

УТВЕРЖДАЮ

Первый заместитель генерального
директора – главный инженер
ОАО «МАПИД»

А.С. Маслов

06.08.2026 г.

ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ЗАДАНИЕ

на проведение процедуры закупки по выбору организации на оказание услуг по
продлению неисключительных прав (продление лицензий) на использование
программного обеспечения «Dr.Web» или аналогичного ПО, совместимого с
установленным

1. Процедуру закупки провести в соответствии с «Порядком осуществления закупок товаров (работ, услуг) за счет собственных средств ОАО «МАПИД», утвержденным приказом №309 от 09.07.2026.
2. Проведение процедуры закупки возложить на конкурсную комиссию ОАО «МАПИД», утвержденную приказом №10-ОД от 15.01.2026 года.
3. Требования к закупаемому товару/работам/услугам:
 - 3.1 наименование предмета заказа: продление неисключительных прав Dr.Web Desktop Security Suite (или аналогичного ПО, совместимого с установленным) в количестве 500 пользовательских лицензий на защиту рабочих станций + 300 дополнительных лицензий, Dr.Web Server Security Suite (или аналогичного ПО, совместимого с установленным) в количестве 5 лицензий на защиту серверов, Dr.Web Mail Security Suite (или аналогичного ПО, совместимого с установленным) в количестве 10 лицензий на защиту почтового трафика;
 - 3.2 описание технических, технологических, конструктивных и иных характеристик и показателей закупаемого товара/работ/услуг: в соответствии с требованиями, предъявляемыми к программному комплексу «Dr.Web»;
 - 3.3 ориентировочная стоимость (стартовая): 32 000 руб.
 - 3.4 порядок формирования цены: маркетинговые исследования.
4. Условия поставки/подряда/оказания услуг:
 - 4.1 порядок оплаты: предпочтительна отсрочка платежа;
 - 4.2 сроки поставки/выполнения работ/оказания услуг: август 2026 года;
 - 4.3 место поставки/выполнения работ/оказания услуг: ул. Р. Люксембург, 205.
5. Источник финансирования: собственные средства.
6. Срок для подготовки и проведения процедуры закупки: не позднее «20» августа 2026 г.
7. Потенциальные участники: ---
8. Иные сведения: ---.
9. Приложение: Приложение 1 на 3 листа, докладная записка Игнатика П.А. от 03.08.2026.

Задание подготовил
Ведущий инженер-программист
по информационной безопасности

И.о. начальника отдела информационных
технологий, ведущий администратор системный

Начальник службы контроля и
охранно-режимной деятельности

П.А.Игнатик

Д.И.Кузюкович

И.А.Дорошкевич

Техническое задание

Для нужд ОАО «МАПИД» необходимо осуществить продление неисключительных прав Dr.Web Desktop Security Suite в количестве 500 пользовательских лицензий на защиту рабочих станций + 300 дополнительных лицензий, Dr.Web Server Security Suite в количестве 5 лицензий на защиту серверов, Dr.Web Mail Security Suite в количестве 10 лицензий на защиту почтового трафика;. Срок действия продленной лицензии – 1 (Один) год с даты окончания текущей лицензии (31.08.2026г).

1. Общие требования:

Предоставляемые неисключительные права (лицензии) на использование ПО включают в себя право на воспроизведение, ограниченное правом инсталляции, копирования и запуска, предоставляемое с единственной целью передачи этого права конечным пользователям.

Предоставленная лицензия должна быть полностью совместима с уже установленным ПО: LBW-BC-12M-500-B3, Неисключительное право на использование ПО Dr.Web Desktop Security Suite в количестве 500 пользовательских лицензий на защиту рабочих станций, LBS-AC-12M-5-B3, Неисключительное право на использование ПО Dr.Web Server Security Suite в количестве 5 лицензий на защиту серверов, LBP-AAC-12M-10-B3, Неисключительное право на использование ПО Dr.Web Mail Security Suite в количестве 10 лицензий на защиту почтового трафика Server.

Программный продукт должен иметь сертификат соответствия 2013/027/ВУ.

