

СОГЛАСОВАНО:

Заместитель генерального директора по
цифровой трансформации

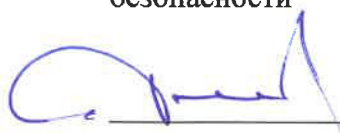


«04» 08 2026 г.

Д.А. Анищенко

УТВЕРЖДАЮ:

Заместитель генерального директора по
безопасности



«04» 08 2026 г.

В.В. Катков

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на оказание услуг по повышению уровня защищенности технических и программных средств
в части инфраструктурных сервисов и информационных систем
ПАО «Россети Центр»

Термины, определения и сокращения

DNS	(Domain Name Service) распределенная, иерархически организованная масштабируемая система хранения и обработки сетевой идентификационной информации, функционирующая на прикладном уровне (Application Layer) стека TCP/IP и модели OSI
HTTP	(Hypertext Transfer Protocol) сетевой протокол прикладного уровня стека TCP/IP, функционирующий по бесстатусной модели «клиент-сервер» и предназначенный для распределенной, совместной работы с гипермедийными информационными системами
HTTPS	(Hyper Text Transfer Protocol Secure) защищенная модификация протокола прикладного уровня HTTP, представляющая собой технологический стек, в котором транспортный синтаксис и семантика сообщений HTTP инкапсулируются внутрь криптографического протокола TLS (или исторически SSL) для обеспечения сквозной безопасности передаваемых данных
IP	(Internet Protocol) маршрутизируемый сетевой протокол прикладной независимости, относящийся к сетевому уровню и составляющий фундаментальную основу межсетевого взаимодействия в стеке протоколов TCP/IP
LDAP	(Lightweight Directory Access Protocol) сетевой протокол прикладного уровня (Application Layer) стека TCP/IP, функционирующий по модели «клиент-сервер» и предназначенный для централизованного поиска, извлечения, аутентификации и управления структурированной информацией об объектах и ресурсах в специализированных службах каталогов
RFC	(Request for Comments) официальная, серийно пронумерованная и неизменяемая публикация в форме технического документа, содержащая спецификации, стандарты, протоколы, отчеты об исследованиях и методические рекомендации, на основе которых обеспечивается архитектурная и технологическая совместимость компонентов глобальной сети Интернет
SMTP	(Simple Mail Transfer Protocol) сетевой протокол прикладного уровня стека TCP/IP, функционирующий по модели «клиент-сервер» и предназначенный для надежной и эффективной передачи, маршрутизации и ретрансляции сообщений электронной почты в асинхронных распределенных сетях связи
TCP	(Transmission Control Protocol) дуплексный, ориентированный на соединение транспортный протокол, обеспечивающий гарантированную, последовательную и безошибочную доставку структурированных потоков байтов между процессами на конечных узлах сети
TCP/IP	сетевая модель передачи данных, представленных в цифровом виде. Модель описывает способ передачи данных от источника информации к получателю.
TLS	(Transport Layer Security Protocol) криптографический протокол общего назначения, функционирующий на стыке транспортного и прикладного уровней (модель TCP/IP), который предназначен для обеспечения конфиденциальности, целостности и аутентификации данных при их транзите в распределенных компьютерных сетях
UDP	(User Datagram Protocol) минималистичный сетевой протокол транспортного уровня, предназначенный для передачи данных в виде

	независимых пакетов (датаграмм) без предварительного установления логического соединения и без обеспечения механизмов контроля доставки.
URL	(Uniform Resource Locator) стандартизированная символьная строка, выполняющая функцию унифицированного сетевого идентификатора, которая не только уникально именуется конкретный информационный ресурс в пространстве имен Интернета, но и однозначно определяет его местонахождение, предоставляя первичный механизм доступа к нему посредством явного указания протокола взаимодействия.
VLAN	(Virtual Local Area Network) логическая топология сети, сконфигурированная на канальном уровне модели OSI поверх физической инфраструктуры коммутации, обеспечивающая разделение единого широковебического домена на множество изолированных сегментов
ГОСТ	Государственный стандарт
ИБ	Информационная безопасность
ИС	Информационная система, включенная в рамки оказания услуги
ИТ	Информационные технологии
ЛВС	Локальная вычислительная сеть
Модель OSI	Абстрактная семиуровневая концептуальная и архитектурная схема, стандартизирующая процессы сетевого взаимодействия и передачи данных в гетерогенных вычислительных системах
ОРД	Организационно-распорядительный документ
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
Поверхность атаки	Общее количество возможных уязвимых мест
ППР	План производства работ
СК	Служба каталогов
Стек TCP/IP	стандартизированная иерархическая совокупность сетевых протоколов различных уровней, обеспечивающая сквозное межсетевое взаимодействие, адресацию, маршрутизацию и гарантированную доставку данных в гетерогенных децентрализованных компьютерных сетях
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЧТЗ	Частное техническое задание

