УДК 34

ОБЕСПЕЧЕНИЕ РЕЖИМА СЕКРЕТНОСТИ ПРИ УДАЛЕННОЙ РАБОТЕ И ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ СЕРВИСОВ

***Глотова В.О.*[1],**

Студент юридического института

ФГАОУ ВО «Белгородский государственный национальный исследовательский университет»

Россия, г. Белгород

Алферова Д.А.
Студент юридического института

ФГАОУ ВО «Белгородский государственный национальный исследовательский университет»

Россия, г. Белгород

Аннотация. В статье анализируются правовые, организационные и технические аспекты обеспечения режима государственной тайны в условиях дистанционной занятости и использования облачных вычислений. Рассматриваются изменения в российском законодательстве, вступившие в силу в 2024–2026 годах, а также актуальные статистические данные об угрозах информационной безопасности. Особое внимание уделяется требованиям ФСТЭК России, вопросам допуска к государственной тайне, использованию государственной единой облачной платформы и практическим мерам защиты информации.

[1] *Научный руководитель - **Гриневич К.В.**, Ассистент кафедры теории и истории государства и права «Белгородский государственный национальный исследовательский университет», Россия, г. Белгород*
***Grinevich K.V.** Assistant of the Department of Theory and History of State and Law "Belgorod State National Research University", Russia, Belgorod*

Ключевые слова: государственная тайна, удаленная работа, облачные сервисы, информационная безопасность, ФСТЭК, допуск к гостайне, ГЕОП, кибератаки, защита информации.

SECURITY AT WORK AND CLOUD SERVICES

Glotova V.O.,
Student of the Law Institute
Federal State Autonomous Educational Institution of Higher Education "Belgorod State National Research University"
Russia, Belgorod

Alferova D.A.
Student of the Law Institute
Federal State Autonomous Educational Institution of Higher Education "Belgorod State National Research University"
Russia, Belgorod

Annotation: The article analyzes the legal, organizational, and technical aspects of ensuring the regime of state secrets in the context of remote employment and the use of cloud computing. It examines the changes in Russian legislation that came into force in 2024-2026, as well as current statistical data on information security threats. Special attention is given to the requirements of the Federal Service for Technical and Export Control of Russia, issues related to access to state secrets, the use of the state unified cloud platform, and practical measures for protecting information.

Keywords: state secrets, remote work, cloud services, information security, FSTEC, access to state secrets, GEO, cyberattacks, and information protection.

Цифровая трансформация государственного управления, получившая дополнительный импульс в последние годы, объективно требует пересмотра

традиционных подходов к защите информации ограниченного доступа. Удаленный формат исполнения служебных обязанностей стал неотъемлемой частью трудовых отношений, однако практика перевода части сотрудников на дистанционную работу создает новые каналы утечки сведений, составляющих государственную тайну. Дополнительным вызовом для системы защиты государственной тайны (ЗГТ) стало внедрение облачных технологий, которые размывают традиционные периметры безопасности. Целью настоящей работы является комплексный анализ современных правовых, технических и организационных проблем обеспечения режима секретности при удаленной работе и эксплуатации облачных сервисов.

Правовое регулирование в рассматриваемой сфере претерпело в 2024-2026 годах значительные изменения, направленные на адаптацию законодательства о государственной тайне к реалиям цифровой экономики. Ключевым событием стало обновление базового перечня сведений, составляющих государственную тайну, утвержденного Указом Президента РФ от 30 ноября 1995 г. № 1203. Указом Президента РФ от 24 июня 2025 г. № 412 в этот перечень были внесены изменения, уточняющие категории информации, подлежащей особой защите в условиях цифровизации [1]. В частности, в перечень включены сведения, раскрывающие основы государственной политики в сфере мобилизационной подготовки и в Российской Федерации.

Одновременно были актуализированы правила допуска должностных лиц и граждан к государственной тайне. Постановлением Правительства РФ от 7 февраля 2024 г. № 132 утверждены новые правила допуска, которые заменили ранее действовавшую инструкцию 2010 года. [2]. Среди ключевых новшеств – расширение перечня оснований для отказа гражданину в допуске, включая включение претендента в реестр иностранных агентов, а также уточнение процедур прекращения допуска [2]. Впоследствии Постановлением Правительства РФ от 8 июля 2025 г. № 1028 в указанные правила были внесены дополнительные изменения, касающиеся хранения решений

Межведомственной комиссии по защите государственной тайны и уточнения условий прекращения допуска при прекращении исполнения обязанностей, связанных с доступом к гостайне [3].

