

Вестник Евразийской науки / The Eurasian Scientific Journal <https://esj.today>

2020, №4, Том 12 / 2020, No 4, Vol 12 <https://esj.today/issue-4-2020.html>

URL статьи: <https://esj.today/PDF/41ECVN420.pdf>

**Ссылка для цитирования этой статьи:**

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 №4, <https://esj.today/PDF/41ECVN420.pdf> (доступ свободный). Загл. с экрана. Яз. рус., англ.

**For citation:**

Borozdin A.N., Kovarda V.V. (2020). Analysis of the information security system in the process of digitalization of its turnover within the EEU in the aspect of improving economic security. *The Eurasian Scientific Journal*, [online] 4(12). Available at: <https://esj.today/PDF/41ECVN420.pdf> (in Russian)

*Выполнено в рамках государственного задания Министерства науки и высшего образования Российской Федерации (тема №1.13.20Ф «Концептуальные основы обеспечения экономической безопасности Российской Федерации в условиях цифровизации: контуры пространственных преобразований»)*

УДК 338; 339

ГРНТИ 06.51.02; 06.51.65; 06.51.77

**Бороздин Алексей Николаевич**

ФГБОУ ВО «Юго-Западный государственный университет», Курск, Россия

Доцент

E-mail: l-boro@yandex.ru

**Коварда Владимир Васильевич**

ФГБОУ ВО «Юго-Западный государственный университет», Курск, Россия

Доцент

Кандидат физико-математических наук, доцент

E-mail: kovarda@yandex.ru

## **Анализ системы обеспечения защиты информации в процессе цифровизации ее оборота в рамках ЕАЭС в аспекте повышения экономической безопасности**

**Аннотация.** В статье рассмотрены актуальные вопросы исследования правового обеспечения защиты трансграничного оборота данных в рамках цифровизации хозяйственных процессов в ЕАЭС в императиве экономической безопасности.

В первой части работы рассмотрена взаимосвязь «экономическая безопасность – цифровая экономика (цифровизация) – защита информации при трансграничном обороте», приведены отдельные положения из нормативных правовых документов. Отмечена необходимость формирования системы защиты данных от несанкционированного доступа к информации в рамках трансграничной передаче.

Во второй части работы проанализировано национальное законодательство каждой страны ЕАЭС о персональных данных, а также о возможности трансграничного перемещения информации. Определено, что только две страны-участницы ЕАЭС ратифицировали присоединение к Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. – Россия и Республика Армения. Так, в соответствии с российским законодательством, адекватную защиту прав субъектов персональных данных обеспечивает Республика Казахстан. В итоге, Беларусь и Киргизия, по мнению российской стороны, не могут надлежащим образом обеспечить безопасность

персональных данных при их трансграничной передаче. Однако, если трансграничная передача персональных данных предусмотрена международными договорами Российской Федерации, то она возможна.

По результатам анализа определено, что проблема создания единых криптографических средств защиты информации при информационном взаимодействии в ЕАЭС чрезвычайно актуальна в настоящее время, а использование криптографических средств защиты информации производителей стран, не входящих в ЕАЭС, увеличивает риски экономической и национальной безопасности.

В заключении статьи сделаны соответствующие выводы.

**Ключевые слова:** трансграничный оборот данных; цифровая экономика; экономическая безопасности; криптография; персональные данные

### Введение

Перспективы расширения использования цифровых технологий в хозяйственной деятельности в рамках Евразийского экономического союза не вызывают сомнения, о чем свидетельствует, например, программа «Цифровая повестка ЕАЭС»<sup>1</sup>. В указанном документе определены основные этапы цифровизации до 2025 года, в т. ч. развитие электронной торговли, цифровая прослеживаемость и т. д. Однако, процесс цифровизации имеет и потенциально негативные стороны, связанные с перманентным обеспечением кибербезопасности [1–2] и возможным увеличением безработицы [3–6]. Если рассматривать более детально, то одним из наиболее значимых вопросов в рамках расширения цифровизации является обеспечение безопасности оборота информации, в частности, персональных данных при организации информационного потока. В глобальном масштабе, трансграничные потоки данных в период с 2005 по 2014 год выросли в 45 раз, достигнув 2,8 трлн долл. США, и влияние этого процесса на прирост мирового ВВП оказалось выше, чем влияние мировой торговли товарами<sup>2</sup>. В рамках ЕАЭС в законодательстве персональных данных (ПДн) России, Республики Беларусь и Армении категории «персональные данные» схожи и представляют собой любую информацию или сведение, относящиеся к прямо или косвенно определенному или определяемому физическому лицу (субъект ПДн). Законодательства о ПДн Республики Казахстан и Кыргызской Республики дополнительно включают в понятие «персональные данные» информацию и сведения о субъекте ПДн, которые зафиксированы на материальном носителе (бумажном, электронном либо ином).

ПДн являются информацией ограниченного распространения (конфиденциальной информацией) и не подлежат передаче и распространению третьим лицам без согласия на то субъекта ПДн, за исключением случаев, установленных законодательством стран-участниц ЕАЭС, а также, когда субъект ПДн самостоятельно, лично счёл необходимым разместить ПДн в публичном пространстве.

Следует отметить, что среди других видов конфиденциальной информации ПДн наиболее чувствительные, так как непосредственно затрагивают права и свободы человека и гражданина и включают в себя многие идентификационные признаки: прямые и косвенные, по которым можно определить субъекта ПДн. В связи с чем меры по обеспечению безопасности

---

<sup>1</sup> ЦИФРОВАЯ ПОВЕСТКА ЕАЭС 2016-2019-2025 [Электронный ресурс]. – URL: [http://www.eurasiancommission.org/ru/Documents/digital\\_agenda\\_eaeu.pdf](http://www.eurasiancommission.org/ru/Documents/digital_agenda_eaeu.pdf).

