Article

СРАВНЕНИЕ ТРАНСФОРМАЦИИ НЕКОТОРЫХ ПОЛОЖЕНИЙ ИНФОРМАЦИОННОГО ЗАКОНОДАТЕЛЬСТВА РОССИИ И ЕС В КОНТЕКСТЕ РЕАЛИЗАЦИИ КОНЦЕПЦИИ КИБЕРБЕЗОПАСНОСТИ

Петр Меньшиков*
Лаурита Михина**

DOI 10.24833/2073-8420-2023-3-68-77-88

Введение. *В статье рассматриваются законодательные основы в сфере информационной и кибербезопасности в России и Европейском Союзе, а также актуальные изменения. Изучаются изменения в законодательстве РФ после принятия 30 декабря 2021 г. № 441-ФЗ «О внесении изменений в статью 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации» и статьи 3 и 5 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации»,[1] а также Конвенция 108 Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» (T-PD) 1981 года[2], Протокол о внесении поправок в Конвенцию о защите физических лиц в отношении обработки персональных данных, принятый Комитетом министров на его 128-й сессии в Эльсиноре 18 мая 2018 года. (Конвенция 108+),[3] Руководящие принципы по защите физических лиц в отношении обработки персональных данных политическими кампаниями и для них 2021 года.[4]*

* **Меньшиков Петр Витальевич**, доктор политических наук, доцент, заведующий кафедрой медийной политики и связей с общественностью МГИМО МИД России
e-mail: p.menshikov@odin.mgimo.ru
ORCID ID: 0000-0001-6547-6032

** **Михина Лаурита Константиновна**, магистрант кафедры МПиСО «Новые медиа и стратегические коммуникации» МГИМО МИД России
e-mail: mik-laura888@yandex.ru
ORCID ID: 0000-0002-7628-3284

[1] Федеральный закон от 30.12.2021 N 441-ФЗ "О внесении изменений в статью 15.3 Федерального закона "Об информации, информационных технологиях и о защите информации" и статьи 3 и 5 Федерального

Материалы и методы. *Материалы исследования составили Федеральный закон от 30.12.2021 N 441-ФЗ «О внесении изменений в статью 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации» и статьи 3 и 5 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации», ФЗ от 27.07.2006 N 152 «О персональных данных»,[5] ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации» от 28.12.2012 N 272,[6] Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» от 12.06.2002 N 67-ФЗ,[7] 108 Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» (T-PD), Конвенция 108+ и Руководящие принципы по защите физических лиц в отношении обработки персональных данных политическими кампаниями и для них 2021 года. Методологическую основу исследования составили следующие общенаучные и специальные методы познания правовых явлений и процессов в сфере защиты персональных данных: метод системно-структурного анализа; метод синтеза социально-правовых явлений; сравнительно-правовой метод; формально-логический метод.*

Результаты исследования. *Российская Федерация реализует многие положения Руководящих принципов по защите физических лиц в отношении обработки персональных данных. Однако есть те предложения, которые не нашли отражение в российских законах. Кроме того, Руководящие принципы по защите физических лиц в отношении обработки персональных данных фактически разрешают организациям передавать данные социальным сетям для рекламы, что в России может быть расценено как нарушение законодательства.*

Обсуждение и заключение. *В настоящий момент сохраняется неопределенность в связи с сотрудничеством России и стран Европы и выходом России из Совета Европы, ЕСПЧ и СПЧ. В скором времени Россия определит перечень европейских конвенций, которые больше не отвечают ее национальным интересам, и денонсирует их. В случае, если Конвенция 108 не попадет в этот перечень, то Россия сможет оставаться участницей Конвенции, а следовательно, и связанных документов. Но все же даже в случае денонсирования рассматриваемой Конвенции и связанных с ней документов некоторые ее позитивные практики могут быть адаптированы российскими законодателями и в немного измененном виде отображены в российских ФЗ.*

закона «О внесении изменений в отдельные законодательные акты Российской Федерации». [Электронный ресурс]. – Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202112300008

[2] 108 Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» (T-PD), 1981. [Электронный ресурс]. – Режим доступа: https://rm.coe.int/1680078c46

[3] Протокол о внесении поправок в Конвенцию «О защите физических лиц в отношении обработки персональных данных», принятый Комитетом министров на его 128-й сессии в Эльсиноре 18 мая 2018 года. (Конвенция 108+) [Электронный ресурс]. – Режим доступа: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[4] Руководящие принципы по защите физических лиц в отношении обработки персональных данных политическими кампаниями и для них 2021 года.

[5] ФЗ от 27.07.2006 N 152 «О персональных данных». [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61801/

[6] ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации» от 28.12.2012 N 272. ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации» от 28.12.2012 N 272. [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_139994/

[7] Федеральный закон «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» от 12.06.2002 N 67-ФЗ. [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_37119/

Введение

С недавних пор в России началась модернизация действующих законов в области информационно-коммуникационной безопасности и кибербезопасности.