Существенную роль в регулировании использования облачных сервисов для обработки секретных данных играет ведомственное нормотворчество. С 1 марта 2026 г. вступил в силу Приказ ФСТЭК России от 11 апреля 2025 г. № 117, который устанавливает требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий и государственных учреждений [4]. Данный документ заменил действовавшее более десяти лет Постановление № 17 и, как отмечают эксперты, задает принципиально новый подход к защите информации, основанный не на формальной классификации, а на непрерывном процессе обеспечения безопасности и доказательстве эффективности принимаемых мер [5].

Особого внимания заслуживают положения Приказа ФСТЭК № 117, касающиеся удаленного доступа. Документ устанавливает, что удаленный доступ должен осуществляться с использованием сетей связи на территории Российской Федерации, а также предусматривает применение строгой аутентификации и мер по защите каналов передачи данных [4, с. 9]. Кроме того, установлены жесткие сроки устранения уязвимостей: критические уязвимости должны устраняться за 24 часа, уязвимости высокого уровня опасности – не более чем за 7 дней [6].

Переход на удаленный формат работы создает благоприятную среду для реализации широкого спектра угроз информационной безопасности, что подтверждается тревожной статистикой.

Согласно данным компании «Еса Про», за 2025 год 73% всех утечек данных из российских организаций пришлось на государственный сектор – всего было слито более 105 млн строк данных с записями о пользователях и компаниях [7]. Аналитики связывают «лидерство» госсектора в первую очередь

с политической мотивацией хакеров, нацеленных на государственные организации, а также с недостаточным уровнем кибербезопасности некоторых ведомств [8].

Не менее тревожная ситуация наблюдается в сфере облачных вычислений. По данным облачного провайдера Nubes, за неполные восемь месяцев 2025 года количество кибератак на облачные и гибридные сервисы в России превысило совокупный показатель за 2023-2024 годы и достигло 105 миллионов [9, с. 4]. Наиболее распространенными типами атак являются XSS-атаки (40%), мошеннический фишинг (25%), DDoS-атаки и вредоносные приложения (по 15%) [9]. При этом в 54% случаев атаки начинались с техники подбора или использования уже украденных логинов и паролей, что напрямую связано с человеческим фактором сотрудников и подрядчиков [10].

Как отмечает Т. К. Ижболдина, дистанционный формат работы, при всей его гибкости и удобстве, создает множество уязвимостей: от использования ненадежных сетей и личных устройств до рисков фишинга и утечек данных [11, с. 297].

Обеспечение режима государственной тайны в условиях удаленной работы требует комплексного подхода, сочетающего правовые, организационные и технические меры.

В организационной плоскости ключевое значение имеет корректировка локальных нормативных актов организаций, работающих с секретными сведениями. Необходимо внести изменения в инструкции по обеспечению режима секретности, четко регламентировав порядок действий сотрудников при дистанционной работе, включая требования к рабочему месту, каналам связи и порядку уничтожения черновиков.

Федеральная служба по техническому и экспортному контролю (далее ФСТЭК) России в своих рекомендациях по обеспечению безопасности объектов критической информационной инфраструктуры при дистанционной работе (письмо от 20 марта 2020 г. № 240/84/389) определила ряд обязательных

мер, сохраняющих актуальность и в 2025-2026 годах. К числу таких мер относятся: проведение инструктажа работников о правилах безопасного удаленного взаимодействия; определение перечня средств вычислительной техники, предоставляемых работникам для удаленной работы; назначение минимально необходимых прав и привилегий пользователям; идентификация удаленных средств вычислительной техники по физическим адресам; организация защищенного доступа с применением средств криптографической защиты информации [12].

Важным элементом организационной работы является регулярное обучение сотрудников основам информационной безопасности и правилам обращения с секретными сведениями в цифровой среде. Как показывает статистика, значительная часть инцидентов связана именно с человеческим фактором и недостаточной осведомленностью персонала о существующих угрозах.

В технической плоскости обеспечение режима секретности при удаленной работе требует реализации следующих приоритетных направлений.

