К вопросу о совершенствовании системы статистических показателей безопасности применения цифровых технологий

Михаил Юрьевич Карышев
Самарский государственный университет путей сообщения, г. Самара, Россия

В статье изложены некоторые результаты исследования проблем совершенствования безопасности применения цифровых технологий на новом этапе развития информационно-коммуникационных технологий (ИКТ). Актуальность объясняется тем, что использование ИКТ в современных условиях развития информационного общества и цифровой трансформации экономики, с одной стороны, ведет к получению известных положительных социально-экономических эффектов, но с другой – предполагает неизбежное возникновение негативных последствий. С вопросами защиты интересов личности, общества и государства от внутренних и внешних информационных угроз связано понятие информационной безопасности. Расширение его границ – от низкоуровневых технических мероприятий по защите информационных систем (компьютерной безопасности и кибербезопасности) до стратегического управления экономическим производством в данном контексте – привело к появлению новой релевантной категории: цифровой безопасности – и диктует целесообразность объединения перечисленных терминов в обобщающее понятие «безопасность применения цифровых технологий».

Автором проанализированы существующие методологические подходы к статистическому исследованию рассматриваемых проблем и выработан ряд предложений по совершенствованию соответствующей системы статистических показателей. Для достижения поставленной цели в процессе анализа были использованы методы дескриптивной статистики, корреляционно-регрессионный анализ, а также методы машинного обучения (в частности, различные варианты алгоритмов классификации на основе деревьев решений).

Изучая информационные и методические источники, имеющие опосредованное отношение к статистическим ресурсам (инспектировалась широко известная веб-платформа Kaggle, объединяющая исследователей в области науки о данных и машинного обучения), автор проанализировал результаты тематического опроса компаний. В итоге моделирования влияния фактора «безопасность применения цифровых технологий» на эффективность экономической деятельности было установлено, что его вариация примерно на треть определяет уровень экономической эффективности компании в рамках представленной совокупности. Использование методов машинного обучения позволило получить приемлемые по качеству предсказательные модели классификации компаний по видам экономической деятельности в том же факторном контексте.

С практической точки зрения, по мнению автора, применение предложенного в работе подхода к формированию системы статистических показателей будет полезно для управления процессами, обеспечивающими безопасность применения цифровых технологий в масштабе предприятия, региона и страны в целом.

Ключевые слова: информационно-коммуникационные технологии, информационная безопасность, цифровая безопасность, безопасность применения цифровых технологий, статистический анализ, система статистических показателей.
JEL: C33, L86, O33.
doi: https://doi.org/10.34023/2313-6383-2023-30-3-20-32.

Для цитирования: Карышев М.Ю. К вопросу о совершенствовании системы статистических показателей безопасности применения цифровых технологий. Вопросы статистики. 2023;30(3):20–32.

On Improving the System of Statistical Indicators of the Secure Use of Digital Technologies

Mikhail Yu. Karyshev
Samara State Transport University (SSTU), Samara, Russia

The article presents some results of the study of problems of improving the secure use of digital technologies in the new stage of the development of information and communication technologies (ICT). The relevance is explained by the fact that the use of ICT in the current conditions of the development of the information society and the digital transformation of the economy not only leads to the known positive socio-economic effects but also presupposes the inevitable negative impacts. The objective of protecting the interests of an individual, society, and the state from internal and external information threats is related to the concept of information security. The expansion of its boundaries – from low-level technical measures for the protection of information systems (computer security and cybersecurity) to the strategic management of economic production in this context – has created a new relevant category, digital security, and dictates the expediency of combining these terms into a general concept of «secure use of digital technologies».

The author analyzed the existing methodological approaches to the statistical study of the problems under consideration and developed several proposals for improving the corresponding system of statistical indicators. Methods of descriptive statistics, correlation-regression analysis, and machine learning methods (in particular, various variants of classification algorithms based on decision trees) were used in the analysis to achieve this goal.

While studying information and methodological sources which are indirectly related to statistical resources (a well-known web platform that brings together researchers in the field of data science and machine learning, Kaggle, was examined), the author analyzed the results of a thematic survey of companies. As a result of modeling the influence of the «secure use of digital technologies» factor on the efficiency of economic activity, it was established that its variation by about a third determines the level of economic efficiency of the company within the presented population. The application of machine learning techniques has resulted in acceptable quality predictive models for classifying companies by economic activity in the same factor context.

From a practical point of view, according to the author, the application of the proposed approach to the formation of a system of statistical indicators shall be beneficial for managing processes that ensure the security of the use of digital technologies at the enterprise, region, and country level as a whole.

Keywords: information and communication technologies, information security, digital security, secure use of digital technologies, statistical analysis, system of statistical indicators.

JEL: C33, L86, O33.

doi: https://doi.org/10.34023/2313-6383-2023-30-3-20-32.

For citation: Karyshev M.Yu. On Improving the System of Statistical Indicators of the Secure Use of Digital Technologies. *Voprosy Statistiki.* 2023;30(3):20–32. (In Russ.)

Введение

Цифровая трансформация, при всех ее уже претворенных в жизнь или еще только ожидаемых позитивных социально-экономических эффектах, неизбежно создает информационно-технологические неопределенности и уязвимости, которые могут представлять потенциальную угрозу интересам общества, бизнеса и государства, ставить под удар их информационную безопасность.

Вопросы информационной безопасности в контексте развития информационного общества и цифровой трансформации экономики становятся актуальным предметом статистических исследований, результативность проведения которых определяется в том числе и выбором используемой системы показателей. В этом контексте целью данного исследования является совершенствование системы статистических показателей безопасности применения цифровых технологий, достижение которой требует принятия определенных допущений и решения ряда задач.

Прежде всего во избежание несогласованности в дефинициях и для упрощения понимания предметной области в рамках данной работы будем считать встречающиеся в научной литературе терминологические сочетания со словом безопасность (информационная, информационно-коммуникационная, компьютерная, кибер-, цифровая) нестрогими синонимами и предлагаем использовать формулировку «безопасность применения цифровых технологий» в качестве обобщающего понятия.

Далее, принципиально необходимо трансформировать представление о совокупности процессов, связанных с информационной безопасностью, из исключительно технологической области в более широкое измерение, включающее в себя также социально-экономический контекст (что можно обнаружить в примерах подобных наборов индикаторов и сейчас, однако это не является единой системой).