1. Общие сведения об Услугах

Заказчик – ПАО «Россети Центр»

Места оказания услуг:

Исполнительный аппарат	119017, г. Москва, ул. Малая Ордынка, д. 15
Белгородэнерго	308009, г. Белгород, ул. Преображенская, д. 42
Брянскэнерго	241050, г. Брянск, ул. Советская, д.35
Воронежэнерго	394033, г. Воронеж, ул. Арзамасская, 2
Костромаэнерго	156961, г. Кострома, пр. Мира, д.53
Курскэнерго	305029, г. Курск, ул. К. Маркса, д.27
Липецкэнерго	398059, г. Липецк, ул. 50 лет НЛМК, д.33
Орелэнерго	302030, г. Орёл, пл. Мира, д.2
Смоленскэнерго	214019, г. Смоленск, ул. Тенишевой, д.33

Тамбовэнерго	392030, г. Тамбов, Моршанское шоссе, 23
Тверьэнерго	170006, г. Тверь, ул. Бебеля, д.1
Ярэнерго	150003, г. Ярославль, ул. Воинова, д. 12

Исполнитель – юридическое лицо, выбранное Заказчиком на конкурсной основе для оказания услуг.

2. Цели оказания Услуг

Целью оказание Услуг является повышение уровня защищенности технических и программных средств путем оптимизации конфигураций как на открытом уровне, так и на уровне недокументированных конфигурационных возможностей ПО и ИС, за счет уменьшения поверхности атаки в части инфраструктурных сервисов и информационных систем ПАО «Россети Центр», входящих в границы Услуг.

3. Задачи оказания Услуг

Задачами оказания Услуг являются:

- проведение обследования ИТ- и ИБ-активов, архитектуры ИС, включенных в рамки оказания услуги (далее – ИС) и подготовка отчета об обследовании ИС и дорожной карты изменений.

- разработка частных технических заданий (далее – ЧТЗ) и планов производства работ (далее – ППР) по результатам предварительного обследования ИС и в соответствии со следующими нормативными источниками и методическими документами по оптимизации конфигураций ИС:

- методический документ ФСТЭК России 'Меры защиты информации в государственных информационных системах';
- приказ ФСТЭК России N239 'Об утверждении Требований по обеспечению безопасности значимых объектов КИИ'. Применяется к ИС, отнесенным к значимым объектам критической информационной инфраструктуры и приравненных к ним;
- рекомендации CIS Benchmarks для соответствующего класса ОС и прикладного ПО, входящих в рамки услуг;
- руководства и рекомендации производителей ПО, функционирующего в рамках каждой ИС, в части конфигурационных параметров безопасности.
- внутренние ОРД заказчика в части обеспечения информационной безопасности, предоставленные заказчиком в соответствии с п. 8.1 ТЗ.

- реализация, совместно со специалистами Заказчика, изменений конфигураций ИС, в соответствии с ППР, согласованными в рамках п. 5, в соответствии с процессом управления изменениями Заказчика. Подготовка результирующего документа – отчет об оказании услуг.

- проведение сравнительного инструментального анализа уровня защищенности до и после реализации изменений конфигураций ИС, а именно:

- базовое сканирование исходного состояния ИС (средство инструментального сканирования согласуется с Заказчиком на этапе Обследования);
- контрольное сканирование ИС, после применения изменений;
- сравнительный анализ результатов сканирования с подготовкой – Отчета по результатам оказания услуги по каждой ИС. Отчет должен подтвердить исполнение всех требований ЧТЗ.

4. Границы оказания Услуг

Перечень ИС Заказчика, включенных в рамки оказания Услуг, и их характеристики приведены в Таблице 1.

