Информационное общество: политика и факторы развития

ДОВЕРИЕ И БЕЗОПАСНОСТЬ В ПРОЦЕССАХ ЦИФРОВОГО РАЗВИТИЯ СФЕРЫ ДЕЯТЕЛЬНОСТИ

Катин Александр Владимирович

Институт развития информационного общества, генеральный директор, руководитель дирекции отраслевых программ
РЭУ имени Г. В. Плеханова, старший преподаватель базовой кафедры цифровой экономики ИРИО
Москва, Российская Федерация
alexander.katin@iis.ru

Хохлов Юрий Евгеньевич

Кандидат физико-математических наук, доцент
Академик Российской инженерной академии
Институт развития информационного общества, председатель совета директоров
РЭУ имени Г. В. Плеханова, научный руководитель базовой кафедры цифровой экономики ИРИО
Москва, Российская Федерация
yuri.hohlov@iis.ru

Аннотация

Разработана концептуальная схема и набор показателей для мониторинга и оценки уровня доверия и безопасности при цифровой трансформации сферы деятельности. Концептуальная схема включает оценку доверия и безопасности сферы деятельности в целом, а также уровень доверия и безопасности в организациях сферы деятельности. Концептуальная схема описывается наборами измеримых показателей. Проведена апробация концептуальной схемы на основе статистических данных Росстата за 2022 г. для 12 приоритетных сфер деятельности

Ключевые слова

цифровое развитие; цифровая трансформация; цифровая экономика; цифровые технологии; доверие, информационная безопасность; средства обеспечения информационной безопасности

Введение

Вопросы обеспечения информационной безопасности и доверия при использовании цифровых технологий являются одними из важнейших факторов, влияющих на процессы цифровой трансформации сфер деятельности в целом и организаций в частности. Получение ожидаемых социальных и экономических эффектов возможно только в том случае, когда технологии, решения и услуги, применяемые для цифрового развития безопасны и хорошо защищены, а пользователи им доверяют.

Кроме того, следует отметить, что многие организации, входящие в приоритетные сферы деятельности, обладают и эксплуатируют элементы критической информационной инфраструктуры, защита которых относится к сфере безопасности государства – т. е. к задаче первостепенной важности.

Целью данного исследования является разработка и апробация концептуальной схемы мониторинга и оценки уровня доверия и безопасности как важного фактора, влияющего на цифровое развитие сферы деятельности. Под сферой деятельности понимается отрасль экономики, сектор социальной сферы или система государственного управления, т. е. совокупность организаций, обладающих общностью производимой продукции или оказываемых услуг.

https://doi.org/10.52605/16059921_2024_digital_99-112

Пилотная апробация концептуальной схемы проведена на примере нескольких сфер деятельности, для которых доступны статистические данные для выбранного набора показателей.

Статья состоит из пяти разделов: первый посвящен обзору существующих подходов к оценке уровня доверия и безопасности; второй – описанию разработанной концептуальной схемы мониторинга и оценки уровня доверия и безопасности для отдельно взятой сфере деятельности; третий – описанию перечня предлагаемых показателей, четвертый – описанию методологии сбора данных, пятый – результатам апробации данного подхода.

1 Подходы к оценке доверия и безопасности для цифрового развития сферы деятельности

На сегодняшний день отсутствует общепринятая методология мониторинга и оценки уровня доверия и безопасности в отдельно взятой сфере деятельности. Существующие подходы к такой деятельности в основном направлены на анализ обеспечения информационной безопасности и доверия применительно к использованию цифровых технологий в целом.

В июне 2023 года Всемирным банком была опубликована «Отраслевая модель зрелости кибербезопасности» [1] (далее – модель Всемирного банка), которая направлена на систематизацию информации об отрасли в структурированном виде, что может способствовать лучшему пониманию общих проблем, потребностей и приоритетов сферы деятельности с точки зрения обеспечения информационной безопасности и доверия. Модель Всемирного банка включает в себя три уровня оценки:

- национальный: содержит оценку общегосударственных элементов обеспечения кибербезопасности, которые влияют на зрелость сферы деятельности в области информационной безопасности и доверия из-за их всеобъемлющей роли для обеспечения безопасности страны или отдельных сфер деятельности;
- отраслевой: содержит оценку политик, планов, рекомендаций, стандартов и требований, установленных на уровне сферы деятельности для управления рисками кибербезопасности;
- организационный: содержит оценку деятельности по обеспечению информационной безопасности и доверия ключевых организаций, функционирующих в рамках сферы деятельности.

На каждом из приведенных выше уровней в модели Всемирного банка предлагается проводить анализ по пяти размерностям: система управления кибербезопасностью, система реагирования на риски, мониторинг информационной безопасности и доверия, механизмы наращивания потенциала кибербезопасности и система реагирования на инциденты информационной безопасности.

Менее релевантной, но не менее значимой является деятельность по оценке и сопоставлению уровня развития информационной безопасности в разных странах, осуществляемая в рамках подготовки Глобального индекса кибербезопасности [2] Международного союза электросвязи (далее - Индекс). Данный индекс отражает уровень обеспечения информационной безопасности по странам, при этом оцениваются следующие виды деятельности по обеспечению кибербезопасности:

- правовые меры
- технические меры
- организационные меры;
- меры по развитию потенциала страны в сфере информационной безопасности и доверия;
- меры по организации сотрудничества в этой сфере (международное, межведомственное, межотраслевое).

