УДК 330:51-77:338

К. Н. Горпинченко

ФГБОУ «Кубанский государственный аграрный университет им. И.Т. Трубилина», Краснодар, e-mail: kubkng@mail.ru

А. В. Булатникова

ФГБОУ «Кубанский государственный аграрный университет им. И.Т. Трубилина», Краснодар, e-mail: bulatnikovaa166@gmail.com

Г. А. Глебов

ФГБОУ «Кубанский государственный аграрный университет им. И.Т. Трубилина», e-mail: glebovga777@gmail.com

РЕГУЛИРОВАНИЕ И ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ СТАТИСТИКЕ

Ключевые слова: информационная безопасность, социально-экономическая статистика, электронный сбор данных, электронное правительство.

Актуальность статьи обусловлена важностью сохранения информации в процессе сбора социально-экономических статистических данных. Целью исследования является анализ основных направлений регулирования и нормативно-правовых аспектов информационной безопасности при предоставлении социально-экономической статистической информации, нормативно-правовых, технологических, кадровых аспектов организации деятельности по информационной безопасности при сборе, передаче, аналитике, обработке, хранении статистических данных; анализ реализации государственных программ в сфере защиты статистической информации; анализа основных положений Стратегии развития Росстата по переходу на электронный сбор данных; функций каждого уровня ГИС «ЦАППСД» по обеспечению защиты информации. Материалами исследования являются данные нормативно-правовых документов, регламентирующих сферу зашиты информации при сборе статистических данных; аналитических материалов, научных статей и учебных пособий по теме исследования. Проведено сравнение данных об использовании инструментов искусственного интеллекта в сборе и защите информации, получены данные об увеличении количества предприятий, использующих искусственный интеллект для организации процессов. В целях проведения научного анализа использованы методы анализа, сравнения, обобщения, классификации, синтеза информации на основе методологии системного и объективного научного подхода. По итогам проведенного научного анализа в рамках исследования сделаны выводы о системном внедрении цифровых технологий, в т.ч., инструментов искусственного интеллекта для защиты информации при сборе статистических данных и аналитики.

K. N. Gorpinchenko

Kuban State Agrarian University named after I.T. Trubilin, Krasnodar, e-mail: kubkng@mail.ru

A. V. Bulatnikova

Kuban State Agrarian University named after I.T. Trubilin, Krasnodar, e-mail: bulatnikovaa166@gmail.com

G. A. Glebov

Kuban State Agrarian University named after I.T. Trubilin, e-mail: glebovga777@gmail.com

REGULATION AND LEGAL ASPECTS OF INFORMATION SECURITY IN SOCIO-ECONOMIC STATISTICS

Keywords: information security, socio-economic statistics, electronic data collection, electronic government.

The relevance of the article is due to the importance of preserving information in the process of collecting socio-economic statistical data. The purpose of the study is to analyze the main directions of regulation and regulatory aspects of information security in the provision of socio-economic statistical information, regulatory, technological, personnel aspects of the organization of information security activities in the

collection, transmission, analysis, processing, storage of statistical data; analysis of the implementation of state programs in the field of statistical information protection; analysis of the main provisions of the Rosstat Development Strategy for the transition to electronic data collection; functions of each level of GIS "TSAPPSD" to ensure information security. The research materials are the data of normative legal documents regulating the sphere of information protection in the collection of statistical data; analytical materials, scientific articles and textbooks on the research topic. A comparison of data on the use of artificial intelligence tools in the collection and protection of information was carried out, data on an increase in the number of enterprises using artificial intelligence to organize processes was obtained. In order to conduct scientific analysis, methods of analysis, comparison, generalization, classification, and synthesis of information based on the methodology of a systematic and objective scientific approach were used. Based on the results of the scientific analysis carried out within the framework of the study, conclusions were drawn about the systematic introduction of digital technologies, including artificial intelligence tools for information protection in the collection of statistical data and analytics.

Введение

Актуальность исследования обусловлена тем, что в современных условиях глобальной цифровой экономики охрана информации и деятельность по информационной безопасности является неотъемлемой частью национальной безопасности государства. Увеличение количества преступлений, совершенных при помощи информационных технологий, подтверждает данный тезис, свидетельствует о том, что в настоящее время информационные технологии становятся средством нарушений закона и прав физических и юридических лиц. В сфере статистических измерений охрана информации и информационная безопасность играют ведущую роль в связи с важностью объективного получения и обработки информации, которая становится впоследствии основой для социально-экономических прогнозов.

