**УТВЕРЖДАЮ**

Зам. председателя

Комиссии по закупкам

**\_\_\_\_\_\_\_\_\_\_\_\_** С.А. Иваненко

«27» июня 2025 г.

**ИЗВЕЩЕНИЕ О ПРОВЕДЕНИИ**

**ЗАПРОСА КОТИРОВОК В ЭЛЕКТРОННОЙ ФОРМЕ**

на право заключения договора на

предоставление на условиях простой (неисключительной) лицензии права на использование программы: антивирус DrWeb.

ВЕРСИЯ 3

г. Севастополь

2025

**1.Общие сведения.**

1.1. Запрос котировок не является формой открытого конкурса или публичного аукциона, поэтому он не попадает под урегулирование 447-449 статей 1 части ГК РФ и 1057-1061 статей 2 части ГК РФ. Также Заказчик имеет право отказаться от всех полученных Заявок по любой причине или прекратить процедуру закупки до окончания срока подачи заявок, не неся при этом никакой ответственности перед Участниками.

1.2. ООО «СЕВАСТОПОЛЬЭНЕРГО» (далее по тексту «Заказчик») проводит запрос котировок на **Предоставление на условиях простой (неисключительной) лицензии права на использование программы: антивирус DrWeb.** (далее по тексту – Услуги).

Контактное лицо по вопросам технического задания: Тлеуов Илья Кадырович,

Телефон:. 8 (8692) 57-23-23

e-mail: [Ilya.Tleuov@sevenergo.net](mailto:Ilya.Tleuov@sevenergo.net)

Контактное лицо по общим вопросам организации закупки: Папоротный Алексей Петрович,

Телефон: 8 (8692) 53 98 00

e-mail: [Aleksey.paporotnyj@sevenergo.net](mailto:Aleksey.paporotnyj@sevenergo.net)

Официальный адрес электронной почты: [kanc@sevenergo.net](mailto:kanc@sevenergo.net)

1.3. В настоящем запросе котировок может принять участие любое юридическое или группа лиц, физическое лицо, в том числе индивидуальный предприниматель, прошедшее аккредитацию в порядке, установленном регламентом Услуги электронной площадки «Электронные торги России».

# **2. Требования к качеству, техническим характеристикам, функциональным характеристикам (потребительским свойствам), к эксплуатационным характеристикам предмета закупки.**

2.1. Услуги должны соответствовать установленным характеристикам согласно Техническому заданию (Приложение № 4) к настоящей документации.

2.2. Наименование и технические характеристики Услуг указаны в Техническом задании (Приложение № 4) к настоящей документации.

2.3. Оказание Услуг должно соответствовать условиям Технического задания (Приложение № 4).

# **3. Требования к описанию Участниками закупки оказываемых Услуг.**

3.1. Описание Услуги в соответствии с Техническим заданием (Приложение № 4) документации о закупке.

# **4. Место, условия и сроки выполнения Услуг.**

4.1. Место выполнения Услуг: в соответствии с Техническим заданием (Приложение № 4).

4.2. Условия выполнения Услуг: в соответствии с Техническим заданием (Приложение № 4).

4.3. Срок выполнения Услуг: в соответствии с Техническим заданием (Приложение № 4).

**5. Требования к гарантийному сроку и (или) объему предоставления гарантий качества оказываемых Услуг.**

5.1. В соответствии с условиями проекта договора.

# **6. Требования к содержанию, форме, оформлению и составу Заявки.**

6.1. Заявка на участие в запросе котировок, все документы, входящие в состав Заявки, должны быть составлены на русском языке.

6.2. Участники закупки формируют Заявки на участие в Запросе котировок, в форме электронного документа в соответствии с требованиями электронной торговой площадки.

6.3. Заявка на участие в запросе котировок должна содержать документы и сведения, указанные в п. 21 настоящей документации.

6.4. Заявки на участие в запросе котировок направляются оператору электронной площадки (https://torgi82.ru/) в форме электронных копий документов, подписанных с помощью электронной подписи (далее – ЭП).

6.5. Заявка должна быть составлена в соответствии с Приложением № 2 к настоящей документации.

6.6. Все документы, входящие в заявку, должны быть подготовлены на русском языке за исключением тех документов, оригиналы которых на ином языке. Указанные документы должны быть представлены на языке оригинала с подтверждением подлинности указанных документов (апостилированные копии, либо нотариально заверенный перевод на русский язык, либо перевод на русский язык, заверенный участником Запроса или лицом, уполномоченным таким участником Запроса).

6.7. Документы, подписанные ЭП Участника закупки, лица, имеющего право действовать от имени Участника закупки, признаются документами, подписанными собственноручной подписью участника закупки, лица, имеющего право действовать от имени участника, заверенные печатью организации.

6.8. Наличие ЭП участника закупки подтверждает, что документ отправлен от имени участника закупки и являются точными цифровыми копиями документов-оригиналов.

6.9. Любой Участник закупки вправе подать только одну Заявку.

6.10. Любой Участник запроса котировок имеет возможность отозвать или изменить поданную Заявку до дня и времени окончания срока подачи Заявок. После отзыва Заявки Участник запроса котировок имеет возможность повторно сформировать и подать до дня и времени окончания срока подачи заявок.

6.11. Соблюдение Участником указанных требований означает, что информация и документы, входящие в состав Заявок на участие в запросе котировок, поданы от имени Участника, и он несет ответственность за подлинность и достоверность информации и документов.

**7. Сведения о начальной (максимальной) цене договора.**

7.1. **639 920,72 (шестьсот тридцать девять тысяч девятьсот двадцать) рублей, 72 копейки.**

**8. Расходы Подрядчика при исполнении условий Договора.**

8.1. Начальная (максимальная) цена Договора включает в себя все расходы Поставщика, связанные с исполнением обязательств по договору с учетом расходных материалов, расходов на перевозку, страхование, уплату таможенных пошлин, налогов и других обязательных платежей, предусмотренных законодательством РФ.

