

УДК 336.148

Е. А. Федченко

ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»,
Москва, e-mail: eafedchenko@fa.ru

Э. И. Дышекова

ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»,
Москва, e-mail: dyshekova.ellina@mail.ru

Н. А. Малышева

ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»,
Москва, e-mail: nataliyamalyshevaa@mail.ru

ФОРМИРОВАНИЕ МОДЕЛИ ЦИФРОВОЙ ЗРЕЛОСТИ ОРГАНОВ ГОСУДАРСТВЕННОГО ФИНАНСОВОГО КОНТРОЛЯ

Ключевые слова: государственный финансовый контроль, цифровизация, цифровая зрелость, государственные информационные системы, информационная безопасность.

В настоящее время особую актуальность приобретает цифровизация органов государственной власти, в том числе финансового контроля, поскольку информационные системы выступают ключевыми цифровыми средствами межведомственного информационного обмена, повышения прозрачности работы государственных органов и принятия наиболее эффективных и обоснованных управленческих решений. Такая ситуация диктует государственному финансовому контролю объективную необходимость в поиске новых, более совершенных и актуальных форм и методов цифрового контроля, а также в разработке новых подходов к решению теоретических, методических и практических задач контрольной деятельности, в том числе формирование модели цифровой зрелости. Предметом исследования выступают организационно-цифровые аспекты, влияющие на функционирование системы государственного финансового контроля. Объектом исследования признается система государственного финансового контроля, которая используется в настоящее время. Теоретическая обоснованность заключается в построении модели цифровой зрелости органов государственного финансового контроля, что позволит сделать вывод о цифровом развитии и перспективах цифровизации государственного управления.

Е. А. Fedchenko

Financial University under the Government of the Russian Federation, Moscow,
e-mail: eafedchenko@fa.ru

E. I. Dyshekova

Financial University under the Government of the Russian Federation, Moscow,
e-mail: dyshekova.ellina@mail.ru

N. A. Malysheva

Financial University under the Government of the Russian Federation, Moscow,
e-mail: nataliyamalyshevaa@mail.ru

FORMATION OF A MODEL OF DIGITAL MATURITY OF STATE FINANCIAL CONTROL BODIES

Keywords: state financial control, digitalization, digital maturity, state information systems, information security.

Currently, digitalization of public authorities, including financial control, is becoming particularly relevant, since information systems are key digital means of interdepartmental information exchange, increasing transparency in the work of government agencies and making the most effective and informed management decisions. This situation dictates the objective need for state financial control to search for new, more advanced and relevant forms and methods of digital control, as well as to develop new approaches to solving theoretical, methodological and practical tasks of control activities, including the formation of a model of digital maturity. The subject of the study is organizational and digital aspects that affect the functioning of the state financial control system. The object of the study is the system of state financial control, which is currently in use. The theoretical validity lies in building a model of digital maturity of state financial control bodies, which will allow us to draw a conclusion about digital development and the prospects for digitalization of public administration.

Введение

В настоящее время уделяется большое внимание цифровизации органов государственного управления, в том числе органам государственного финансового контроля, так как информационные системы являются ключевыми цифровыми инструментами межведомственного обмена информацией, повышения прозрачности деятельности государственных органов, принятия наиболее актуальных и точных управленческих решений.

В сложившихся условиях государственный финансовый контроль остро нуждается в поиске продвинутых форм и инструментов цифрового контроля, а также в создании новых способов решения методических и практических аспектов контрольной деятельности, включая разработку модели цифровой зрелости. Предметом исследования являются организационно-цифровые факторы, влияющие на функционирование системы государственного финансового контроля. Объектом исследования служит система государственного финансового контроля. Теоретическая значимость исследования заключается в построении модели цифровой зрелости органов государственного финансового контроля, что даст возможность оценить уровень цифрового развития и перспективы цифровизации государственного управления.

Цель исследования заключается в построении модели цифровой зрелости органов государственного финансового контроля, определяющую этапную реализацию, критериальный подход по выбранным блокам практической деятельности органов контроля.