Цель исследования: изучение правовых аспектов и основных направлений регулирования информационной безопасности в сфере социально-экономической статистики.

Материал и методы исследования

Основными методами исследования являются методы объективного научного анализа: анализ, синтез. описание, сравнение, классификация научной информации на основе объективного системного научного подхода.

Материалом для исследования являются материалы нормативных документов федерального законодательства: федеральные законы, стратегии развития, государственные программы по теме исследования.

Результаты исследования и их обсуждение

Под информационной безопасностью социально-экономической статистики понимается создание системы защиты государственных интересов, прав и свобод граждан и юридических лиц в сфере распространения и существования статистической информации, в также защиты от нарушения данных прав и интересов, которые могут заключаться в несанкционированном доступе и использовании информации. Информационная безопасность в данной сфере включает два основных аспекта: регуляторный (правовой) и технологический. Под правовым аспектом понимается разработка и функционирование правовых норм в сфере защита незаконного использования и распространения социально-экономической информации, предотвращение неразрешенного доступа, изменения и уничтожения информации. Технологический аспект включает в себя создание единой технической инфраструктуры для защиты от проникновения и информационных инцидентов, технологическая защита от проникновения в государственные информационные системы, в которых содержатся статические данные социально-экономической сферы.

Информационная безопасность является приоритетным направлением государственной деятельности, внедрение которого ведется на уровне государственной программы «Информационное общество», которая направлена на повышение качества доступа к информационно-коммуникационной сети, а также внедрение современных форм защиты информационных каналов от незаконных проникновений.

Нормативное регулирование данной сферы включает в себя документы, представленные на рисунке 1 [1-3].

Как следует из данных на рисунке 1, нормативное регулирование данного вопроса разработано на федеральном уровне и регламентирует взаимоотношения между субъектами информации, защиту информации на уровне ее обработки, использования, трансляции и хранения.

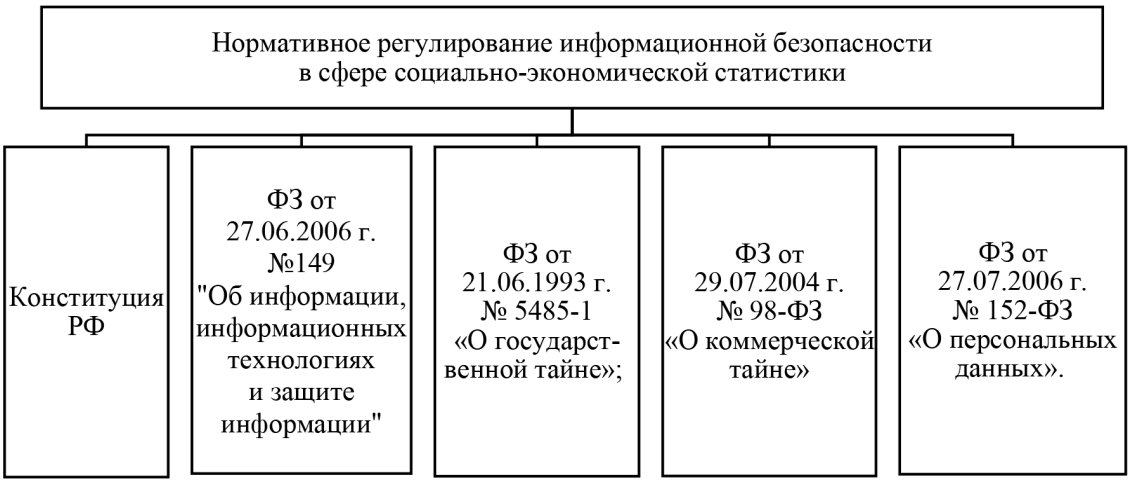

Рис.1. Нормативное регулирование информационной безопасности в сфере социально-экономической статистики

