**Безопасность цифровых технологий: статистический аспект оценки и анализа**

*Использование информационно-коммуникационных технологий в условиях современной реальности ведет не только к получению известных положительных социально-экономических эффектов, но и предполагает неизбежное возникновение связанных с этим негативных последствий.**С вопросами защиты интересов личности, общества и государства от внутренних и внешних информационных угроз связано понятие информационной безопасности. Расширение ее границ – от низкоуровневых технических мероприятий по защите информационных систем (компьютерной безопасности и кибербезопасности) до стратегического управления экономическим производством – привело к появлению более релевантной категории: цифровой безопасности.* *В контексте такой трансформации логичным представляется объединение этих понятий и категорий в общий термин «безопасность цифровых технологий». Цель данной статьи состоит в том, чтобы обозначить подходы к этому обобщенному понятию с позиций статистического исследования.*

**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, способные представлять собой потенциальную угрозу интересам общества, бизнеса и государства. В узком техническом смысле это обстоятельство находит выражение в виде несанкционированных действий, ведущих к нарушению: конфиденциальности (раскрытию информации), целостности (изменению или уничтожению информации), доступности (отказу в доступе к информационным источниками) и служит предметом изучения информационной безопасности.

Система официальных взглядов и основные положения в этой сфере отражены в Доктрине информационной безопасности РФ [1], 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») и других тематических источниках. На международном уровне изучением проблематики информационной безопасности занимается ряд международных организаций, каждая из которых действует в определенном профильном секторе: так, Организация экономического сотрудничества и развития (ОЭСР, OECD) акцентирует внимание на социальных и экономических аспектах; разработка технических стандартов возложена, в частности, на Международную организацию по стандартизации (ИСО, ISO) и Международную электротехническую комиссию (МЭК, IEC); вопросами киберпреступности занимаются Совет Европы, Управление Организации Объединенных Наций по наркотикам и преступности (UNODC) и Интерпол.

Сегодня в мире отмечается четкая тенденция к инверсии – если ранее информационный контур безопасности ведения бизнеса очерчивали 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 безопасность цифровую, что вполне явно прослеживается в тематических публикациях Организации экономического сотрудничества и развития: “OECD Guidelines for information security” (2002) [3], “OECD Digital Security Risk Management” (2015) [4], “OECD Policy Framework on Digital Security” (2022) [5]. Последняя из перечисленных публикаций содержит 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 рисунке 1.

