

УДК 004.0

DOI: 10.34670/AR.2026.90.35.020

Динамика расходов на продукты и услуги в области информационной безопасности в промышленном секторе России

Иосип Игорь Викторович

ООО НТЦ «БИНАРТЕЛЕКОМ»,
119021, Российская Федерация, Москва, переулок Оболенский, 10, стр. 1;
e-mail: 7290916@mail.ru

Аннотация

Внедрение в настоящее время современных цифровых технологий повышает конкурентоспособность, эффективность процессов и коммуникаций. Но одновременно с этим для организаций повышаются и риски, связанные с вероятностью потерь и утечек данных, сбоев и остановки работы информационных ресурсов и оборудования, управляемого цифровыми технологиями. Цель исследования — проведение литературного обзора, формирование эмпирической базы данных и оценка динамики расходов на продукты и услуги в области информационной безопасности в промышленном секторе России. В исследовании применялись такие методы общенаучного познания как системный анализ, временные ряды, анализ синтез. А также табличный — для обеспечения визуализации хода и результатов работы. В текущем исследовании оценивается динамика и структура расходов организаций промышленности России на цифровизацию и продукты и услуги в области информационной безопасности. Отмечается значительное влияние пандемии COVID-19 и санкционного режима на динамику показателей. В целом на текущий момент расходы на обеспечение кибербезопасности составляют порядка 5% от общих расходов в промышленности на цифровые технологии. В разрезе отдельных видов деятельности максимальный уровень расходов отмечается в секторах нефте- и газодобычи, нефтепереработки, металлургии, в электроэнергетике. Таким образом, очевидно, что компании экспортоориентированного сырьевого и топливно-энергетического профиля обеспечивают свою информационную безопасность в максимальной степени.

Для цитирования в научных исследованиях

Иосип И.В. Динамика расходов на продукты и услуги в области информационной безопасности в промышленном секторе России // Экономика: вчера, сегодня, завтра. 2026. Том 16. № 5А. С. 205-212. DOI: 10.34670/AR.2026.90.35.020

Ключевые слова

Динамика, кибербезопасность, промышленный сектор, расходы, риски, цифровизация, факторы, экономика, методология исследования.

Введение

Процессы цифровизации, являющиеся объективным отражением технического прогресса, ставят перед экономикой новые вызовы. С одной стороны, внедрение современных цифровых технологий повышает конкурентоспособность, эффективность процессов и коммуникаций. Но одновременно с этим для организаций повышаются и риски, связанные с вероятностью потерь и утечек данных, сбоев и остановки работы информационных ресурсов и оборудования, управляемого цифровыми технологиями [Голикова, Иода, 2018; Михневич, 2022; Шевырева, 2021]. Это создаёт необходимость формирования системы защиты от киберугроз в контексте построения в России цифровой экономики [Коноплева, Корыстов, Тесленко, 2019].

Минбалеев А.В. указывает на то, что современное высокотехнологичное конкурентоспособное предприятие представляет собой сложную систему, отдельные технологические процессы которой связаны информационными технологиями в единую систему управления технологическими процессами [Минбалеев, Берестнев, Евсиков, 2023]. Соответственно, чем выше технологический уровень развития того или иного промышленного предприятия, тем больше внимания следует уделять вопросам информационной безопасности и защиты от киберугроз. Автор упоминает в работе также Нацпроект «Цифровая экономика», где раздел «Информационная безопасность» указан отдельным пунктом цифровизации отечественной экономики.

Это подчёркивает, что обеспечение информационной защиты является одним из системообразующих направлений государственного развития. Хотя оно и находится на предпоследнем месте по объёмам целевого финансирования в Нацпроекте с долей от общих расходов на построение цифровой экономики в стране в 2018-2024 гг. в 1% по данным Гончарова Ю.А. [Гончаров, 2018].

Как отмечает Махалина О.М., на ликвидацию последствий инцидентов в области информационной безопасности ещё в 2018 г. расходовалось 16,1 млн руб. в расчёте на 1 инцидент для крупных предприятий и 1,6 млн руб. для представителей среднего бизнеса [Махалина, Махалин, 2020]. Со временем объём требуемых расходов растёт и будет расти вслед за увеличением объёмов информации и управляемых цифровыми технологиями производственных, технологических и управленческих процессов [Яхтин, 2021].

