УДК 004.056

5.2.2. Математические, статистические и инструментальные методы в экономике

КИБЕРБЕЗОПАСНОСТЬ И СОХРАНЕНИЕ ЦИФРОВОГО СУВЕРЕНИТЕТА ЭКОНОМИКИ

Панина Ульяна Евгеньевна
Ассистент

Цукахина Мария Александровна
Ассистент

Хажоков Мансур Муратович
студент

Арзамасцева Дарина Игоревна
студент

Шепелев Артем Геннадьевич
студент
ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина», Краснодар, Россия

Надежная защита экономических данных от кибератак становится все более важной по мере того, как экономика становится все более цифровой. Учитывая растущую частоту событий и изощренные методы кибератак, мы принимаем во внимание существующие проблемы поддержания кибербезопасности в области защиты экономической информации. Рассматриваются современные достижения в области информационной безопасности, такие как цифровой суверенитет, распределение затрат на защиту информации и влияние политики импортозамещения на рост отечественной ИТ-индустрии. Проанализированы основные опасности, с которыми сталкиваются государственные и бизнес-структуры, а также категории экономически ценных данных, которые наиболее уязвимы для угроз. На основе статистических данных, аналитических исследований и нормативных документов делаются выводы о текущем состоянии кибербезопасности в России и необходимости комплексного подхода к сохранению экономической информации в условиях современных цифровых угроз

Ключевые слова: КИБЕРБЕЗОПАСНОСТЬ, ЭКОНОМИЧЕСКИЕ ДАННЫЕ, ЦИФРОВОЙ СУВЕРЕНИТЕТ, ИНФОРМАЦИОННЫЕ УГРОЗЫ, ИМПОРТОЗАМЕЩЕНИЕ, ИТ-БЕЗОПАСНОСТЬ

http://dx.doi.org/10.21515/1990-4665-211-030

UDC 004.056

5.2.2. Mathematical, statistical and instrumental methods in economics

CYBERSECURITY AND PRESERVING THE DIGITAL SOVEREIGNTY OF THE ECONOMY

Panina Ulyana Evgenievna
assistant

Tsukakhina Maria Alexandrovna
assistant

Khazhokov Mansur Muratovich
student

Arzamasceva Darina Igorevna
student

Shepelev Artem Gennadievich
student
Kuban State Agrarian University named after I. T. Trubilin, Krasnodar, Russia

Reliable protection of economic data from cyber-attacks is becoming increasingly important as the economy becomes more digital. Given the increasing frequency of events and sophisticated methods of cyber-attacks, we take into account the existing challenges of maintaining cybersecurity in the field of economic information protection. The article examines modern achievements in the field of information security, such as digital sovereignty, cost allocation for information protection, and the impact of import substitution policies on the growth of the domestic IT industry. The main dangers faced by government and business structures are analyzed, as well as the categories of economically valuable data that are most vulnerable to threats. Based on statistical data, analytical studies, and regulatory documents, conclusions are drawn about the current state of cybersecurity in Russia and the need for an integrated approach to preserving economic information in the face of modern digital threats

Keywords: CYBERSECURITY, ECONOMIC DATA, DIGITAL SOVEREIGNTY, INFORMATION THREATS, IMPORT SUBSTITUTION, INFORMATION SECURITY

Кибербезопасность и цифровой суверенитет становятся все более важными составляющими как экономической стабильности, так и национальной безопасности по мере того, как мировая экономика стремительно становится цифровой. Цифровые технологии влияют на все аспекты жизни – от государственных услуг и управления важнейшей инфраструктурой до финансовых операций и логистики. Киберугрозы, такие как хакерские атаки на банки и корпорации, кражи персональных данных и нестабильность государственных информационных ресурсов, растут в тандеме с нашей растущей зависимостью от цифровых систем. Например, в 2023 г. каждая вторая организация подверглась хакерской атаке, а глобальный ущерб от киберпреступлений превысил 8 трлн долл.

На экономическую независимость напрямую влияет цифровой суверенитет, который определяется как способность государства управлять своими данными, технологиями и цифровой экосистемой. Устойчивость национальной экономики может быть поставлена под угрозу внешними ограничениями, такими как санкции в области информационных технологий или зависимость от иностранного программного обеспечения. Таким образом, необходимость обеспечения собственной кибербезопасности и импортозамещающих решений усугубилась из-за ограничений на поставки технологий в Российскую Федерацию в 2022-2023 гг.

