УДК 342.723
DOI 10.52452/19931778_2024_1_56

ПРАВОВЫЕ ФОРМЫ И МЕТОДЫ ДОСТИЖЕНИЯ ЗАЩИЩЕННОСТИ ЛИЧНОСТИ ОТ ИНФОРМАЦИОННЫХ УГРОЗ В ЦИФРОВОЙ СРЕДЕ

О.В. Гречкина

Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации, Москва

grechkina-ov@ranepa.ru

Поступила в редакцию 31.10.2023

Даны результаты исследования, посвященного выявлению правовых форм и методов достижения защищенности личности от информационных угроз в цифровой среде. В данной сфере деятельности государства определен ряд форм обеспечения информационной безопасности. Обоснован вывод о том, что обеспечение информационной безопасности личности в основе своей проявляется через правотворческую, правоприменительную и управленческую и контрольно-надзорную деятельность государства.

Ключевые слова: информационная безопасность личности, информационные правоотношения, информационная угроза, правоприменительная и управленческая деятельность, охранительная деятельность, контрольная (надзорная) деятельность.

Развитие научно-технической мысли неуклонно подводит общество к цифровизации различных сфер жизнедеятельности, все большее количество направлений общественной жизни подвергается внедрению цифровых и информационных технологий.

Однако также необходимо учитывать, что столь стремительный рост цифровой мысли и темпы внедрения ее в различные направления абсолютно закономерно приумножают тот уровень угроз, с которыми может столкнуться или уже сталкивается человек и гражданин. Возникновение таких угроз непрерывно поднимает вопрос о противодействии угрозам человеку в информационной среде, методах борьбы с ними и их превенции. Информационная среда, в сегодняшнем ее понимании и представлении, неразрывно связана с цифровыми технологиями, информационной инфраструктурой и т.д., однако все же личность (человек) в ней занимает центральное место, поскольку именно человек является конечным потребителем того информационного продукта, который генерируется в информационной сфере.

В этой связи современной наукой выработана терминологическая единица «информационная безопасность личности». Исходя из общего понимания информационной безопасности как определённого уровня обеспеченности защиты жизнедеятельности человека от угроз, возникающих при информационном взаимодействии [1, с. 58], в данном контексте информационную безопасность личности можно раскрыть как состояние защищенности прав, свобод и законных интересов человека и гражданина в сфере информационного взаимодействия.

Представляется, что информация есть результат взаимодействия субъектов и в юридическом смысле приобретает очертание правоотношений, неотъемлемым элементом состава которых является наличие субъективных прав и обязанностей. Именно поэтому в качестве объекта защиты в представленном определении указаны права, свободы и законные интересы и человек рассматривается как носитель таких прав и участник информационных правоотношений.

В науке имеет место также определение информационной безопасности личности как состояния защищенности, исключающего риск причинения какого-либо вреда человеку [2, с. 102]. С таким определением нельзя согласиться, поскольку оно, во-первых, не определяет объект защиты, а к тому же не учитывает те источники, материалы или технологии, те угрозы информационной безопасности личности, которые содержат лишь потенциальный вред, однако при этом нарушают те или иные права и свободы (например – пропаганда и дезинформация).

В силу основных положений, закреплённых в Конституции Российской Федерации, а равно и в силу общего смысла правового регулирования правоотношений между человеком и государством в Российской Федерации человек, его права и свободы признаются высшей ценностью и, более того, защищаются государством на различных уровнях. Данное конституционное положение в разрезе темы информационной безопасности личности свидетельствует о том, что государственный контроль и регулирование безопасности личности в цифровой и информа-

ционной среде является прямой обязанностью государства.

В этой связи необходимо говорить не только о защите персональных данных граждан и иных информационных ресурсов в случае, если одной из сторон цифровых правоотношений является государство (оказание государственных услуг или использование государственной информационной инфраструктуры), но и при тех обстоятельствах, когда гражданин вступает в цифровые правоотношения в частном порядке, взаимодействует с частными операторами информации, сторонними ресурсами и т.д. На основе приоритета прав и свобод человека формируется и основывается информационная безопасность государства на стратегическом уровне планирования.