Целью подготовки настоящей статьи является проведение литературного обзора, формирование эмпирической базы данных и оценка динамики расходов на продукты и услуги в области информационной безопасности в промышленном секторе России.

Материалы и методы исследования

В рыночных условиях финансовый аспект является ключевым фактором развития любого направления, в том числе защиты от киберугроз (рассматриваемых в ряде научных работ [Башкиров, 2018; Прибочий, 2021; Сухоруков, Гнатенко, 2024]), в том числе отдельно – в контексте регулирования финансовых вопросов [Гусева, 2024; Белоусова, 2019; Махмудова, 2021]. Текущее исследование направлено на анализ расходов организаций промышленного сектора России за 2024 г. в направлении обеспечения информационной безопасности в разрезе кодов ОКВЭД. Также справочно показана динамика общего объёма затрат в этом направлении с 2019 по 2024 гг. Нижний предел исследования обусловлен отсутствием данных по финансированию направления информационной безопасности до 2019 г. в рамках

статобследования Росстата [Росстат, 2024].

В исследовании применялись такие методы общенаучного познания как системный анализ, временные ряды, анализ синтез. А также табличный – для обеспечения визуализации хода и результатов работы.

Ключевым источником данных является раздел Росстата «Наука, инновации и технологии» в части итогов статистического наблюдения по форме №3-информ [Росстат, 2024], где представлены основные итоги использования цифровых технологий организациями России за последние годы.

Результаты и обсуждение

Затраты промышленных компаний на цифровизацию постоянно растут, что обусловлено рядом факторов: увеличением охвата процессами цифровизации новых сфер экономики, технологическим развитием промышленности, инфляцией, санкционными запретами. Динамика этого процесса представлена в таблице 1.

Таблица 1 - Затраты организаций промышленного сектора на цифровизацию и продукты и услуги в области информационной безопасности в 2019-2024 гг., млрд. руб.

Год	Затраты на цифровизацию (общие), млрд. руб.	Прирост к пред. году, %	Затраты на информационную безопасность, млрд. руб.	Прирост к пред. году, %	Доля от общих затрат, %
2019	312	...	9,0	...	2,9
2020	360	15	20,8	131	5,8
2021	479	33	21,5	3	4,5
2022	573	20	20,5	-5	3,6
2023	585	2	31,4	53	5,4
2024	704	20	34,4	10	4,9

Примечание: составлено автором на основе данных [Росстат, 2024].

Как видно из таблицы 1, общие затраты промышленных предприятий на цифровизацию за период 2019-2024 гг. выросли более чем вдвое. Максимальный прирост наблюдался в 2021 г., очевидно, что могло быть связано, как и многие другие аспекты общественных и экономических отношений в данный период, с резким повышением спроса на цифровые услуги вследствие пандемии COVID-19. Также существенным был прирост в 2022 и 2024 гг. – по 20%. Минимальный рост наблюдался в 2023 г. – всего лишь 2%, что, вероятно, обусловлено в том числе и усложнением процедуры закупок оборудования и программного обеспечения за рубежом вследствие ограничительных санкций. Но в 2024 г. в целом динамика вернулась к досанкционным значениям.

Затраты на информационную безопасность демонстрируют совершенно иную динамику: максимум прироста наблюдался в 2020 и 2023 гг., очевидно, по обстоятельствам также возникшим в связи с началом пандемии COVID-19, затем в условиях преодоления санкционных ограничений, когда расходы резко выросли. В 2022 г. затраты на обеспечение кибербезопасности падали по сравнению с 2021 г., очевидно, вследствие ухода с российского рынка ряда зарубежных компаний при введении экономических санкций со стороны недружественных государств.

В относительном выражении удельного веса расходов на информационную безопасность в

общем объёме затрат на цифровизацию в промышленном секторе максимумы наблюдались в 2020 и 2023 гг., когда показатель превышал 5% (5,8% и 5,4%) соответственно. В 2019 г. доля таких расходов была минимальной – 2,9%.

