УДК 338.2 **DOI: 10.18413/2409-1634-2024-10-3-0-8**

Маслова И.А.

ЦИФРОВАЯ БЕЗОПАСНОСТЬ В СОВРЕМЕННОМ МИРЕ

Орловский государственный университет имени И. С. Тургенева,
Россия, 302026, г. Орел, ул. Комсомольская, 95

e-mail: tera_27@mail.ru

Аннотация
На протяжении нескольких десятилетий двигателем современного общества является технологический прогресс. Его инновации, новые и постоянно совершенствующиеся средства и принципы являются основными составляющими нашего сегодняшнего сосуществования. Информационные технологии формируют и развивают коммуникацию между субъектами рынка, экономические отношения, рабочую среду, социальное взаимодействие в больших и малых масштабах. Именно поэтому замена предшествующей технологии на принципиально новые способы и методы, всегда сопровождается изменениями в мире. Если информационный, высокопроизводительный и высокосетевой мир, еще несколько лет назад был отдаленным видением будущего, то активное использование передовых технологий и постепенный переход на новый формат деятельности сделали его реально настоящим. Главным сырьем для цифровой трансформации являются данные, которые признаются решающим фактор успеха современного бизнеса. Ключевые компетенции успешных компаний будут в долгосрочной перспективе заключаться в сборе, обработке, соединении и, главное, защите этих данных. Объясняется это тем, что сведения, формируемые в информационно-коммуникационной системе предприятия, позволяют определить эффективность работы структурных подразделений для совершенствования бизнес-процессов, сигнализируют о тенденциях их развития, тем самым помогают менеджерам принимать обоснованные управленческие решения. Указанная информация представляет интерес не только для самой компании, но и для конкурентов и киберпреступников, поэтому требует полноценной защиты. В статье раскрыты результаты теоретического исследования вопросов защиты цифровых сведений, устройств и ресурсов в современном мире, сделан вывод о дальнейшем совершенствовании законодательства РФ о цифровой безопасности.

Ключевые слова: данные, цифровые технологии, цифровизация, защита, безопасность, цифровая безопасность
Информация для цитирования: Маслова И.А. Цифровая безопасность в современном мире // Научный результат. Экономические исследования. 2024. Т. 10. № 3. С. 85-93. DOI: 10.18413/2409-1634-2024-10-3-0-8

Irina A. Maslova | **DIGITAL SECURITY IN TODAY'S WORLD**

I.S. Turgenev Oryol State University,
95 Komsomolskaya St., Oryol, 302026, Russia

e-mail: tera_27@mail.ru

Abstract
For several decades, the engine of modern society has been technological progress. Its innovations, new and constantly improving means and principles are the main components of our current coexistence. Information technologies shape and develop communication between market actors, economic relations, working environment, social interaction on large and small scales. That is why the replacement of previous technology with fundamentally new ways and methods, is always accompanied by changes in the world. If the informational, highly productive and highly networked world was a distant vision of the future just a few years ago, the active use of advanced technologies and gradual transition to a new format of activity have made it a real present. The main raw material for digital transformation is data, which is recognized as a decisive factor in the success of modern business. In the long term, the key competencies of successful companies will lie in collecting, processing, connecting and, most importantly, protecting this data. This is explained by the fact that the information formed in the information and communication system of the enterprise allows determining the efficiency of structural units to improve business processes, signaling trends in their development, thus helping managers to make informed management decisions. This information is of interest not only for the company itself, but also for competitors and cybercriminals, so it requires full protection. The article reveals the results of theoretical research into the protection of digital information, devices and resources in the modern world, and concludes on further improvement of the Russian legislation on digital security.