Доктрина информационной безопасности (далее – Доктрина), утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, которая по своей сути является осевым документом, образующим систему противодействия информационным угрозам, придает первостепенное значение обеспечению и защите конституционных прав и свобод человека и гражданина посредством перечисления национальных интересов в информационной сфере.

Важно отметить и иные тезисы Доктрины о национальной безопасности в информационной сфере, поскольку они определяют направления и формы деятельности государства по обеспечению информационной безопасности. Так, в перечне национальных интересов в Доктрине, помимо обеспечения защиты информационной инфраструктуры, развития технологий и международного сотрудничества, упоминается и тезис о важности доведения до широкой общественности (внутренней и зарубежной) достоверной информации, связанной с государственной политикой Российской Федерации и позицией России в отношении тех или иных событий в стране и мире. Данное положение, которое, на первый взгляд, имеет опосредованное отношение к обеспечению информационной защищенности личности, имеет прямую связь с противодействием угрозе негативного информационного воздействия на личность извне.

В настоящее время сложившаяся геополитическая обстановка в Европейском регионе и мире формирует новые информационные угрозы, которые в основе своей направлены на дестабилизацию внутренней обстановки в России, подрывную деятельность по отношению к власти и обществу. Упомянутый информационный прогресс приводит также и к тому, что для распространения пропаганды, дестабилизирующей дезинформации и воздействия на политическую и социальную волю субъектов, а таким образом и на основы государственности, источник этой пропаганды больше не нуждается в прямом физическом доступе к объекту информационного воздействия.

Наличие таких обстоятельств вынуждает государственные силы обеспечения информационной безопасности использовать ограничительные меры по отношению к источникам или информационным платформам, которые используются для пропаганды и дезинформации. В результате возникновения новых форм информационного негативного воздействия появляется очередная необходимость разграничения пределов невмешательства государства в частную жизнь, а также устранения разногласий по вопросу свободы доступа к различным (альтернативным) информационным ресурсам.

В целом же функционал государства обеспечен рядом правовых форм, позволяющих прямо или опосредованно влиять на правоотношения под своей юрисдикцией, коими и является информационное взаимодействие. В общем понимании, речь идет о правотворческой, правоприменительной и управленческой, контрольно-надзорной деятельности.

Говоря о правотворческой форме обеспечения информационной безопасности в целом и безопасности личности в частности, отметим, что на характер правотворчества в данной сфере решающее воздействие оказывает особенность регулируемых правоотношений и их предмета. В данном случае первостепенно необходимо поднять вопрос о специфичности предмета правового регулирования. Современная наука описала круг предметов, попадающих под правовое регулирование законодательства об обеспечении информационной безопасности [3, с. 62].

К первой категории предметов относится информация как таковая, то есть вся совокупность данных, сведений и сообщений, ресурсов. В контексте защиты информационной безопасности личности в данной категории нас интересует защита персональных данных и частной жизни личности от любых посягательств. Соответственно, под этим понимается такая деятельность государства, при которой обеспечивается борьба с незаконными посягательствами (преступностью) и создание такой цифровой инфраструктуры, которая обеспечит практическую невозможность незаконной утечки частной информации.

Вторая категория раскрывается через защиту прав субъектов информационных правоотношений, в том числе прав человека и гражданина. При этом под защитой прав, свобод и законных интересов понимается либо недопустимость неправомерного воздействия на субъекта

с использованием той или иной информации (социально неприемлемая информация, пропаганда и дезинформация и т.д.), либо какое-либо ограничение «информационных, цифровых прав» и права на информацию.

Третья категория опосредована защитой информационной инфраструктуры, то есть обеспечением свободного и безопасного доступа к данным, по существу, отнесенным к публичной информации. Ярким примером является политика «цифрового государства», которая направлена на тотальную цифровизацию государственных услуг [4, с. 48]. В данном контексте государству надлежит гарантировать гражданам безопасность использования той или иной информационной и цифровой инфраструктуры, цифровых объектов и т.д. Именно такой характер правового регулирования обеспечивает наиболее успешную организационно-правовую основу для обеспечения цифровой безопасности личности [5, с. 72]. Важным в правовом регулировании общественных отношений, возникающих в связи с использованием цифровых технологий и данных, является учет того обстоятельства, что понятие «цифровые права» по своему содержанию значительно шире буквального понимания нормы части 4 статьи 29 Конституции Российской Федерации, раскрывающей содержание «права на информацию».

