УДК 338.24

Т. И. Ломаченко

Российский государственный университет нефти и газа им. И. М. Губкина, Москва, Россия

Н. С. Популов

Российский государственный университет нефти и газа им. И. М. Губкина, Москва, Россия, e-mail: dragonspyr@mail.ru

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ФОРМИРОВАНИЯ ЦИФРОВОЙ ЭКОНОМИКИ

Ключевые слова: NGFW, импортозамещение, кибербезопасность, оценка эффективности, межсетевой экран, экономико-методический подход, корпоративные сети.

В статье рассматриваются теоретико-экономические аспекты обеспечения информационной безопасности в условиях формирования цифровой экономики. Показано, что цифровизация хозяйственной деятельности сопровождается ростом зависимости предприятий от информационных ресурсов и увеличением масштабов потенциального экономического ущерба от киберинцидентов. В этих условиях информационная безопасность приобретает характеристики экономического блага, обеспечивающего сохранность активов, устойчивость бизнес-процессов и предсказуемость функционирования организаций. Особое внимание уделено влиянию институциональных факторов, включая государственное регулирование и политику импортозамещения, на структуру затрат и выбор средств защиты информации. Обосновано, что внедрение средств информационной безопасности должно рассматриваться как инвестиционное решение, направленное на снижение уровня неопределенности и трансакционных издержек. Предложен подход к оценке эффективности защитных мероприятий на основе сопоставления ожидаемого и предотвращённого экономического ущерба. Показано, что рациональное распределение ресурсов в сфере информационной безопасности позволяет минимизировать риски и обеспечить устойчивость функционирования предприятия в условиях цифровой трансформации.

T. I. Lomachenko

Gubkin Russian State University of Oil and Gas, Moscow, Russia

N. S. Populov

Gubkin Russian State University of Oil and Gas, Moscow, Russia,
e-mail: dragonspyr@mail.ru

SUSTAINABILITY OF THE INFORMATION SECURITY SYSTEM BASED ON IMPORT SUBSTITUTION IN THE DIGITAL ECONOMY

Keywords: NGFW, import substitution, cybersecurity, efficiency evaluation, firewall, economic and methodological approach, corporate networks.

The article examines the theoretical and economic aspects of information security in the context of the digital economy. It is shown that digitalization increases the dependence of enterprises on information resources and amplifies the scale of potential economic losses caused by cyber incidents. Under these conditions, information security acquires the characteristics of an economic good that ensures asset protection, business continuity, and predictability of organizational performance. Particular attention is paid to institutional factors, including government regulation and import substitution policy, which influence cost structures and the selection of security solutions. The paper substantiates that investments in information security should be considered as economic decisions aimed at reducing uncertainty and transaction costs. An approach to evaluating the effectiveness of security measures based on expected and prevented economic damage is proposed. It is demonstrated that rational allocation of resources in the field of information security contributes to risk minimization and enhances enterprise resilience in the digital transformation environment.

В условиях активной цифровизации экономики и перехода предприятий на современные сетевые технологии проблема защиты корпоративных сетей от внешних угроз и кибератак приобретает особую значимость. Особенно актуальна эта проблема в российском контексте, где политика импортозамещения в сфере информаци-

онной безопасности стала стратегическим приоритетом государства [10]. Внешнеэкономические ограничения 2022–2024 гг. привели к прекращению обновления и поддержки ряда зарубежных средств киберзащиты, включая NGFW [8]. В этих условиях первостепенной задачей стало внедрение отечественных межсетевых экранов нового поколения, обеспечивающих сопоставимый уровень защищённости и соответствие национальным стандартам. Одновременно такой переход требует всесторонней технической и экономической оценки, так как сопряжён со значительными затратами и влияет на стратегию информационной безопасности организации [1,6]. Следовательно, использование методических подходов, с учетом современных условий, позволяет системно оценивать угрозы и формировать требования к защите корпоративной сети. Цель исследования заключается в обосновании комплексного подхода к построению системы управления информационной безопасностью, с учетом современных требований к защите информации на предприятии, учитывающие законодательные, организационные, кадровые, цифровые решения для обеспечения соответствия требованиям бизнеса.

