**Безопасность применения 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 (**логично объединить это множество пересекающихся понятий и категорий в общий термин «безопасность применения цифровых технологий»). Цель данной статьи состоит в том, чтобы обозначить подходы к этому обобщенному понятию с позиций статистического исследования, преобразовать существующую систему показателей путем включения в нее новых индикаторов из сферы корпоративной аналитики и, наконец, осуществить оценку и анализ влияния безопасности цифровых технологий на результаты работы предприятий и организаций различных видов экономической деятельности.*

**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.

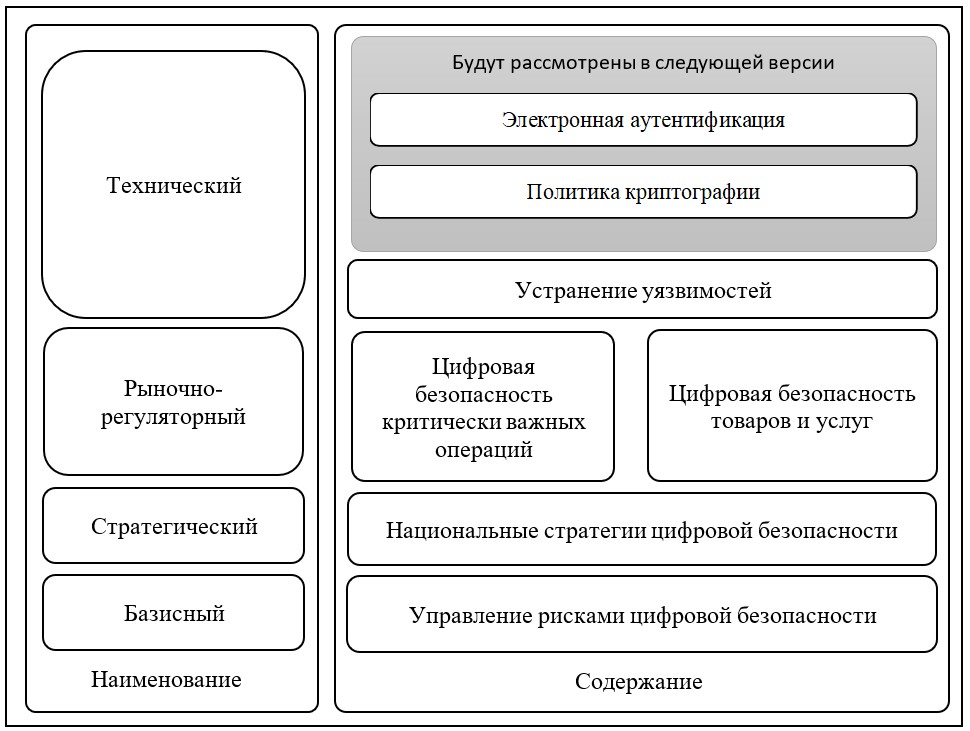


Рис. 1. **Уровни иерархической структуры политики цифровой безопасности OECD**

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, где Российская Федерация, набрав 98,06 балла из 100, разделила 5-е место с Объединенными Арабскими Эмиратами и Малайзией в общем рейтинге и единолично заняла 1-е место в рейтинге стран Содружества Независимых 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 в поисках конкретики следует обратиться к международным и национальным органам статистики. Так, статистическая служба Европейского союза (Евростат, Eurostat) ежегодно (с 2002 г.) проводит и публикует результаты опроса сообщества по теме использования информационно-коммуникационных технологий (ИКТ) и электронной коммерции на предприятиях. Статистические данные были получены в результате обследования предприятий, проведенных Национальными статистическими органами стран-членов Евросоюза в первые месяцы 2022 года: было опрошено около 150400 предприятий с 10 и более сотрудниками или самозанятыми лицами из 1,47 млн предприятий в ЕС.