Здесь также необходимо отметить, что развитие технологий порождает новые пределы невмешательства государства в частную жизнь гражданина и человека, поскольку именно частная жизнь (персональные данные, переписки и информационный контент частного характера) в большинстве своем перенесена в цифровое пространство. В данном контексте государство при совершенствовании правового регулирования должно учитывать, что право свободно искать, получать, передавать, производить и распространять информацию любым законным способом значительно расширено до перечня таких прав, как право на охрану частной информации в цифровой среде, право на свободный доступ к информационным ресурсам, не отнесенным законом к ограниченным, право на свободный доступ к сети Интернет и обеспечение соответствующими технологиями; перечня таких принципов, как принцип свободного и равного доступа к информации, принцип распространения государственного суверенитета на цифровое пространство (цифровой суверенитет), принцип невмешательства государства в свободный обмен информацией посредством цифровых технологий, приоритета использования передовых технологий в непосредственном участии населения в осуществлении государственной власти и т.д.

В случае с правоприменительной и управленческой деятельностью также необходимо учитывать ряд специфических обстоятельств. Так конституционная новелла (пункт «м» статьи 71 Конституции Российской Федерации) наряду с обороной и безопасностью относит к исключительному предмету ведения Федерации обеспечение информационной безопасности личности, общества и государства при применении информационных технологий и обороте цифровых данных. Данное положение указывает на то, что государственная политика в сфере информационной безопасности личности занимает отдельное место в структуре национальной безопасности, а деятельность органов государственной власти в этом направлении сопоставима по своему значению, например, с оборонной государства от внешней военной угрозы. Очевидно, что в существующих условиях переоценка такой угрозы попросту невозможна, в связи с чем государство берет на себя охранительную функцию в сфере информационного взаимодействия и безопасности. Также важно учитывать, что пресечение угрозы информационной безопасности, в том числе с преступной составляющей, в большинстве случаев возможно за счет управленческих действий на этапе, когда такая угроза еще является потенциальной.

В разрезе реализации охранительной функции государства в сфере информационной безопасности личности и защиты прав субъекта информационных правоотношений возникает вопрос о том, какое количество правоотношений, возникающих по поводу обработки информации, преимущественно относится к частным правоотношениям между двумя негосударственными субъектами. Объектом таких правоотношений зачастую служат персональные данные физических лиц. Такая информация имеет особую специфику, поскольку результатом ее утечки зачастую является угроза совершения неправомерных действий в отношении собственника персональных данных.

При этом охранительная деятельность государства становится актуальной только при тех обстоятельствах, когда потенциальная угроза неправомерного использования данных перерастает в прямую и непосредственную. Использование административных рычагов воздействия на указанные правоотношения должно выражаться в повышении уровня образованности населения в вопросе информационной безопасности и оборота персональных данных, стимулировании развития технологий, позволяющих повышать эффективность защиты персональных данных, развитии взаимодействия государства и гражданского общества в вопро-

сах обеспечения информационной безопасности. Одним из средств непосредственного взаимодействия государства с гражданским обществом по вопросам обеспечения информационной безопасности является целевое сотрудничество с операторами связи и иными операторами информационных систем, направленное на финансовое стимулирование внедрения передовых технологий в сфере обеспечения защиты данных.

Иным аспектом правоприменительной и управленческой деятельности государства в сфере обеспечения информационной безопасности является борьба государства с информацией, которая составляет угрозу непосредственным воздействием на личность. Основными угрозами в данном направлении выступают так называемый «информационный террор» и распространение социально неприемлемой или иной противоправной информации.

Фактически явление информационного террора (информационного терроризма) является элементом информационной войны, которая, в свою очередь, служит одним из элементов гибридного противостояния полюсов мировой политической системы. Правовая точка зрения на данный вопрос заключается в том, что различные научные подходы раскрывают понятие информационного террора по-разному. Единой точкой соприкосновения является подход о необходимости наиболее широкой трактовки данного термина с целью всеобъемлющей борьбы с самим явлением [6, с. 108].