В связи с растущей зависимостью современной экономики от цифровых технологий кибербезопасность является важнейшим вопросом для поддержания цифрового суверенитета. С ростом числа изощренных кибератак под угрозой находится не только экономическая безопасность отдельных предприятий, но и государства в целом. Учитывая эти обстоятельства, необходим методический подход к защите информационных активов, учитывающий как технологические, так и человеческие факторы.

Структура, представленная на рисунке 1, объединяющая организационные, кадровые и технические элементы, является примером комплексного подхода к кибербезопасности. Такая многоуровневая схема защиты, гарантирующая безопасность данных, непрерывность бизнеса и соответствие нормативным требованиям, создает прочную основу для цифровой экономики.

Рисунок 1 – Структура компонентов системы кибербезопасности с учетом современных угроз и требований [сост. авторами]

Инвестиции в информационную безопасность и жизнеспособность экономики государств в цифровую эпоху тесно связаны, согласно современной экономической теории цифрового суверенитета. Теория «цифрового баланса сил» (Р. Дейберт, 2020) утверждает, что страны с высокими затратами на информационную безопасность создают технологический иммунитет, гарантирующий их конкурентные преимущества на глобальной цифровой арене. Как показывает анализ,

распределение затрат на информационную безопасность по регионам мира имеет явную асимметрию (рис. 2).

Лидируют Европа (23%) и Северная Америка (46%), что свидетельствует об их сильной зависимости от цифровых технологий и знаний о киберугрозах. Китай (8%), Юго-Восточная Азия (4%) и Латинская Америка (5%), которые быстро развиваются, также имеют большие перспективы для роста инвестиций в ближайшие годы. Имея совокупную долю рынка в 2,3%, Россия и СНГ по-прежнему находятся на периферии глобального рынка информационной безопасности, что подчеркивает необходимость продвижения политики защиты цифрового суверенитета в этих странах. Растущие расходы на кибербезопасность превращаются в условие долгосрочного роста экономики в контексте цифровой трансформации.

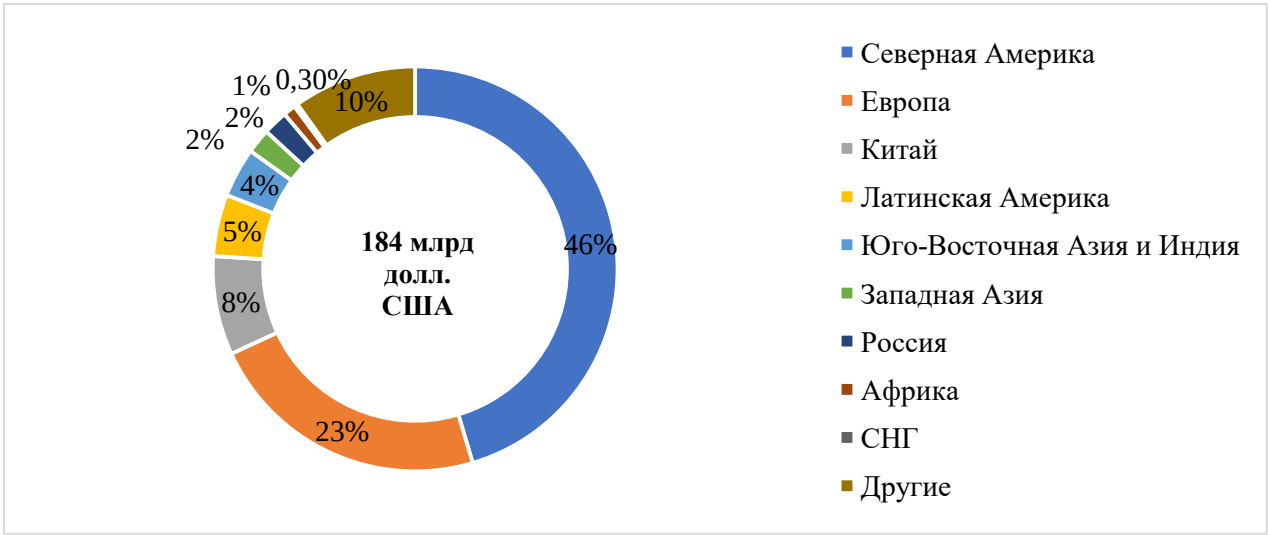

Рисунок 2 – Топ-10 государств по объёмам затрат на ИБ: количественная оценка в контексте глобальных тенденций [2]

В современной цифровой экономике ценность данных, которые становятся как активом, так и слабым местом бизнеса, постоянно возрастает. Информация превращается в стратегический актив, который нуждается в уникальной защите. Как показано на рисунке 3, наиболее

уязвимыми категориями данных в российском сегменте Интернета являются те, которые имеют значительную коммерческую и социальную ценность.