У этого был ряд причин, в том числе информационное противостояние ряда западных стран с Россией, дезинформация и попытки некоторых государств пересмотреть итоги Великой Отечественной войны, как следствие растущей тенденции ухудшений отношений с Западом в целом, так и пандемия COVID-19, во время которой, когда весь мир «перешел в онлайн», участились случаи призывов к насилию в сети, разжигания экстремизма, а также онлайн-мошенничества. Все это создало прямую угрозу для российских граждан и суверенитета страны. Необходимо было законодательно закрепить механизм защиты инфраструктуры и населения от данных типов угроз. В свою очередь, и страны Запада активно модернизируют, адаптируют действующие законы в области информационной безопасности. Несмотря на новые политические реалии и явную пробуксовку переговоров по развитию совместной практики в сфере безопасности персональных данных, для России и Европейского Союза все еще остаются площадки для налаживания сотрудничества в данной области. Однако ряд положений европейского законодательства противоречит российскому. Тема информационной и кибербезопасности после начала пандемии и специальной военной операции России на Украине вошла в топ повесток большинства стран мира. Законодательство в информационной сфере во многих из них уже претерпело ряд изменений. В связи с этим изучение и анализ законодательного опыта других стран в сфере безопасности данных и информационной безопасности, а также его сопоставление с российским является крайне актуальным.

Исследование

Актуальные изменения в российском законодательстве о персональных данных и информационной безопасности

После участившихся случаев мошенничества и кибератак с началом пандемии COVID-19 в ряд законов Российской Федерации были внесены существенные изменения. Так, Федеральный закон от 30.12.2021 N 441-ФЗ изменил 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации». В Статье 15.3. говорится о порядке ограничения доступа к информации, которая распространяется с нарушением закона. Теперь статья гласит, что Генеральный прокурор Российской Федерации или его заместители вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере СМИ, с требованием о принятии мер по ограничению доступа к информационным ресурсам, которые распространяют, помимо всего прочего, ложные сообщения об актах терроризма и иной недостоверной общественно значимой информации или информации, содержащей обоснование и (или) оправдание осуществления экстремистской деятельности, включая террористическую деятельность, предложение о приобретении поддельного документа, предоставляющего права или освобождающего от обязанностей.

Новая редакция закона борется с дезинформацией, особенно в области терроризма и любым поощрением экстремистской, террористической или мошеннической деятельности. Закон вводит вполне уместные запреты, поскольку: а) любое ложное предупреждение о готовящейся попытки террористического акта, во-первых, в форме розыгрыша, например, попросту отнимает время у ответственных органов, которые в это время могли бы направить свои усилия на решения других неотложных проблем, во-вторых, может служить отвлекающим маневром для совершения террористического акта, но уже в другом месте, в связи с чем должна налагаться ответственность на информаторов; б) в интернет-среде, например, в блого-сфере, растет число публикаций, призывающих, если не к насилию, то к саботажу или поддержке той деятельности, которая в России считается незаконной, куда также относится продажа поддельных документов.

В настоящее время в условиях санкций и все более радикального, недоказанного или ложного распространения материала в отношении России важно верифицировать любую информацию, в противном случае недостоверная новость может привести к серьезным волнениям внутри страны. Таким образом, поправка актуальна и важна с точки зрения защиты от ложной или экстремистской информации, пропаганды, особенно сейчас. Однако не хватает законодательных пояснений в отношении термина «поддельный документ». Наверняка речь

идет не только о печатной форме, но в том числе, различного рода сделок или незаконной передачи прав. Возможно, в скором времени нам предстоит увидеть разъяснение Верховного Суда о данном положении.

Согласно законодательным изменениям, доступ к информации и информационным ресурсам также может быть ограничен в связи с распространением информационных материалов уже не только иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории Российской Федерации, но и организации, деятельность которой запрещена в соответствии с Федеральным законом от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности» или Федеральным законом от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму»[8, 9]. В России существует перечень организаций, деятельность которых запрещена в РФ по весьма обоснованным причинам, среди которых: разжигание расовой ненависти, призывы к насилию и т.д. Поэтому любые сообщения, поступающие от источника, относящегося к числу запрещенных на территории РФ, должны проверяться и, в случае содержания радикальных или незаконных призывов, блокироваться.

Федеральный закон от 30.12.2021 № 441-ФЗ также внес ряд поправок в Федеральный закон от 29 декабря 2020 года № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». Например, были скорректированы нормы, посвященные функционированию единой биометрической системы. Во-первых, в Законе в пункте 11 Статьи 14.1. о Применении информационных технологий в целях идентификации физических лиц теперь четко прописано, что ЕБС является государственной информационной системой. Во-вторых, в пункте 12 появилось важное разъяснение, регламентирующее порядок утверждения любых положений ЕБС, ее функционирования и взаимодействия с иными информационными системами. Такой порядок утверждается Правительством РФ по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (ФСБ), уполномоченным органом по защите прав субъектов персональных данных (Роскомнадзор) и Центральным банком Российской Федерации. Таким образом, это изменение раскрывает некую последовательность в отношении работы ЕБС. Это, в свою очередь, в случае каких-либо судебных разбирательств в отношении функционирования ЕБС со стороны граждан, упрощает адвокатам, прокурорам изучение дела согласно положениям данного пункта.