Материалы и методы исследования

В ходе исследования применялись общенаучные методы исследования, такие как анализ и синтез, индукция и дедукция, наблюдение, системный и логический анализ, сравнение, систематизация практического материала, системный и комплексный подходы, метод формализации.

Результаты исследования и их обсуждение

В настоящее время органами контроля проводятся контрольные и экспертно-аналитические мероприятия по оценке цифрового развития органов государственного управления, представляются рекомендации по совершенствованию действующих государственных информационных сервисов.

Так Счетной палатой Российской Федерации проведено экспертно-аналитическое мероприятие «Оценка текущего состояния федеральных государственных информационных систем с точки зрения перспектив цифровизации государственного управления» [1] направленное на цифровую оценку текущего состояния федеральных государственных информационных систем. По итогам экспертно-аналитического мероприятия с использованием методологии управления информационными технологиями (COBIT) определено, что сложившийся механизм государственных информационных сервисов, превышающий по совокупной стоимости 296 млрд руб. требует доработки, совершенствования [2, 3]. Наиболее важные выводы, сделанные по итогам мероприятия, можно свести к следующим замечаниям (рисунок).

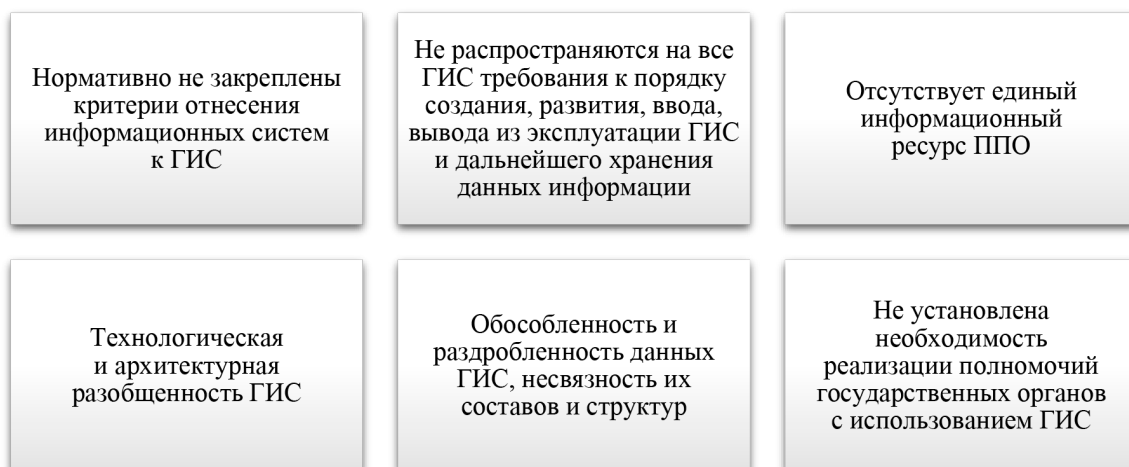


Рис. 1. Итоги проведенного экспертно-аналитического мероприятия [1]

В этой связи действующие наработки федеральных ГИС требуют совершенствования для дальнейшего цифрового развития организаций сектора государственного управления.

Если рассматривать цифровую зрелость Казначейства России, то следует отметить, что реализуется ведомственная программа цифровой трансформации Федерального казначейства на 2024 год и плановый период 2025–2026 годов по направлению (подпрограмма) «Повышение качества управления бюджетным процессом и эффективности управления общественными финансами» на 2022–2030 годы.