Индекс публикуется раз в 2 года, в 2020 году Россия заняла 5 место, набрав 98,06 баллов из 100. В 2024 году Россия вошла в группу «продвинутых стран», набрав 92,13 баллов из 100.

Еще одним подходом к мониторингу и оценке уровня обеспечения кибербезопасности является Национальный индекс кибербезопасности [3] Академии электронного управления (далее – Национальный индекс), в котором оценивается готовность стран предотвращать киберугрозы и управлять инцидентами, связанными с информационной безопасностью. В основу концептуальной схемы Национального индекса положены угрозы информационной безопасности, реагировать на

которые обязана каждая страна: недоступность электронных сервисов; нарушение целостности данных и нарушение конфиденциальности данных. Национальный индекс фокусируется на измеримых аспектах деятельности по обеспечению кибербезопасности среди которых:

- действующее законодательство в сфере кибербезопасности;
- наличие организационных структур, ответственных за обеспечение информационной безопасности;
- механизмы сотрудничества в сфере обеспечение кибербезопасности;
- конкретные результаты деятельности: стратегии и политики, технологические решения, планы развития.

По состоянию на 2023 год в Национальном индексе кибербезопасности Россия находится на 30 месте.

Всемирным банком в сотрудничестве с Институтом развития информационного общества в 2017–2018 гг. была разработана методика оценки уровня развития цифровой экономики DECA (Digital Economy Country Assessment), предназначенная для различных стран мира и протестированная в России [4]. Одним из факторов, существенно влияющих на развитие цифровой экономики, оцениваемых в рамках указанной методики, выделено доверие и безопасность. Концептуальная схема предметной области данного фактора в DECA включает следующие аспекты:

- государственная политика и регулирование (включает оценку национальной политики в сфере обеспечения информационной безопасности, а также наличие мероприятий, направленных на повышение осведомленности граждан и организаций по обеспечению информационной безопасности при использовании цифровых технологий);
- организационные меры по обеспечению информационной безопасности (содержит оценку групп реагирования на чрезвычайные ситуации в области информационной безопасности, а также наличия механизмов государственно-частного партнерства и координации вопросов обеспечения информационной безопасности).

Среди имеющихся подходов к мониторингу и оценке информационной безопасности и доверия следует также отметить деятельность Организации по экономическому сотрудничеству и развитию, которая разработала методологию [5] и публикует данные [6] результатов опросов организаций по вопросам использования информационных технологий, включая аспекты, связанные с оценкой уровня информационной безопасности и доверия.

Несмотря на то, что не все описанные подходы напрямую относятся к обеспечению информационной безопасности и доверия в отдельных сферах деятельности, основные аспекты приведенных методологий будут учтены при формировании концептуальной схемы для целей настоящего исследования.

2 Концептуальная схема мониторинга доверия и безопасности для цифрового развития сферы деятельности

С учетом проведенного в разделе 1 анализа подходов, сформирована следующая концептуальная схема оценки доверия и безопасности при цифровой трансформации сферы деятельности (см. рисунок 1).

Концептуальная схема включает в себя два блока:

- оценка уровня обеспечения доверия и безопасности в процессах цифровой трансформации сферы деятельности, т. е. общих элементов организационных и технических мер, разработанных и применяемых для всей сферы деятельности;
- оценка уровня обеспечения доверия и безопасности в процессах цифровой трансформации организаций сферы деятельности, т.е. организационных и технических мер, принимаемых организациями сферы деятельности в рамках собственной деятельности.