В пункт 13 также были внесены корректировки относительно функционирования ЕБС. Там говорится, если физическое лицо, желающее разместить свои биометрические данные в ЕБС, находится за рубежом, то сделать это можно только, если: а) его личность при таком размещении будет подтверждена с использованием документа, удостоверяющего личность гражданина РФ; б) у физлица уже есть учетная запись в единой системе идентификации и аутентификации (ЕСИА, портал госуслуг) ; в) личность указанного в такой записи лица ранее была подтверждена при личной явке. Кроме того, подчеркивается, что сделать это можно исключительно с использованием российского ПО для обработки биометрических персональных данных и с применением пользовательского оборудования, например, телефона или компьютера, имеющего в своем составе идентификационный модуль, то есть SIM.

Изменения также затронули подпункт «ф» 20-го абзаца. Если проведение идентификации/аутентификации биометрических персональных данных необходимо для реализации полномочий публичных органов власти, то обработка этих данных также осуществляется с применением ЕБС. В целом прослеживается тенденция, что ЕБС трансформируется в крупную систему, концентрирующую с целью контроля и безопасности большие объемы биометрии.

Если раньше, согласно поправкам к ФЗ 07.08.2001 № 115 «О противодействии легализации (отмыванию) доходов, полученных

[8] Федеральный закон от 25 июля 2002 года N 114-ФЗ «О противодействии экстремистской деятельности». [Электронный ресурс]. – Режим доступа: https://base.garant.ru/12127578/

[9] Федеральный закон от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму». [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_58840/

преступным путем, и финансированию терроризма»,[10] к ЕБС подключались банки, то теперь это осуществляют и публичные институты, что делает характер ЕБС всеобъемлющим. В случае, если для реализации полномочий госорганов необходимо обработать биометрические персональных данные, которые не проходят по параметрам в ЕБС, то госорганы могут применить другие государственные информационные системы, владельцами/операторами которых являются аккредитованные государственные органы. Это изменение, в свою очередь, демонстрирует мобильность работы с данными, но также в лишний раз показывает, что уполномоченные органы имеют множество путей для получения различной информации по биометрии, что помогает составить наиболее полную картину о физическом лице.

В Законе также сказано, что необходимо обеспечить безопасность персональных данных в соответствии с ФЗ от 27 июля 2006 года № 152-ФЗ «О персональных данных». То есть теперь, согласно базовым правилам законодательства, все законы постепенно выстраиваются в одну взаимосвязанную систему и приводятся в соответствии друг с другом.

Обеспечение безопасности данных, в том числе биометрических, является первостепенной задачей IT-сектора, а также – сложностью. Одним из важнейших положений, появившихся в новой версии ФЗ № 479 «О внесении изменений в отдельные законодательные акты Российской Федерации» от 29.12.2020 стало то, что теперь аккредитованные госорганы в государственных информационных системах могут вести сбор и передачу биометрических персональных данных для размещения в ЕБС и использовать информацию после обработки биометрических персональных данных физических лиц из ЕБС только, если они были произведены в соответствии с изменениями по удаленной регистрации физлиц в ЕБС. Данное изменение призвано обезопасить госорганы от использования ложных данных или полученных незаконным путем, что, конечно, в целом повышает безопасность работы ЕБС. В противном случае, это может привести к целой череде ошибок с использованием персональных данных. Также Закон гласит, что осуществлять в государственных информационных системах аккредитованных госорганов иные операции по обработке биометрических персональных данных запрещено. Так, данное положение строго ограничивает случаи, когда государственные учреждения могут проводить операции с персональными биометрическими данными, что вносит ясность в понимание прав госорганов в плане работы с биометрическими данными, а также способствует обеспечению безопасности данных, поскольку искореняет возможность использования незаконных или ложных данных. Суммируя вышесказанное, Закон делает попытку обеспечения общей безопасности в ЕБС.

В предыдущей версии Федерального закона от 30.12.2021 № 441-ФЗ (имеем в виду ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» от 29.12.2020 № 479-ФЗ), где впервые было введено обязательное требование для банков с универсальной лицензией по открытию счетов и выдачи кредитов через ЕБС, словосочетание «граждане Российской Федерации» было заменено на «физических лиц». Понятие «физическое лицо» шире и включает в себя не только граждан РФ, но также лиц иностранных государств и лиц без гражданства. Здесь законодатели не дают каких-либо пояснений. В связи с этими изменениями Закон распространяет проведение идентификации на всех граждан, а не только на граждан РФ. Теоретически иностранец может удаленно в банке получить кредит, при этом ранее, как изложено в ФЗ «Об отмывании», подтвердив свою личность при личной явке, и его данные пойдут в систему (исключение, как было указано ранее, составляет случай, если человек находится за границей России. Тогда удаленно совершить операцию может только гражданин РФ).

По сути, это важнейшее изменение. Это подтверждает общую политическую линию государства по контролю иностранной деятельности в Российской Федерации. В некотором смысле данные изменения в Законе можно сравнить с Законом «Об иноагентах». Так, эти два закона служат своего рода лакмусовой бумажкой, высвечивая действия иностранных граждан или лиц без граждан-

[10] ФЗ 07.08.2001 N 115 «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_32834/

ства на территории России. В итоге ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» от 29.12.2020 № 479-ФЗ также может помочь выявить экстремистов (или даже террористов), которые по неосторожности сдали свои биометрические данные в ЕБС.