Федеральное казначейство за 2024 год обеспечило достижение всех результатов, контрольных точек и показателей ГП Российской Федерации «Управление государственными финансами и регулирование финансовых рынков», заключающиеся в следующем:

1) посещаемость цифровых информационно-аналитических сервисов, востребованных участниками бюджетного процесса при обеспечении исполнения федерального бюджета, казначейском обслуживании, организации учета и распределения поступлений, в 2024 году составила 16,3 млн штук (при плановом значении показателя – 14 млн штук);

2) доля цифровых сервисов, которые реализованы с использованием информационных систем и используются физическими и юридическими лицами для платежей за оказание государственных и муниципальных услуг, в 2024 году составила 92 % (при плановом значении показателя – 91 %);

3) доля отечественного программного обеспечения и компонентов, используемых в ведомственных информационных системах, в 2024 году составила 93,8 % (при плановом значении показателя – 93,5 %);

4) доля современных средств ИТ-инфраструктуры, используемых в процессах эксплуатации и развития государственных и ведомственных информационных систем в 2024 году составила 82,1 % (при плановом значении показателя – 82 %);

5) доля обработанных заявлений на получение квалифицированных сертификатов электронных подписей, в 2024 году составила 99,9 % (при плановом значении показателя – 96,5 %);

6) доля лицевого счета для учета операций администраторов доходов бюджетов,

операции по которым переведены в подсистему управления доходами ГИИС «Электронный бюджет» из ИС АСФК, в 2024 году составила 6,1 % (при плановом значении показателя – 6,1 %);

7) доля размещенных в ГИС ГМУ планов финансово-хозяйственной деятельности с целью осуществления контроля закупочной деятельности учреждений в 2024 году составила 100 % (при плановом значении показателя – 100 %);

8) среднегодовое предельное значение остатка средств на ЕКС в 2024 году составило 232,1 млрд руб. (при плановом значении показателя – не более 500 млрд руб.);

9) уровень качества контрольных мероприятий в 2024 году прогнозируется на уровне 94 % (при плановом значении показателя – 93 %) и т.д. [4].

Можно сделать вывод, что обеспечена реализация мероприятий ведомственной программы цифровой трансформации Казначейства России на 2024 год и плановый период 2025–2026 годов, с достижением 100% установленных на 2024 год значений показателей. В этой связи дальнейшее развитие ведомственного проекта должно быть ориентировано на совершенствование отдельных процессов с целью повышения эффективности и оптимизации деятельности в рамках реализации поставленных задач.

Отметим, что распоряжением Правительства Российской Федерации от 16.03.2024 № 637-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления» утверждена цифровая стратегия органов государственного управления, определены индикаторы цифровой трансформации, бенефициары стратегического направления, показатели проектов стратегического управления.

Цифровая трансформация направлена на полный переход электронного документооборота, автоматизацию и упрощение межведомственного взаимодействия с созданием единого информационного пространства, формирование автоматизированного рабочего места государственного служащего с отечественным ПО, цифровой архивный учет, роботизацию бюджетного процесса, централизацию данных в ГИИС «Электронный бюджет».

Поскольку цифровая трансформация выступает ключевым направлением развития органов государственного управления, в том

числе органов государственного финансового контроля необходимо предложить цифровую оценку зрелости [5].

Отметим, что в научных исследованиях по-разному подходят к определению цифровой зрелости. Так Кричевский М.Л. предложил «модель оценки цифровой зрелости организации посредством генерации выбранных факторов, участвующих в построении оценки. В качестве входных факторов выбраны следующие параметры: корпоративная культура (отношение организации к цифровым инновациям); технологии (применяемые компанией информационно-коммуникативные технологии); организация (сформулированная и реализуемая стратегия в части цифровой трансформации); инсайты (способ использования данных о внутренних бизнес-процессах при принятии решений). Выходными переменными являлись категории цифровой зрелости» [10]. Шкарупета Е.В. представила видение цифрового паспорта промышленного предприятия ГИСП из трех «колодцев», 27 направлений и 123 поднаправлений оценки, результатов оценки уровня цифровой зрелости 8 лидеров промышленной цифровизации, а также уровней цифровой зрелости в разрезе основных, вспомогательных и технологических процессов. Дополнительно конкретизировала уровень цифровой зрелости по направлению искусственного интеллекта. Отметила, что «цифровая зрелость – есть целевой образ результата, а цифровая готовность должна рассматриваться как совокупность цифровых навыков и знаний сотрудников предприятий, их цифровой грамотности, а также доверия к сервисам, внедряемым в ходе цифровой трансформации» [11].