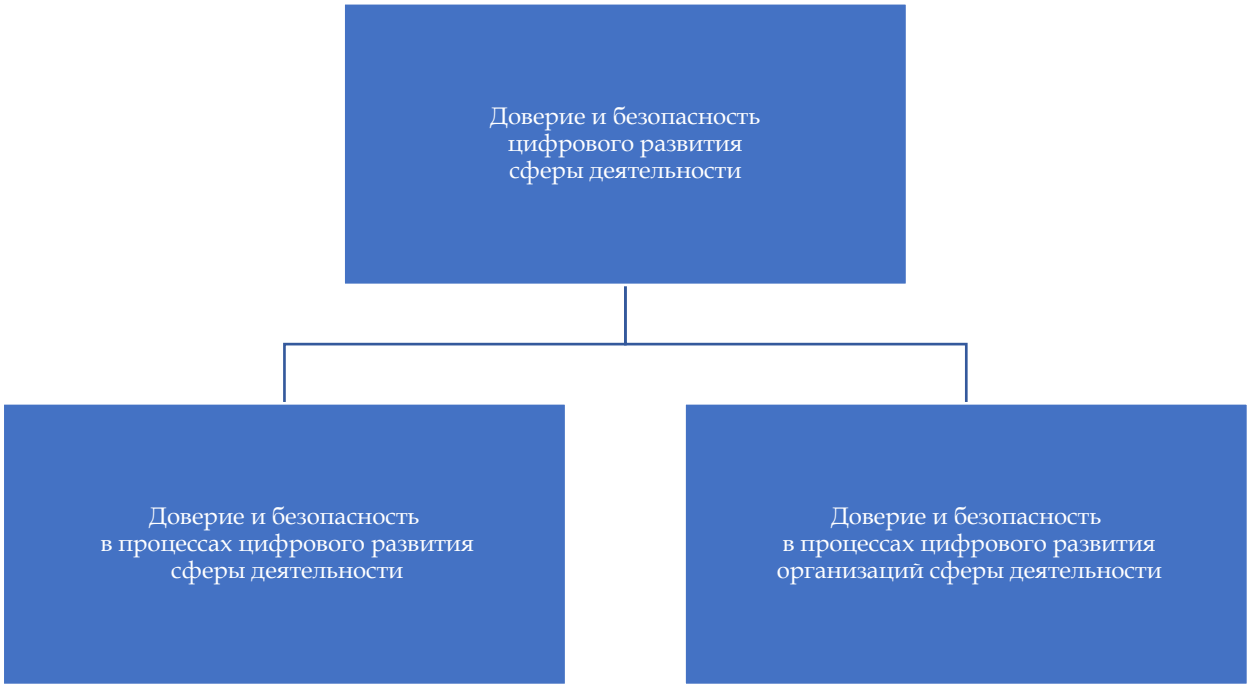

Рисунок 1. Концептуальная схема оценки доверия и безопасности при цифровой трансформации сферы деятельности

Оценка межотраслевых элементов обеспечения доверия и информационной безопасности обладает большой значимостью как для органов власти, отвечающих за обеспечение информационной безопасности в стране или отдельной сфере деятельности, так и компаниям–поставщикам технологий, решений и сервисов в сфере информационной безопасности при определении направлений дальнейшего развития и использования цифровых технологий. Данная оценка также должна включать регуляторные, организационные и технические механизмы, функционирующие на национальном уровне, но оказывающие влияние на состояние информационной безопасности и доверия отдельно взятой сферы деятельности.

Оценка уровня доверия и информационной безопасности в процессах цифрового развития в отдельных организациях сферы деятельности необходима, поскольку цифровые технологии, решения и сервисы все глубже проникают в разнообразные деловые процессы. Угрозы информационной безопасности, связанные с потерей или несанкционированным раскрытием данных организации влекут серьезные риски, поскольку с одной стороны способны привезти к финансовым и репутационным потерям, а с другой – свести к нулю ожидаемые эффекты от цифрового развития.

3 Показатели мониторинга и оценки доверия и безопасности для цифрового развития сферы деятельности

3.1 Обеспечение доверия и безопасности в процессах цифрового развития сферы деятельности

Для мониторинга и оценки уровня доверия и безопасности в процессах цифрового развития сферы деятельности в целом был сформирован перечень показателей, позволяющих оценить принимаемые на уровне сферы деятельности усилия в разрезе организационных, регуляторных и технических мер обеспечения доверия и безопасности.

1. *Политика обеспечения доверия и безопасности в процессах цифровой трансформации сферы деятельности.*

Данный показатель позволяет оценить уровень развития организационных мер обеспечения доверия и безопасности в процессах цифровой трансформации сферы деятельности, а также сопоставить их между собой. Для расчета значения показателя осуществляется поиск одного или нескольких документов, принятых для всей рассматриваемой сферы деятельности, определяющих

комплекс организационных мер, которые, в случае их наличия, должны проверяться на соответствие следующим характеристикам:

- в документах определено текущее и целевое состояние уровня доверия и безопасности в процессах цифровой трансформации сферы деятельности;
- в документах определены цели, задачи и показатели обеспечения доверия и безопасности в процессах цифровой трансформации сферы деятельности;
- в документах зафиксирована система управления их реализацией, явно выявлены заинтересованные стороны, их права и обязанности;
- в документах учтена специфика сферы деятельности (особенности организации деловых процессов, специализированные угрозы, дополнительные регуляторные требования, значимость сферы деятельности для экономики, государственной и общественной безопасности, включая наличие элементов критической информационной инфраструктуры);
- в самих документах, либо во их исполнение, утверждён план реализации (содержащий сроки исполнения, ответственных, объемы финансирования).

Оценка показателя осуществляется по пятибалльной школе с помощью опроса профильных экспертов

2. *Уровень нормативного правового регулирования обеспечения доверия и безопасности в процессах цифровой трансформации сферы деятельности*.

Показатель позволяет оценить уровень нормативного правового обеспечения доверия и безопасности в процессах цифровой трансформации сферы деятельности. Высокие значения данного показателя позволяют говорить о благоприятной обстановке для цифрового развития сферы деятельности.

Под нормативным правовым регулированием понимается установление общеобязательных правовых норм, которые призваны упорядочить общественные отношения, возникающие между гражданами, юридическими лицами и органами власти.

В данном случае требуется установить факт наличия нормативного правового регулирования обеспечения доверия и безопасности в процессах цифровой трансформации сферы деятельности, а также оценить его полноту, качество и актуальность. Для расчета показателя должен проводиться опрос профильных экспертов, которым предлагается оценить по отдельности полноту, качество и актуальность нормативного правового регулирования вопросов обеспечения доверия и безопасности взаимоотношений, возникающих в процессах цифровой трансформации сферы деятельности.

3. *Уровень нормативного технического регулирования обеспечения доверия и безопасности в процессах цифровой трансформации сферы деятельности*

Данный показатель позволяет оценить уровень стандартизации при обеспечении доверия и безопасности в процессах цифровой трансформации сферы деятельности. Высокие оценки позволяют говорить о зрелом состоянии системы нормативного технического регулирования процессов цифрового развития в соответствующей сфере.

В данном случае требуется установить наличие национальных стандартов для характеристики процессов обеспечения доверия и безопасности при цифровом развитии сферы деятельности, а также оценить полноту, качество и актуальность регулирования посредством опроса профильных экспертов.

