УДК 332.01:332.05

Э. А. Туганова
Казанский инновационный университет им. В.Г. Тимирясова, Казань,
e-mail: elina_airatovna@mail.ru

К. А. Мызрова
АНО «Центр стратегических исследований Ульяновской области», Ульяновск,
e-mail: kamyzr@mail.ru

Ю. Н. Захарова
Краснознамённое училище имени генерала армии С.М. Штеменко, Краснодар,
e-mail: zaharova81j@mail.ru

О. В. Качагина
ФГБОУ «Ульяновский государственный университет», Ульяновск,
e-mail: okatschagina@mail.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ДРАЙВЕР РАЗВИТИЯ ЭКОНОМИЧЕСКИХ ПРОЦЕССОВ РЕГИОНА В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Ключевые слова: информационная безопасность, цифровая экономика, цифровизация, IT рынок, технологии, данные, информация, организация, компания, фирма, экономический процесс, социально-экономическое развитие.

Цифровую трансформацию экономики невозможно представить без развития IT рынка и применения в бизнес-процессах и информационно-коммуникационной техники и технологий. Развитие цифровой экономики предполагает, что чем выше уровень информационной безопасности компании или организации, тем больше у неё возможностей применения прогрессивных информационно-коммуникационных технологий в экономических процессах. Именно этот нематериальный актив, который невозможно купить за деньги, представляет собой неизмеримо высокую цену, состоящую из таких существенных активов, как имидж, деловая репутация организации/компании, финансовая устойчивость, если речь идёт о компании. Эффективность работы по информационной безопасности определяется её действенностью на местах, в каждом субъекте Российской Федерации. В статье авторами приводится перечень нормативных актов, регулирующих информационную безопасность, а также аналогичные документы регионального уровня. Нестабильная ситуация, сложившаяся в период специальной военной операции, вынуждает искать новые пути для повышения информационной безопасности в целях минимизации рисков в будущем. Авторы описывают действенные инструменты информационной безопасности на примере республики Татарстан. Авторами рассматривается опыт Республики Татарстан как одного из лидеров цифровой трансформации, так по рейтингу «Сколково» находящегося в пятёрке лучших регионов по цифровой трансформации государственного управления. Развитие центров обработки данных (ЦОД) в регионе поможет смягчить последствия кризиса и открыть новые возможности. Таким образом, региональные ЦОДы являются одним из действенных инструментов информационной безопасности.

E. A. Tuganova
Kazan Innovative University named after V.G. Timiryasov, Kazan,
e-mail: elina_airatovna@mail.ru

X. A. Myzrova
ANO «Center for Strategic Studies Ulyanovsk region», Ulyanovsk, e-mail: kamyzr@mail.ru

Yu. N. Zakharova
Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after Army General S.M.Shtemenko, Krasnodar, e-mail: zaharova81j@mail.ru

O. V. Kachagina
Ulyanovsk State University, Ulyanovsk, e-mail: okatschagina@mail.ru

INFORMATION SECURITY AS A DRIVER FOR THE DEVELOPMENT OF ECONOMIC PROCESSES IN THE REGION IN THE DIGITAL ECONOMY

Keywords: information security, digital economy, digitalization, IT market, technologies, data, information, organization, company, firm, economic process, socio-economic development.

It is impossible to imagine the digital transformation of the economy without the development of the IT market and the use of information and communication technology and technologies in business processes. The development of the digital economy assumes that the higher the level of information security of a company or organization, the more opportunities it has to use advanced information and communication technologies in economic processes. It is this intangible asset, which cannot be bought for money, that represents an immeasurably high price, consisting of such essential assets as the image, business reputation of the organization/company, financial stability, if we are talking about the company. The effectiveness of information security work is determined by its effectiveness on the ground, in each subject of the Russian Federation. In the article, the authors provide a list of normative acts regulating information security, as well as similar documents at the regional level. The unstable situation that has developed during the special military operation forces us to look for new ways to improve information security in order to minimize risks in the future. The authors describe effective information security tools using the example of the Republic of Tatarstan. The authors consider the experience of the Republic of Tatarstan as one of the leaders of digital transformation, and according to the rating of Skolkovo, which is in the top five regions for digital transformation of public administration. The development of data processing centers (data centers) in the region will help mitigate the effects of the crisis and open up new opportunities. Thus, regional data centers are one of the effective tools of information security.