Информация по расходам в разрезе отдельных направлений промышленного производства представлена в таблице 2.

Таблица 2 - Затраты организаций промышленного сектора на цифровизацию и продукты и услуги в области информационной безопасности в 2024 г. в разрезе кодов ОКВЭД2, млрд. руб.

ОКВЭД	Затраты на цифровизацию (общие), млрд руб.	Затраты на информационную безопасность, млрд руб.	%	% от общих затрат
По всем видам экономической деятельности				
-	5244	209	-	4,0
Промышленные предприятия				
-	704	34,3748	100	4,9
В	108	5,8	16,8	5,4
05	6,9	0,1	0,2	1,0
06	66,6	4,5	13,2	6,8
07	9,0	0,4	1,0	4,0
08	8,8	0,0	0,1	0,5
09	16,2	0,8	2,2	4,6
С	459	19,0	55,2	4,1
10	20,4	0,4	1,1	1,8
11	5,4	0,1	0,4	2,4
12	3,8	0,0	0,03	0,3
13	0,8	0,0	0,04	2,0
14	1,7	0,0	0,1	2,1
15	0,4	0,0	0,01	1,2
16	2,9	0,0	0,1	1,4
17	5,4	0,1	0,2	1,4
18	1,4	0,1	0,3	6,5
19	68,8	7,2	20,9	10,4
20	37,0	1,6	4,6	4,3
21	7,9	0,1	0,2	1,0
22	5,8	0,1	0,2	1,4
23	7,2	0,3	0,8	4,0
24	50,2	2,1	6,1	4,2
25	62,1	1,3	3,8	2,1
26	51,4	1,1	3,1	2,1
27	13,7	0,2	0,6	1,5
28	25,4	0,6	1,6	2,2
29	20,1	1,4	4,2	7,1
30	48,9	1,8	5,2	3,6
31	2,3	0,0	0,04	0,6
32	2,4	0,0	0,09	1,4
33	13,8	0,5	1,4	3,5
D	126	8,9	25,9	7,1
E	11,1	0,7	2,1	6,6

Примечание: составлена автором на основе данных [Росстат, 2024].

Как видно из таблицы 2, среди всех организаций промышленного сектора по уровню затрат на продукты и услуги в области информационной безопасности лидируют отрасли нефте- и газодобычи, нефтепереработка, металлургия, а также электроэнергетика, на которые в сумме приходится порядка 2/3 (66,1%) всех расходов промышленных организаций. Ещё около 10% расходов приходится на транспортное машиностроение. На остальные промышленные направления приходится менее 24%.

Таким образом, наблюдается существенный структурный перекос финансирования в сторону сырьевых экспортоориентированных отраслей и производства автомобилей, что повышает риски кибербезопасности для промышленности страны в целом, особенно для высокотехнологичных и несырьевых направлений.

В контексте удельного веса затрат на информационную безопасность в общей массе расходов промышленных организаций на цифровые технологии лидируют предприятия тех же сырьевых направлений. При средней доле расходов на кибербезопасность в промышленности в 4,9% максимума этот показатель для производства кокса и нефтепродуктов (10,4%), добычи нефти и газа (6,8%), производстве автотранспортных средств (7,1%), электроэнергетике (7,1%). То есть, среди лидеров снова наблюдаются преимущественно сырьевые отрасли и автомобилестроение.

Заключение

Динамика расходов на информационную безопасность имеет нестабильный характер, который значительно зависит от социально-экономической обстановки в стране. Так, резкий рост расходов наблюдался во время пандемии COVID-19 (2020 г.) и в 2023 г. во время наиболее сложного периода развития процессов импортозамещения вследствие санкций. Удельный вес расходов на кибербезопасность варьируется от 2,9% до 5,8%, но за последние 2 года находится в пределах 5%.

