ЧЕЛОВЕЧЕСКИЙ ФАКТОР

УДК 341.17 DOI: 10.31249/snsn/2023.03.08

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ЭЛЕМЕНТ ИНТЕГРАЦИИ В РАМКАХ ЕАЭС

Ермак Кристина Андреевна[1]

Ведущий сотрудник-администратор Центра анализа и прогнозирования союзных интеграционных процессов, Минск, Беларусь,
e-mail: kristina.ermak, 2102@mail.ru

Аннотация. *В статье рассматриваются предпосылки для создания системы противодействия информационным и киберугрозам Евразийского экономического союза (ЕАЭС) в качестве условия и элемента региональной интеграции в текущем контексте глобальных трансформаций мирового порядка. Показан российский и зарубежный опыт в данной области. Анализируется потенциал государств – членов ЕАЭС и результаты их двустороннего и многостороннего взаимодействия в сфере обеспечения информационной безопасности как значимой составляющей цифровой повестки Союза. Обозначаются направления, которые в будущем могут стать основой Стратегии информационной безопасности ЕАЭС и позволят противостоять новым вызовам современного информационного пространства.*

Ключевые слова: *информационная безопасность; кибербезопасность; информационное пространство; региональное сотрудничество; ЕАЭС; цифровая повестка; интеграция.*

Для цитирования: Ермак К.А. Информационная безопасность как элемент интеграции в рамках ЕАЭС // Социальные новации и социальные науки. – 2023. – № 3. – С. 132–142.

URL: https://sns-journal.ru/ru/archive/ DOI: 10.31249/snsn/2023.03.08

Рукопись поступила 27.05.2023.
Принята к печати 10.08.2023.

Введение

В условиях современных глобальных трансформаций системы международных отношений переосмысление угроз миру и безопасности, а также переоценка подходов к борьбе с ними входят в число стратегических задач современных государств. В свою очередь, вовлеченность стран в процессы интеграционного строительства открывает пространство возможностей для укрепления национального и интеграционного потенциалов во многих областях, начиная от социально-экономической и политической и заканчивая информационной областью, обеспечение устойчивости которой может стать мощной опорой для формирования эффективных интеграционных структур.

Вопросы информационной безопасности заняли центральное место в повестке дня международных организаций на глобальном и региональном уровнях. Активная работа в этом направлении ведется и в рамках интеграционных объединений евразийского пространства, таких как Евразийский экономический союз (ЕАЭС), Союзное государство, Содружество Независимых Государств (СНГ), Организация Договора о коллективной безопасности (ОДКБ), Шанхайская организация сотрудничества (ШОС), Ассоциация государств Юго-Восточной Азии (АСЕАН) и БРИКС. ЕАЭС, являющийся одним из наиболее успешных и стремительно развивающихся проектов евразийского интеграционного строительства, нуждается в расширении содержания союзной повестки в области информационной безопасности.

Концептуально-правовые основы информационной безопасности: международный опыт

Спектр глобальных вызовов расширился, включив с свою орбиту новые угрозы, связанные с применением информационных технологий (ИТ). В последние десятилетия многочисленные инциденты, нарушающие функционирование информационного пространства, доказали, что отсутствие должной регулятивной базы – прямая угроза существованию государства как такового [Joubert, 2010].

В последующие годы эти выводы нашли свое подтверждение в высказываниях и публикациях представителей элит и экспертного сообщества США. Еще в 1993 г. Джон Аркилла и Дэвид Ронфельд, сотрудники американского исследовательского центра РЭНД (англ. RAND (research and development) Corporation), отметили связь между информационной революцией и военной стратегией. В своем исследовании эксперты обозначили позицию, согласно которой распространение ИТ может оказать существенное влияние на природу международных конфликтов [Arquilla, Ronfeldt, 1993].