4. *Уровень реагирования на компьютерные инциденты при цифровой трансформации сферы деятельности*.

Этот показатель характеризует уровень технических мер обеспечения безопасности и доверия в процессах цифровой трансформации сферы деятельности через наличие и уровень спецификации центра(ов) мониторинга, информирования и реагирования на угрозы и компьютерные инциденты в отдельной сфере деятельности (SOC, CERT, CIRT).

По аналогии с определением [7], под центром мониторинга, информирования и реагирования на компьютерные инциденты в сфере деятельности понимается постоянно действующая организационная структура, в задачи которой входит отслеживание и реагирование на угрозы и инциденты информационной безопасности на уровне всей сферы деятельности.

Расчет значений данного показателя связан с экспертной оценкой наличия и эффективности функционирования соответствующих центров мониторинга, информирования и реагирования на угрозы и компьютерные инциденты в отдельной сфере деятельности.

3.2 Обеспечение доверия и безопасности в процессах цифрового развития организаций сферы деятельности

Для мониторинга уровня обеспечения доверия и безопасности в процессах цифрового развития на уровне отдельных организаций сферы деятельности сформирован комплекс показателей для оценки реализуемых организационных мер (например, наличие соответствующих политик и ответственных исполнителей), а также технических мер (таких как применение базовых и инновационных инструментов обеспечения информационной безопасности). Кроме того, представляется критически важным оценить уровень зависимости организаций от иностранного оборудования и программного обеспечения в области доверия и безопасности. Высокий уровень использования отечественных решений является залогом успешной реализации политики в области достижения цифрового суверенитета. С другой стороны, зависимость от иностранных программных продуктов и оборудования может порождать дополнительные риски.

5. *Доля организаций сферы деятельности, имеющих политику обеспечения доверия и безопасности.*

Данный показатель позволяет оценить наличие организационных мер обеспечения доверия и безопасности в отдельных организациях сферы деятельности.

Под организационными мерами обеспечения доверия и безопасности будет пониматься наличие в организациях сферы деятельности политики обеспечения доверия и безопасности, зафиксированной в действующем регламентном документе (например, в документе, регламентирующем обеспечение информационной безопасности в организации). Под политикой (обеспечения) информационной безопасности понимается формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности [8, п. 3.2.18].

6. *Доля организаций сферы деятельности, имеющих структурное подразделение, ответственного за обеспечение доверия и безопасности*

Этот показатель позволяет оценить уровень зрелости организационных мер по обеспечению доверия и безопасности в организациях сферы деятельности. В частности, под структурным подразделением, ответственным за обеспечение информационной безопасности в организации понимается организационно-техническая структура организации, реализующая решение определенной задачи, направленной на противодействие угрозам информационной безопасности организации [8, п. 3.4.5].

7. *Доля организаций сферы деятельности, применяющих основные меры обеспечения доверия и безопасности*

Показатель необходим для оценки уровня наличия и использования технических мер обеспечения доверия и безопасности в организациях сферы деятельности. Применительно к обеспечению информационной безопасности под техническими мерами понимается совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности [8, п. 3.6.3].

Для расчета значения данного показателя во внимание принимаются используемые в организациях такие средства и действия как биометрические средства аутентификации пользователей, программные средства автоматизации процессов анализа и контроля защищенности компьютерных систем, программные/ аппаратные средства, препятствующие несанкционированному доступу вредоносных программ, регулярно обновляемые антивирусные программы, резервное копирование данных на носители, находящиеся физически не на территории организации, системы обнаружения вторжения в компьютер или сеть, спам – фильтр, средства строгой аутентификации, средства шифрования, средства электронной подписи, технические средства аутентификации пользователей.

8. *Доля организаций сферы деятельности, использующих технологии сбора, обработки и анализа больших данных преимущественно для обеспечения доверия и безопасности*

9. *Доля организаций сферы деятельности, использующих технологии искусственного интеллекта преимущественно для обеспечения доверия и безопасности*

Данные показатели позволяют оценить, насколько часто организации используют продвинутые технологические решения (основанные на технологиях работы с большими данными или искусственного интеллекта). В силу усложнения процессов цифрового развития появляется все больше угроз, с которыми сложно справляться традиционными средствами обеспечения информационной безопасности, поэтому важно понимать, какова доля организаций сферы деятельности, имеющих компетенции и возможности внедрять и использовать новейшие инструменты обеспечения кибербезопасности.

10. *Доля организаций сферы деятельности, столкнувшихся с проблемами, связанными с компьютерными инцидентами.*

Большое количество компьютерных инцидентов может влиять на уровень доверия к цифровым технологиям, а также сигнализировать о недостаточном уровне развития организационных и технических мер, принимаемых организацией для обеспечения доверия и безопасности в процессах цифровой трансформации.

Компьютерные инциденты могут приводить к прекращению эксплуатации информационных систем, к уничтожению или повреждению данных, к утечке конфиденциальных данных и т. д.

11. *Доля затрат на продукты и услуги в области доверия и безопасности в общих затратах организаций сферы деятельности на цифровые технологии.*

Показатель рассчитывается как доля совокупных затрат всех организаций сферы деятельности на доверие и безопасность в общем бюджете на цифровые технологии рассматриваемой сферы деятельности. Показатель позволяет оценить, насколько приоритетной для организаций сферы деятельности является обеспечение доверия и безопасности. По данным исследования опыта российских компаний [9], в среднем доля расходов только на информационную безопасность составляет 15% от общего бюджета на ИТ. Чем ближе значение доли затрат к этой цифре, тем более ответственно организации исследуемой сферы деятельности подходят к обеспечению информационной безопасности.

