УДК 004

Гриднев Кир Максимович

студент

3 курс, факультет «Информатика и вычислительная техника»

Донской государственный технический университет

Россия, г. Ростов-на-Дону

ИНФОРМАЦИОННАЯ СИСТЕМА ЗАЩИТЫ УДАЛЕННОГО ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. *В статье рассматриваются актуальные подходы к проектированию и внедрению информационных систем защиты удаленного доступа к ресурсам корпоративных сетей в Российской Федерации. В условиях массового перехода на дистанционный формат работы и усиления киберугроз, автор анализирует уязвимости традиционных VPN-решений и предлагает переход к архитектуре сетевого доступа с нулевым доверием.*

Основное внимание уделено интеграции отечественных средств защиты информации, сертифицированных ФСТЭК и ФСБ России, для обеспечения конфиденциальности и целостности данных. В работе предложена модель комплексной системы защиты, включающая многофакторную аутентификацию (MFA), механизмы строгого разграничения прав доступа и шифрование каналов связи по ГОСТ-алгоритмам. Результатом исследования является методика построения защищенного удаленного доступа, минимизирующая риск несанкционированного проникновения в периметр организации и обеспечивающая соответствие требованиям законодательства в области защиты КИИ и персональных данных.

Ключевые слова: *удаленный доступ, информационная безопасность, импортозамещение*

Abstract. *This article examines current approaches to the design and implementation of information systems for protecting remote access to corporate network resources in the Russian Federation. Amid the widespread transition to remote work and increasing cyber threats, the author analyzes the vulnerabilities of traditional VPN solutions and proposes a transition to a zero-trust network access architecture.*

The focus is on the integration of domestic information security tools certified by the Federal Service for Technical and Export Control (FSTEC) and the Federal Security Service (FSB) of Russia to ensure data confidentiality and integrity. The paper proposes a model for a comprehensive security system that includes multi-factor authentication (MFA), strict access rights delimitation mechanisms, and

communication channel encryption using GOST algorithms. The result of the study is a methodology for building secure remote access that minimizes the risk of unauthorized intrusion into the organization's perimeter and ensures compliance with legal requirements for the protection of critical information infrastructure and personal data.
Keywords: *remote access, information security, import substitution*

Введение

В современном мире, где цифровая трансформация пронизывает все сферы жизни, а удаленная работа стала не временной мерой, а устойчивой реальностью, вопрос защиты удаленного доступа к информационным ресурсам приобрел для России особое, стратегическое значение. С одной стороны, мы являемся свидетелями активного развития цифрового государства: портал «Госуслуги», система межведомственного электронного взаимодействия (СМЭВ), единая биометрическая система и множество отраслевых государственных информационных систем (ГИС) требуют от граждан и организаций постоянного и безопасного подключения. С другой стороны, геополитическая обстановка, массовый уход зарубежных вендоров и беспрецедентный рост числа кибератак на российскую критическую информационную инфраструктуру (КИИ) вынуждают государство и бизнес кардинально пересматривать подходы к организации удаленного доступа.

Таким образом, информационная система защиты удаленного доступа в России — это не просто набор технологических решений, а сложный, многоуровневый организм, функционирующий в жестких рамках национального законодательства, опирающийся на отечественную криптографию и развивающийся под влиянием уникальных угроз и регуляторных требований. В данном эссе мы рассмотрим ключевые компоненты, нормативную базу, технологические решения и основные вызовы, стоящие перед российскими специалистами в области информационной безопасности при организации защищенного удаленного доступа.

Нормативно-правовая база: диктат регулятора

В отличие от многих западных стран, где стандарты безопасности носят рекомендательный характер, в России требования к защите удаленного доступа имеют силу закона и строго регламентированы, прежде всего, Федеральной службой по техническому и экспортному контролю (ФСТЭК России). Ключевым событием последнего времени стало вступление в силу с 1 марта 2026 года Приказа ФСТЭК России №117, который пришел на смену действовавшему ранее Приказу №17. Этот документ фундаментально меняет подход к защите информации в государственных и муниципальных информационных системах, превращая безопасность в непрерывный, управляемый и измеримый процесс. Приказ №117 унифицирует подходы к защите данных, снижает риски утечек и, что крайне важно для нашей темы, учитывает современные реалии: облачные технологии, удаленный доступ, мобильные рабочие места и возрастающую роль подрядчиков.