**9. Начальная (максимальная) сумма цен за 1 (единицу) работ (услуг)**

9.1. **не установлено.**

**10. Форма, сроки и порядок оплаты Услуги.**

10.1. В соответствии с проектом договора.

**11. Порядок формирования цены договора.**

11.1. В соответствии с Планом закупок товаров (работ, услуг) ООО «СЕВАСТОПОЛЬЭНЕРГО», с учетом расходов на перевозку, страхование, уплату таможенных пошлин, налогов и других обязательных платежей.

**12. Порядок формирования начальной (максимальной) цены договора.**

12.1. Определена методом сопоставимых рыночных цен (анализа рынка).

**13. Порядок, место, дата начала и дата и время окончания сроков подачи заявок на участие в закупке.**

13.1. Заявки на участие в Запросе котировок предоставляются по адресу: https://torgi82.ru/, начиная с момента размещения настоящего извещения и закупочной документации по запросу котировок: **с** **момента размещения Извещения до 09-00 (мск) «03» июля 2025 года.**

**14. Требование к Участникам закупки и привлекаемым ими субподрядчикам и (или) Подрядчикам и перечень документов, предоставляемых для подтверждения их соответствия указанным требованиям.**

14.1. Для участия в запросе котировок Участник закупок должен соответствовать следующим требованиям:

- Соответствие участника закупки требованиям законодательства РФ к лицам, осуществляющим поставки товаров, выполнение работ, оказание услуг, которые являются предметом закупки;

- Не проводится процедура ликвидации, отсутствует решение арбитражного суда о признании банкротом;

- Неприостановление деятельности участника закупки в порядке, установленном Кодексом Российской Федерации об административных правонарушениях, на день подачи Заявки на участие в закупке;

- Отсутствие у участника задолженности по начисленным налогам, сборам и иным обязательным платежам;

- Отсутствие сведений об Участнике закупок в реестре недобросовестных поставщиков, предусмотренного Федеральным законом от 18.07.2011 г. № 223-ФЗ;

-Отсутствие в предусмотренном Федеральным законом от 05.04.2013 № 44-ФЗ  «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» реестре недобросовестных поставщиков сведений об Участнике;

- Отсутствие на момент проведения Закупки вступивших в силу решений суда о ненадлежащем исполнении участником закупки обязательств по договорам (контрактам) на поставку товаров, выполнение работ, одноименных закупаемым работам за последние 2 года;

- отсутствие у участника Запроса задолженности по начисленным налогам, сборам и иным обязательным платежам в бюджеты любого уровня или государственные внебюджетные фонды за прошедший календарный год, размер которой превышает 5% балансовой стоимости активов участника Запроса по данным бухгалтерской отчетности за последний завершенный отчетный период;

- участник закупки не должен являться юридическим или физическим лицом, в отношении которого применяются специальные экономические меры, предусмотренные подпунктом а) пункта 2 Указа Президента РФ от 03.05.2022 г. № 252 «О применении ответных специальных экономических мер в связи с недружественными действиями некоторых иностранных государств и международных организаций», либо являться организацией, находящейся под контролем таких лиц;

- участник закупки не должен являться иностранным агентом в соответствии с Федеральным законом от 14 июля 2022 года №255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием».

14.2. Требования к Участникам закупок применяются в равной мере ко всем Участникам запроса котировок.

14.3. При выявлении несоответствия Участника закупок требованиям, установленным в извещении и документации запроса котировок, Комиссия отказывает Участнику закупок в допуске к участию, и заявка признается несоответствующей требованиям.

14.4. Перечень документов, представляемых Участниками закупки для подтверждения их соответствия установленным требованиям, указаны в п. 21.

14.5. Участник обязан:

* + - * 1. предоставить разъяснения отдельных положений своей заявки по требованию Заказчика;
        2. не предоставлять заведомо ложных и недостоверных сведений в составе заявки;
        3. не изменять и не отзывать заявку на участие в закупке после окончания срока подачи заявок;
        4. обеспечить действие заявки на условиях и в сроки, изложенных и установленных в такой заявке Участника;
        5. самостоятельно отслеживать размещенные Заказчиком в ЕИС разъяснения и изменения Извещения, Документации, информацию о принятых в ходе процедуры закупки решениях, сформулированных в соответствующих протоколах/уведомлениях.

**15. Формы, порядок, дата начала и дата окончания срока предоставления Участникам закупки разъяснений положений Закупочной документации.**

15.1. Любой Участник Запроса вправе направить запрос разъяснений положений документации в письменной форме в срок не позднее, чем за три рабочих дня до дня окончания срока подачи Заявок через ЭТП, в порядке предусмотренном регламентом Работы ЭТП.**.**

15.2. Запрос на разъяснение положений закупочной документации подается на сайте <https://torgi82.ru/> в конкретной процедуре закупки и подписывается ЭП.

15.3. Заказчик в течение 3 (трех) рабочих дней со дня поступления указанного запроса, размещает в Единой информационной системе zakupki.gov.ru ответ с разъяснениями положений вместе с указанием сути поступившего запроса, в том случае, если поступивший запрос поступил Заказчику не позднее, чем за 3 (три) рабочих дня до дня окончания срока подачи заявок. При этом Заказчик вправе не осуществлять такое разъяснение в случае, если указанный запрос поступил позднее, чем за 3 (три) рабочих дня до даты окончания срока подачи Заявок.

15.4. Ответ с разъяснениями вместе с указанием сути поступившего запроса размещаются в Единой информационной системе и на сайте оператора электронной площадки, без указания источника поступления запроса.