В условиях формирования цифровой экономики информационная безопасность приобретает не только технологическое, но и экономическое значение, выступая фактором сохранения стоимости активов и устойчивости хозяйственной деятельности предприятий. Нарушения в функционировании информационных систем приводят к прямым и косвенным экономическим потерям, включая рост трансакционных издержек, снижение эффективности бизнес-процессов и увеличение уровня неопределенности. В этой связи обеспечение информационной безопасности целесообразно рассматривать как инвестиционное направление, связанное с рациональным распределением ресурсов, направленным на минимизацию ожидаемого ущерба и поддержание устойчивости функционирования экономических субъектов. Такой подход позволяет перейти от исключительно технического восприятия защиты информации к её интерпретации как элемента экономической безопасности предприятия.

Развитие цифровой экономики в России, ускоренный переход предприятий на удалённые модели работы, рост нагрузки на корпоративные сети и усложнение ландшафта угроз формируют необходимость качественно новых подходов к обеспечению сетевой безопасности [9,16]. В этих условиях политика импортозамещения стала не только нормативным и технологическим требованием, но и существенным экономическим фактором, влияющим на устойчивость бизнеса и стратегическое развитие организаций. В частности, рынок межсетевых экранов нового поколения (NGFW) трансформируется под воздействием внешнеэкономических ограничений, потребности в технологическом суверенитете и необходимости формирования доверенной среды для функционирования информационных инфраструктур [14].

Изменение стратегических задач, развитие новых направлений, подключение облачных сервисов или необходимость соблюдения обновлённых регуляторных требований неизбежно влечёт за собой перестройку ИТ-систем (ИТ – информационные технологии), а затем – корректировку механизмов защиты. Важно отметить и тенденцию к локализации технологий в условиях импортозамещения [10]. В России наблюдается активное формирование рынка отечественных NGFW-решений, которые ориентируются не только на соответствие национальным стандартам, но и на интеграцию с российскими экосистемами программного обеспечения. Это делает их более доступными и надёжными для государственных и корпоративных структур, которые обязаны соблюдать требования по технологической независимости. Сформировавшиеся макроэкономические предпосылки импортозамещения неразрывно связаны с усиливающейся ролью государственного регулирования в сфере информационной безопасности (ИБ). В таблице 1 представлены ключевые нормативно-правовые акты, определяющие правовые рамки использования отечественных средств защиты, включая межсетевые экраны нового поколения (NGFW), а также их влияние на требования к построению корпоративных сетей [11-12,16-18].

Нормативно-правовая база, формирующая требования к информационной безопасности и использованию отечественного программного обеспечения, определяет не только регуляторные рамки, но и непосредственно влияет на структуру и динамику рынка технических средств защиты.

Таблица 1

Основные нормативно-правовые акты Российской Федерации
по защите информации и информационной безопасности

Нормативный акт	Краткое содержание документа	Значение для импортозамещения и NGFW
ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	Закрепляет базовые принципы защиты информации и обязанности операторов ИС	Формирует общую правовую основу применения технических средств защиты
ФЗ № 152-ФЗ «О персональных данных»	Устанавливает требования к защите персональных данных и каналов их передачи	Обосновывает необходимость применения сетевых средств защиты
ФЗ № 187-ФЗ «О безопасности критической информационной инфраструктуры»	Определяет обязанности субъектов КИИ по обеспечению защищённости ИС	Фактически закрепляет приоритет отечественных сертифицированных NGFW
Постановление Правительства РФ № 878 «О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»	Ограничивает закупку иностранного ПО при наличии российских аналогов	Создаёт обязательный спрос на отечественные NGFW
Постановление Правительства РФ № 719 «О подтверждении производства российской промышленной продукции»	Устанавливает критерии отнесения ПО к продукции российского происхождения	Регулирует включение NGFW в реестр российского ПО

