УДК 336.025, 004.451

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЦИФРОВОГО ПРОСТРАНСТВА (ОПЫТ НАЛОГОВЫХ ОРГАНОВ)

М.А. Троянская, А.А. Астаев, А.Д. Троянская
Оренбургский государственный университет, Оренбург, email: m_troyanskaya@mail.ru

Аннотация. *В настоящее время в России реализуется задача цифровизации государственного аппарата, чтобы построить современную информационную систему для экономики и социальной сферы. Эта трансформация коснулась и налоговой сферы, где внедряются цифровые технологии для упрощения и ускорения взаимодействия с гражданами. В налоговой сфере цифровизация проявляется в электронных услугах, создании «Личного кабинета налогоплательщика» и переходе к безбумажному документообороту, что помогает повысить эффективность контроля, например, через автоматизированную систему контроля налога на добавленную стоимость (НДС). В налоговом мониторинге внедряется риск-ориентированный подход, позволяющий учитывать специфику отраслей и акцентировать внимание на операциях с высоким риском. Проходит модификацию проект по интеграции корпоративных информационных систем с автоматизированной системой «Налог-3». Процедуры налогового контроля автоматизируются через системы АСК «НДС-2» и АСК «НДС-3». Дополнительно внедряются онлайн-кассы, мобильные приложения для самозанятых, развиваются «Личный кабинет налогоплательщика» и ресурс бухгалтерской отчетности. Приложение «Мой налог» отличается удобством регистрации и аналитикой для граждан и бизнеса, позволяя изменять режим налогообложения без посещения налогового органа. Все цифровые новшества реализуются с учетом требований по информационной безопасности, чтобы обеспечить защиту данных при электронном взаимодействии. Предоставление госуслуг через сайт ФНС и портал «Госуслуги» максимально упростило работу с налоговыми органами. В связи с указанными факторами возникает потребность исследовать направления развития деятельности налоговых органов в рамках обеспечения безопасности и определение перспективных направлений ее развития.*

Ключевые слова*: цифровое пространство, информация, информационная безопасность, налоговые органы, цифровизация, клиентоцентричность, налоговое администрирование.*

ENSURING THE SECURITY OF THE DIGITAL SPACE (EXPERIENCE OF TAX AUTHORITIES)

M.A. Troyanskaya, A.A. Astaev, A.D. Troyanskaya
Orenburg State University, Orenburg, email: m_troyanskaya@mail.ru

Abstract. *Currently, Russia is implementing the task of digitalizing the state apparatus in order to build a modern information system for the economy and the social sphere. This transformation has also affected the tax sector, where digital technologies are being introduced to simplify and accelerate interaction with citizens. In the tax sphere, digitalization is manifested in electronic services, the creation of a "Taxpayer's Personal Account" and the transition to paperless document management, which helps to increase the effectiveness of control, for example, through an automated value added tax (VAT) control system. A risk-based approach is being introduced in tax monitoring, which allows taking into account the specifics of industries and focusing on high-risk transactions. The project for the integration of corporate information systems with the automated Tax-3 system is undergoing modification. Tax control procedures are automated through the VAT-2 and VAT-3 tax control systems. Additionally, online sales registers, mobile applications for the self-employed are being introduced, a "Taxpayer's Personal Account" and an accounting reporting resource are being developed. The My Taxes app is convenient for registration and analytics for citizens and businesses, allowing them to change the tax regime without visiting a tax authority. All digital innovations are implemented taking into account information security requirements to ensure data protection during electronic interaction. The provision of public services through the FTS website and the Gosuslugi portal has made working with tax authorities as easy as possible. In connection with these factors, there is a need to explore the directions of development of the activities of tax authorities in the framework of ensuring security and identifying promising areas for its development.*

Keywords: *digital space, information, information security, tax authorities, digitalization, client-centricity, tax administration.*

Дата поступления статьи в редакцию: 05.11.2025
Дата принятия статьи в печать: 03.12.2025