Введение

Актуальность темы исследования заключается в том, что на сегодняшний мир, страну, регионы уже невозможно представить без цифровой трансформации экономики, без развития IT рынка и применения в бизнес-процессах и информационно-коммуникационной техники и технологий. В такую картину дня органично вписывается требование оперативных мер по обеспечению информационной безопасности (ИБ) сведений и данных, касающихся государственных структур и бизнес структур, экономики в целом.

Научным обществом ещё не сформировано однозначное определение понятия «цифровая экономика», «информационная безопасность», «цифровая трансформация экономики» не смотря на высокую актуальность и практическую значимость. Причина этому – сверхбыстрое развитие цифровой практики, информация быстро устаревает.

В соответствии с Указом Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в РФ на 2017-2030 гг.» [1]: «цифровая экономика – это хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объёмов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг».

В рамках реализации Указов Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [2] и от 21.07.2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года» [3], в том числе с целью решения задачи по обеспечению ускоренного внедрения цифровых технологий в экономике и социальной сфере, Правительством Российской Федерации сформирована национальная программа «Цифровая экономика Российской Федерации» утвержденная протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7 [4].

Вопросами, касающимися информационной безопасности, занимаются многие исследователи. Вопросы влияния цифровизации на экономику России рассматривается в работах отечественных учёных, например, А.М. Баранова [5], Д.Е. Бекбергеневой [6], Н.В. Днепровской [7], А.А. Мироедова [8], Д.А. Нагорного [9], А.В. Пролубникова [10] и др.

Большинство понятий, связанных с информационной безопасностью определяются Указом Президента Российской Федерации от 30.03.2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [11], Указ Президента РФ от 01.05.2022. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [12], а также Федеральным законом № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры (КИИ) РФ» [13] и Федеральным законом

от 29.12.2022 г. № 584-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» [14].

Несмотря на то, что данная тема является дискуссионной в научных публикациях российских исследователей, а также в средствах массовой информации, остаются вопросы, которые недостаточно изучены и проанализированы в данной сфере. Поэтому будет целесообразным осветить более подробно современное состояние информационной безопасности в стране и на примере Республики Татарстан.

Несмотря на то, что данная тема является дискуссионной в научных публикациях российских исследователей, а также в средствах массовой информации, остаются вопросы, которые недостаточно изучены и проанализированы в данной сфере. Поэтому будет целесообразным осветить более подробно современное состояние информационной безопасности в стране и на примере Республики Татарстан.

Нестабильная ситуация, сложившаяся в период специальной военной операции, вынуждает искать новые пути для повышения информационной безопасности в целях минимизации рисков в будущем. Авторы описывают действенные инструменты информационной безопасности на примере республики Татарстан.

Материалы и методы исследования

Методологической основой исследования послужили Указы Президента РФ, федеральные законы Российской Федерации, а также аналогичные акты регионального уровня, труды российских экономистов по исследуемой теме. Авторами применён анализ документов, обобщения, а также использовались сравнительный анализ, системный и ситуационный подходы. Инструментарий авторов включает способы научного познания (индукция, дедукция, обобщения).

Цель исследования заключаются в описании некоторых особенностей развития цифровой экономики, информационной безопасности компаний в современный период. Задачи: выявить современные инструменты информационной безопасности в республике Татарстан.

Теоретическая значимость работы заключается в описании некоторых трендов в области цифровой экономики и информационной безопасности. Практическая значимость исследования определяется в выявлении проблем по информационной безопасности организаций на уровне региона, описанием опыта Республики Татарстан для развития действенных инструментов в информационной безопасности.

Результаты исследования и их обсуждение

Главным ресурсом, обеспечивающим конкурентное преимущество организаций, становится информация и осуществляемая на её основе инновационная деятельность. В сложившихся условиях у организаций всё более возрастает необходимость реагировать на изменения. Параметры, характеризующие возможности комплексов технических средств информационных систем, в последние годы возросли и продолжают расти. Проектирование сложных технических комплексов и систем управления различными объектами всё более переходит в виртуальную среду, где проектные решения базируются на математических моделях, а не принимаются на основе натуральных испытаний [15, с.13-14].

