УДК 316.485.6

УТРАТА ГОСУДАРСТВЕННОЙ МОНОПОЛИИ НА ПЕРСОНАЛЬНЫЕ ДАННЫЕ КАК РИСК НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

А. Г. КЛИМАШИН [1)]

[1)]*Институт социологии Национальной академии наук Беларуси, ул. Сурганова, 1, корп. 2, 220072, г. Минск, Беларусь*

С каждым годом становится все очевиднее, что в последние десятилетия государственные структуры подавляющего большинства стран стремительно утрачивают монополию на персональные данные своих граждан. По мнению автора, это представляет определенную угрозу как для личности, так и для национальной безопасности в целом. Проблема вызвана тем, что с развитием интернет-технологий возрастает число сервисных компаний, которые предоставляют услуги информационного характера: доступ к банкам данных, подключение к интернету, разработка приложений для мобильных устройств и т. д. При оказании этих услуг большинство компаний осуществляют сбор персональных данных. При этом необходимость подобных мер не всегда очевидна. Сегодня сложилась ситуация, когда множество сторонних организаций уже получили значительный массив персональной информации, контроль за использованием которой крайне затруднителен. Приводятся результаты последних социологических исследований, согласно которым всего 47 % граждан чувствуют себя в безопасности при работе с глобальной сетью.

Ключевые слова: персональные данные; сведения о личности; личная тайна; монополия; защита личности; информационная безопасность граждан; хостинг; провайдер; разработчики приложений; ощущение безопасности.

PERSONAL DATA STATE MONOPOLY LOOSING AS A NATIONAL SECURITY RISK

A. G. KLIMASHIN [a]

[a]*Institute of Sociology, National Academy of Sciences of Belarus, 1 Surhanava Street, 2 building, Minsk 220072, Belarus*

It is obvious that in recent decades, the state structures of the vast majority of countries are headily losing the monopoly on citizens' personal data. In the author's view, this also poses a threat to the individual and to national security in general. The problem is caused by the fact that the development of Internet technologies increases the number of different service companies that provide information services: access to information data banks, Internet connection, applications for mobile devices and so on. When providing such services, most companies collect personal data and the need for such measures is not always obvious. However, we have come to a situation where many third-party companies have already collected a significant amount of information about citizens, the control of which is extremely difficult.

Keywords: personal data; personal secret; monopoly; personal protection; information security of citizens; hosting; provider; application developers; sense of safety.

Образец цитирования:
Климашин АГ. Утрата государственной монополии на персональные данные как риск национальной безопасности. *Журнал Белорусского государственного университета. Социология.* 2019;3:107–112.

For citation:
Klimashin AG. Personal data state monopoly loosing as a national security risk. *Journal of the Belarusian State University. Sociology.* 2019;3:107–112. Russian.

Автор:
Александр Геннадьевич Климашин – аспирант отдела социологии государственного управления. Научный руководитель – академик НАН Беларуси, доктор философских наук, профессор Е. М. Бабосов.

Author:
Aleksandr G. Klimashin, postgraduate student at the department of the state service sociology.
alexandr89by@mail.ru

Введение

Вопрос защиты информации был актуален всегда. С давних пор наиболее важные сведения кодировались специальными методами. Так, например, во времена Киевской Руси активно использовались иносказания [1, с. 9–20]. Технические средства стали применяться для защиты информации при Петре Первом и получили более широкое распространение с возникновением СССР [1]. При этом актуализация вопроса связана с развитием интернет-технологий и ростом количества пользователей интернета, а также с постоянным увеличением производительности цифровых устройств [2]. Защита информации строится по принципам выявления подлежащих защите объектов информации и определения мер охраны в зависимости от вероятности и значительности ущерба. Одним из таких объектов защиты выступают личная тайна и персональные данные граждан. Следует отметить, что цифровое пространство активно используется некоторыми государствами и транснациональными корпорациями для ведения информационно-алгоритмической войны и воздействия на общественное сознание при помощи методов социальной психологии. Кроме того, персональные данные, собираемые в сети, применяются как крупными группировками для вербовки граждан, так и отдельными злоумышленниками в противоправных целях. Поэтому в цифровую эпоху вопрос информационной безопасности личности занимает центральное место в сфере социологии безопасности, а защита личности выходит на первый план в дискуссиях об обеспечении не только личной, но и корпоративной, а также национальной безопасности [2; 3].