Согласно данным, ценность данных и частота кибератак существенно коррелируют. Из-за их широкого использования во всем, от целевого маркетинга до мошеннических схем, персональные данные стали наиболее распространенным типом событий (30%).Коммерческая тайна (18%) и платежная информация (15%), представляющие особый интерес для организованных киберпреступных группировок, составляют вторую группу риска.

Медицинские данные (12%) и учетные записи (10%), две менее популярные, но не менее значимые категории среди хакеров, требуют особого внимания из-за возможного ущерба, который может быть нанесен в результате их вторжения. Несмотря на весьма скромные показатели взломов, защита данных клиентов (7%) и частной переписки (3%), тем не менее, имеет решающее значение, поскольку их разглашение может нанести серьезный ущерб репутации компании.

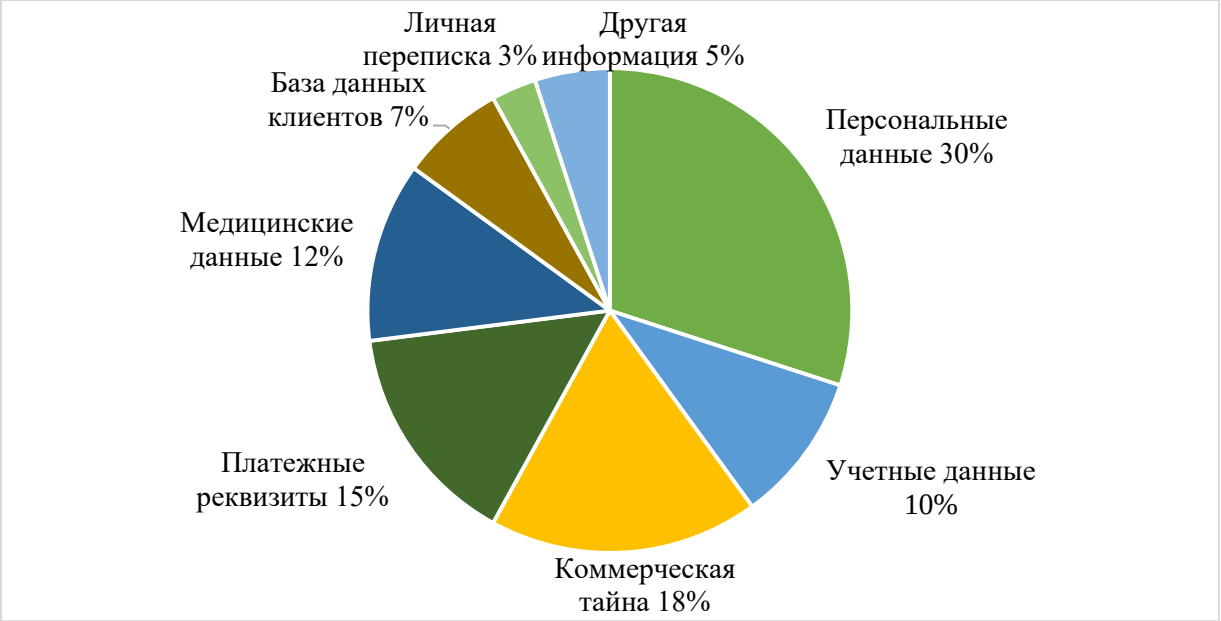

Рисунок 3 – Долевое соотношение категорий данных, подверженных кибератакам, в российском сегменте интернета на 2024 г. [2]

Угрозы информационной безопасности быстро развиваются в современную цифровую эпоху, что требует постоянного мониторинга и анализа меняющейся среды киберрисков. Данные за 2022-2024 гг. показывают заметные изменения в структуре инцидентов информационной безопасности, которые отражают то, как хакеры адаптировались к более строгим мерам безопасности.

Наиболее заметной тенденцией стал резкий рост числа атак вредоносного программного обеспечения, которое всего за три года выросло с 21% до 27%. Этот факт, а также тот факт, что количество инцидентов с проникновением в информационные системы возросло с 2% до 6%, делает очевидным, что хакеры развивают свою тактику от простых методов взлома к сложным многоэтапным операциям.