Таблица 2

Проблемы импортозамещения NGFW для предприятий

Проблема	Сущность	Влияние на стратегию безопасности предприятия
Функциональная зрелость отечественных решений	Отдельные российские NGFW уступают зарубежным аналогам по глубине поведенческой аналитики и уровню автоматизации	Требуется дополнительная настройка, пилотирование и поэтапное внедрение
Историческая зависимость от зарубежных экосистем	Инфраструктура крупных организаций часто построена вокруг иностранных платформ и форматов	Повышаются затраты и сроки миграции, возрастает риск ошибок интеграции
Кадровый дефицит	Недостаток специалистов с практическим опытом работы с отечественными средствами защиты	Увеличиваются издержки на обучение и сопровождение
Совместимость в сложных ИТ-средах	Ограниченная интеграция отечественных NGFW с рядом зарубежных корпоративных и облачных систем	Требуется пересмотр архитектуры или отказ от части зарубежных сервисов
Ограниченный доступ к технической поддержке	Невозможность заключения или продления сервисных контрактов	Снижение устойчивости системы защиты и рост времени восстановления
Зависимость от зарубежных облачных сервисов	Риск блокировки или ограничения доступа к инфраструктуре поставщика	Потеря доступности критичных сервисов

Государственные требования к сертификации, локализации разработки и исключению зависимости от зарубежных поставщиков создают устойчивый и прогнозируемый спрос на отечественные решения, формируя благоприятные условия для их цифрового развития отечественных предприятий. Для систематизации указанных факторов и оценки их влияния на стратегию информационной безопасности в таблице 2 представлены основные проблемы импортозамещения NGFW для предприятий.

Современные межсетевые экраны нового поколения рассматриваются как инструменты, которые позволяют организациям:

– Снижать вероятность успешных внешних атак.

– Уменьшать затраты, связанные с инцидентами безопасности.

– Поддерживать стабильную работу цифровой инфраструктуры.

– Обеспечивать соответствие нормативным требованиям.

– Повышать общую устойчивость и конкурентоспособность бизнеса.

Для предприятий внедрение NGFW – это не только вопрос повышения уровня технической защищённости, но и возможность снизить риски простоя, утечки данных, финансовых потерь и репутационных ущербов, что напрямую связано с экономической устойчивостью бизнеса [4]. Вследствие этого отечественные NGFW становятся элементом не только технологического, но и стратегического доверия, обеспечивая устойчивость цифровых процессов и снижая риски, связанные с использованием зарубежных решений. Сводный перечень основных требований, учитывающих как особенности межсетевых экранов нового поколения, так и общие условия эксплуатации ИТ-инфраструктуры предприятия, представлен в таблице 3.

Помимо функциональных и архитектурных требований, сформированных с учётом текущей структуры корпоративной сети и используемых технических решений, при выборе и оценке NGFW необходимо учитывать ряд дополнительных условий, связанных с эксплуатацией, развитием ИТ-инфраструктуры и обеспечением устойчивости бизнес-процессов, а это в свою очередь, требуют от предприятий комплексного подхода к построению системы защиты, включающего как сетевые средства обнаружения, так и централизованное управление политикой информационной безопасности [7,13].

Такой подход предполагает интеграцию организационных, технологических и экономических механизмов защиты информации в рамках единой системы управления безопасностью предприятия. Он обеспечивает согласованность действий различных подразделений организации, включая ИТ-службы, подразделения информационной безопасности и управленческий персонал.