Сегодня наука уделяет большое внимание становлению информационного общества. Различные его аспекты изучают зарубежные и отечественные ученые Р. Ф. Абдеев, В. Ю. Арчаков, Е. М. Бабосов, А. В. Бузгалин, Г. Г. Васильев, О. Н. Вертинская, А. В. Гулякевич, А. Н. Данилов, Г. М. Евелькин, М. В. Ильин, О. С. Макаров, П. Г. Никитенко, А. Тоффлер и др. В своих работах они описывают теоретические модели информационного общества, опираясь на анализ современных тенденций развития мирового социума, глобальных политических и социально-экономических процессов. Многие зарубежные социологи и технические специалисты, такие как Д. Альбертс, Дж. Гебхарт, Г. С. Джоуэт, Н. Кардозо, М. Либицки, Д. А. Мальтизи, Р. Д. Маклорин, Дж. Макафи, Э. Портной, А. Эделыптейн и пр., активно исследуют вопросы информационного противоборства и информационной безопасности. Научное осмысление различных аспектов информационной безопасности осуществлялось российскими учеными А. В. Возженниковым, В. Н. Цыгичко и др. Некоторые исследователи также рассматривают проблему защиты личности от вредного информационного воздействия на психику.

Несмотря на многогранность определения и разницу в интерпретации информационной безопасности, следует сознавать, что прежде всего она направлена на защиту интересов субъектов информационных отношений. Ее основными компонентами являются конфиденциальность, целостность и доступность. При этом информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации. Это принципиально более широкое понятие. Субъект информационных отношений может получить вред в том числе и от поломки системы. В наши дни для многих открытых организаций защита от несанкционированного доступа к информации (*конфиденциальность*) часто стоит по важности отнюдь не на первом месте. Информационная безопасность – многомерная область деятельности, в которой успех может принести только систематический, комплексный подход [4].

Актуальность проработки проблемы в нашей стране очевидна в связи с принятием Концепции информационной безопасности Республики Беларусь и обсуждением проекта закона «О персональных данных».

В 2013 г. в средствах массовой информации стали появляться многочисленные сообщения о новом явлении – кибершпионаже. Широкую известность приобрели проект *WikiLeaks* и сеть «Красный октябрь». Кроме того, участились случаи копирования чужого контента и кражи интеллектуальной собственности. В этот же период государственные органы США и Китая публично высказали взаимные претензии к продукции массового потребления с недокументированными (негласными) возможностями сбора информации. Под подозрение тогда попала почти вся продукция фирм *Huawei* и *ZTE* с китайской стороны и продукция компании *CISCO* с американской стороны. Публичные заявления Эдварда Сноудена фактически подтвердили эти обвинения и активное участие американских государственных структур в сборе персональных данных граждан и чиновников, а также коммерческих сведений о корпорациях и пр. [5].

Таким образом, спектр проблем кибербезопасности очень широк – от технической незащищенности до уязвимости систем, отвечающих за проведение операций с денежными средствами. Ранее обеспечение информационной безопасности сводилось лишь к защите информации (да и то далеко не всей, а только государственной и служебной тайны). Однако объектами правовой защиты в области информационной безопасности выступают права личности и интересы общества в информационной сфере, собственно информация и информационные системы. Сегодня эти объекты видятся необходимыми компонентами состояния информационной безопасности. Вместе с тем особую роль начинает играть защита персональных данных.