Key words: data; digital technologies; digitalization; digitalization; protection; security; digital safety

Information for citation: Maslova I.A. “Digital security in today's world”, *Research Result. Economic Research*, 10(3), 85-93, DOI: 10.18413/2409-1634-2024-10-3-0-8

Введение

В последние годы благодаря цифровым технологиям и методам стало возможным значительное повышение производительности и создание совершенно новых бизнес-моделей. Многие отрасли, включая музыкальный бизнес, банковский сектор, туристическую индустрию, здравоохранение и образование, хорошо продвинулись в этом направлении, тем не менее, столкнулись с рядом проблем при внедрении в свою деятельность информационных технологий. Несмотря на положительные моменты, цифровизация меняет правила игры и мир в целом. Она вызывает огромные потрясения в экономике и обществе, в сфере труда, потребления, сотрудничества и коммуникации. Цифровизация обостряет вопросы защиты данных, поскольку приводит к росту количества угроз информационной

безопасности. Сегодня у простых граждан страны снижается доверие к цифровой среде из-за опасений по поводу того, соблюдаются ли поставщиками услуг основные права, такие как защита персональных данных. Согласно проведённому опросу среди обучающихся Орловского государственного университета имени И.С. Тургенева, только 22 % опрошенных полностью доверяют интернет-компаниям, таким как поисковые системы, социальные сети и службы электронной почты. Поэтому правовые и технические вопросы, связанные с трансграничной обработкой и использованием данных, являются весьма актуальными и требуют решения на законодательном уровне. Должна быть разработана единая политика размещения информации, основанная на общих принципах, например, безопасности данных и их суверенитета, которых должны придерживаться все участники информационной сферы. Цель работы – исследовать вопросы защиты цифровых сведений, устройств и ресурсов в современном мире, выявить проблемы и предложить меры по их устранению.

Методы

Исследование базировалось на обзоре современных публикаций и интернет-ресурсов, посвященных цифровой безопасности. В работе была использована совокупность мыслительных приемов и способов, такие как, анализ, дедукция, индукция, сравнение, обобщение данных. В частности в статье проведен анализ организаций, пострадавших от атак программ-вымогателей, состав лидеров рынка кибербезопасности России и разработчиков ИТ- средств по защите информации на рынке по результатам 2022 года, а также нормативной базы, посвященной цифровой безопасности.

Результаты

Результаты теоретического исследования вопросов защиты цифровых сведений, устройств и ресурсов в современном мире позволили, сделан вывод о дальнейшем совершенствовании законодательства РФ о цифровой безопасности. Итоги исследования могут быть использованы при подготовке учебно-методических комплексов и проведении практических и семинарских занятий по дисциплине «Экономическая безопасность» и др.

Обсуждение

Цифровая трансформация общества требует изменения парадигмы в политике обработки данных. Поскольку информация – главное сырье цифровой экономики. Граждане, руководство компаний и собственники бизнеса должны быть уверены в том, что их данные защищены от неправомерного использования. Пользователи и потребители должны иметь возможность принимать самостоятельные решения о раскрытии своих данных. Безопасность информации, её суверенитет являются важными краеугольными камнями демократического общества. Поскольку, как считает А.Р. Назаретян «помимо психологического дискомфорта, который человек испытывает от осознания слежки и незащищенности своих действий в цифровой среде, формируется ощущение сомнительной подлинности своего выбора и действий, совершающихся в интернет-пространстве» [Назаретян, А.Р., 2020].

Информационные технологии сегодня рассматриваются как необходимое условие для успеха экономики, основанной на знаниях. Без надежной и безопасной инфраструктуры информационно-коммуникационных технологий (ИКТ) увеличивается риск потери конкурентоспособности и будущей

жизнеспособности России. Руководство отечественных компаний считает, что цифровизация бизнеса – это путь в будущее. Но вместе с тем, использование информационных технологий несет определенные угрозы для предпринимательской деятельности экономических субъектов. Как считают К.Е. Следнева, Т.Б. Кувалдина «проблема цифровых угроз превращается в глобальное явление, затрагивающее каждого – от обычных граждан до крупных компаний и государственных органов» [Следнева К.Е., 2024].

По данным Statista ситуация с угрозами ИТ-безопасности во многих областях оценивается как высокая во всех странах мира [Статиста 2024 …] (Рис. 1).