Таблица 1. Перечень ИС Заказчика, включенных в рамки оказания Услуг

№ п/п	Наименование ИС	Количество аппаратных серверов	Количество виртуальных серверов
1.1	Внешний DNS сервис	0	2
1.2	Служба каталогов	17	17
1.3	Внешний почтовый шлюз (Kaspersky Secure Mail Gateway)	0	3
1.4	Система учета массовых отключений (СУМО)	0	1
1.5	Система прокси (Kaspersky Web Traffic Security)	0	2
1.6	Система резервного копирования (КиберБэкап)	1	2
1.7	Система виртуализации (zVirt)	46	0

Системы № 1.1, 1.3, 1.4, 1.5, 1.6 являются централизованными.

Системы № 1.2, 1.7 являются централизованными с филиальной инфраструктурой.

В рамках оказания услуги входит создание ЧТЗ (по одному ЧТЗ на каждую ИС) и ППР (количество ППР зависит от характера планируемых изменений конфигураций и может варьироваться для каждой ИС в зависимости от технической необходимости).

Перечень разрабатываемых в рамках услуги документов приведен в Табл.2.

Таблица 2. Перечень разрабатываемых документов

№ п/п	Наименование разрабатываемых документов
1.	Отчет об обследовании (включает перечень обследованного оборудования и ПО, общую информацию и архитектуру, возможности унификации, конфигурации компонентов и оценку защищенности)
2.	Частные технические задания
3.	Планы производства работ
4.	Дорожная карта изменений
5.	Отчет по результатам оказания услуги с описанием реализованных изменений и сравнительным анализом
6.	Презентация

Проведение изменений на смежных информационных и инфраструктурных системах в рамках оказания услуги не входит. Работы по изменению конфигурации ограничены конфигурацией самих ИС и ОС, на которых они функционируют. В случае обнаружения критических недостатков конфигураций смежных систем, рекомендации по их корректировке включаются Исполнителем в Отчёт об обследовании.

5. Состав, содержание и описание Услуг

Исполнитель обязан оказать Услуги в составе и объеме, указанном в Табл. 3.

Таблица 3. Состав, содержание и описание Услуг

№ п/п	Наименование Услуги	Состав Услуг	Отчетная документация
1.	Повышение уровня защищенности технических и программных средств в части инфраструктурных сервисов и информационных систем	1.1 Предварительное обследование	1. Отчет об обследовании
		1.2 Разработка ЧТЗ и ППР	1. Дорожная карта изменений 2. ЧТЗ (по 1 (одному) ЧТЗ на каждую ИС) 3. ППР (не менее 1 (одного) ППР на каждую ИС)
		1.3 Реализация изменений	-
		1.4 Подготовка отчетных документов	1. Отчет по результатам оказания услуги 2. Презентация

Обследование (документальное и инструментальное) проводится для каждой ИС на предмет уязвимостей, результаты включаются в Отчет об обследовании.

По результатам обследования и анализа архитектуры реализации, Исполнитель создает ЧТЗ на каждую из ИС, Дорожную карту изменений и ППР для проведения работ по изменению конфигураций.

До и после применения изменений в ИС необходимо провести инструментальное сканирование ИС на предмет уязвимостей программными средствами сканирования, согласованными Заказчиком (MaxPatrol, XSpider и т.п.), с подготовкой файл-отчетов.

На основании разработанных и согласованных Заказчиком ППР Исполнитель совместно с сопровождением работника отдела информационной безопасности и экспертов Заказчика проводит конфигурационные изменения в соответствии с регламентом изменений Заказчика и фиксирует полученный результат.

6. Требования к отчетности

6.1 В рамках предоставления Услуг Исполнитель разрабатывает и предоставляет Заказчику следующую отчетность:

- отчет об обследовании – включая результаты документального и инструментального обследования;
- дорожная карта применения изменений;
- комплект ЧТЗ (7 шт. ЧТЗ в составе комплекта);
- комплект ППР (не менее 7 шт. ППР в составе комплекта);
- отчет по результатам оказания услуги – включая описание реализованных изменений конфигураций и сравнительным анализом уровня защиты;
- презентация.

6.2 Вся отчетная документация предоставляется по форме Исполнителя и направляется Заказчику для согласования до даты завершения подэтапа оказания Услуги. Документация предоставляется в печатной и электронной форме.

