**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 в данном контексте – привело к появлению более релевантной категории: цифровой безопасности.* *Представляется логичным объединить это множество пересекающихся 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.*

**Обзор существующих официальных методологий**

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.

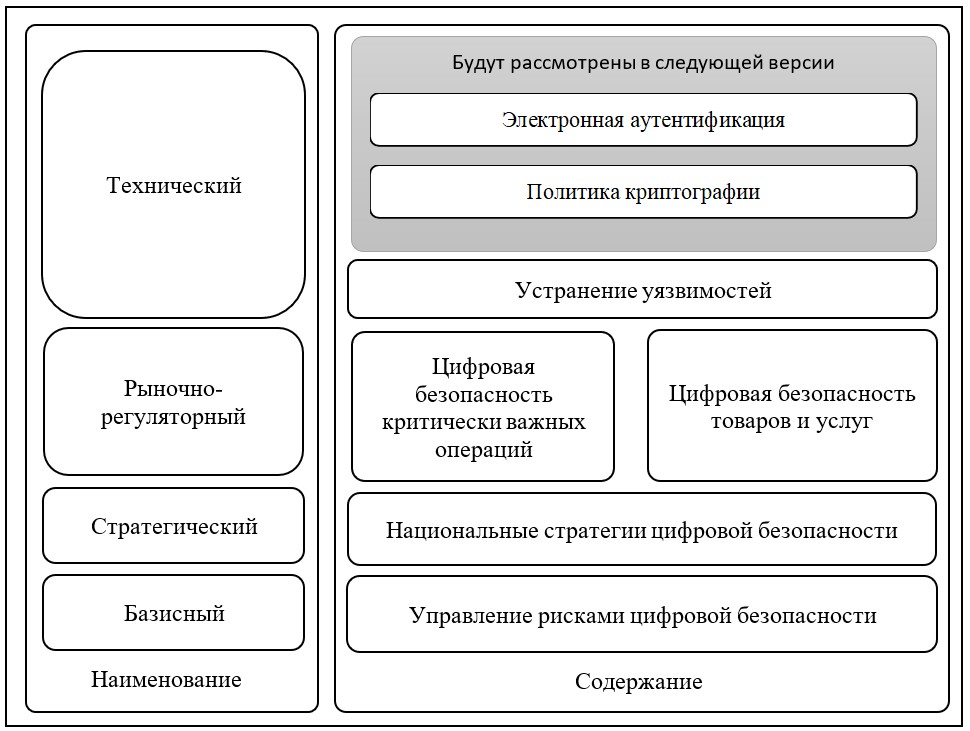


Рис. 1. **Уровни иерархической структуры политики цифровой безопасности**

Источник: [5, p. 7].

Рекомендации ОЭСР, 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 этой международной организации в области методологии измерения информационного общества [6]).

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 [7]. 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. [8], 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 в себе каких-либо данных о количественной стороне деятельности участников процесса создания киберугроз и их отражения, их мотивах и последствиях.

Очевидно, что приведенные выше методологические разработки в области информационной (цифровой, кибер-) безопасности носят более концептуальный, чем практический характер, и малопригодны для статистического анализа.

Статистическая служба Европейского союза (Евростат, Eurostat) занимается сбором статистической информации по странам-членам ЕС и гармонизацией статистических методов, используемых данными странами.

Результаты ежегодного (с 2002 г.) опроса сообщества «Использование ИКТ и электронная коммерция на предприятиях» 2022 года. Статистические данные были получены в результате обследования предприятий, проведенных Национальными статистическими органами в первые месяцы 2022 года [9].

В 2022 г. было опрошено около 150400 предприятий с 10 и более сотрудниками или самозанятыми лицами из 1,47 млн предприятий в ЕС. Из этих млн предприятий примерно 83 процента были малыми предприятиями (с 10-49 работниками или самозанятыми), 14 процентов средними (20-249 работников) и 3 процента крупными предприятиями (250 и более работников).

Таблица 2

**Информационно-коммуникационная безопасность предприятий в странах Европейского союза**

(в процентах от обследуемых предприятий)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Показатели | *X min* |  | *X max* | *Медиана* | *KV, %* |
| Используют как минимум одну меру безопасности ИКТ | 62 | 88,0 | 98 | 90 | 8,6 |
| Информируют работников об их обязанностях в области безопасности ИКТ | 32 | 57,0 | 75 | 60 | 18,6 |
| Имеют разработанные инструкции по мерам, практикам или процедурам по безопасности ИКТ | 15 | 37,8 | 68 | 36 | 34,1 |
| Имеют страховку от инцидентов, связанных с ИКТ | 4 | 20,8 | 71 | 14 | 75,0 |
| Составили или проверили существующие инструкции по безопасности ИКТ предприятия в течение последних 12 месяцев | 7 | 24,9 | 43 | 21 | 38,2 |
| Пережили инциденты безопасности, связанные с ИКТ, имевшие некоторые последствия в отчетном (2021) году | 11 | 20,5 | 44 | 19 | 35,6 |