**16. Дата рассмотрения Заявок Участников закупки и подведения итогов Закупочной процедуры.**

16.1. Открытие доступа состоится **09:00 (время московское) «03» июля 2025 года.**

16.2. Рассмотрение заявок состоится **не позднее 14:00 (время московское) «08» июля 2025 года.**

16.3. Подведение итогов состоится **не позднее 14:00 (время московское) «10» июля 2025 года.**

**17. Критерии оценки и сопоставления заявок на участие в закупке.**

17.1. Цена договора – значимость критерия – 100%.

**18. Порядок оценки и сопоставления заявок на участие в закупке.**

18.1. Закупочная комиссия осуществляет отбор и оценку Заявок и в соответствии с критериями и сопоставлением Заявок выявляет лучшие условия исполнения договора установленными Документацией о запросе котировок.

18.2. Оценка Заявок включает отборочную стадию и оценочную стадию:

а) Отборочная стадия:

В рамках отборочной стадии Закупочная комиссия проверяет:

- правильность оформления Заявки;

- соответствие участников закупки требованиям извещения и документации о закупке;

- соответствие Услуги требованиям документации о закупке.

18.3. Заказчик имеет право отказаться от всех полученных заявок и/или прекратить процедуру закупки в любой момент, до окончания срока подачи заявок без объяснения причин, не неся при этом никакой ответственности перед Участниками.

18.4. Заказчик вправе изменить сроки (дату и время) рассмотрения заявок и/или подведения итогов закупки по сравнению с указанными в Извещении и Документации датами, без уведомления Участников закупки о переносе таких сроков.

18.5. Заказчик вправе отклонить заявку Участника в случае, если его Цена договора превышает установленную начальную (максимальную) сумму цен за единицу либо превышает установленную начальную (максимальную) цену отдельно взятой позиции продукции, установленной в Техническом задании (если в Техническом задании указано несколько позиций).

18.6. Заказчик вправе отклонить заявку Участника в случае предоставления недостоверных и/или противоречивых и/или ложных сведений, содержащихся в составе заявке на день его подачи.

18.7. При проверке правильности оформления Заявки Закупочная комиссия вправе не обращать внимания на мелкие недочеты и погрешности, которые не влияют на существо Заявки.

18.8. При проведении рассмотрения котировок, Закупочная комиссия может запросить у Участников разъяснения и дополнения их Заявок. При этом Закупочная комиссия не вправе запрашивать разъяснения или требовать документы, меняющие суть Заявки.

18.9. При рассмотрении Заявок на участие в закупках, Участник закупки не допускается Закупочной комиссией в случаях:

- не предоставление документов и сведений, требование о наличии которых установлено Документацией о запросе котировок либо наличие в таких документах недостоверных сведений об участнике запроса котировок или о Услугах, на оказание которых размещалась закупка;

- несоответствие Заявки на участие в запросе котировок требованиям, установленным Документацией о проведении запроса котировок.

18.10. Заказчик вправе проверять соответствие предоставленных участником закупки сведений и документов действительности, в том числе путем направления запросов в государственные органы, лицам, указанным в заявке.

18.11. Результаты рассмотрения оформляются протоколом, в котором содержаться сведения о Заказчике, о проводимом запросе котировок, дата, время номер и количество Заявок, поданных на участие в данном Запросе, об отклоненных Заявках с обоснованием причин отклонения.

б) Оценочная стадия:

18.12. В рамках оценочной стадии Закупочная комиссия оценивает, сопоставляет Заявки и проводит их ранжирование по степени предпочтительности для Заказчика, исходя из критериев указанных в п.18.14 настоящей документации.

18.13. Оценка и сопоставление Заявок осуществляются Комиссией в целях выявления лучших условий исполнения Договора в соответствии с единственным критерием «Цена договора». Указанный критерий применяется на этапе оценки и сопоставления заявок. Договор с победителем запроса заключается на фиксированную сумму, указанную в Извещении. Предложение участника не должно превышать указанной в настоящем Извещении начальной (максимальной) суммы цен за единицу либо установленной начальной (максимальной) цены отдельно взятой позиции продукции, установленной в Техническом задании (если в Техническом задании указано несколько позиций). В случае несоответствия данному требованию, заявка участника подлежит отклонению.

*Оценка и сопоставление заявок по критерию «Цена договора» проводится вне зависимости от применяемой участником закупки системы налогообложения.*

18.14. На основании оценки и сопоставления Заявок, каждой Заявке присваивается порядковый номер относительно других Заявок, по мере уменьшения степени выгодности, исполнения договора.

18.15. Заявке, в которой содержатся лучшие условия исполнения договора, присваивается первый номер.

18.16. В случае если в нескольких Заявках содержатся одинаковые условия исполнения договора, меньший порядковый номер присваивается Заявке, которая поступила ранее других Заявок на участие в запросе котировок.

18.17. Результаты оценки и сопоставления Заявок, оформляется итоговым протоколом, в котором содержаться сведения о Заказчике, о проводимом запросе котировок, дата, время номер и количество Заявок, поданных на участие в данном Запросе, об отклоненных Заявках с обоснованием причин отклонения, сведения о победителе в проведении запроса котировок, о признании запроса котировок несостоявшимся (если запрос котировок признан несостоявшимся), а также цене закупаемых Услуг.

18.18. Протоколы, составляемые в ходе заседания Закупочной комиссии, подписываются всеми присутствующими на заседании членами Закупочной комиссии и размещаются в Единой информационной системе и на сайте ЭТП не позднее чем через 3 (Три) дня со дня их подписания.

**19. Описание предмета закупки.**

19.1. Описание предмета закупки должно соответствовать Техническому заданию (Приложение № 4).

**20. Описание закупаемой Услуги**

Описание закупаемой Услуги должно соответствовать Техническому заданию (Приложение № 4).