12. *Доля организаций сферы деятельности, использовавших российское программное обеспечение для обеспечения доверия и безопасности.*

Данный показатель позволяет оценить уровень использования в организациях сферы деятельности отечественного программного обеспечения в области доверия и безопасности. Чем выше значение показателя, тем ниже зависимость от импортных программных продуктов.

Под российским программным обеспечением понимается программное обеспечение, произведенное отечественными (российскими) производителями программного обеспечения (ПО), которыми могут быть признаны российские юридические лица, в которых не менее чем 51% долей в уставном капитале или акций, производных инструментов и других инструментов корпоративного контроля принадлежат прямо или косвенно российским гражданам или государственным образованиям, а также физическим лицам, являющимся гражданами и налоговыми резидентами РФ [10].

13. *Доля организаций сферы деятельности, использовавших российское оборудование для обеспечения доверия и безопасности.*

Показатель позволяет оценить уровень использования отечественного (цифрового) оборудования для обеспечения доверия и безопасности (межсетевые экраны, анализаторы спектра, устройства для идентификации, поисковое оборудование и т. п.) в организациях сферы деятельности. Чем выше значение показателя, тем ниже зависимость российских организаций от импортного оборудования.

Под оборудованием отечественного производства понимается [11] оборудование, имеющее сертификаты или декларации соответствия, произведенное российскими организациями, которыми могут быть признаны российские юридические лица, в которых не менее чем 51% долей в уставном капитале или акций, производных инструментов и других инструментов корпоративного контроля принадлежат прямо или косвенно российским гражданам или государственным образованиям, а также физическим лицам, являющимся гражданами и налоговыми резидентами РФ, которые обеспечивают полный цикл тестового и сервисного сопровождения.

4 Методология построения комплексного индекса доверия и безопасности как фактора цифрового развития сферы деятельности

Для интегральной оценки доверия и безопасности для цифрового развития сферы деятельности была разработана методология расчета комплексного индекса на основе показателей из раздела 3.

Для подсчета комплексного индекса и его составляющих значения всех используемых показателей нормализуются (переводятся в безразмерную величину в интервале от 0 до 1). В качестве процедуры нормализации используется расчет расстояния значения показателя до эталонной меры. Указанная процедура основана на расчете (путем деления) отношения текущего значения показателя сферы деятельности к нормализующему (эталонному) значению:

$$P_j^i = \Pi_j^i / \mathrm{H}_j, \quad (1)$$

где

P_j^i – нормализованное значение *j*-го показателя *i*-ой сферы деятельности,

Π_j^i – текущее исходное значение *j*-го показателя *i*-ой сферы деятельности,

H_j – нормализующее значение для *j*-го показателя (например, максимальное количество баллов или 100% для соответствующих показателей).

Нормализующие значения выбираются близкими к максимальным. В случае сильного разброса значения показателя, превышающего два стандартных отклонения от среднего, максимальное и нормализующее значение ограничиваются двумя стандартными отклонениями от среднего.

Комплексный индекс рассчитывается как среднее арифметическое индексов-компонентов (подындексов) «Доверие и безопасность в процессах цифрового развития сферы деятельности» и «Доверие и безопасность в процессах цифрового развития организаций сферы деятельности».

Подындексы в свою очередь рассчитываются как среднее арифметическое, входящих в них показателей (см. выше концептуальную схему и показатели).

5 Пилотная апробация

В 2023 году была проведена пилотная апробация разработанного подхода к мониторингу и оценке доверия и безопасности для цифрового развития отдельной сферы деятельности. Комплексный индекс для оценки доверия и безопасности, как фактора цифрового развития различных сфер деятельности, рассчитывался по данным 2022 г. доступным из результатов федерального статистического наблюдения по форме №3-информ [12]. В перечень использованных в пилотной апробации показателей вошли: оценка уровня использования организациями сфер деятельности программных средств обеспечения информационной безопасности, как в целом, так и только отечественных (показатели № 7 и 12), а также уровень затрат на доверия и безопасность организаций сфер деятельности (показатель №11).

Расчет значений остальных показателей, приведенных в разделе 3 невозможен без проведения опроса организаций и профильных экспертов.

Как и в других направлениях мониторинга цифрового развития, расчет показателей проводился для следующих приоритетных сфер деятельности (в скобках – соответствующие разделы и коды ОКВЭД2):

1. сельское хозяйство (a);
2. добыча полезных ископаемых (b);
3. обрабатывающая промышленность (c);
4. коммунальная инфраструктура и электроэнергетика (d и e);
5. строительство (f);
6. торговля (g);
7. транспорт и логистика (h);
8. финансовые услуги (k);
9. наука (72);
10. высшее образование (85.22);
11. здравоохранение (86);
12. государственное и муниципальное управление (84.11.1, 84.11.2 и 84.11.3).

Полученные результаты в виде рейтинга сфер деятельности представлены на рис. 2.

