**Цифровая безопасность экономики: статистический аспект оценки и анализа**

*Использование информационно-коммуникационных технологий (ИКТ) 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 узкотехнических позиций такие отрицательные проявления находят выражение в виде несанкционированных действий, ведущих к нарушению: конфиденциальности (раскрытию информации), целостности (изменению или уничтожению информации), доступности (отказу в доступе к информационным источниками).* *С вопросами защиты интересов личности, общества и государства от внутренних и внешних информационных угроз связано понятие информационной безопасности: в этом направлении система официальных взглядов и основные положения отражены в Доктрине информационной безопасности РФ, Федеральном законе «Об информации, информационных технологиях и о защите информации» и др.*

*По мере возрастания влияния цифровых технологий на экономику происходило объективное расширение границ области информационной безопасности – от низкоуровневой технической деятельности по защите информационных систем до стратегического управления экономическим производством. В результате возникла инверсия – если ранее технические специалисты очерчивали информационный контур безопасности ведения бизнеса, то теперь политику информационной безопасности определяют представители высшего менеджмента исходя из оценки рисков, прежде всего, экономического характера. В этом контексте категория «информационная безопасность» трансформировалась в безопасность цифровую, что вполне явно прослеживается в тематических публикациях Организации экономического сотрудничества и развития (ОЭСР): “OECD Guidelines for information security” (2002), “OECD Digital Security Risk Management” (2015), “OECD Policy Framework on Digital Security” (2022). Цель данной статьи состоит в том, чтобы сформулировать феномен цифровой безопасности как объект статистического исследования, определить его границы и структуру, сформировать систему показателей и осуществить выбор методов их анализа.*

**Введение**

**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. Cherdantseva, Y. Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals // Organizational, Legal, and Technological Dimensions of Information System Administrator / Y. Cherdantseva, J. Hilton. — IGI Global Publishing, 2013.