Федеральная служба государственной статистики (Росстат) – методики расчета показателей федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации». Показатели:

2019 г.: «Количество подготовленных специалистов по образовательным программам в области информационной безопасности, с использованием в образовательном процессе отечественных высокотехнологичных комплексов и средств защиты информации», «Средний срок простоя государственных информационных систем в результате компьютерных атак»;

2020 г.: «Объем затрат на продукты и услуги в области информационной безопасности», «Доля населения, использовавшего отечественные средства зашиты информации, по субъектам Российской Федерации (в процентах от общей численности населения, использовавшего сеть «Интернет» в течение последних 12 месяцев, соответствующего субъекта)».

Таблица 3

**Население, столкнувшееся с проблемами информационной безопасности, по субъектам Российской Федерации**

(в процентах от обследуемых лиц в возрасте от 15 до 74 лет)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Показатели | *X min* |  | *X max* | *Медиана* | *KV, %* |
| *Сталкивались с такими проблемами:* |  |  |  |  |  |
| Заражение вирусом, что привело к потере информации и/или времени на их удаление | 0,7 | 5,1 | 22,0 | 4,6 | 76,3 |
| Несанкционированный доступ к компьютеру (информационным ресурсам, информационным системам) | 0,1 | 1,7 | 19,2 | 1,2 | 142,8 |
| Несанкционированная рассылка (спам) | 3,8 | 23,5 | 81,9 | 21,5 | 55,0 |
| Получение по электронной почте мошеннических писем с просьбой выслать персональные данные | 0,1 | 2,6 | 9,2 | 2,0 | 84,6 |
| Перенаправление на фальшивые сайты с просьбой указать персональные данные | 0,0 | 1,9 | 8,0 | 1,4 | 88,1 |
| Посещение детьми нежелательных сайтов, контакты детей с потенциально опасными людьми через сеть Интернет | 0,0 | 0,6 | 3,3 | 0,4 | 98,4 |
| Хищение денежных средств или персональных данных | 0,0 | 0,5 | 5,7 | 0,3 | 162,3 |
| Использование мобильного телефона неизвестными лицами | 0,0 | 1,7 | 39,2 | 0,4 | 320,3 |
| Использование электронной почты неизвестными лицами | 0,0 | 1,0 | 28,6 | 0,3 | 369,1 |
| Другие проблемы информационной безопасности | 0,2 | 3,5 | 2,4 | 20,8 | 111,4 |
| *Не сталкивались с проблемами информационной безопасности* | 12,8 | 69,4 | 92,2 | 70,9 | 20,5 |

Таблица 4

**Население, использовавшее средства защиты информации, по субъектам Российской Федерации**

(в процентах от обследуемых лиц в возрасте от 15 до 74 лет)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Показатели | *X min* |  | *X max* | *Медиана* | *KV, %* |
| *Использовали – всего:* | 36,1 | 71,7 | 98,8 | 73,0 | 16,1 |
| *из них:* |  |  |  |  |  |
| Антивирусные средства | 29,2 | 68,5 | 98,8 | 69,9 | 18,1 |
| Антиспамовые фильтры | 1,7 | 15,2 | 13,6 | 53,9 | 58,4 |
| Средства родительского контроля или фильтрации Интернет-ресурсов | 0, | 2,1 | 1,7 | 9,9 | 87,8 |
| Другие средства защиты | 0,1 | 2,1 | 1,1 | 12,4 | 121,4 |
| *Не используют средства защиты* | 0,4 | 18,3 | 16,9 | 60,0 | 52,0 |
| *Затруднились ответить* | 0,6 | 10,1 | 10,2 | 28,4 | 61,2 |

Дальнейшее проведение данного исследования требует выполнения ряда действий. Во-первых, во избежание путаницы с дефинициями и для упрощения понимания предметной области логично будет объединить вышеуказанный набор понятий в общий термин «безопасность цифровых технологий». Во-вторых, в поисках практически ценных сведений представляется верным 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.

**Формирование системы показателей на основе лучших практик**

**Анализ экономической эффективности в контексте безопасности цифровых технологий**

**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. OECD Guide to Measuring the Information Society 2011. – P.: OECD Publishing, 2011. – 204 p.
7. ITU Publications. Global Cybersecurity Index 2015. URL: https://www.itu.int/pub/D-STR-SECU-2015
8. ITU Publications. Global Cybersecurity Index 2020. URL: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
9. Eurostat Statistics Explained. IT security in enterprises. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT\_security\_in\_enterprises