Результаты социологических исследований

Отсутствие единообразной интерпретации гражданами понятия «кибербезопасность» вынуждает нас использовать более общие вопросы в социологических исследованиях. По результатам социологического опроса, проведенного весной 2019 г. на базе Института социологии НАН Беларуси, 74,1 % (суммарный процент ответов «да» и «скорее да») респондентов (всего было опрошено 2013 человек) считают, что новые технологии в большей степени делают нашу жизнь комфортной и здоровой. Однако этот же опрос выявил и обеспокоенность граждан вопросами безопасности: 33,8 % респондентов считают, что новые технологии делают нашу жизнь беспокойной и опасной, а 47,2 % опрошенных полагают, что новые технологии могут иметь непредвиденные побочные риски для здоровья и экологии. В сравнении с ощущением безопасности в реальной жизни чувство защищенности в связи с развитием интернет-технологий и при работе с глобальной сетью у граждан намного ниже. Так, в собственном жилище себя ощущают в безопасности 90 % респондентов, на улицах – 84,7 %, на стадионах – 72,1 %. При использовании интернета защищенными себя чувствуют всего 47,3 % (из которых лишь 19,6 % ответили «да», а остальные – «скорее да, чем нет»).

Характер угроз в сети будет совершенно различным, так как она слишком неоднородна и используется людьми для слишком широкого спектра целей. Данный вопрос требует отдельного изучения. Однако анализ показал, что одна из наиболее популярных тем на форумах и конференциях, посвященных проблемам информационной безопасности, – защита персональных данных[1]. Сегодня в Республике Беларусь предпринята попытка законодательно урегулировать вопрос, однако следует учитывать, что большинство хостингов и разработчиков приложений находятся на территории иностранных государств, и, соответственно, белорусское законодательство на них не распространяется. К сожалению, решения белорусских судов крайне редко признаются во многих европейских странах.

На текущий момент в мире нет достоверной информации о количестве провайдеров, хостингов и разработчиков программных средств. Получение такой статистики затруднено в силу отсутствия единой международной базы и лицензирования в данной сфере. Этот факт демонстрирует, что общество не в состоянии контролировать, кто и зачем получает доступ к персональной информации. Долгое время в большинстве стран мира не было законов о защите персональных данных и их сбор никак не регулировался. Значительная часть популярных хостингов находится в странах Европейского союза (Нидерланды, Германия и др.), США, Индии и Китае. Вместе с тем Регламент ЕС 2016/679 (*General Data Protection Regulation*, *GDPR*) о защите персональных данных принят лишь 27 апреля 2016 г. Что касается США и Китая, то они намеренно не вводят единого федерального закона о защите персональной информации, так как производят программные продукты, осуществляющие массовый сбор и анализ персональных данных лиц по всему миру. Нет юридического решения в отношении тех данных, которые уже были получены и используются как в маркетингово-рекламных, так и в преступных целях.

Социальные сети значительно упростили различным сообществам и группировкам первичную оперативную разработку кандидатов, т. е. фактически монополия правоохранительных органов на доступ к персональным данным перестает быть таковой, причем довольно быстрыми темпами. Вместе с тем в теории общественного договора она обоснована исключительным правом государства на насилие. Не секрет, что многие коммерческие и некоммерческие организации активно пользуются механизмами купли-продажи, сбора, обработки и хранения чужих персональных данных. Однако социальные сети способствуют не только потребительскому экстремизму, но и выявлению среди граждан страны «противника» лиц с неудачной карьерой, неудовлетворенностью социальными устоями по сообщениям в прессе, высказываниям в комментариях, блогах и социальных сетях для последующей вербовки в радикальные группировки [6; 7]. При этом следует понимать, что угроза национальной безопасности кроется не в социальных сетях, так как фактически у пользователей есть возможность скрывать профиль от посторонних, вписывать туда ненастоящие данные и т. д., а в том, что существует ярко выраженная тенденция со стороны владельцев сервисов запрашивать у пользователя копию паспорта, номер мобильного телефона, геолокацию, доступ к контактам и т. п. Механизмы полного или частичного отказа от сбора персональных данных фактически отсутствуют. Именно этот аспект следует считать значительным риском для обеспечения защиты граждан Беларуси и вытекающих из этого вопросов национальной безопасности. Вместе с тем необходимость запроса персональных данных владельцы и разработчики интернет-технологий аргументируют той же безопасностью. Философский вопрос заключается в том, кто должен быть гарантом соблюдения прав граждан в этой сфере – государство или некая со-