Инновации представляют собой базовый вектор развития новой экономики, являются основой деятельности высокотехнологичных и наукоёмких отраслей, а также высшего профессионального образования, уровень которого, наряду с инновационной составляющей является показателем конкурентоспособности на мировом рынке [15, с.17].

Цифровизация как этап развития информационного общества [16] не означает автоматическое развитие цифровой экономики, а создаёт новые возможности для хозяйствующих субъектов.

Согласно Доктрине информационной безопасности Российской Федерации [17]: «информационная безопасность РФ – состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства».

Злободневность решения данной задачи в Российской Федерации подтверждает

анализ кибератак на интернет-индустрию в 2022 году. Со ссылкой на «Лабораторию Касперского» здесь приводится цифра, превышающая 1,5 млрд. записей [18]. При этом средний ущерб для организаций вырос с 2,6 млн.руб. ещё в третьем квартале 2022 года до 5 млн.руб. в четвертом.

Львиная доля интернет-покушений в стране приходится не на коммерческие тайны (18 %), завладев которыми можно обогатиться. Процент атак на учётные данные составил 17 %, всякого рода другая информация – 12 %. Под прицелом была медицинская информация – 7%, данные платёжных карт и переписка – по 5 % в обоих случаях. Очевидно внимание киберпреступников к персональным данным – 36 %. [19].

Такого рода информнападения опровергают привычное представление о том, что киберпреступники охотятся за финансовой наживой. Под ударом оказалась деловая репутация организации или компании/фирмы. Именно этот нематериальный актив, который невозможно купить за деньги, представляет собой неизмеримо высокую цену, состоящую из таких существенных активов, как имидж, деловая репутация организации/компании, финансовая устойчивость, если речь идет о компании. Соответственно, утечка данных из таких структур влечёт за собой недоверие населения, потребителей, отток последних и/или потеря клиентов.

Таким образом, жертвами интернет-нападений являются госструктуры, учреждения медицины, бизнес-структуры. Следовательно, возрастание количества кибервзломов – это и экономическая, и гражданская информационная безопасность.

С учётом остроты вопроса, в Российской Федерации внесены существенные изменения в законодательные основы по информационной безопасности. Так, Указ Президента РФ «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [20] направлен на активизацию деятельности в сфере информбезопасности как государственных структур, так и бизнеса.

Обеспечение информационной безопасности – осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления [21].

Указ Президента РФ ответственность за обеспечение ИБ возложил на госорганы исполнительной власти государства и регионов, фонды и корпорации с государственным участием, имеющие стратегическое значение акционерные общества, предприятия и корпорации – системообразующие субъекты в экономике страны, юридические лица критической информационной инфраструктуры (КИИ – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры) [22].

К КИИ на основе закона относятся государственные органы, государственные учреждения, российские и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса в области атомной энергетики, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей [22].

Вышеназванный Указ Президента РФ, по своей сути – это стратегия, нацеленная на минимизирование, то есть – максимальное использование в интересах страны широких возможностей с целью заметного сокращения ущерба от кибернападок, а по большому счёту – эффективного отражения информационных атак. Реализация заявленной повестки возможна лишь при объединении компетенций ярких представителей рынка, интересантов органов государственной власти и ключевых акторов индустрий. Наряду с названным документом, увидели свет множество нормативных актов, законопроектов, призванных обуздать волну информатак.

В этой связи Указ Президента РФ «О мерах по обеспечению технологической не-

зависимости и безопасности критической информационной инфраструктуры Российской Федерации» [23] адресован объектам критической информационной инфраструктуры (КИИ). Таковым указывается на необходимость перехода преимущественно отечественную радиоэлектронную продукцию и телекоммуникационное оборудование. Наконец, с 01 марта 2023 г. вступил в силу Федеральный закон «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» [24]. Согласно принятым поправкам, иностранными мессенджерами запрещено пользоваться в финансово-хозяйственной деятельности госкомпаниям, государственным и муниципальным унитарным предприятиям, публично-правовым компаниям, хозяйственным обществам, доля государства которых превышает 50%, кредитным организациям, ряду не кредитных финансовых организаций. Под свой бдительный контроль Роскомнадзор берёт деятельность крупных классифайдов. Нарушение ими законодательных требований подпадает вплоть до уголовной ответственности [25].

