Advances in Law Studies (2020). Vol. 8. Special issue: 79–85
DOI 10.29039/2409-5087-2020-8-5-79-85

ЦИФРОВЫЕ ТЕХНОЛОГИИ
И ЮРИДИЧЕСКАЯ ПРАКТИКА

Правовые режимы защиты персональных данных в условиях цифровизации

УДК 34(340)

Петрова Дарья Анатольевна
Кандидат политических наук, доцент кафедры теории и истории государства и права,
Дальневосточный федеральный университет, Юридическая школа; E-Mail: petrova.dan@dvfu.ru.

Статья получена: 17.03.2020. Рассмотрена: 14.04.2020. Одобрена: 19.05.2020. Опубликована онлайн: 04.06.2020.

Работа выполнена при финансовой поддержке Гранта Президента РФ № НШ-2668-2020.6 «Национально-культурные и цифровые тренды социально-экономического и политико-правового развития Российской Федерации в XXI веке».

Аннотация. Научно-исследовательской целью данной статьи является проблематизация правового регулирования работы с персональными данными и иной конфиденциальной информацией в условиях масштабной цифровизации. Предпринята попытка систематизации основных понятий, используемых при освещении темы информационной безопасности, таких как информация, типы защищаемых данных, утечка информации, типы и каналы утечек информации. Особое внимание уделено режиму безопасности персональных данных: определяются правовая база, особенности назначения санкций, пробелы и коллизии во взаимодействии законодательных актов. Автор приходит к выводу о недостаточности и противоречивости правового регулирования вопросов, связанных с персональными данными и утечками информации, в российском законодательстве.

Ключевые слова: информация, информационная безопасность, персональные данные, утечки информации

Как это ни парадоксально, но в век развития информационных технологий особую актуальность приобрел вопрос информационной безопасности. Перевод практически всех данных в цифровой формат привел к тому, что сохранить значимые сведения становится всё сложнее. Проблема актуальна на всех уровнях: на государственном, корпоративном и личном. Так, на государственном уровне, по словам бывшего министра связи и массовых коммуникаций России, только за один год страна подвергается кибератакам 57 млн раз [7]. Примеры с утечкой информации Сбербанка [16], Альфа-Банка [18], Apple и многих других также говорят о том, что корпорации также не защищены от виртуального взлома. Да и на личном уровне: кто из нас не отвечал с возмущением на телефонные звонки с предложениями записаться на бесплатную пробную процедуру чего-либо? Прежде чем погрузиться в анализ правового регулирования работы с персональными данными, необходимо

LEGAL REGIMES FOR THE PROTECTION OF PERSONAL DATA IN THE CONTEXT OF DIGITALIZATION

Petrova Darya Anatolevna
PhD in Political Science, Associate Professor of the Department of Theory and History of State and Law, Far Eastern Federal University Law School; E-mail: petrova.dan@dvfu.ru.

Manuscript received: 17.03.2020. Revised: 14.04.2020. Accepted: 19.05.2020. Published online: 04.06.2020.

This work was financially supported by the Russian Federation Presidential Grant No. НШ-2668-2020.6 "National-Cultural and Digital Trends in the Socio-Economic, Political and Legal Development of the Russian Federation in the 21st Century".

Abstract. The research purpose of this article is to problematize the legal regulation of working with personal data and other confidential information in the context of large-scale digitalization. An attempt is made to systematize the main concepts used in covering the topic of information security, such as information, types of protected data, information leaks, types and channels of information leaks. Special attention is paid to the personal data security regime: the legal framework, features of sanctions, gaps and conflicts in the interaction of legislative acts are determined. The author concludes that there is insufficient and contradictory legal regulation of issues related to personal data and information leaks in Russian legislation.