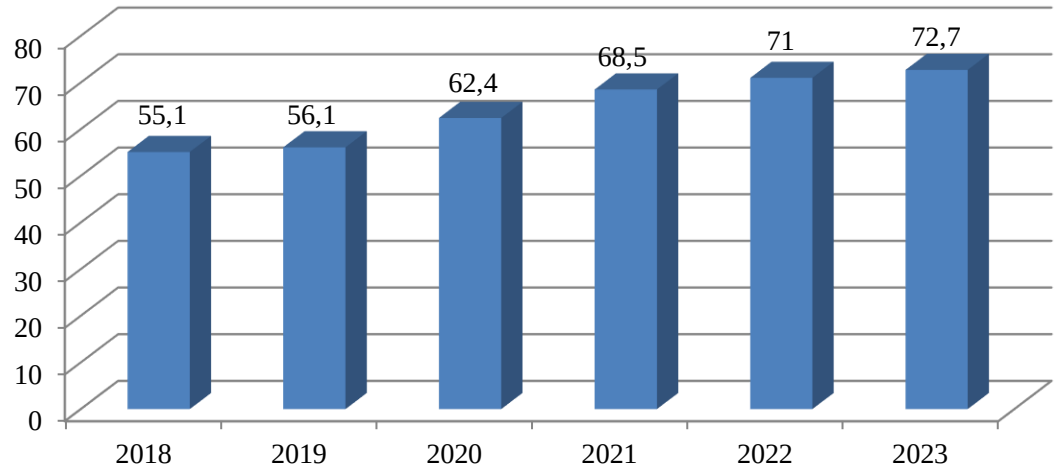

Рис. 1. Ежегодная доля организаций, пострадавших от атак программ-вымогателей во всем мире с 2018 по 2023 гг., в %
Fig. 1. Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023, in %

В сфере кибербезопасности в России осуществляют деятельность свыше 30 компаний. Лидерами среди них по итогам 2022 года являются отечественные компании Лаборатория Касперского, Positive Technologies, BI.ZONE [Статиста 2024 …] (рис. 2). С началом российско-украинского конфликта в 2022 году, часть иностранных организаций, обеспечивающих защиту в сфере информационных технологий, покинуло российский рынок.

К лидерам рынка средств защиты данных относятся две российские компании – Лаборатория Касперского (16,0%) и Positive Technologies (12,4%) [Статиста 2024 …] (Рис. 3).

1. Лаборатория Касперского
2. Positive Technologies
3. BI.ZONE
4. Check Point Software Technologies
5. Ростелеком-Солар
6. ИнфоТеКС
7. Cisco
8. Fortinet
9. Код Безопасности
10. Крипто-Про

Рис. 2. Лидеры рынка кибербезопасности России по итогам 2022 года
Fig. 2. Leaders of the Russian cybersecurity market by the end of 2022