Годом позднее политолог Майкл Маззар выступил на ежегодной конференции Института стратегических исследований американского военного колледжа (U.S. Army War College) с докладом, в котором он обосновывал концепцию «Revolution in Military Affairs» (RMA), подразумевающую достижение прогресса в военном деле посредством активного вовлечения информационно-технологического потенциала [Mazarr, 1994]. В основе концепции лежало положение об информационном доминировании, которое было взято на вооружение оборонным ведомством США, что стало ключом к реализации теоретических разработок на практике не только в американской, но и в международной информационной среде.

Обращаясь к информационной проблематике, следует учитывать многочисленность трактовок понятий «кибербезопасность» и «информационная безопасность» в зарубежном и российском дискурсах. Исходя из дефиниций западных правовых документов, между данными понятиями проводится четкое разграничение: «кибербезопасность» охватывает безопасность серверов и сетевых ресурсов [National Cyber Strategy … , 2018], а «информационная безопасность» затрагивает более широкий спектр вопросов распространения информации и управления информационными потоками.

Официальное определение понятия «кибербезопасность» в государственных нормативных правовых актах Российской Федерации отсутствует, но активно используется в научной среде, в основном как синоним «информационной безопасности». Последняя, однако, является концепцией с более комплексным содержанием, поэтому получила широкое распространение в доктринальных документах РФ, в которых во главу угла ставится обеспечение безопасности данных в любом информационно-цифровом формате от внешних рисков и угроз [Указ Президента … , 2016]. Аналогичный подход как в доктринальных документах, так и в практическом поле использует Китай.

В КНР разработка подходов к обеспечению безопасности в информационной сфере началась в конце 1990-х годов. В 1994 г. на национальном уровне был принят первый документ – Правила регулирования, обеспечивающие безопасность компьютерных и информационных систем; в 1997 г. – Закон о безопасности сетевой инфраструктуры и сети Интернет. Наиболее прогрессивным актом стал Закон о кибербезопасности, который вступил в силу 1 июня 2017 г. [Рогожин, 2017]. Примечательными являются два элемента китайской политики в области информационной безопасности: приоритет обеспечения социальной стабильности и контроля внутригосударственных процессов; экономический и промышленный шпионаж против иностранных компаний и предприятий [Стратегия Китая … , 2020].

Создание ШОС придало импульс согласованию коллективного подхода к вопросам информационной безопасности. Опубликованное в 2006 г. заявление Совета глав государств – членов ШОС по международной информационной безопасности [Заявление глав государств-членов ШОС … , 2006] положило начало активному взаимодействию в области информационной безопасности

по линии шанхайской организации. Стоит отметить, что этот позитивный опыт во многом предопределил шаги государств – членов ЕАЭС в данном направлении, что более детально будет изложено ниже.

Первым доктринальным документом, который заложил основы российского правового подхода, стала Доктрина информационной безопасности Российской Федерации в редакции от 9 сентября 2000 г. (далее Доктрина) [Доктрина информационной безопасности … , 2000]. По мере интенсификации и усложнения информационных процессов в 2016 г. ее содержание претерпело изменения [Указ Президента … , 2016]; в новой редакции были закреплены основные информационные угрозы, а также сформулирована стратегическая цель обеспечения информационной безопасности в области обороны. Впоследствии, в 2021 г., информационная безопасность нашла свое отражение и в виде стратегического приоритета в Стратегии национальной безопасности РФ (далее Стратегия) [Указ Президента Российской Федерации … , 2021]. Общей целью обоих документов (Доктрины и Стратегии) было провозглашено обеспечение суверенитета страны в информационном мировом пространстве.

Российская Федерация стала государством – инициатором глобального обсуждения данного вопроса на уровне ООН, а также на иных региональных и двусторонних площадках [Бедрицкий, 2013]. Еще в 1998 г. Россией был подготовлен проект резолюции Генеральной Ассамблеи ООН (ГА ООН) «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», который был принят на 58-й сессии без голосования [Достижения в сфере информатизации и телекоммуникаций … , 2023]. Хотя резолюция не содержала конкретных указаний на возможность использования киберпространства в военных целях, а также мер по запрету создания и развития «информационного оружия», документ стал отправной точкой для начала обсуждения вопросов информационной безопасности в рамках ООН.

