



DOI: <https://doi.org/10.15688/ek.jvolsu.2021.3.2>

UDC 338.2  
LBC 65.054

Submitted: 15.06.2021  
Accepted: 29.06.2021

## NATIONAL INFORMATION RISKS OF BIG DATA

Vasily A. Yakhtin

Volgograd State University, Volgograd, Russian Federation

**Abstract.** The importance of this research is determined by the impact of Industry 4.0 technologies on national economic security. The Russian government aims to use modern information technologies as a leading tool of global competitiveness. The scale of public spending on the information & communication and end-to-end technologies development and implementation in the Russian Federation exceeds the majority of socially significant national projects. Industry 4.0 technologies not only provide successful development of the state, but also carry potential threats and risks. The article analyzes the big data technologies impact on the information systems security of private organizations and government agencies. The article considers interpretations of the “big data” category formulated by foreign and domestic researchers. The study reveals a trend describing an increasing number of incidents related to the leakage of personal data and other valuable information. The author modeled the possible damage caused by leaks of personal data and other valuable information incurred by private organizations and government agencies of the Russian Federation for the period from 2016 to 2019. The article identifies the need for improving Russian legislation in the field of big data collection and use. Moreover, the author identifies the necessity for encouraging the introduction of modern information security tools in private organizations and government agencies.

**Key words:** information risks, end-to-end technologies, Industry 4.0, big data, personal data leakage, economic security.

**Citation.** Yakhtin V.A. National Information Risks of Big Data. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Ekonomika* [Journal of Volgograd State University. Economics], 2021, vol. 23, no. 3, pp. 16-25. (in Russian). DOI: <https://doi.org/10.15688/ek.jvolsu.2021.3.2>

УДК 338.2  
ББК 65.054

Дата поступления статьи: 15.06.2021  
Дата принятия статьи: 29.06.2021

## НАЦИОНАЛЬНЫЕ ИНФОРМАЦИОННЫЕ РИСКИ БОЛЬШИХ ДАННЫХ

Василий Александрович Яхтин

Волгоградский государственный университет, г. Волгоград, Российская Федерация

**Аннотация.** Значимость исследования влияния технологий индустрии 4.0 на национальную экономическую безопасность обусловлена нацеленностью Российского государства использовать современные технологии (в том числе информационные) в качестве ведущего инструмента глобальной конкуренции. Масштабы государственных расходов, направленных на развитие и внедрение информационно-коммуникационных и сквозных технологий, превышают большинство социально значимых национальных проектов. Однако технологии индустрии 4.0 не только предопределяют благополучное развитие государства, но также несут в себе потенциальные угрозы и риски. В статье проведен анализ влияния технологий работы с большими данными на безопасность информационных систем частных организаций и государственных структур. Рассмотрены трактовки категории «большие данные», сформулированные зарубежными и отечественными исследователями. Выявлен тренд увеличения количества инцидентов, связанных с утечкой персональных данных и иной ценной информации. Смоделирован возможный ущерб, понесенный частными организациями и государственными структурами Российской Федерации за период с 2016 по 2019 г. вследствие утечек персональных данных и иной ценной информации. Определена необходимость совершенствования законодательства в области сбора и использования больших данных,

стимулирования внедрения современных инструментов защиты информации в частных организациях и государственных структурах.

**Ключевые слова:** информационные риски, сквозные технологии, индустрия 4.0, большие данные, утечка персональных данных, экономическая безопасность.

**Цитирование.** Яхтин В. А. Национальные информационные риски больших данных // Вестник Волгоградского государственного университета. Экономика. – 2021. – Т. 23, № 3. – С. 16–25. – DOI: <https://doi.org/10.15688/ek.jvolsu.2021.3.2>

## Введение

Отличительной чертой прошедших десятилетий стало стремительное развитие информационно-коммуникационных технологий в глобальном масштабе. Начиная от повсеместного распространения сети Интернет и заканчивая образованием сложных «киберфизических систем», технологии стали основополагающим конкурентным преимуществом множества стран, в том числе в сфере экономики. В мировом научном сообществе подобное преобразование получило название «Индустрия 4.0», подразумевающее переход на полностью автоматизированное производство с использованием цифровых технологий, управляемое интеллектуальными системами в режиме реального времени в постоянном взаимодействии с внешней средой, выходящее за границы одного предприятия, с перспективой объединения в глобальную промышленную сеть вещей и услуг (IoT) [Четвертая промышленная революция ...]. Ключевой особенностью, отличающей данный этап промышленной революции от предшествующих, является синергия самых передовых информационных технологий и физических производственных факторов, позволяющая существенно повысить эффективность хозяйственных процессов за счет масштабно-генерируемого объема данных. Общепринято, что технологический спектр индустрии 4.0 образуют следующие базовые технологии:

- большие данные (big data);
- автоматизация и роботизация;
- симуляция;
- промышленный интернет вещей;
- облачные платформы и вычисления;
- виртуальная реальность;
- искусственный интеллект.