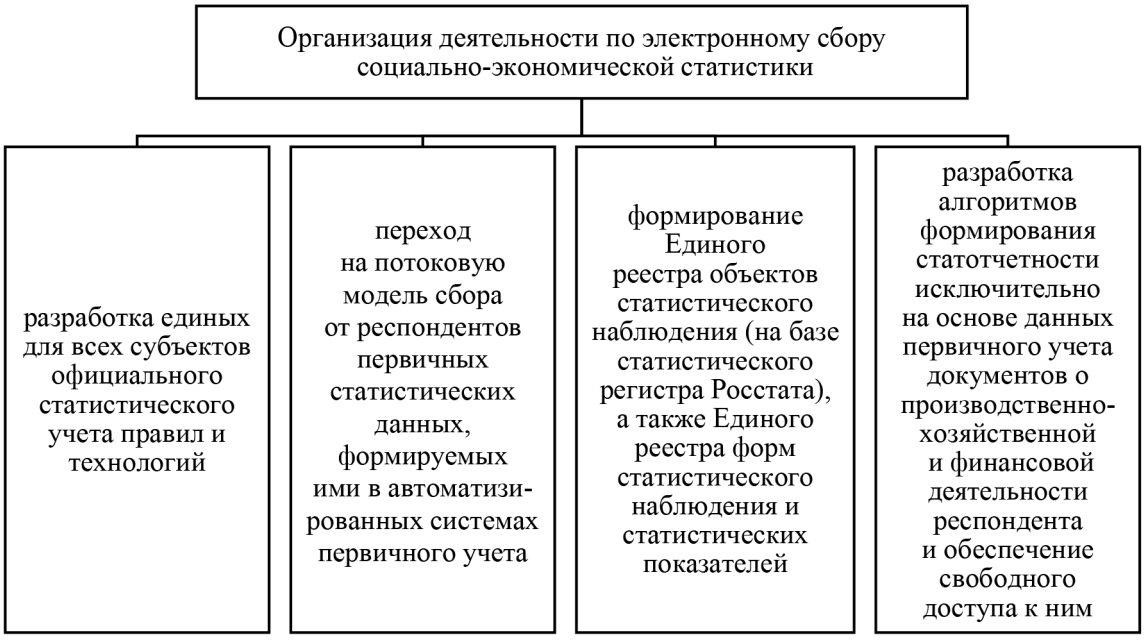

Рис. 2. Организация деятельности по электронному сбору социально-экономической статистики

Информационная безопасность в данной сфере направлена на организацию деятельности «электронного правительства», которое получает социально-экономическую статистическую информацию в электронном виде. Защита информации предусмотрена в Стратегии развития Росстата и системы государственной статистики РФ до 2024 года [4]. На основании Стратегии предусмотрено внедрение электронного сбора статистических данных, которые повышают точность и достоверность информации, а также повышают скорость предоставления и существенно экономят бюджетные средства при обработке данных. Данная деятельность выполняется в формате организации видов деятельности, которые представлены на рисунке 2.

На каждом из этих этапов необходимым является организация деятельности по защите информации и обеспечению информационной безопасности. Данная деятельность предполагает нормативно-правовой, технологический и кадровый уровни:

- на нормативно-правовом уровне производится разработка нормативной документации, формирующей правовое поле

сбора, использования и охраны статистической информации, разработку регламентов по электронному сбору информации, внесение изменений в федеральные, региональные и локальные нормативные документы; регламентация использования электронной цифровой подписи и систем электронного документооборота;

- обеспечение отечественного технологического обеспечения, в т.ч., отечественного программного обеспечения по защите электронного сбора социально-экономических данных о деятельности регионов, предприятий, личных хозяйств и других субъектов сбора статистической информации;

- работа с кадрами включает в себя обучение работе с порталами, навыкам информационной безопасности, ответственному отношению по использованию конфиденциальных данных и учетных корпоративных записей [5].

При этом к декабрю 2024 году отечественные предприятия произведут переход на российское программное обеспечение, а к 2030 году 80% российский компаний будут переведены на отечественное ПО [4].

В результате перехода на цифровые технологии предоставления данных будут достигнуты целевые показатели, указанные на рисунке 3 [4].

