СЕКЦИЯ «ЦИФРОВИЗАЦИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЕВРАЗИЙСКОМ РЕГИОНЕ»

ДВУСТОРОННИЕ СОГЛАШЕНИЯ КАК ГАРАНТИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЕАЭС

А. А. Халатян

РАУ, Республика Армения, Ереван, annkhalatyan13@gmail.com

Неощутимый и постепенный переход к «Индустрии 5.0», предполагающей синтезирование искусственного интеллекта и человеческого разума, ознаменовал стремительную цифровизацию практически всех сфер жизнедеятельности человека.

Цифровизацию следует квалифицировать как бинарное кодирование данных, которые могут обрабатываться компьютерами и многими другими устройствами с вычислительной мощностью, преимущественно имеющими доступ к информационно-телекоммуникационным сетям.

Обозначенное явление способствует развитию информационных отношений и провоцирует развитие кибернетической преступности, тем самым вызывая необходимость обеспечения информационной безопасности, в особенности в рамках экономических интеграционных объединений.

В свою очередь, информационная безопасность в интеграционных объединениях экономического характера должна толковаться как совокупность доступности и целостности информации, в том числе персональных данных.

Примером таких интеграционных объединений является Евразийский экономический союз (далее – «ЕАЭС»), к деятельности в сфере информационной безопасности которого можно отнести создание интегрированной информационной системы ЕАЭС для трансграничной передачи персональных данных в электронном виде в соответствии с Соглашением Правительств государств-членов Таможенного союза «О создании, функционировании и развитии интегрированной информационной системы внешней и взаимной торговли Таможенного союза» в 2010 году, а также запуск трека по обсуждению цифровой повестки в 2016 году.

Более того, в ЕАЭС уже действуют механизмы отбора, проработки и финансирования таких цифровых инициатив и цифровых проектов, как проекты по цифровой прослеживаемости товаров, экосистеме цифровых

транспортных коридоров, трансграничному обороту данных, цифровой промышленной кооперации.

Однако, учитывая темп развития информационных технологий и осуществления электронных торговых операций, можно констатировать невозможность права ЕАЭС обеспечить надлежащий уровень реагирования.

В данном контексте возможные пробелы права ЕАЭС восполняются национальным правом каждого государства-члена ЕАЭС, некоторые нормативные правовые акты в области информационной безопасности которого будут далее рассмотрены:

1. В Республике Армения

• с 2007 года действует Национальная компьютерная группа реагирования на чрезвычайные ситуации (CERT-AM), действующая при поддержке Интернет-общества Армении.

• в 2017 году была принята Концепция информационной безопасности и разработана «Повестки цифровой трансформации Армении до 2030 года», в которой определены этапы цифрового скачка (2018-2020 годы), цифрового ускорения (2020-2025 годы) и развития на основе цифровизации (2026-2030 годы).

Республика Армения является участником Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и Будапештской Конвенции о преступности в сфере компьютерной информации.

Более того, в качестве примеров потенциала гибкости национального права и показателя уровня реагирования армянского законодателя на те или иные подлежащие урегулированию изменения в обществе, можно выделить Постановление Правительства Республики Армения «Об определении перечня электронных услуг», Закон Республики Армения «О государственном содействии развитию сферы высоких технологий», соответствующие положения Налогового кодекса Республики Армения, определяющие место оказания электронных услуг, готовящиеся изменения Трудового кодекса Республики Армения, конкретизирующие регулирование осуществления трудовой деятельности дистанционно, а также Закон Республики Армения «О защите персональных данных», регламентирующий порядок трансграничной передачи персональных данных. Представленные нормативные правовые акты в контексте совокупного толкования регулируют осуществление предпринимательской деятельности в сфере информационных технологий, а также обеспечивают соблюдение требований правомерной обработки персональных данных.

2. В Республике Беларусь

• в 2019 году утверждена Концепция информационной безопасности.

• в 2021 году принят Закон «О персональных данных» № 99-З.

Республика Беларусь поддержала инициативу Российской Федерации о создании новой Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих ИКТ на 2021-2025 годы в соответствии с резолюцией Генеральной Ассамблеи Организации Объединенных Наций (далее – «ГА ООН») 75/240, а также с 2019 по 2021 годы принимает участие в заседаниях рабочей группы открытого состава (РГОС) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

Республика Беларусь стала соавтором принятой в мае 2021 года по инициативе Российской Федерации резолюции ГА ООН 75/282 «О противодействии использованию информационных и коммуникационных технологий в преступных целях», которая определила модальности работы специального комитета для разработки под эгидой ООН универсальной международной конвенции по борьбе с использованием ИКТ в преступных целях.