Криптографическая защита информации. Использование сертифицированных ФСБ России средств криптографической защиты информации (СКЗИ) для всех каналов передачи данных, содержащих сведения, составляющие государственную тайну. Это требование закреплено в Приказе ФСТЭК № 117, который предписывает организацию защищенного доступа с удаленных средств вычислительной техники к серверам с применением VPN-клиентов и иных средств криптографической защиты [12].

Контроль доступа и аутентификация. Внедрение систем управления идентификацией и доступом (IAM) на основе принципа минимально необходимых привилегий. Приказ ФСТЭК № 117 устанавливает обязательную двухфакторную аутентификацию работников при удаленном доступе, при этом один из факторов должен обеспечиваться устройством, отделенным от объекта

критической информационной инфраструктуры, к которому осуществляется доступ [12].

Защита конечных точек. Использование специализированных защищенных операционных систем и средств доверенной загрузки для удаленных рабочих мест, с которых осуществляется доступ к секретным сведениям. Особое внимание уделяется применению средств антивирусной защиты и систем класса EDR (Endpoint Detection and Response), обеспечивающих поведенческий анализ и оперативное реагирование на инциденты [5].

Безопасность облачной инфраструктуры. Размещение информационных систем, обрабатывающих государственную тайну, допускается исключительно в государственной единой облачной платформе (ГЕОП) или иных аттестованных центрах обработки данных, расположенных на территории Российской Федерации.

С 1 января 2025 года в России начала работу государственная единая облачная платформа (ГЕОП) под названием «Гособлако». Постановление, регулирующее ее функционирование, было подписано Председателем Правительства Михаилом Мишустиным [13]. «Гособлако» позиционируется как универсальная платформа для размещения и работы информационных систем и ресурсов различных министерств, ведомств, государственных внебюджетных фондов, публично-правовых компаний и социально ориентированных некоммерческих организаций.

Для облачных услуг на ГЕОП введены строгие требования по информационной безопасности, включая регулярные проверки, обязательную отчетность и аттестацию систем, которая стала обязательной с марта 2026 года [14]. Проект приказа Минцифры России, размещенный для общественного обсуждения, предусматривает, что программные и аппаратные компоненты информационно-телекоммуникационной инфраструктуры должны быть реализованы на отечественных продуктах, включенных в соответствующие

реестры Минцифры и Минпромторга, а средства защиты информации должны иметь соответствующий сертификат ФСБ или ФСТЭК. Кроме того, технические средства, обрабатывающие информацию, средства ее защиты и оборудование центров обработки данных должны размещаться на территории Российской Федерации [15].

Важно отметить, что в соответствии с указанным документом информационно-телекоммуникационная инфраструктура ГЕОП не предназначена для обработки сведений, составляющих государственную тайну [15]. Для работы с гостайной требуются специализированные облачные среды с более высоким уровнем защиты и аттестацией по соответствующим классам защищенности.

Современный этап развития правового регулирования и технического обеспечения защиты государственной тайны характеризуется переходом от разрозненных мер к формированию целостной системы, адекватной вызовам цифровой эпохи. За 2024–2026 годы российским законодателем и профильными регуляторами (ФСТЭК, ФСБ) создана значительная нормативная база, охватывающая практически все аспекты обращения с секретными сведениями в условиях удаленной работы и облачных вычислений.

Ключевыми тенденциями являются: ужесточение требований к допуску граждан к государственной тайне и усиление ответственности за их нарушение; создание суверенной облачной инфраструктуры (ГЕОП) для государственных информационных систем; внедрение обязательной криптографической защиты информации при передаче по каналам связи; разработка специальных требований к удаленному доступу, включая многофакторную аутентификацию и контроль конечных устройств.

Вместе с тем практическая реализация принятых нормативных актов сталкивается с определенными трудностями, связанными с необходимостью масштабной модернизации существующих информационных систем и переобучения персонала. Дальнейшее развитие системы защиты

государственной тайны должно идти по пути создания детализированных методических рекомендаций, совершенствования инструментов контроля и мониторинга, а также повышения уровня цифровой грамотности сотрудников, допущенных к работе с секретными сведениями.

Библиографический список

1. О внесении изменений в перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203 : Указ Президента РФ от 24 июня 2025 г. № 412 // Собрание законодательства Российской Федерации. – 2025. – № 26. – Ст. 4850.