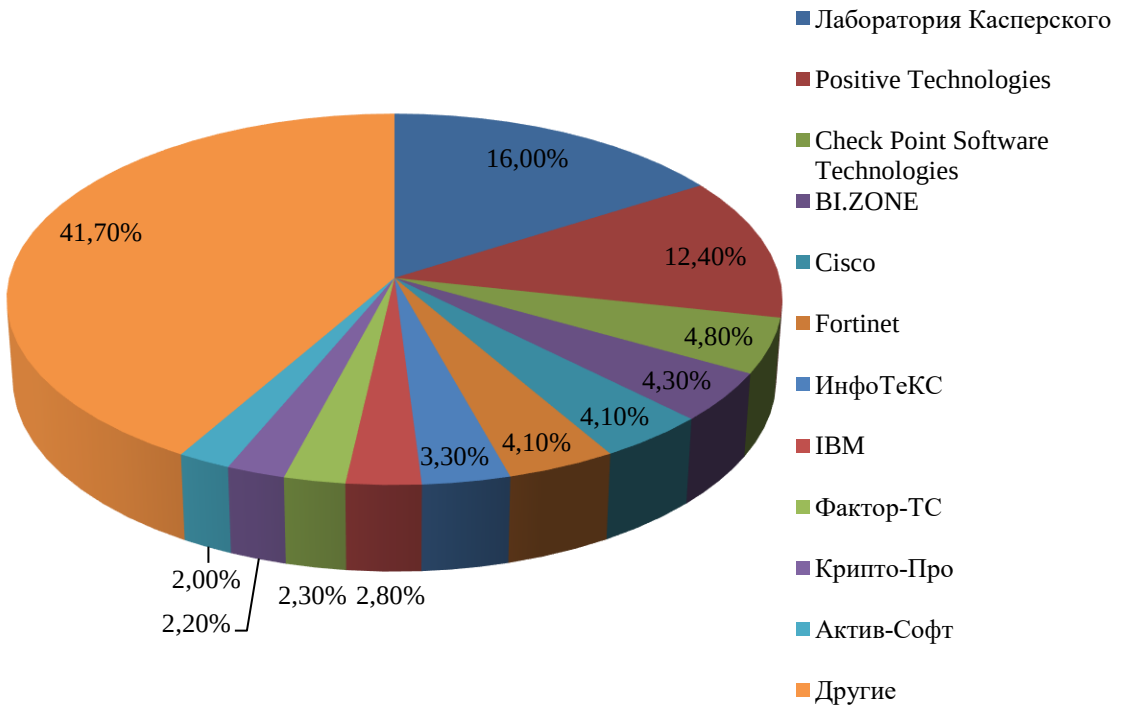

Рис. 3. Доли разработчиков ИТ-продуктов, средств по защите информации на рынке по результатам 2022 года
Fig. 3. Shares of IT product developers, information security tools on the market based on the results of 2022

По мнению Т.К. Примак, О.А. Серовой сегодня возникает необходимость в активизации участия государства в обеспечении кибербезопасности, в том числе в процессах определения понятия и видов киберпреступлений, выработки мер борьбы с этим явлением, подготовки специалистов соответствующей квалификации [Примак Т.К., 2019].

Если крупный бизнес заботиться о своей информационной безопасности, то руководители малых и средних предприятий не совсем ещё осознали необходимость защиты используемых информационно-коммуникационных систем. Только после кибератаки, выхода устройств из строя и парализации всех бизнес-процессов, к ним приходит осознание того, что нужно осуществлять инвестиции в кибербезопасность. Например, омский предприниматель В. Шкуренко в июне 2024 года высказался о необходимости усиления мер безопасности, только когда киберпреступники взломали базу данных ТД «Шкуренко», вследствие чего возникли глобальные проблемы с логистикой товаров [РИА Омск-информ …].

Безопасность и защита данных в России должны укрепляться устойчиво и эффективно. В частности, малые и средние предприятия должны распознавать опасности и защищаться от них, чтобы в полной мере использовать возможности, связанные с цифровизацией. Их необходимо поддержать в принятии соответствующих защитных мер, значительно повышающих уровень безопасности данных, вплоть до выделения им субсидий из бюджета или специальных фондов.

Россия стремится занять лидирующую позицию во многих цифровых инновациях в области прогрессивных технологий. Однако соперничество и противостояние сильны, особенно со стороны США, Германии и стран Юго-Восточной Азии (Япония, Южная Корея, Китай), которые не заинтересованы в развитии промышленного сектора в нашей стране, поскольку цифровизация промышленности открывает дополнительный потенциал создания совокупной стоимости. Перевод на цифру производственного процесса повышает его эффективность, производительность труда и сокращает издержки производства. Несмотря на введение экономических санкций, отечественные промышленные предприятия развиваются, разрастаются, погружаются в новые технологии, становясь всё более привлекательной мишенью для хакеров. По данным «РТК-Солар» за последние три года отечественные промышленные предприятия столкнулись почти с 600 тыс. кибератак. Их пик пришелся на 4 квартал 2022 года, а после небольшого спада угрозы опять усилились. Преступники сосредоточились на обзоре ИТ-периметров экономических субъектов (простукивание сканерами, изыскание новых плохо защищенных сервисов и серверов, применение компьютерного шпионажа) [РТК-Солар …] (Рис. 4).