**21.** **Требование к составу Заявки на участие в запросе котировок.**

21.1. Участнику необходимо предоставить в составе Заявки следующие документы:

- опись документов (Приложение №1);

- заявка на участие в запросе котировок, оформленная в соответствии с Приложением № 2;

- анкету Участника запроса котировок (Приложение №3);

- описание Услуг в соответствии с Техническим заданием (Приложение №4);

- коммерческое предложение;

- копию устава/другого учредительного документа;

- копию документа удостоверяющего личность индивидуального предпринимателя/физического лица, только для индивидуальных предпринимателей или физических лиц;

- полученную не ранее чем за 6 (Шесть) месяцев до дня размещения извещения в Единой информационной системе и на сайте https://torgi82.ru/ о проведении запроса котировок копию выписки из Единого государственного реестра юридических лиц (для юридического лица), выписки из Единого государственного реестра индивидуальных предпринимателей (для индивидуальных предпринимателей);

- документ, подтверждающий полномочия лица на осуществление действий от имени юридического лица (копия решения о назначении или об избрании либо приказа о назначении физического лица на должность, в соответствии с которым такое физическое лицо обладает правом действовать от имени участника закупки и лица, выступающего на стороне участника закупки без доверенности. В случае, если от имени юридического лица действует иное лицо, Заявка на участие в запросе котировок должна содержать также соответствующую доверенность, заверенную печатью и подписанную руководителем юридического лица или уполномоченным этим руководителем лицом, либо заверенную копию такой доверенности.

- копию свидетельства о постановке на учет в налоговом органе;

- согласие на обработку персональных данных (Приложение №5), *только для индивидуальных предпринимателей или физических лиц*;

- документы, подтверждающие соответствие Участника требованиям, установленным в Техническом задании (Приложение №4) *(при необходимости)*

# **22. Условия признания запроса котировок несостоявшимся.**

22.1. Запрос котировок, может быть признан несостоявшимся в нескольких случаях:

- не подано ни одной заявки либо подана только одна заявка на участие в Запросе;

- все Заявки участников запроса котировок признаны несоответствующими установленным требованиям.

22.2. В случае если запрос котировок признан несостоявшимся, могут быть приняты следующие решения:

- осуществить закупку у единственного поставщика.

# - заключить договор в случае, если единственная предоставленная заявка от участника, подавшего его, полностью соответствуют требованиям Извещения и Документации;

# - провести повторную закупку любым из способов, в любой форме принятых в Положении, который Заказчик сочтет целесообразным использовать.

# **23. Порядок заключения договора по итогам запроса котировок.**

23.1. По результатам запроса котировок договор заключается не ранее чем через 10 (Десять) дней и не позднее чем через 20 (Двадцать) дней с даты размещения в ЕИС итогового протокола, составленного по результатам конкурентной закупки.

23.2. В случае если победитель в проведении запроса котировок, не представил Заказчику подписанный со своей стороны договор в течение 5 (пяти) дней, такой победитель признается уклонившимся от заключения договора.

23.3. Заказчик вправе заключить договор с участником, занявшим второе рейтинговое место в запросе котировок, если заявка такого Участника соответствует требованиям Извещения и Документации.

23.4. Договор заключается не позднее, чем через 20 (Двадцать) дней после размещения итогового протокола запроса котировок в Единой информационной системе. Заказчик заключает договор, который составляется путем включения в него условий исполнения договора, предусмотренных Извещением и Документацией и предложенных победителем в Заявке на участие в запросе котировок.

23.5. В случае, если при заключении и исполнении договора изменяется объем, цена или сроки исполнения договора по сравнению с указанными в протоколе, составляемом по результатам проведенного запроса котировок, то не позднее 10 (Десяти) рабочих дней со дня внесения таких изменений в договор, информация об этих изменениях подлежит размещению в единой информационной системе.

23.6. В случае расторжения договора в связи с неисполнением или ненадлежащим исполнением Подрядчиком своих обязательств по такому договору, Заказчик вправе заключить договор с Участником закупки, заявке которого присвоено второе рейтинговое место, с согласия такого Участника. Если до расторжения договора Подрядчиком частично исполнены обязательства по такому договору, при заключении нового договора объем подлежащих оказанию Услуг должен быть уменьшен с учётом оказанных Услуг по договору, ранее заключенному с победителем закупки. При этом цена договора должна быть уменьшена пропорционально объему оказанных Услуг.

**24. Отзыв заявки на участие в закупке.**

24.1. Участник размещения заказа вправе изменить, дополнить или отозвать свою Заявку после ее подачи в любой момент до даты окончания подачи заявок.

**25. Прочие положения.**

25.1. Участник самостоятельно несет все расходы, связанные с подготовкой и подачей заявки, участием в закупке и заключением договора, а Заказчик по этим расходам не отвечает и не имеет обязательств независимо от хода и результатов данной закупки.

25.2. Заказчик обеспечивает разумную конфиденциальность относительно всех полученных от Участников сведений, в том числе содержащихся в заявках. Предоставление этой информации другим Участникам или третьим лицам возможно только в случаях, прямо предусмотренных действующим законодательством РФ.

**26. Внесение изменений в Извещение и Документацию.**

26.1. Решение о внесении изменений в Извещение и/или Документацию может быть принято Заказчиком в любой момент до окончания срока подачи заявок.

26.2. В случае внесения изменений до окончания срока подачи заявок (в том числе продления срока окончания подачи заявок) Участник закупки, уже подавший заявку, вправе принять любое из следующих решений:

отозвать поданную заявку;

не отзывать поданную заявку, продлив при этом срок её действия на соответствующий период времени и внеся в неё другие необходимые (по мнению Участника закупки) изменения;

не отзывать поданную заявку и не изменять срок её действия.

26.3. Внесение изменений в Извещение и Документацию после окончания срока подачи заявок не допускается за исключением случаев изменения сроков (дат) рассмотрения Заявок Участников закупки и подведения итогов процедуры закупки.