Создание и применение вышеуказанных технологий как ключевого фактора усиления конкурентных преимуществ на государствен-

ном уровне обозначено и в Российской Федерации. Подтверждением тому стала принятая Стратегия экономической безопасности Российской Федерации до 2030 года [Указ Президента РФ от 13.05.2017 г. № 208]. Прежде всего, в Стратегии закреплялся факт наличия угрозы, вызванной стремлением развитых государств использовать свои преимущества в уровне развития экономики, высоких технологий (в том числе информационных) в качестве инструмента глобальной конкуренции [Указ Президента РФ от 13.05.2017 г. № 208]. Кроме того, во избежание подобной угрозы экономической безопасности и в целях достижения экономического роста была обозначена необходимость реализации комплекса мер по созданию условий для разработки и внедрения современных технологий, а также создания и устойчивого развития перспективных высокотехнологичных секторов экономики. Позже государством была разработана национальная программа «Цифровая экономика», целью которой стало наращивание эффективности ключевых отраслей экономики за счет внедрения высоких технологий. В соответствии с федеральным проектом «Цифровые технологии» государство намерено добиться собственной независимости в сфере технологий индустрии 4.0 (сквозных технологий) путем поддержки отечественных институтов развития [Паспорт ...]. Реализация данного федерального проекта подразумевает значительное бюджетное и внебюджетное финансирование, превышающее большинство прочих, в том числе социально значимых, федеральных проектов (см. рис. 1).

Учитывая масштабы инвестиций, государство сделало серьезную ставку на информационно-коммуникационные и сквозные технологии как на одни из ключевых факторов устойчивого экономического развития и обеспечения национальной экономической безопасности. Однако стоит еще раз подчеркнуть, что технологии индустрии 4.0 не только спо-

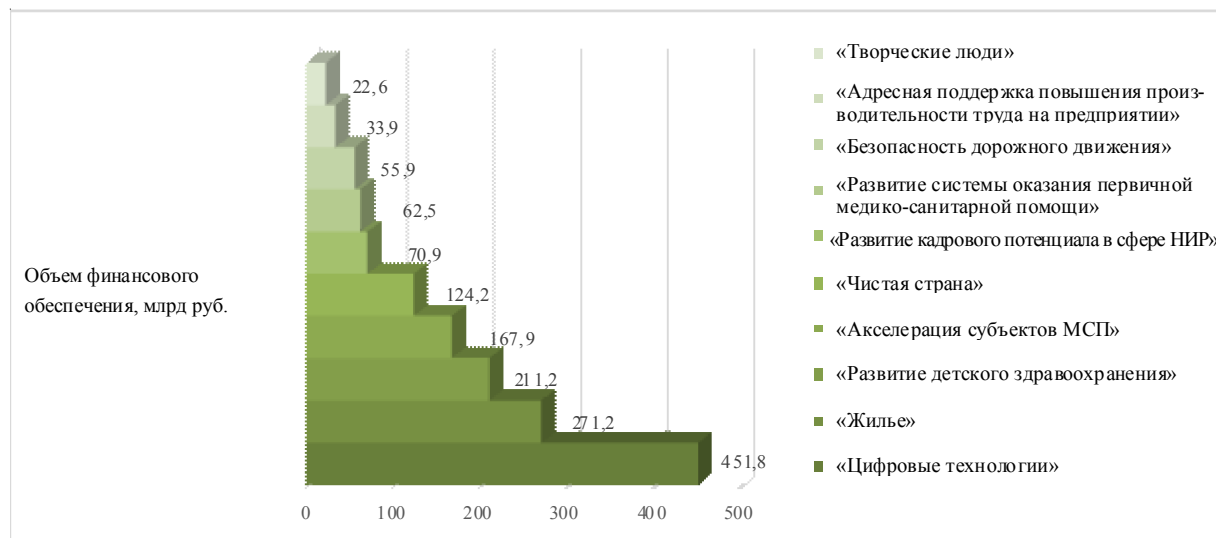


Рис. 1. Суммарный объем финансового обеспечения федеральных проектов Российской Федерации, млрд руб.

Примечание. Составлено автором по: [Будущее России ...].

способствуют благополучному развитию государства, но также несут в себе потенциальные угрозы и риски их реализации.

### Что такое большие данные?

Любая информационная технология представляет угрозу для безопасности информации, поскольку подразумевает работу с определенным набором данных в цифровом виде. Как известно, находясь в цифровом формате, информация легко подвергается копированию, видоизменению, удалению. Ввиду наличия подобных рисков пользователем по своему усмотрению используются традиционные методы защиты информации: ограничение доступа, использование защищенных каналов связи, организация физической защиты помещений и собственно технических средств. Но что если информация представляет собой особую ценность для ее изначального владельца, а субъект при этом даже не подозревает о возможной утечке ценных для него данных? В эпоху стремительного развития технологий индустрии 4.0 реализация подобной угрозы становится все более и более вероятной ввиду появления возможности генерации значительных объемов данных, накапливаемых в результате оцифровывания физического мира.