Особым отличительным признаком информационного терроризма является его транснациональный характер. Источник информационной угрозы может осуществлять противоправные действия удаленно, используя при этом информационную инфраструктуру, на которую распространяется цифровой суверенитет Российской Федерации. Инструментами информационного терроризма выступают кибератаки на информационную инфраструктуру органов государственной власти, крупнейших организаций, совершаемые с целью дестабилизации их работы и распространения дезинформации, а также вновь возникшее явление информационно-психологических операций. Под этим собирательным термином, возникшим по большей степени благодаря публицистике, подразумевается ряд противоправных действий, направленных на насыщение российского информационного пространства дезинформирующими сведениями и пропагандой.

В отношении борьбы с кибератаками на информационную инфраструктуру одной из форм противодействия является государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, организационно-правовой основой которой является Указ Президента от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Преимущественный объем задач, возложенный на силы обеспечения информационной безопасности, заключается в координации действий и обмене сведениями между органами государственной власти и владельцами информационных ресурсов, операторами связи и т.д., а также превентивных мерах по оценке состояния информационной инфраструктуры. В вопросах же борьбы с «информационно-психологическими операциями» системные методы и средства не сформированы. Одной из причин такого «пробела» служит характер информации и способ ее распространения. Основой деятельности правонарушителей является распространение неправдивой и вредоносной информации в сети Интернет с использованием общедоступных платформ обмена информацией, таких как социальные сети, форумы, сервисы видеохостинга и прочее. В данном случае борьба с таким явлением сопряжена с анализом большого количества информации и тотальным контролем информационного публичного взаимодействия частных лиц.

Статьей 3 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» регламентирован принцип установления ограничений доступа к информации только федеральными законами. Не учитывая информацию, отнесенную законом к государственной или иной тайне, и исходя из анализа статьи 9 указанного Федерального закона, можно сделать вывод, что целями ограничения доступа к информации является защита конституционного строя, нравственности, здоровья, прав и законных интересов других лиц. Особое значение в данном контексте имеет информация, которая по тем или иным причинам отнесена к виду социально неприемлемой. Ограничение оборота такой информации имеет философско-правовой аспект, который заключается в субъективности понятия «социально неприемлемая информация».

Конституционными положениями предусмотрено, что Российская Федерация является демократическим и правовым государством, в котором каждая личность обладает определенным объемом свобод, в том числе свободой совести, мысли и слова. Вместе с тем субъективность морально-этических взглядов и нрав-

ственности в современном обществе, учитывая отсутствие конкретной определенности в значении термина «социально неприемлемая информация», позволяет недопустимо широко трактовать понятие. Соответственно, в тех или иных случаях приходится неоправданно часто жертвовать частным интересом во благо публичного интереса или распространять критерий неприемлемости на ту информацию, которая по тем или иным причинам к ней не относится.

Представляется, что меры по борьбе с неприемлемой информацией должны быть основаны на принципе сочетания ограничительных и запретительных мер. Необходимо создание нормативных механизмов ранжирования информации от условно неприемлемой (с морально-этической точки зрения), доступ к которой может быть ограничен в зависимости от характеристик потребителя этой информации, до вредной и неправомерной (которая несет непосредственную угрозу конституционному строю, национальным интересам и безопасности государства, имеет целью причинение вреда жизни и здоровью своего потребителя), доступ к которой надлежит ограничивать в полной мере.

Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» регламентирован общий перечень запрещенной к обороту информации (статьи 9 и 10), а также основания и порядок судебного ограничения доступа к информации той или иной категории. Вместе с тем основной проблемой остается точечный характер тех правовых мер (ограничение доступа и применение уголовной либо административной ответственности), которые используются для защиты от нежелательной, неприемлемой и незаконной информации, поскольку существование такой информации в информационном пространстве зависит от скорости ее обнаружения должностными лицами контрольно-надзорных органов.

Заключительной третьей формой обеспечения информационной безопасности личности является деятельность по государственному контролю (надзору) в сфере информации, информационных технологий и защиты информации. При этом в вопросе осуществления контрольно-надзорной деятельности вновь возникает ранее поднятый вопрос о соблюдении баланса между публичными интересами и интересами частных лиц и бизнеса [7, с. 143].