Эффективность работы по информационной безопасности определяется её действенностью на местах, в каждом субъекте РФ. Рассмотрим это на примере Татарстана в условиях цифровой экономики.

В 2022 году, а он в республике был объявлен Годом цифровизации, выручка IT отрасли увеличилась почти на 30%, и в сравнении с 2021 г. рост составил от 116 до 150 млрд руб. В условиях ограничения ввоза и возрастающей потребности в отрасли выросли продажи отечественного оборудования и программного обеспечения внутри страны. По Татарстану – это 150 млрд. руб. валовой выручки [26]. Бюджет реализации Государственной программы цифровой трансформации РТ [27] в 2022 и 2023 годах предусматривает по 4,6 млрд руб., в 2024 и 2025 годах – по 3,8 млрд руб. Общий объём финансирования программы рассчитан на сумму 16,8 млрд руб. С учётом современных экономических вызовов, эти цифры были скорректированы: по первоначальному варианту на 2022 год планировалось выделить более 1 млрд руб., в 2023 году – 974,8 млн руб., а в 2024 г. – 675,8 млн руб. [28]

В Татарстане, как в субъекте Российской Федерации, проводится единая политика по защите данных, снижению уровня уязвимости систем, внедрению новых методов и технологий работы [29] В рамках Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации определилось деловое взаимодействие с Национальным координационным центром по компьютерным инцидентам.

В республике реализуется региональный проект «Информационная безопасность», начало которому было положено Указом Президента РФ «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [30] в части решения задач по направлению «Информационная безопасность», затем доработан в соответствии с изменениями и дополнениями в Указе Президента РФ «О национальных целях развития Российской Федерации на период до 2030 года» [31]. В числе мер по информационной безопасности внедрены сертификационные средства защиты информационных систем, аттестованы государственные системы управления.

В 2022 г. созданным Центром предотвращения киберугроз Республики Татарстан выявлено и отражено 380 тыс. DDoS атак (DDoS атака (от англ. Distrbuted Denial of Service – распределенная атака, которая создаёт нагрузку на сервере и приводит к отказу системы) (в десять раз больше по сравнению с 2021 г.) [32]. При этом мощность DDoS атак в 2022 году составила 3,5 Гбит/с. Центр обеспечивает полную информационную защиту Центра обработки данных (ЦОД) правительства республики. Заблокировано более 15 тыс. атакующих IP адресов; отфильтровано нелегитимных запросов к информационным системам – 12 млрд; просканировано на наличие уязвимости – 2400 серверов [33].

На день подготовки данной научной статьи в Республике Татарстан действует постановление Кабинета Министров Республики Татарстан с задачами по цифровизации на 2023 год [33]. В числе целевых показателей по цифровизации на текущий 2023 г. и плановый период до 2026 г. сказано о необходимости Министерству цифрового развития государственного управления, информационных технологий и связи Республики Татарстан разработать перечень мер по обеспечению информационной безопас-

ности для объектов критической информационной инфраструктуры. При этом, такого рода мероприятия должны быть рассчитаны на широкий спектр отраслей экономики республики.

В частности, 27 марта 2023 г. в Татарстане создан межвузовский центр противодействия киберугрозам (MSSP SOC), функционирующий на базе Консорциума опорных вузов: Казанского Национального исследовательского технического университета имени А.Н. Туполева, Казанского федерального университета, Казанского государственного энергетического университета и Университета Иннополис. Научно-технический, интеллектуальный потенциал названных учебных заведений не позволяет сомневаться в том, что в надёжных руках решение главной задачи – повышение уровня информационной безопасности российских вузов федерального и регионального значения.

Заключение

Таким образом, развитие цифровой экономики предполагает, что чем выше уровень информационной безопасности компании или организации, тем больше у неё возможностей применения прогрессивных информационно-коммуникационных технологий в экономических процессах. Зачастую бизнес сектор более заинтересован в оснащении современной техникой и технологиями, нежели в затратах, связанных с информационной безопасностью.