Таблица 3

Обобщённые требования к NGFW и системе сетевой защиты предприятия

Параметры защиты системы	**Содержание требований**
Архитектурно-функциональные	Обеспечение защиты сетевого периметра и внутренних сегментов, поддержка логической сегментации сети, контроль взаимодействия с демилитаризованной зоной (DMZ), возможность интеграции в существующую архитектуру без её кардинальной перестройки
Производительность и масштабируемость	Пропускная способность, достаточная для обработки текущих объёмов сетевого трафика с учётом включённых механизмов анализа, наличие запаса производительности и возможности развития системы сетевой защиты при росте нагрузки
Управляемость и администрирование	Централизованное управление политиками безопасности, прозрачность конфигураций, контроль изменений и воспроизводимость настроек в рамках регламентированной эксплуатации
Интеграция и совместимость	Поддержка взаимодействия со службой каталогов и другими корпоративными сервисами, корректная работа в существующей ИТ-среде и совместимость с используемыми техническими решениями
Контроль и анализ сетевого трафика	Анализ сетевых соединений, выявление потенциально опасной активности, поддержка механизмов обнаружения и предотвращения атак, а также мониторинг состояния сетевых потоков
Журналирование и аудит	Ведение журналов сетевых событий и действий администраторов, возможность использования данных для аудита, анализа инцидентов и соблюдения внутренних регламентов
Надёжность и эксплуатационная устойчивость	Стабильная работа системы сетевой защиты, минимизация влияния на доступность корпоративных сервисов и поддержка механизмов восстановления работоспособности
Экономические и организационные	Предсказуемость затрат на внедрение и эксплуатацию, соответствие внутренним процессам управления ИТ и информационной безопасностью, а также условиям долгосрочного использования решения