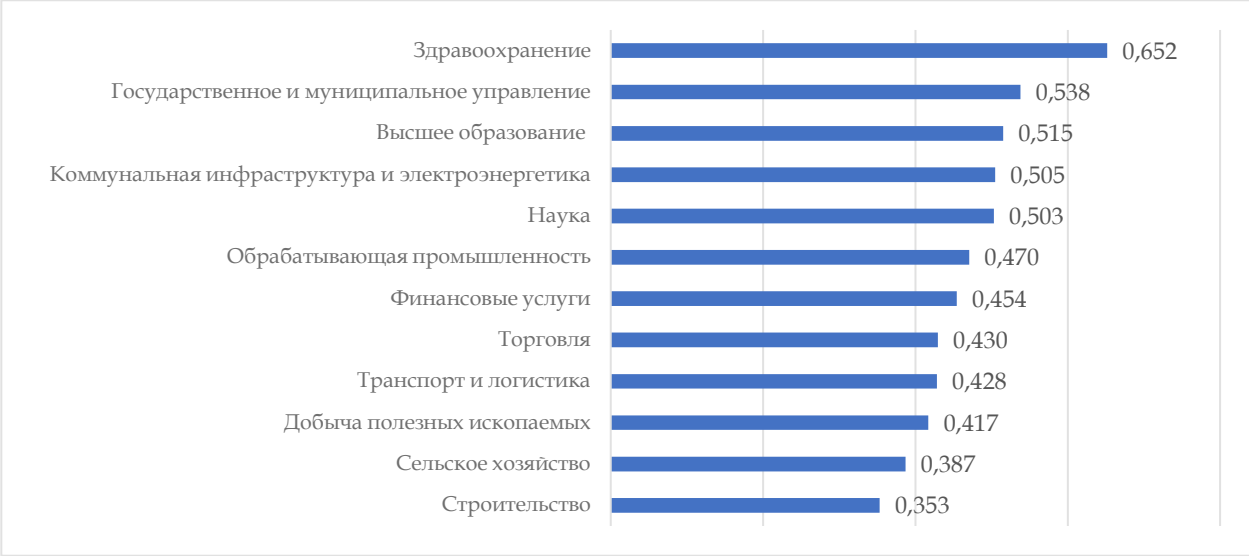

Рисунок 2. Рейтинг отдельных сфер деятельности по комплексному индексу доверия и безопасности для цифрового развития, 2022 г.

В рейтинге лидирует сфера здравоохранения, что логично, поскольку данная сфера деятельности оперирует значительными объемами строго охраняемой информации, содержащей медицинские данные пациентов. Среди лидеров находятся государственное и муниципальное управление, а также высшее образование. Организации этих сфер деятельности также обрабатывают значительные объемы персональных данных пользователей, хранят и обмениваются сведениями, включающими государственную тайну и данные для служебного пользования. Их деятельность строго регулируется нормативными актами, что вынуждает их тратить значительные ресурсы для обеспечения информационной безопасности. Среди явно отстающих можно отметить строительство и сельское хозяйство. Организации из этих сфер деятельности меньше используют цифровые технологии, и как следствие, меньше вкладываются в обеспечение информационной безопасности. К тому же объемы строго охраняемых данных в этих организациях существенно ниже, чем, например, в сфере здравоохранения. Более детально причины и составляющие лидерства можно проанализировать на основе расчетов отдельных составляющих комплексного индекса, представленных ниже (рис. 3–5).

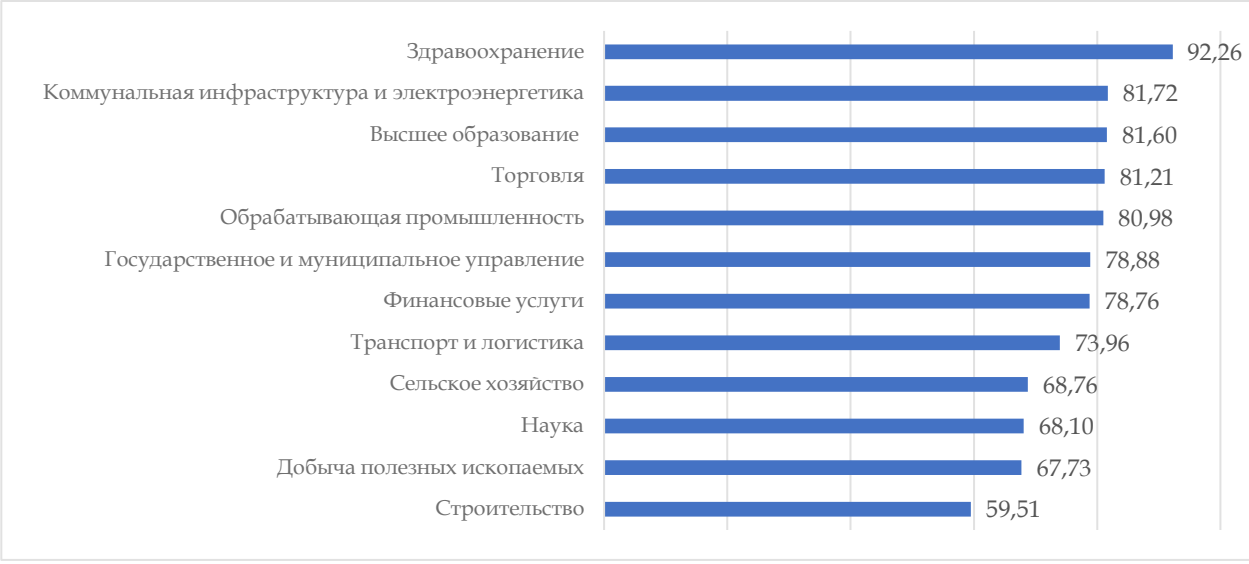

Рисунок 3. Доля организаций, использовавших средства обеспечения информационной безопасности, 2022 г.