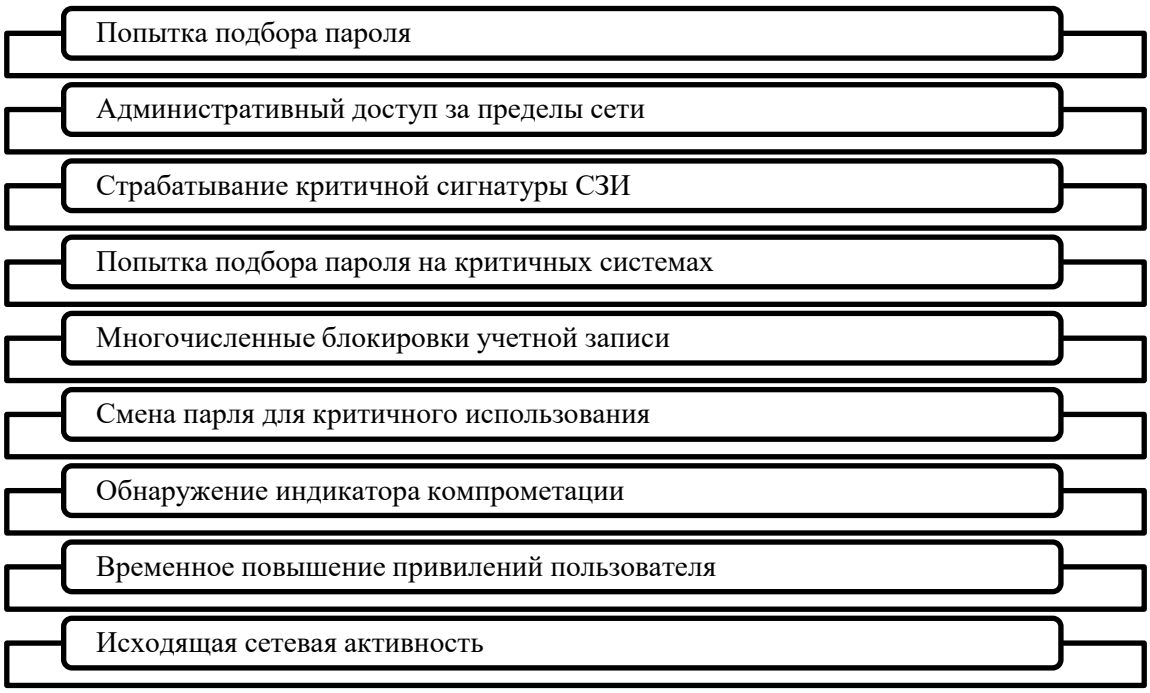

Рис. 4. Самые значительные инциденты в промышленности 2021-2024
Fig. 4. The most significant incidents in industry 2021-2024

Большую долю инцидентов в промышленности составляют операции с пользовательскими учетными записями и контролем над ними, а именно подбор пароля (в том числе от критичных систем), административный доступ за пределы сети, многочисленные блокировки учетных записей [РТК-Солар …].

Одним из важнейших вопросов в сфере цифровой безопасности является также передача данных в другие страны. Баланс между интересами потребителей, компаний и безопасностью часто понимается и организуется в других регионах мира по-иному, чем в нашей стране. Поэтому важно заручиться международными соглашениями и конвенциями по этим вопросам. Только благодаря единым международным нормам можно будет минимизировать риск, связанный с промышленным шпионажем и кибератаками. В подтверждение можно привести высказывание, Т.К. Примак, О.А. Серова, которые считают, что «с учетом сложности, опасности, глобального характера киберпреступлений целесообразно укреплять международное сотрудничество, внедрять нормативные акты национального и международного характера, согласовывать национальные и международные акты, присоединяться к наиболее важным конвенциям, регулирующим эту сферу, обмениваться специальными знаниями в области информационных технологий, программного обеспечения и т.д.» [Примак Т.К, 2019]. Такого же мнения придерживается Н.А. Крайнова, заключая, что «проблема цифровой безопасности не является сугубо внутригосударственной. Решать её предстоит сообща – всему мировому сообществу» [Крайнова Н.А., 2019].