Отдельно следует подчеркнуть зафиксированное снижение затрат в 2022 г. относительно 2021 г., что, вероятно, отражает влияние ухода с российского рынка ряда зарубежных компаний и поставщиков, а также возникшие разрывы в цепочках поставок продуктов и услуг по кибербезопасности. Данный провал может свидетельствовать не о снижении потребности в защите, а о временном ограничении возможностей закупок и реализации проектов, что повышает уязвимость в переходный период.

Оценка общего объёма расходов в разрезе кодов ОКВЭД2 показала, что лидерами по объёму затрат на продукты и услуги в области информационной безопасности выступают нефте- и газодобыча, нефтепереработка, металлургия и электроэнергетика, на которые совокупно приходится около 2/3 всех расходов промышленных организаций (66,1%). Ещё порядка 10% формирует транспортное машиностроение, тогда как на остальные направления приходится менее 24%. Аналогичный перекос подтверждается и в показателях удельного веса: при среднем уровне по промышленности 4,9% максимальные значения характерны для производства кокса и нефтепродуктов (10,4%), добычи нефти и газа (6,8%), производства автотранспортных средств (7,1%) и электроэнергетики (7,1%). Таким образом, наиболее высокие доли и объёмы затрат сосредоточены преимущественно в сырьевых, экспортоориентированных сегментах и частично в автомобилестроении.

Выявленная концентрация ресурсов имеет двойственный эффект. С одной стороны, она отражает повышенную критичность и капиталоемкость инфраструктуры в указанных отраслях, а также высокую цену инцидентов. С другой стороны, столь выраженный перекос, выявленный

в рамках проведенного анализа, может стать «залогом» роста системных рисков кибербезопасности для промышленности в целом, поскольку высокотехнологичные и несырьевые направления могут оставаться в зоне недофинансирования и, следовательно, повышенной уязвимости. В практическом плане это означает необходимость более сбалансированного подхода к распределению ресурсов и развитию мер киберустойчивости в промышленности, ориентированного не только на отрасли-лидеры по бюджетам, но и на сектора, обеспечивающие технологическое обновление и диверсификацию экономики.

Библиография

1. Башкиров Н.И. Защита инфраструктуры США от киберугроз // Правовое обеспечение развития социального государства в свете целей устойчивого развития: сборник материалов Международной научно-практической конференции: в 2 ч. Уфа, 12-13 ноября 2018 г. / отв. ред. Р.В. Нигматуллин. Уфа: Башкирский государственный университет, 2018. Ч. 1. С. 71–80.
2. Белоусова Е. Страхование – защита от киберугроз // Современные страховые технологии. 2019. № 5. С. 84–87.
3. Голикова О.А., Иода Е.В. Цифровая экономика России: открывающиеся возможности и риски // Социально-экономические явления и процессы. 2018. Т. 13, № 104. С. 147–151.
4. Гончаров Ю.А. Особенности финансирования и приоритеты национальной программы «Цифровая экономика» // Горизонты экономики. 2018. № 5(45). С. 90–94.
5. Гусева Н.М. Контроль учета расходов на информационную безопасность // Бюджетный учет. 2024. № 10(238). С. 44–48.
6. Коноплева Ю.А., Корыстов В.А., Тесленко Д.В. Кибербезопасность как фактор развития цифровой экономики // Вестник Северо-Кавказского федерального университета. 2019. № 4(73). С. 49–55. DOI: 10.37493/2307-907X-2019-73-4-49-55.
7. Махалина О.М., Махалин В.Н. Цифровизация бизнеса увеличивает затраты на информационную безопасность // Управление. 2020. Т. 8, № 1. С. 134–140. DOI: 10.26425/2309-3633-2020-1-134-140.
8. Махмудова И.Н. Технологии, формирующие бизнес: защита от киберугроз // Экономика и предпринимательство. 2021. № 10 (135). С. 1089–1092. DOI: 10.34925/EIP.2021.135.10.209.
9. Минбалеев А.В., Берестнев М.А., Евсиков К.С. Обеспечение информационной безопасности оборудования добывающей промышленности в квантовую эпоху // Известия Тульского государственного университета. Науки о Земле. 2023. № 1-1. С. 567–584. DOI: 10.46689/2218-5194-2023-1-1-567-584.
10. Михневич В. Киберриски – что это? // Современные страховые технологии. 2022. № 1. С. 14–17.
11. Наука, инновации и технологии: сведения об использовании цифровых технологий и производстве связанных с ними товаров и услуг (итоги статнаблюдения по ф. № 3-информ) // Росстат. URL: <https://rosstat.gov.ru/statistics/science>.
12. Прибочий М. Защита от киберугроз: новые тренды информационной безопасности бизнеса // Системный администратор. 2021. № 7-8 (224-225). С. 30–33.
13. Сухоруков Р.Н., Гнатенко Ю.А. Блокчейн в кибербезопасности: революционная защита от киберугроз // Тенденции развития науки и образования. 2024. № 105-14. С. 81–84. DOI: 10.18411/tmio-01-2024-706.
14. Шевырева А.Д. Инновации и безопасность электронного бизнеса // Актуальные вопросы современной экономики. 2021. № 9. С. 359–366. DOI: 10.34755/IROK.2021.48.44.062.
15. Яхтин В.А. Национальные информационные риски больших данных // Вестник Волгоградского государственного университета. Экономика. 2021. Т. 23, № 3. С. 16–25. DOI: 10.15688/ek.jvolsu.2021.3.2.