В связи с этим, заметим, что жёсткость наказания нормативных актов рассчитана скорее не на устрашение бизнеса, а на придание ему импульса для принятия им конкретных решений в деле усиления защиты своих же IT-активов от информационных атак. Тем более, по мнению IT-экспертов, внимание государства к ИБ значительно возрастает. Например, под действие майского Указа Президента РФ подпадает более широкий круг организаций, чем по предыдущим, например, 187 – ФЗ о КИИ, а в обеспечение ИБ теперь вовлекаются первые лица компаний. Один из главных трендов – активный переход российских компаний на отечественные операционные системы. В этой связи прогнозируется рост числа кросс-платформенных хакерских инструментов. Результаты исследований аналитиков показывают возрастание количества атак без применения злоумышленниками новых методов и увеличение числа успешных взломов в 2023 г. по причинам: роста числа уязвимостей и их неустранение, нехватка кадров более чем у 90% компаний, уход иностранных вендоров ИБ [34].

Следует ожидать атаки, появившихся в 2022 г. ранее неизвестных APT-группировок, которые стремились нанести репутационный ущерб государственным структурам и бизнесу. Эксперты подчёркивают важность смены парадигмы обеспечения ИБ в пользу обеспечения цифровой устойчивости организации, предприятия. ИБ необходимо обеспечивать точечно, сфокусировавшись на самых ценных активах компании, негативное воздействие на которые может привести к наступлению недопустимых для бизнеса событий [34], а под ними следует понимать остановку бизнес-процессов.

Библиографический список

1. Указ Президента РФ от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в РФ на 2017-2030 гг. Президент России. [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 20.04.2023).

2. Указ Президента Российской Федерации от 07.05.2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года». Президент России. [Электронный ресурс]. URL:http://www.kremlin.ru/acts/bank/4302 (дата обращения: 03.02.2023).

3. Указ Президента Российской Федерации от 21.07.2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года». Президент России. [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/45726 (дата обращения: 20.04.2023).

4. «Цифровая экономика РФ». Министерство цифрового развития, связи и массовых коммуникаций. [Электронный ресурс]. URL: https://digital.gov.ru/ru/activity/directions/858/?utm_referrer=https%3a%2f%2fyandex.ru%2f] (дата обращения: 20.04.2023).

5. Баранов А.М. Информационная экономика как основа экономической системы: теоретико-методологический аспект: дис… докт. экон. наук. Москва, 2010. 200 с.

6. Бекбергенева Д.Е. Управление цифровизацией социально-экономического развития региона: автореф. дис. … докт. экон. наук. Ростов-на-Дону, 2022. 55 с.

7. Днепровская Н.В. Формирование инновационной среды цифровой экономики: дис… докт. экон. наук. Москва, 2020. 352 с.

8. Мироедов А.А. Совершенствование управления региональной экономикой на базе новой концепции его информационного обеспечения: автореф. дис. … докт. экон. наук. Иваново, 2007. 39 с.

9. Нагорный Д.А. Цифровая трансформация мировой экономики: тенденции и перспективы: автореф. дис. … докт. экон. наук. Москва, 2021. 29 с.

10. Пролубников А.В. Трансформация государственной экономической политики в условиях модернизации и цифровой национальной экономики: автореф. дис. … докт. экон. наук. Санкт-Петербург, 2022. 42 с.

11. Указ Президента Российской Федерации от 30.03.2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». Президент России. [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/47688 (дата обращения: 06.03.2023).

12. Указ Президента РФ от 01.05.2022. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Официальный интернет-портал правовой информации. [Электронный ресурс]. URL: http://pravo.gov.ru/links/kremlin/ (дата обращения: 27.02.2023).

13. Федеральный закон № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры (КИИ) РФ» [Электронный ресурс]. URL: http://www.consultant. ru. (дата обращения: 27.03.2023).

14. Федеральный закон от 29.12.2022 г. № 584-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации». Президент России. URL: http://www.kremlin.ru/acts/bank/48823 (дата обращения: 28.03.2023).

15. Иванова Т.Ю., Мызрова К.А. Развитие инструментов менеджмента на основе формирования образовательных сетей в условиях экономики знаний: монография. Ульяновск: УлГУ, 2016. 226 с.

16. Стратегия развития информационного общества в РФ на 2017–2030 годы. Президент России. [Электронный ресурс]. URL: http://kremlin.ru/acts/bank/41919 (дата обращения: 01.04.2023).

17. Доктрина информационной безопасности Российской Федерации. Дата подписания: 05.12.2016 Опубликован: 06.12.2016. Утверждена Указом Президента Российской Федерации от 05. 12.2016 г. № 646. Президент России. [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 29.03.2023).