Важно отметить, что регулятор постоянно совершенствует законодательство РФ по обеспечению информационной безопасности. Ещё в 2006 году были приняты Федеральные законы № 149-ФЗ об информации, информационных технологиях и о защите информации, 152-ФЗ о правилах работы с персональными данными. Чуть позже, в

2011 году был введен закон № 68-ФЗ, который регулирует использование электронной подписи. Спустя шесть лет, появился закон № 187-ФЗ, описывающий правила защиты IT-инфраструктуры на предприятиях, работающих в сферах, критически важных для государства. Совсем недавно, Указом Президента Российской Федерации от 01.05.2022 г. № 250 введены дополнительные меры по обеспечению информационной безопасности в стране. Таким образом, государство пытается устранить разрозненные правила защиты данных, снять правовую неопределенность и возможные варианты обхода законодательства. В настоящее время работа продолжается над Цифровым Кодексом Российской Федерации, который должен отрегулировать весьма объемную систему общественных отношений в информационном пространстве, в первую очередь оборот данных и сведений в цифровом формате.

Обеспечение доверия, безопасности и защиты данных во всё более оцифрованном мире – совместная задача многих заинтересованных сторон. Помимо правительства, бизнеса, науки, сами пользователи должны осознавать важность и необходимость обеспечения информационной безопасности. Не только операторы критической инфраструктуры, которые выполняют юридические обязательства по кибербезопасности, но и бизнес-структуры, простые обыватели должны постоянно работать над повышением уровня безопасности своих данных. Кроме того, на государственном уровне важно определить ключевые технологии и навыки, необходимые для поддержания и развития цифрового суверенитета.

Заключение

Цифровизация – это, прежде всего, предпринимательский проект. Чтобы достичь этого, нужно предоставить свободу развития для рисковых инвестиций, инновационной продукции или новейших услуг на основе данных. Одновременно важно ликвидировать неясности, противоречия в нормативной базе и обеспечить информационную безопасность. Это касается обязанности и готовности нести ответственность за совершённые противоправные действия, соблюдения авторских прав и честной конкуренции. Все модели, которые используют цифровые технологии должны быть предметом открытого, инновационного соперничества. Кроме того, одной из задач цифровизации должна стать разработка таких бизнес-моделей и технологий, которые бы позволяли использовать данные, не ставя под угрозу неприкосновенность частной жизни или безопасность данных в целом.

В России необходимо пересмотреть национальную законодательную базу, касающуюся цифровизации и обеспечения информационной безопасности. Мы поддерживаем инициативу разработки Цифрового Кодекса России, который будет следовать вышеупомянутым принципам открытой и равной конкуренции, безопасности данных и их суверенитета.

Список литературы

1. Крайнова Н.А. «Международная цифровая безопасность»: миф или реальность / Н.А. Крайнова // Криминология: вчера, сегодня, завтра. 2019. № 4 (55). С. 42-46.

2. Кувалдина Т.Б. Статус учетной информации в целях обеспечения экономической безопасности предприятия / Т.Б. Кувалдина, Л.А. Руди, Г.В. Неделько // Актуальные вопросы развития экономики: материалы Международной научно-практической конференции, Омск, 16 ноября 2017 года. Омск: Финансовый университет при Президенте Российской Федерации, Омский филиал, 2017. С. 230-233.

3. Назаретян А.Р. Цифровая безопасность, защищенность и анонимность в интернет пространстве как новые ценности современного общества / А.Р. Назаретян // Социальная интеграция и развитие этнокультур

в евразийском пространстве. 2020. Т. 2. № 9. С. 209-214.