Примером технологии, оперирующей колоссальными массивами данных, является

сквозная технология, получившая название big data (в переводе с англ. – большие данные). Первоначально термин «big data» получил распространение в западных средствах массовой коммуникации в начале 2000-х гг., после того как отраслевой аналитик Дуг Лэйни сформулировал наиболее встречающееся определение технологии работы с большими данными, аккумулирующее в себе «единство трех V» [Big Data ...]:

1. Объем (Volume): организации собирают данные из различных источников, включающих бизнес-транзакции, интеллектуальные устройства (IoT), промышленное оборудование, социальные сети, а также множество других источников. Обеспечение хранения подобных объемов информации в прошлом было весьма проблематичным, но с появлением более дешевых методов аккумуляции информации, таких как «Data Lake» и «Hadoop», ситуация изменилась в лучшую сторону.

2. Скорость (Velocity): с развитием концепции интернета вещей (IoT) потоки данных на предприятиях стали своевременно обрабатываться с беспрецедентной скоростью. RFID-метки, датчики и интеллектуальные счетчики позволяют формировать колоссальные потоки информации в режиме, близком к реальному времени.

3. Разнообразие (Variety): данные поступают во всех типах форматов – от структури-

рованных числовых данных, используемых в традиционных базах данных, до неструктурированных текстовых документов, электронных писем, видео, аудио, данных биржевых котировок и финансовых транзакций.

Впоследствии данный термин приобрел популярность в научных и деловых кругах по всему земному шару. Исследования в области больших данных вели такие западные ученые, как К. Линч [Lynch, 2008, с. 28–29], Г. Пресс [Press, 2013], М. Кокс и Д. Элсуорт [Cox et al., 1997], Б. Кастерс и Е. Уршич [Custers et al., 2016], В. Майер-Шенбергер и К. Кукьер [Майер-Шенбергер и др., 2014], Д. Бойд и К. Кроуфорд [Boyd et al., 2012], Р. Китчин [Kitchin, 2014]. Однако даже по прошествии многих лет унифицированного определения концепции «больших данных» не существует. Среди представителей отечественной науки также не было достигнуто общего понимания феномена «больших данных», что повлекло за собой публикацию множества статей и исследований, посвященных данной теме. Так, в докладе «Что такое цифровая экономика? Тренды, компетенции, измерение», подготовленном коллективом Института статистических исследований и экономики знаний (ИСИЭЗ) НИУ ВШЭ, было дано следующее определение больших данных: это технологии сбора, обработки и хранения структурированных и неструктурированных массивов информации, характеризующихся значительным объемом и быстрой скоростью изменений (в том числе в режиме реального времени), что требует специальных инструментов и методов работы с ними [Что такое цифровая экономика ... , 2019].

Российский центр компетенций и анализа стандартов ОЭСР определяет big data как огромные массивы данных, полученные в результате слияния различных видов социально-экономической деятельности при помощи интернет-сервисов, таких как социальные сети, электронная коммерция, электронное здравоохранение и электронное правительство [Леващенко, 2016]. При этом отдельно отмечается особая роль больших данных в содействии росту новых отраслей, процессов, продуктов, а также усилению конкурентных преимуществ.

Наиболее объемное определение больших данных было предложено в проекте фе-

дерального закона «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”». В соответствии с законопроектом большие данные – это «совокупность неперсонифицированных данных, классифицирующая по групповым признакам, в том числе информационные и статистические сообщения, сведения о местоположении движимых и недвижимых объектов, количественные и качественные характеристики видов деятельности, поведенческие аспекты движимых и недвижимых объектов, полученных от различных владельцев данных либо из различных структурированных или неструктурированных источников данных, посредством сбора с использованием технологий, методов обработки данных, технических средств, обеспечивающих объединение указанной совокупности данных, ее повторное использование, систематическое обновление, форма представления которых не предполагает их отнесение к конкретному физическому лицу» [О внесении изменений ...].

Однако указанный законопроект не был поддержан представителями российского бизнес-сообщества. Несмотря на отмеченный в определении неперсонифицированный характер собираемых данных, представителями бизнеса неоднократно заявлялось о наличии угрозы интересам граждан Российской Федерации в части ограничения оборота данных о них. Определение больших данных в законопроекте, по мнению представителя Ассоциации больших данных, сформулировано настолько широко и расплывчато, что потенциально включало любые общедоступные данные, в то время как оператором подобных данных мог быть зарегистрирован любой человек, имеющий доступ хоть к какой-то информации. В конечном итоге законопроект был отклонен Правительством Российской Федерации.

Многообразие рассмотренных определений позволяет выделить ключевые особенности категории «большие данные»: подразумевает сбор, обработку, а также хранение структурированных и неструктурированных массивов информации; обусловлена стремительным развитием информационно-коммуникационных технологий; позволяет существенно повысить

эффективность хозяйственных процессов, снизить риски деятельности, усилить конкурентные преимущества субъектов экономики.