[1]Internet Governance Forum [Электронный ресурс]. URL: www.intgovforum.org/multilingual/tags/about (дата обращения: 29.04.2019).

вокупность доверенных субъектов? Наиболее традиционным и понятным видится, скорее, первое, однако серьезным вызовом для реализации такого подхода на практике является то, что иностранными компаниями *Google Inc.*, *Facebook Inc.*, ООО «Яндекс», *Telegram Inc.* уже захвачена бóльшая часть аудитории и на текущий момент собран огромный массив данных о гражданах страны. Это заставляет нас переосмыслить традиционные подходы к гарантиям безопасности и искать новые решения.

Согласно данным отчета Института современных медиа (*MOMRI*, Москва), самыми популярными мессенджерами в России являются:

1) *WhatsApp* – 71 % пользователей смартфонов в Москве и 59 % в общем по России;

2) *Viber* – 44 % владельцев смартфонов среди москвичей и 49 % по стране в целом;

3) *Telegram* – 28 % пользователей гаджетов в столице, 19 % – по всей России (сведения на начало 2018 г.) [8].

Серверов ни одного из указанных продуктов нет ни в России, ни в Беларуси [3].

Российско-болгарская компания *Online Market Intelligence* по заказу «Лаборатории Касперского» провела схожий опрос, согласно которому самым используемым белорусами мессенджером оказался *Viber* (93 %). За остальные мессенджеры респонденты проголосовали следующим образом: *Skype* (62 %), *WhatsApp* (41 %), *Telegram* (35 %) [9].

Мессенджеры приобрели свою популярность благодаря тому, что были предназначены для мобильных платформ, что существенно повышало оперативность и удобство коммуникации. *Telegram* во многом позиционируется как самый безопасный мессенджер, что обеспечило ему значительную часть клиентской базы. Вместе с тем у экспертов отсутствует уверенность, что безопасность – это реа-льная забота производителя, а не просто реклама. Вопреки распространенному мнению о безопасности мессенджера *Telegram* стоит задуматься о том, как происходит передача информации. Сотрудники Фонда электронных рубежей (*Electronic Frontier Foundation*) Н. Кардозо, Дж. Гебхарт, Э. Портной называют безопасными совершенно другие сервисы: *ChatSecure*, *CryptoCat*, *Signal*, *Silent Phone* и пр. [10].

Российские эксперты для проведения аналогичного исследования среди необходимых критериев отмечают следующие: 1) степень централизации (*централизованный сервис* – требует сервера, может быть заблокирован; *федеративный* – сеть из серверов, которые общаются друг с другом; *децентрализованный* – протокол *P2P*, т. е. каждый клиент является одновременно и сервером); 2) возможность анонимной регистрации и использования; 3) наличие сквозного шифрования (*E2EE*); 4) защита социального графа (т. е. отсутствие сбора сведений о контактах пользователя и другой метаинформации). Сложно сказать, какой мессенджер лучше: все зависит от того, какие параметры важны для пользователя и какой именно продукт используется в его кругу общения, но из вышеуказанных критериев видно, что большинство мессенджеров, включая *Telegram*, используют централизованный сервер для передачи данных. Независимо от норм законодательства проверить, есть ли в коде программы метод дублирования ключей шифрования, невозможно.