Dynamics of Expenditures on Information Security Products and Services in the Industrial Sector of Russia

Igor' V. Iosip

LLC STC "BINARTELECOM",
119021, 10, bld. 1, Obolenskiy lane, Moscow, Russian Federation;
e-mail: 7290916@mail.ru

Iosip I.V.

Abstract

The current introduction of modern digital technologies increases competitiveness, efficiency of processes, and communications. However, at the same time, risks associated with the probability of data loss and leakage, failures, and shutdowns of information resources and equipment controlled by digital technologies also increase for organizations. The purpose of the study is to conduct a literature review, form an empirical database, and assess the dynamics of expenditures on information security products and services in the industrial sector of Russia. The research employed such methods of general scientific cognition as system analysis, time series, analysis, and synthesis. As well as the tabular method — to ensure visualization of the progress and results of the work. The current study assesses the dynamics and structure of expenditures of Russian industrial organizations on digitalization and information security products and services. The significant impact of the COVID-19 pandemic and the sanctions regime on the dynamics of indicators is noted. In general, at present, expenditures on ensuring cybersecurity amount to about 5% of total expenditures on digital technologies in industry. In the context of individual types of activities, the maximum level of expenditures is observed in the sectors of oil and gas production, oil refining, metallurgy, and the electric power industry. Thus, it is obvious that companies of an export-oriented raw material and fuel and energy profile ensure their information security to the maximum extent.

For citation

Iosip I.V. (2026) Dinamika raskhodov na produkty i uslugi v oblasti informatsionnoy bezopasnosti v promyshlennom sektore Rossii [Dynamics of Expenditures on Information Security Products and Services in the Industrial Sector of Russia]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 16 (5A), pp. 205-212. DOI: 10.34670/AR.2026.90.35.020

Keywords

Dynamics, cybersecurity, industrial sector, expenditures, risks, digitalization, factors, economy, research methodology.