Наконец, предварительно проанализировав уже существующий опыт (на корпоративном, национальном и международном уровнях), следует приступить к осознанному формированию своего варианта системы. В ее основе должна находиться концепция – исчисление статистического показателя как фиксация состояния одного из этапов процесса нарушения безопасности применения цифровых технологий. Такой подход должен обеспечить некую преемственность исчисляемых показателей, более четкое понимание природы самого отслеживаемого процесса и, как результат, возможность его успешного анализа и приемлемо точного прогноза.

Обзор существующих подходов

Система официальных взглядов и основные положения в этой сфере отражены в Доктрине информационной безопасности Российской Федерации[1],

[1] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646). URL: https://www.garant.ru/products/ipo/prime/doc/71456224/.

Федеральном законе «Об информации, информационных технологиях и о защите информации»[2], семействе стандартов (например, ГОСТ Р ИСО/МЭК 27000–2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»[3]) и других тематических источниках. На глобальном уровне изучением проблематики информационной безопасности занимается ряд международных организаций, каждая из которых действует в определенном профильном секторе. Так, Организация экономического сотрудничества и развития (ОЭСР) акцентирует внимание на социальных и экономических аспектах; разработка технических стандартов возложена, в частности, на Международную организацию по стандартизации (ИСО; *англ.* International Organization for Standardization – ISO) и Международную электротехническую комиссию (МЭК; *англ.* International Electrotechnical Commission – IEC); вопросами киберпреступности занимаются Совет Европы, Управление Организации Объединенных Наций по наркотикам и преступности (*англ.* United Nations Office on Drugs and Crime – UNODC) и Интерпол.

Проблематика обеспечения защиты информации в условиях цифровой экономики в той или иной степени отражена в целом ряде научных публикаций отечественных и зарубежных ученых. Исследуются как общее состояние сферы информационной безопасности (например, в работах [1 и 2]), так и степень ее взаимосвязи с социально-экономическими процессами на основе анализа различных количественных индикаторов. В частности, обнаруженная авторами исследования [3] корреляция выбранных тематических показателей позволяет сделать вывод о том, что цифровая трансформация экономики и общества выступает ключевым драйвером экономического развития только при условии обеспечения информационной и кибербезопасности.

«Состояние информационного развития страны складывается из комплекса подсистем, которые образуют единую национальную базу и выводят единый дифференцированный показатель уровня обеспечения и развития информационной безопасности на территории страны. Ключевым фактором эффективности выступает своевременный учет и анализ основных (базовых) показателей информационной безопасности, который показывает сильные и слабые стороны развития информационной безопасности в разрезе субъектов страны» [4, с. 1162]. Авторы работы проводят анализ эффективности методики оценки информационной безопасности в разрезе субъектов страны и делают вывод о «необходимости внесения новых государственных поправок в оценку показателей развития информационной безопасности. Требуется создание новых методик расчета и систем мониторинга уровня информационной безопасности на территории страны» [там же].

В исследовании [5] представлен критический обзор системы индикаторов для количественной оценки эффективности национальной политики в области информационной безопасности и по результатам анализа внесены предложения для ее улучшения. Выработаны рекомендации по расчету прогнозных значений индикаторов в такой системе, и предложен метод расчета интегрального показателя оценки эффективности национальной политики в сфере информационной безопасности на базе авторской квалиметрической модели, предполагающей использование экспертных оценок.

Не только страны и регионы, но в первую очередь отдельные организации, руководствуясь своими экономическими целями, заинтересованы в мониторинге информационной безопасности собственного бизнеса на основе расчета соответствующих показателей. Одно из таких решений представлено в работе [6] в виде модели измерения эффективности информационной безопасности: она включает в свой состав 10 критических факторов успеха, 100 ключевых показателей эффективности и шесть уровней производительности. При этом сформированный набор индикаторов в силу единства методики расчета и способности разносторонне характеризовать исследуемый объект вполне может рассматриваться в качестве системы статистических показателей.

Сегодня в мире отмечается четкая тенденция к инверсии – если ранее информационный контур безопасности ведения бизнеса очерчивали

[2] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями). URL: https://base.garant.ru/12148555/.

[3] ГОСТ Р ИСО/МЭК 27000–2012. Национальный стандарт Российской Федерации «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности». URL: https://docs.cntd.ru/document/1200102762/.

технические специалисты, то теперь политику информационной безопасности определяют представители высшего менеджмента исходя из оценки рисков, прежде всего экономического характера. В этом контексте привычная категория «информационная безопасность» фактически трансформировалась в «цифровую безопасность», что вполне явно прослеживается в тематических публикациях ОЭСР[4]. Так, в [7] содержится свод рекомендаций по управлению цифровой безопасностью применительно к разным уровням детализации: от базисного, интуитивно понятного, отражающего социально-экономические эффекты, и до самого продвинутого, затрагивающего технические аспекты цифровых технологий. Структура политики такого управления пластична и в последней версии (2022 г.) представлена на рис. 1.