Keywords: information, information security, personal data, information leaks

Вид конфиденциальной информации	*Назначение*	*Уточняющий НПА*
Тайна следствия	Данные предварительного расследования не подлежат разглашению без санкции прокурора, следователя и дознавателя	Ст. 161 Уголовно-процессуального кодекса России
Коммерческая тайна	Сведения любого характера (производственные, технические, экономические, организационные и др.), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
Служебная тайна	Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами	Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» как рамочный документ
Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ

определиться с некоторыми ключевыми понятиями, в частности, что именно подразумевается под информацией и защита какой именно информации регламентирована российским законодательством?

Согласно Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информация — это сведения (сообщения, данные) независимо от формы их представления, в том числе и в цифровом формате. Информация в зависимости от категории доступа к ней подразделяется на общедоступную и на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа) [11].

В настоящий момент федеральным законодательством охраняются два типа информации — сведения, составляющие государственную тайну, и конфиденциальная информация.

Государственная тайна — защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации [9]. Правовой режим государственной тайны регламентируется Законом РФ от 21.07.1993 № 5485-1 «О государственной тайне», Постановлением Правительства РФ от 22.08.1998 № 1003 «Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне» и др.

К конфиденциальной информации, согласно Федеральному закону от 27.07.2006 № 149-ФЗ (ред. от 02.12.2019) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 13.12.2019), относятся следующие сведения (см. таблицу).

Данный список не является исчерпывающим, законом предусмотрено существование и иных видов конфиденциальной информации. В отношении всех этих сведений должен соблюдаться ограниченный доступ, однако нередко часть сведений выходит за рамки дозволенных границ хранения информации. В этом случае говорят об утечке информации.

Утечка информации — это неконтролируемое распространение информации за пределы организации, помещения, здания, какой-либо

территории, а также определенного круга лиц, которые имеют доступ к этой информации [12].

Говоря об утечке информации, прежде всего, анализируют каналы ее утечки. Канал утечки информации представляет собой совокупность источника (носителя информации), приемника информации (нарушителя), а также физической среды, по которой происходит распространение информации от источника к приемнику.

Каналы утечки информации, исходя из способов реализации угроз безопасности информации, можно классифицировать следующим образом:

- технические каналы утечки информации;
- несанкционированный доступ к информации;
- каналы утечки информации без использования технических средств.

Утечка информации по техническому каналу — неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. Несанкционированный доступ к информации — доступ к информации, осуществляемый с нарушением установленных прав и(или) правил доступа к информации с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам [12].

Согласно ст. 14 Федерального закона «О государственной охране» одной из обязанностей органов государственной охраны является осуществление во взаимодействии с органами федеральной службы безопасности мер по противодействию утечке информации по техническим каналам [8].

Охватить все виды конфиденциальной информации и режимы их безопасности в одной статье не представляется возможным, поэтому в настоящей работе далее речь пойдет об обеспечении сохранности персональных данных.

Если сведения, составляющие государственную, служебную и коммерческую тайну, всегда были целью заинтересованных лиц, то атаки на записи пользовательских данных стали особенно актуальными после вхождения в практику Big Data. С появлением новой практики возникли и новые игроки — информационные брокеры, или брокеры данных, — компании, специализирующиеся на сборе и продаже личных данных [17]. Особенно брокеры данных популярны в США, где нет специализированного закона о защите персональных данных. Компании составляют досье на человека из различных источников, отражая в нем уровень его дохода, предпочтения в еде, часто используемые сайты, круг знакомств в социальных сетях и т.д., а затем передают эту информацию заинтересованным организациям.

В работе А.И. Савельева содержатся наглядные иллюстрации применения практики информационных брокеров [15]. В частности, одним из наиболее наглядных примеров может являться деятельность сингапурского банка, службы которого отслеживали банковские транзакции, делали вывод о вкусах клиента и направляли ему индивидуальное предложение. Например, клиент расплатился в обеденный перерыв банковской карточкой рядом с улицей, где есть итальянский ресторан. У банка и ресторана заключено партнерское соглашение. Зная, что клиент предпочитает итальянскую еду, банк отправляет смс-уведомление со специальным предложением в этом заведении [15].