7. Сроки оказания Услуг

Дата начала оказания Услуг – 18.11.2026

Длительность оказания Услуг – 22 (двадцать два) рабочих дня, не позднее 18.12.2026 г.

Поэтапная длительность Услуг приведена в Табл. 4

Таблица 4. Поэтапная длительность Услуг

№ п/п	Наименование Услуг	Состав Услуг	Дата начала подэтапа	Дата завершения подэтапа
1.	Повышение уровня защищенности технических и программных средств в части инфраструктурных сервисов и информационных систем	1.1 Предварительное обследование	02.11.2026	23.11.2026
		1.2 Разработка ЧТЗ, Дорожной карты и ППР	24.11.2026	27.11.2026
		1.3 Реализация изменений	30.11.2026	11.12.2026
		1.4 Подготовка отчетных документов	14.12.2026	18.12.2026

8. Требования к порядку оказания Услуг

8.1 Заказчик в течение 2 (двух) рабочих дней после начала оказания Услуг предоставляет по запросу Исполнителя следующую информацию:

- проектную и эксплуатационную документацию по ИС (при наличии);
- комплекты ОРД в части обеспечения информационной безопасности;
- комплекты ОРД (в том числе регламенты) в части процесса управления изменениями (при наличии);
- отчеты по результатам последнего (актуального) аудита/пентеста;
- контакты ответственных работников, включенных в рабочую группу.

8.2 Заказчик на время оказания Услуг обеспечивает создание и функционирование Рабочей группы, включающей в себя:

- работников, ответственных за эксплуатацию ИС (как со стороны ИТ-подразделений, так и со стороны ИБ-подразделений), имеющих административные права доступа в ИС и/или права согласования проведения изменений конфигураций ИС;
- работника отдела информационной безопасности, обладающего полномочиями сопровождения работ по изменению конфигураций ИС;
- куратора услуги со стороны Заказчика;
- сервис-менеджера со стороны Исполнителя;
- экспертов со стороны Исполнителя.

8.3 На этапе проведения обследования ИС Заказчик обеспечивает возможность проведения удаленных собеседований с работниками Заказчика, имеющими административные права доступа в ИС для сбора информации о текущей конфигурации ИС и особенностях ее эксплуатации, а также проведения инструментального обследования.

8.4 Заказчик обеспечивает предоставление Исполнителю удаленного доступа в соответствии с процедурой «Управление доступами и полномочиями в информационных системах ПАО «Россети Центр» и ПАО «Россети Центр и Приволжье» РГ ЦА БП 15/07-08/2022 для обеспечения возможностей проведения работ по изменению конфигураций ИС (согласно согласованным ППР) и проведения инструментального обследования.

8.5 Проведение инструментального обследования проводится при условии предоставления Заказчиком письма-согласия на проведение работ, содержащего перечень IP-адресов внешнего сетевого периметра (при наличии) и внутренних сетевых объектов.

8.6 Исполнитель, в целях исключения негативного влияния изменений конфигураций на сервисы Заказчика, на этапе создания ППР проводит тестирование предлагаемых конфигураций на стенде (тестовом контуре) Заказчика. Заказчик на время оказания Услуг предоставляет тестовый контур для следующих ИС:

- система учета массовых отключений (СУМО);
- система виртуализации.

При этом ППР в обязательном порядке должен включать в себя следующие разделы:

- этапность внесения конфигурационных изменений;
- тестирование работоспособности ИС;
- план отката изменений ИС.

8.7 Время проведения работ по согласованным ППР согласуется с Заказчиком.

8.8 При создании ППР Исполнитель должен ориентироваться на минимизацию времени потенциального простоя ИС.

8.9 Работы по изменению конфигураций ИС проводятся в соответствии и объеме с согласованными Заказчиком ЧТЗ и ППР, с сопровождением экспертов Заказчика и работника отдела информационной безопасности. Заказчик обеспечивает возможность участия экспертов Заказчика и работника отдела информационной безопасности при проведении работ по изменению конфигураций.

8.10 Для оценки изменений, реализованных в процессе оказания Услуг, используются результаты инструментального обследования. Инструментальное обследование проводится Исполнителем в два этапа: первый – в рамках предварительного обследования, второй – после завершения проведения изменений конфигураций ИС. Инструментальное обследование проводится средствами сканирования Заказчика: MaxPatrol VM, Kaspersky Security Centre, утилита AVZ.