Стоит заметить, что политическая ситуация в мире, связанная с проведением «спецоперации» России на территории Украины, также способствует разработке законодательной базы в России в области безопасности данных. Например, теперь в России действует закон, обязывающий всех трудовых мигрантов сдавать отпечатки пальцев и другие биометрические данные. Все, кто приехал в Россию работать, должны сдавать биометрию (и проходить медосвидетельствование) в течение 30 дней после въезда. Прибывшие с другими целями на срок более 3 месяцев должны сдать биометрию в течение 90 дней.

Подводя итог, следует сказать, что, безусловно, главным опасением в отношении ЕБС является сама безопасность данных. К сожалению, вместе с развитием искусственного интеллекта совершенствуются и навыки мошенников, среди которых не только простые торговцы данными, но и преследующие более опасные цели люди. В настоящее время на информационную структуру России совершается значительное количество кибератак, борьбу с которыми в России провозгласили ряд других официальных документов. Помимо попыток усилить защиту систем данных в России также необходимо провести информационную кампанию, разъясняющую действие данных законов. Больше половины граждан РФ не знают о киберугрозах, о том, как обезопасить свои данные и, более того, зачем вообще это делать. Пока что система законов в сфере регулирования IT, в том числе в сфере ЕБС, представляется сырой и требует пояснений от законодателей, которые пока продолжают рассматривать сценарии по созданию надежного механизма ее функционирования. Об этом свидетельствует и тот факт, что банки попросили регулятор отложить выдачу кредитов по биометрии из-за больших финансовых затрат и просто потому, что не успевают подготовить к этому своих сотрудников. Тем не менее, справедливо заметить, что за последние 3 года Россией был совершен прорыв в области цифровизации и защиты персональных данных. Подтверждением как раз могут являться некоторые законодательные изменения, рассмотренные выше.

108-ая Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» (T-PD) (Конвенция 108+) и Руководящие принципы к ней

Организации, проводящие политические кампании, обрабатывают персональные данные сотрудников и волонтеров кампании, а также кандидатов или потенциальных кандидатов. Кроме того, они также собирают большое количество персональных данных об избирателях, среди которой не только их контактная информация из национального или местного списка избирателей, предоставленного органом, регулирующим выборы, но также и информация о пожертвованиях, финансовых взносах и об их отношении, например, к партии и избирательных намерениях. Растет зависимость организаций, проводящих политические кампании, от частных компаний, которые предоставляют брокерские, аналитические и маркетинговые услуги. В итоге вся система сбора, обработки и хранения персональных данных во время политической кампании очень сложна и непрозрачна. Использование цифровых технологий на выборах, согласно документу, создает угрозы демократии. Например, массовое профилирование электората или рассылка сообщений узким категориям избирателей. Все это приводит к появлению filter-bubble (мыльных информационных пузырей), то есть целенаправленному представлению избирателю только той информации, которая соответствует его избирательным предпочтениям, что может выступать в качестве инструмента для манипулирования и создавать другие угрозы. В перспективе это также может привести к политическому абсентеизму, поляризации общества и росту числа фальсификаций на выборах.

В связи с этим в 2018 году Совет Европы принял Протокол о внесении поправок в Конвенцию о защите физических лиц в отношении обработки персональных данных, тем самым расширив Конвенцию 108 «О защите физических лиц в отношении обработки персональных данных» 1981 года. Теперь документ носит название Конвенция 108+. В ноябре 2021 года Совет Европы разработал Руководящие принципы по защите физических лиц в отношении обработки персональных данных к данной Конвенции, которые предлагают странам-участницам Конвенций руководство по обработке данных, имеющих отношение к политическими кампаниями. Но правила применяются

исключительно к обработке персональных данных избирателей (или потенциальных избирателей) и не распространяются на обработку персональных данных кандидатов, потенциальных кандидатов или сотрудников и волонтеров.

Особый акцент Принципы делают на персональные данные о политических взглядах избирателей, которые защищены статьей 6 108-й Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных». В принципах четко сказано, что обработка данных электората должна быть соразмерной по отношению к законным целям политических кампаний, отражая права и свободы, а сбор данных о предпочтениях избирателей должен быть соразмерен этим целям и не должен приводить к вмешательству в интересы, права и свободы избирателя. Например, согласно документу, эти данные не должны использоваться для вознаграждения сторонников (видимо, организаций-участников кампаний) политическими льготами.

Важное положение, которые прописано в документе, это то, что согласие на обработку персональных данных должно быть получено в каждом контексте, в котором политические кампании взаимодействуют с избирателями – на пороге, по телефону, по электронной почте, в текстовом сообщении, через социальные сети и т.п. Молчание, бездействие не является таким согласием. В российском законодательстве, а именно в ФЗ от 27.07.2006 N 152 «О персональных данных» в статье 15 аналогичным образом говорится, что обработка персональных данных в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. В статье 10 п. 5 также прописано, что «обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных».