### Чем опасны большие данные?

Исходя из рассмотренных определений, сквозная технология big data в силу своей специфики не просто оперирует различной информацией, описанной в цифровом виде, но генерируют колоссальные массивы данных в целях их дальнейшей аналитики. Помимо различной технической информации, получаемой с датчиков устройств, подобные массивы данных содержат персональные и иные конфиденциальные данные пользователей. Источниками персональных данных, как правило, выступают социальные сети и корпоративные базы данных. Президент Ассоциации российских банков академик РАН Г.А. Тосунян в рамках открытой дискуссии отмечал: «Когда мы собираем кредитные истории, то предполагается, что это уже обработанная специальным образом информация, которая принадлежит бюро кредитных историй, поскольку они торгуют ей. Но значительная часть этих данных – это персональная информация. И здесь уже возникает спорный момент: где начинаются большие данные, которые можно использовать, а где это будет вторжение в личную

жизнь» [Дяченко, 2018]. Как известно, подобные данные имеют наибольшую ценность и часто подвергаются краже со стороны злоумышленников.

Утечки непосредственно персональных данных из объемных массивов уже имели место в Российской Федерации в последние годы. Примером тому стал нашумевший случай, произошедший в 2019 г.: персональные данные более 900 тысяч клиентов российских банков оказались в открытом доступе в сети Интернет [Утечка на миллион, 2019]. Ущерб от подобного происшествия не поддается точной оценке, однако наиболее вероятным последствием стало увеличение числа попыток совершения банковского мошенничества. Так, например, представляясь службой безопасности банка, правонарушители могли попытаться ввести в заблуждение доверчивых пользователей, демонстрируя знание персональных данных, или же воспользоваться личными данными в иных преступных целях.

Всего за 9 месяцев 2020 г., по данным InfoWatch (рис. 2), количество утечек информации ограниченного доступа из коммерческих организаций, государственных структур и органов государственной власти в Российской Федерации составило 302 случая, превысив значение предшествующего аналогичного периода на 5,6 % [Утечки информации ...]. Сред-

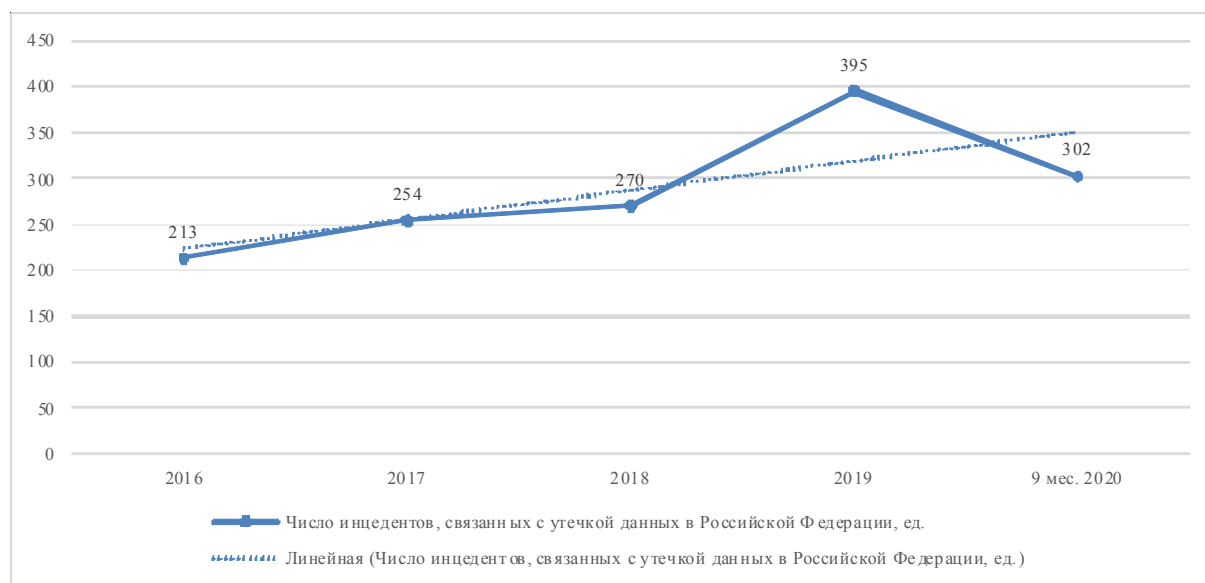


Рис. 2. Число инцидентов, связанных с утечкой данных в коммерческих организациях, государственных структурах и органах государственной власти Российской Федерации, ед.

Примечание. Составлено автором по: [Утечки информации ...].

няя величина одной утечки составляет приблизительно 320 тыс. украденных записей и платежной информации, что значительно меньше среднемировых показателей (5,7 млн записей) ввиду незначительной распространенности в хозяйственной деятельности технологий работы с массивами данных. Однако можно с уверенностью заявить о существовании тренда увеличения числа инцидентов, связанных с утечкой ценных данных.