На рис. 3 представлен расчет уровня использования организациями средств обеспечения информационной безопасности в разрезе по сферам деятельности. Абсолютным лидером по данному показателю выступает сфера здравоохранения. Среди отстающих можно отметить добычу полезных ископаемых и строительство.

На рисунке 4 представлен результат оценки уровня использования отечественных средств обеспечения информационной безопасности в рассматриваемых сферах деятельности. В тройку лидеров вошли сферы здравоохранения, высшего образования, а также коммунальной инфраструктуры и электроэнергетики, что говорит о значительных усилиях организаций данных сферы деятельности в области импортозамещения. В целом же ситуация по данному показателю далека от идеала. Зависимость от иностранных программных продуктов в области информационной безопасности все еще велика.

Рисунок 4. Доля организаций, использовавших отечественные средства обеспечения информационной безопасности, 2022 г.

На рисунке 5 представлен расчет доли затрат на информационную безопасность в общих затратах на цифровое развитие всех организаций исследуемых сфер деятельности.

Рисунок 5. Доля затрат на информационную безопасность в общих затратах на цифровые технологии в организациях, 2022 г.

Лидерами по данному показателю являются сферы государственного и муниципального управления, науки, а также здравоохранения. Отстающими по данному показателю являются высшее образование и сельское хозяйство. Как видно из результатов федерального статистического наблюдения [13], даже лидер – государственное и муниципальное управление, значительно отстает по уровню затрат на информационную безопасность от эталонного значения в 15%. Это может свидетельствовать о недостаточной приоритетности данной деятельности, что уже сегодня порождает значительные риски как для организаций приоритетных сфер деятельности, так и для потребителей их услуг и сервисов.

Заключение

Доверие и безопасность – существенный фактор, влияющий на цифровой развитие сферы деятельности. Без должного ответственного подхода к обеспечению доверия и безопасности цифровое развитие сферы деятельности будет крайне затруднено, поскольку низкий уровень доверия пользователей к цифровым технологиям и сервисам, применяемым в сфере деятельности будет приводить к потерянным инвестициям вследствие отказа от предлагаемых сервисов, а неадекватно принимаемые меры по обеспечению защиты информации и данных, прежде всего пользовательских и коммерчески значимых – неотвратимо приведет в финансовым и репутационным потерям в организациях сфер деятельности.

Разработанная концептуальная схема содержит показатели, позволяющие оценить уровень обеспечения доверия и безопасности на уровне всеq сферы деятельности, а также меры, принимаемые организациями сферы деятельности. Унифицированный набор показателей также позволяется сравнивать отдельные сферы деятельности между собой, выявлять лидеров, у которых можно перенять лучшие практики.

Пилотная апробация предложенного подхода продемонстрировала его применимость, однако для полноценного использования разработанного инструментария требуется проводить дополнительные опросы организаций и экспертов, поскольку имеющихся данных федерального статистического наблюдения явно недостаточно. Включение в расчет всех предложенных концептуальной схемой показателей может в значительной степени расширить понимание ситуации с уровнем доверия и безопасности в стране и разрабатывать более целенаправленную политику по обеспечению высокого уровня доверия и безопасности для каждой из рассмотренных сфер деятельности.

Благодарности

В работе использованы результаты научно-методической работы по обеспечению реализации задач по созданию и функционированию механизма формирования условий для цифровой трансформации отраслей экономики и секторов социальной сферы через акселерацию цифровых платформ, а также прикладного экономического исследования «Исследование путей и механизмов стратегической координации процессов цифровой трансформации отраслей экономики, социальной сферы и государственного управления» выполненных в 2022-2023 гг. сотрудниками Всероссийской академии внешней торговли Министерства экономического развития Российской Федерации совместно с экспертами Института развития информационного общества.

Литература

1. Sectoral cybersecurity maturity model – version 1.0 – June 2023 (public consultation draft) URL: https://documents1.worldbank.org/curated/en/099062623085028392/pdf/P172637 07c36b702309f7303dbb7266e1cf.pdf (дата обращения 13.12.2024)
2. Global Cybersecurity Index. URL: https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx (дата обращения 13.12.2024)
3. Национальный индекс кибербезопасности. URL: https://ega.ee/ru/success_story/national-cyber-security-index/ (дата обращения 13.12.2024)
4. Анализ текущего состояния развития цифровой экономики в России. М.: Институт развития информационного общества, 2018. – 166 с. URL: http://iis.ru/wp-content/uploads/2020/12/DECARussia2018rus.pdf (дата обращения 13.12.2024)

5. The OECD Model Survey on ICT Usage by Businesses 2nd Revision URL: https://web-archive.oecd.org/2015-10-26/376630-ICT-Model-Survey-Usage-Businesses.pdf (дата обращения 13.12.2024)
6. ICT Access and Usage by Businesses. URL: https://data-explorer.oecd.org/vis?lc=en&df[ds]=dsDisseminateFinalDMZ&df[id]=DSD_ICT_B%40DF_BUSINESSES&df[ag]=OECD.STI.DEP&df[vs]=1.0&av=true&pd=2012%2C&dq=.A.B1_B.._T.S_GE100%2BS_GE10&to[TIME_PERIOD]=false&vw=tb (дата обращения 13.12.2024)
7. ГОСТ Р ИСО/МЭК ТО 18044–2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности
8. ГОСТ Р 53114-2008 Группа Т00. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения
9. Безопасность в облаках и не только: исследование-прогноз для CISO на 2024 год. URL: https://yandex.cloud/ru/blog/posts/2024/03/information-security-research (дата обращения 13.12.2024)
10. Постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»
11. Постановление Правительства РФ от 10 июля 2019 г. № 878 "О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, о внесении изменений в постановление Правительства Российской Федерации от 16 сентября 2016 г. N 925 и признании утратившими силу некоторых актов Правительства Российской Федерации"
12. Сведения об использовании цифровых технологий и производстве связанных с ними товаров и услуг (итоги статнаблюдения по ф. № 3-информ) URL: https://rosstat.gov.ru/storage/mediabank/3-inf_2022.rar (дата обращения 13.12.2024)