Афанасьев А.А. дал «характеристику методики оценки цифровой зрелости промышленного производства, реализованной с целью мониторинга достижения национальной цели по цифровой трансформации» [12]. По нашему мнению, все авторы доказывают, что цифровая зрелость должна определяться показателями достижения национальных целей по определенным отраслевым направлениям.

Цифровая зрелость государственных органов определяется показателями достижения национальных целей, утв. Указом Президента РФ от 21.07.2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года». Так приказом Минцифры России от 28.12.2024

№ 1210 «Об утверждении методики расчета показателя «Достижение «цифровой зрелости» государственного и муниципального управления, ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, предполагающей автоматизацию большей части транзакций в рамках единых отраслевых цифровых платформ и модели управления на основе данных с учетом ускоренного внедрения технологий обработки больших объемов данных, машинного обучения и искусственного интеллекта» государственной программы Российской Федерации «Информационное общество» определены алгоритмы расчета показателей цифровой зрелости и показатели (ЦЗгос – достижение «цифровой зрелости» государственного и муниципального управления; ЦЗсоц – достижение «цифровой зрелости» ключевых отраслей социальной сферы; ЦЗЭК – достижение «цифровой зрелости» ключевых отраслей экономики). Компонент ЦЗгос рассчитывается согласно методике расчета показателя «Достижение «цифровой зрелости» государственного и муниципального управления» ФП «Цифровое государственное управление» НП «Экономика данных и цифровая трансформация государства». Достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы оценивается на основании индикаторов, перечень которых формируется индивидуально для каждой отрасли. Перечень индикаторов, характеризующих достижение «цифровой зрелости» на 2030 г., а также методики расчета каждого из индикаторов утверждаются президиумом Правительственной комиссии по цифровому развитию после согласования с органами исполнительной власти по соответствующим отраслям.

В настоящее время органы государственного финансового контроля могут определять цифровую зрелость по следующим индикаторам, определяющих функциональную, профессиональную значимость и достижения показателей национальных целей, это *цифровые сервисы, кадровый потенциал, цифровая организационная культура, качество профессионально-функционального обеспечения, качество профессионально-информационного обеспечения, качество цифровых данных, защита-безопасность цифровой информации*. Считаю целесообразным введение перечня критериев для обоснованной оценки каждого из блоков

(таблица 1). При этом интегральная оценка цифровой зрелости органа контроля будет представлять средневзвешенное значение указанных критериев:

$$ЦЗ_{\text{сп}} = \frac{\sum_{i=1}^7 X_i \times a_i}{\sum_{i=1}^7 a_i},$$

где X_i – оценка соответствующего блока,
 a_i – удельный вес, присваиваемый каждой оценке.

Уровень удельного веса должен устанавливаться самостоятельно каждым контрольным органом в соответствии с соблюдением принципа независимости. Оценка цифровой зрелости по данным критериям будет более объективной и позволит реально оценить темпы цифровизации органа государственного финансового контроля [6, 7].

В табл. 2 представим модель цифровой зрелости органа государственного финансового контроля, сформированную из ключевых блоков и уровню достижимости зрелости. Модель цифровой зрелости органа государственного финансового контроля может быть интегрирована во внутренние документы, регламентирующие организационные аспекты или годовой план деятельности контрольного органа.

Интересно останавливаться на блоке «Защита-безопасность цифровой информации», то необходимо реализовывать комплексные меры, которые включают разра-

ботку и внедрение политики безопасности, которая охватывает как информационную сферу, так и финансовую, которая является неотъемлемой частью обеспечения целостности, конфиденциальности, доступности информации. Основой политики информационной безопасности является принцип законности, многоуровневой защиты, адаптивности, комплексности. Ее ключевые элементы включают анализ рисков и угроз, соблюдение нормативных требований, обучение персонала, регулярный аудит, а также управление доступом. Разработка и внедрение политики безопасности является неотъемлемой частью обеспечения безопасности.