Неоднократно в науке поднимался вопрос о том, насколько соответствует деятельность службы балансу частного и публичного интереса и каким образом органу надлежит в практике осуществления контрольных (надзорных) и правоприменительных функций соблюдать указанный баланс, если сами действующие нормативно-правовые акты не очертили четкие границы между частным и публичным [8, с. 138]. С точки зрения хозяйствования персональные данные клиентов являются ценнейшим экономическим ресурсом, использование которого позволяет автоматизировать деятельность предприятия, повысить качество обслуживания, а также проводить исследование рынка. Вместе с тем существующее положение дел указывает на то, что зачастую персональные данные становятся объектом перепродажи с целью простого приобретения выгоды, что, в свою очередь, в большинстве случаев приводит к причинению того или иного вреда собственнику персональных данных. Передача третьим лицам персональных данных в значительной степени повышает риски мошеннических и иных неправомерных действий в отношении субъектов персональных данных [9, с. 226], что в свою очередь порождает риск, несоизмеримый с интересами бизнеса и субъектов хозяйствования.

Из содержания Постановления Правительства Российской Федерации от 29 июня 2021 г. № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных» следует, что из инструментов превентивного реагирования на угрозы, связанные с неправомерным использованием персональных данных, орган, уполномоченный на осуществление соответствующего контроля, обладает лишь такими средствами, как информирование, обобщение правоприменительной практики, объявление предостережения, консультирование и профилактический визит.

Все перечисленные инструменты имеют лишь надзорный характер и не направлены на превентивное противодействие возможной утечке персональных данных или передаче таких данных третьим лицам, в отношении которых имеются достаточные основания полагать возможность совершения ими противоправных действий с персональными данными. При этом куда более эффективными методами превентивной защиты персональных данных может являться внедрение технологий, позволяющих, во-первых, достоверно отследить любые действия, совершаемые с персональными данными каждого субъекта (включая их обработку, хранение и передачу третьим лицам), а во-вторых, сформировать реестр недобросовестных операторов персональных данных, чьи действия прямо или косвенно привели к компрометации персональных данных или неправомерным действиям с такими данными.

Указанные механизмы позволят повысить эффективность деятельности контролирующих

органов в сфере персональных данных с целью обезопасить личность от нежелательных последствий их утечки или передачи третьим лицам.

Как результат изучения информационной безопасности личности и угроз, возникающих в связи с цифровой социализацией человека и гражданина, можно сделать следующие выводы.

Стремительное развитие технологий и технического прогресса, наряду с порождаемыми благами цифровой цивилизации, образует определенные угрозы, в первую очередь для человека и гражданина (личности) как первичной и самой малозащищённой единицы общества. В данной связи обязанностью государства, исходя из конституционных положений и общих принципов правового регулирования, является купирование таких угроз и защита интересов информационной безопасности личности на этапах превентивного реагирования и облегчения последствий для жертв неправомерных действий в информационной среде.

Обеспечение информационной безопасности личности в основе своей проявляется через правотворческую, правоприменительную и управленческую и контрольно-надзорную деятельность государства.

Ориентиром правотворческой деятельности государства в данной сфере, ввиду ее специфичности, связанной с риском необоснованного притеснения частного интереса, должна служить задача вывести на первый план увеличение роли управленческих инструментов, направленных на профилактику рисков и купирование угроз, а не инструментов охранительной функции государства.

Правоприменение и управление должно исходить из задачи сформировать единую систему технологически оснащенных органов, чьей основной функцией будет не только защита государственной информационной инфраструктуры, но и – первостепенно – защита человека и гражданина от кибертеррора и информационно-психологического воздействия.

Контрольно-надзорная деятельность, используя риск-ориентированный подход, должна формироваться на основе защиты личности от рисков до тех пор, пока таковые становятся фактической реальностью, в частности в вопросах обеспечения безопасности обработки персональных данных.

Статья подготовлена в рамках научно-исследовательской работы на основании государственного задания Российской академией народного хозяйства и государственной службы при Президенте Российской Федерации № 5.5-2023-1 «Совершенствование законодательства в области защищенности личности от информационных угроз в цифровой среде».