В Принципах также говорится, что в случае, когда организация, проводящая политическую кампанию, собирается обработать персональные данные, ссылаясь на «законное основание, установленное законом», то такие основания должны быть написаны в соглашении, а их правовая основа – указана в политике конфиденциальности организации. В качестве примера в Принципах говорится, что организации могут утверждать, что обработка данных необходима для реализации «общественных интересов или преобладающих законных интересов контролера или третьей стороны». Эти интересы также должны быть четко определены законом и должным образом указаны в политике конфиденциальности. Это находит отражение в российском законодательстве. В статье 6 ФЗ от 27.07.2006 № 152 «О персональных данных» говорится, что обработка персональных данных будет являться законной, если она необходима для «осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных». Кроме того, в этой статье в целом предусмотрен ряд случаев, когда обработка персональных данных является законной. По сути, такая обработка является законной, если персональные данные представляют общедоступную информацию. Общедоступная информация, в свою очередь, может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничениями. Но при этом указывается, что использовать такую информацию возможно только при наличии доказательства, что информация была сделана общедоступной самим ее обладателем.

Принципы признают, что организации политических кампаний могут быть обязаны собирать и сообщать информацию о донорах кампании в соответствии с национальным законодательством о финансировании выборов. В российских реалиях это положение актуально, что находит свое отражение в ряде законов, например, в ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации» от 28.12.2012 № 272.

В Принципах говорится, что политическая организация не должна передавать данные избирателей другим организациям, например, с предполагаемыми аналогичными политическими целями или идеологическими взглядами, не имея законного основания или получения явного согласия избирателя. Они также не должны получать данные из социальных сетей в целях создания профи-

лей электората. Однако в документе написано, что в случае, «если избиратель является членом организации или положительно выразил желание следить за кандидатом или партией на платформе социальных сетей, то кампания может обоснованно предположить, что он / она захочет получать дальнейшие сообщения от кандидата или партии». Кодификация этого принципа российским государством может создать правовой вакуум для манипуляций.

Важнейшие положения, вводящиеся Принципами, касаются обработки специальной категории данных о политических взглядах. Так, согласно Конвенции 108+, политические партии и другие организации собирают большие объемы персональных данных, которые раскрывают фактические или предполагаемые политические взгляды, и эти данные относятся к специальной категории данных. Но «персональные данные для информации, которую они раскрывают, касающейся расового или этнического происхождения, политических убеждений, членства в профсоюзах, религиозных или других убеждений, здоровья или сексуальной жизни, допускаются только в тех случаях, когда соответствующие гарантии закреплены в законе, дополняя гарантии Конвенции». При этом такие гарантии должны защищать от рисков, которые обработка конфиденциальных данных может представлять для интересов, прав и основных свобод субъекта данных, особенно риск дискриминации. Дан комментарий, что политические организации могут обрабатывать персональные данные в каждой из этих специальных категорий при условии принятия соответствующих мер предосторожности. В Принципах говорится, «если политические партии и другие организации, проводящие предвыборную кампанию, полагаются на законное основание согласия для сбора данных о политических взглядах и отправки политических сообщений посредством электронных или бумажных сообщений, они должны убедиться, что у них есть соответствующие записи о согласии от физического лица. Также должны быть установлены процедуры регистрации отзыва согласия». Это, в свою очередь, соответствует российскому законодательству, поскольку как уже было сказано, ФЗ № 152 «О персональных данных» ясно дает понять, что обработка данных в целях политической агитации (а также продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи) может осуществляться только с согласия субъекта этих персональных данных. Также в Законе говорится, что оператор должен доказать, что он получил согласие субъекта на обработку. Иначе такая обработка признается осуществляемой без предварительного согласия, то есть незаконной. Что касается отзыва согласия, то это тоже отображено в российском законе. Так, «оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных», если они были обработаны без согласия. В целом, в российской практике избирательных кампаний довольно часто встречаются случаи сбора и передачи персональных данных избирателей для эффективности политической агитации без предварительного согласия субъектов персональных данных. Это прямое нарушение ФЗ «О персональных данных». Самое распространенное нарушение подобного рода – рассылка. Субъект данных имеет полное право предъявить оператору требования немедленно прекратить обработку его данных, и оператор обязан это сделать.

В принципах говорится, что субъекты данных имеют полное право на получение информации о том, как была получена их личная информация и из какого источника. Они также имею право на безоговорочное удаление персональных данных, если возражают против обработки данных в целях политического маркетинга. Кроме того, что, к сожалению, не реализуется в правовой форме на территории России, согласно Принципам, субъекты данных имеют право на получение информации о причинах, лежащих в основе обработки их персональных данных политическими кампаниями. Прямо говорится, что они имеют право на возмещение ущерба, правда не обозначается, в какой форме и объеме. Безусловно, европейский документ также уделяет огромное внимание безопасности данных, о чем свидетельствует статья 7 Конвенции. Так, в нем прямо говорится, что «политические партии и другие организации, проводящие предвыборную кампанию, должны предоставить полный отчет о том, как были получены и обрабатываются персональные данные, а также продемонстрировать соответствие требованиям любой сторонней организации, которая обрабатывает персональные данные от их имени».