Введение

Актуальность исследования обусловлена тем, что преобразования в экономике России невозможны без совершенствования работы государственного сектора и особенно налоговых органов, обеспечивающих основную часть доходов бюджета. Именно поэтому цифровизация налоговой сферы становится ключевым направлением для повышения прозрачности, улучшения условий бизнеса и сокращения теневого сектора. По итогам 2024 года ФНС России отметила рост использования своих цифровых сервисов, так чат-бот «Таксик» активно используется для получения информации, выросли доля электронных деклараций и уровень удовлетворенности граждан услугами. В 2024 году ФНС России протестировала цифровую кадровую платформу, внедрила веб– и мобильные приложения для развития кадрового резерва и обучила почти 14 тысяч сотрудников человекоцентричности, поднявшись на первое место в стране по этому показателю. Количество востребованных цифровых сервисов увеличилось, а ведомство стало лидером по клиентоцентричности среди федеральных органов.

Проблема, затронутая в данной статье, является достаточно разработанной. Первая группа исследований посвящена проблематике развития деятельности налоговых органов в условиях цифровой среды [1-4]. Вторую группу исследований образуют работы отечественных ученых, изучающих вопросы комплексного обеспечения безопасности при деятельности экономических агентов [5-7]. Третья группа исследований объединяет в себе труды, посвященные проблемам обеспечения информационной безопасности налоговых органов [8, 9]. Однако, системных научных работ, исследовавших направления развития деятельности налоговых органов в рамках обеспечения комплексной безопасности в современных условиях, в настоящее время еще не проводилось, что свидетельствует об актуальности и своевременности исследования.

Результаты исследования

Цифровизация налоговых правоотношений приводит к расширению числа их участников, включая иностранные компании и новых посредников в лице операторов электронного документооборота и других специализированных организации. Это существенно меняет функционирование налоговой системы и требует правового регулирования новых цифровых процессов, в том числе в части обеспечения безопасности цифрового пространства. В научно-исследовательских работах налоговые органы рассматриваются в качестве субъекта обеспечения безопасности цифрового пространства при реализации налогового администрирования.

С точки зрения управления, налоговое администрирование в широком смысле раскрывает его суть, включая не только контроль, но и прогнозирование поступлений, координацию органов и оптимизацию налоговых ставок. Тем не менее, контроль остается ключевой функцией налогового администрирования, хотя существуют и другие важные задачи. Вопрос о функциях налогового администрирования является теоретическим, и среди исследователей существуют разные взгляды на этот счет. Наиболее логичной считается позиция М.В. Мишустина, который относит к функциям налогового администрирования планирование, организацию, мотивацию и контроль, применяя подход классической теории управления, однако подчеркивает, что в налоговой сфере все эти функции подчинены контрольной [10]. Хотя в настоящее время в практике все больше уделяется внимания клиентоориентированному подходу и внедряются цифровые технологии, благодаря которым отношения между налогоплательщиками и налоговыми органами становятся проще и удобнее, это не меняет сути самого понятия налогового администрирования. Основные функции – контроль, планирование, организация и мотивация – сохраняются, а цифровизация лишь добавляет новые способы их осуществления.

Несмотря на то, что цифровизация играет важную роль в современной экономике, большинство научных работ обращается к вопросам использования цифровых технологий лишь частично, в основном фокусируясь на оптимизации контроля, например, за счет сбора данных о деятельности налогоплательщиков. Также изучаются вопросы доверия, налоговой культуры и дисциплины, что связано с контрольной функцией, но выходит за ее пределы. Таким образом, даже аспекты, не связанные непосредственно с цифровыми технологиями, например, проблемы обеспечения безопасности в цифровом пространстве, имеют значение, потому что их развитие может быть существенно улучшено с применением новых цифровых решений, что позволяет снизить издержки и повысить эффективность налогового администрирования.