Заключение

Таким образом, в последние десятилетия государственные структуры подавляющего большинства стран утрачивают монополию на персональные данные своих граждан. Это представляет определенную угрозу как для личности, так и для национальной безопасности в целом. При этом под персональными данными следует понимать не только информацию, позволяющую установить личность гражданина, но и сведения об истории его перемещений, поисковых запросах и т. д. Риск возникающей проблемы состоит в том, что при развитии интернет-технологий быстро возрастает число различных сервисных компаний, которые предоставляют услуги информационного характера: доступ к банкам данных, подключение к интернету, разработка цифровых приложений, облачные сервисы, хранение данных на серверах и т. п. При оказании такого рода услуг большинство компаний осуществляют сбор персональных данных в самом широком смысле этого понятия. На текущий момент неизвестно, кто обладает этими сведениями и как они используются. Во многом процесс распространения персональной информации полностью неконтролируем и не поддается эффективной аналитике. Назвать точное количество хостингов в мире крайне сложно. Еще сложнее сказать, сколько всего существует разработчиков приложений. Именно по этой причине большинство граждан понятия не имеют о том, кто фактически получает доступ к их поисковым запросам, контактам и пр. Часть правительств уже обеспокоились этим вопросом. Так, например, по заказу правительства Российской Федерации в 2018 г. на основе тендера «Лабораторией Касперского» была разработана система контроля обмена информацией «Тайга». Ранее схожая система под названием *Trusted Device* была создана в США компанией *CISCO*, однако она изначально писалась для нужд бизнес-среды, а не правительства.

Правовые подходы гласят, что монополия на информацию о своих гражданах есть только у государства. Это утверждение вытекает из монопольного права государства на насилие и проведение

оперативно-розыскных мероприятий, которое является исключительной компетенцией правоохранительных органов [11]. Оперативно-розыскная деятельность выстраивается от объекта разработки, т. е. от конкретной личности. Преступление совершает определенное лицо, и само преступное посягательство совершается, как правило, в отношении конкретного лица [12, гл. 28]. Большинство преступлений невозможны без обладания точной информацией о предмете посягательства, а также без пополнения рядов различных группировок новыми участниками. Именно поэтому центральным звеном при осуществлении любых оперативно-розыскных мероприятий выступает личность [12], а получение ее персональных данных является сущностью таких мероприятий. Говоря о сборе сведений о личности какими-либо приложениями, можно фактически говорить о проведении оперативно-розыскных действий неуполномоченными субъектами.

Обязанность охраны личной тайны закреплена в ст. 28 Конституции Республики Беларусь. Это означает, что такая охрана относится к необходимым функциям государства. С точки зрения практически любой концепции создания государства она выступает гарантом безопасности жизни его граждан. Только при недопущении совершения преступлений в отношении своих граждан государство может обеспечить внутреннюю стабильность. В связи с этим крайне важно не допускать разглашения персональных данных третьим лицам. Большинство работников IT-сферы говорят о необходимости доступа к персональной информации пользователей для качественной работы их сервисов. Однако обоснованность этого не всегда очевидна. Зачастую сбор персональных данных происходит в маркетинговых целях: для дальнейшей перепродажи этих баз данных, использования их для навязывания рекламы, изучения социальной психологии в области потребления различных товаров [13].

Из этого можно сделать вывод, что вместе со всеми удобствами, которые нам дали интернет-технологии, сильно увеличился спектр рисков, связанных с безопасностью. При этом ощущение защищенности граждан в интернете значительно ниже, чем в реальной жизни. Во многом это связано с неизвестностью того, как протекают те или иные процессы, и неуверенностью в том, можно ли доверять крупным корпорациям. Стала очевидной утрата государственной монополии на персональные данные своих граждан. Этот факт влечет за собой пересмотр статуса личности в процессе обеспечения безопасности как таковой. В качестве возможных путей разрешения сложившейся ситуации эксперты предлагают создание защищенных сред и отечественной системы доверенных устройств, повышение общей цифровой грамотности населения. Кроме того, гипотетическим выходом из положения они считают право граждан на анонимность в сети. Если позволить неопределенному кругу лиц использовать неофициальные профили в соцсетях и распределенные сети типа *Tor*, а также разрешить создавать отечественные мессенджеры, то это затруднило бы зарубежным хостингам столь активный сбор информации и явно способствовало бы защите национальных интересов. Вместе с тем стоит задуматься о размещении и развертывании серверов наиболее популярных интернет-продуктов на территории Беларуси.