Доля более традиционных категорий инцидентов, таких как сетевые атаки (-4%), несанкционированный доступ (-8%) и использование уязвимостей (-6%), также снижается. Эта динамика определяется как переориентация захватчиков на более успешную тактику нападения, так и усилением основных мер защиты организаций. Особое внимание следует уделить постоянному росту числа случаев компрометации учетных записей (+1%) и утечек информации (+2%), что подчеркивает сохраняющуюся уязвимость систем аутентификации и необходимость усиления контроля доступа. Тот факт, что в данном случае отсутствует динамика веб-атак, говорит о том, что стратегии защиты сегментов и атаки были сбалансированы.

Таблица 1 – Динамика распределения инцидентов информационной безопасности по типам, % [5]

Тип инцидента	**2022 г.**	**2023 г.**	**2024 г.**	**Изменение, +/-**
Заражение вредоносным ПО	21	23	27	6
Срабатывание сигнатур сенсоров SOC (EDR, NTA, Anti-APT)	14	16	16	2
Эксплуатация уязвимостей	20	17	14	-6
Несанкционированный доступ к ИС и сервисам	19	17	11	-8
Сетевые атаки	12	10	8	-4
Использование нелегитимного ПО	6	7	7	1
Компрометация учетных записей	5	6	6	1
Компрометация информационных систем	2	3	6	4
Утечка информации	1	2	3	2
Веб-атаки	2	2	2	0

В 2022-2024 гг. наблюдался рост числа сложных и высокорискованных инцидентов, которые могут нанести серьезный ущерб кибербезопасности российских организаций. Наиболее серьезные (масштабные) случаи имели устойчивую тенденцию к росту и были связаны с незаконным доступом к информационным системам и сервисам. Такого рода угрозы особенно опасны, поскольку позволяют хакерам не только красть информацию, но и скрытно действовать в бизнес-сетях в течение длительного периода времени, тем самым увеличивая масштаб атаки.

Число случаев несанкционированного доступа к IP-адресам и сервисам выросло на 13 % всего за три года (с 36% до 49%), что свидетельствует о росте числа наиболее вредоносных случаев. Это говорит о том, что хакеры теперь с большей вероятностью используют стратегии скрытого проникновения в сеть, такие как компрометация учетной записи или использование слабых мест в защите периметра.

Одновременно снижение процента заражений вредоносными программами (-12 %) и использования несанкционированного программного обеспечения (-11 %) показывает, насколько хорошо работают методы endpoint protection и контроля лицензионного программного обеспечения. Предприятия должны модифицировать свои системы безопасности, чтобы соответствовать этим растущим опасностям, уделяя особое внимание контролю доступа и мониторингу аномальных действий.