<sup>2</sup> ЦИФРОВАЯ ПОВЕСТКА Евразийского экономического союза до 2025 года: перспективы и рекомендации [Электронный ресурс]. – URL: <http://eec.eaunion.org/ru/act/dmi/SiteAssets/Обзор%20ВБ.pdf>.

ПДн отличаются своим содержанием и составом, от принимаемых мер по обеспечению безопасности других видов конфиденциальной информацией, хотя и присутствуют схожие моменты.

Принимаемые меры по обеспечению безопасности ПДн могут существенно различаться в разных странах в зависимости от категории ПДн, установленных уровней защищенности информационных систем ПДн, принятых стандартов по информационной безопасности и в целом от государственного подхода к защите данного вида обрабатываемой информации.

Еще одной важной категорией данных является информация, содержащая коммерческую тайну, особенность которой заключается в возможности оказания существенного влияния на позиции организации (отрасли и т. д.) на рынке.

В целом, эти вышеприведенные две категории данных в условиях расширения их оборота в рамках цифровизации способны оказать существенное воздействие на расположение конкурентных сил, развитие разных сегментов и экономики в целом, и, таким образом, на состояние экономической безопасности.

### **Анализ взаимосвязи экономической безопасности с цифровизацией и системой обеспечения защиты персональных данных в рамках трансграничного обмена**

Экономическая безопасность характеризует некое состояние, в рамках которого обеспечивается защита экономических интересов национальной экономики, а все факторы влияния условно можно разделить на внешние и внутренние. Рост степени конкуренции, мировые тенденции [7–8] и логическое развитие диктуют необходимость оптимизации всех хозяйственных процессов в целях повышения эффективности деятельности и обеспечения интересов страны в экономической сфере, чему способствует расширение применения цифровых технологий [9–10]. В связи с этим, среди вызовов и угроз экономической безопасности в соответствующей Стратегии<sup>3</sup> указано, что опасность представляет стремление отдельных стран использовать свои преимущества в области экономики и цифровых технологий в качестве инструмента конкурентной борьбы. При этом отмечается недостаточная инновационная активность и отставание в сфере технологий цифровой экономики.

Исходя из отмеченного выше одной из приоритетных целей государственной политики в области повышения уровня экономической безопасности является повышение конкурентоспособности экономической системы России посредством развития технологий цифровой экономики (отмечено на рисунке 1). В соответствии с Указом Президента РФ №204<sup>4</sup> был разработан национальный проект по направлению «цифровая экономика Российской Федерации». Одной из целей нацпроекта является создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств<sup>5</sup>. Именно вопросы безопасности как функционирования формируемой системы, так и баз данных используются критиками в процессе обсуждения перспектив построения

<sup>3</sup> Указ Президента РФ от 13.05.2017 N 208 "О Стратегии экономической безопасности Российской Федерации на период до 2030 года" [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_216629/](http://www.consultant.ru/document/cons_doc_LAW_216629/).

<sup>4</sup> Указ Президента РФ от 07.05.2018 N 204 (ред. от 21.07.2020) "О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года" [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_297432/](http://www.consultant.ru/document/cons_doc_LAW_297432/).

<sup>5</sup> "Паспорт национального проекта "Национальная программа "Цифровая экономика Российской Федерации" (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 N 7) [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_328854/](http://www.consultant.ru/document/cons_doc_LAW_328854/).

цифровой экономики. Таким образом, необходимо параллельное развитие системы как технологий по обороту информации, так и обеспечению кибербезопасности, в частности, защиты данных в рамках их перемещения в результате межведомственного обмена (в т. ч. трансграничного).



**Рисунок 1.** Взаимосвязь экономической безопасности, цифровой экономики и оборота данных (составлено авторами)

Особую актуальность приобретают вопросы перемещения данных (сведений) в рамках трансграничного обмена информацией в масштабе ЕАЭС, где также прорабатываются вопросы цифровизации, в частности, цифровая повестка ЕАЭС до 2025 г. (в т. ч. развитие электронной торговли и цифровой прослеживаемости товаров). В связи с этим, Решением Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об Основных направлениях реализации цифровой повестки Союза до 2025 года» определены приоритеты проработки инициатив в рамках реализации цифровой повестки Евразийского экономического союза до 2025 года, в числе которых приоритет имеет «Соглашение об обороте данных в Союзе (в том числе о защите персональных данных)».

Итак, расширение использования цифровых технологий подразумевает рост оборота данных различного характера, в т. ч. персональных данных, недобросовестное и незаконное использование которых может иметь негативные последствия как для конкретного субъекта, так и представлять угрозу развития всей системы цифровой экономики (например, снижение степени доверия и устранение от участия в экономических процессах, осуществляемых на цифровой платформе). В конечном итоге, систематические проблемы (нарушения) в рамках оборота данных окажут существенное влияние на как состояние национальной и экономической безопасности России, так и экономической безопасности интеграционного

объединения ЕАЭС. Данное утверждение имеет исключительное значение и подтверждается координатором экспертной площадки (до октября 2018 г.), аналитиком онтологии данных А.Ю. Сорокиной, которая отмечает: «В основе бизнес-моделей и цепочек добавленной стоимости цифровой экономики – данные. Выработка общих подходов к регулированию оборота данных на пространстве ЕАЭС позволяет найти ответ на важнейший вызов по созданию ценности на основе данных, ее удержанию и извлечению выгоды для экономик государств-членов»<sup>1</sup>. Таким образом, развитие системы защиты информации в процессе трансграничного оборота в рамках цифровой экономики имеет приоритетное значения в рамках обеспечения экономической безопасности.