Библиографические ссылки

1. Бабаш АВ, Баранова ЕК, Ларин ДА. *Информационная безопасность. История защиты информации в России.* Москва: КДУ; 2013. 736 с.

2. Климашин АГ. Возрастание рисков информационной безопасности личности в социальных сетях. В: *Информационная революция и вызовы новой эпохи – стимулы формирования современных подходов к информационной безопасности: материалы Международной научно-практической конференции; 29–30 ноября 2018 г.; Минск, Беларусь. Том 1.* Минск: ИНБ; 2019. с. 173–177.

3. Бабосов ЕМ. Обеспечение информационной безопасности – фактор устойчивого развития Беларуси. *Веснік Брэсцкага ўніверсітэта. Серыя 1. Філасофія. Паліталогія. Сацыялогія.* 2012;2:133–141.

4. Бобкова ВА. *Информационная безопасность и ее составляющие* [Интернет]. 12 марта 2015 г. [процитировано 29 апреля 2019 г.]. Доступно по: https://studfiles.net/preview/2012615/.

5. Безкоровайный ММ, Татузов АЛ. Кибербезопасность – подходы к определению понятия. *Вопросы кибербезопасности.* 2014;1:22–27.

6. Климашин АГ. Информационная безопасность личности в цифровую эпоху. *Известия Национальной академии наук Беларуси. Серия гуманитарных наук.* 2019;64(2):145–150. DOI: 10.29235/2524-2369-2019-64-2-145-150.

7. Климашин АГ. Сетевые террористические сообщества. В: Яскевич ЯС, Терещенко ОВ, Гафарова ЮЮ, редакторы. *Социальные коммуникации в современном мире. Сборник научных статей по материалам работы Первого белорусского философского конгресса; 18–20 октября 2017 г.; Минск, Беларусь.* Минск: БГУ; 2018. с. 387–392.

8. Исследование Telegram аудитории [Интернет]. 16 января 2018 г. [процитировано 29 мая 2019 г.]. Доступно по: http://momri.org/2018/momrinews/issledovanie-telegram-auditorii/.

9. Составлен Топ-5 самых популярных соцсетей и мессенджеров в Беларуси [Интернет]. 31 октября 2018 г. [процитировано 11 марта 2019 г.]. Доступно по: https://thinktanks.by/publication/2018/10/31/sostavlen-top-5-samyh-populyarnyh-sotssetey-i-messendzherov-v-belarusi.html.

10. Cardozo N, Gebhart G, Portnoy E, editors. *Secure Messaging Scorecard: a Study of the Electronic Frontier Foundation* [Internet]. 2018 [cited 2019 March 11]. Available from: https://www.eff.org/node/82654.

11. Об оперативно-розыскной деятельности: Закон Республики Беларусь от 15 июля 2015 г. № 307-З. Национальный центр правовой информации Республики Беларусь. Минск; 2019.

12. Блинов ЮС, Вагин ОА, Вандышев АС, Володько НП, Горяинов КК, Гриб ВГ и др. *Оперативно-розыскная деятельность*. Горяинов КК, Овчинский ВС, Синилов ГК, Шумилов АЮ, редакторы. 2-е издание, дополненное и переработанное. Москва: Инфра-М; 2004. 848 с.

13. Сухарева О. Прямой маркетинг: закон о персональных данных коренным образом изменил правовой статус информации о потребителе. *Арсенал предпринимателя.* 2010;2:18–24.