Информационное взаимодействие в ФНС России осуществляется между центрами обработки данных, подразделениями внутри одного органа, между налоговыми органами различных уровней, а также с внешними организациями и налогоплательщиками. Архитектура информационных систем стро-

ится на централизации вычислительных данных и хранилищ информации, где все объекты обращаются к централизованным сервисам в специализированных филиалах. ФНС активно обменивается данными с разными государственными и финансовыми структурами по защищенным каналам связи, используя современные средства и соглашения. В структуру информационных систем входят такие элементы, как АИС «Налог-3», федеральные информационные адресные системы и реестры актов гражданского состояния, а защита информации обеспечивается для каждого объекта индивидуально через отдельные системы безопасности.

Появление новых задач спровоцировало трансформацию информационной инфраструктуры ФНС, развитие новых ИТ-комплексов и доработку существующих систем, что, в свою очередь, подчеркнуло необходимость дальнейшей модернизации и унификации архитектуры. В процессе автоматизации дополнительных функций особое внимание уделяется тиражируемости решений, единому информационному пространству, требованиям к отчуждаемости, доступности и импортозамещению компонентов. Общий подход направлен на то, чтобы каждая система легко интегрировалась, могла работать автономно при необходимости и была устойчива к сбоям. При проектировании акцент делается на создание абстрактных слоев для интеграции, четкое распределение общих ресурсов, использование российских ИТ-решений и создание максимально доступной и независимой от отдельных компонентов архитектуры. Все это ведет к необходимости дальнейшей централизации и адаптации архитектуры систем безопасности.

С 2017 года ФНС России внедряет работу компонентов своих информационных систем в георасределенном режиме между основным и резервным центрами обработки данных: главным ЦОД в Дубне и резервным в Городце. Требования к катастрофоустойчивости предусматривают «бесшовное» переключение между площадками с простоем системы не более суток и допустимой потерей данных не более одного часа. Оба центра связаны высокоскоростным каналом, хотя их мощность может различаться и не все подсистемы обязательно размещаются на обеих площадках. Для повышения надежности ключевые компоненты теперь масштабированы между Дубной и Городцом, что позволяет создать в рамках цельного информационного пространства гео-кластер с дублированием основных элементов и равномерным распределением нагрузки. Благодаря этому пользователи работают с системой как с единым центром обработки данных без необходимости самостоятельно переключаться между площадками. Этот подход сокращает время восстановления системы при сбоях и минимизирует возможные простои или потери данных. Однако, в Концепции системы управления информационной безопасностью ФНС России указывается, что требуется доработать средства обеспечения информационной безопасности, чтобы адаптировать их к новому режиму и учесть возможный рост лицензионных и аппаратных требований из-за дублирования защитных мер.

Организационная база системы обеспечения безопасности информации строится на сотрудниках центрального аппарата ФНС России, налоговых органов, подведомственных и других организаций, которые реализуют и контролируют политику информационной безопасности, применяя комплекс мер противодействия угрозам. Руководство системой осуществляет руководитель ФНС России, а методологию и координацию – Управление информационной безопасности. Ключевую роль в поддержании защиты играют администраторы информационной безопасности, которые отвечают за реализацию мероприятий по защите информации, применение защитных средств и контроль доступа. Также рассматриваемая структура включает работников подразделений, занимающихся мониторингом состояния информационной безопасности и контролем исполнения процессов. Все сотрудники ФНС и подведомственных организаций реализуют комплекс мер противодействия угрозам, следуют положениям политики информационной безопасности и строго соблюдают правила защиты. В структуре организационной базы особое место занимает Управление информационной безопасности ФНС, которое определяет методологический подход для всей системы.