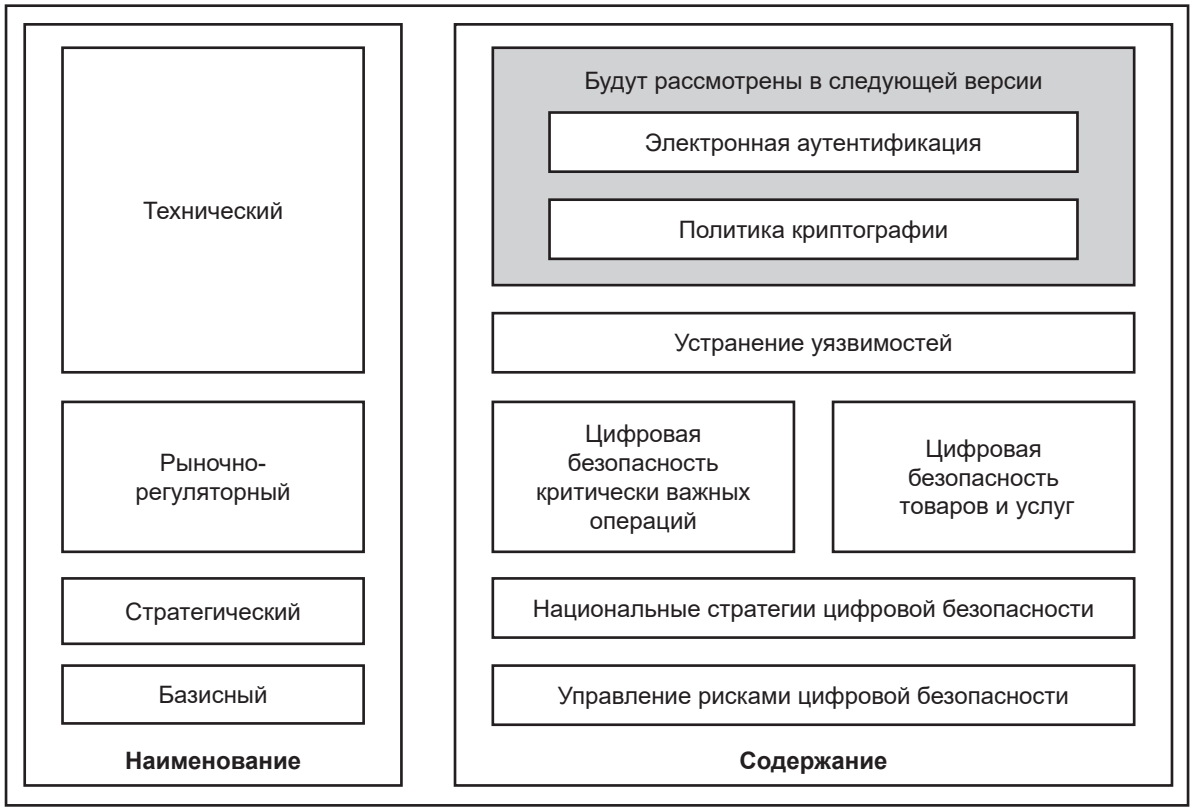

Рис. 1. **Уровни иерархической структуры политики цифровой безопасности ОЭСР**

Источник: [7, p. 7].

Подготовленный ОЭСР и опубликованный в 2019 г. отчет [8] обобщает результаты деятельности этой организации в области разработки основ и набора статистических показателей, которые можно было бы использовать для оценки методов управления рисками информационной (в принятой ОЭСР терминологии – цифровой) безопасности предприятий. В частности, был разработан и опробован инструмент проведения такого обследования, соответствующий предложенной структуре.

Международный союз электросвязи (МСЭ; *англ*. International Telecommunication Union – ITU) – одна из старейших в мире организаций, действующих сегодня под эгидой ООН, – разработала (совместно с компанией ABI Research) Глобальный индекс кибербезопасности (ГИК; *англ*. Global Cybersecurity Index – GCI) и впервые опубликовала его в 2015 г. [9]. Этот интегральный показатель отражает успехи стран мира на пути к достижению целей по основным направлениям кибербезопасности (см. таблицу 1).

[4] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Paris: OECD Publ., 2002. 29 p. doi: https://doi.org/10.1787/9789264059177-en-fr; Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. Paris: OECD Publ., 2015. 72 p. doi: https://doi.org/10.1787/9789264245471-en; [7].

Таблица 1

Основные направления Глобального индекса кибербезопасности

Направление	Содержание
Правовые меры	Оценка наличия правовых институтов и структур, занимающихся вопросами кибербезопасности и киберпреступности
Технические меры	Оценка наличия технических институтов и платформ, занимающихся кибербезопасностью
Организационные меры	Оценка наличия институтов координации политики и стратегий развития кибербезопасности на национальном уровне
Меры по наращиванию потенциала	Оценка наличия программ исследований и разработок, образования и обучения, сертифицированных специалистов и агентств государственного сектора, способствующих наращиванию потенциала кибербезопасности
Меры сотрудничества	Оценка наличия партнерств, механизмов сотрудничества и сетей обмена информацией в области кибербезопасности

Источник: составлено автором по [10].

В 2020 г., согласно источнику [10], в состав проиндексированной совокупности вошло 169 государств, где Российская Федерация, набрав 98,06 балла из 100, разделила 5-е место с Объединенными Арабскими Эмиратами и Малайзией в общем рейтинге и единолично заняла 1-е место в рейтинге стран Содружества Независимых Государств. Специализированная анкета для построения индекса включает ряд вопросов по каждому из сформулированных направлений и предполагает получение ответов с использованием профильных компетенций в части законов и нормативных актов, деятельности общественных организаций, научных школ и центров разработок, а также других аспектов из области кибербезопасности. Полученные данные обобщаются в показатели, которым на основе оценок специально привлекаемых экспертов присваиваются определенные веса в зависимости от важности их вклада, после чего исчисляется сам индекс путем осреднения показателей на арифметической или геометрической основе. К сожалению, Глобальный индекс кибербезопасности не предоставляет какую-либо количественную информацию, характеризующую процесс создания киберугроз, их мотивы, отражение и последствия.

Результаты методологических разработок международных организаций в области информационной (цифровой, кибер-) безопасности получают свое логическое развитие в стандартах международных и национальных органов статистики. Учитывая значительный уровень гармонизации существующей статистической методологии в этой сфере и во избежание повторяемости, целесообразно будет в первом случае рассмотреть систему показателей, используемую при обследовании организаций (например, стран Евросоюза), а во втором – домашних хозяйств (применительно к населению Российской Федерации).

Статистическая служба Европейского союза (Евростат) ежегодно (с 2002 г.) проводит и публикует результаты опроса предприятий об использовании ими информационно-коммуникационных технологий (ИКТ) и электронной коммерции. Наиболее актуальные статистические данные были получены в результате обследований предприятий, проведенных национальными статистическими органами стран – членов Евросоюза в первые месяцы 2022 г.: было опрошено около 150 400 предприятий с 10 и более сотрудниками или самозанятыми лицами из 1,47 млн предприятий в ЕС.

Некоторые дескриптивные статистики совокупности стран ЕС по ряду показателей информационной безопасности предприятий приведены в таблице 2.