Некоторые дескриптивные статистики совокупности стран ЕС по ряду показателей информационно-коммуникационной безопасности предприятий (буквально, «ICT security in enterprises») [9] приведены в таблице 2. Как отмечают евростатистики, в 2022 году 92 % предприятий ЕС с 10 и более сотрудниками или самозанятыми лицами использовали хотя бы одну меру для обеспечения целостности, доступности и конфиденциальности данных и систем ИКТ. Более чем каждое третье предприятие (37 %) сообщило о наличии документов, устанавливающих меры, практику или процедуры по обеспечению безопасности ИКТ. На каждом четвертом предприятии (24 %) эти документы были определены или рассмотрены в течение последних 12 месяцев. Каждое четвертое предприятие (25 %) было застраховано от инцидентов безопасности ИКТ. Наконец, в 2021 году более чем каждое пятое предприятие (22 %) столкнулось с последствиями инцидентов безопасности, связанных с ИКТ. Следует отметить, что значения коэффициента вариации (*KV*) с его пороговым значением в 33 процента характеризуют совокупность стран Евросоюза как «пограничную» в оценке ее однородности по большинству анализируемых показателей.

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) в рамках реализации федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» осуществляет разработку методик расчета тематических показателей, находящих отражение в публикациях об использовании информационных технологий населением и организациями. Наряду с этим Росстат в коллаборации с Министерством общественного развития, связи и массовых коммуникаций РФ (Минцифры России) и Национальным исследовательским университетом «Высшая школа экономики» (НИУ ВШЭ) регулярно публикует статистические сборники, посвященные информационному обществу и цифровой экономике (например, [10-11]). Результаты проведенного Росстатом в 2022 г. Выборочного федерального статистического наблюдения по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей содержат, в частности, данные об инцидентах информационной безопасности и средствах защиты, применяемых для их предотвращения (табл. 3 и 4).

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 |

Явно прослеживаемая в таблицах высокая степень неоднородности совокупности регионов России по большинству показателей предполагает наличие типических региональных групп по признакам интенсивности и номенклатуры угроз информационной безопасности: где-то население постоянно сталкивается с такого рода инцидентами, где-то – лишь изредка.

Проведенный обзор используемых в настоящее время официальных методологий профильных и статистических организаций выявил ряд проблем, среди которых множественность понятия информационной безопасности и фрагментарность структуры ее индикаторов. Это обстоятельство в рамках исследования требует выполнения ряда действий. Во-первых, во избежание несогласованности в дефинициях и для упрощения понимания предметной области логично будет объединить вышеуказанный набор понятий безопасности (информационная, информационно-коммуникационная, компьютерная, кибер-, цифровая) в общий термин «безопасность применения цифровых технологий». Во-вторых, в целях повышения качества и развития существующей системы статистических показателей представляется верным четко определить ее структуру, а также увеличить «мощность» этой системы путем включения в нее индикаторов, используемых, например, в сфере корпоративной аналитики.

**Формирование системы показателей на основе лучших практик**

Необходимым условием получения научно обоснованных результатов оценки и анализа объекта статистического исследования служит наличие соответствующей системы показателей, представляющей собой «комплекс взаимосвязанных и расположенных в логической последовательности показателей, всесторонне характеризующих состояние и развитие массовых явлений общественной жизни» [13, с. 21]. Большое значение теории статистических показателей придавала еще советская школа статистики: «Система, совокупность всегда более значима, чем сумма отдельных частей, так как помимо информации о частях она несет информацию о том новом, что появляется в результате взаимодействия частей, информацию о развитии системы в целом. Рассматриваемое положение математиками в общем виде формулируется так: функция системы больше суммы функций составляющих ее частей, т. е. *f(x, y) > f (x) + f(y)»* [14, с. 226]. При этом, согласно положениям диалектического материализма, справедливо отмечалось, что «системы статистических показателей нельзя представлять стабильными, они изменяются вслед за изменениями отражаемой ими действительности» [там же, с. 228].

Современными отечественными учеными-статистиками предлагается, например, в статье [15], осуществлять формирование системы статистических показателей, руководствуясь рядом принципов, среди которых фигурируют такие как: *принцип системного подхода* (в совокупности разнообразные статистические показатели полностью описывают объект исследования), *принцип информативности при минимизации числа статистических показателей* (показатели должны быть максимально информативны, при этом их количество должно быть минимально) и *принцип количественной определенности оценки* (для показателей должна быть определена количественная оценка, они должны иметь эталонное или нормативное значение, должен быть известен диапазон принимаемых значений); однако же, разумеется, далеко не всегда эти принципы могут быть практически выполнимы.