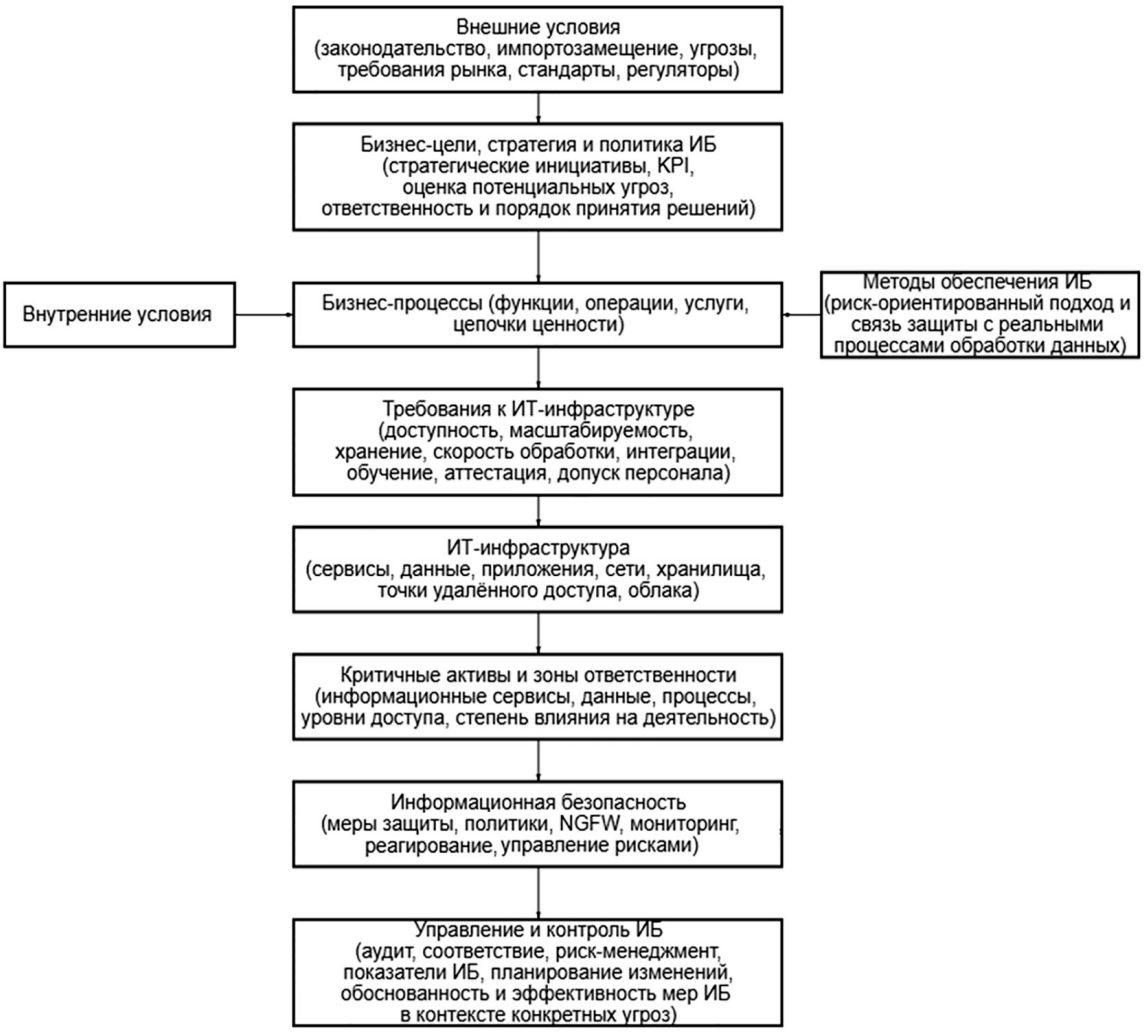

Рис. 1. Комплексный подход к обеспечению информационной безопасности предприятия
Источник: составлено автором

Комплексная реализация мер защиты позволяет учитывать не только технические параметры функционирования сети, но и влияние угроз на устойчивость бизнес-процессов, финансовые показатели и непрерывность деятельности предприятия. В результате формируется целостная модель обеспечения информационной безопасности, ориентированная на минимизацию рисков и повышение устойчивости корпоративной цифровой инфраструктуры.

Современные внешние киберугрозы характеризуются высокой динамичностью и эволюционным развитием, связанным как с усложнением корпоративных ИТ-ландшафтов, так и с ростом доступности инструментов атаки [3]. Следовательно, одним из наиболее значимых факторов, влияющих на структуру угроз, является переход организаций к распределённым моделям работы и активное использование удалённого доступа [5]. Это приводит к расширению потенциальных точек входа, что облегчает злоумышленникам проведение разведки и подбор уязвимых элементов инфраструктуры. Структура распределения успешных атак по отраслям экономики также подтверждает приоритетность защиты корпоративных сетей. Наибольшая доля инцидентов приходится на государственный сектор, промышленность и ИТ-компании, что отражает фокус злоумышленников на объектах с высокой концентрацией критически значимых данных и сервисов. Данные, представленные на рисунке 2, демонстрируют отраслевую дифференциацию жертв кибератак и позволяют определить приоритетные направления применения средств NGFW.

Рис. 2. Доля успешных кибератак на российские организации за 1-2 квартал 2025 года
Источник: составлено автором

Согласно недавнему отчёту Positive Technologies, уже в первом полугодии 2025 г. на государственные учреждения пришлось около 21% всех успешных кибератак на организации, что стало максимальным значением за последние три года. В данных условиях эффективная нейтрализация внешних угроз невозможна без применения современных комплексных средств кибербезопасности, способных проактивно обнаруживать и предотвращать различные типы атак.

В результате проведённого исследования установлено, что обеспечение информационной безопасности в условиях цифровой экономики должно рассматриваться как экономическая категория, связанная с управлением рисками, распределением ресурсов и снижением трансакционных издержек. Показано, что цифровизация усиливает зависимость предприятий от информационных ресурсов и увеличивает потенциальный экономический ущерб от киберинцидентов, что требует формирования устойчивой системы защиты информации.

Выявлено, что институциональные факторы, включая нормативно-правовое регулирование и политику импортозамещения, оказывают существенное влияние на структуру затрат и выбор средств защиты, формируя ограничения и стимулы для хозяйствующих субъектов. Обосновано, что внедрение средств информационной безопасности должно рассматриваться как инвестиционное решение, направленное на снижение ожидаемого ущерба и обеспечение устойчивости функционирования предприятия.

Предложенный подход к оценке эффективности защитных мер на основе сопоставления ожидаемого и предотвращённого ущерба позволяет количественно обосновывать затраты на безопасность и рассматривать их как элемент рационального распределения ресурсов. Полученные результаты подтверждают, что экономически обоснованное обеспечение информационной безопасности способствует снижению уровня неопределенности и повышению устойчивости предприятий в условиях цифровой экономики [1,2].