References

1. Babash AV, Baranova EK, Larin DA. *Informatsionnaya bezopasnost'. Istoriya zashchity informatsii v Rossii* [Information security. History of information security in Russia]. Moscow: KDU; 2013. 736 p. Russian.

2. Klimashin AG. [Increasing risks of personal information security in social networks]. In: *Informatsionnaya revolyutsiya i vyzovy novoi epokhi – stimuly formirovaniya sovremennykh podkhodov k informatsionnoi bezopasnosti. Materialy Mezhdunarodnoi nauchno-prakticheskoi konferentsii; 29–30 noyabrya 2018 g.; Minsk, Belarus'. Tom 1* [Information revolution and challenges of a new era – incentives for the formation of modern approaches in information security. Proceedings of the International scientific and practical conference; 2018 November 29–30; Minsk, Belarus. Volume 1]. Minsk: National Security Institute of the Republic of Belarus; 2019. p. 173–177. Russian.

3. Babosov EM. Provision of information security as a factor for sustainable development of Belarus. *Vesnik of Brest University. Series 1. Philosophy. Politology. Sociology.* 2012;2:133–141. Russian.

4. Bobkova VA. [Information security and its components]. 2015 March 12 [cited 2019 April 29]. Available from: https://studfiles.net/preview/2012615/. Russian.

5. Bezkorovainy MM, Tatuzov AL. Cybersecurity approaches to the definition. *Cybersecurity issues.* 2014;1:22–27. Russian.

6. Klimashin AG. Individual information security in digital era. *Proceedings of the National Academy of Sciences of Belarus. Humanitarian Series.* 2019;64(2):145–150. DOI: 10.29235/2524-2369-2019-64-2-145-150. Russian.

7. Klimashin AG. Network terrorist communities. In: Yaskevich YaS, Tereshchenko OV, Gafarova YuYu, editors. *Sotsial'nye kommunikatsii v sovremennom mire. Sbornik nauchnykh statei po materialam raboty Pervogo belorusskogo filosofskogo kongressa; 18–20 oktyabrya 2017 g.; Minsk, Belarus'* [Social communications in the modern world: collected articles on materials of work of the First Belarusian Congress of Philosophy; 2017 October 18–20; Minsk, Belarus]. Minsk: Belarusian State University; 2018. p. 387–392. Russian.

8. [Research Telegram audience] [Internet]. 2018 January 16 [cited 2019 May 29]. Available from: http://momri.org/2018/momrinews/issledovanie-telegram-auditorii/.

9. [Compiled Top 5 most popular social networks and instant messengers in Belarus] [Internet]. 2018 October 31 [cited 2019 March 11]. Available from: https://thinktanks.by/publication/2018/10/31/sostavlen-top-5-samyh-populyarnyh-sotssetey-i-messendzherov-v-belarusi.html.

10. Cardozo N, Gebhart G, Portnoy E, editors. *Secure Messaging Scorecard: a Study of the Electronic Frontier Foundation* [Internet]. 2018 [cited 2019 March 11]. Available from: https://www.eff.org/node/82654.

11. About operatively-search activity: Law of the Republic of Belarus from 15 July 2015 No. 307-3. National center of the legal information of the Republic of Belarus. Minsk; 2019. Russian.

12. Blinov YuS, Vagin OA, Vandyshev AS, Volod'ko NP, Goryainov KK, Grib VG, et al. *Operativno-rozysknaya deyatel'nost'* [Operatively-search activity]. Goryainov KK, Ovchinskii VS, Sinilova GK, Shumilov AYu, editors. 2th edition, supplemented and revised. Moscow: Infra-M; 2004. 848 p. Russian.

13. Sukhareva O. [Direct marketing: law on personal data radically changed the legal status of information about the consumer]. *Arsenal predprinimatelya.* 2010;2:18–24. Russian.

Статья поступила в редколлегию 25.04.2019.
Received by editorial board 25.04.2019.