Если рассматривать технические методы, то возможно использовать криптографическую защиту. А именно шифрование данных (далее – AES, RSA), которое представляет шифрование, которое преобразует исходные данные в зашифрованный вид, доступ к которым могут получить только те, у кого на это есть право пользования. В современных системах самыми эффективными считаются AES и RSA. AES (Advanced Encryption Standard) – это симметричный блочный алгоритм шифрования, который использует 128-битные блоки данных и ключи длиной 128, 192 или 256 бит, применяя многократные раунды перестановки и замены для обеспечения криптостойкости. Блоки обрабатываются независимо друг от друга, что увеличивает скорость работы, но при этом его безопасность зависит от надежного хранения ключа.

Таблица 1

Перечень критериев для обоснованной оценки каждого блока цифровой зрелости органа государственного финансового контроля

Ключевые блоки	Критерии
Цифровые сервисы	Доля цифровых сервисов, реализуемых контрольными органами в общем числе проектов
Кадровый потенциал	Балльная система оценивания сотрудников контрольного органа по применению цифровых технологий
Цифровая организационная культура	Интегральная оценка на основе опроса работников к внедрению цифровых решений
Качество профессионально-функционального обеспечения	Уровень вовлеченности работников в реализуемые цифровые практики в общем числе сотрудников
Качество профессионально-информационного обеспечения	Интегральная оценка качества доступности и удобства облачных систем и автоматизированных платформ
Качество цифровых данных	Интегральная оценка качества доступности цифровых данных
Защита-безопасность цифровой информации	Доля применяемых систем защиты информации, информационных систем в общем объеме цифровых сервисов

Источник: составлено авторами на основе [6, 8].

Таблица 2

Модель цифровой зрелости органа государственного финансового контроля

Блоки	Цифровая организационная культура	Кадровый потенциал	Качество профессионального обеспечения	Цифровые сервисы	Защита-безопасность цифровой информации	Качество цифровых данных	Качество профессионального информационного обеспечения
Уровень	Ориентированность на развитие «перекрестных» цифровых навыков: создание цифрового взаимодействия с другими государственными органами, занимающимися управлением финансами, с целью повышения общей цифровой зрелости в сфере финансов и бюджета.						
Уровень 5 – Развивающейся	Готовность персонала к инновациям и постоянному совершенствованию	Наличие цифровых компетенций у каждого работника	Связь применяемых практик процессного управления с трендами цифровизации	Цифровые продукты успешно применяются практически в каждом реализуемом проекте/мероприятии	Применяются система защиты информации, информационные системы	Системный доступ к необходимым информационным данным	Доступность и удобство облачных систем и автоматизированных платформ
Уровень 4 – Системный	Большая часть сотрудников готовы к цифровизации, часть сотрудников настроены негативно	Большинство работников обладают базовыми цифровыми компетенциями, лишь некоторые являются продвинутыми пользователями ИТ	Процессное управление осуществляется посредством использования информационных платформ, но сами процессы могут быть не связаны с цифровизацией	Цифровые инструменты внедряются всеми структурными подразделениями, но используются при осуществлении определенных мероприятий	Внедряется система обучения сотрудников базовым инструментам защиты информации	Налажена система информационного обеспечения, доступ к большей части данных	Облачные системы просты и понятны в использовании, однако отдельные модули требуют наличия дополнительных навыков от пользователей
Уровень 3 – Определенный	Положительно настроены к инновациям только сотрудники подразделений, ответственных за цифровизацию	Цифровыми навыками обладают только сотрудники подразделений, ответственных за цифровизацию	Малая часть практик процессного управления связана с цифровыми инструментами	Отсутствие собственных цифровых инструментов	Защита информации применяется только сотрудниками подразделений, ответственных за цифровизацию	Наличие существенных проблем доступа к необходимым цифровым данным	Облачные системы и информационные платформы неудобны, значительная часть сотрудников сталкивается с трудностями их использования
Уровень 2 – Производный	Необходимость цифровой трансформации деятельности не всегда осознаётся, что приводит к ряду проблем. Сотрудники могут проявлять сопротивление внедрению цифровых инструментов, испытывая недостаток квалификации для их использования. Кроме того, наблюдается дефицит специалистов, способных работать со статистическими данными и математическими моделями. В организации также отсутствуют автоматизированные информационные системы, что усложняет управление и анализ данных.						