Рис.3. Целевые показатели Стратегии по результатам перехода на электронный сбор социально-экономических данных

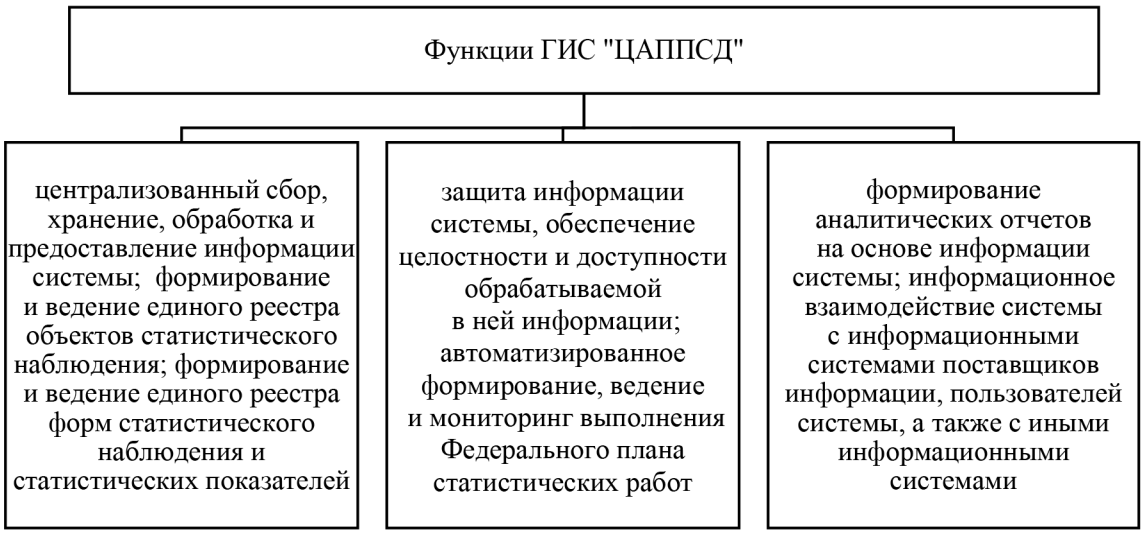

Рис. 4. Функции ГИС «ЦАППСД»

Для ведения сбора и аналитики статданных формируется единая информационная система как элемент национальной системы управления данными. Базовой технологической интеграционной системой, которая обеспечивает сбор и защиту информации при электронном сборе статданных, является ГИС «Цифровая аналитическая платформа предоставлении статистических данных». Ее функции представлены на рисунке 4 [4].

В сфере защиты информации каждый участник системы выполняет предусмотренные нормативными документами функции, соблюдение которых необходимо и регламентировано. Данный функционал предусматривает действия каждого участника для того, чтобы предотвратить утечку данных, несанкционированное использование информации либо ее изменение. Важность исполнения регламентов подтверждается тем фактом, что утечки информации часто происходят по вине самих пользователей систем, когда пользователи переходят на рабочих компьютерах по внешним подозрительным ссылкам, переходят на фишинговые сайты, вводят корпоративные учетные записи для регистрации на внешних сайтах. Создавая таким образом провоцирующие факторы для проникновения в информационную систему, пользователи повышают ее уязвимость. В связи с этим при работе с ГИС «ЦАППСД» необходимо организовать обучение сотрудников по обязательному исполнению всех требований регламентов и выделению отдельных защищенных рабочих мест для передачи статданных по защищенным криптоканалам. Регламент четко описывает функционал каждого участника ГИС «ЦАППСД» на рисунке 5 [4].

Как следует из данных рис.5, функционал участников определен требованиями безопасности. Защите подлежит вся информация, которая зафиксирована в ГИС «ЦАППСД» и хранится в ней для использования данных в целях проведения статистических измерений. Вся информация о статистических данных делится на два больших блока:

- информация, которая доступна при авторизации в систему;
- информация, доступ к которой не может быть ограничен для широкого круга пользователей на основании законодательства [4].

Выделяются следующие критерии защиты социально-экономической статистической информации:

-индикаторный;
- ресурсно-целевой;
- программно-целевой [7].