### **Анализ национальных законодательств стран-участниц ЕАЭС в рамках обеспечения безопасности трансграничной передачи персональных данных**

Развитие интеграционных процессов в масштабах ЕАЭС, касающихся, прежде всего, хозяйственной деятельности, и в соответствии с мировыми тенденциями, требует расширения использования цифровых технологий. В связи с этим, как на национальном уровне (например, нацпроект «Цифровая экономика Российской Федерации» и Указ Президента РФ №204), так и на наднациональном (например, Цифровая повестка ЕАЭС) приняты соответствующие документы. В конечном итоге, одним из результатов вышеотмеченного процесса должно быть формирование систем цифровой прослеживаемости движения товаров процессе движения на территории ЕАЭС, а также электронной торговли, цифровых транспортных коридоров, которые предусматривают трансграничный обмен сведениями (данными). В итоге, возникает необходимость развития системы обеспечения безопасности информации в рамках электронного взаимодействия. Безопасность ПДн представляет собой состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в информационных системах ПДн<sup>6</sup>.

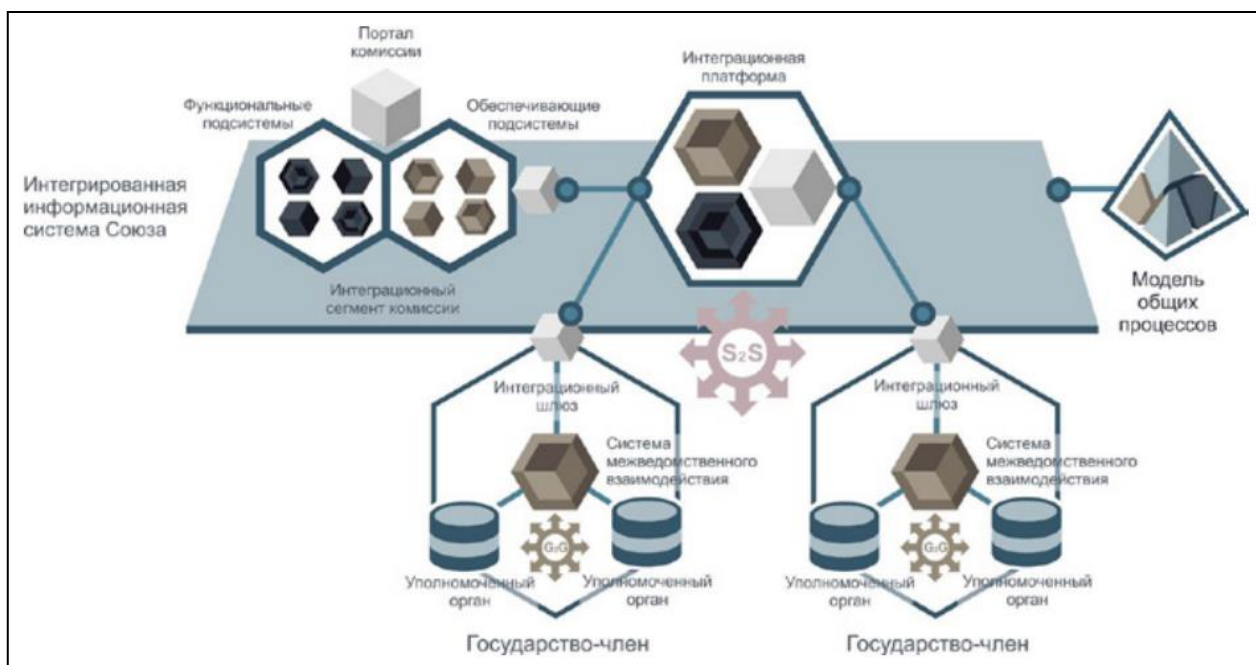
Трансграничная передача ПДн означает передачу или предоставление персональных данных другим государствам. Между странами-участницами ЕАЭС трансграничная передача ПДн в электронном виде осуществляется посредством интегрированной информационной системы Евразийского экономического союза (ИИС ЕАЭС), условная схема которой приведена на рисунке 2.

ИИС ЕАЭС представляет собой организационную совокупность территориально распределенных государственных информационных ресурсов и информационных систем уполномоченных органов, информационных ресурсов и информационных систем Евразийской экономической комиссии (Комиссия, ЕЭК), объединенных национальными сегментами государств-членов и интеграционным сегментом Комиссии<sup>7</sup>. Национальный сегмент государства-члена, интеграционный сегмент Комиссии – информационные системы, обеспечивающие информационное взаимодействие информационных систем уполномоченных органов и информационных систем Комиссии в рамках ИИС<sup>7</sup>.