Из данных таблицы 2 следует, что в 2022 г. в среднем 88,0% предприятий в ЕС с 10 и более сотрудниками или самозанятыми лицами использовали хотя бы одну меру для обеспечения целостности, доступности и конфиденциальности данных и систем ИКТ. Больше трети предприятий (37,8%) сообщили о наличии документов, устанавливающих меры, практику или процедуры по обеспечению безопасности ИКТ. На каждом четвертом предприятии (24,9%) эти документы были определены или рассмотрены в течение последних 12 месяцев. Каждое пятое предприятие (20,8%) было застраховано от инцидентов безопасности ИКТ. Наконец, в 2022 г. каждое пятое предприятие столкнулось с последствиями инцидентов безопасности, связанных с ИКТ. Следует отметить, что значения коэффициента вариации (C_V) с его пороговым значением в 33% характеризуют совокупность организаций стран Евросоюза как «пограничную» в оценке ее однородности по большинству показателей.

Таблица 2

Характеристики информационной безопасности предприятий в странах Европейского союза
(в процентах от обследуемых предприятий)

Характеристики	X_{min}	$\bar{x}$	X_{max}	Медиана	C_V, %
Используют как минимум одну меру безопасности ИКТ	62	88,0	98	90	8,6
Информируют работников об их обязанностях в области безопасности ИКТ	32	57,0	75	60	18,6
Имеют разработанные инструкции по мерам, практикам или процедурам по безопасности ИКТ	15	37,8	68	36	34,1
Имеют страховку от инцидентов, связанных с ИКТ	4	20,8	71	14	75,0
Составили или проверили существующие инструкции по безопасности ИКТ предприятия в течение последних 12 месяцев	7	24,9	43	21	38,2
Пережили инциденты безопасности, связанные с ИКТ, имевшие некоторые последствия в отчетном (2021) году	11	20,5	44	19	35,6

Примечание. Здесь и далее в таблицах 3 и 4: X_{min} – минимальное значение показателя; $\bar{x}$ – среднее значение показателя; X_{max} – максимальное значение показателя; C_V – коэффициент вариации.

Источник: расчеты автора.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) в рамках реализации федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» осуществляет разработку методик расчета тематических показателей, находящих отражение в публикациях об использовании информационных технологий населением и организациями. Федеральная служба государственной статистики (Росстат) в сотрудничестве с Минцифры России и Национальным исследовательским университетом «Высшая школа экономики» (НИУ ВШЭ) регулярно публикует статистические сборники, посвященные информационному обществу и цифровой экономике. Результаты проведенного Росстатом в 2022 г. выборочного федерального статистического наблюдения по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей содержат, в частности, данные об инцидентах информационной безопасности и средствах защиты, применяемых для их предотвращения (см. таблицы 3 и 4).

Таблица 3

Дескриптивные статистические показатели, характеризующие проблемы информационной безопасности, с которыми сталкивалось российское население
(в процентах от обследуемых лиц в возрасте от 15 до 74 лет)

Наличие/отсутствие проблем	X_{min}	$\bar{x}$	X_{max}	Медиана	C_V, %
Сталкивались со следующими проблемами:					
Заражение вирусом, что привело к потере информации и/или времени на их удаление	0,7	5,1	22,0	4,6	76,3
Несанкционированный доступ к компьютеру (информационным ресурсам, информационным системам)	0,1	1,7	19,2	1,2	142,8
Несанкционированная рассылка (спам)	3,8	23,5	81,9	21,5	55,0
Получение по электронной почте мошеннических писем с просьбой выслать персональные данные	0,1	2,6	9,2	2,0	84,6
Перенаправление на фальшивые сайты с просьбой указать персональные данные	0,0	1,9	8,0	1,4	88,1
Посещение детьми нежелательных сайтов, контакты детей с потенциально опасными людьми через сеть Интернет	0,0	0,6	3,3	0,4	98,4
Хищение денежных средств или персональных данных	0,0	0,5	5,7	0,3	162,3
Использование мобильного телефона неизвестными лицами	0,0	1,7	39,2	0,4	320,3
Использование электронной почты неизвестными лицами	0,0	1,0	28,6	0,3	369,1
Другие проблемы информационной безопасности	0,2	3,5	2,4	20,8	111,4
Не сталкивались с проблемами информационной безопасности	12,8	69,4	92,2	70,9	20,5

Источник: расчеты автора по данным Росстата.

Таблица 4

Использование российским населением средств защиты информации
(в процентах от обследуемых лиц в возрасте от 15 до 74 лет)

Использование/неиспользование средств защиты	X_{min}	$\bar{x}$	X_{max}	Медиана	C_V, %
Использовали средства защиты – всего	36,1	71,7	98,8	73,0	16,1
из них: антивирусные средства	29,2	68,5	98,8	69,9	18,1
антиспамовые фильтры	1,7	15,2	13,6	53,9	58,4
средства родительского контроля или фильтрации интернет-ресурсов	0,	2,1	1,7	9,9	87,8
другие средства защиты	0,1	2,1	1,1	12,4	121,4
Не используют средства защиты	0,4	18,3	16,9	60,0	52,0
Затруднились ответить	0,6	10,1	10,2	28,4	61,2

Источник: расчеты автора по данным Росстата.

Явно прослеживаемая в таблицах высокая степень неоднородности совокупности регионов Российской Федерации по большинству показателей указывает на наличие типов региональных групп по признакам интенсивности и номенклатуры угроз информационной безопасности: в одних регионах население постоянно сталкивается с такого рода инцидентами, в других – лишь изредка (некоторое исключение здесь составляет та часть населения, которая вообще не сталкивалась с проблемами информационной безопасности).

Проведенный обзор научных изысканий отечественных и зарубежных ученых, а также используемых в настоящее время официальных методологий профильных и статистических организаций выявил ряд проблем, среди которых следует отметить множественность трактовок самого понятия информационной безопасности и некоторую фрагментарность применяемых систем статистических показателей. В целях совершенствования существующей системы статистических показателей представляется логичным разработать новый подход к формированию структуры такой системы. Методологически такой подход должен быть основан на реализации количественного измерения отдельных этапов процесса нарушения безопасности применения цифровых технологий, что позволит обеспечить системность и гармонизацию отбираемых показателей.