2. Об утверждении Правил допуска должностных лиц и граждан Российской Федерации к государственной тайне : Постановление Правительства РФ от 7 февраля 2024 г. № 132 // Собрание законодательства Российской Федерации. – 2024. – № 7. – Ст. 987.

3. О внесении изменений в постановление Правительства Российской Федерации от 7 февраля 2024 г. № 132 : Постановление Правительства РФ от 8 июля 2025 г. № 1028 // Собрание законодательства Российской Федерации. – 2025. – № 28. – Ст. 4672.

4. Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений : Приказ ФСТЭК России от 11 апреля 2025 г. № 117 // Официальный интернет-портал правовой информации. – URL: http://publication.pravo.gov.ru/document/0001202506170011 (дата обращения: 30.03.2026).

5. Как Приказ № 117 ФСТЭК меняет защиту государственных систем [Электронный ресурс] // РБК Компании. – 2026. – 24 марта. – URL: https://companies.rbc.ru/news/iff2sDTMll/kak-prikaz--117-fstek-menyaet-zaschitu-gosudarstvennyih-sistem (дата обращения: 30.03.2026).

6. Официальная публикация приказа ФСТЭК России от 11.04.2025 № 117 [Электронный ресурс] // Extrim-Security. – 2025. – 18 июня. – URL: https://extrim-security.ru/news-ib/tpost/40can4lp51-ofitsialnaya-publikatsiya-prikaza-fstek (дата обращения: 30.03.2026).

7. Хакеры власть не признают [Электронный ресурс] // Коммерсантъ. – 2025. – 22 декабря. – URL: https://www.kommersant.ru/doc/8313330 (дата обращения: 30.03.2026).

8. Почти три четверти утечек данных в 2025 году пришлись на госсектор [Электронный ресурс] // Коммерсантъ. – 2025. – 22 декабря. – URL: https://www.kommersant.ru/doc/8313440 (дата обращения: 30.03.2026).

9. «Коммерсант»: в 2025 году хакеры совершили 105 млн атак на облачные сервисы РФ [Электронный ресурс] // Смотрим.ру. – 2025. – 30 августа. – URL: https://smotrim.ru/article/4664678 (дата обращения: 30.03.2026).

10. С начала года хакеры совершили более 100 млн атак на облачные сервисы России [Электронный ресурс] // Коммерсантъ. – 2025. – 29 августа. – URL: https://www.kommersant.ru/doc/8005344 (дата обращения: 30.03.2026).

11. Ижболдина, Т. К. Особенности обеспечения информационной безопасности в условиях удаленной работы = Features of ensuring information security in the context of remote work / Т. К. Ижболдина // Информационные технологии обеспечения комплексной безопасности в цифровом обществе : материалы VII Всероссийской молодёжной научно-практической конференции с международным участием, Уфа, 23-24 мая 2025 г. / Уфимский университет науки и технологий ; редкол.: Д. С. Юнусова (отв. ред.) [и др.]. – Уфа, 2025. – С. 297-301.

12. ФСТЭК разработала рекомендации по обеспечению безопасности объектов КИИ при дистанционной работе [Электронный ресурс] // D-Russia.ru. – 2020. – 24 марта. – URL: https://d-russia.ru/fstjek-razrabotala-rekomendacii-po-obespecheniju-bezopasnosti-obektov-kii-pri-distancionnoj-rabote.html (дата обращения: 30.03.2026).

13. Правительство утвердило регламент работы «Гособлака» [Электронный ресурс] // CNews. – 2024. – 12 июля. – URL: https://zoom.cnews.ru/news/item/606920 (дата обращения: 30.03.2026).

14. Обзор изменений в законодательстве за июнь 2025 года [Электронный ресурс] // UDV Group. – 2025. – 8 июля. – URL: https://udv.group/about/blog/obzor-izmeneniy-v-zakonodatelstve-za-iyun-2025-goda (дата обращения: 30.03.2026).

15. Минцифры разработало требования к информационной безопасности «Гособлака» [Электронный ресурс] // Парламентская газета. – 2025. – 6 июня. – URL: https://www.pnp.ru/social/mincifry-razrabotalo-trebovaniya-k-bezopasnosti-gosoblaka.html (дата обращения: 30.03.2026).