Утечки конфиденциальных данных влекут за собой и значительный финансовый ущерб. По данным ежегодного исследования IBM и Института Понемона, описывающего стоимость утечек данных по всему миру, средний ущерб, возникающий в результате одной утечки, в 2020 г. составляет приблизительно 3,68 млн долл. США [Cost of a Data ... , 2020] (при расчете были исключены очень небольшие и очень большие по объему утечки). Примечателен тот факт, что понесенный ущерб не сразу отражается на финансовом состоянии пострадавшей организации, а распределяется в течение долгосрочного периода. Основная его доля приходится на первый год (от 60 до 67 % ущерба), в то время как оставшаяся часть распределяется между вторым годом (порядка 20–25 %) и всеми последующи-

ми (от 8 до 20 % понесенного ущерба). На одну утраченную запись приходится в среднем 146 долл. США. Что наиболее примечательно, утечки непосредственно персональных данных подразумевали гораздо больший ущерб: в случае атаки злоумышленников – 175 долл. США, во всех иных случаях – 150 долл. США.

Воспользовавшись результатами исследования IBM и Института Понемона, а также фактами, полученными из аналитических отчетов InfoWatch за последние годы, возможно предположить суммы ущерба, понесенного за период с 2016 по 2019 г. в результате утраты данных в Российской Федерации (рис. 3).

Представленная модель не отражает точного финансового ущерба, понесенного отечественными организациями и государственными структурами, а лишь описывает динамику данного процесса в соответствии со среднемировыми статистическими значениями. Исходя из построенной модели, средний приблизительный финансовый ущерб, понесенный российскими коммерческими и некоммерческими организациями, а также государственными структурами в 2019 г., превысил значения 1,5 млрд долл. США. По курсу на декабрь 2020 г. в российской валюте данный

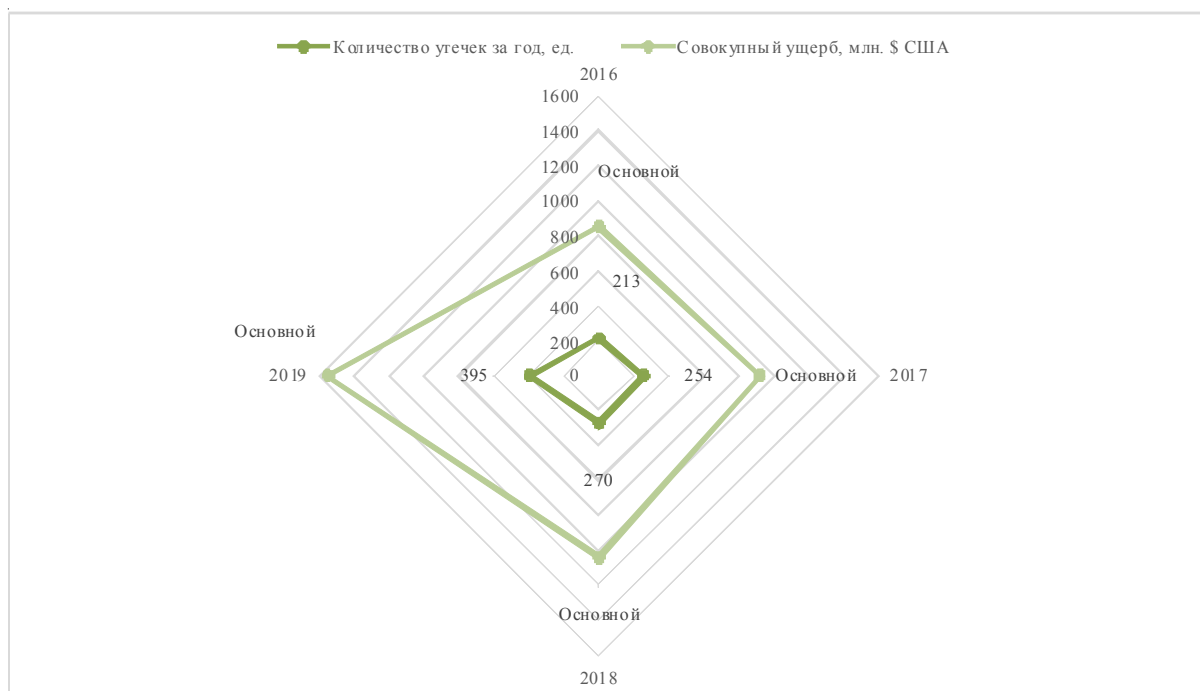


Рис. 3. Совокупный финансовый ущерб от утечки данных в Российской Федерации, млн долл. США

Примечание. Составлено автором по [Cost of a Data ... , 2020; Утечки информации ...].