В данном теоретическом контексте очевидно, что система статистических показателей безопасности применения цифровых технологий – в силу высокой степени динамики процессов в этой сфере – не может являться косной структурой, а должна, в первую очередь, отражать логику особенностей этого развития. Такой подход выражен на рис. 2, где концептуальная схема формирования системы показателей содержит два компонента, отображающих аспекты оценки и анализа: характерный, учитывающий особенности предметной области – «Процесс», и общий («Направление» и «Масштаб»), свойственный для логики построения систем показателей в целом.

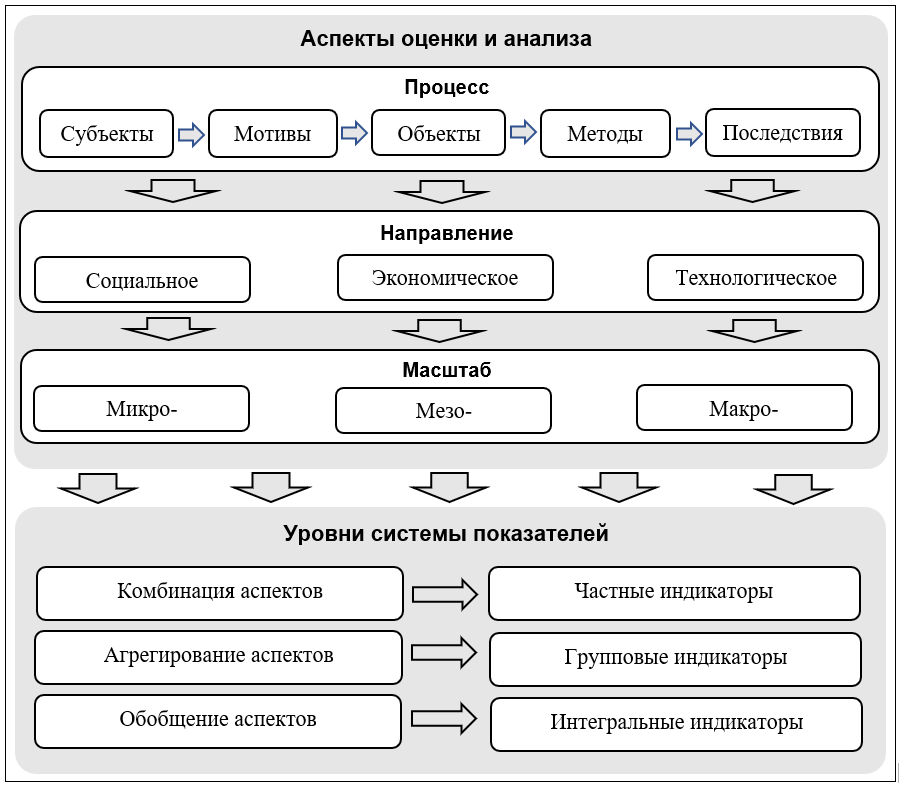


Рис. 2. **Концептуальная схема формирования системы статистических показателей безопасности применения цифровых технологий**

В результате состав показателей системы формируется динамически при сохранении общей структуры, основанной на логике взаимосвязи аспектов (пример практической реализации схемы представлен в таблице 5).