Подразделения информационной безопасности ФНС России и подведомственных организаций выполняют функции администрирования безопасности информации и управляют системой обеспечения безопасности информации на своих участках, несут ответственность за комплексное администрирование, то есть должны увязывать управление безопасностью с администрированием информационных процессов. Для повышения эффективности работы в этой области планируется расширять штат сотрудников, повышать их квалификацию и централизовать функции защиты информации. Особое внимание уделяется регулярной подготовке и переподготовке персонала, а также обучающим тренингам, особенно при изменениях в информационных системах или внедрении новых технологий. Организационную основу деятельности составляют документы, иерархия которых представлена на рисунке 1.

Рис. 1. *Схема организационно-распорядительных документов ФНС России при обеспечении безопасности в цифровом пространстве*

Источник: составлено авторами по данным [11].

При этом на каждом объекте могут использоваться дополнительные документы, если они не противоречат общей политике ФНС России в области информационной безопасности и действующему законодательству России.

Система управления информационной безопасностью строится на основе единой организационной базы и работает по принципу иерархичности и непрерывности, что позволяет охватывать все этапы обращения защищаемой информации. Такая система обеспечивает координацию, контроль действий по обеспечению информационной безопасности, взаимодействует с компетентными органами, управляет рисками, проводит аудит эффективности, предъявляет требования к модернизации механизмов защиты и анализирует результаты их применения. Для повышения эффективности управления создан Центр управления безопасностью информации, который централизует ключевые задачи, включая мониторинг, расследование инцидентов, создание системы аутентификации и контроль доступа пользователей к информационным системам ФНС России.

В информационных системах ФНС России при использовании средств криптографической защиты информации необходимо обеспечивать постоянное протоколирование их работы и контроль целостности программного обеспечения для всех элементов, использующих такие средства. Все криптографические ключи должны быть надежно защищены от несанкционированного доступа, хищения, уничтожения или раскрытия, а оборудование, применяемое для работы с ключами, должно иметь физическую защиту. Для уменьшения рисков компрометации ключей устанавливаются конкретные сроки их действия, чтобы они использовались только ограниченное время. Особое внимание уделяется развитию электронных подписей, которые обеспечивают целостность и подлинность данных, при этом необходимо учитывать, что пользователи могут выступать потенциальными нарушителями. Все используемые средства криптографической защиты информации должны соответствовать техническим регламентам, сопровождаться полной документацией и быть сертифицированы Федеральной службой безопасности (ФСБ) России. Встраивание средств криптографической защиты информации в прикладные системы допускается только по согласованию с ФСБ и при проведении требуемых оценок [12]. Использование несертифицированных средств криптографической защиты и программного обеспечения строго запрещено. Кроме того, в соответствии с положениями Концепции системы управления информационной безопасностью ФНС России, средства криптографической защиты информации должны быть интегрированы в схемы электронного документооборота ФНС России, взаимодействовать с программами по определенным требованиям и обеспечивать специальные процедуры по работе с ключами.

Системы обеспечения безопасности информации на физическом уровне в условиях функционирования ФНС России создают защищенную оболочку вокруг объектов информатизации. На технологическом уровне формируется надежная программная и аппаратная защита информационных систем ФНС России. Исполнительные и поддерживающие механизмы на пользовательском уровне допускают к работе только авторизованных пользователей, а также обеспечивают защиту рабочих станций, серверов и индивидуальных пользовательских сред. На сетевом уровне эти механизмы разделяют информационные ресурсы и средства их обработки на отдельные зоны и сегменты, организуют защищенный обмен между ними и ограничивают точки взаимодействия. На канальном уровне обеспечивается внешняя защитная оболочка информационных систем ФНС, а также организуется защищенный обмен информацией с государственными органами, удаленными, мобильными и внешними пользователями. Для защиты информации используются криптографические средства, которые обеспечивают конфиденциальность, подлинность и целостность данных, а необходимость их применения определяет руководство ФНС России.