Как следует из вышеизложенных фактов, подходы к обеспечению информационной и кибербезопасности крупнейших мировых держав актуализируют информационную повестку не только на региональном, но и на глобальном уровнях. Позитивным трендом стало включение информационного измерения в повестку международных интеграционных объединений, ярким примером чего может служить Цифровая повестка ЕЭАС.

Цифровая повестка ЕАЭС как интеграционная платформа обеспечения информационной безопасности

Несмотря на то, что развитие интеграции в информационной сфере напрямую не закреплено в Договоре о ЕАЭС от 2014 г. (далее Договор) [Договор о Евразийском экономическом союзе, 2023], данное направление имеет статус самостоятельного вектора евразийской интеграции. С момента подписания Договора был предпринят ряд шагов, заложивших основу для дальнейших

практических действий в цифровой сфере. Так, в 2016 г. был запущен процесс обсуждения цифровой повестки среди стран – членов ЕАЭС, которая стала новой вехой в развитии интеграции региона. Фундамент союзной цифровой повестки заложили два документа: Заявление о Цифровой повестке ЕАЭС, подписанное 26 декабря 2016 г. главами государств-членов; а также Решение Высшего совета ЕАЭС об Основных направлениях реализации цифровой повестки ЕАЭС до 2025 г., принятое 11 октября 2017 г. [Заявление о цифровой повестке … , 2018 ; Об основных направлениях … , 2017]. В 2023 г. цифровая повестка стала приоритетным направлением председательства России в высших органах ЕАЭС.

Текущая цифровая повестка ЕАЭС включает в себя вопросы отраслевой трансформации союзной экономики, автоматизации процессов управления и адаптации рынков товаров, услуг, капитала и трудовых ресурсов к цифровым изменениям [Цифровая повестка ЕАЭС … , 2023]. Ее реализация с последующим созданием единого цифрового пространства является базисом для разработки общей Стратегии информационной безопасности Союза.

Несмотря на наличие консенсуса среди государств – членов ЕЭАС о необходимости обеспечения информационной безопасности евразийской интеграции, о чем свидетельствует работа по защите информационных систем в рамках Союза [Бороздин, Коварда, 2020], правовое закрепление стратегических целей и механизмов по их достижению находится на этапе становления, а перспектива формирования единого цифрового пространства не представляется достижимой в короткие сроки.

В 2016 и 2017 гг. было проведено совместное исследование Евразийской экономической комиссии (ЕЭК) и Группы Всемирного банка по изучению международного опыта развития цифрового пространства [Цифровая повестка Евразийского экономического союза … , 2018], в рамках которого были проанализированы национальные инициативы стран – членов ЕАЭС, а также опыт по формированию цифровой повестки стран АСЕАН, Совета сотрудничества арабских государств Персидского залива (ССАГПЗ) и ЕС. На основании проведенной работы были выработаны рекомендации по созданию единого цифрового пространства ЕАЭС. Важным выводом стало обоснование возможности внедрения цифровой повестки на региональном уровне без первичной адаптации цифровых механизмов к «национальному климату».

Цифровая повестка ЕАЭС по праву может рассматриваться как перспективное направление интеграционных процессов в рамках Союза, которое способно вывести евразийскую интеграцию на качественно новый уровень. Интеграционный потенциал цифровой повестки заключается не только в ускорении роста союзной и, как следствие, национальных экономик стран ЕАЭС, но и в разработке новых подходов и практик применения цифровых механизмов в различных областях взаимодействия. Однако для его реализации необходимо сформировать прочную нормативно-

правовую и институциональную базу, которая обеспечит информационную безопасность интеграции в рамках ЕАЭС.