---

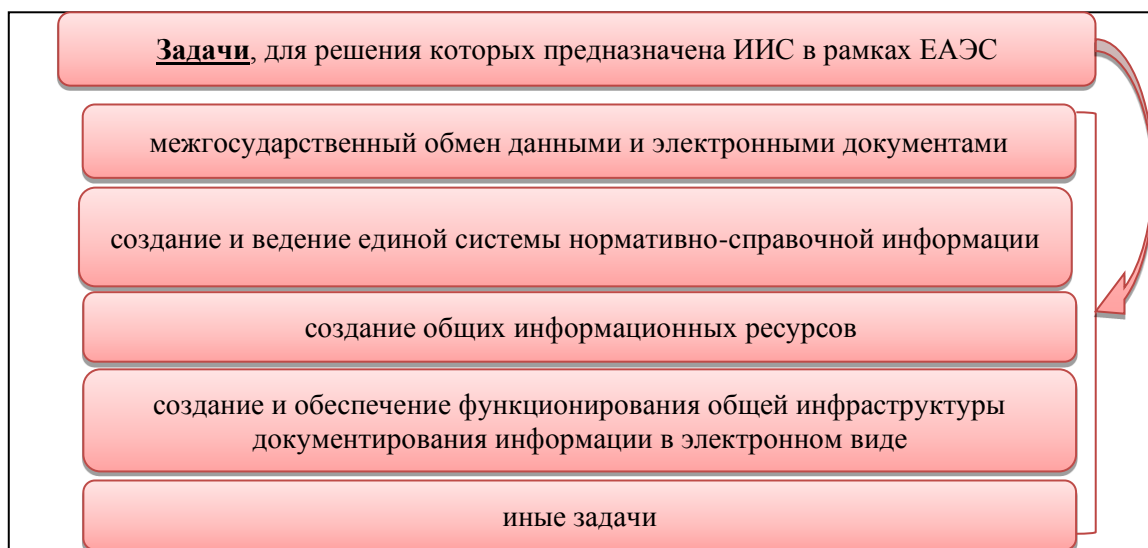
<sup>6</sup> «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК РФ 15.02.2008) [Электронный ресурс]. – URL: <https://fstec.ru/component/attachments/download/289>.

<sup>7</sup> Договор о Евразийском экономическом союзе (Подписан в г. Астане 29.05.2014) (ред. от 08.05.2015) (с изм. и доп., вступ. в силу с 12.08.2017) [Электронный ресурс]. – URL: <http://www.consultant.ru>.



**Рисунок 2.** Архитектура интегрированной информационной системы ЕАЭС  
(рисунок заимствован из сборника «ЦИФРОВАЯ ПОВЕСТКА ЕАЭС 2016-2019-2025»<sup>1</sup>)

В рамках ЕАЭС ИИС предназначена для решения задач, которые представлены на рисунке 3.



**Рисунок 3.** Задачи, для решения которых предназначена ИИС в рамках ЕАЭС (составлено авторами)

ИИС является продолжением интегрированной информационной системы внешней и взаимной торговли, которая была создана в соответствии с Соглашением Правительств государств-членов Таможенного союза «О создании, функционировании и развитии интегрированной информационной системы внешней и взаимной торговли Таможенного союза» 21 сентября 2010 года и реализация которой осуществлялась в 2011–2014 гг.

В ИИС при трансграничном взаимодействии между таможенными органами стран-участниц ЕАЭС при реализации общих процессов осуществляется обмен сведениями, среди которых присутствуют персональные данные физических лиц: фамилия, имя, отчество, сведения о документе, удостоверяющем личность физического лица, уникальный

идентификатор физического лица и другие<sup>8</sup>. Кроме того, между компетентными органами стран-участниц ЕАЭС осуществляется обмен сведениями в сфере трудовой миграции и социального обеспечения.

В соответствии со статьей 361 Таможенного кодекса ЕАЭС, таможенные органы вправе проводить сбор информации о лицах, осуществляющих внешнеэкономическую деятельность, связанную с перемещением товаров через таможенную границу Союза, либо иную деятельность в отношении товаров, находящихся под таможенным контролем, включая сведения о физических лицах: персональные данные (фамилия, имя, отчество), дата и место рождения, пол, адрес места жительства, реквизиты документа, удостоверяющего личность, включая личный (индивидуальный идентификационный) номер физического лица (при наличии), идентификационный (регистрационный, учетный) номер налогоплательщика (при наличии) и частота перемещения этими лицами товаров через таможенную границу Союза. При этом сбор информации осуществляется таможенными органами при совершении таможенных операций и посредством ее получения от других государственных органов государств-членов<sup>9</sup>.

19 декабря 2005 года Россия ратифицировала Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года (Конвенция 1981 года), взяв на себя обязательства по соответствию внутреннего законодательства данной конвенции. 27 июля 2006 г. Россией был принят Федеральный закон № 152-ФЗ «О персональных данных», статьей 12 которого определено следующее:

- пункт 1 – «Трансграничная передача ПДн на территории иностранных государств, являющихся сторонами Конвенции 1981 года, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн, осуществляется в соответствии с Федеральным законом № 152-ФЗ «О персональных данных»...»;
- пункт 2 – «Уполномоченный орган по защите прав субъектов ПДн утверждает перечень иностранных государств, не являющихся сторонами Конвенции 1981 года и обеспечивающих адекватную защиту прав субъектов ПДн. Государство, не являющееся стороной Конвенции 1981 года, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн, при условии соответствия положениям Конвенции 1981 года действующих в соответствующем государстве норм права и применяемых мер безопасности ПДн»;
- пункт 3 – «Трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн, может осуществляться в случаях: ... предусмотренных международными договорами Российской Федерации...»<sup>10</sup>.

Конвенцию 1981 года ратифицировали две страны-участницы ЕАЭС – Россия и Республика Армения. В соответствии с приказом Роскомнадзора от 15.03.2013 N 274 (ред. от 14.01.2019) «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке

---

<sup>8</sup> Решение Коллегии Евразийской экономической комиссии от 21.08.2018 № 128 «О технологических документах, регламентирующих информационное взаимодействие при реализации средствами интегрированной информационной системы Евразийского экономического союза общего процесса «Обеспечение обмена сведениями между таможенными органами государств – членов Евразийского экономического союза в процессе контроля и подтверждения фактического вывоза товаров за пределы таможенной территории Евразийского экономического союза» [Электронный ресурс]. – URL: <http://www.consultant.ru>.