Для централизованной обработки данных в информационных системах ФНС России создана система центров обработки данных Минфина России и подведомственных федеральных органов, в которую входят Федеральный и Резервный центры обработки данных, расположенные в Московской и Нижегородской областях. Эти центры и, при необходимости, другие объекты информатизации объединены в единую регионально-распределенную систему, представляющую собой виртуальный центр обработки данных. Для размещения информационных систем ФНС России такой центр должен быть аттестован по требованиям информационной безопасности согласно установленным нормативам. За выполнение задач по информационной безопасности центра отвечает система обеспечения безопасности информации, внедряемая в каждом центре обработки данных. Технологические процессы и приложения распределяются между центрами, а связь между ними осуществляется по защищенным логическим каналам с использованием современных стандартов и криптографических средств защиты. Для организации изолированных сегментов применяются виртуальные локальные сети, а обмен данными между сегментами контролируется межсетевыми экранами, которые создаются как распределенные кластеры. Во всей виртуальной инфраструктуре используются сертифицированные средства защиты виртуальной среды и сетевого трафика. Коммуникации между элементами информационной системы внутри центра четко описываются профилями технологических процессов, вместо привычных правил межсетевого экранирования.

В целях достижения целей обеспечения информационной безопасности в ФНС России реализуется перечень мероприятий, обеспечивающий противодействие утечкам сведений конфиденциального характера (рис. 2).

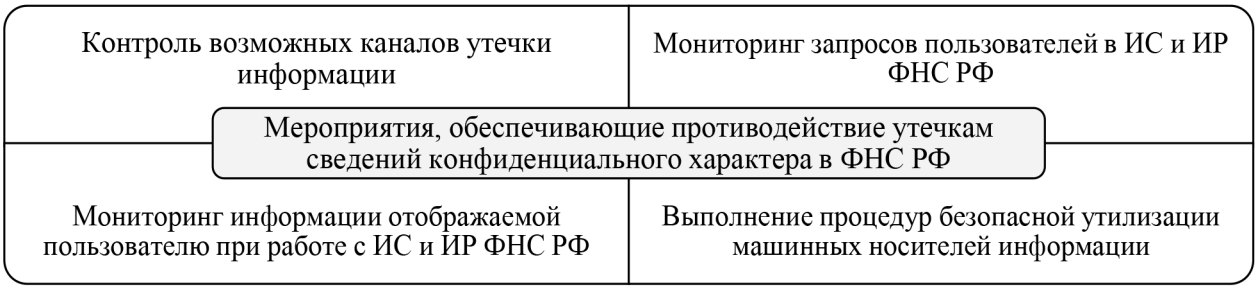

Рис. 2. *Перечень мероприятий, обеспечивающий противодействие утечкам сведений конфиденциального характера в ФНС России*

Источник: составлено авторами по данным [11].

Как видно из рисунка 2, для предотвращения утечки информации в информационных системах ФНС России необходимо реализовывать средства контроля на всех точках взаимодействия с внешней средой, таких как выходы в интернет и использование съемных носителей. При необходимости должны применяться меры защиты данных, передаваемых по техническим каналам, а также визуальной информации, включая видеонаблюдение за работой пользователей. Риск утечки можно дополнительно снизить, разделяя информационную среду на изолированные плоскости безопасности. Важной мерой является мониторинг действий пользователей, в том числе фиксация событий входа в отдельные режимы систем, выполнения запросов, предоставления информации, ее переноса или печати, а также использования вычислительных ресурсов.