4. Примак Т.К. Цифровая безопасность: правовое регулирование, соотношение с кибербезопасностью / Т.К. Примак, О.А. Серова // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2019. № 2 (56). С. 57-60.

5. РИА Омск-информ [Электронный ресурс]. URL: https://dzen.ru/a/Zo0dqQRNLicftjy_

6. РТК-Солар Тренды страхования киберрисков на российском рынке // https://rt-solar.ru/?utm_source=yandex&utm_medium=cpc&utm_campaign=Brand_search_rf&utm_content

7. Сизьунго М., Московкин В.М., Ваганова О.В. Пространственно-временной анализ процессов цифровизации российских регионов // Научный результат. Экономические исследования. 2022. Т. 8. № 3. С. 48-62.

8. Следнева К.Е. Нивелирование цифровых угроз как средство обеспечения экономической безопасности в современном мире / К.Е. Следнева, Т.Б. Кувалдина // Сибирская финансовая школа. 2024. № 1 (153). С. 98-107.

9. Статиста 2024 [Электронный ресурс]. URL: https://www.statista.com/accounts/pa

10. Центр стратегических разработок Прогноз развития рынка кибербезопасности в Российской Федерации на 2023-2027 годы [Электронный ресурс]. URL: https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-kiberbezopasnosti-v-rossiyskoy-federatsii-na-2023-2027-gody/

References

1. Kraynova, N.A. "International digital security": myth or reality / N.A. Kraynova // *Criminology: yesterday, today, tomorrow*. 2019. No. 4 (55). P. 42-46.

2. Kuvaldina, T.B. The status of accounting information in order to ensure the economic security of an enterprise / T.B. Kuvaldina, L.A. Rudi, G.V. Nedelko // *Current issues in economic development: materials of the International scientific and practical conference*, Omsk, November 16, 2017. Omsk: Financial University under the President of the Russian Federation, Omsk branch, 2017. P. 230-233.

3. Nazaretyan, A.R. Digital security, protection and anonymity in the Internet space as new values of modern society / A.R. Nazaretyan // *Social integration and development of ethnocultures in the Eurasian space*. 2020. Vol. 2, No. 9. P. 209-214.

4. Primak, TK Digital security: legal regulation, relationship with cybersecurity / TK Primak, OA Serova // *Bulletin of the Kaliningrad branch of the St. Petersburg University of the Ministry of Internal Affairs of Russia*. 2019. No. 2 (56). P. 57-60.

5. RIA Omsk-inform [Electronic resource]. URL: https://dzen.ru/a/Zo0dqQRNLicftjy_

6. RTK-Solar Cyber risk insurance trends in the Russian market // https://rt-solar.ru/?utm_source=yandex&utm_medium=cpc&utm_campaign=Brand_search_rf&utm_content

7. Munenge S., Moskovkin V.M., Vaganova O.V. (2022), “Spatial and temporal analysis of digitalization processes in russian regions”, *Scientific result. Economic research*, 8, 3, 48-62.

8. Sledneva, K.E. Leveling digital threats as a means of ensuring economic security in the modern world / K.E. Sledneva, T.B. Kuvaldina // *Siberian financial school*. 2024. No. 1 (153). P. 98-107.

9. Statista 2024 [Electronic resource]. URL: https://www.statista.com/accounts/pa

10. Center for Strategic Research Forecast for the development of the cybersecurity market in the Russian Federation for 2023-2027 [Electronic resource]. URL: https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-kiberbezopasnosti-v-rossiyskoy-federatsii-na-2023-2027-gody/

Информация о конфликте интересов: авторы не имеют конфликта интересов для декларации.

Conflicts of Interest: the author has no conflict of interest to declare.

Маслова Ирина Алексеевна, доктор экономических наук, профессор, профессор кафедры экономики, финансов и бухгалтерского учета, Орловский государственный университет имени И.С. Тургенева (г. Орел, Россия)

Irina A. Maslova, Doctor of Economics, Professor, Professor of the Department of Economics, Finance and Accounting, I.S. Turgenev Oryol State University (Oryol, Russia)