Однако общая цифровая повестка не снимает вопросы защиты цифрового и информационного суверенитета стран – участниц ЕАЭС, которые также должны быть учтены в ходе дальнейшей разработки Стратегии информационной безопасности ЕАЭС. Неслучайно этот аспект закреплен в Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 г.: «Государства-члены самостоятельно разрабатывают, формируют и реализуют национальную политику в сферах цифровизации экономики, связи и информатизации, обеспечения устойчивого функционирования и безопасности единого информационного пространства и инфраструктуры связи, в том числе реализуют национальные мероприятия по развитию цифровой повестки» [Об основных направлениях … , 2017].

Цифровой суверенитет, который подразумевает «право государства самостоятельно формировать информационную политику, распоряжаться информационными потоками, обеспечивать информационную безопасность независимо от внешнего влияния» [Цифровой суверенитет, 2021], на сегодняшний день подвергается вполне реальным угрозам. В этой связи особый интерес приобретает концепция, разработанная в 2011 г. китайским профессором Фан Биньсином (более известным как «отец великого китайского файервола»), ядро которой составляют четыре принципа: полного контроля государства над собственным сегментом Интернета; защиты этого сегмента от вмешательства извне; равноправия в процессе использования интернет-ресурсов; недопустимости контроля сервисов доступа к национальным сегментам Интернета [Ковачич, 2019].

Показательным примером операционализации концепции цифрового суверенитета могут служить двусторонние усилия со стороны Российской Федерации и Китая по реализации мер обеспечения безопасности в информационном и киберпространстве на национальных уровнях. Так, в 2014 г. китайской стороной была впервые проведена Всемирная конференция по управлению Интернетом, в ходе которой был сделан ряд заявлений со стороны Председателя КНР Си Цзиньпина, в частности о правах каждого государства на суверенный Интернет [Селищев, 2019]. А в 2015 г. Китай документально закрепил общность подходов с Россией, заключив межправительственное соглашение о сотрудничестве в области обеспечения международной информационной безопасности. В качестве основной угрозы в соответствующей области в документе определено использование информационно-коммуникационных технологий «в гражданской и военной сферах в целях, несовместимых с задачами обеспечения международного мира, безопасности и стабильности, для подрыва суверенитета и безопасности государств и вмешательства в их внутренние дела, нарушения неприкосновенности частной жизни граждан, дестабилизации внутриполитической и социально-экономической обстановки, разжигания межнациональной и межконфессиональной вражды» [Соглашение между Правительством Российской Федерации … , 2016].

Также в документе содержится тезис о распространении государственного суверенитета на национальный сегмент интернет-пространства. Из результатов договоренностей следует, что оба государства рассматривают нарушение цифрового суверенитета как вмешательство во внутренние дела. Однако усиление интеграционной динамики ведет к необходимости экстраполировать опыт двустороннего взаимодействия на многосторонний уровень.

В региональном контексте защита цифрового суверенитета в качестве неотъемлемой составляющей информационной безопасности интеграционного объединения получила закрепление в Стратегии кибербезопасности Европейского Союза (ЕС) [The EU's Cybersecurity Strategy … , 2020]. Опыт ЕС, бесспорно, может быть полезен с точки зрения его адаптации для евразийского альянса.

В более широком ключе информационная безопасность представлена в Стратегии коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 г. [Стратегия коллективной безопасности … , 2016], а также в Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности [Соглашение о сотрудничестве … , 2015]. Определенные положения вышеприведенных документов могут быть доработаны и стать составляющими Стратегии информационной безопасности ЕАЭС, в том числе: а) выработка единых правил взаимодействия в сфере информационной безопасности с опорой на механизмы цифровой повестки; б) создание единого органа, координирующего межгосударственное сотрудничество по обеспечению информационной безопасности и реализации цифровой повестки; в) учреждение единого мониторингового центра, осуществляющего сбор и анализ данных о наличии информационных угроз различного характера; г) укрепление взаимодействия по линии ЕАЭС-ОДКБ-СНГ с целью обмена информацией и опытом для более эффективной деятельности по данному направлению.