Новый приказ устанавливает запрет на бесконтрольное использование прав администратора и накладывает жесткие ограничения на дистанционное подключение к контуру государственных информационных систем. Если сотрудник использует для работы личное устройство, организация обязана обеспечить защиту канала связи, строгую многофакторную аутентификацию и, что самое главное, исключить прямой несанкционированный доступ к системе. Привычные для многих схемы, основанные на применении несертифицированных VPN-клиентов или прямом пробросе портов (port forwarding), отныне перестают соответствовать нормативным требованиям. Кроме того, Приказ №117 расширяет зону ответственности: теперь требования обязательны для любых информационных систем, используемых в работе государственных органов и учреждений, независимо от их официального статуса ГИС.

Одновременно с ФСТЭК активную позицию занимает и Федеральная служба безопасности (ФСБ России), которая регулирует использование средств криптографической защиты информации (СКЗИ). Взаимодействие с государственными информационными системами, в частности с Единой

системой идентификации и аутентификации (ЕСИА), теперь требует применения сертифицированных СКЗИ класса КС3 и выше. Роскомнадзор, в свою очередь, в 2025 году дал рекомендации владельцам российских частных виртуальных сетей отказаться от использования иностранных протоколов шифрования при передаче данных, сделав шаг в сторону полной минимизации зависимости от зарубежных решений.

Таким образом, российское законодательство последовательно движется к модели, при которой удаленный доступ — это всегда контролируемый, аттестованный и криптографически защищенный процесс, не оставляющий места «серым» схемам.

Архитектура защиты: от классического VPN к Zero Trust

Под давлением регулятора и в условиях новых угроз происходит эволюция архитектуры систем удаленного доступа в России. Традиционная модель «периметр — доверенная сеть», подразумевавшая создание VPN-туннеля между устройством пользователя и корпоративной сетью, сегодня признается недостаточной. Как отмечают эксперты, компрометация удаленного пользователя открывает двери во всю внутреннюю инфраструктуру, что может повлечь за собой утечки данных и атаки шифровальщиков.

На смену классическому VPN приходит концепция нулевого доверия (Zero Trust), активно внедряемая в российских государственных и коммерческих структурах. Ее ключевой принцип — «никогда не доверяй, всегда проверяй». Вместо предоставления широкого доступа ко всем ресурсам сети, система выдает пользователю минимально необходимые права только для выполнения конкретной задачи. В России этот подход находит практическое воплощение в системах управления привилегированным доступом (PAM — Privileged Access Management).

Примером такого решения является продукт ГК «Солар» — Solar SafeInspect с модулем WEB-портал, сертифицированный ФСТЭК России. Архитектура этого решения предельно показательна. Администратор или

подрядчик подключается к специальному WEB-порталу, проходит строгую аутентификацию, после чего получает доступ к целевым системам внутри изолированной сессии по протоколам RDP, SSH или HTTPS. При этом на устройство пользователя не требуется установка каких-либо VPN-клиентов или дополнительного ПО — все взаимодействие происходит через веб-интерфейс. Самое важное — прямого сетевого взаимодействия между потенциально небезопасным устройством администратора и критической инфраструктурой ГИС не происходит. Все сессии изолированы, а действия привилегированных пользователей полностью протоколируются и контролируются. Такая архитектура в точности соответствует новым требованиям Приказа №117, который требует исключения прямого доступа к защищаемым системам.

Технологическая платформа: российское шифрование по ГОСТ

Невозможно говорить о защите удаленного доступа в России, не затронув тему криптографии. Уход зарубежных производителей (Cisco, Juniper и др.) и требования законодательства стимулировали бурный рост рынка отечественных СКЗИ. Сегодня весь трафик, передаваемый при удаленном доступе к государственным информационным системам и объектам КИИ, должен шифроваться исключительно с использованием российских криптографических алгоритмов, стандартизированных в серии ГОСТ.