Библиографический список

1. Gordon L. A., Loeb M. P. The Economics of Information Security Investment // ACM Transactions on Information and System Security. 2002. Vol. 5(4). P. 438–457. DOI: 10.1145/581271.581274.

2. Kotenko I. V., Saenko I. B., Sineshchuk Yu. S., Kuvatov V. V., Chudakov O. V. Optimization of the cybersecurity system structure based on accounting of the prevented damage cost // Proceedings of the 12th Int. Conf. on Security of Information and Networks (Sochi, 2019). 2019. DOI: 10.1145/3357613.3357620.

3. Positive Technologies. Актуальные киберугрозы: I–II кварталы 2025 года. Аналитический отчет PT ESC, 2025. URL: https://ptsecurity.com/research/analytics/aktual-nye-kiberugrozy-i-ii-kvartaly-2025-goda/ (дата обращения: 16.01.2026).

4. Аналитический отчет по обеспечению кибербезопасности сетевой инфраструктуры // InfoWatch. 2025. [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/analitika/tendentsii-v-obespecheniikiberbezopasnosti-setevoy-infrastruktury (дата обращения: 25.01.2026).

5. Афанасьева Д. В. Информационная безопасность при удаленной работе // Известия ТулГУ. Технические науки. 2021. № 5. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-pri-udalennoy-rabote (дата обращения: 22.01.2026).

6. Васильев А. Экономика кибербезопасности в мире // Cifra. Информационные технологии и телекоммуникации. 2024. №1 (1). URL: https://itech.cifra.science/archive/1-1-2024-january/10.18454/itech.2024.1.1 (дата обращения: 03.02.2026). DOI: 10.18454/itech.2024.1.1.

7. Гродзенский Я. С. Информационная безопасность: учебное пособие. Москва: РГ-Пресс, 2020. 144 с.

8. Джангиров М. Ф. Импортозамещение на рынке информационной безопасности // Молодой ученый. 2023. № 1 (448). С. 4–7. URL: https://moluch.ru/archive/448/98664 (дата обращения: 10.02.2026).

9. Лебедев А. С. Цифровая экономика: новые угрозы и вызовы для экономической безопасности россии // Инновации и инвестиции. 2023. № 5. URL: https://cyberleninka.ru/article/n/tsifrovaya-ekonomika-novye-ugrozy-i-vyzovy-dlya-ekonomicheskoy-bezopasnosti-rossii (дата обращения: 03.02.2026).

10. Попова И. Н., Сергеева Т. Л. Импортозамещение в современной России: проблемы и перспективы // Beneficium. 2022. № 2 (43). URL: https://cyberleninka.ru/article/n/importozameschenie-v-sovremennoy-rossii-problemy-i-perspektivy (дата обращения: 15.01.2026).

11. Постановление Правительства от 10 июля 2019 г. N 878 «О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (ред. от 08.07.2025) // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_329382/ (дата обращения: 02.02.2026).

12. Постановление Правительства от 7 июля 2015 г. N 719 «О подтверждении производства российской промышленной продукции» (ред. от 27.03.2025) // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_183175/ (дата обращения: 02.02.2026).

13. Приступа А. С. Методология оценки эффективности обеспечения безопасности в экономических информационных системах: дис. … канд. экон. наук. Москва, 2005. 164 с.

14. Российский рынок межсетевых экранов нового поколения (NGFW) // TAdviser. 2025. [Электронный ресурс]. URL: https://www.tadviser.ru/a/262435 (дата обращения: 18.01.2026).

15. Углова И. А. Цифровая экономика: информационная и экономическая безопасность // Проблемы развития национальной экономики на современном этапе. 2018. С. 428-436.

16. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (ред. от 25.11.2024) // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/447665bba1533b8994dee2a039b9455dad11d56f/ (дата обращения: 10.02.2026).

17. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 12.12.2024) // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 01.02.2026).

18. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 24.06.2025) // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 02.02.2026).