показатель составляет почти 114,5 млрд рублей. На протяжении последних четырех лет сумма ущерба стабильно увеличивалась: за 4 года рост составил 696 млн долл. США. Данный факт наталкивает на мысль о сохранении подобной тенденции в будущем.

Суммарно за четыре года, в соответствии с моделью, ущерб превысил 332 млрд руб. (по курсу на 02.12.2020). В сравнении с совокупными запланированными расходами на федеральный проект «Цифровые технологии» рассчитанная сумма ущерба составляет более 73 %. Данный факт наглядно демонстрирует наличие колоссальной угрозы, формируемой со стороны новейших технологий, в частности технологий сбора и анализа больших данных. Учитывая факт существования стабильной динамики увеличения числа инцидентов, связанных с утечкой ценных данных, а также намерения государства использовать сквозные технологии как один из ключевых факторов устойчивого экономического развития, необходима разработка механизмов управления рисками информационной безопасности с опорой на опыт зарубежных стран: начиная от совершенствования правовой среды и заканчивая способствованием внедрению современных инструментов защиты информации в частных организациях и государственных структурах. В противном случае потенциальные положительные эффекты от внедрения новейших технологий могут быть нивелированы отрицательным воздействием последних на социально-экономические процессы.

### **Выводы**

Таким образом, проведенный анализ рисков информационной безопасности, возникающих в результате распространения сквозных технологий, позволяет сделать следующие ключевые выводы:

1. Генерация больших данных, одной из ключевых сквозных технологий, подразумевает сбор колоссальных массивов структурированной и неструктурированной информации, которая, помимо технических индикаторов, также содержит персональные данные пользователей и иные данные, представляющие ценность.

2. В Российской Федерации, наряду с другими странами, ежегодно происходят крупные утечки информации, в совокупности влекущие за собой утрату миллионов записей персональных данных.

3. Наблюдается устойчивый тренд на увеличение числа инцидентов, связанных с утечкой данных в коммерческих организациях, государственных структурах и органах государственной власти Российской Федерации.

4. Утечки персональных и иных ценных данных влекут за собой значительный финансовый ущерб, ежегодно насчитывающий сотни миллионов в долларовом эквиваленте. В Российской Федерации суммы подобного ущерба стабильно увеличивались на протяжении последних четырех лет.

5. Существующий тренд на увеличение числа инцидентов, связанных с утечкой ценных данных, а также наличие заинтересованности государства в формировании устойчивого конкурентного преимущества на основе сквозных технологий свидетельствуют о необходимости выработки отлаженного механизма управления рисками информационной безопасности: начиная с совершенствования законодательных основ и заканчивая повсеместным внедрением более совершенных технических инструментов защиты информации.

### **СПИСОК ЛИТЕРАТУРЫ**

- Будущее России. Национальные проекты // ТАСС, информационное агентство. – Электрон. текстовые дан. – Режим доступа: <https://futurerussia.gov.ru> (дата обращения: 24.11.2020). – Загл. с экрана.
- Дяченко, О. Большие данные и искусственный интеллект на службе банку / О. Дяченко // Национальный банковский журнал. – 2018. – Электрон. текстовые дан. – Режим доступа: <http://nbj.ru/publs/upgrade-modernizatsija-i-razvitie/2018/03/02/bol-shie-dannye-i-iskusstvennyi-intellekt-na-sluzhbe-banku/index.html> (дата обращения: 27.11.2020). – Загл. с экрана.
- Леващенко, А. Экономика, управляемая большими данными / А. Леващенко // Центр компетенций и анализа стандартов ОЭСР РАНХиГС. – 2016. – Электрон. текстовые дан. – Режим доступа: <https://oecd-russia.org/analytics/ekonomika-upravlyaemaya-bolshimi-dannymi.html> (дата обращения: 25.11.2020). – Загл. с экрана.