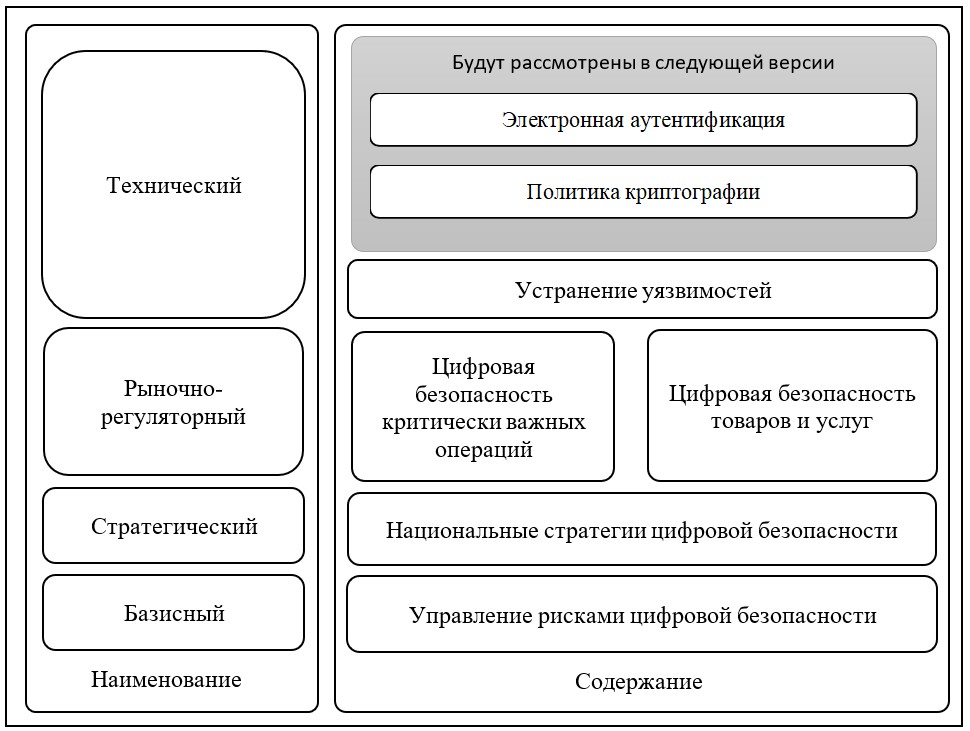


Рис. 1. **Уровни иерархической структуры политики цифровой безопасности**

Источник: [5, p. 7].

Эти рекомендации, если рассматривать их в качестве методологических основ для количественного анализа процессов цифровой безопасности, обладают весьма заметным недостатком: они лишь декларируют направления деятельности, но не предлагают механизм практической реализации (в отличие, например, от разработок ОЭСР в области измерения информационного общества методом анкетирования).

Международный союз электросвязи (МСЭ, ITU) – одна из старейших в мире организаций, действующих сегодня под эгидой Организации объединенных наций – в некоторой степени исправила этот пробел, разработав (совместно с компанией ABI Research) Глобальный индекс кибербезопасности (Global Cybersecurity Index, GCI) и впервые опубликовав его в 2015 году [6]. Этот интегральный показатель отражает успехи стран мира на пути к достижению целей по основным направлениям кибербезопасности (таблица 1).

Таблица 1

**Компоненты Глобального индекса кибербезопасности**

|  |  |
| --- | --- |
| Наименование | 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. |

В 2020 году (последняя публикация Индекса пришлась на 2021 г. [7], а следующая ожидается в 2023 г.) в состав проиндексированной совокупности вошло 169 государств. Специализированная анкета для построения Индекса включает ряд вопросов по каждой из сформулированных мер 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 для статистики, Глобальный индекс кибербезопасности не несет каких-либо количественных данных о деятельности участников процесса создания киберугроз и их отражения, их мотивах и последствиях.

Очевидно, что существующие сегодня официальные методологические разработки в области информационной (цифровой, кибер-) безопасности носят более концептуальный, чем практический характер, и малопригодны для осуществления анализа явлений и процессов реальной жизни. Такое обстоятельство в рамках данного исследования требует выполнения ряда действий. Во-первых, следует объединить, что представляется вполне логичным, вышеуказанный набор весьма путано связанных между собой понятий в общий термин «безопасность цифровых технологий». Во-вторых, в поисках практически ценных данных и методических разработок будет правильным обратиться к лучшим практикам отечественных и зарубежных профильных компаний. Это позволит достичь поставленной цели настоящей работы – обозначить подходы к безопасности цифровых технологий с позиций статистического исследования: а именно, определить границы и структуру, сформировать систему показателей, осуществить выбор методов их анализа.

**Заключение**

**Литература**

1. Доктрина информационной безопасности Российской Федерации (утв. Указов Президента РФ от 5 декабря 2016 г. № 646). URL: https://www.garant.ru/products/ipo/prime/doc/71456224/
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. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. — P.: OECD Publications, 2002. — 30 p.
4. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. — P.: OECD Publishing, 2015. — 74 p.
5. OECD Policy Framework on Digital Security. – P.: OECD Publishing, 2022. – 38 p.
6. ITU Publications. Global Cybersecurity Index 2015. URL: https://www.itu.int/pub/D-STR-SECU-2015
7. ITU Publications. Global Cybersecurity Index 2020. URL: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E