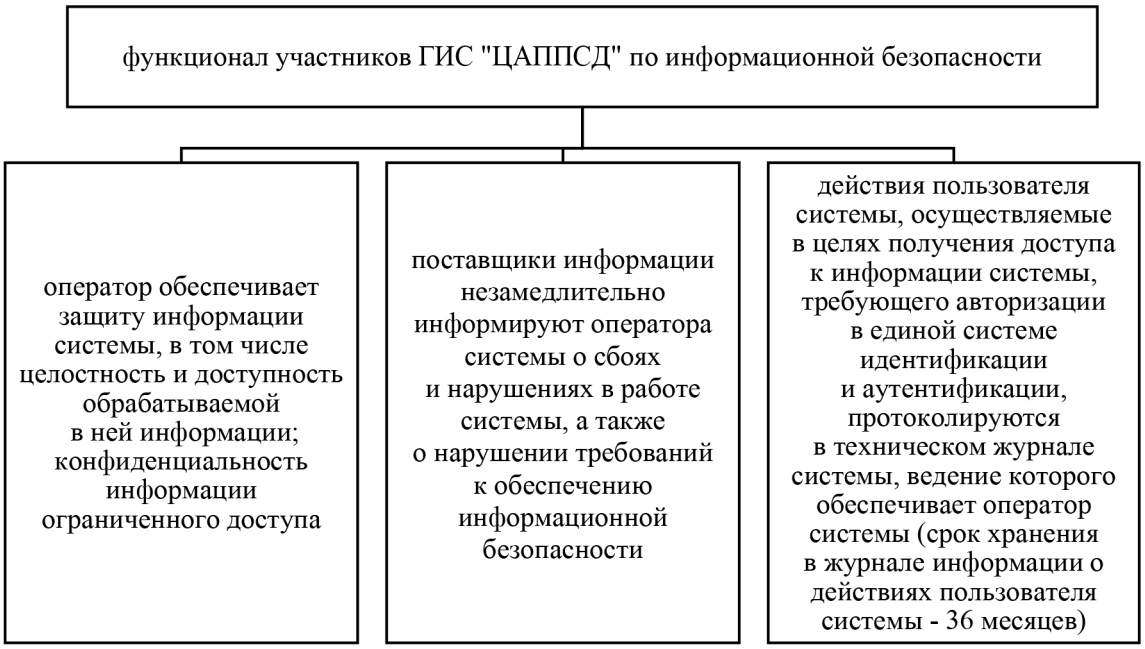

Рис. 5. Функционал участников ГИС «ЦАППСД» по информационной безопасности

В рамках индикаторного критерия оцениваются количественные изменения, которые может нести программа в результате нарушения информационной безопасности, например, в случае, если произошла утечка информации: оценка количества утечки информации, оценка сохранения конфиденциальности информации, отсутствие утечки информации при передаче ее через электронные средства связи.

Ресурсно-функциональный критерий дает возможность оценить уровень систематической, стабильной деятельности всех сфер ГИС, отсутствие внешних проникновений, инцидентов и других способов нарушения целостности системы;

- программно-целевой критерий позволяет оценить системность изменений всех подуровней ГИС на интеграцию и совмещенность, минимальные расхождения, которые создаются при отсутствии единства программных средств и загрузки данных «вручную».

С точки зрения критичности защищенности выделяются несколько уровней информационной безопасности социально-экономических статданных: стабильный, предкризисный и кризисный. Стабильный уровень означает работу всех сфер системы на должном уровне защиты и определяется как системный, обеспечивающий достаточную защиту. Предкризисный уровень означает наличие угроз, которые могут возвратить систему в стабильный уровень при условии принятия своевременных мер. Кризисный уровень свидетельствует о низком уровне управленческой деятельности в сфере защиты информации, отсутствии необходимых управленческих навыков по организации и контролю деятельности в сфере информационной безопасности.

Схематически деятельность по обеспечению сохранности информации можно представлена на рисунке 6 [5].

Деятельность по защите статической информации и обеспечении информационной безопасности должна планироваться на всех уровнях управления и включать в себя стратегический, тактический и операционный уровни. Стратегический уровень означает, что на уровне руководства организации должны быт выделены штатные сотрудники, отвечающие за реализации стратегии информационной безопасности организации, должна быть проведена работа по внедрению и оснащению современных отечественных средств программного обеспечения, современного оборудования, которое в состоянии по своим техническим характеристикам быть совмещенным с данными средствами защиты, установлены необходимые криптоканалы, которые защищают информацию должным способом. На тактическом уровне должны быть разработаны необходимые регламенты, должностные инструкции, проведены инструктажи, оборудованы рабочие места сотрудников. На операционном уровне необходимо, чтобы каждый сотрудник выполнял свои должностные инструкции, обеспечивал исполнение регламентов и взаимодействия по должности.

