**Цифровая безопасность экономики: 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. По мере возрастания влияния цифровых технологий на экономику происходит объективное расширение границ информационной безопасности – от низкоуровневых технических мероприятий по защите информационных систем до стратегического управления экономическим производством – и ее трансформация в более объемлющую категорию «цифровая безопасность». Цель данной статьи состоит в том, чтобы обозначить подходы к феномену цифровой безопасности с позиций статистического исследования: определить границы и структуру, сформировать систему показателей и осуществить выбор методов их анализа.*

**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 (OECD) акцентирует внимание на социальных и экономических аспектах; разработка технических стандартов возложена, в частности, на Международную организацию по стандартизации (ISO), Международную электротехническую комиссию (IEC), Исследовательскую комиссию ITU-T SG17 Международного союза электросвязи (ITU); 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. При этом структура политики такого управления пластична и в последней версии имеет вид (рис. 1.):

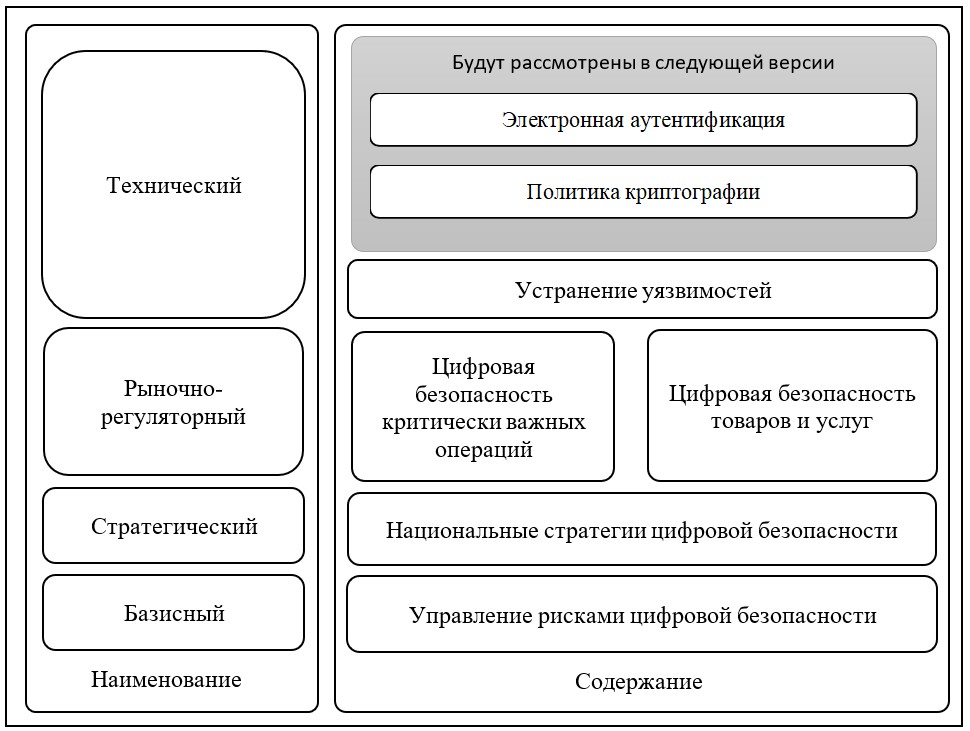


Рис. 1. **Уровни иерархической структуры политики цифровой безопасности**

Источник: [5, p. 7].

**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.