Среди ключевых вендоров на этом рынке можно выделить:

1. «ИнфоТеКС» с семейством продуктов ViPNet. Это, пожалуй, самый известный российский бренд в области защищенных сетей. ViPNet TLS Gateway представляет собой высокопроизводительный криптошлюз, обеспечивающий аутентификацию пользователей по сертификатам и организацию защищенных соединений по протоколу TLS с использованием российских криптоалгоритмов (ГОСТ Р 34.10-2012 для электронной подписи, ГОСТ 28147-89 для шифрования и имитозащиты). Продукты ViPNet используются для защиты удаленного доступа сотрудников, сдачи

электронной отчетности, дистанционного банковского обслуживания и электронного документооборота.

2. «Код Безопасности» с решением «Континент TLS VPN». Это средство криптографической защиты информации сертифицировано ФСБ и ФСТЭК России и активно применяется для защиты удаленного доступа в государственных и финансовых организациях.

3. «С-Терра СиЭсПи». Решения этой компании сочетают проверенные мировые протоколы (IKE/IPsec) с российскими ГОСТ криптоалгоритмами, что позволяет обеспечивать конфиденциальность и целостность передаваемых данных, одновременно выполняя требования регуляторов. Оборудование «С-Терра» входит в число рекомендованных для защиты подключения к системе межведомственного электронного взаимодействия РФ (СМЭВ РФ).

4. «КриптоПро» с решением NGate. Универсальный шлюз удаленного доступа и VPN, сертифицированный ФСБ России, позволяющий импортозаместить зарубежные аналоги, в частности Cisco AnyConnect. NGate поддерживает протоколы TLS и IPSec в соответствии с российскими криптостандартами и предоставляет возможность двухфакторной аутентификации.

Важно отметить, что все эти решения не только проходят сертификацию в ФСБ, но и включаются в Единый реестр российских программ для ЭВМ и БД Минцифры, что является обязательным условием для использования в государственных и многих коммерческих организациях. Более того, облачные провайдеры, такие как Selectel, уже предлагают своим клиентам сервис «ГОСТ VPN», где защищенное подключение организуется с использованием оборудования ViPNet Coordinator, а шифрование трафика осуществляется в полном соответствии с требованиями ФСБ и ФСТЭК. ГК «Солар» также предоставляет сервис ГОСТ VPN, который получил аттестат соответствия высшему, первому уровню защищенности персональных данных (УЗ-1) и

первому классу защищенности государственных информационных систем (К1).

Государственные информационные системы: ЕСИА как единый центр аутентификации

Говоря об удаленном доступе к информационным ресурсам в масштабах всей страны, нельзя обойти вниманием Единую систему идентификации и аутентификации (ЕСИА), которая обеспечивает санкционированный доступ граждан и организаций к информации в государственных и иных информационных системах. Хотя технически ЕСИА и портал «Госуслуги» — это разные системы, для большинства пользователей они неразрывно связаны.

Архитектура ЕСИА построена на принципах централизованного управления идентификационными данными. Система использует протокол OAuth 2.0 / OpenID Connect для авторизации доступа к подключенным сервисам. С 2025 года были введены новые требования по безопасности: все информационные системы, интегрируемые с ЕСИА, обязаны использовать сертифицированные СКЗИ класса КС3, пройти аттестацию по требованиям информационной безопасности, а взаимодействие осуществлять через шлюзовой модуль (API Gateway). В системе безопасности самого портала «Госуслуги» используется комплексный набор механизмов: межсетевые экраны (Next-Generation Firewall), средства анализа содержимого, системы предотвращения вторжений (IPS/IDS), антивирусные средства и средства мониторинга защищенности. Таким образом, ЕСИА является не просто удобным интерфейсом, а мощной инфраструктурой защиты, обеспечивающей безопасную аутентификацию миллионов пользователей при удаленном доступе к государственным услугам.

Актуальные угрозы и статистика утечек

Ужесточение требований к защите удаленного доступа — не бюрократическая прихоть, а вынужденная реакция на реальную угрозовую обстановку. Статистика последних лет в России выглядит крайне тревожно. По данным компании F6, в 2025 году в открытом доступе оказалось более 760

млн строк с персональными данными россиян. Хотя количество инцидентов утечек (250 в 2025 году против 455 в 2024-м) снизилось, общий объем скомпрометированных записей персональных данных в 2025 году составил 1 343 млн.