Концепция формирования системы показателей безопасности применения цифровых технологий

Необходимым условием получения научно обоснованных результатов оценки и анализа объекта статистического исследования служит наличие соответствующей системы индикаторов, представляющей собой «комплекс взаимосвязанных и расположенных в логической последовательности показателей, всесторонне характеризующих состояние и развитие массовых явлений общественной жизни» [11, с. 21].

Современными отечественными учеными-статистиками предлагается (например, в [12, с. 80]) осуществлять формирование системы статистических показателей, руководствуясь рядом принципов, среди которых фигурируют такие как: *принцип системного подхода* (в совокупности разнообразные статистические показатели полностью описывают объект исследования); *принцип информативности при минимизации числа статистических показателей* (показатели должны быть максимально информативны, при этом их количество должно быть минимально) и *принцип количественной определенности оценки* (для показателей должна быть определена количественная оценка, они должны иметь эталонное или нормативное значение, должен быть известен диапазон принимаемых значений).

Очевидно, что система статистических показателей безопасности применения цифровых технологий – в силу высокой степени динамики процессов в этой сфере – не может являться статичной структурой, а должна отражать развитие. Такой подход продемонстрирован на рис. 2, где концептуальная схема формирования системы показателей содержит два компонента, отображающих аспекты оценки и анализа: характерный, учитывающий особенности предметной области – «Процесс», и общий («Направление» и «Масштаб»), свойственный логике построения систем в целом.

В результате состав показателей системы формируется динамически при сохранении общей структуры, основанной на логике взаимосвязи аспектов (пример практической реализации схемы представлен в таблице 5).

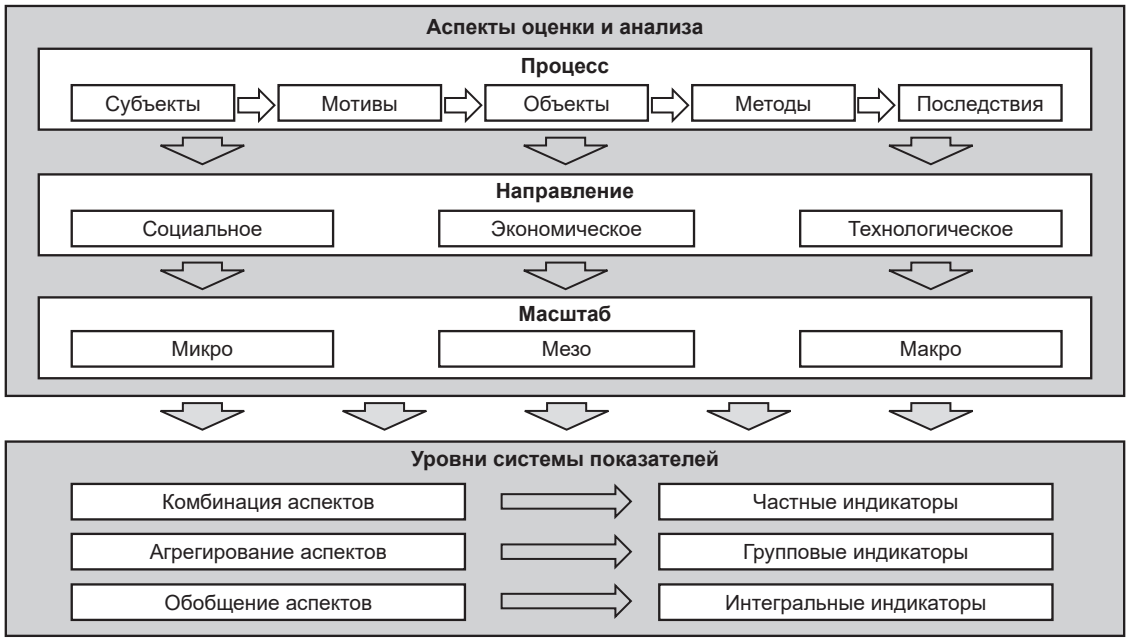

Рис. 2. **Концептуальная схема формирования системы статистических показателей безопасности применения цифровых технологий**

Источник: составлено автором.

Таблица 5

Примеры индикаторов – представителей системы статистических показателей безопасности применения цифровых технологий

Направление	Показатели по этапам процесса	Масштаб
	Субъект	
Технологическое	Число инцидентов, характеризующих внутренние и внешние по отношению к деятельности организации источники киберугроз, единиц	Микро
Экономическое	Число сотрудников по информационной безопасности в штате организации, человек	Микро
Социальное	Доля домашних хозяйств, пострадавших от злонамеренных действий неизвестных лиц через социальные сети и онлайн-сервисы, в процентах	Макро
	Мотив	
Технологическое	Доля инцидентов, связанных с кибермошенничеством, в процентах	Микро
	Число инцидентов, связанных с кибертерроризмом, единиц	Макро
Экономическое	Доля организаций, столкнувшихся с вымогательством посредством использования цифровых технологий, в процентах	Мезо Макро
Социальное	Доля лиц в домашнем хозяйстве, сталкивавшихся с угрозами разглашения личной информации с целью вымогательства, в процентах	Микро
	Объект	
Технологическое	Число инцидентов, связанных с попытками проникновения внутрь периметра информационной системы организации, единиц	Микро
	Доля инцидентов в центрах хранения данных, связанных с кибербезопасностью, в процентах	Макро
Экономическое	Структура внутренних информационных ресурсов организации, в процентах	Микро
	Доля организаций, имеющих полнофункциональный сайт с административной частью, в процентах	Мезо Макро
Социальное	Число учетных записей в социальных сетях в среднем на одного члена домашнего хозяйства, единиц	Микро
	Метод	
Технологическое	Число инцидентов, связанных с отказом в обслуживании запросов клиентов сайта организации в связи с кибератаками, единиц	Микро
	Число зарегистрированных вредоносных программ по видам, единиц	Макро
Экономическое	Доля организаций, подвергшихся кибератакам по видам, в процентах	Макро
Социальное	Доля домашних хозяйств, столкнувшихся с кибермошенничеством с использованием методов социальной инженерии, в процентах	Макро
	Последствия	
Технологическое	Объем утраченных данных организации вследствие кибератаки, гигабайт (терабайт, петабайт и т. д.)	Микро
Экономическое	Величина ущерба из-за кибератаки на сайт организации, млн рублей	Микро
	Величина финансовых потерь в результате кибератак, млн рублей	Макро
Социальное	Периодичность потери контроля над учетными записями, случаев за период (например, за год)	Микро
	Доля домашних хозяйств, отказавшихся от использования цифровых услуг правительства и бизнеса в целях защиты информации, в процентах	Мезо Макро

Источник: составлено автором.