Нередко брокеры используют и закрытые данные почтовых учетных записей. В 2019 г. 14 млрд записей пользовательских данных оказались в открытом доступе, что вдвое больше чем в 2018 г., по сведениям Info Watch [17]. В начале декабря 2019 г. в азиатском сегменте Yahoo и Gmail были взломаны и размещены на удаленном сервере 2,7 млрд адресов электронной почты, к половине из этих адресов был и пароль [5]. Поскольку зачастую среди пользователей практикуется использование одного пароля для нескольких учетных записей, то под ударом оказывается информация и данные различных компаний со всего мира.

Утечки персональных данных не обошли стороной и все известные социальные сети. В 2019 г. самый громкий скандал произошел с Facebook, Twitter, LinkedIn и GitHub. По прогнозам специалистов экспертно-аналитического центра InfoWatch, в 2020 г. доля умышленных утечек информации будет только

расти. И основная причина этих утечек — слишком быстрый темп цифровизации [4], в связи с чем компании не успевают разработать эффективный механизм защиты данных.

Проблема сталкеров в Китае также приобретает актуальность в связи со строительством «умных городов», инфраструктура которых основывается на последних технологических разработках [14].

В России деятельность информационных брокеров ограничена Законом о защите персональных данных [10], который требует письменного согласия владельца на обработку информации. Однако, заполняя согласие на обработку при получении дисконтной карты, при подписке на новинки магазина, клиент может обнаружить в форме согласия пункт, позволяющий передавать данные третьим лицам. Это строчка позволит брокерам использовать данные клиентов в дальнейшем.

Каковы же санкции, предусмотренные за утечку персональных данных?

В отношении персональных данных законодатель выбрал бланкетный способ изложения правовых норм, регламентирующих ответственность за нарушение закона о защите персональных данных. Поэтому определить объем и меры ответственности можно, обратившись к Кодексу об административных правонарушениях и Уголовному кодексу.

Кодекс об административных правонарушениях разграничивает сбор данных в автоматизированной форме и неавтоматизированной. Невыполнение оператором обязанности по хранению, систематизации и накоплению информации влечет по п. 8 ст. 13.11 наложение штрафов для граждан от 30 до 50 тыс. руб., на должностных лиц — от 100 до 200 тыс. руб., на юридические лица — от 1 до 6 млн руб.

Ст. 272 Уголовного кодекса устанавливает санкции для лиц за неправомерный доступ к защищаемой информации, если доступ повлек за собой уничтожение, блокирование, модификацию либо копирование компьютерной информации. Преступление наказывается штрафом (до 200 тыс. руб.), либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет. С использованием служебного положения штраф возрастает до 500 тыс. руб, а ограничение свободы изменяется на срок до четырех лет.

Таким образом, можно говорить, что санкции за нарушения закона о защите персональных данных ощутимы, скорее, для граждан и среднего сегмента компаний, которые не располагают значимым количеством данных. Также нам видится по крайней мере две существенные проблемы реализации Закона при утечках персональных данных.

Во-первых, из сферы действия закона выпадает государственное использование фотографии или иного изображения гражданина по основаниям ст. 152.1 Гражданского кодекса РФ. Так, указанная статья гласит, что согласие гражданина на обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, на которых он изображен) не требуется в случаях, когда:

1. Использование изображения осуществляется в государственных, общественных или иных публичных интересах.
2. Изображение гражданина получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и др.), за исключением случаев, когда такое изображение является основным объектом использования.

Второй случай имеет принципиальное значение в свете развития информационных технологий, поскольку именно в местах свободного посещения ведется видеосъемка с функцией распознавания лиц [2]. Логично предположить, что раз технология распознает лицо, сличая с изображением на видеосъемке, существует некая база изображений граждан. Информации о ней мало, и согласия как на обработку изображений, так и на их хранение гражданами не давалось. Таким образом, из-под действия закона о защите персональных данных выводится целый пласт данных. Также открытым остается вопрос о том, какова надежность места хранения изображений.