Источник: составлено авторами на основе [8].

В свою очередь RSA, является асимметричный алгоритмом, который основывается на сложности факторизации больших чисел. Используется пара ключей: открытый для шифрования и проверки подписи, а закрытый для расшифрования и подписи данных. Длина ключа варьируется от 1024 до 4096 бит. RSA более надежен с точки зрения передачи ключей и подписей, но при этом уступает в скорости AES.

Для достижение максимальной безопасности и производительности в рамках информационных систем можно использовать комбинацию данных шифрования.

Использование электронной цифровой подписи также является способом защиты от утечки данных. В соответствии с законодательством на данный момент применяются три вида электронной подписи: простая, усиленная неквалифицированная, усиленная квалифицированная. В отношении которых так же применяется криптография, то есть для усиления защиты можно так же применять более сложное шифрование, в то же время можно использовать многофакторную аутентификацию: биометрию, пароль, аппаратный токен, одноразовый пароль и т. д. Необходимо устанавливать срок действия ключа и регулярно его обновлять.

Для безопасного хранения ключей шифрования используются аппаратные модули безопасности HSM (hardware security module), которые также предназначены для выполнения криптографических операций. В системах HSM интегрируется для защиты данных, документооборота, электронной цифровой подписи, а также в системах межведомственного взаимодействия.

Внедрение средств сетевой безопасности, например Firewall (Межсетевой экран), который обеспечивает фильтрацию трафика для предотвращения атак и мониторинга активности обеспечивает сегментацию внутренних ресурсов, защищает периметр сети, там самым предотвращает утечку данных. Регулярное обновление политики безопасности и тестирование защиты безопасности снижает киберриски [7, 9].

В дополнение можно интегрировать систему обнаружения и предотвращения вторжений, например IDS или IPS. IDS (Intrusion Detection System) проводит анализ сетевого и системного трафика, в процессе выявляя аномалии и потенциальные угрозы. А IPS (Intrusion Prevention System) в свою очередь не только обнаруживает атаки, но и автома-

тически их блокирует в режиме реального времени. В государственных информационных системах данные технологии могут защитить базы данных финансовой отчетности, предотвратить атаки на веб ресурсы, а также контролировать действия пользователей, тем самым выявлять попытки несанкционированного доступа и проводя анализ поведенческих аномалий [7, 9].

При интеграции данных систем с Firewall, возможно достижение эффективной защиты. Так же IDS/IPS при использовании технологий машинного обучения могут прогнозировать атаки и адаптироваться к новым видам угроз. Для безопасности ключей можно внедрить квантовое распределение, который представляет собой метод передачи криптографических ключей и основывается на принципах квантовой механики, тем самым обеспечивает абсолютную безопасность благодаря тому, что механически невозможно незаметно перехватить ключ. Его отличие от других алгоритмов в том, что любое вмешательство изменяет квантовые состояния фотонов и мгновенно обнаруживается. Создание национальной квантовой сети в интеграции квантового распределения с другими современными криптосистемами, позволит обеспечить квантовую устойчивость и высокую производительность, при этом минимизируя возможность утечки данных. При использовании современных технологических решений, шифрования и систем возможно обеспечить безопасность имеющихся данных от внешних и внутренних угроз. Грамотное внедрение и использование имеющихся механизмов предотвратит несанкционированное проникновение в базы данных и обеспечит максимальный контроль за системой.