В приведенном в таблице 5 перечне имеется ряд показателей, представляющих технологический уровень предметной области, в названии которых используется термин «инцидент».

Под инцидентом информационной безопасности (ИБ), согласно ГОСТ Р ИСО/МЭК 27000–2012, понимается одно или несколько нежелательных или неожиданных событий ИБ, которые со значительной степенью вероятности приводят к компрометации операций бизнеса и создают угрозы для ИБ. Инциденты имеют широкую классификацию, но прежде всего следует выделять две их основные группы: преднамеренные, включающие в себя весь набор способов и методов создания угроз ИБ (фишинг, брутфорс, программы-вымогатели, черви, трояны и т. п.), и случайные, вызванные ошибками пользователей, нелицензированным программным обеспечением и прочими причинами.

В этой связи оценку и анализ безопасности применения цифровых технологий весьма удобно представлять как последовательность этапов некоего процесса отслеживания такого инцидента (субъект – мотив – объект – методы – последствия). Например, от его инициатора (злоумышленника) через мотив (хулиганство, мошенничество, терроризм) к объекту (информационный ресурс гражданина, корпорации, правительства) посредством всего спектра доступных методов и до результата в виде финансовых и репутационных потерь. При этом возможен и позитивный вариант такого процесса: например, субъект (инженер службы ИБ) – мотив (защита информационного ресурса) – объект (информационные системы и сети) – метод (алгоритм действий со стороны службы ИБ) – последствия (угроза конфиденциальности, целостности и доступности ресурса предотвращена).

Вполне ясно, что исчисление некоторых показателей такой системы, относящихся к мезо- (регион страны, вид экономической деятельности) и макроуровням (страна), требует проведения специальных выборочных обследований, что на практике трудно реализуемо в связи со множеством ожидаемых проблем в решении программно-методологических и организационных вопросов.

Анализ данных опроса о готовности компаний к киберугрозам

В процессе поиска новых примеров систем показателей, пусть даже опосредованно относящихся к статистической методологии безопасности применения цифровых технологий, был проинспектирован целый ряд общедоступных информационных ресурсов, в частности веб-платформа Kaggle – созданная в 2010 г. и действующая под характерным лозунгом «Home of Data Science» система организации конкурсов по исследованию данных. Обнаруженный здесь набор данных, полученных в итоге исследования «Готовность российских компаний к киберугрозам. Cyber risks readiness. Russia 2018–2020», по своей сути представляет собой не что иное, как результаты тематического конъюнктурного обследования. Данные, представленные в панельном виде, включают 1146 наблюдений за три года с 2018 по 2020 г. для 382 российских компаний различных видов деятельности (информационные технологии и телекоммуникации, финансы, строительство, производство, энергетика, медицина и др.). Этот массив характеризуется как финансовыми показателями [среди которых, например, показатель собственного капитала (ROE), известный по модели Дюпон (DuPont model)], так и результатами экспертных оценок готовности компаний к киберугрозам.

В рамках изучения набора данных был проведен анализ взаимосвязи индикаторов финансово-экономического состояния компаний и уровня их готовности к киберугрозам. Из исходного набора индикаторов был отобран ряд показателей – их характеристики представлены в таблице 6.

Типы этих величин определялись на основе следующей принятой (как статистиками, так и специалистами в области анализа данных) классификации: числовые (непрерывные и дискретные) и категориальные (номинальные, то есть неупорядоченные, и порядковые, или ординальные). Наряду с этим, в соответствии с логикой анализа отобранные показатели в зависимости от своей роли были поделены на факторные и результативные.

Анализ значений матрицы коэффициентов парной корреляции (см. таблицу 7) показал наличие тесных связей между некоторыми показателями; в итоге из их числа были исключены две величины – показатель рентабельности активов (ROA) и показатель готовности персонала к киберугрозам (PEOPLE).

Таблица 6

Набор показателей результатов исследования готовности российских компаний к киберугрозам

Показатель	Роль	Тип	Определение
ROE	результат	непрерывный	*показатель рентабельности собственного капитала компании*
ROA	результат	непрерывный	*показатель рентабельности активов компании*
IND	фактор	номинальный	*показатель принадлежности компании к определенному виду экономической деятельности*; принимает значения от 1 («IT и телеком-компании») до 7 («Другие»)
INFR	фактор	ординальный	*показатель уровня готовности организации к киберугрозам с точки зрения инфраструктуры*; принимает полученные на основе экспертных оценок значения от 1 («низкий») до 5 («высокий»)
PEOPLE	фактор	ординальный	*показатель уровня готовности организации к киберугрозам с точки зрения менеджмента организации и уровня подготовленности сотрудников*; методика и диапазон оценок те же
PARTNERS	фактор	ординальный	*показатель уровня готовности организации к киберугрозам с точки зрения взаимодействия организации с партнерами и поставщиками*; методика и диапазон оценок те же

Источник: составлено автором.

Таблица 7

Коэффициенты парной корреляции набора показателей

Метки	ROE	ROA	INFR	PEOPLE	PARTNERS
ROE	1,000	0,008	0,117	0,078	0,001
ROA	0,008	1,000	0,521	0,357	0,256
INFR	0,117	0,521	1,000	0,706	0,295
PEOPLE	0,078	0,357	0,706	1,000	0,229
PARTNERS	0,001	0,256	0,295	0,229	1,000

Источник: расчеты автора.