Несколько лет назад в странах Европы при распространении агитационных материалов в каждом сообщении избирателю по

закону нужно было указывать, во-первых, источник получения персональных данных, во-вторых, какие он имеет права в отношении их использования, в-третьих, сведения о личности держателя. Скорее всего, это информация не устарела и остается актуальной, что, конечно, все же лучше проверить в официальных источниках этих государств. Однако в российских реалиях данные принципы не действуют. Во время избирательной кампании многие данные транспортируются из одной Избирательной комиссии в другую просто посредством сарафанного радио. Тем не менее, реализовать данные принципы на территории России все же возможно.

В Руководящих принципах прописано, что участники кампании «не должны записывать какую-либо информацию о домохозяйстве субъекта и его обитателях, кроме той, которая свободно и конкретно предоставлена избирателем о его/ее политических взглядах и/или предпочтениях. Они не должны расспрашивать о других членах семьи (особенно детях), арендаторах или жильцах. Они не должны собирать информацию о домашнем хозяйстве или его имуществе (например, автомобилях или других предметах) с целью получения выводов о политических предпочтениях или интересах». Для России реализация этого принципа остается проблематичной. Многие участники кампаний – волонтеры, с которыми порой проводят недостаточно полный инструктаж в отношении того, какие данные можно и нельзя запрашивать. Могут приобретаться «лишние» персональные данные, после чего происходит их утечка. Причины этого также кроятся в низком уровне правовой грамотности граждан. Чтобы решить эту проблему, во всех организациях, которые так или иначе задействованы в избирательной или политической кампаниях, должна проводится информационно-разъяснительная работа. Так, все организаторы и участники кампании обязательно должны быть в курсе правовых последствий за нарушение российского законодательства. Как предлагают Принципы, во время политических кампаний могут работать контролеры, ответственные за безопасность данных.

Есть, однако, в данных Принципах положение, которое, во-первых, противоречит пункту 4.2. 10 самих Принципов (ранее авторами указывалось, что, согласно Принципам, политическая организация не должна передавать данные избирателей другим организациям, например, с предполагаемыми аналогичными политическими целями или идеологическими взглядами, не имея законного основания или получения явного согласия избирателя), а во-вторых, не отвечает требованиям российского законодательства. Так, в документе говорится, что организации, участвующие в политической кампании, могут пересылать персональные данные компаниям социальных сетей в целях цифровой рекламы группам единомышленников. Прописано, что в таком случае обе организации берут на себя совместный контроль над персональными данными и что никакие персональные данные не должны передаваться компаниям социальных сетей в целях рекламы без соответствующего уведомления субъектов данных.

В России в 2021 году президентом был подписан Указ о блокировке незаконной агитации в СМИ, согласно которому Роскомнадзор может прекратить распространение в сети Интернет агитационных материалов, изготовленных или распространяемых с нарушением требований законодательства РФ. К противоправным материалам относятся спланированные, финансируемые агитационные акции, которые оплачиваются не из избирательного фонда кандидата, и материалы, изготовленные с участием несовершеннолетних или иностранцев. Многие подсказки на этот счет можно также найти в статье 56 Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» от 12.06.2002 N 67-ФЗ.

Таким образом, положение, предложенное Руководящими принципами, с точки зрения применения к реалиям России, представляется незаконным. Кроме того, нет пояснений, кто относится к категории «единомышленников». С точки зрения безопасности данных, это является большим пробелом в данном документе.

Результаты исследования

Были рассмотрены законодательные основы в сфере информационной безопасности и кибербезопасности в России и ЕС. Проведенный сравнительный анализ некоторых положений российских законов, Конвенции Совета Европы и Руководящих принципов показал, что подход европейского законодательства в области защиты персональных данных, относящихся к их обработки во время политических кампаний представляется новаторским, однако местами противоречит российскому.

Заключение

В заключение надо отметить, что в целом Российская Федерация реализует многие положения Руководящих принципов Совета Европы. Есть и те предложения, которые не нашли отражение в российских законах и при этом представляются интересными. О некоторых было сказано выше. Можно в качестве примера привести и ряд других, среди которых внимание к вопросу безопасности при использовании данных геолокации и необходимости оценки рисков с целью избежать утечки/удаления персональных данных и другие. Говорится о том, что политика конфиденциальности должна быть легкодоступной и адаптированной для соответствующих лиц. Безусловно, проблема нелегального сбора так называемых cookies актуальна для всего мира. Многие сайты прибегают к манипуляции при описании политики конфиденциальности и изменении настроек, играя на незнании пользователей о том, что их данные могут быть использованы в интересах организации и что им вряд ли захочется подавать в суд на компанию, если согласие было получено обманным путем. Однако Принципы фактически разрешают организациям передавать данные социальным сетям для рекламы, что в России может быть расценено как нарушение законодательства. В данном случае можно обратиться к законодательной практике в отношении таких вопросов и посмотреть, какие решения уже выносили российские суды. В целом 19 декабря 2005 года, когда была ратифицирована сама Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных», Россия заявила, что в соответствии с подпунктом «а» пункта 2 статьи 3 Конвенции не будет применять Конвенцию к персональным данным в ряде случаев. Так, например, Россия оставила за собой право устанавливать ограничения прав субъекта персональных данных на доступ к персональным данным о себе в целях защиты безопасности государства и общественного порядка.