Заключение

Основу совершенствования системы государственного финансового контроля составляет цифровая трансформация, в этой связи предлагаемая модель цифровой зрелости будет положена в основу достижения KPI руководителями органов государственного финансового контроля. Модель цифровой зрелости включает ключевые блоки, критериальный подход к блокам, эволюционные этапы цифровой зрелости и аналитические показатели. В этой связи предлагаемые направления совершенствования системы государственного финансового контроля направлены на использование и развитие

цифровых инструментов защиты информации, информационных систем, позволяющих не только оптимизировать рутинные задачи и сократить трудовые затраты сотрудников органов контроля, но и обеспечить своевременность выявления нарушений и рисков финансово-бюджетной сферы, получать обоснованные результаты оценки контрольных и экспертно-аналитических мероприятий. В то же время ставится вопрос о развитии государственных информацион-

ных сервисов органов государственного финансового контроля, повышении цифровой культуры сотрудниками, создания единого информационного ресурса, содержащего сведения об услугах, функциях и полномочиях федеральных органов исполнительной власти и государственных внебюджетных фондов Российской Федерации, создании технологической и архитектурной интеграции государственных информационных систем, цифровых данных.

Библиографический список

1. Отчет о результатах экспертно-аналитического мероприятия «Оценка текущего состояния федеральных государственных информационных систем с точки зрения перспектив цифровизации государственного управления» [Электронный ресурс]. URL: <https://perquogiajfxi8zvbspqzmdzl03uzk.pdf> (дата обращения: 20.03.2025).
2. О цифровой трансформации Счётной палаты РФ в 2022 году [Электронный ресурс]. URL: <https://О цифровой трансформации Счётной палаты РФ в 2022 году. Digital Russia> (дата обращения: 25.02.2025).
3. Отчет о работе Счетной палаты Российской Федерации в 2023 году [Электронный ресурс]. URL: <https://2s9l597z2ddcymmd4c34y25090vcvatc.pdf> (дата обращения: 25.02.2025).
4. Проект итогового доклада о результатах деятельности Федерального казначейства за 2024 год и основных направлениях деятельности на среднесрочную перспективу. Информация официального сайта Федерального казначейства: [Электронный ресурс]. URL: https://roskazna.gov.ru/upload/iblock/dad/Itogovyy-doklad-za-2024-god_.docx?ysclid=m8ixfrufq411219399 (дата обращения: 25.02.2025).
5. Федченко Е.А. Развитие стандартизации внутреннего государственного финансового контроля // Вестник Алтайской академии экономики и права. 2024. № 8–2. С. 353–359.
6. Государственный контроль в финансово-бюджетной сфере / Э.А. Исаев, С.А. Андреев, И.М. Ванькович и др. М.: Прометей, 2023. 648 с.
7. Межсетевые экраны: новое поколение [Электронный ресурс]. URL: <https://Межсетевые экраны: новое поколение // Журнал сетевых решений / LAN. Издательство «Открытые системы»> (дата обращения: 20.03.2025).
8. Клейтон Д., Риддл К., Арай Ф.Д. и др. Внутренний аудит по Сойеру: сохранение и повышение стоимости организаций: учебное пособие / перевод с английского // Институт внутренних аудиторов. 7-е изд. М.: Internal Audit Foundation, 2019. 380 с.
9. Стихаенко Р.М., Гаев Л.В. Нейронные сети в сфере кибербезопасности: обнаружение и предотвращение кибератак // Инновационные исследования: проблемы внедрения результатов и тенденции развития: Сборник статей по итогам Международной научно-практической конференции, Пермь, 24 декабря 2023 года. Sterlitamak: ООО «Агентство международных исследований», 2023. С. 188–191.
10. Кричевский М.Л., Мартынова Ю.А., Дмитриева С.В. Оценка цифровой зрелости предприятия // Вопросы инновационной экономики. 2022. Т. 12, № 4. С. 2545–2560.
11. Шкарупета Е.В. Практические аспекты оценки цифровой зрелости промышленных предприятий в условиях пилотирования инноваций в цифровых сервисах ГИСП // Информатизация в цифровой экономике. 2023. Т. 4, № 1. С. 9–22.
12. Афанасьев А.А. Оценка цифровой зрелости промышленного производства в контексте его цифровой трансформации // Экономика, предпринимательство и право. 2024. Т. 14, № 7. С. 3595–3612.