Эксперты отмечают, что большинство утечек данных происходит через скомпрометированные учетные записи сотрудников, полученные с помощью фишинга или подобранные в результате атак перебора паролей. Удаленный доступ, особенно если он не защищен должным образом, является одним из основных векторов атак. Злоумышленники взламывают подрядчиков для атак через цепочку поставок, а привилегированные пользователи становятся основной мишенью.

Показательно, что за 2025 год аналитики F6 зафиксировали активность 27 прогосударственных хакерских групп, нацеленных на Россию и страны СНГ, причем 7 из них были выявлены впервые. Количество атак программ-вымогателей выросло на 15%, и в 15% инцидентов целью злоумышленников было не получение выкупа, а разрушение инфраструктуры. Эти цифры наглядно демонстрируют, что защита удаленного доступа перестала быть внутренним делом отдельной организации — это вопрос национальной кибербезопасности.

Вызовы импортозамещения и пути их решения

Одной из главных проблем для российских компаний при построении системы защищенного удаленного доступа сегодня является необходимость импортозамещения. Массовый уход зарубежных вендоров оставил многие организации без привычных средств защиты, поддержки и обновлений. Переход на российские аналоги — процесс сложный, дорогостоящий и требующий высокой квалификации.

Тем не менее, российский ИБ-рынок демонстрирует впечатляющую динамику. Согласно заявлениям вендоров, в ИБ-отрасли продукция российского производства почти вытеснила иностранное ПО и постепенно приходит на смену зарубежному оборудованию. При этом ключевая задача —

не просто заменить «импорт на импорт», а адаптировать лучшие мировые практики под российские реалии и нормативную базу.

Власти, в свою очередь, стимулируют этот процесс административными мерами. Проект постановления правительства РФ, разработанный Минцифры, предполагает, что право на обязательную предустановку приложений на устройства, продаваемые в России, сохраняется только в том случае, если сервисы компании не функционируют при активированном у пользователя VPN. Кроме того, обсуждается возможность лишения статуса аккредитованных ИТ-компаний, чьи сервисы обеспечивают доступ к ресурсам через VPN. Хотя прямых запретов для граждан пока не вводится, тренд на полную локализацию трафика и контроль над каналами передачи данных очевиден.

Заключение

Информационная система защиты удаленного доступа к информационным ресурсам в Российской Федерации сегодня представляет собой уникальный феномен. С одной стороны, это высокотехнологичная и строго регламентированная среда, в которой переплелись требования ФСТЭК, ФСБ, Минцифры и отраслевых регуляторов. С другой стороны, это быстрорастущий рынок отечественных решений — от криптошлюзов ViPNet и «Континента» до PAM-систем «Солар» и облачных сервисов ГОСТ VPN.

Главный вывод, который можно сделать, заключается в следующем: удаленный доступ в России перестал быть «зоной компромисса» между удобством и безопасностью. Новый Приказ ФСТЭК №117, архитектура Zero Trust, обязательное использование ГОСТ-шифрования и жесткий контроль привилегированных пользователей означают, что безопасный удаленный доступ становится единственно возможным.

Для российских организаций это означает необходимость комплексной трансформации. Недостаточно купить VPN-шлюз — нужно внедрять PAM, переходить на сертифицированные СКЗИ, проводить аттестацию информационных систем и обучать персонал. Однако альтернативы нет: в

условиях нарастающего числа киберугроз и геополитического давления защита удаленного доступа — это не просто соблюдение формальных требований, а вопрос выживания бизнеса и сохранения государственных информационных ресурсов. И российская индустрия информационной безопасности, опираясь на мощный научно-технический задел в области криптографии и системного администрирования, готова к этим вызовам.

Использованные источники:

1. Бабиш А. В., Баранова Е. К. Проектирование систем защищенного удаленного доступа: Учебное пособие. — М.: ИНФРА-М, 2024.
2. Лукацкий А. В. Бизнес-затраты на информационную безопасность. — 3-е изд. — М.: Альпина Паблишер, 2024. (В части обоснования выбора отечественных средств защиты).
3. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. — М.: ДМК Пресс, 2025. — 520 с.