26.4. Изменения в извещение и/или документацию о закупке размещаются Заказчиком в том же порядке, в котором осуществлялось официальное размещение извещения и документации о закупке в ЕИС.

26.5. Участники закупки должны самостоятельно отслеживать размещенные Заказчиком в ЕИС разъяснения и изменения Документации, информацию о принятых в ходе процедуры закупки решениях, сформулированных в соответствующих протоколах/уведомлениях

**27. Запрет и ограничение закупок товаров (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), происходящих из иностранных государств, работ, услуг, соответственно выполняемых, оказываемых иностранными лицами.**

Запрет не применяется на основании пп. «к» п. 10 Постановление №1875 (запрет, предусмотренный пунктом 1 Постановления №1875, может не применяться при осуществлении в соответствии с Федеральным законом "О закупках товаров, работ, услуг отдельными видами юридических лиц" закупок товаров, указанных в позициях 1 - 21, 30, 32, 45 - 47, 49 - 52, 55 - 60, 62, 69 - 86, 88, 92 - 128, 137, 138, 140 - 145 приложения N 1 к настоящему постановлению, извещение об осуществлении которых размещено в единой информационной системе и приглашение принять участие в которых направлено либо договор с единственным поставщиком (исполнителем, подрядчиком) при осуществлении которых заключен до 1 июля 2025 г.)

**1.1.** Документом, подтверждающими страну происхождения товара **Российская Федерация, является - номер реестровой записи из реестра российской промышленной продукции,** предусмотренного статьей 17.1 Федерального закона "О промышленной политике в Российской Федерации", содержащей в том числе:

* информацию о совокупном количестве баллов за выполнение (освоение) на территории Российской Федерации соответствующих операций (условий) (если в отношении такого товара постановлением Правительства Российской Федерации от 17 июля 2015 г. N 719 "О подтверждении производства российской промышленной продукции" за выполнение (освоение) на территории Российской Федерации соответствующих операций (условий) установлены требования о совокупном количестве баллов), которое составляет или превышает значение, определенное постановлением Правительства Российской Федерации от 17 июля 2015 г. N 719 "О подтверждении производства российской промышленной продукции" для целей осуществления закупок;
* информацию об уровне радиоэлектронной продукции (для товара, являющегося в соответствии с постановлением Правительства Российской Федерации от 17 июля 2015 г. N 719 "О подтверждении производства российской промышленной продукции" радиоэлектронной продукцией первого уровня или радиоэлектронной продукцией второго уровня).

**1.2.** Документом, подтверждающими страну происхождения товара из государств - **членов Евразийского экономического союза (за исключением Российской Федерации), является - номер реестровой записи из евразийского реестра промышленных товаров государств - членов Евразийского экономического союза,** порядок формирования и ведения которого устанавливается правом Евразийского экономического союза (далее - евразийский реестр промышленных товаров), содержащей в том числе:

* информацию о совокупном количестве баллов за выполнение (освоение) на территории Евразийского экономического союза соответствующих операций (условий) (если в отношении такого товара правом Евразийского экономического союза за выполнение (освоение) на территории Евразийского экономического союза соответствующих операций (условий) установлены требования о совокупном количестве баллов), которое составляет или превышает значение, определенное правом Евразийского экономического союза;

информацию об уровне радиоэлектронной продукции (для товара, являющегося в соответствии с правом Евразийского экономического союза радиоэлектронной продукцией первого уровня или радиоэлектронной продукцией второго уровня).

**Приложение №1**

**ОПИСЬ ДОКУМЕНТОВ**

**представляемых для участия в Запросе котировок на право заключения договора**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. Настоящим \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ подтверждает, что для

*(указать наименование (фамилию, имя, отчество Участника закупки*)

участия в запросе котировок на\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, нами

*(предмет договора)*

направляются нижеперечисленные документы:

|  |  |  |  |
| --- | --- | --- | --- |
| **№№ п\п** | **Наименование документа** | **Кол-во листов** | **Номера страниц** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |

**Руководитель организации** *(для юридических лиц)* \_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

*(подпись) Ф.И.О.*

**Участник закупки** *(для физических лиц)* \_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

*(подпись) Ф.И.О.*

# 

# 

# 

# **Приложение №2**

# **ЗАЯВКА**

**на участие в Запросе котировок на право заключения договора**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*(оформляется на бланке организации (для юридических лиц)*

1. Изучив извещение и документацию о проведении запроса котировок на право заключения договора на \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(наименование предмета договора)*

опубликованное в сети Интернет по адресу zakupki.gov.ru и на ЭТП <https://torgi82.ru/> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(полное наименование участника запроса котировок с указанием организационно-правовой формы)*

ИНН \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(ИНН участника запроса котировок),*

юридический адрес \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(юридический адрес участника запроса котировок)*

фактический адрес: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(фактический адрес участника запроса котировок)*

выражает согласие исполнить указанные в извещении о проведении запроса котировок требования и направляет настоящую заявку:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Наименование передаваемых прав** | | | | | **Цена,**  **руб.** | | | **Кол-во, шт.** | | **Стоимость, руб.** |
| 1 | Неисключительное право на использование ПО Dr.Web Desktop Security Suite (LBW-BC-12M-340:340-D3), Неисключительное право на использование ПО Dr.Web Server Security Suite (LBS-AC-12M-35:30-D3), Неисключительное право на использование ПО Dr.Web Mail Security Suite (LBP-AAC-12M-250:250-D3), Неисключительное право на использование ПО Dr.Web Gateway Security Suite (LBG-AC-12M-130:130-D3) | | | | |  | | | 1 | |  |
| 2 | Дистрибутив Медиа-комплект «Dr.Web для бизнеса сертифицированный» ФСТЭК России (сертификат №3509 действует до 27.01.2029г.) | | | | |  | | | 2 | |  |
|  | Общая стоимость: | | | | |  | | | | | |
|  |  |  |  |  |  |  |  | **ИТОГО:** | |  | |

1. Мы подтверждаем согласие на **Предоставление на условиях простой (неисключительной) лицензии права на использование программы: антивирус DrWeb** для нужд ООО «СЕВАСТОПОЛЬЭНЕРГО»в соответствии с требованиями технического задания и проекта договора.