8.11 По результатам внедрения изменений конфигураций ИС и подготовки отчета по результатам оказания услуги Исполнитель также готовит Презентацию. Результаты оказания услуги должны быть предоставлены Заказчику в рамках отдельной встречи.

9 Требования по информационной безопасности

9.1 Доступ сотрудников Исполнителя в помещения Заказчика и к его ИТ-инфраструктуре осуществляется строго по предварительным заявкам и в согласованные технологические окна.

9.2 Все действия специалистов Исполнителя в системах Заказчика должны выполняться под именными (персонифицированными) учетными записями. Использование общих (разделяемых) учетных записей запрещено.

9.3 При необходимости удаленного доступа Исполнитель обязан использовать исключительно предоставленные Заказчиком защищенные каналы (VPN) с обязательной двухфакторной аутентификацией (2FA). Все сессии удаленного контроля подлежат обязательной записи и аудиту со стороны Заказчика.

9.4 Мобильные устройства и ноутбуки Исполнителя, подключаемые к технологическому контуру Заказчика, должны пройти проверку на отсутствие вредоносного ПО, иметь установленные актуальные обновления ОС и сертифицированное антивирусное ПО.

10. Перечень руководящих нормативных и правовых документов

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Указ Президента Российской Федерации от 30 марта 2022 года № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»;
- Приказ ФСТЭК России от 21 декабря 2017 года № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- Приказ ФСТЭК России от 25 декабря 2017 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Методический документ «Методика оценки угроз безопасности информации» (утвержден ФСТЭК России 5 февраля 2021 года);
- Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;
- ГОСТ Р 51275-2006 «Защита информации. Объект автоматизации. Факторы, воздействующие на информацию. Общие положения»;
- ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
- ГОСТ Р ИСО/МЭК 27001–2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

11. Требования по обеспечению режима конфиденциальности

11.1 До начала выполнения работ и предоставления доступов Исполнитель обязан подписать с Заказчиком Соглашение о неразглашении конфиденциальной информации (NDA).

11.2 Исполнитель несет полную юридическую и финансовую ответственность за действия своего персонала, включая разглашение коммерческой тайны, персональных данных или внутренней информации Заказчика.

11.3 Все сотрудники Исполнителя должны быть под роспись ознакомлены с локальными нормативными актами Заказчика в области ИБ перед допуском к информационным системам и инфраструктурным сервисам.

12. Требования к Исполнителю

12.1 «Исполнитель в течение 3 (трех) рабочих дней с даты заключения Договора обязан предоставить Заказчику официальное подтверждение (авторизационное письмо/сертификат) от производителей ПО (АО «Лаборатория Касперского», ООО «Киберпротект», ООО «ОРИОН»), подтверждающее право Исполнителя оказывать услуги по настройке и технической поддержке данного ПО на объектах Заказчика».

12.2 Исполнитель должен иметь действующую лицензию Федеральной службы по техническому и экспортному контролю (ФСТЭК России) на деятельность по технической защите конфиденциальной информации. В перечень выполняемых работ и оказываемых услуг, составляющих лицензируемый вид деятельности, в обязательном порядке должно входить:

- контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
- установка, монтаж, испытания, ремонт средств защиты информации (программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

13. Меры по предоставлению национального режима.

Основание: постановление Правительства Российской Федерации от 23.12.2024 № 1875 «О мерах по предоставлению национального режима при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, закупок товаров, работ, услуг отдельными видами юридических лиц».

Предоставление национального режима в соответствии с ПП 1875 от 23.12.2024.	
ОКПД 2	Мера применения национального режима (запрет, ограничение, преимущество)
62.02.30.000	Не применяется*

*Запрет по строке 146 Приложения №1 постановления Правительства Российской Федерации от 23.12.2024 № 1875 устанавливается в отношении Программ для электронной вычислительной машины и (или) баз данных. Настоящая закупка проводится на право заключения Договора на оказание услуг по повышению уровня защищенности технических и программных средств в части инфраструктурных сервисов и информационных систем.

В рамках настоящей закупочной процедуры Программы для электронной вычислительной машины и (или) базы данных не закупаются.