Формы сотрудничества государств ЕАЭС в области информационной безопасности

Государствам ЕАЭС важно найти общий подход к обеспечению информационной безопасности на основе применения результатов двусторонних практик, учитывая разноскоростной характер интеграции между отдельными членами. Ярким примером служит Союзное государство, в числе результативных проектов которого союзные программы «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий», «Совершенствование системы защиты информационных ресурсов... в условиях нарастания угроз в информационной сфере ("Паритет")» и др. [Постановление Высшего Государственного Совета … , 2018]. Знаковым событием в процессе объединения усилий двух стран по противодействию информационным угрозам стало утверждение в марте 2023 г. Концепции информационной безопасности Союзного государства, в которой в качестве основной цели провозглашается защита нацио-

нальных интересов стран-партнеров в информационной сфере на основе повышения резистентности их информационных инфраструктур и борьбы с деструктивным воздействием на их информационные ресурсы [Об утверждении Концепции информационной безопасности … , 2023].

Учитывая опыт Союзного государства, не случайно, что Соглашение о сотрудничестве в области обеспечения международной информационной безопасности, подписанное Правительствами Беларуси и России в 2013 г. [Соглашение между Правительством Республики Беларусь … , 2015], предвосхитило развитие сети двусторонних контактов по линии информационной безопасности между странами ЕАЭС. В 2021 г. было подписано аналогичное соглашение между Правительствами России и Киргизии, закрепившее стремление сторон координировать позиции по ключевым вопросам и наращивать двустороннее взаимодействие путем реализации совместных инициатив [О подписании Соглашения между Правительством Киргизской Республики … , 2021]. В феврале 2022 г. Армения и Россия согласовали проект межправительственного Соглашения о сотрудничестве в области обеспечения информационной безопасности, которое вступило в силу 5 мая 2023 г. [Соглашение между Правительством Российской Федерации и Правительством Республики Армения … , 2023].

Кроме того, государства – члены ЕАЭС участвуют и по отдельности в ряде иных форматов обеспечения информационной безопасности. Так, Армения принимает участие в обеспечении международной информационной безопасности в рамках СНГ, ОДКБ, а также Будапештской конвенции о преступности в сфере компьютерной информации 2001 г. Беларусь, Казахстан и Кыргызстан вовлечены во взаимодействие в данной сфере со странами по линии ШОС, ОДКБ и СНГ. В дополнение к этим площадкам Россия осуществляет свою деятельность в рамках БРИКС.

Очевидно, что для своевременной реализации стратегических направлений формирования и развития цифрового пространства ЕАЭС до 2025 г. следует учитывать особенности регионального контекста [Стратегические направления формирования и развития … , 2023]. Будет справедливым отметить, что уровень обеспечения информационной безопасности в национальных масштабах стран Союза существенно различается вследствие многих факторов, в первую очередь неравномерного распространения цифровой культуры среди населения[1].

Наконец, аргументом в пользу создания единой системы информационной безопасности ЕАЭС служат и результаты международных исследований, свидетельствующие о повышении уровня опасности кибератак, противодействие которым потребует скоординированных действий членов Союза. Согласно данным Всемирного экономического форума за 2022 г., появляются но-

[1] Так, по данным лаборатории Kaspersky, в первую десятку стран, наиболее незащищенных от информационных атак, входят Таджикистан (1 место), Китай (3 место), Казахстан (8 место) и Узбекистан (9 место). Среди стран ЕАЭС Россия находится на 12 позиции, Кыргызстан занимает – 14, Беларусь – 35, а Армения – 47 место [Cyberthreat Real … , 2023].