В зависимости от сферы деятельности в организации можно выделить несколько направлений сохранности и защиты социально-экономической статистики (рисунок 7) [5].

В целях эффективной деятельности по обеспечению защиты информации важно организовать при электронном сборе данных системное взаимодействие на уровне трех подсистем: информационного обеспечения организационно-управленческого процесса, защиты информационной среды, мониторинга уровня информационной безопасности.

Данная деятельность может быть эффективно организована на основе использования инструментов искусственного интеллекта, которые активно внедряются в настоящее время в управленческую, производственную, финансовую и охранную сферу предприятий (рисунок 8) [8].

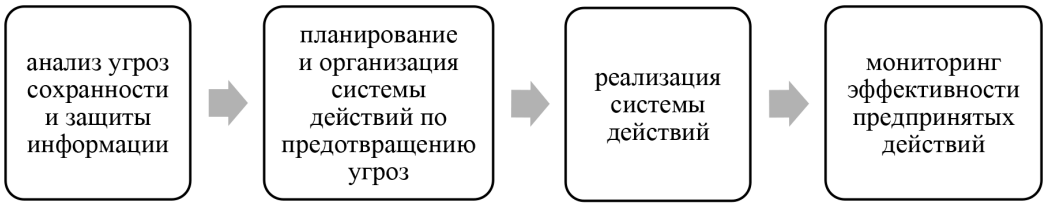

Рис. 6. Схема функционирования по сохранности и защите информации

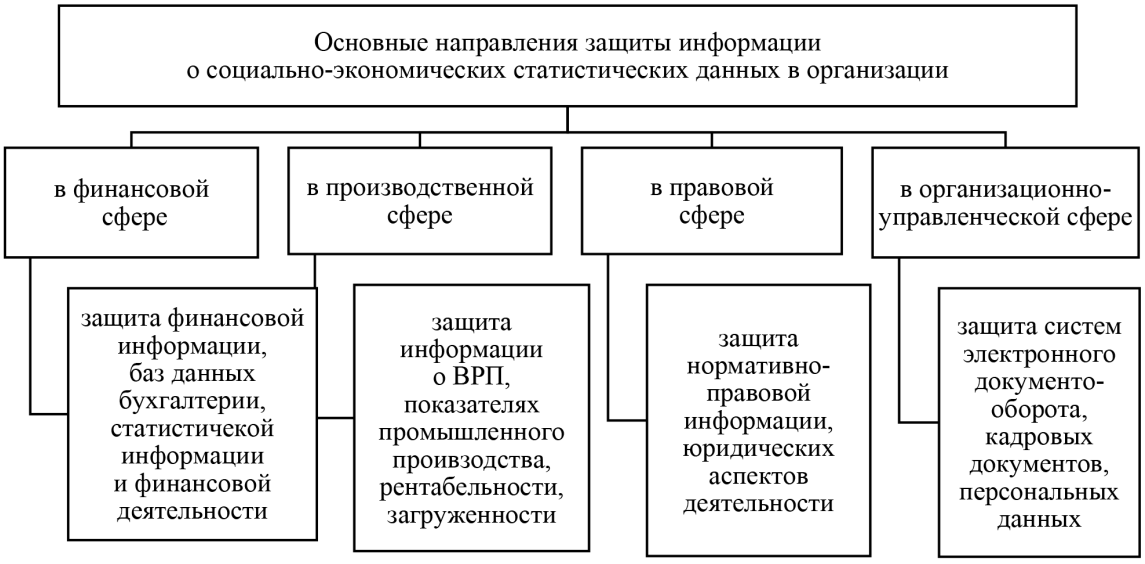

Рис. 7. Основные направления защиты информации о социально-экономических статистических данных в организации