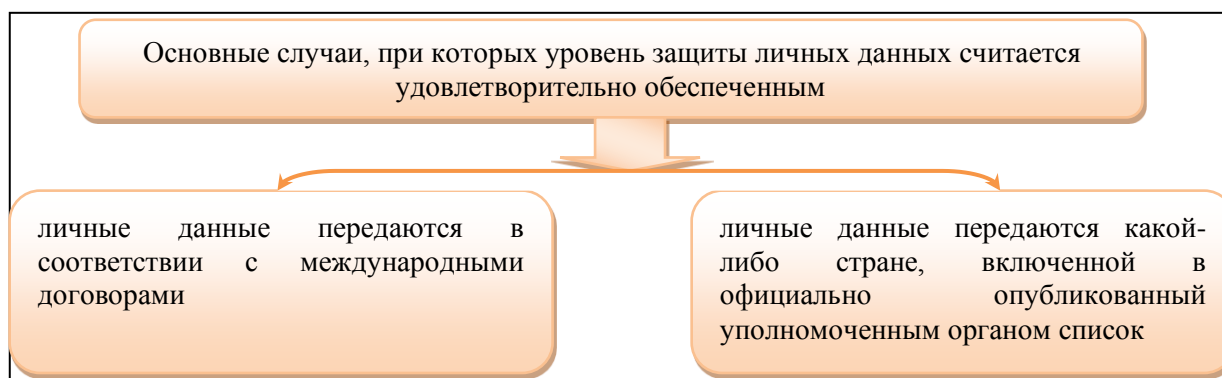
<sup>9</sup> Таможенный кодекс Евразийского экономического союза [Электронный ресурс]: Договор о Таможенном кодексе Евразийского экономического союза от 12.04.2017 года // <http://www.consultant.ru>.

<sup>10</sup> Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017) «О персональных данных» [Электронный ресурс]. – URL: <http://www.consultant.ru>.

персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных» адекватную защиту прав субъектов ПДн обеспечивает Республика Казахстан. Тем самым страны-участницы ЕАЭС – Республика Беларусь и Кыргызская Республика, по мнению российской стороны, не могут надлежащим образом обеспечить безопасность ПДн при их трансграничной передаче. Однако, если трансграничная передача ПДн предусмотрена международными договорами Российской Федерации, то она возможна.

Критериев, определяющих адекватность защиты прав субъектов ПДн на территории иностранного государства, действующим законодательством Российской Федерации не предусмотрено<sup>11</sup>.

В Республике Армении порядок и условия обработки ПДн регулируются Законом Республики Армения от 13 июня 2015 года № ЗР-49 «О защите личных данных» (ред. от 23.07.2019). Статьей 27 данного закона предусмотрена передача личных данных другим государствам. В пункте 2 статьи 27 указано: «Личные данные могут быть переданы другому государству без разрешения уполномоченного органа, если в этом государстве обеспечен удовлетворительный уровень защиты личных данных. Удовлетворительный уровень защиты личных данных считается обеспеченным в случаях, представленных на рисунке 4.



*Рисунок 4. Основные случаи, при которых уровень защиты личных данных считается удовлетворительно обеспеченным (составлено авторами)*

Пунктом 6 статьи 27 установлено: «личные данные, находящиеся в распоряжении государственных органов, могут быть переданы органам иностранных государств только в рамках межгосударственных договоров, а негосударственным органам – в соответствии с нормами статьи 27 вышеуказанного закона»<sup>12</sup>.

Положения норм статей по трансграничной передаче ПДн национальных законодательств Республики Армения и России схожи, что обусловлено намерениями этих стран соответствовать принципам Конвенции 1981 года.

В Кыргызской Республике правовое регулирование работы с ПДн осуществляется в соответствии с Законом Кыргызской Республики от 14 апреля 2008 года № 58 (ред. от 20.07.2017) «Об информации персонального характера». Трансграничная передача ПДн предусмотрена статьей 25. Согласно пункта 1 данной статьи: «При трансграничной передаче персональных данных держатель (обладатель) массива персональных данных, находящийся под юрисдикцией Кыргызской Республики, передающий данные, исходит из наличия международного договора между сторонами, согласно которому получающая сторона

<sup>11</sup> «Ответы на вопросы в сфере защиты прав субъектов персональных данных». Официальный сайт Роскомнадзора [Электронный ресурс]. – URL: <https://rkn.gov.ru/treatments/p459/p468/>.

<sup>12</sup> Закон Республики Армения от 13 июня 2015 года № ЗР-49 «О защите личных данных» [Электронный ресурс]. – URL: <http://www.consultant.ru>.



обеспечивает адекватный уровень защиты прав и свобод субъектов персональных данных и охраны персональных данных, установленный в Кыргызской Республике»<sup>13</sup>.

В Республике Казахстан общественные отношения в сфере ПДн регулирует Закон Республики Казахстан от 21 мая 2013 года N 94-V (ред. от 28.12.2017) «О персональных данных и их защите». Статьей 16 данного закона предусмотрена трансграничная передача ПДн. В частности определено, что трансграничная передача ПДн на территорию иностранных государств осуществляется только в случае обеспечения этими государствами защиты ПДн, иначе она может осуществляться в случаях, предусмотренных международными договорами, ратифицированными Республикой Казахстан<sup>14</sup>.