вые вызовы, с которыми сталкиваются государства и их частные структуры в информационной среде [Global Cybersecurity Outlook … , 2022]. Угрозами, вызывающими особое беспокойство, признаны вредоносные программы-вымогатели, которые блокируют компьютер, а затем требуют «выкуп» за его разблокировку; инструменты социальной инженерии, способные продвигать определенные установки и стандарты поведения пользователей; вредоносная деятельность инсайдеров (частных лиц или корпораций) по раскрытию конфиденциальной информации коммерческих структур, краже информации и интеллектуальной собственности и пр. [Global Cybersecurity Outlook … , 2022]. Несмотря на то, что данные угрозы существуют в глобальном масштабе, принятие превентивных мер на уровне интеграционных объединений поможет предупредить риски их возникновения и принять соразмерные шаги по их купированию на начальных стадиях.

Заключение

На современном этапе мирового развития положительная экономическая и политическая динамика развития международных акторов во многом зависит от уровня разработанности и реализации их информационной / цифровой повестки. В этой связи лидерам стран – участниц ЕАЭС необходимо проявить политическую волю и готовность углублять интеграцию с опорой на транспарентный диалог и совместные усилия по преодолению цифровых препятствий.

В текущих условиях кардинальных трансформаций миропорядка происходят серьезные сдвиги в национальных приоритетах стран ЕАЭС и их партнеров. Однако для членов Союза представляется исключительно важным сохранение в новом международном контексте готовности инвестировать не только экономические, но и политические ресурсы в региональные интеграционные институты, обеспечение информационной безопасности и реализация цифровой повестки которых послужат новым импульсом для расширения основ евразийской интеграционной идеи.

Список литературы

1. Бедрицкий А. Международные договоренности по киберпространству: возможен ли консенсус? // Перспективы. Электронный журнал. – 2013. – 24.10. – URL: https://www.perspektivy.info/book/mezhdunarodnyje_dogovoronnosti_po_kiberprostranstvu_vozmozhen_li_konsensus_2013-10-24.htm (дата обращения 12.01.2023).
2. Бороздин А.Н., Коварда В.В. Анализ системы обеспечения защиты информации в процессе цифровизации ее оборота в рамках ЕАЭС в аспекте повышения экономической безопасности // Вестник Евразийской науки. – 2020. – Т. 12, № 4. – URL: https://esj.today/PDF/41ECVN420.pdf (дата обращения 12.01.2023).
3. Договор о Евразийском экономическом союзе (редакция, действующая с 3 апреля 2023 года) // Электронный фонд правовых и нормативно-технических документов. – 2023. – 03.04. – URL: https://docs.cntd.ru/document/420205962?ysclid=lcw191gj5y748754679 (дата обращения 11.01.2023).
4. Доктрина информационной безопасности Российской Федерации // Контур Норматив. – 2000. – 09.09. – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=40613&ysclid=lcw12estgy371372874 (дата обращения 08.01.2023).
5. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // Организация Объединенных Наций. – 2023. – URL: https://www.un.org/disarmament/ru/достижения-в-сфере-информатизации-и-т/ (дата обращения 11.01.2023).
6. Заявление глав государств-членов ШОС по международной информационной безопасности // Шанхайская организация сотрудничества. – 2006. – 15.06. – URL: http://scochn.beta2.ria.ru/documents/20060615/44820.html (дата обращения 12.01.2023).