Программный интерфейс всех антивирусных средств, включая средства управления, должен включать русский и английский язык.

Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке.

Антивирусные средства должны включать:

- лицензионный файл ключа;
- программные средства антивирусной защиты рабочих станций и серверов;
- программные средства централизованного управления, мониторинга и обновления на ОС Windows, Linux;
- обновляемые антивирусные базы данных;

2. Требования к программному обеспечению антивирусной защиты рабочих станций:

Программные средства антивирусной защиты рабочих станций под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:

- Microsoft Windows 10 (32-bit и 64-bit),
- Microsoft Windows 11 (32-bit и 64-bit)

Программные средства антивирусной защиты рабочих станций под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:

- резидентный антивирусный мониторинг;
- антивирусное сканирование по команде пользователя или администратора;
- защита от еще неизвестных вредоносных программ на основе эвристического анализа;
- обнаружение руткитов (скрытых файлов/системных аномалий);
- защита от шифровальщиков и несанкционированного изменения файлов;
- блокировка сменных носителей информации и устройств (USB);

- интеграция с центром безопасности Windows;
- самозащита антивирусных продуктов от вредоносных программ, злоумышленников или неквалифицированных пользователей;
- проверка наличия актуальных обновлений системы;

3. Требования к программному обеспечению антивирусной защиты серверов:

Программные средства антивирусной защиты систем серверов под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС в русской или английской редакции:

- Microsoft Windows Server 2008 R2;
- Microsoft Windows Server 2012, 2012 R2;
- Microsoft Windows Server 2016-2025;

Программные средства антивирусной защиты файловых серверов под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:

- резидентный антивирусный мониторинг;
- антивирусное сканирование по команде пользователя или администратора;
- защита от еще неизвестных вредоносных программ на основе эвристического анализа;
- обнаружение руткитов (скрытых файлов/системных аномалий);
- защита от шифровальщиков и несанкционированного изменения файлов;
- интеграция с центром безопасности Windows;
- самозащита антивирусных продуктов от вредоносных программ, злоумышленников;
- проверка наличия актуальных обновлений системы;
- наличие системы централизованного сбора с клиентских рабочих мест потенциально опасных образцов вредоносного кода и возможность централизованно или вручную отправлять образцы вредоносного кода вирусным экспертам.

4. Требования к системе управления антивирусной защитой:

Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:

- установку и удаление программных средств антивирусной защиты на рабочие места пользователей и сервера;
- автоматизированное обновление программных средств антивирусной защиты и антивирусных баз;
- сбор логов и аудит инцидентов по рабочим станциям;
- учет и аудит лицензий;
- разделение рабочих станций на группы с индивидуальными настройками защиты.

5. Требования к обновлению антивирусных баз:

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

- реализована возможность создания зеркала обновлений для экономии трафика;
- зеркало обновлений можно создать на любом ПК сети;
- типы обновлений: обновление БД сигнатур вирусов, программных компонентов, обновление ядра.

6. Требования к технической поддержке.

На протяжении всего срока действия лицензионного соглашения должна быть обеспечена техническая поддержка производителя, включающая в себя:

- Выпуск исправлений для программного обеспечения (устраняющих подтвержденные дефекты программного обеспечения);
- Выпуск регулярных обновлений для баз данных;
- Поддержка в случае ошибок, затрагивающих функциональность программного обеспечения;
- Поддержка в случае ошибок и вопросов по регулярным обновлениям баз;
- Поддержка в случае ошибочных срабатываний программного обеспечения;
- Поддержка в случае восстановления утраченных или поврежденных данных лицензии;
- Поддержка по вопросам о необходимом порядке действий, таким как:
 - порядок и источник загрузки программного обеспечения;
 - основные вопросы по установке;
- Поддержка по вопросам, связанным с приобретением и продлением лицензии на пользование программного обеспечения.

Техническая поддержка предоставляется по следующим каналам: электронная почта или портал самообслуживания.

7. Гарантийные обязательства

Гарантия предоставляется на весь объем оказываемых услуг