В Республике Беларусь трансграничная передача ПДн определена в Законе Республики Беларусь «О персональных данных» (принят 13.06.2019, официально в юридическую силу не вступил). Пунктом 1 статьи 10 предусмотрено следующее: «трансграничная передача ПДн запрещается, если в другом государстве не обеспечивается надлежащий уровень их защиты, кроме случаев, когда: ... сбор, обработка, распространение, предоставление ПДн осуществляются в рамках исполнения международного договора Республики Беларусь...»<sup>15</sup>.

В результате анализа национального законодательства о ПДн стран-участниц ЕАЭС можно сформулировать выводы, которые кратко представлены на рисунке 5, а дальше приведены соответствующие пояснения.



**Рисунок 5.** Основные результаты сравнительного анализа национальных законодательств стран ЕАЭС о защите персональных данных при их трансграничной передаче в процессе цифровизации (составлено авторами)

<sup>13</sup> Закон Кыргызской Республики от 14 апреля 2008 года № 58 (ред. от 20.07.2017) «Об информации персонального характера» [Электронный ресурс]. – URL: <http://www.consultant.ru>.

<sup>14</sup> Закон Республики Казахстан от 21 мая 2013 года № 94-V (ред. от 28.12.2017) «О персональных данных и их защите» [Электронный ресурс]. – URL: <https://online.zakon.kz>.

<sup>15</sup> Закона Республики Беларусь «О персональных данных» [Электронный ресурс]. – URL: <http://www.pravo.by>.

1. Трансграничная передача ПДн возможна при наличии соответствующих международных договоров.

2. Обеспечение безопасности ПДн при их обработке достигается с помощью комплекса мер: правовых, организационных и технических. Применение указанных мер является обязанностью оператора обработки ПДн, а сами данные меры зависят от принимаемых внутри государств нормативных актов и технических стандартов по информационной безопасности.

3. Безопасность трансграничной передачи ПДн характеризуется большей степенью техническим аспектом их защиты, в частности применением криптографических средств защиты информации. Данные средства используются для нейтрализации тех угроз безопасности ПДн, которые могут быть закрыты с помощью таких средств. Так, используя шифрование информации, содержащей ПДн, выполняются требования по обеспечению их конфиденциальности и целостности. В конечном итоге, угрозы, связанные с несанкционированным доступом к информации, являются минимальными.

В пункте 2 статьи 19 Закона № ЗР-49 «О личных данных» Республики Армения сказано прямо: «Оператор при обработке личных данных обязан использовать шифровальные средства для обеспечения защиты информационных систем, содержащих личные данные...», в то время как в законодательствах Республики Казахстан и Республики Беларусь прямая норма отсутствует. В России и Кыргызской Республики применение криптографических средств защиты информации зависит от установленных требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации и Правительством Кыргызской Республики уровни защищенности ПДн. Таким образом, единый подход к организации обеспечения безопасности передачи ПДн с применением криптографических средств защиты информации, содержащей ПДн в странах-участниц ЕАЭС отсутствует.

В странах-участниц ЕАЭС криптографическая защита строится с учетом разработки собственных криптографических алгоритмов, взятых за основу в качестве национальных стандартов. Так, в соответствии с Решением Совета Евразийской экономической комиссии от 18.09.2014 №73 «О Концепции использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов» – «Государства-члены используют национальные стандарты криптографических алгоритмов создания и проверки ЭЦП. Применяемые органами государственной власти государств-членов способы реализации криптографических алгоритмов между собой несовместимы, что обусловлено различными подходами к обеспечению информационной безопасности». В настоящее время эти положения являются актуальными.

В Решении Совета Евразийской экономической комиссии от 18.09.2014 №73 сказано: «В случае если в соответствии с законодательством или соответствующим соглашением государств-членов требуется обеспечить конфиденциальность документа, информация, содержащаяся в электронном документе, может быть зашифрована (преобразована с использованием средств криптографической защиты информации). Порядок применения средств криптографической защиты информации в таких случаях устанавливается международными договорами в рамках Союза». Из данного положения вытекает, что конфиденциальную информацию не обязательно шифровать, она может быть зашифрована, что противоречит самой сути понятия конфиденциальности информации, то есть ограничения её доступа.

4. Из национальных законодательств стран-участниц ЕАЭС видно, что ПДн являются конфиденциальной информацией и в настоящее время ПДн передаются в ИИС между странами для таможенных целей. Но, что касается международных договоров стран-участниц

ЕАЭС по трансграничной передаче ПДн и их защите в рамках совместной интеграции, которые бы определяли все согласованные и единые необходимые мероприятия по безопасной обработке ПДн с достаточным уровнем их защищенности, то они отсутствуют.

В праве ЕАЭС имеется международный договор, который декларирует при информационном взаимодействии в ИИС общие требования к защите информации ограниченного доступа, в том числе криптографической защите информации, циркулирующей в компонентах ИИС. Так, защита информации в ЕАЭС осуществляется в соответствии с техническим заданием на создание ИИС ЕАЭС, утвержденным Решением N 137 Коллегии Евразийской экономической комиссии «Об утверждении технического задания на создание интегрированной информационной системы Евразийского экономического союза» (Техническое задание). В Техническом задании указано, что защита информации в ИИС должна обеспечиваться в соответствии с требованиями к созданию, развитию и функционированию трансграничного пространства доверия, разрабатываемыми Комиссией во взаимодействии с уполномоченными органами и утверждаемыми ею. Кроме того, защита от несанкционированного доступа к информации в ИИС должна обеспечиваться в соответствии с требованиями Технического задания и с учетом положений технических, технологических, методических и организационных документов, утверждаемых Комиссией для целей обеспечения унификации применяемых организационных и технических решений при создании, обеспечении функционирования и развитии интегрированной системы и поддержания надлежащего уровня защиты информации.