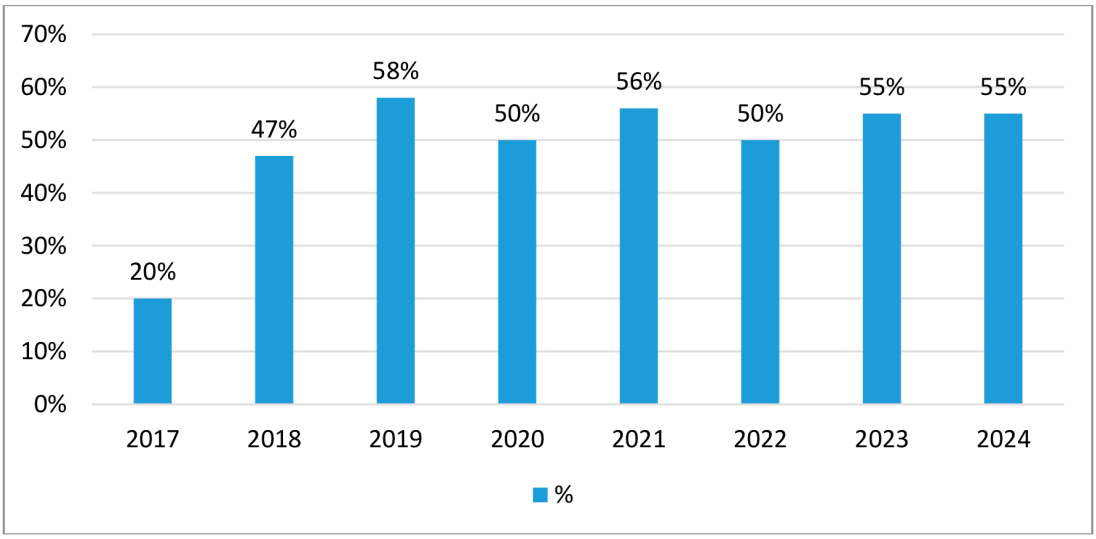

Рис. 8. Доля организаций в мире, которые используют искусственный интеллект

Как следует из данных рисунка 8, количество организаций, которые применяют ИИ в процессах, стабильно увеличивается, что подтверждает важность синхронизации предоставления статистических данных с использованием механизмов ИИ и защиты информационных систем от хакерских атак и других форм информационных инцидентов. В настоящее время деятельность по нарушению целостности информационных систем резко возросла. Действенным инновационным направлением в преодолении подобного рода автоматизированных проникновений является внедрение в системы информационной безопасности – инструментов искусственного интеллекта. При этом регулирование данного процесса находится в стадии формирования. Инструменты ИИ позволяют в целом внедрить системы автоматизации задач статической обработки и наблюдения, ускоряют количественное измерение больших объемов данных, способствуют экономии бюджетных средств и созданию цифровых архивов данных, которые в зависимости от заданных задач позволяют создать новые алгоритмы обработки и использования информации (рисунок 9) [6].

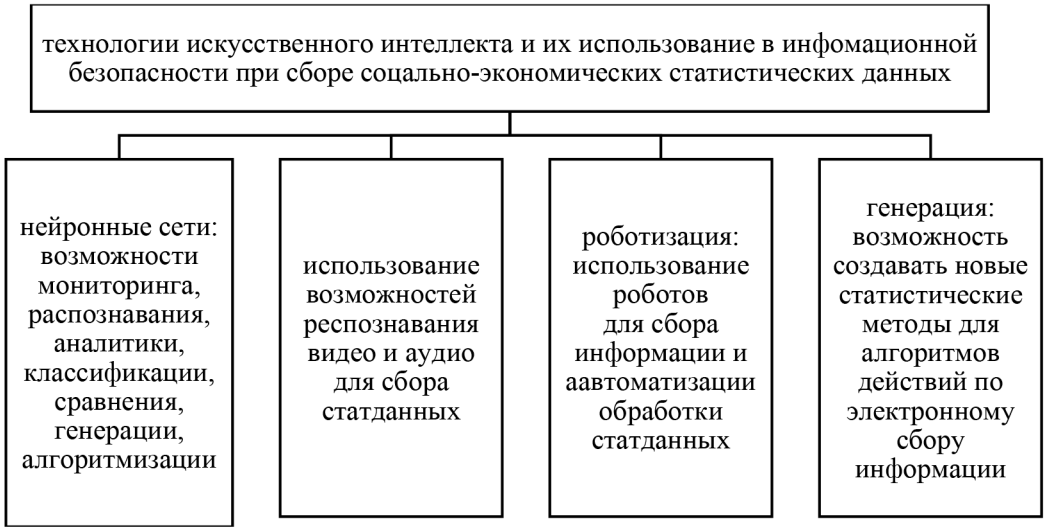

Рис. 9. Технологии искусственного интеллекта и их использование в информационной безопасности при сборе социально-экономических статистических данных