3. Настоящей Заявкой на участие в запросе котировок сообщаем, что в отношении \_

*(наименование Участника закупки (для юридических лиц), наименование индивидуального предпринимателя)*

-не проводится процедура ликвидации, отсутствует решение арбитражного суда о признании банкротом;

-не приостановлена деятельность, предусмотренная Кодексом Российской Федерации об административных правонарушениях.

- у участника отсутствует задолженность по начисленным налогам, сборам и иным обязательным платежам.

- об участнике отсутствуют сведения в реестре недобросовестных поставщиков, предусмотренном статьей 5 Федерального закона от 18 июля 2011 года № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц».

- участник закупки не является юридическим или физическим лицом, в отношении которого применяются специальные экономические меры, предусмотренные подпунктом а) пункта 2 Указа Президента РФ от 03.05.2022 г. № 252 «О применении ответных специальных экономических мер в связи с недружественными действиями некоторых иностранных государств и международных организаций», либо являться организацией, находящейся под контролем таких лиц;

- участник закупки не является иностранным агентом в соответствии с Федеральным законом от 14 июля 2022 года №255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием».

4. Если наша Заявка будет принята, и мы будем признаны победителем в проведении запроса котировок, мы берем на себя обязательства подписать договор, в соответствии с требованиями документации о запросе котировок и условиями нашей заявки.

5. Мы подтверждаем, что соответствуем требованиям, установленным в документации о запросе котировок, и заверяем правильность всех данных, указанных в Заявке.

Контактное лицо: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(указать ФИО, должность, контактные телефоны, факс, адрес, E-mail)*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(Наименование Участника закупки) (подпись) (расшифровка подписи)*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(Должность подписавшего заявку) (подпись) (расшифровка подписи)*

# **Приложение №3**

**Анкета участника закупки**

|  |
| --- |
| **1. Полное и сокращенное наименования организации и ее организационно-правовая форма:**  (на основании Учредительных документов установленной формы (устав, положение и др.), свидетельства о государственной регистрации, свидетельства о внесении записи в единый государственный реестр юридических лиц)  Ф.И.О. участника закупки–физического лица/физического лица, зарегистрированного в качестве индивидуального предпринимателя |
| 1. Юридический, почтовый и фактический адрес |
| **3. Регистрационные данные:**  Дата, место и орган регистрации юридического лица,  (на основании Свидетельства о государственной регистрации или иного документа, выдаваемого при регистрации)  Паспортные данные для участника закупки – физического лица/физического лица, зарегистрированного в качестве индивидуального предпринимателя  Дата, место и орган регистрации физического лица, зарегистрированного в качестве индивидуального предпринимателя (на основании Свидетельства о государственной регистрации в качестве индивидуального предпринимателя) |
| 1. **ИНН, КПП, ОГРН, ОКПО** |
| **5. Банковские реквизиты:**  5.1. Наименование обслуживающего банка  5.2. Расчетный счет  5.3. Корреспондентский счет  5.4. Код БИК |
| 1. **Использование упрощенной системы налогообложения (УСН)**   указать использует / не использует |
| 1. **Принадлежность к субъектам малого и среднего предпринимательства** |
| 1. **Контактное лицо участника закупки,**   **номер контактного телефона,**  **электронной почты,**  **факса участника закупки** |

**Приложение №4**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**Предоставление на условиях простой (неисключительной) лицензии права на использование программы: антивирус DrWeb**