- Майер-Шенбергер, В. Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим / В. Майер-Шенбергер, К. Кукбер; пер. с англ. И. Гайдюк. – М.: Манн, Иванов и Фербер, 2014. – 240 с.
- О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»: Проект Минкомсвязи России от 14.02.2020 г. // Федеральный портал проектов нормативных правовых актов. – Электрон. текстовые дан. – Режим доступа: <https://regulation.gov.ru/projects#npa=9958140391> (дата обращения: 25.11.2020). – Загл. с экрана.
- Паспорт федерального проекта «Цифровые технологии» // Сайт национальной программы «Цифровая экономика Российской Федерации». – Электрон. текстовые дан. – Режим доступа: <https://digital.ac.gov.ru/poleznaaya-informaciya/4106> (дата обращения: 24.11.2020). – Загл. с экрана.
- Указ Президента Российской Федерации от 13.05.2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» // Портал Президента России. – Электрон. текстовые дан. – Режим доступа: <http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102432051> (дата обращения: 24.11.2020). – Загл. с экрана.
- Утечка на миллион // Коммерсантъ. – 2019. – № 99 (10 июня). – С. 8. – Электрон. текстовые дан. – Режим доступа: <https://www.kommersant.ru/daily/2019-06-10> (дата обращения: 25.11.2020). – Загл. с экрана.
- Утечки информации ограниченного доступа: отчет за 9 месяцев 2020 г. // Аналитический отчет InfoWatch. – Электрон. текстовые дан. – Режим доступа: <https://www.infowatch.ru/analytics/reports/30708> (дата обращения: 26.11.2020). – Загл. с экрана.
- Четвертая промышленная революция. Популярно о главном технологическом тренде XXI века // TAdviser. – Электрон. текстовые дан. – Режим доступа: <https://www.tadviser.ru/a/371579> (дата обращения: 23.11.2020). – Загл. с экрана.
- Что такое цифровая экономика? Тренды, компетенции, измерение / авт. кол.: Г. И. Абдрахманова [и др.]; науч. ред. Л. М. Гохберг // XX Апрель. Междунар. науч. конф. по проблемам развития экономики и общества, г. Москва, 9–12 апр. 2019 г. – М.: Изд. дом Высшей школы экономики, 2019. – С. 14–15.
- Big Data: What it is and Why it Matters // Аналитическая компания SAS. – Электрон. текстовые дан. – Режим доступа: [https://www.sas.com/ru\\_ru/insights/big-data/what-is-big-data.html](https://www.sas.com/ru_ru/insights/big-data/what-is-big-data.html) (дата обращения: 25.11.2020). – Загл. с экрана.
- Boyd, D. Critical Questions for Big Data / D. Boyd, K. Crawford // *Information, Communication & Society*. – 2012. – Vol. 15, № 5. – P. 37–41. – DOI: 10.1080/1369118X.2012.678878.
- Cost of a Data Breach Report, 2020 // IBM & Ponemon Institute. – Electronic text data. – Mode of access: <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/> (date of access: 01.12.2020). – Title from screen.
- Cox, M. Application-Controlled Demand Paging for Out-of-Core Visualization: Report NAS-97-010, July 1997 / M. Cox, D. Ellsworth. – Electronic text data. – Mode of access: <https://www.nasa.gov/assets/pdf/techreports/1997/nas-97-010.pdf> (date of access: 26.11.2020). – Title from screen.
- Custers, B. Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection / B. Custers, H. Uršič // *International Data Privacy Law*. – 2016. – Vol. 6, № 1. – P. 4–15. – DOI: 10.1093/idpl/ipv028.
- Kitchin, R. Big Data, New Epistemologies and Paradigm Shifts / R. Kitchin // *Big Data & Society*. – 2014. – Vol. 1, № 1. – P. 1–12. – DOI: 10.1177/2053951714528481.
- Lynch, C. Big Data: How do Your Data Grow? / C. Lynch // *Nature*. – 2008. – № 7209. – P. 28–29. – DOI: 10.1038/455028a.
- Press, G. A Very Short History of Big Data / G. Press // *Forbes.com*. – 2013. – Electronic text data. – Mode of access: <https://www.forbes.com/sites/gilpress/2013/05/09/a-very-shorthistory-of-big-data/#92208b965a18> (date of access: 26.11.2020). – Title from screen.

## REFERENCES

- Budushhee Rossii. Nacional'nye proekty [The Future of Russia. National Projects]. *TASS, informacionnoe agentstvo* [TASS News Agency]. URL: <https://futurerussia.gov.ru> (accessed 24 November 2020).
- Djachenko O. Bol'shie dannye i iskusstvennyj intellekt na sluzhbe banku [Big Data and Artificial Intelligence at the Service of a Bank]. *Nacional'nyj bankovskij zhurnal* [National Banking Journal], 2018. URL: <http://nbj.ru/pubs/upgrade-modernizatsija-i-razvitie/2018/03/02/bolshie-dannye-i-iskusstvennyi-intellekt-na-sluzhbe-banku/index.html> (accessed 27 November 2020).
- Levashhenko A. Jekonomika, upravljajemaja bol'shimi dannymi [Big Data Economy]. *Centr kompetencij i analiza standartov OJeSR RANHiGS* [RANEPa Center of Competence and Analysis of OECD Standards], 2016. URL: <https://>