В настоящий момент также уместно отметить недавние события, а именно выход России из Совета Европы, ЕСПЧ и СПЧ. В скором времени Россия определит перечень европейских конвенций, которые больше не отвечают интересам страны и денонсирует их. Если же Конвенция 108+ не попадет в этот перечень, то Россия сможет оставаться участницей Конвенции, а следовательно, и связанных с ней документов, не являясь государством-членом Совета Европы. Если же Конвенцию денонсирует, то ряд ее позитивных положений могут быть адаптированы законодателями и в измененном виде отображены в федеральных законах РФ.

Литература:

1. Бойко С.М. Новые стратегические ориентиры России в области международной информационной безопасности // Международная жизнь. 2021. № 6. С. 52-61.
2. Жидко Е.А., Попова Л.Г. Информационная безопасность модернизируемой России: постановка задачи // Информация и безопасность. 2011. Т. 14. № 2. С. 181-190.
3. Кошкин А.П. Политика информационной безопасности России в условиях цифровизации общества // Цифровая экономика: тенденции и перспективы развития: Сборник тезисов докладов национальной научно-практической конференции: в двух томах, Москва, 22–23 октября 2020 года. Том 1. М., 2020. С. 299-302.
4. Павлишин Б.И., Шевкуненко М.Ю., Инюкин А.Ф. Информационная безопасность как фактор обеспечения национальной безопасности России // Актуальные аспекты управления региональными экосистемами в условиях цифровизации экономики и общества: современные подходы и технологии: материалы международной научно-практической конференции, Краснодар, 25–31 октября 2021 года. Краснодар, 2021. С. 288-292.
5. Савин С.О. О подходах России к международной информационной безопасности // Международная жизнь. 2022. № 4. С. 130-132.
6. Серегин М.И. Информационная безопасность как одна из основных составляющих национальной безопасности современной России // Вопросы политологии. 2017. № 2(26). С. 113-117.
7. Соколова Е.А., Ермошина А.Ю. Роль Банка России в обеспечении информационной безопасности финансовой системы государства // Тенденции развития науки и образования. 2020. № 60-5. С. 78-81. DOI: 10.18411/lj-04-2020-102.

8. Фалеев М.И., Черных Г.С. Угрозы национальной безопасности государства в информационной сфере и задачи МЧС России в этой области деятельности // Стратегия гражданской защиты: проблемы и исследования. 2014. Т. 4. № 1(6). С. 21-34.
9. Халиуллин А.И. Противодействие киберпреступности в России как элемент международной информационной безопасности // Проблемы укрепления законности и правопорядка: наука, практика, тенденции. 2017. № 10. С. 165-172.
10. Чернухин Э.В. О российских инициативах в области противодействия использованию информационно-коммуникационных технологий в преступных целях // Международная жизнь. 2021. № 2. С. 146-151.
11. Ясносокирский Ю.А. Международное информационное право как регулятор международных отношений в сфере информационно-коммуникационных технологий // Международная жизнь. 2022. № 3. С. 88-91.

COMPARISON OF THE TRANSFORMATION OF SOME PROVISIONS OF THE INFORMATION LEGISLATION OF RUSSIA AND THE EU IN THE CONTEXT OF THE CYBER SECURITY CONCEPTION

Introduction. *The article discusses the legislative framework in the field of information and cyber security in Russia and the European Union, as well as relevant changes to them. The changes in the legislation of the Russian Federation after the adoption on December 30, 2021 No. 441-FZ "On Amendments to Article 15.3 of the Federal Law "On Information, Information Technologies and Information Protection" and Articles 3 and 5 of the Federal Law "On Amendments to Certain Legislative Acts of the Russian Federation", as well as Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) of 1981, Protocol amending the Convention for the Protection of Individuals with regard to the Processing of Personal Data, adopted by the Committee of Ministers on its 128th session in Elsinore on 18 May 2018. (Convention 108+), 2021 Guidelines for the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns.*

Materials and methods. *The research materials were compiled by the Federal Law of December 30, 2021 No. 441-FZ "On Amending Article 15.3 of the Federal Law "On Information, Information Technologies and Information Protection" and Articles 3 and 5 of the Federal Law "On Amending Certain Legislative Acts of the Russian Federation ", Federal Law of July 27, 2006 No. 152 "On Personal Data", Federal Law "On measures of influence on persons involved in violations of fundamental human rights and freedoms, rights and freedoms of citizens of the Russian Federation" of December 28, 2012 No. 272, Federal Law "On Fundamental Guarantees of Electoral Rights and the Right to Participate in a Referendum of Citizens of the Russian Federation" No. 67-FZ of June 12, 2002, 108 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), Convention 108+ and the Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns 2021. The methodological basis of the study was the following general scientific and special methods of cognition of legal phenomena and processes in the field of personal data protection: the method of system-structural analysis; method of synthesis of social and legal phenomena; comparative legal method; formal-logical method.*

Results of the study. *The Russian Federation implements many of the provisions of the Guidelines for the Protection of Individuals with regard to the processing of personal data. However, there are those proposals that are not reflected in Russian laws. In addition, the Guidelines for the Protection of Individuals with regard to the processing of personal data actually allow organizations to transfer data to social networks for advertising, which in Russia can be regarded as a violation of the law.*