Кроме того, подписаны международные договоры, предусматривающие при обмене электронными документами при трансграничном взаимодействии использование международных рекомендаций и стандартов, взятых за основу. Прежде всего, это – «Стандарт X.509» – стандарт ITU-T X.509 «Информационные технологии. Взаимосвязь открытых систем. Справочник: Структуры сертификатов открытых ключей и атрибутов»; «Стандарт XAdES» – стандарт XML Advanced Electronic Signature, описывающий расширенный формат электронной цифровой подписи (электронной подписи) в формате XML; «Стандарт XMLDSig» – стандарт синтаксиса и обработки электронной цифровой подписи (электронной подписи) в формате XML, а также применяемая инфраструктура открытых ключей (Public Key Infrastructure) в соответствии с рекомендациями X.509 Public Key Infrastructure. При этом должны использоваться согласованные криптографические стандарты ЭЦП и согласованные криптографические стандарты функции хеширования, утверждаемые Комиссией<sup>16</sup>.

Учитывая, что в национальных законодательствах стран-участниц ЕАЭС должны использоваться средства криптографической защиты информации и реализуемые ими криптографические алгоритмы шифрования и создания электронных подписей собственной отечественной разработки, то, следовательно, криптографические стандарты в ЕАЭС должны быть унифицированными в рамках международных соглашений. Но, как сказано в Решении Совета Евразийской экономической комиссии от 18.09.2014 №73 «О Концепции использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов» – «Применение единых криптографических средств ЭЦП при трансграничном электронном обмене данными между органами государственной власти государств-членов в настоящее время невозможно, поскольку в соответствии с нормативно-правовой базой государств-членов к использованию в государствах-членах допускаются только сертифицированные по национальным стандартам

---

<sup>16</sup> Решение Коллегии Евразийской экономической комиссии от 28.09.2015 № 125 «Об утверждении Положения об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией» [Электронный ресурс]. – URL: <http://www.consultant.ru>.

криптографические средства». Поэтому проблема создания единых криптографических средств защиты информации при информационном взаимодействии в ЕАЭС актуальна, а использование криптографических средств защиты информации производителей стран, не входящих в ЕАЭС, увеличивает риски экономической и национальной безопасности.

В Страсбурге 10 октября 2018 года состоялось подписание протокола о внесении изменений в европейскую Конвенцию 1981 года (Протокол). Россия, наряду с 19 государствами-членами Совета Европы, поддержала обновленную редакцию договора. Изменения касаются обязательств по усилению контроля над оборотом ПДн, обработки «специального» типа данных, таких как биометрия или генетические данные, а также регулирования трансграничного обмена и международного сотрудничества<sup>17</sup>.

В новой редакции Конвенции 1981 года предусмотрены единые правила для отказа в трансграничной передаче ПДн, если государство обязано соблюдать согласованные правила защиты, установленные региональной международной организацией<sup>18</sup>. В связи с этим противоречивым является аспект, затрагивающий следующий практический вопрос: каким образом тогда возможна трансграничная передача ПДн в рамках информационного взаимодействия в ЕАЭС на основе составленных между странами-участницами ЕАЭС международных договоров, в то время как новые правила Конвенции 1981 года требуют к странам присоединившимися к обновленной конвенции соблюдать нормы, установленные ею (т.е. Конвенцией)? В данном случае, странам-участницам ЕАЭС, не являющимися участниками Конвенции 1981 г. необходимо будет подписать и ратифицировать новые правила Конвенции 1981 г., а также привести свое национальное законодательство в сфере защиты ПДн в соответствие с нормами обновленной конвенции.

Учитывая, что вступление модернизированной Конвенции 1981 г. в силу ожидается в течение пяти лет, целесообразно предложить выработать странами-участницами ЕАЭС на этот период единые требования и меры по обеспечению безопасности ПДн при трансграничной передаче в рамках информационного взаимодействия в ИИС.

5. В странах-участниц ЕАЭС в целом отведена малая роль защите прав субъектов ПДн, в частности при трансграничной передаче ПДн в ИИС. Данный факт обусловлен рядом выявленных причин, среди которых «отставание» национальных законодательств от общепризнанных международных норм права в области соблюдении прав человека и основных свобод. Осложняющим моментом является отсутствие единой выработанной политики по безопасной обработке ПДн, циркулирующих в ИИС, и отвод данной проблемы на уровень национальных законодательств. К тому же, отсутствуют единые критерии, определяющие адекватность защиты прав субъектов ПДн на территории государств, не входящих в ЕАЭС. Так, в странах Европейского союза данные критерии установлены и нашли своё отражение в Регламенте N 2016/679 Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)» (Принят в г. Брюсселе 27.04.2016). В то же время ни одна из стран-участниц ЕАЭС не соответствует критериям при оценке адекватности страны и не рассматривается, с точки зрения законодательства Европейского Союза о ПДн, в качестве страны, обеспечивающей адекватный

---

<sup>17</sup> «Россия подписала протокол изменений в европейскую конвенцию о защите персональных данных» [Электронный ресурс]. – URL: [http://www.cnews.ru/news/line/2018-10-11\\_rossiya\\_podpisala\\_protokol\\_izmenenij\\_v\\_evropejskuyu](http://www.cnews.ru/news/line/2018-10-11_rossiya_podpisala_protokol_izmenenij_v_evropejskuyu).