TRUST AND SECURITY IN SECTORAL DIGITAL DEVELOPMENT

Katin, Alexander Vladimirovich

Institute of the Information Society, CEO, head of Directorate of sectoral programs
Plekhanov Russian University of Economics, IIS-based Digital economy department, senior lecturer
Moscow, Russian Federation
alexander.katin@iis.ru

Hohlov, Yuri Eugenyevich

Candidate of physical and mathematical sciences, associate professor
Full member of the Russian Engineering Academy
Institute of the Information Society, chairman of the Board of directors
Plekhanov Russian University of Economics, IIS-Based Digital Economy Department, scientific advisor
Moscow, Russian Federation
yuri.hohlov@iis.ru

Abstract

A conceptual framework and a set of indicators have been created for monitoring and evaluation of trust and security during sectoral digital development. The conceptual framework includes an assessment of trust and security in sectoral digital development, as well as the level of trust and security in organizations. The conceptual framework is described by sets of measurable indicators. The conceptual framework was tested based on Rosstat statistical data in 2022 for 12 priority sectors.

Keywords

digital development; digital transformation; digital economy; digital technologies; trust, information security; information security tools

References

1. Sectoral cybersecurity maturity model – version 1.0 – June 2023 (public consultation draft) URL: https://documents1.worldbank.org/curated/en/099062623085028392/pdf/P172637 07c36b702309f7303dbb7266e1cf.pdf (date accessed 13.12.2024)
2. Global Cybersecurity Index. URL: https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx (data obrashheniya 13.12.2024)
3. Naczional`ny`j indeks kiberbezopasnosti. URL: https://ega.ee/ru/success_story/national-cyber-security-index/(date accessed 13.12.2024)
4. Analiz tekushhego sostoyaniya razvitiya czifrovoj e`konomiki v Rossii. M.: Institut razvitiya informaczionnogo obshhestva, 2018. – 166 s. URL: http://iis.ru/wp-content/uploads/2020/12/DECARussia2018rus.pdf (data obrashheniya 13.12.2024)
5. The OECD Model Survey on ICT Usage by Businesses 2nd Revision URL: https://web-archive.oecd.org/2015-10-26/376630-ICT-Model-Survey-Usage-Businesses.pdf (date accessed 13.12.2024)
6. ICT Access and Usage by Businesses. URL: https://data-explorer.oecd.org/vis?lc=en&df[ds]=dsDisseminateFinalDMZ&df[id]=DSD_ICT_B%40DF_BUSINESSES&df[ag]=OECD.STI.DEP&df[vs]=1.0&av=true&pd=2012%2C&dq=.A.B1_B.._T.S_GE100%2BS_GE10&to[TIME_PERIOD]=false&vw=tb (date accessed 13.12.2024)
7. GOST R ISO/ME`K TO 18044-2007 Informaczionnaya tekhnologiya. Metody` i sredstva obespecheniya bezopasnosti. Menedzhment inczidentov informaczionnoj bezopasnosti
8. GOST R 53114-2008 Gruppa T00. Zashhita informaczii. Obespechenie informaczionnoj bezopasnosti v organizaczii. Osnovny`e terminy` i opredeleniya
9. Bezopasnost` v oblakakh i ne tol`ko: issledovanie-prognoz dlya CISO na 2024 god. URL: https://yandex.cloud/ru/blog/posts/2024/03/information-security-research (date accessed 13.12.2024)

10. Postanovlenie Pravitel`stva RF ot 16 noyabrya 2015 g. # 1236 «Ob ustanovlenii zapreta na dopusk programmnogo obespecheniya, proiskhodyashhego iz inostranny`kh gosudarstv, dlya czelej osushhestvleniya zakupok dlya obespecheniya gosudarstvenny`kh i municzipal`ny`kh nuzhd»
11. Postanovlenie Pravitel`stva RF ot 10 iyulya 2019 g. # 878 "O merakh stimulirovaniya proizvodstva radioe`lektronnoj produkczii na territorii Rossijskoj Federaczii pri osushhestvlenii zakupok tovarov, rabot, uslug dlya obespecheniya gosudarstvenny`kh i municzipal`ny`kh nuzhd, o vnesenii izmenenij v postanovlenie Pravitel`stva Rossijskoj Federaczii ot 16 sentyabrya 2016 g. N 925 i priznanii utrativshimi silu nekotory`kh aktov Pravitel`stva Rossijskoj Federaczii"
12. Svedeniya ob ispol`zovanii czifrovy`kh tekhnologij i proizvodstve svyazanny`kh s nimi tovarov i uslug (itogi statnablyudeniya po f. # 3-inform) URL: https://rosstat.gov.ru/storage/mediabank/3-inf_2022.rar (date accessed 13.12.2024)