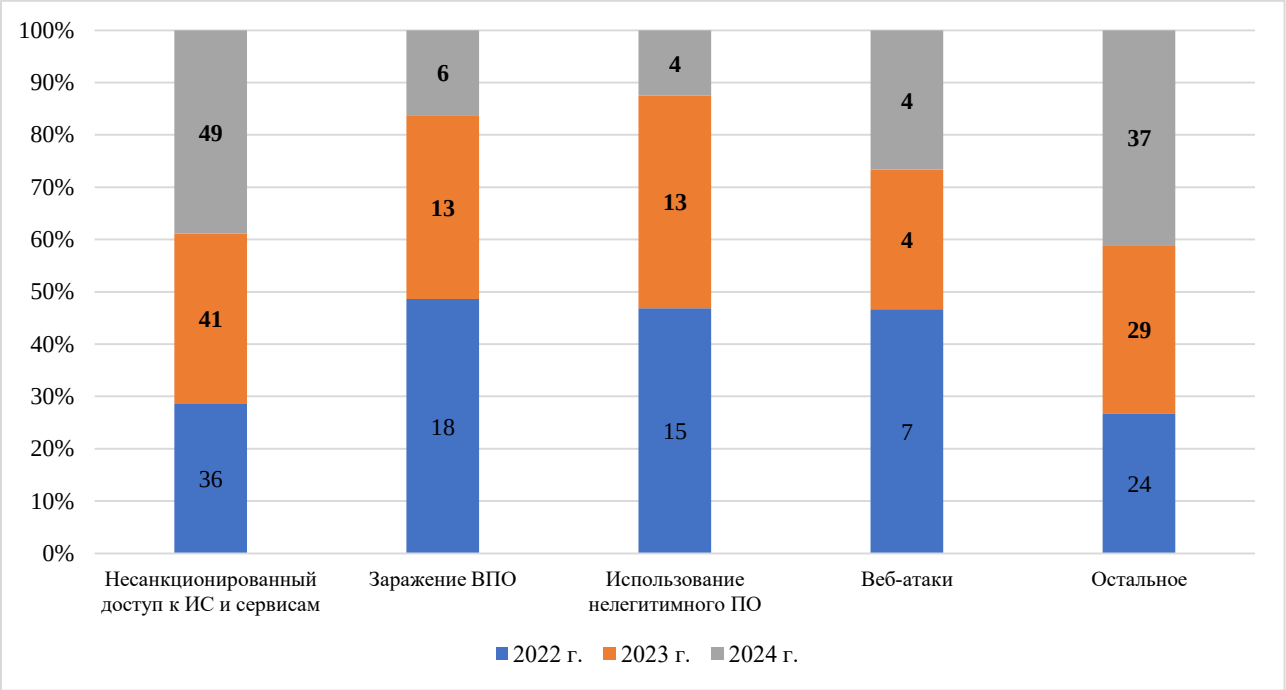

Рисунок 4 – Динамика наиболее критичных (High) киберинцидентов в российских компаниях за 2022-2024 гг. [5]

Анализ динамики российского рынка ИТ в период с 2022 по 2030 гг. является типичной иллюстрацией технических изменений в экономике в связи с импортозамещением. Представленная информация в таблице 2 показывает, как экономика знаний, ориентированная на услуги, сменила парадигму, ориентированную на «железоцентричную». Наиболее примечательным является опережающий рост сегментов информационной

безопасности, что согласуется с идеей «безопасность как основа цифровизации».

Российский ИТ-рынок стабильно меняется, и потенциальные направления быстро вытесняют существующие подразделения (оборудование и ИТ-услуги). Две отрасли с наиболее динамичным ростом – разработка программного обеспечения (+5 %) и облачные технологии (+5 % к 2030 г.) – соответствуют мировым тенденциям цифровизации. В то же время рынок информационной безопасности находится на подъеме, достигнув к 2026 г. 15%-ной доли рынка, что свидетельствует о его зрелости и необходимости дальнейшего технологического прогресса.

Объем рынка вырос почти в три раза, с 1,5 трлн руб. до 4,4 трлн руб. это свидетельствует о критическом значении ИТ-отрасли для российской экономики, но после 2024 г. рынок информационной безопасности развивается медленнее, что потребует переоценки стратегий кибербезопасности, особенно в связи с растущими рисками для облачной инфраструктуры. На необходимость создания гибридных моделей безопасности, сочетающих традиционные и облачные технологии защиты, указывает постоянный спрос на облачные решения (ежегодный рост составляет 0,5-1%). В течение последующих десяти лет эти модели устанавливали новые стандарты в отношении кадровой политики и расходов на ИТ-безопасность.

Таблица 2 – Количественная оценка динамики сегментов ИТ-рынка и ИБ-услуг в РФ: объемы и темпы роста, % [1]

Показатель	Годы								
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Облачная инфраструктура и услуги ЦОД	7	7	8	8	9	10	10	11	12
Информационная безопасность	12	13	14	14	14	15	15	15	15
Программное обеспечение (без ИБ)	18	18	20	21	22	22	22	23	23
ИТ-услуги (без ИБ)	30	28	28	27	26	25	25	23	23
Оборудование инфраструктуры ИТ и ПК	34	33	31	30	29	28	28	27	27
Весь сектор, млрд. руб	1548	1840	2190	2510	2848	3212	3588	3965	4402

Для решения современных проблем информационной безопасности необходимы надежные технологические решения, и российские разработчики играют в этом важную роль. Их решения приобретают все большее значение для защиты государственных учреждений, корпоративного сектора и персональных данных граждан в условиях цифровой трансформации и эскалации киберугроз.

Согласно анализу конкурентной среды, в 2023 г. местные компании будут занимать 57% российского рынка решений для обеспечения информационной безопасности (включая «Лабораторию Касперского», Positive Technologies, Infotex и других российских поставщиков). Однако 10-ная доля иностранных компаний говорит о том, что некоторые отрасли, такие как бизнес-решения или специализированное программное обеспечение, продолжают полагаться на них.