18. Андрей Крупин. Итоги 2022 года: интернет-индустрия 04.01.2023. Программное обеспечение [Электронный ресурс]. URL: https://3dnews.ru/1079351/itogi-2022-goda-internet (дата обращения: 03.05.2023).

19. Актуальные киберугрозы / Positive technologies [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q2/ (дата обращения: 15.04. 2023).

20. Указ Президента РФ от 01.05.2022. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru/links/kremlin/ (дата обращения: 27.02.2023).

21. Доктрина информационной безопасности Российской Федерации. Дата подписания: 05.12.2016 Опубликован: 06.12.2016. Утверждена Указом Президента Российской Федерации от 05. 12.2016 г. № 646. Официальный сайт Президента России [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 29.03.2023).

22. Федеральный закон № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры (КИИ) РФ». [Электронный ресурс]. URL: http://wwwconsultant. ru. (дата обращения: 27.03.2023).

23. Указ Президента Российской Федерации от 30.03.2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». Президент России. Официальный сайт. [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/47688 (дата обращения: 06.03.2023).

24. Федеральный закон от 29.12.2022 г. № 584-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации». Президент России. [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/48823 (дата обращения: 28.03.2023).

25. Президент подписал закон о регулировании работы классифайдов. Интерфакс. [Электронный ресурс]. URL: https://www.interfax.ru/russia/879186 (дата обращения: 20.04.2023).

26. В 2022 году выручка ИТ-отрасли Татарстана выросла почти на 30%. 25.01.2023. Реальное время [Электронный ресурс]. URL: https://realnoevremya.ru/news/271677-v-2022-godu-vyruchka-it-otrasli-tatarstana-vyrosla-pochti-na-30\ (дата обращения: 01.02. 2023).

27. Постановление Кабинета Министров Республики Татарстан от 18.10. 2021. № 980 «Об утверждении государственной программы Республики Татарстан «Цифровой Татарстан» (с изменениями на 30 декабря 2022 года) (в ред. Постановлений КМ РТ от 22.07.2022 N 711, от 30.12.2022 N 1500) [Электронный ресурс]. URL: https://docs.cntd.ru/document/577916303 (дата обращения: 10.03.2023).

28. Максим Кокунин. ИИ в «Народном контроле», радиологический дата-центр: задачи цифровизации Татарстана в 2023 году. Реальное время [Электронный ресурс]. URL: https://m.realnoevremya.ru/articles/275041-kabmin-utverdil-zadachi-cifrovizacii-tatarstana-v-2023-godu (дата обращения: 10.03.2023).

29. Из доклада министра министерства цифрового развития государственного управления, информационных технологий и связи Республики Татарстан «Об итогах года цифровизации в Республике Татарстан в 2022 году и задачах по цифровизации на 2023 год». Ежегодная коллегия 26.01.2023. Официальный Татарстан [Электронный ресурс]. URL: https://digital.tatarstan.ru/buklet.htm (дата обращения: 27.02.2023).

30. Указ Президента Российской Федерации от 07.05.2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года». Президент России. [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/4302 (дата обращения: 03.02.2023).

31. Указ Президента РФ от 21 июля 2020 г. N 474 «О национальных целях развития Российской Федерации на период до 2030 года». Президент России. [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/45726 (дата обращения: 28.03.2023).

32. Из доклада министра министерства цифрового развития государственного управления, информационных технологий и связи Республики Татарстан «Об итогах года цифровизации в Республике Татарстан в 2022 году и задачах по цифровизации на 2023 год». Ежегодная коллегия 26.01.2023. [Электронный ресурс]. URL: https://digital.tatarstan.ru/buklet.htm (дата обращения: 27.02.2023).

33. Постановление Кабинета Министров РТ «Об итогах Года цифровизации в Республике Татарстан и задачах по цифровизации на 2023 год». Официальный портал правовой информации Республики Татарстан [Электронный ресурс]. URL: https://pravo.tatarstan.ru/npa_kabmin/post?npa_id=1167541 (дата обращения: 29.03.2023).

34. Кибербезопасность 2022-2023. Тренды и прогнозы. 13.01.2023. Positive Technologies, 2002–2023 / Positive technologies [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib (дата обращения: 30.03.2023).