**Общая информация об объекте закупки**

**Объект закупки**: Продление имеющейся лицензии на использование антивирусного программного обеспечения Dr.Web

**Место оказания услуги**: г. Севастополь, ул.Хрусталёва, дом 44.

1. **Общие требования**
   1. Участники конкурса на использование антивирусного программного продукта должны иметь статус официального партнера компании производителя, что является подтверждением их квалификации и прав на поставку антивирусных продуктов и/или лицензий. При заключении контракта необходимо предоставить копии документов, подтверждающих статус официального партнера компании производителя.
   2. Все компоненты Системы должны принадлежать одной торговой марке с единой службой технической поддержки на русском языке. Техническая поддержка должна предоставляться непосредственно производителем поставляемых программных продуктов.
   3. В рамках всей организации должны использоваться единые антивирусные средства независимо от степени конфиденциальности обрабатываемой информации. Отдельно стоящие ПК, не подключённые к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, должны быть защищены интегрированным программным продуктом, включающим в себя защиту от проникновения и активации всех типов вредоносных программ (антивирус), спама (персональный антиспам) и обеспечивать возможность их включения в единую систему антивирусной защиты.
   4. Поставляемые средства защиты должны представлять масштабируемое решение, обеспечивающее устойчивое функционирование в локальной сети заказчика.
   5. Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке.
   6. Все антивирусные средства, функционирующие под операционной системой типа Windows, включая средства управления, должны обладать контекстной справочной системой на русском языке.
   7. Участник конкурса должен предоставить единый серийный номер для всех поставляемых по условиям конкурса продуктов.
   8. Поставляемый серийный номер должен иметь возможность отложенной активации. Срок действия лицензионных ключевых файлов на все поставляемые по условиям конкурса программные продукты должен начинаться с момента активации серийного номера.
   9. Система лицензирования не должна иметь привязку к используемому на защищаемых объектах аппаратному обеспечению. Система должна позволять перенос лицензий с одних защищаемых объектов (в том числе рабочих станций и серверов) на иные без необходимости перепривязки или получения дополнительных лицензий.
   10. Срок поставки: 15 (пятнадцать) рабочих дней с момента подписания договора.
2. **Требования к предмету закупки (Спецификация)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование** | **Характеристика** | **Ед. изм.** | **Кол-во:** |
| 1. | Неисключительное право на использование ПО Dr.Web Desktop Security Suite (LBW-BC-12M-340:340-D3),  Неисключительное право на использование ПО Dr.Web Server Security Suite (LBS-AC-12M-35:30-D3),  Неисключительное право на использование ПО Dr.Web Mail Security Suite (LBP-AAC-12M-250:250-D3),  Неисключительное право на использование ПО Dr.Web Gateway Security Suite (LBG-AC-12M-130:130-D3) | Продление имеющейся лицензии на использование антивирусного программного обеспечения Dr.Web Desktop Security в количестве 340 шт., Dr.Web Server Security Suite в количестве 35 шт., Dr.Web Mail Security Suite в количестве 250 шт., Dr.Web Gateway Security Suite в количестве 130 шт.  Антивирусные средства должны включать:  -программные средства защиты рабочих станций;  -программные средства защиты файловых серверов;  -программные средства защиты почтовых серверов и шлюзов;  -программные средства защиты интернет шлюзов;  -программные средства централизованного управления, мониторинга и обновления;  -обновляемые базы данных сигнатур вредоносных программ всех типов и атак;  -эксплуатационную документацию на русском языке.  Срок действия продлеваемой лицензии: не менее 12 месяцев.  Данная лицензия после получения Сублицензиатом подлежит активации, в последствии с помощью Лицензиата происходит разбивка на 2 серийных номера:  1 серийный номер (Dr.Web Desktop Security Suite 320 ПК, Dr.Web Server Security Suite 30 серверов, Dr.Web Gateway Security Suite 130 интернет шлюзов, Dr.Web Mail Security Suite 250 почтовых ящиков).  2 серийный номер (Dr.Web Desktop Security Suite 20 ПК, Dr.Web Server Security Suite 5 серверов).  Серийный номер имеющейся лицензии: 5LYT-579G-786P-GFA4 | шт. | 1 |
| 2. | Дистрибутив Медиа-комплект «Dr.Web для бизнеса сертифицированный»  ФСТЭК России (сертификат №3509 действует до 27.01.2029г.) | Поставка Dr.Web на материальном носителе осуществляется в виде записанных на электронных носителях установочных файлов Dr.Web, комплекта электронных справочных, содержащих подробные указания по приемке, установке, настройке и эксплуатации Dr.Web, а также формуляра на бумажном носителе, поставляемых в картонном конверте. | шт. | 2 |

\*В настоящее время в ИТ-инфраструктуре ООО «Севастопольэнерго» установлено, настроено, протестировано на совместимость с другим прикладным ПО и используется Dr.Web Desktop Security Suite на 350 рабочих станциях, и Dr.Web Server Security Suite на 30 файловых серверах, Dr.Web Mail Security Suite на 250 почтовых ящиках, Dr.Web Gateway Security Suite на 150 интернет-шлюзах.

Внедрение ПО других производителей означает необходимость переустановки, внедрения и настройки ПО на всех рабочих станциях и файловых серверах организации. Выполнение этих работ повлечет дополнительные финансовые расходы (привлечение персонала, обучение собственного персонала), а также займет значительное время, что неизбежно отразится на качестве и оперативности работы сотрудников организации. Таким образом, внедрение ПО других производителей, является нецелесообразным. В связи с вышеизложенным и необходимостью обеспечения соответствия приобретаемой лицензии используемому у Заказчика антивирусному программному обеспечению, эквивалент на указанную лицензию не предусмотрен согласно п.3 ч.6.1 ст.3 ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц" от 18.07.2011№223-ФЗ.