Отрасль по-прежнему фрагментирована; мелкие разработчики составляют 33% рынка, что способствует хорошей конкуренции, но также затрудняет принятие решений покупателями. Учитывая государственную поддержку сектора информационной безопасности и ужесточение правил, регулирующих использование зарубежного программного обеспечения,

можно ожидать, что доля российских поставщиков продолжит расти в ближайшие годы. Тем не менее, создание полных аналогов зарубежных решений в области облачной безопасности, Интернета вещей и промышленных систем по-прежнему будет оставаться основным препятствием.

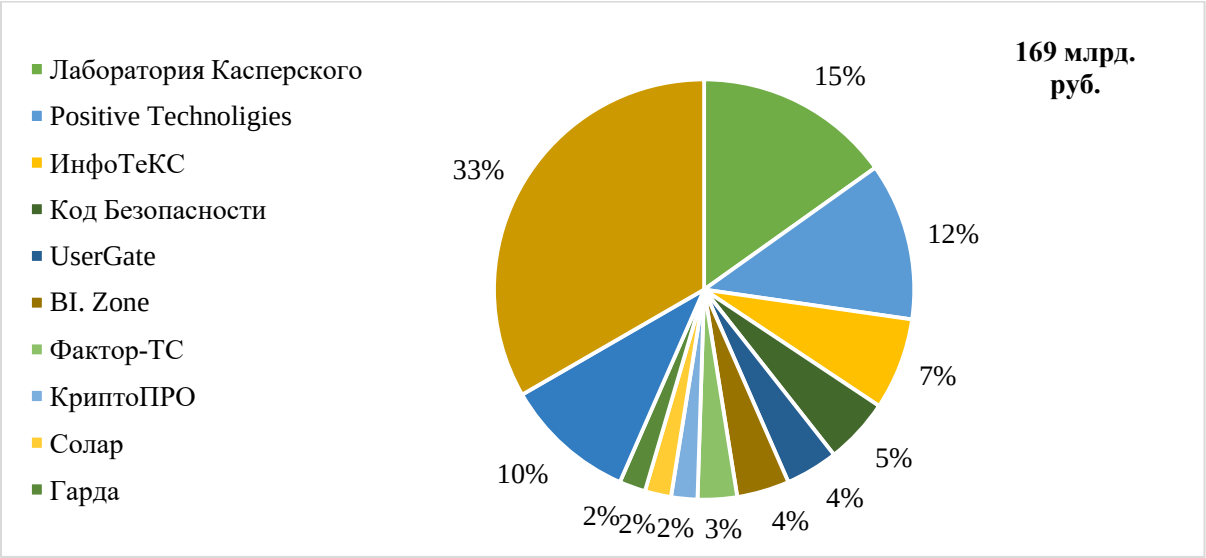

Рисунок 5 – Структура конкурентной среды на рынке разработчиков решений информационной безопасности в РФ (2023 г.): распределение долей игроков [1].

Для обеспечения информационной безопасности организации в условиях цифровой трансформации и роста киберугроз необходима комплексная стратегия, учитывающая организационные, технические и человеческие факторы. Основные области, показанные на рисунке 6, представляют собой основные приоритеты для создания успешной системы киберзащиты на сегодняшний день.

Совершенствование нормативно-правовой базы особенно важно, поскольку невозможно гарантировать соблюдение международных норм и правил без четко определенных стандартов и предписаний. Основой безопасности по-прежнему является техническая защита, но в нынешних

условиях это требует не только установки средств защиты, но и их умелой интеграции в ИТ-инфраструктуру.

В дополнение к предотвращению существующих угроз, такое сочетание действий позволяет компаниям создавать надежную систему безопасности, которая может быть скорректирована в соответствии с новыми требованиями цифровой среды.