Интересным с точки зрения защиты персональных данных является заявление губерна-

тора Приморского края О.Н. Кожемяко об использовании тепловизоров для выявления граждан, нарушающих режим самоизоляции [3]. Согласно разъяснению Роскомнадзора [13] информация, получаемая при помощи тепловизора — температура, — также относится к персональным данным, и гражданин должен дать письменное согласие на обработку этой информации. Случай с измерением температуры не подходит под перечень случаев, когда письменное согласие не требуется. Также неясно, будет ли храниться эта информация и каким образом. Поэтому правомерность подобных распоряжений достаточно спорна с юридической точки зрения.

Недовольство граждан политикой государства в отношении применения личных данных уже вызвало судебное разбирательство. В Москве 7 октября 2019 г. гражданка Попова оспаривала действия московского Правительства по использованию технологии распознавания лиц в системе видеонаблюдения российской столицы. Гражданка требовала признать действия московского Правительства незаконными. Суд в удовлетворении иска отказал, однако оговорился, что система сравнивает изображение с видеокамеры с фотографией, которой располагает полиция. Дело направлено в апелляционную инстанцию.

Во-вторых, Закон о персональных данных не имеет экстерриториального действия. В условиях, когда утечка информации произошла по вине иностранного оператора (как, например, Facebook или Twitter), механизм защиты прав граждан действовать не будет. Российский закон о персональных данных всё же оговаривает свое действие в отношении иностранных компаний. Федеральный закон обязывает иностранные компании хранить сведения о россиянах на российских серверах. За отказ локализировать базы данных предполагался сначала штраф 3 000 руб., а в настоящий момент — 4 млн руб. Так, были оштрафованы Facebook и Twitter [6]. Сумма штрафа, на наш взгляд, скорее, выглядит как легальная плата за сбор данных, поскольку никак не сопоставима с доходами названных компаний. За нарушение законодательства даже не предусмотрена блокировка иностранного оператора на территории России. Такая политика создает парадокс — ужесточаются правила в отношении российских компаний, но дается зеленый свет иностранным.

Иная практика сложилась в Европейском Союзе. Принятый в 2018 г. Общий регламент по защите данных как раз распространяет свое действие на всех операторов, которые обрабатывают персональные данные граждан ЕС, даже если эти компании не находятся на территории Союза. На основании процедуры Общего регламента за нарушение конфиденциальности данных были присуждены штрафы американским компаниям Google, Uber и Facebook в размере 50 млн евро в отношении каждого оператора.

В условиях, когда инновационные цифровые технологии и алгоритмические системы знают о нас сегодня значительно больше, чем мы о них, их влияние на нашу публичную и повседневную жизнь колоссально, государственная политика России в отношении защиты персональных данных противоречива [1]. Первое противоречие заключается в том, что государство ограничивает действие Закона о персональных данных. И сохранность государственного хранилища личных сведений вызывает больше вопросов, чем хранение данных в коммерческих компаниях. Второе противоречие связано с предоставлением карт-бланша иностранным компаниям по сбору информации. Слабо контролируя деятельность иностранных фирм по недопущению утечек информации, Закон о персональных данных не имеет никаких четких механизмов привлечения иностранных нарушителей к ответственности.

Литература

1. Баранов П.П., Мамычев А.Ю., Мордовцев А.Ю. Права и свободы человека в цифровую эпоху: проблемы и перспективы политико-правовой динамики // Балтийский гуманитарный журнал. — 2019. — №4(29). — С. 320–324.
2. Воронов А. Их рассматривает полиция: Москва развертывает общегородскую систему распознавания лиц [Электронный ресурс] // Коммерсант. — URL: https://www.kommersant.ru/doc/3819737 (дата обращения: 06.04.2020).
3. Выявлять массовые скопления людей будут дронами с тепловизорами [Электронный ресурс] // Новости Владивостока на VL.ru. — URL: https://www.newsvl.ru/vlad/2020/04/05/189070/ (дата обращения: 06.04.2020).