Таблица 5

**Примеры индикаторов-представителей системы статистических показателей безопасности применения цифровых технологий**

|  |  |  |
| --- | --- | --- |
| Направление | Показатели по звеньям процесса | Масштаб |
|  | ***Субъект*** |  |
| Технологич. | Соотношение числа инцидентов, связанных с внутренними и внешними для организации источниками киберугроз | Микро |
| Экономич. | Число сотрудников по информационной безопасности в штате организации | Микро |
| Социологич. | Доля домохозяйств, пострадавших от злонамеренных действий неизвестных лиц в сфере защиты информации | Макро |
|  | ***Мотив*** |  |
| Технологич. | Доля инцидентов, связанных с кибермошенничеством | Микро |
| Технологич. | Число инцидентов, связанных с кибертерроризмом | Макро |
| Экономич. | Доля организаций, столкнувшихся с вымогательством средств посредством использования цифровых технологий | Мезо  Макро |
| Социологич. | Доля лиц в домохозяйстве, сталкивавшихся с угрозами разглашения личной информации с целью вымогательства | Микро |
|  | ***Объект*** |  |
| Технологич. | Число инцидентов, связанных с попытками проникновения внутрь периметра информационной системы организации | Микро |
| Технологич. | Доля инцидентов в центрах хранения данных, связанных с кибербезопасностью | Макро |
| Экономич. | Структура внутренних информационных ресурсов организации | Микро |
| Экономич. | Доля организаций, имеющих полнофункциональный сайт с административной частью | Мезо  Макро |
| Социологич. | Число учетных записей в социальных сетях в среднем на одного члена домохозяйства | Микро |
|  | ***Метод*** |  |
| Технологич. | Число инцидентов, связанных с отказом в обслуживании запросов клиентов сайта организации в связи с кибератаками | Микро |
| Технологич. | Число зарегистрированных вредоносных программ по видам | Макро |
| Экономич. | Доля организаций, подвергшихся кибератакам по видам | Макро |
| Социологич. | Доля домохозяйств, столкнувшихся с кибермошенничеством с использованием методов социальной инженерии | Макро |
|  | ***Последствия*** |  |
| Технологич. | Объем утраченных данных организации вследствие кибератаки | Микро |
| Экономич. | Величина ущерба по причине кибератаки на сайт организации | Микро |
| Экономич. | Величина финансовых потерь в результате кибератак | Макро |
| Социологич. | Периодичность потери контроля над учетными записями | Микро |
| Социологич. | Доля домохозяйств, отказавшихся от использования цифровых услуг правительства и бизнеса в целях защиты информации | Мезо  Макро |

Примечательным моментом перечня является ряд показателей, весьма репрезентативно представляющих технологический уровень предметной области и оперирующих термином «инцидент». Под инцидентом информационной безопасности (ИБ), согласно [16], понимается появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угроз ИБ. Инциденты имеют широкую классификацию, но наиболее актуально выделять две их группы: преднамеренные, включающие в себя весь набор способов и методов создания угроз ИБ (фишинг, брутфорс, программы-вымогатели, черви, трояны и т.п.), и случайные, вызванные ошибками пользователей, нелицензированным программным обеспечением и пр.

В этой связи оценку и анализ безопасности применения цифровых технологий весьма удобно представлять как изучение звеньев некоторого процесса отслеживания такого инцидента (субъект-мотив-объект-методы-последствия). Например, от его инициатора (злоумышленника) через мотив (хулиганство, мошенничество, терроризм) к объекту (информационный ресурс гражданина, корпорации, правительства) посредством всего спектра доступных методов и до результата в виде финансовых и репутационных потерь. При этом возможен и позитивный вариант такого процесса: например, субъект (инженер службы ИБ) – мотив (защита информационного ресурса) – объект (информационная системы и сети) – методы (алгоритм действий со стороны службы ИБ) – последствия (угроза конфиденциальности, целостности и доступности ресурса предотвращена).

Вполне ясно, что исчисление приведенных в перечне показателей, относящихся к мезо- (регион страны, вид экономической деятельности) и макро- (страна) уровням, требует проведения специальных выборочных обследований и на практике трудно реализуемо в связи с массой ожидаемых проблем в решении программно-методологических и организационных вопросов.

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

**Основные выводы**

**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
10. Информационное общество в Российской Федерации. 2020: статистический сборник [Электронный ресурс] / Федеральная служба государственной статистики; Нац. исслед. ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2020. URL: https://rosstat.gov.ru/storage/mediabank/lqv3T0Rk/info-ob2020.pdf
11. Цифровая экономика: 2023: краткий статистический сборник / Г.И. Абдрахманова, С.А. Васильковский, К.О. Вишневский и др.; Нац. исслед. ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2023. – 120 с.
12. Выборочное федеральное статистическое наблюдение по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей. URL: https://gks.ru/free\_doc/new\_site/business/it/ikt21/index.html
13. Зарова Е. В., Проскурина Н. В. Теоретические основы региональной статистики. Самара: Изд-во СГЭА, 2004. 62 с.
14. Суслов И. П. Теория статистических показателей. М.: Статистика, 1975. 264 c.
15. Алетдинова А. А. Формирование системы статистических показателей инновационного потенциала организации // Экономика, статистика и информатика. Вестник УМО. №6(2), 2011 C. 78-81
16. ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности». URL: https://docs.cntd.ru/document/1200068822