<sup>18</sup> «Россия подписала протокол изменений в европейскую конвенцию о защите персональных данных» [Электронный ресурс]. – URL: <http://d-russia.ru/rossiya-podpisala-protokol-izmenenij-v-evropejskuyu-konventsiyu-o-zashite-personalnyh-dannyh.html>.

уровень защиты ПДн, несмотря даже на факты ратификации Россией и Республикой Армения Конвенции 1981 года. Всё это вызывает определенные трудности свободного обмена ПДн и их защиты как в рамках тесных интеграционных процессов ЕАЭС, так и при взаимодействии со странами Европейского союза по тем или иным основаниям.

### **Заключение**

Цифровизация экономических процессов является одним из наиболее перспективных направлений повышения эффективности как национальной экономики России, так всего интеграционного объединения ЕАЭС, что, в конечном итоге, приведет к повышению уровня экономической безопасности. Данный процесс неразрывно связан с трансграничным оборотом данных разного характера и применения (персональных данных; информации, составляющей коммерческую тайну и т. д.). В связи с этим, необходимо обеспечить конфиденциальность передаваемой и хранимой информации, от эффективности защиты которой зависит результативность формирования пространства доверия (решением Коллегии Евразийской экономической комиссии от 27 сентября 2016 г. принята Стратегия развития трансграничного пространства доверия), и, в конечном итоге, экономическая и национальная безопасность. Однако, именно в этом аспекте имеются нерешенные вопросы как касающиеся шифрования передаваемых данных, так и единых требований и мер по обеспечению безопасности информации.

## ЛИТЕРАТУРА

1. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. №3(31). С. 18–23.
2. Халин В.Г., Чернова Г.В. Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски // Управленческое консультирование. 2018. № 10. С. 46–63.
3. Кознов А.Б. Влияние цифровизации на рынок труда // Международный журнал гуманитарных и естественных наук. 2019. vol.4–2. С. 177–179.
4. Ахапкин Н.Ю., Волкова Н.Н., Иванов А.Е. Развитие цифровой экономики и перспективы трансформации российского рынка труда // Вестник ИЭ РАН. 2018. №5. С. 51–65.
5. Сизова И.Л., Хусяинов Т.М. Труд и занятость в цифровой экономике: проблемы российского рынка труда // Вестник СПбГУ. Социология. 2017. Т. 10. Вып. 4. С. 376–396.
6. Кузнецов Н.В. Изменение структуры занятости и профессионально-квалификационных требований в эпоху цифровизации экономики // Современные проблемы науки и образования. 2018. № 5. URL: <http://science-education.ru/ru/article/view?id=27992> (дата обращения: 26.07.2020).
7. Лаптев Р.А. Национальная экономика России в системе мирохозяйственных связей // Общество: политика, экономика, право. 2018. № 8. С. 25–27.
8. Лаптев Р.А., Коварда В.В. Анализ внешнеэкономических интересов России на мировом рынке // Научное обозрение: теория и практика. 2018. № 6. С. 8–17.
9. Положихина М.А. Регулирование процесса цифровизации экономики: европейский и российский опыт // Россия и современный мир. 2018. URL: <https://cyberleninka.ru/article/n/regulirovanie-protsessa-tsifrovizatsii-ekonomiki-evropeyskiy-i-rossiyskiy-opyt>.
10. Лаптев Р.А., Коварда В.В., Рогов Р.А. Основные направления развития системы прослеживаемости товаров в качестве фактора обеспечения безопасности России в условиях расширения процесса глобализации // Вестник Евразийской науки. 2020. №1. <https://esj.today/PDF/15ECVN120.pdf>.

**Borozdin Alexey Nikolaevich**

Southwest state university, Kursk, Russia  
E-mail: l-boro@yandex.ru

**Kovarda Vladimir Vasilievich**

Southwest state university, Kursk, Russia  
E-mail: kovarda@yandex.ru

## **Analysis of the information security system in the process of digitalization of its turnover within the EEU in the aspect of improving economic security**

**Abstract.** Topical issues of researching the legal support for the protection of cross-border data traffic within the framework of digitalization of business processes in the EAEU in the imperative of economic security are discussed in the article.

In the first part of the work, the relationship "economic security – digital economy (digitalization) – protection of information in cross-border circulation" is considered, some provisions from regulatory legal documents are given. The need to form a data protection system against unauthorized access to information within the framework of cross-border transmission is noted.

The second part of the work analyzes the national legislation of each EAEU country on personal data, as well as on the possibility of cross-border movement of information. It was determined that only two EAEU member states have ratified accession to the Council of Europe Convention on the Protection of Individuals with regard to Automated Processing of Personal Data of January 28, 1981 – Russia and the Republic of Armenia. Thus, in accordance with Russian legislation, the Republic of Kazakhstan provides adequate protection of the rights of subjects of personal data. As a result, Belarus and Kyrgyzstan, according to the Russian side, cannot properly ensure the security of personal data during their cross-border transfer. However, if the cross-border transfer of personal data is provided for by international treaties of the Russian Federation, then it is possible.

Based on the results of the analysis, it was determined that the problem of creating unified cryptographic means of protecting information during information interaction in the EAEU is extremely urgent at the present time, and the use of cryptographic means of protecting information from producers of countries outside the EAEU increases the risks of economic and national security.

In the conclusion of the article, the corresponding conclusions are drawn.

**Keywords:** cross-border data circulation; digital economy; economic security; cryptography; personal data