Если управление ИТ-инфраструктурой ФНС России делегируется внешнему исполнителю (аутсорсинг), вопросы информационной безопасности должны быть четко регламентированы в контракте. Обязательно заключение соглашения о неразглашении конфиденциальной информации и исполнение всех требований законодательства по защите данных, лицензированию, сертификации и трудовым отношениям. В контракте должны быть отражены права ФНС на аудит, возможность одностороннего расторжения договора, а также требования по регламенту доступа к ресурсам и информированию о несанкционированном доступе. Исполнители и их подрядчики обязаны быть уведомлены о своих обязанностях по безопасности. Особые правила информационной безопасности прописываются для новых или разрабатываемых информационных систем. Требования по информационной безопасности должны учитываться на ранних этапах создания и развития информационных систем, а при покупке готовых компонентов необходимо строго соблюдать формальный процесс приобретения и тестирования. Все условия безопасности должны быть зафиксированы в договорах с поставщиками. Для обеспечения корректности входных данных приложений информационных систем в ФНС России требуется процедура их верификации. При разработке и внедрении программного обеспечения сводятся к минимуму риски, связанные с нарушением целостности в результате сбоев, оформляются и хранятся технологические карты и процедуры. Внедрение нового прикладного программного обеспечения допускается только после комплексного тестирования на специально изолированных стендах, что позволяет выявить все возможные угрозы для эксплуатации, безопасности, совместимости и удобства работы. Чтобы исключить внедрение несанкционированных изменений, в ФНС России жестко контролирует доступ к исходным кодам и сопровождающей документации с помощью системы централизованного хранения – библиотеки исходных текстов. Все разрабатываемые программные решения обязательно проходят автоматизированную проверку на уязвимости.

Неавтоматизированной считается обработка конфиденциальной информации, если с ней работают сотрудники ФНС России и подведомственных организаций без использования вычислительной техники, то есть вручную. Если же для работы с электронными копиями бумажных документов применяются компьютеры, такая обработка считается автоматизированной. Для всех процессов, связанных с неавтоматизированной обработкой конфиденциальных документов, устанавливаются особые условия: документы должны надежно защищаться, храниться и учитываться по строго регламентированным правилам. Осуществляется персональная ответственность сотрудников за порядок работы с такими документами, их учет и сохранность. Вводятся положения о работе с документами в специально выделенных помещениях, регламентируются все этапы обращения: от издания и передачи до уничтожения и архивирования. Для каждой операции и документа ведется учет, фиксируются все движения, регистрируются все необходимые данные о документе и его истории. Правила доступа устанавливают строгую систему разрешений и предотвращают несанкционированное ознакомление или вынос документов, при этом степень конфиденциальности документов определяется и четко разграничивается.

В неавтоматизированных системах налоговых органов информация обрабатывается сотрудниками с помощью средств вычислительной техники, однако такие действия не относятся к автоматизированным системам или специально созданным подсистемам, имеющим нормативную документацию и аттестованным в соответствии с законодательством. В этих системах может находиться как информация ограниченного доступа, размещенная на файловых серверах и серверах баз данных для нужд подразделений или всей ФНС России, так и общедоступная информация, к которой можно получить доступ через интернет-ресурсы. Защита информации должна соответствовать требованиям 3-го класса защищенности по Приказу ФСТЭК №17 [13]. Для контроля реального состояния защищенности, работоспособности системы и своевременного выявления инцидентов проводится постоянный мониторинг, осуществляется он силами СУИБ ФНС России и Центра управления безопасностью информации. Такой мониторинг обеспечивает совершение пользователями только разрешенных действий, а за счет постоянного анализа состояния и предсказания возможных угроз удается предотвращать инциденты и выявлять нарушения в режиме защиты информации.

Для анализа трафика, выявления сетевых событий, аномалий и нарушений в информационных системах ФНС России используются различные журналы мониторинга, включая журналы операторов, администраторов, системные логи и логи ошибок. Их регулярная проверка помогает выявлять нарушения, собирать статистику отклонений и определять меры для предотвращения новых инцидентов. Все журналы хранятся в течение установленного срока и активно применяются в расследованиях нарушений и инцидентов, поскольку они могут содержать как информацию о легитимных действиях, так и о попытках несанкционированного доступа. Средства ведения журналов должны быть защищены от несанкци-

онированного вмешательства. Попытки внешних атак на системы ФНС России обязаны регистрироваться и предупреждаться только сертифицированными средствами защиты, которыми централизованно управляет ведомственный центр ФНС и сообщает о таких инцидентах в ГосСОПКА.