- oecd-russia.org/analytics/ekonomika-upravlyaemaya-bolshimi-dannymi.html (accessed 25 November 2020).
- Majer-Shenberger V., Kuk'er K. *Bol'shie dannye. Revoljucija, kotoraja izmenit to, kak my zhivem, rabotaem i myslim* [Big Data. A Revolution that Will Transform How We Live, Work, and Think]. Moscow, Mann, Ivanov and Ferber Publ., 2014. 240 p.
- O vnesenii izmenenij v Federal'nyj zakon «Ob informacii, informacionnyh tehnologijah i o zashhite informacii»: Proekt Minkomsvjazi Rossii ot 14.02.2020 g. [On Amendments to the Federal Law “On Information, Information Technologies and Information Protection”: The Ministry of Communications of the Russian Federation Draft Dated February 14, 2020]. *Federal'nyj portal proektov normativnyh pravovyh aktov* [The Federal Portal of Draft Regulatory Legal Acts]. URL: <https://regulation.gov.ru/projects#npa=9958140391> (accessed 25 November 2020).
- Pasport federal'nogo proekta «Cifrovye tehnologii» [Passport of the Federal Project “Digital Technologies”]. *Sajt nacional'noj programmy «Cifrovaja jekonomika Rossijskoj Federacii»* [Website of the National Program “Digital Economy of the Russian Federation”]. URL: <https://digital.ac.gov.ru/poleznaya-informaciya/4106> (accessed 24 November 2020).
- Ukaz Prezidenta Rossijskoj Federacii ot 13.05.2017 g. № 208 «O Strategii jekonomicheskoj bezopasnosti Rossijskoj Federacii na period do 2030 goda» [The Decree of the President of the Russian Federation No. 208 Dated May 13, 2017 “On the Economic Security Strategy of the Russian Federation for the Period up to 2030”]. *Portal Prezidenta Rossii* [Portal of the President of Russia]. URL: <http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102432051> (accessed 24 November 2020).
- Utechka na million [Leak for a Million]. *Kommersant*, 2019, June 10, no. 99 (June 10), p. 8. URL: <https://www.kommersant.ru/daily/2019-06-10> (accessed 25 November 2020).
- Utechki informacii ogranichenogo dostupa: otchet za 9 mesjacev 2020 [Restricted Information Leaks: Report for 9 Month of 2020]. *Analiticheskij otchet InfoWatch* [InfoWatch Analytical Report]. URL: <https://www.infowatch.ru/analytics/reports/30708> (accessed 26 November 2020).
- Chetvertaja promyshlennaja revoljucija. Populjarno o glavnom tehnologicheskom trende XXI veka [The Fourth Industrial Revolution. The Main Technological Trend of the 21<sup>st</sup> Century for a Non-Specialist Reader]. *TAdviser*. URL: <https://www.tadviser.ru/a/371579> (accessed 23 November 2020).
- Abdrahmanova G.I. et al. Chto takoe cifrovaja jekonomika? Trendy, kompetencii, izmerenie [What is the Digital Economy? Trends, Competencies, Measurement]. *XX Apr. Mezhdunar. nauch. konf. po problemam razvitija jekonomiki i obshhestva, Moskva, 9–12 apr. 2019 g.* [The 20<sup>th</sup> April International Scientific Conference on the Development of Economy and Society. Moscow, April 9–12, 2019]. Moscow, Izdatel'skiy dom Vysshey shkoly ekonomiki, 2019, pp. 14–15.
- Big Data: What It is and Why It Matters. *Analiticheskaya kompaniya SAS* [SAS Analytical Agency]. URL: [https://www.sas.com/ru\\_ru/insights/big-data/what-is-big-data.html](https://www.sas.com/ru_ru/insights/big-data/what-is-big-data.html) (accessed 25 November 2020).
- Boyd D., Crawford K. Critical Questions for Big Data. *Information, Communication & Society*, 2012, vol. 15, no. 5, pp. 37–41. DOI: 10.1080/1369118X.2012.678878.
- Cost of a Data Breach Report 2020. *IBM & Ponemon Institute*. URL: <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/> (accessed 1 December 2020).
- Cox M., Ellsworth D. *Application Controlled Demand Paging for Out of Core Visualization. Report NAS-97-010*, 1997. URL: <https://www.nas.nasa.gov/assets/pdf/techreports/1997/nas-97-010.pdf> (accessed 26 November 2020).
- Custers B., Uršič H. Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection. *International Data Privacy Law*, 2016, vol. 6, no. 1, pp. 4–15. DOI: 10.1093/idpl/ipv028.
- Kitchin R. Big Data, New Epistemologies and Paradigm Shifts. *Big Data & Society*, 2014, vol. 1, no. 1, pp. 1–12. DOI: 10.1177/2053951714528481.
- Lynch C. Big Data: How Do Your Data Grow? *Nature*, 2008, no. 7209, pp. 28–29. DOI: 10.1038/455028a.
- Press G. A Very Short History of Big Data. *Forbes.com*, 2013. URL: <https://www.forbes.com/sites/gilpress/2013/05/09/a-very-shorthistory-of-big-data/#92208b965a18> (accessed 26 November 2020).

### **Information About the Author**

**Vasily A. Yakhtin**, Postgraduate Student, Department of Economic Theory, World and Regional Economics, Volgograd State University, Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation, ea-191\_442755@volsu.ru, <https://orcid.org/0000-0001-6211-0844>

### **Информация об авторе**

**Василий Александрович Яхтин**, аспирант кафедры экономической теории, мировой и региональной экономики, Волгоградский государственный университет, просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация, ea-191\_442755@volsu.ru, <https://orcid.org/0000-0001-6211-0844>