Моделирование обозначенной зависимости путем последовательного включения в уравнение множественной регрессии оставшихся факторов (восьми показателей) привело к следующим результатам. Доля общей дисперсии определена на треть (значение скорректированного коэффициента детерминации составило 0,323). Коэффициенты при вошедших в модель регрессорах показывают, что наибольшее влияние на эффективность экономической деятельности компаний оказывает «инфраструктурный» фактор (INFR: 11,497); далее следует сотрудничество с деловыми партнерами (PARTNERS: 1,316). Оба эти показателя, учитывая их ординальный характер, были введены в модель как дискретные числовые переменные. Исходный фактор (IND) в процессе моделирования был преобразован в шесть фиктивных переменных (седьмая, отражающая отраслевое значение «Другие», была исключена во избежание проявления мультиколлинеарности). Единственным из вошедших в уравнение регрессии «отраслевых» факторов стал индикатор принадлежности компании к сфере медицины (Medicine: -1,271). Показатель F-статистики, характеризующий качество модели, составил 140,8. Все коэффициенты при регрессорах значимы при 1%-ом уровне. В целом можно утверждать, что, учитывая все же опосредованное влияние безопасности применения цифровых технологий на экономическую деятельность, модель выполнила свою функцию – четко показала вклад технологий в эффективность процесса экономического производства в размере 32,3%.

Однако настоящий набор данных предоставляет возможность расширить границы анализа, проводимого традиционными статистическими методами, в направлении использования алгоритмов машинного обучения, что вполне приемлемо: «В контексте предсказательного моделирования какова разница между машинным обучением и статистикой? Четкой разграничительной линии, которая разделяет эти две дисциплины, нет. Машинное обучение тяготеет к большему вниманию к разработке эффективных алгоритмов, которые масштабируются до больших данных в целях оптимизации предсказательной модели. Статистика обычно больше сосредоточена на теории вероятностей и опорной структуре модели» [13, с. 252]. В этой связи было решено осуществить построение и обучение модели классификации набора данных, где целевой переменной (выходом, *англ*. output) является принадлежность компании к определенному классу, объединившему ряд видов деятельности, а факторами (предикторами, *англ*. features) – полученные экспертным путем оценки степени готовности компании к киберугрозам. Для формирования таких классов прежде всего из совокупности в силу понятных причин были исключены компании информационно-технологической и телекоммуникационной сферы,

после чего оставшиеся компании были распределены на два класса: «сервисные» (финансы и медицина) и «производственные» (промышленность, строительство, энергетика).

Классифицирование проводилось несколькими широко известными методами: от самого простого в вычислительном отношении «k-ближайших соседей» (K-Nearest Neighbors) и до основанных на алгоритме «Дерево решений» (собственно, сам Decision Tree, а также Random Forest и один из вариантов семейства методов Boosting). В качестве оценки использовалась метрика ROC AUC (Aria Under the Curve), то есть площадь под кривой, характеризующей скорость обучения модели, основанной на том или ином алгоритме классификации: чем больше площадь, тем выше качество обученной модели (результаты представлены на рис. 3).

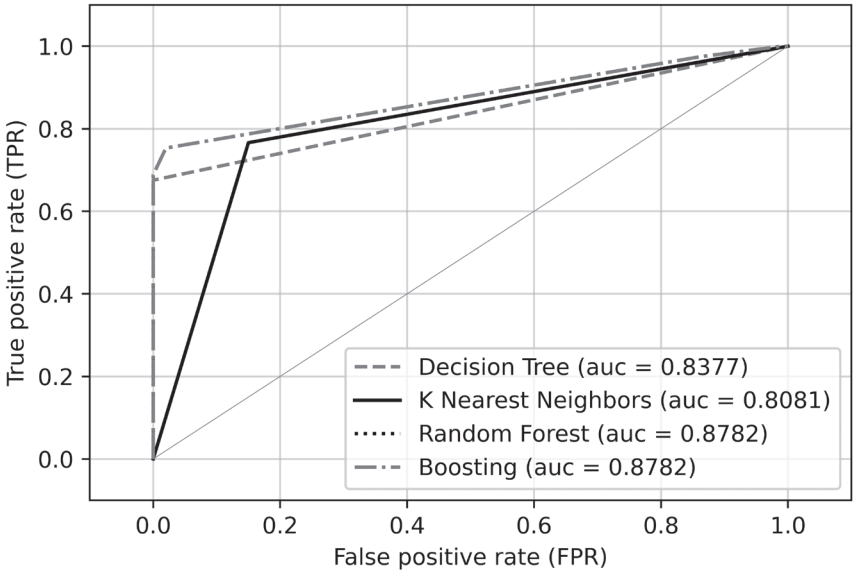

Рис. 3. **Графики ROC выбранного пула классификаторов**

Источник: расчеты автора.

Очевидно, что все три варианта применения деревьев решений начинают процесс классификации одинаково эффективно (их графики буквально сливаются в одну линию), но далее те из них, что используют не одно «дерево», а множество (Random Forest и Boosting), показывают лучший результат. Таким образом, с помощью методов машинного обучения удалось обобщить особенности отраслевой дифференциации компаний по степени их готовности к киберугрозам, что в целом подтверждает ценность сформированной авторами исследования системы показателей.

Заключение

Современные международные методологические разработки способствуют решению задач по количественному измерению процессов безопасности применения цифровых технологий лишь фрагментарно и не формируют целостного представления о структуре и закономерностях развития предметной области. Непрерывный процесс появления все новых информационно-коммуникационных технологий и, следовательно, статистических источников, отражающих применение этих технологий организациями и домашними хозяйствами, повышает уровень важности данной проблематики.

Вместе с тем существующий сегодня международный опыт в области статистического изучения процессов нарушения и защиты информационной безопасности успешно адаптируется к российским реалиям, что явно подтверждается публикациями отечественной статистики. Наличие подобного методологического базиса создает возможность для формирования принципиально новой профильной системы статистических показателей, способной осуществить комплексный охват предмета исследования, используя для этого уже исчисляемые частные и интегральные индикаторы.

Предлагаемый в качестве реализации такой системы подход основан на представлении о процессе безопасности применения цифровых технологий как логической цепи «субъект – мотив – объект – метод – последствия», что позволяет структурировать анализ процессов, проецировать их развитие по направлениям (социальное, экономическое, технологическое) и по масштабу (микро-, мезо-, макроуровни), но потребует корректировки программ проводимых наблюдений.

Практическая ценность изложенного в работе подхода заключается не только в том, что он привнесет новый смысл в собираемую статистику, но также будет полезен при анализе и администрировании процессов нарушения безопасности применения цифровых технологий в масштабе предприятий различных видов экономической деятельности, регионов и страны в целом.