7. Заявление о цифровой повестке Евразийского экономического союза // Электронный фонд правовых и нормативно-технических документов. – 2018. – 17.09. – URL: https://docs.cntd.ru/document/551108000 (дата обращения 12.01.2023).
8. Ковачич Л. Китайский пример заразителен // Ведомости. – 2019. – 28.01. – URL: https://www.vedomosti.ru/opinion/articles/2019/01/28/792659-primer (дата обращения 05.01.2023).
9. О подписании Соглашения между Правительством Российской Федерации и Правительством Киргизской Республики о сотрудничестве в области обеспечения международной информационной безопасности // Министерство иностранных дел Российской Федерации. – 2021. – 26.02. – URL: https://www.mid.ru/ru/foreign_policy/international_safety/1416591/?ysclid=lcw1uqy4m0713876356 (дата обращения 12.01.2023).
10. Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года // Электронный фонд правовых и нормативно-технических документов. – 2017. – 10.11. – URL: https://docs.cntd.ru/document/555625953?ysclid=lcw1lkwge9647243922 (дата обращения 12.01.2023).
11. Об утверждении Концепции информационной безопасности Союзного государства // Министерство иностранных дел Российской Федерации. – 2023. – 01.03. – URL: https://www.mid.ru/ru/foreign_policy/news/1856195/?TSPD_101_R0=08765fb817ab2000d6e7e294ad6b00db63ab105abd305c0618fdc98056bfc2c42885dc6276125b5408c67a6c0b1430007769e3029b9fae7b49a4fe861c1489e649c83cfab25b4 c0 b9622 c629 f7725205 a7 a8 f9 a74 b973 a36 b84976 fb8 c6127 8 f (дата обращения 20.03.2023).
12. Постановление Высшего Государственного Совета Союзного государства Беларуси и России от 19 июня 2018 г. № 3 «О выполнении Приоритетных направлений и первоочередных задач дальнейшего развития Союзного государства на среднесрочную перспективу (2014–2017 годы) и дальнейшем развитии Союзного государства на 2018–2022 годы» // Информационно-правовой портал «Гарант. ру». – 2018. – 19.06. – URL: https://base.garant.ru/71972538/?ysclid=lcw1s4ouv6491429803 (дата обращения 12.01.2023).
13. Рогожин А. КНР – Закон о кибербезопасности принят // ИМЭМО. – 2017. – 01.02. – URL: https://www.imemo.ru/news/events/text/knr-zakon-o-kiberbezopasnosti-prinyat (дата обращения12.01.2023).
14. Селищев Н. Всемирная конференция по интернету открывается в Китае // ТАСС. – 2019. – 20.10. – URL: https://tass.ru/ekonomika/7021930?ysclid=l2wdyv67d (дата обращения 12.01.2023).
15. Соглашение между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности // Электронный фонд правовых и нормативно-технических документов. – 2015. – 27.02. – URL: https://docs.cntd.ru/document/499074140 (дата обращения 12.01.2023).
16. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 года // Официальное опубликование правовых актов. – 2016. – 10.08. – URL: http://publication.pravo.gov.ru/Document/View/0001201608100001?rangeSize=1 (дата обращения 12.01.2023).
17. Соглашение между Правительством Российской Федерации и Правительством Республики Армения о сотрудничестве в области обеспечения информационной безопасности от 19 апреля 2022 года (вступило в силу 5 мая 2023 года) // Официальное опубликование правовых актов. – 2023. – 05.05. – URL: http://publication.pravo.gov.ru/Document/View/0001202305050001 (дата обращения 12.05.2023).
18. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 года (вступило в силу для Российской Федерации 4 июня 2015 года) // Официальное опубликование правовых актов. – 2015. – 04.06. – URL: http://publication.pravo.gov.ru/Document/View/0001201506040007 (дата обращения 05.01.2023).
19. Стратегические направления формирования и развития цифрового пространства Евразийского экономического союза в перспективе до 2025 года // Евразийская экономическая комиссия. – URL: http://www.eurasiancommission.org/ru/act/dmi/workgroup/materials/Documents/Стратегические%20направления%20формирования%20цифрового%20пространства%20ЕАЭС%20(проект).pdf (дата обращения 12.01.2023).
20. Стратегия Китая по обеспечению информационной безопасности: политический и технический аспекты / Чекменева Т.Г., Ершов Б.А. [и др.] // Bulletin Social-Economic and Humanitarian Research. – 2020. – № 7 (9) – С. 78–97. – URL: https://readera.org/strategija-kitaja-po-obespecheniju-informacionnoj-bezopasnostipoliticheskij-i-14118405 (дата обращения 10.01.2023).
21. Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года // Организация Договора о коллективной безопасности. – 2016. – 18.10. – URL: https://odkb-csto.org/documents/statements/strategiya_kollektivnoy_bezopasnosti_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_na_period_do_/?ysclid=lcw1q5diwb406117606#loaded (дата обращения 12.01.2023).
22. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Консультант. – 2021. – 02.07. – URL: http://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения 08.01.2023).
23. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный сайт Президента Российской Федерации. – 2016. – 05.12. – URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения 10.01.2023).