Данные цифровые технологии позволяют усилить защиту и передачу информации технологиями многофакторной аутентификации и распределенного реестра. При многофакторной аутентификации дополняются количество паролей системы, что затрудняет ее взлом. Многофакторная аутентификация является необходимой при электронном сборе статических данных как эффективный способ защиты системы. Технологии распределенного реестра позволяют создать дополнительную защиту при передаче данных и снижают вероятность похищения данных. При этом в целом технологии нейронных сетей как искусственно созданных технологий, которые сохраняют как машинные возможности, так и возможности к самообучению, создают эффективную защиту от утечки данных и способствуют сохранности информации, ускорению ее аналитики, внедрения технологий использования «больших данных» для проведения анализа социально-экономической статистической информации. При этом необходимо учитывать тот факт, что использование инструментов ИИ требует серьезной и продуманной работы по написанию алгоритмов для того, чтобы получить объективные данные, которые машинные технологии могут интерпретировать в зависимости от заданной задачи.

Выводы

Таким образом, по итогам проведенного исследования можно сделать следующие выводы.

Обеспечение информационной безопасности социально-экономической статистики является приоритетным направлением деятельности, необходимой для достаточного уровня защиты предоставляемой и обрабатываемой информации в условиях цифровой экономики.

Организация данной деятельности на настоящий момент направлена на создание новой парадигмы статистического наблюдения и включает в себя нормативно-правовой, технологический и кадровый аспекты, определяющие основные направления работы по созданию надежного уровня защиты информации.

Нормативный уровень включает в себя нормы федерального законодательства в сфере защиты информации, ее объективности и сохранности; стратегии развития ведомства по информационной безопасности, локальные документы. Основные нормативные положения отражены в Стратегии развития Росстата и системы государственной статистики РФ до 2024 года, в соответствии с которой внедряются форматы электронного сбора статистических данных, что способствует повышению точности и достоверности информации, скорости предоставления и экономии бюджетных средств при обработке данных.

Технологический уровень подразумевает наличие в организации необходимого современного отечественного ПО и технических средств обработки, передачи и сохранности информации.

Кадровый уровень является той базовой основой, которая создает достаточно высокий уровень компетенций сотрудников, который позволяет им эффективно выполнять свои должностные обязанности и соблюдать все нормы и правила информационной безопасности.

В условиях цифровой экономики защита социально-экономической статистической информации поддерживает деятельность «электронного правительства», является составным элементом национальной системы управления информацией, снижает нагрузку на бизнес и способствует интеграции информации на единых информационных ресурсах.

Основными инструментами создания информационной безопасности в сфере социально-экономической статистики являются инструменты искусственного интеллекта: многофакторная аутентификация, автоматизация сбора данных, облачное хранение информации, передача информации по защищенным каналам. Данная деятельность обеспечивает информационную безопасность перехода традиционной отчетности к новым источникам социально-экономических статистических данных.

Библиографический список

1. Конституция Российской Федерации // СПС Консультант. URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 11.04.2024).

2. ФЗ от 27.06.2006 №149 «Об информации, информационных технологиях и защите информации»// СПС Консультант. URL: http://www.cikrf.ru/izbiratel/normakt/zakon_inf.html (дата обращения: 14.04.2024).

3. ФЗ от 27.07.2006 г. № 152-ФЗ «О персональных данных» // СПС Консультант. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 12.04.2024).

4. Стратегия развития Росстата и системы государственной статистики РФ до 2024 г. URL: https://rosstat.gov.ru/storage/mediabank/Strategy.pdf (дата обращения: 12.04.2024).

5. Вострецова Е.В. Основы информационной безопасности: учебное пособие. Екатеринбург: Изд-во Урал. ун-та, 2019.

6. Искусственные нейронные сети: учебник / коллектив авторов; под ред. В.В. Цехановского. М.: КНОРУС, 2023.

7. Статистика: учебник для вузов / сост.: И.И. Елисеева и др. М.: Юрайт, 2024.

8. Статистика искусственного интеллекта. URL: https://inclient.ru/ai-stats/ (дата обращения: 12.04.2024).