Материалы статьи, в том числе данные и программные скрипты, размещены в репозитории автора по адресу: https://github.com/karyshev63rus/it_security.

Литература

1. **Хочуева Ф.А.** и др. Информационная безопасность сквозь призму цифровой экономики // Современные наукоемкие технологии. 2018. № 11–1. С. 65–71. URL: https://top-technologies.ru/ru/article/view?id=37239.

2. **Schatz D., Bashroush R.** Economic Valuation for Information Security Investment: A Systematic Literature Review // Information Systems Frontiers. 2017. Vol. 19. Iss. 5. P. 1205–1228. doi: https://doi.org/10.1007/s10796-016-9648-8.

3. **Yerina A.M., Honchar I.A., Zaiets S.V.** Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society // Science and Innovation. 2021. Vol. 17. No. 3. P. 3–13. doi: https://doi.org/10.15407/scine17.03.003.

4. **Листопад М.Е., Коротченко С.Е.** Совершенствование методики оценки системы информационной безопасности в России // Национальные интересы: приоритеты и безопасность. 2017. Т. 13. Вып. 6. С. 1162–1175. doi: https://doi.org/10.24891/ni.13.6.1162.

5. **Прокопьев А.В., Прокопьева Т.В.** Теоретические аспекты разработки критериев эффективности национальной политики Российской Федерации в сфере информационной безопасности // Теория и практика общественного развития. 2021. № 12(166). С. 110–120. doi: https://doi.org/10.24158/tipor.2021.12.14.

6. **Bernik I., Prislan K.** Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation // PLoS ONE. 2016. 11(9):e0163050. doi: https://doi.org/10.1371/journal.pone.0163050.

7. OECD. OECD Policy Framework on Digital Security: Cybersecurity for Prosperity. Paris: OECD Publ., 2022. 38 p. doi: https://doi.org/10.1787/a69df866-en.

8. OECD. Measuring Digital Security Risk Management Practices in Business // OECD Digital Economy Papers, No. 283. Paris: OECD Publ., 2019. 63 p. doi: https://doi.org/10.1787/7b93c1f1-en.

9. ITU. Global Cybersecurity Index 2015. Geneva: ITU Publ., 2015. URL: https://www.itu.int/pub/D-STR-SECU-2015.

10. ITU. Global Cybersecurity Index 2020. Geneva: ITU Publ., 2023. URL: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

11. **Зарова Е.В., Проскурина Н.В.** Теоретические основы региональной статистики. Самара: Изд-во СГЭА, 2004. 62 с.

12. **Алетдинова А.А.** Формирование системы статистических показателей инновационного потенциала организации // Экономика, статистика и информатика. Вестник УМО. 2011. № 6(2). С. 78–81.

13. **Брюс П., Брюс Э., Гедек П.** Практическая статистика для специалистов Data Science. СПб.: БВХ-Петербург, 2021. 352 с.

Информация об авторе

Карышев Михаил Юрьевич – д-р экон. наук, доцент, профессор кафедры «Экономика и логистика на транспорте», Институт управления и экономики, Самарский государственный университет путей сообщения. 443066, г. Самара, ул. Свободы, д. 2В. E-mail: m.karishev@samgups.ru. ORCID: https://orcid.org/0000-0001-8648-7742.

References

1. **Khochueva F.A.** et al. Information Security Through the Prism of the Digital Economy. *Modern High Technologies*. 2018;11(part 1):65–71. (In Russ.) Available from: https://top-technologies.ru/ru/article/view?id=37239.

2. **Schatz D., Bashroush R.** Economic Valuation for Information Security Investment: A Systematic Literature Review. *Information Systems Frontiers*. 2017;19(5):1205–1228. Available from: https://doi.org/10.1007/s10796-016-9648-8.

3. **Yerina A.M., Honchar I.A., Zaiets S.V.** Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. *Science and Innovation*. 2021;17(3):3–13. Available from: https://doi.org/10.15407/scine17.03.003.

4. **Listopad M.E., Korotchenko S.E.** Improving the Method for Evaluation of the Information Security System in Russia. *National Interests: Priorities and Security*. 2017;6(13):1162–1175. (In Russ.) Available from: https://doi.org/10.24891/ni.13.6.1162.

5. **Prokopev A.V., Prokopeva T.V.** Theoretical Aspects of the Developing Criteria for the Effectiveness of the Russian National Policy in The Matter of Information Security. *Theory and Practice of Social Development*. 2021; 12(166):110–120. (In Russ.) Available from: https://doi.org/10.24158/tipor.2021.12.14.

6. **Bernik I., Prislan K.** Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation. *PLoS ONE*. 2016;11(9):e0163050. Available from: https://doi.org/10.1371/journal.pone.0163050.

7. OECD. *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity*. Paris: OECD Publ.; 2022. 38 p. Available from: https://doi.org/10.1787/a69df866-en.

8. OECD. Measuring Digital Security Risk Management Practices in Business. *OECD Digital Economy Papers*, No. 283. Paris: OECD Publ.; 2019. 63 p. Available from: https://doi.org/10.1787/7b93c1f1-en.

9. ITU. *Global Cybersecurity Index 2015*. Geneva: ITU Publ.; 2015. Available from: https://www.itu.int/pub/D-STR-SECU-2015.

10. ITU. *Global Cybersecurity Index 2020*. Geneva: ITU Publ.; 2023. Available from: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

11. **Zarova E.V., Proskurina N.V.** *Theoretical Foundations of Regional Statistics*. Samara: SGEA Publ.; 2004. 62 p. (In Russ.)

12. **Aletdinova A.A.** Formation of System of Statistical Factors of Innovation Potential of Organizations. *Economics, Statistics and Informatics. Vestnik UMO*. 2011;6(2):8–81. (In Russ.)

13. **Bruce P., Bruce E., Gedek P.** *Practical Statistics for Data Science Specialists*. St. Petersburg: BVH-Petersburg; 2021. 352 p.

About the author

Mikhail Yu. Karyshev – Dr. Sci. (Econ.), Associate Professor, Professor, Department of Economics and Logistics in Transport, Institute of Management and Economics, Samara State Transport University (SSTU). 2V Svoboda Str., Samara, 443066, Russia. E-mail: m.karishev@samgups.ru. ORCID: https://orcid.org/0000-0001-8648-7742.