Контроль безопасности информации на объектах информатизации ФНС России осуществляется регулярно или при выявлении нарушений. Его цель состоит в подтверждении соответствия требованиям политики информационной безопасности и установленного режима защиты, а также поиске причин нарушений при их возникновении. За выполнение этих задач отвечают специалисты отделов информационной безопасности, а также, при необходимости, организации, лицензированные ФСТЭК России. Основная задача контроля заключается в проверке соответствия работы и инфраструктуры заданным требованиям, обоснованности принимаемых мер и своевременности исполнения нормативных документов уровня ФНС России.

В процессе контроля информационной безопасности используются специальные программы для тестирования технических средств обработки информации, причем испытания проводятся в рабочих режимах эксплуатации систем ФНС России. Однако полагаться только на результаты этих тестов нельзя, так как они не дают полного представления о защищенности: найденные уязвимости не являются исчерпывающими, поэтому результаты тестирования обязательно дополняются другими видами исследований. Тестированию подвергаются как встроенные в программное обеспечение и оборудование механизмы защиты, так и специальные средства защиты информации. После контроля оценивается эффективность принимаемых мер защиты, причем защита считается действенной только при выполнении всех требований и достижении поставленных целей. Итоги проверки, причины нарушений и рекомендации отражаются в официальных документах, которые направляются руководству ФНС России.

Аудит деятельности ФНС России по обеспечению безопасности в цифровом пространстве может выполнять как сторонняя организация с необходимым опытом, так и уполномоченный налоговый орган, следуя внутренним регламентам ФНС. Сам аудит включает различные мероприятия, в которых совместно участвуют сотрудники профильных подразделений и сторонние специалисты, а все действия должны быть тщательно согласованы между участниками процесса. На этапе начала аудита решается ряд организационных вопросов, четко определяются и фиксируются документально роли и обязанности аудитора, при этом аудитор обязан сохранять объективность, независимость, конфиденциальность и беспристрастность. План проведения аудита разрабатывается и согласовывается с руководством ФНС России, при этом определяются границы обследуемого объекта и выбираются критерии оценки состояния информационной безопасности совместно с руководством. Сотрудники ФНС России, налоговых органов и подведомственных организаций обязаны сотрудничать с аудитором и предоставлять всю необходимую информацию [12]. Объектами аудита могут выступать документация, регламентирующая порядок обеспечения информационной безопасности, компоненты информационных систем, сотрудники, обрабатывающие защищаемую информацию, а также процессы, направленные на обеспечение информационной безопасности. Для оценки деятельности ФНС России по обеспечению безопасности в цифровом пространстве применяются методики и критерии, установленные внутренними документами ФНС России, требования законодательства, стандарты и специфические требования ФНС. Результатом аудита является отчет о состоянии защищенности информационных систем с рекомендациями по совершенствованию механизмов обеспечения безопасности в ФНС России.

Выводы

Таким образом, в современных условиях налоговые органы играют сразу две ключевые роли в сфере цифровой безопасности: они выступают как субъекты, реализующие меры по защите информации и цифровых сервисов, и одновременно как объекты, требующие надежной защиты от возникающих киберугроз. Эффективная работа налоговых органов напрямую зависит от устойчивости и безопасности используемых ими информационных систем, ведь через них проходит огромный массив чувствительных данных граждан и организаций. Применение информационных технологий помогает сделать работу налоговых органов более эффективной, упростить процедуры для налогоплательщиков и обеспечить переход к электронным услугам и документообороту. Возрастающая цифровизация налоговых процессов, внедрение новых сервисов и автоматизация значительно увеличили эффективность и прозрачность налогового администрирования, но одновременно обострили риски несанкционированного доступа, утечки информации или кибератак. Обеспечение цифровой безопасности становится неотъемлемым условием доверия общества к налоговым органам и всей государственной системе. Без прочных механизмов киберзащиты невозможно гарантировать как законность и прозрачность налоговых опера-

ций, так и защиту прав граждан. Поэтому постоянное развитие системы информационной безопасности, повышение цифровой грамотности сотрудников, внедрение современных технических и организационных мер рассматриваются как приоритетная задача налоговых органов на всех уровнях работы в цифровой среде.