Discussion and conclusion. *At the moment, uncertainty remains in connection with the cooperation between Russia and European countries and Russia's withdrawal from the Council of Europe, the ECtHR and the HRC. In the near future, Russia will determine the list of European conventions that no longer meet its national interests, and denounce them. If Convention 108 is not included in this list, then Russia will be able to remain a party to the Convention and, consequently, to related documents. But still, even if the Convention under consideration and related documents are denounced, some of its positive practices can be adapted by Russian legislators and reflected in the Russian Federal Law in a slightly modified form.*

Petr V. Menshikov,
Doctor of Political Sciences, Associate Professor, Head of the Department of Media Policy and Public Relations, MGIMO University, Russia

Laurita K. Mikhina,
Master student of the Department of New Media and Strategic Communications, MGIMO University, Russia

Ключевые слова:
кибербезопасность, Россия, ЕС, защита персональных данных, информационная безопасность

Keywords:
cybersecurity, Russia, EU, personal data protection, information security

References:

1. Bojko, S.M., 2021. Novye strategicheskie orientiry Rossii v oblasti mezhdunarodnoj informacionnoj bezopasnosti [New strategic guidelines of Russia in the field of international information security]. *Mezhdunarodnaja zhizn' [The International Affairs].* № 6.
2. Zhidko, E.A., Попова Л.Г., 2011. Informacionnaya bezopasnost' moderniziruemoj Rossii: postanovka zadachi [Information security of modernizing Russia: problem statement]. *Informaciya i bezopasnost' [Information and security].* № 2.
3. Koshkin, A.P., 2020. Politika informacionnoj bezopasnosti Rossii v usloviyah cifrovizacii obshchestva [Information security policy of Russia in the conditions of digitalization of society]. *Cifrovaya ekonomika: tendencii i perspektivy razvitiya: Sbornik tezisov dokladov nacional'noj nauchno-prakticheskoj konferencii: v dvuh tomah. Tom 1. [Digital economy: trends and prospects of development: Collection of abstracts of reports of the National Scientific and Practical Conference: in two volumes. Volume 1].*
4. Pavlishin, B.I., Shevkunenko M.YU., Inyukin A.F., 2021. Informacionnaya bezopasnost' kak faktor obespecheniya nacional'noj bezopasnosti Rossii [Information security as a factor of ensuring the national security of Russia]. *Aktual'nye aspekty upravleniya regional'nymi ekosistemami v usloviyah cifrovizacii ekonomiki i obshchestva: sovremennye podhody i tekhnologii: materialy mezhdunarodnoj nauchno-prakticheskoj konferencii [Current aspects of regional ecosystem management in the context of digitalization of the economy and society: modern approaches and technologies: materials of the international scientific and practical conference].*
5. Savin, S.O., 2022. O podhodah Rossii k mezhdunarodnoj informacionnoj bezopasnosti [About Russia's approaches to international information security]. *Mezhdunarodnaja zhizn' [The International Affairs].* № 4.
6. Seregin, M.I., 2017. Informacionnaya bezopasnost' kak odna iz osnovnyh sostavlyayushchih nacional'noj bezopasnosti sovremennoj Rossii [Information security as one of the main components of the national security of modern Russia]. *Voprosy politologii [Questions of Political Science].* № 2(26).
7. Sokolova, E.A., Ermoshina A.Yu., 2020. Rol' Banka Rossii v obespechenii informacionnoj bezopasnosti finansovoj sistemy gosudarstva [The role of the Bank of Russia in ensuring the information security of the financial system of the state. *Tendencii razvitiya nauki i obrazovaniya [Trends in the development of science and education].* № 60-5.
8. Faleev, M.I., Chernyh G.S., 2014. Ugrozy nacional'noj bezopasnosti gosudarstva v informacionnoj sfere i zadachi MCHS Rossii v etoj oblasti deyatel'nosti [Threats to the national security of the state in the information sphere and the tasks of the EMERCOM of Russia in this field of activity]. *Strategiya grazhdanskoj zashchity: problemy i issledovaniya [Strategy of civil protection: problems and research].* № 1(6).
9. Haliullin, A.I., 2017. Protivodejstvie kiberprestupnosti v Rossii kak element mezhdunarodnoj informacionnoj bezopasnosti [Countering cybercrime in Russia as an element of international information security]. *Problemy ukrepleniya zakonnosti i pravoporyadka: nauka, praktika, tendencii. [Problems of strengthening law and order: science, practice, trends]. № 10.*
10. Chernuhin, Je.V., 2021. O rossijskih iniciativah v oblasti protivodejstvija ispol'zovaniju informacionno-kommunikacionnyh tehnologij v prestupnyh celjah [About Russian initiatives in the field of countering the use of information and communication technologies for criminal purposes]. *Mezhdunarodnaja zhizn' [The International Affairs].* № 2.
11. Jasnosokirskij, Ju.A., 2022. Mezhdunarodnoe informacionnoe pravo kak reguljator mezhdunarodnyh otnoshenij v sfere informacionno-kommunikacionnyh tehnologij [International information law as a regulator of international relations in the field of information and communication technologies]. *Mezhdunarodnaja zhizn' [The International Affairs].* № 3.