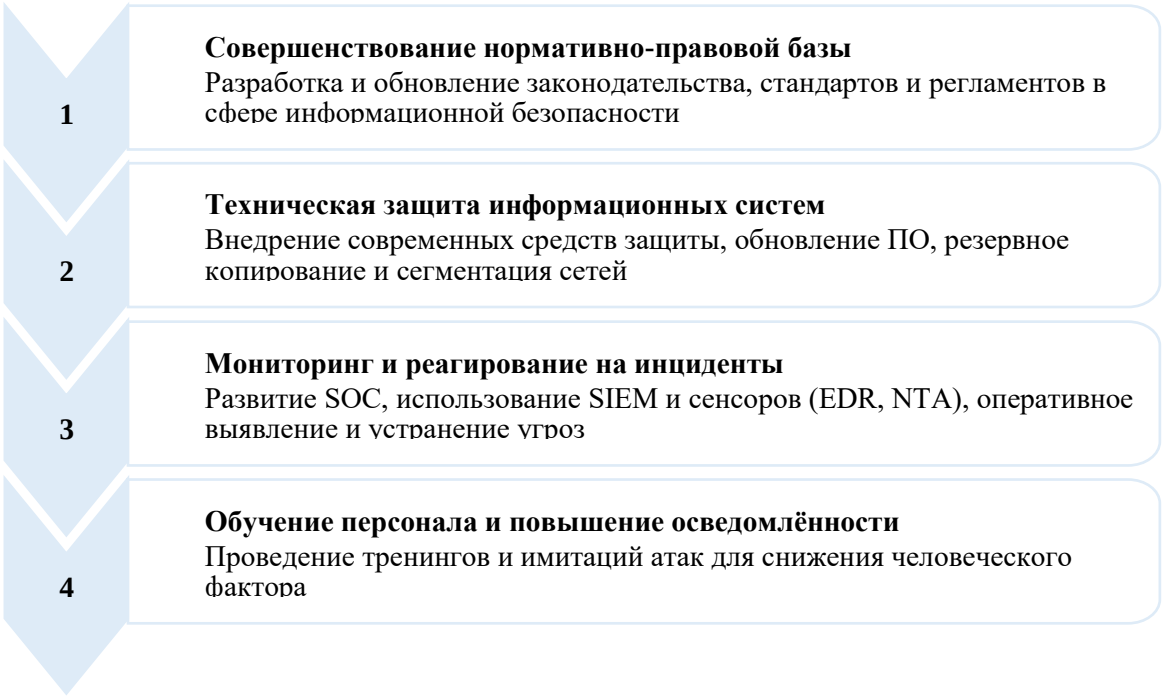

Рисунок 6 – Ключевые направления обеспечения кибербезопасности организации [сост. авторами].

Таким образом по мере того, как мир становится все более подключенным к цифровым технологиям, кибербезопасность и цифровой суверенитет экономики становятся важными составляющими национальной безопасности. Согласно анализу, распространение киберугроз требует комплексной стратегии, сочетающей технологические решения, нормативное регулирование и подготовку кадров. В плане импортозамещения и создания собственных решений в области информационной безопасности российский рынок демонстрирует обнадеживающие тенденции; тем не менее, фрагментация отрасли и продолжающаяся зависимость некоторых сегментов от зарубежных

технологий указывают на необходимость дополнительной консолидации усилий. Последовательный рост облачных технологий и сектора информационной безопасности свидетельствует об их стратегическом значении для цифровой трансформации экономики.

Для поддержания цифрового суверенитета важно продолжать разработку отечественных решений в области кибербезопасности, особенно в области облачных сервисов, Интернета вещей и защиты критически важной инфраструктуры. Одновременно необходимо укреплять нормативно-правовую базу, обучать квалифицированных работников и создавать благоприятные условия для сотрудничества между научным сообществом, промышленностью и правительством. Только при наличии такой многоуровневой стратегии Россия сможет не только противостоять современным киберугрозам, но и занять законное положение в глобальной цифровой экономике, гарантируя долгосрочную технологическую независимость и устойчивый рост.

Список использованных источников

1. B1 Group. Российский рынок информационной безопасности – 2025: Исследование [Электронный ресурс]. – URL: https://b1.ru/local/assets/surveys/russian-information-security-market-survey-2025.pdf (дата обращения: 08.04.2025).

2. Замотайлова, Д. А. Проблемы развития конкуренции в условиях цифровой экономики / Д. А. Замотайлова, Е. В. Попова, Д. Н. Савинская // Мировая экономика XXI века: эпоха биотехнологий и цифровых технологий : Сборник научных статей по итогам работы круглого стола с международным участием, Москва, 15–16 января 2020 года. Том Часть 2. – Москва: Общество с ограниченной ответственностью "КОНВЕРТ", 2020. – С. 67-70. – EDN TVCCHW.

3. Савинская, Д. Н. Предпрогнозный анализ логистических временных рядов на основании показателя Херста / Д. Н. Савинская, Т. А. Недогонова // Современная экономика: проблемы и решения. – 2019. – № 9(117). – С. 18-26. – DOI 10.17308/meps.2019.9/2198. – EDN JEYOHB.