4. Касперская Н. Утечки конфиденциальной информации: почему их все больше и как с ними бороться [Электронный ресурс]. — URL: https://tass.ru/opinions/7164059 (дата обращения: 04.02.2020).
5. Крупнейший дамп в истории: 2,7 млрд аккаунтов, из них 773 млн уникальных данных [Электронный ресурс] // Хабр. — URL: https://habr.com/ru/post/436420/ (дата обращения: 04.02.2020).
6. Литвиненко Ю. Суд оштрафовал Twitter и Facebook за отказ перенести данные в Россию [Электронный ресурс] // Ведомости. — URL: https://www.vedomosti.ru/technology/articles/2020/02/13/822980-twitter (дата обращения: 06.04.2020).
7. Министр связи РФ: государственная тайна в условиях кибератак охраняется очень надежно [Электронный ресурс] // ТАСС. — URL: https://tass.ru/politika/1487313 (дата обращения: 06.04.2010).
8. О государственной охране: Федеральный закон от 27.05.1996 № 57-ФЗ (ред. от 27.12.2019) [Электронный ресурс] // СПС КонсультантПлюс. — URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=341973&fld=134&dst=1000000001,0&rnd=0.6522750962871502#018310521226940502 (дата обращения: 06.04.2020).
9. О государственной тайне: Закон РФ от 21.07.1993 № 5485-1 (ред. от 29.07.2018) [Электронный ресурс] // СПС КонсультантПлюс. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303613&fld=134&dst=1000000001,0&rnd=0.7603249015120057#07814041078348657 (дата обращения: 02.04.2020).
10. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017) [Электронный ресурс] // СПС КонсультантПлюс. — URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=286959&fld=134&dst=1000000001,0&rnd=0.514433496105853#09751787726001224.
11. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 02.12.2019) (с изм. и доп., вступ. в силу с 13.12.2019) [Электронный ресурс] // СПС КонсультантПлюс. — URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=339396&fld=134&dst=1000000001,0&rnd=0.49790699943065#09569450375932171.
12. Р 50.1.056-2005 Техническая защита информации. Основные термины и определения от 01.06.2006 [Электронный ресурс]. — URL: http://docs.cntd.ru/document/1200044768 (дата обращения: 02.04.2020).
13. Разъяснения Роскомнадзора «Особенности использования тепловизоров работодателями — операторами персональных данных — с целью предотвращения распространения коронавируса» [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_347310/ (дата обращения: 06.04.2020).
14. Русакова Е.П., Барулина В.П., Горбачева А.И. Проблемы обеспечения конфиденциальности персональных данных в условиях реализации кампании по созданию «Умных городов» в Китае: недостатки закона о кибербезопасности // Социально-политические науки. — 2018. — № 5. — С. 201–206.
15. Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. — 2015. — № 1. — С. 43–66.
16. Солдатских В., Горячева В. Клиенты Сбербанка попали на черный рынок [Электронный ресурс] // Коммерсант. — URL: https://www.kommersant.ru/doc/4111863?from=main_1 (дата обращения: 06.04.2010).
17. Урманцева А. Переход на личное: в 2019 году утекло вдвое больше персональных данных [Электронный ресурс] // Известия iz. — URL: https://iz.ru/958561/anna-urmantceva/perekhod-na-lichnoe-v-2019-godu-uteklovdvoe-bolshe-personalnykh-dannykh (дата обращения: 04.02.2020).
18. Чернышова Е. Данные клиентов Альфа-Банка утекли в Сеть [Электронный ресурс] // РБК. — URL: https://www.rbc.ru/finances/05/11/2019/5dbc07929a7947c6597cf70f.