3. В Республике Казахстан

• в 2017 году утверждена концепция кибербезопасности «Киберщит Казахстана».

• в 2018 году созданы испытательные лаборатории в сфере информационной безопасности по исследованию вредоносного кода, запущены национальный координационный центр информационной безопасности, частная служба реагирования на компьютерные инциденты и 7 оперативных центров информационной безопасности; принята Государственная программа «Цифровой Казахстан».

• в 2022 году разработана новая редакция концепции кибербезопасности «Киберщит Казахстана» до 2027 года.

С 2018 по 2021 годы Республика Казахстан принимала участие в деятельности по блокированию доступа к более чем 500 тысячам террористических интернет-ресурсов в рамках ШОС.

4. В Республике Кыргызстан

• в 2017 году была утверждена программа цифровой трансформации «Таза Коом» и принята новая редакции Закона «Об информации персонального характера» № 5829.

• в 2019 году была утверждена Концепции информационной безопасности на 2019-2023 годы.

5. В Российской Федерации в 2021 году была принята новая редакция Стратегии национальной безопасности.

Более того,

• в 2009 году подписано Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности.

• в 2013 году заключено Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности.

• в 2014 году заключено Соглашение между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности.

• в 2015 году заключено Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности.

• в 2019 году по предложению Российской Федерации создан Специальный межправительственный комитет ООН открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях.

• в 2021 году Российская Федерация внесла в специальный комитет ООН первую универсальную Конвенцию по борьбе с использованием ИКТ в преступных целях, работу над которой планируется завершить в 2023 году.

В этом же году Российская Федерация в лице Правительства Российской Федерации заключила Соглашение с Правительством Республики Кыргызстан о сотрудничестве в области обеспечения международной информационной безопасности.

• в 2022 году Российская Федерация в лице Правительства Российской Федерации подписала Соглашение с Правительством Республики Армения о сотрудничестве в области обеспечения международной информационной безопасности.

Как можно заметить, уровень развития института информационной безопасности государств-членов ЕАЭС отличен. Именно поэтому, отдельные изменения в национальном праве не представляется эффективным способом обеспечения информационной безопасности на территории ЕАЭС.

В данном смысле Российской Федерации удается гармонизировать национальное право как государств-членов ЕАЭС, так и государств-наблюдателей и государств, выразивших интерес посредством обозначенных выше двусторонних соглашений об обеспечении информационной безопасности. Стоит обратить особое внимание на идентичность текстов соглашений, которые формируют единообразное восприятие и

регулирование рассматриваемого института и способствуют формированию регионального права, в частности права ЕАЭС в области обеспечения информационной безопасности.

Преимущество двусторонних соглашений, способствующих гармонизации законодательств, заключается в восполнении не только теоретического пробела, но и практического.

В контексте практического измерения Республика Армения и Республика Казахстан являются наиболее пассивными. Так, Закон Республики Армения «О защите персональных данных» закрепляет применение мер административной ответственности за неправомерную обработку персональных данных, однако на сегодняшний день не было зафиксировано ни одного случая привлечения к административной ответственности за такую обработку.

При этом, анализируя обозначенные двусторонние соглашения, заключенные между Правительством Российской Федерации и правительствами остальных государств-членов ЕАЭС, можно сделать вывод о том, что концепция информационной безопасности подвергается расширительному толкованию и ставится в родовидовую зависимость от понятия «коллективная безопасность» в соотношении с «суверенитетом» и «территориальной целостностью». Наиболее подходящим направлением для разработки потенциального нормативного правового акта в области обеспечения информационной безопасности в рамках права ЕАЭС является пресечение преступлений в сфере компьютерной информации.

Обобщая сказанное ранее, двусторонние соглашения как инструмент гармонизации законодательств государств-членов ЕАЭС на данный момент являются единственным гарантом обеспечения информационной безопасности в рамках ЕАЭС вне права ЕАЭС и создают предпосылки для принятия соответствующего регионального нормативного правового акта.

Представляется, что обозначенный региональный нормативный правовой акт в области обеспечения информационной безопасности должен содержать

- деление данных на данные оперативного и содержательного уровня,
- регулирование электронных операций экономического характера,
- обозначение потенциальных нарушений информационной безопасности,
- указание на характер ответственности за возможные нарушения информационной безопасности.