24. Цифровая повестка ЕАЭС: рынок рабочей силы, новые технологии, цифровые транспортные коридоры, большие данные // МГИМО. – URL: https://mgimo.ru/upload/2020/02/EEU-digital-agenda.pdf?ysclid=lcw1gn2a54263848447 (дата обращения 12.01.2023).
25. Цифровая повестка Евразийского экономического союза до 2025 года: перспективы и рекомендации // Евразийская экономическая комиссия. – 2018. – URL: https://eec.eaeunion.org/upload/directions_files/a34/a34a8a322ff61b3e9fba79b3006213c0.pdf?ysclid=lcw1ejr28l700836823 (дата обращения 12.01.2023).
26. Цифровой суверенитет // Валдай. Международный дискуссионный клуб. – 2021. – 02.06. – URL: https://ru.valdaiclub.com/multimedia/infographics/tsifrovoy-suverenitet/ (дата обращения 12.01.2023).
27. Arquilla J., Ronfeldt D. Cyberwar is Coming! // Comparative Strategy. – 1993. – Vol. 12, № 2. – P. 141–165. – URL: https://www.rand.org/pubs/reprints/RP223.html (дата обращения 12.01.2023).
28. Cyberthreat Real – Time Map // Лаборатория «Kaspersky». – 2023. – URL: https://cybermap.kaspersky.com/stats (дата обращения 12.01.2023).
29. Global Cybersecurity Outlook 2022. Insight Report January 2022 / World Economic Forum. – 2022. – 34 p. – URL: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf (дата обращения 12.01.2023).
30. Joubert V. Getting the essence of cyberspace; a theoretical framework to face cyber issues // Conference on Cyber Conflict Proceedings 2010 / C. Czosseck, K. Podins (Eds.). – Tallinn : CCD COE Publications, 2010 – P. 111–126. – URL: https://ccdcoe.org/uploads/2018/10/Joubert-Getting-the-Essence-of-Cyberspace.pdf (дата обращения 11.01.2023).
31. Mazarr M.J. The revolution in military affairs: a framework for defense planning // The Strategic Studies Institute. – 1994. – 10.06. – URL: https://www.files.ethz.ch/isn/112738/Revolution_Military_Affairs.pdf (дата обращения 11.01.2023).
32. National Cyber Strategy of the United States of America // The White House. – 2018. – September. – URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения 12.01.2023).
33. The EU's Cybersecurity Strategy for the Digital Decade // European Commission. – 2020. – 16.12. – URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (дата обращения 12.01.2023).

INFORMATION SECURITY AS AN ELEMENT OF INTEGRATION WITHIN THE EAEU

Christina Ermak

Leading Officer-Administrator of the Center for Analysis and Forecasting of Allied Integration Processes, (Minsk, Belarus), e-mail: kristina.ermak. 2102@mail.ru

Abstract. *The article discusses the prerequisites for creating a system to counter information and cyber threats of the Eurasian Economic Union (EAEU) as a condition and element of regional integration in the current context of global transformations of the world order. Shows russian and foreign experience in this area. Analyzes the potential of the EAEU member states and the results of their bilateral and multilateral cooperation in the field of ensuring information security as a significant component of the digital agenda of the EAEU. Highlights the directions, which in the future can become the basis of the EAEU Information Security Strategy and will allow countering the new challenges of the modern information space.*

Keywords: *information security; cybersecurity; information space; regional cooperation; EAEU; digital agenda; integration.*

For citation: Ermak K.A. Information security as an element of integration within the EAEU // Social Novelties and Social Sciences. – 2023. – N 3. – P. 132–142.

URL: https://sns-journal.ru/ru/archive/ DOI: 10.31249/snsn/2023.03.08