қоғамды цифрландыру қоғамның covid-19 пандемиясына дейін және одан кейін бөлінуімен одан әрі күшейе түсті, бұл цифрлық технологиялар саласындағы әрбір мемлекеттің даму деңгейін көрсетті. Оңтүстік Кореяның цифрландыру саясатын табысты ілгерілетудің элементі ұлттық тәсілдер мен киберқауіпсіздік болып табылады.

Қорытындылай келе, елге тән белгілі бір модель бойынша цифрлық ортаны дамытудың маңыздылығы баяндалады және ол бірегей цифрлық ортаны дамытуды жүзеге асыру процесінде маңызды заманауи құрал ретінде қарастырылады.

Түйін сөздер: Сандық кеңістік, цифрлық технологиялар, қоғамды ақпараттандыру, Оңтүстік Корея, киберқауіпсіздік, цифрлық деректер, Интернет.

N.Ye. Khamitova, A.Ye. Belyalova
Al Farabi Kazakh National University, Almaty, Kazakhstan

South Korea's national approaches to information data management

Abstract. This article examines South Korea's main policy related to online authentication and data access control, having major changes and the reasons behind them. It analyzes the driving forces of this policy such as Korea's ICT policy, cybersecurity incidents, and cybersecurity policy. It presents the features of the development of the online authentication process and touches upon the problems of data access control. The article considers digital new projects of South Korea aimed at the development of a digital society.

South Korea's digital environment is one of the most advanced ones in the world. The digitalization of society has intensified even more with the division of society into before and after the Covid-19 pandemic, which showed the level of development of each state in the field of digital technology. National approaches and cybersecurity have become an element of the successful promotion of South Korea's digitalization policy.

In conclusion, the importance of developing the digital environment according to a certain country-specific model is outlined, and it is considered as an important modern tool in the process of implementing the development of a unique digital environment.

Keywords: Digital space, digital technologies, informatization of society, South Korea, Cybersecurity, Digital data, Internet.

References

1. Jang Gye Hyun, Lim Jong In. Technologies of Trust: Online Authentication and Data Access Control in Korea. Carnegie Endowment for International Peace. 2021. P. 11-39.
2. Voloshak V.I. Problemy razvitiya natzionalnoi sistemy kiberbezopstnosti Respubliki Koreya [Problems of development of the national cybersecurity system of the Republic of Korea], Problemy Dalnego Vostoka [Problems of the Far East], 2018. No.3. P.117– 125. [in Russian].
3. Volodenkov S. V. Fenomen tzifrovogo suvereniteta sovremennogo gosudarstva v usloviyahglobalnyh tehnologicheskih transformarzii: soderzhaniye b osobennosti [The phenomenon of digital sovereignty of a modern state in the context of global technological transformations: content and features], Politicheskiye issledovaniya [Political Studies], 2020. P. 3–11. [in Russian].
4. Franck Cochoy, Christian Licoppe, Magdalena Petersson McIntyre. Niklas Sörum. Digitalizing consumer society: equipment and devices of digital consumption. Journal of Cultural Economy. 2020. No.13. P. 1-11.
5. Kim S.J., Bae S. Korean Policies of Cybersecurity and Data Resilience. Carnegie Endowment for International Peace. 2021. P. 39-61.
6. Shilintseva Ye.V., Garusova L.N. Kiberbezopastnost kak osnovnoi faktor natzionalnoi bezopstnosti v Rossii i Respublike Koreya [Cybersecurity as the main factor of national security in Russia and the Republic of Korea], Mezhdunarodyi nauchnyi zhurnal "Sinegeriya nauk" [Synergy of Sciences International Scientific Journal], 2020. No.46. P.220–230. [in Russian].
7. Koibayev B.G., Zoloyeva Z.T. Pravovye aspekty informatizatzii v Respublike Koreya [Legal aspects of informatization in the Republic of Korea], Gumanitarniye I uridicheskiye issledovaniya [Humanitarian and Legal Studies], 2018. No. 1. P. 96 –101. [in Russian].
8. Voskolovich N.A. Osobennosti razvitiya elektronnyh uslug v tsifrovom obshchestve [Features of the development of electronic services in a digital society], Gosudarstvennoe upravlenie. Elektronnyj vestnik [Public Administration. Electronic Bulletin], 2018. No.68. P.410 – 425. [in Russian].
9. Eriksson R. South Korea's Cybersecurity and International Cooperation. Policy Brief. 2019. No. 8. P. 1-3.

Сведения об авторах:

Хамитова Назерке Ермековна – 1 курс докторанты, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан.

Белялова Әйгерім Ермекқызы – Қиыр Шығыс кафедрасының PhD педагогика ғылымдарының докторы, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан.

Хамитова Назерке Ермековна – докторант 1 курса кафедры Дальнего Востока, Казахский национальный университет им. аль-Фараби, Алматы, Казахстан.

Белялова Айгерим Ермековна – Ph.D., доктор педагогических наук, кафедра Дальнего Востока, Казахский национальный университет им. аль-Фараби, Алматы, Казахстан.

Khamitova Nazerke Yermekovna – 1st year PhD student of the Department of the Far East, Al-Farabi Kazakh National University, Almaty, Kazakhstan.

Belyalova Aigerim Yermekovna – PhD, Doctor of Pedagogical Sciences of the Department of the Far East, Al-Farabi Kazakh National University, Almaty, Kazakhstan.