References

1. Baranov P.P., Mamyshev A.Yu., Mordovtsev A.Yu. Rights and freedoms in the digital age: problems and perspectives the political and legal dynamics. *Baltic humanitarian journal*. 2019, no. 4(29), pp. 320–324.
2. Voronov A. They are considered by the police: Moscow is deploying a citywide facial recognition system. *Kommersant*. URL: https://www.kommersant.ru/doc/3819737 (accessed 6 April 2020).
3. Drones with thermal imagers will detect mass concentrations of people. *Vladivostok news on VL.ru portal*. URL: https://www.newsvl.ru/vlad/2020/04/05/189070/ (accessed 6 April 2020).
4. Kasperskaya N. Leaks of confidential information: why there are more and more of them and how to deal with them. *TASS*. URL: https://tass.ru/opinions/7164059 (accessed 4 February 2020).
5. The largest dump in history: 2.7 billion accounts, including 773 million unique data. *Habr*. URL: https://habr.com/ru/post/436420/ (accessed 4 February 2020).
6. Litvinenko Yu. The court fined Twitter and Facebook for refusing to transfer data to Russia. *Vedomosti*. URL: https://www.vedomosti.ru/technology/articles/2020/02/13/822980-twitter (accessed 6 April 2020).
7. Minister of communications of the Russian Federation: state secrets are protected very reliably in the conditions of cyberattacks. *TASS*. URL: https://tass.ru/politika/1487313 (accessed 6 April 2020).
8. About the state protection: Federal law from 27.05.1996 No. 57-FZ (ed. from 27.12.2019). *ConsultantPlus*. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=341973&fld=134&dst=1000000001,0&rnd=0.6522750962871502#018310521226940502 (accessed 6 April 2020).
9. On state secrets: Law of the Russian Federation No 5485-1 from 21.07.1993 (ed. from 29.07.2018). *ConsultantPlus*. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303613&fld=134&dst=1000000001,0&rnd=0.7603249015120057#07814041078348657 (accessed 2 April 2020).
10. On personal data: Law of the Russian Federation from 27.07.2006 No 152-FZ (ed. from 31.12.2017). *ConsultantPlus*. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=286959&fld=134&dst=1000000001,0&rnd=0.514433496105853#09751787726001224.
11. On information, information technologies, and information protection: Law of the Russian Federation from 27.07.2006 No 149-FZ (ed. from 02.12.2019) (with ed. and add., Intro. effective from 13.12.2019). *Consultant plus*.
12. Rosstandart recommendation No. P 50.1.056-2005 Technical protection of information. Basic terms and definitions from 01.06.2006. *Electronic Fund of legal, regulatory and technical documentation*. URL: http://docs.cntd.ru/document/1200044768 (accessed 2 April 2020).

13. Roskomnadzor clarifications "Features of the use of thermal imagers by employers — operators of personal data — in order to prevent the spread of coronavirus". *ConsultantPlus*. URL: http://www.consultant.ru/document/cons_doc_LAW_347310/ (accessed 6 April 2020).
14. Rusakova E.P., Barulina V.P., Gorbacheva A.I. Problems of ensuring the confidentiality of personal data in the context of the implementation of the campaign to create "Smart cities" in China: shortcomings of the law on cybersecurity. *Social and political sciences*. 2018, no. 5, pp. 201–206.
15. Savelev A.I. Problems of application of legislation on personal data in the era of "Big data". *Law. Journal of the Higher school of Economics*. 2015, no. 1, pp. 43–66.
16. Soldatskih V., Goryachev V. Clients of Sberbank was sold on the black market. *Kommersant*. URL: https://www.kommersant.ru/doc/4111863?from=main_1 (accessed 6 April 2010).
17. Urmantseva A. Transition to personal: in 2019, twice as much personal data leaked. *Izvestia iz*. URL: https://iz.ru/958561/anna-urmantceva/perekhod-na-lichnoe-v-2019-godu-uteklo-vdvoe-bolshe-personalnykh-dannykh (accessed 4 February 2020).
18. Chernyshova E. Data of Alfa-Bank clients leaked to the Network. *RBC*. URL: https://www.rbc.ru/finances/05/11/2019/5dbc07929a7947c6597cf70f.