References

1. Bashkirov, N. I. (2018). Zashchita infrastruktury SShA ot kiberugroz [Protecting US infrastructure from cyber threats]. In R. V. Nigmatullin (Ed.), *Pravovoe obespechenie razvitiya sotsial'nogo gosudarstva v svete tseley ustoychivogo razvitiya* [Legal support for the development of the social state in light of the sustainable development goals] (Part 1, pp. 71–80). Bashkir State University.
2. Belousova, E. (2019). Strakhovanie – zashchita ot kiberugroz [Insurance – protection from cyber threats]. *Sovremennye strakhovye tekhnologii* [Modern Insurance Technologies], 5, 84–87.
3. Golikova, O. A., & Ioda, E. V. (2018). Tsifrovaya ekonomika Rossii: otkryvayushchiesya vozmozhnosti i riski [The digital economy of Russia: Emerging opportunities and risks]. *Sotsial'no-ekonomicheskie yavleniya i protsessy* [Socio-Economic Phenomena and Processes], 13(104), 147–151.
4. Goncharov, Yu. A. (2018). Osobennosti finansirovaniya i prioritety natsional'noy programmy "Tsifrovaya ekonomika" [Features of financing and priorities of the national program "Digital Economy"]. *Gorizonty ekonomiki* [Horizons of Economics], 5(45), 90–94.
5. Guseva, N. M. (2024). Kontrol' ucheta raskhodov na informatsionnuyu bezopasnost' [Control of accounting for information security expenses]. *Byudzhethnyy uchët* [Budget Accounting], 10(238), 44–48.
6. Konopleva, Yu. A., Korystov, V. A., & Teslenko, D. V. (2019). Kiberbezopasnost' kak faktor razvitiya tsifrovoy ekonomiki [Cybersecurity as a factor in the development of the digital economy]. *Vestnik Severo-Kavkazskogo federal'nogo universiteta* [Bulletin of the North Caucasus Federal University], 4(73), 49–55. <https://doi.org/10.37493/2307-907X-2019-73-4-49-55>
7. Makhalina, O. M., & Makhalin, V. N. (2020). Tsifrovizatsiya biznesa uvelichivaet zatraty na informatsionnuyu

- bezopasnost' [Business digitalization increases information security costs]. Upravlenie [Management], 8(1), 134–140. <https://doi.org/10.26425/2309-3633-2020-1-134-140>
8. Makhmudova, I. N. (2021). Tekhnologii, formiruyushchie biznes: zashchita ot kiberugroz [Technologies shaping business: Protection from cyber threats]. *Ekonomika i predprinimatel'stvo* [Journal of Economy and Entrepreneurship], 10(135), 1089–1092. <https://doi.org/10.34925/EIP.2021.135.10.209>
9. Minbaleev, A. V., Berestnev, M. A., & Evsikov, K. S. (2023). Obespechenie informatsionnoy bezopasnosti oborudovaniya dobyvayushchey promyshlennosti v kvantovuyu epokhu [Ensuring information security of mining industry equipment in the quantum era]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Nauki o Zemle* [Izvestiya of the Tula State University. Earth Sciences], 1-1, 567–584. <https://doi.org/10.46689/2218-5194-2023-1-1-567-584>
10. Mikhnevich, V. (2022). Kiberriski – chto eto? [Cyber risks – what are they?]. *Sovremennye strakhovye tekhnologii* [Modern Insurance Technologies], 1, 14–17.
11. Pribochiy, M. (2021). Zashchita ot kiberugroz: novye trendy informatsionnoy bezopasnosti biznesa [Protection from cyber threats: New trends in business information security]. *Sistemnyy administrator* [System Administrator], 7-8(224-225), 30–33.
12. Rosstat. (2024). Nauka, innovatsii i tekhnologii: svedeniya ob ispol'zovanii tsifrovyykh tekhnologiy i proizvodstve svyazannykh s nimi tovarov i uslug [Science, innovation and technology: Information on the use of digital technologies and the production of related goods and services]. <https://rosstat.gov.ru/statistics/science>
13. Shevyreva, A. D. (2021). Innovatsii i bezopasnost' elektronnoy biznesa [Innovation and security of electronic business]. *Aktual'nye voprosy sovremennoy ekonomiki* [Current Issues of the Modern Economy], 9, 359–366. <https://doi.org/10.34755/IROK.2021.48.44.062>
14. Sukhorukov, R. N., & Gnatenko, Yu. A. (2024). Blokcheyn v kiberbezopasnosti: revolyutsionnaya zashchita ot kiberugroz [Blockchain in cybersecurity: Revolutionary protection from cyber threats]. *Tendentsii razvitiya nauki i obrazovaniya* [Trends in the Development of Science and Education], 105-14, 81–84. <https://doi.org/10.18411/tmio-01-2024-706>
15. Yakhtin, V. A. (2021). Natsional'nye informatsionnye riski bol'shikh dannykh [National information risks of big data]. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Ekonomika* [Bulletin of Volgograd State University. Economics], 23(3), 16–25. <https://doi.org/10.15688/ek.jvolsu.2021.3.2>