Литература

1. Гончаренко Л.И., Адвокатова А.С. Синергия цифровых технологий и сервисной модели деятельности налоговых органов как драйвер развития налогового администрирования // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2024. Т. 10. № 2 (38). С. 131-145. DOI: 10.21684/2411-7897-2024-10-2-131-145 EDN: TCSSBP.

2. Деева Т.В. Удаленный налоговый контроллинг в условиях цифровой экономики как необходимое требование времени по оптимизации деятельности налоговых органов // Проблемы рыночной экономики. 2020. № 3. С. 155-164. DOI: 10.33051/2500-2325-2020-3-155-164 EDN: QOUPSQ.

3. Филиппова Н.А., Артемьева С.С., Ефремова Т.А. Развитие информатизации налоговых органов в России и ее регионах в условиях цифровой экономики // Вестник НИИ гуманитарных наук при Правительстве Республики Мордовия. 2020. № 2 (54). С. 155-163. EDN: HNDZMY.

4. Ширинова О.А. Развитие налоговых органов в условиях цифровой экономики // Вестник Академии знаний. 2020. № 39 (4). С. 444-447. DOI: 10.24411/2304-6139-2020-10510 EDN: XNGVQJ.

5. Сугарова И.В. Налоговая политика и ее роль в обеспечении экономической безопасности государства // Вестник Северо-Осетинского государственного университета имени К. Л. Хетагурова. 2023. № 4. С. 220-225. DOI: 10.29025/1994-7720-2023-4-220-225 EDN: YHBZWT.

6. Надеждина С.Д. Экономическая безопасность страны и роль налогового администрирования в ее обеспечении // Baikal Research Journal. 2020. Т. 11. № 3. С. 4. DOI: 10.17150/2411-6262.2020.11(3).4 EDN: MXWWMR.

7. Шемякина М.С., Павлов Д.А. Налоговая безопасность и инструменты ее обеспечения в системе экономической безопасности региона // Инновационное развитие экономики. 2023. № 1 (73). С. 221-227. DOI: 10.51832/2223798420231221 EDN: STFMJF.

8. Артемьев Н.В., Панфилов М.А. Взаимодействие налоговых органов и органов внутренних дел при обеспечении налоговой безопасности // Вестник Московского университета МВД России. 2023. № 5. С. 248-253. DOI: 10.24412/2073-0454-2023-5-248-253 EDN: JDUMPY.

9. Маслов К.В. Процессуальные полномочия налоговых органов по обеспечению налоговой безопасности // Правоприменение. 2019. Т. 3. № 1. С. 62-71. DOI: 10.24147/2542-1514.2019.3(1).62-71 EDN: HZYFWD.

10. Мишустин М.В. Информационно-технологические основы государственного налогового администрирования в России: монография. М.: ЮНИТИ, 2005. 251 с. ISBN: 5-238-00839-2 EDN: QQIKCR.

11. Приказ ФНС России от 25.02.2014 № ММВ-7-6/66@ (ред. от 19.06.2018) «Об утверждении Концепции системы управления информационной безопасностью ФНС России». [Электронный ресурс]. URL: https://login.consultant.ru/link/?req=doc&base=LAW&n=301653&dst=100499/ (дата обращения: 06.10.2025).

12. Приказ ФНС России от 06.04.2021 № ЕД-7-24/298@ «О внесении изменений в концепцию информационной безопасности Федеральной налоговой службы». [Электронный ресурс]. URL: https://pravo.ppt.ru/prikaz/fns/n-yed-7-24-298-248834 (дата обращения: 06.10.2025).

13. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.08.2024) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_147084/82d2a16e8bfbe512b8c6eb6b10e7f805cc5d44e2/ (дата обращения: 06.10.2025).