Список литературы

1. Мазуров В.А., Невинский В.В. Понятие и принципы информационной безопасности // Известия АлтГУ. 2003. № 2. С. 57–63.

2. Баринов С.В. О правовом определении понятия «Информационная безопасность личности» // Актуальные проблемы российского права. 2016. № 4 (65). С. 97–105.

3. Колесников Ю.А., Худякова Н.В. Обеспечение информационной безопасности как институт современного российского права // Вестник юридического факультета ЮФУ. 2022. Т. 9. № 2. С. 58–64.

4. Понкин И.В. Концепт цифрового государства: понятие, природа, структура и онтология // Государственная служба. 2021. № 5 (133). С. 47–52.

5. Бекишева С.Р., Карибов Р.М. Проблемы взаимодействия институтов гражданского общества и государства в обеспечении информационных прав граждан // Вестник Дагестанского государственного университета. Серия 3. Общественные науки. 2021. Т. 36. Вып. 4. С. 69–75.

6. Саунина Е.В., Бажина И.Д. Международный опыт правового регулирования противодействия информационному терроризму // Вестник Нижегородского университета им. Н.И. Лобачевского. 2022. № 1. С. 108–115.

7. Терещенко Л.К. Государственный контроль в сфере защиты персональных данных // Право. Журнал Высшей школы экономики. 2018. № 4. С. 142–161.

8. Иванский В.П., Мельничук Г.В. Государственный контроль (надзор) – инструмент противодействия угрозам национальной безопасности в информационной сфере или средство защиты неприкосновенности частной жизни: соотношение частного и публичного интересов // Вестник РУДН. Серия: Юридические науки. 2017. № 1. С. 136–152.

9. Швыряев П.С. Утечки конфиденциальных данных: главный враг внутри // Государственное управление. Электронный вестник. 2022. № 91. С. 226–241.

LEGAL FORMS AND METHODS OF ACHIEVEMENT PERSONAL SECURITY FROM INFORMATION THREATS IN THE DIGITAL ENVIRONMENT

O.V. Grechkina

The results of a study devoted to the identification of legal forms and methods for achieving personal protection from information threats in the digital environment are given. A number of forms of information security have been defined in this area of government activity. The conclusion is substantiated that ensuring the information security of an individual is fundamentally manifested through law-making, law enforcement and managerial, control and supervisory activities of the state.

Keywords: personal information security, information legal relations, information threat, law enforcement and management activities, protective activities, control (supervisory) activities.

References

1. Mazurov V.A., Nevinsky V.V. Concept and principles of information security // News of Altai State University. 2003. № 2. P. 57–63.

2. Barinov S.V. On the legal definition of the concept «Information security of the individual» // Current problems of Russian law. 2016. № 4 (65). P. 97–105.

3. Kolesnikov Yu.A., Khudyakova N.V. Ensuring information security as an institution of modern Russian law // Bulletin of the Faculty of Law of the Southern Federal University. 2022. V. 9. № 2. P. 58–64.

4. Ponkin I.V. Concept of the Digital State: Concept, Nature, Structure and Ontology // Public Service. 2021. № 5 (133). P. 47–52.

5. Bekisheva S.R., Karibov R.M. Problems of interaction between institutions of civil society and the state in ensuring the information rights of citizens // Bulletin of the Dagestan State University. Series 3. Social Sciences. 2021. V. 36. Issue 4. P. 69–75.

6. Saunina E.V., Bazhina I.D. International Experience in Legal Regulation of Combating Information Terrorism // Vestnik of Lobachevsky State University of Nizhny Novgorod. 2022. № 1. P. 108–115.

7. Tereshchenko L.K. State control in the field of personal data protection // Law. Journal of the Higher School of Economics. 2018. № 4. P. 142–161.

8. Ivansky V.P., Melnichuk G.V. State control (supervision) – a tool for countering threats to national security in the information sphere or a means of protecting privacy: the relationship between private and public interests // Vestnik PFUR. Series: Legal sciences. 2017. № 1. P. 136–152.

9. Shvyryaev P.S. Leaks of Confidential Data: The Main Enemy Within // Public Administration. Electronic newsletter. 2022. № 91. P. 226–241.