4. Яхонтова, И. М. Планирование мероприятий по экономической безопасности предприятия на этапе моделирования бизнес-процессов / И. М. Яхонтова, Б. М. Бальжанова, Л. К. Дунская // Россия, Европа, Азия: цифровизация глобального пространства : Сборник научных трудов III Международного научно-практического форума, Невинномысск, 16–21 ноября 2020 года / Под редакцией И. В. Пеньковой. – Невинномысск: Общество с ограниченной ответственностью "СЕКВОЙЯ", 2020. – С. 769-771. – EDN CVWRKM.

5. Кибербезопасность как фактор устойчивого развития цифровой экономики / С. Н. Косников, А. Л. Золкин, Н. В. Артемьев, А. Н. Лепшокова // Экономика и управление: проблемы, решения. – 2024. – Т. 15, № 12(153). – С. 221-229.

6. Соляник, В. Ю. Современные методы обеспечения информационной безопасности социальных систем / В. Ю. Соляник, В. В. Осенний, К. А. Ковалева // Цифровизация экономики: направления, методы, инструменты : Сборник материалов III всероссийской научно-практической конференции, Краснодар, 18–23 января 2021 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2021. – С. 63-65.

7. Янбарцева, А. А. Угрозы кибербезопасности для экономики / А. А. Янбарцева, М. Д. Суслов, Д. А. Логинов // Вектор экономики. – 2024. – № 5(95).

References

1. B1 Group. Rossijskij ry`nok informacionnoj bezopasnosti – 2025: Issledovanie [E`lektronny`j resurs]. – URL: https://b1.ru/local/assets/surveys/russian-information-security-market-survey-2025.pdf (data obrashheniya: 08.04.2025).

2. Zamotajlova, D. A. Problemy` razvitiya konkurencii v usloviyax cifrovoj e`konomiki / D. A. Zamotajlova, E. V. Popova, D. N. Savinskaya // Mirovaya e`konomika XXI veka: e`poxa biotexnologij i cifrovy`x texnologij : Sbornik nauchny`x statej po itogam raboty` kruglogo stola s mezhdunarodny`m uchastiem, Moskva, 15–16 yanvarya 2020 goda. Tom Chast` 2. – Moskva: Obshhestvo s ogranichennoj otvetstvennost`yu KONVERT, 2020. – S. 67-70. – EDN TVCCHW.

3. Savinskaya, D. N. Predprognozny`j analiz logisticheskix vremenny`x ryadov na osnovanii pokazatelya Xersta / D. N. Savinskaya, T. A. Nedogonova // Sovremennaya e`konomika: problemy` i resheniya. – 2019. – № 9(117). – S. 18-26. – DOI 10.17308/meps.2019.9/2198. – EDN JEYOHB.

4. Yaxontova, I. M. Planirovanie meropriyatij po e`konomicheskoj bezopasnosti predpriyatiya na e`tape modelirovaniya biznes-processov / I. M. Yaxontova, B. M. Bal`zhanova, L. K. Dunskaya // Rossiya, Evropa, Aziya: cifrovizaciya global`nogo prostranstva : Sbornik nauchny`x trudov III Mezhdunarodnogo nauchno-prakticheskogo foruma, Nevinnomy`ssk, 16–21 noyabrya 2020 goda / Pod redakciej I. V. Pen`kovoj. – Nevinnomy`ssk: Obshhestvo s ogranichennoj otvetstvennost`yu SEKVOJYa, 2020. – S. 769-771. – EDN CVWRKM.

5. Kiberbezopasnost` kak faktor ustojchivogo razvitiya cifrovoj e`konomiki / S. N. Kosnikov, A. L. Zolkin, N. V. Artem`ev, A. N. Lepshokova // E`konomika i upravlenie: problemy`, resheniya. – 2024. – T. 15, № 12(153). – S. 221-229.

6. Solyanik, V. Yu. Sovremenny`e metody` obespecheniya informacionnoj bezopasnosti social`ny`x sistem / V. Yu. Solyanik, V. V. Osennij, K. A. Kovaleva // Cifrovizaciya e`konomiki: napravleniya, metody`, instrumenty` : Sbornik materialov III vserossijskoj nauchno-prakticheskoj konferencii, Krasnodar, 18–23 yanvarya 2021 goda. – Krasnodar: Kubanskij gosudarstvenny`j agrarny`j universitet imeni I.T. Trubilina, 2021. – S. 63-65.

7. Yanbarceva, A. A. Ugrozy` kiberbezopasnosti dlya e`konomiki / A. A. Yanbarceva, M. D. Suslov, D. A. Loginov // Vektor e`konomiki. – 2024. – № 5(95).