1. **Требования к программным средствам**
   1. Общие требования к системе антивирусной защиты
      1. Программные средства Системы должны обеспечивать определение угроз следующих типов:
         1. классических вирусов;
         2. троянских программ;
         3. руткитов;
         4. сетевых червей;
         5. рекламных программ;
         6. программ автодозвона на платные сайты;
         7. потенциально опасных приложений;
         8. прочих вредоносных программ.
      2. Антивирусная защита должна обеспечивать:
         1. обнаружение и удаление вирусов из файлов, упакованных программами типа PKLITE, LZEXE, DIET, COM2EXE и т.п.;
         2. обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками;
         3. обнаружение вирусов внутри контейнеров и архивных файлов формата ACE (до версии 2.0), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, ARJ, JAR, ISO (включая NRG, образы с нестандартным форматом сектора и не имеющие сигнатур), ZLIB, VCLZIP, VISE, PST, DMG, PDF, GHOST INSTALLER с зашифрованными контейнерами и т.д. без ограничений на уровень вложенности проверяемых объектов;
         4. обнаружение вирусов внутри контейнеров, не имеющих строгого формата (HTML, MIME);
         5. обнаружение вирусов внутри контейнеров с нечетким значением размера объекта (WISE, ACTIVE MARK, 7-ZIP, JAR, ASTRUM WIZARD, CHM, BINARYRES и т.д.);
         6. антивирусную проверку файлов и объектов, имеющих формат Smart Install Maker (SIM); DMG, HFS, XAR, Universal Binary (MacOS); SIS (Symbian 9); INNO SETUP (5.3.9 и выше); SETUP FACTORY (линейки 7,8); XENOCODE; TARMA INSTALL (линейка 3); XZ (UNIX); COMPRESS; SQUAHFS; CHILKAT ZIP; пакеты LHA (AWARD BIOS);
         7. антивирусную проверку в самораспаковывающихся архивах: AppPackager, Astrum Install Wizard, Create Install, Fly Studio, GSFX, Hot Soup, Inno Setup, Install Essen, Install Factory, Linder Setup, NSIS (NullSoft Installation System), RSFX, SEA, Setup Factory, Setup Generator Pro, SXA ZIP, Tarma Install, Thunder Setup System, Wise Installation System, Alloy;
         8. проверку исполняемых файлов упакованных следующими упаковщиками: PELOCK, ENIGMA Protector, NSPACK, NTKRNL, EXECRYPTOR, PESPIN, EXPRESSOR, ASPROTECT, PECOMPACT, PACKMAN, SEA, ULTRAPROTECT, ASPACK, PETITE, NEOLITE, GENPACKER, BERO, RCRYPTOR, PECRYPT, а также почтовых файлов Mozilla Thunderbird- вне зависимости от их размера;
         9. разбор неформатированных почтовых баз и обработка писем с высокой вложенностью (например, переписки с большим количеством ответов и пересылок RE/FW), поддержка формата TNEF;
         10. защиту от вредоносных программ, принадлежащих семействам вредоносных программ, информация о которых имеется в антивирусных базах, созданных после занесения соответствующей информации в антивирусные базы и еще не попавших на анализ в антивирусные лаборатории - как на основе эвристического анализа, так и с помощью технологии поиска похожих вирусов, основанной на анализе расположения участков кода в файле;
         11. обнаружение вредоносных объектов в HTML- и PDF-документах, включая обфусцированные эксплойты в JavaScript, находящиеся в документах данных типов. Возможность извлечения и анализа «невидимых» IFRAME-элементов. Возможность извлечения для проверки скриптов любой сложности и снятие с них защиты;
         12. обнаружение угроз по лицензионным данным (ASPROTECT, PEP и ENIGMA);
         13. обнаружение угроз направленных на 64-разрядные операционные системы, в том числе с помощью специальной 64-битной версии антируткит модуля
         14. обнаружение вредоносных объектов в DEX-файлах (Android).
      3. Используемое антивирусное ядро:
         1. не должно допускать снижение скорости проверки при увеличении размера антивирусных баз;
         2. в связи с возможностью исчерпания ресурсов ОС (в том числе места на диске, памяти) в ходе обработки специальным образом сформированных архивов автоматически выбирать уровень анализа упакованных объектов, а также механизм уменьшения размера промежуточных файлов. При выборе уровня анализа должен учитываться уровень загрузки системы
         3. в целях ускорения проверки архивов и упакованных файлов должно обеспечивать опознание вредоносных программ без запуска распаковщика;
         4. должно обеспечивать защиту от так называемых «почтовых бомб»;
         5. должно обеспечивать работу с файлами размером как менее, так и больше 2 ГБ;
         6. должно поддерживать работу с дисками с LBA-адресацией;
         7. в целях исключения «утечки» оперативной памяти должно использовать механизм распределения динамической памяти уровня антивирусного ядра.
   2. **Требования к системе управления антивирусной защитой (далее - Сервер управления)**
      1. Система управления должна быть построена по клиент-серверной архитектуре с возможностью построения иерархической системы серверов – с возможностью использования в системе антивирусного управления как главных, так подчиненных серверов.
      2. Система управления должна быть реализована на основе Web-интерфейса, поддерживающего Web-браузеры, используемые как в корпоративной сети, так и Web-браузеры, используемые на устройствах и компьютерах, имеющих доступ к сервисам управления антивирусной защитой извне корпоративной сети - в том числе Mozilla Firefox или Internet Explorer. Управление через данные браузеры должно быть доступно с любых ОС, имеющих возможность их установки и запуска.
      3. Система должна включать поддержку кластерного протокола, с помощью которого координируются действия над агентами защиты с разных антивирусных серверов
      4. Система управления должна быть доступной с любой операционной системы, поддерживающей браузеры Mozilla Firefox или Internet Explorer (в том числе с ОС Microsoft Windows и ОС типа UNIX (Linux, FreeBSD, Solaris)), без ограничений на использование последних версий браузеров и без доустановки какого-либо программного обеспечения как на стороне сервера управления, так и на стороне администратора Системы. Контроль работы Системы должен быть также возможен консоли управления, функционирующей на мобильных устройствах iPhone
      5. В целях безопасности все ПО, входящее в состав антивирусного сервера (в том числе необходимое для доступа с помощью браузера) должно поставляться в виде единого дистрибутива и принадлежать одной торговой марке.
      6. Система управления должна включать систему управления лицензиями, позволяющую распределять между серверами в рамках иерархической сети необходимое количество лицензий
      7. Установка антивирусного сервера Системы должна быть возможна на:
         1. Microsoft Windows Server 2008;
         2. Microsoft Windows Server 2008 R2
         3. Microsoft Windows Server 2012;
         4. Microsoft Windows Server 2012 R2
         5. Microsoft Windows Server 2016;
         6. Microsoft Windows Server 2019;
         7. Microsoft Windows 7;
         8. Microsoft Windows 8;
         9. Microsoft Windows 8.1;
         10. Microsoft Windows 10;
         11. FreeBSD 10.3 и выше;
         12. Linux, при наличии библиотеки glibc 2.13 и выше.
      8. Установка агента управления антивирусной защиты должна быть возможна на:
         1. Linux glibc 2.13 и выше для платформ Intel x86/amd64;
         2. Microsoft Windows XP Professional SP2 и выше;
         3. Microsoft Windows Server 2003 SP2;
         4. Microsoft Windows Vista (также с SP1 и выше);
         5. Microsoft Windows Server 2008 (также с SP1 и выше);
         6. Microsoft Windows 7;
         7. Microsoft Windows Server 2012 (также с R2);
         8. Microsoft Windows Server 2016;
         9. Microsoft Windows 8;
         10. Microsoft Windows 10;
         11. ОС Android 4.4 и выше;
         12. OS X/macOS версий 10.10-10.15.
      9. Система управления должна иметь возможность:
         1. просмотра и сравнения состава аппаратно-программного обеспечения на станциях антивирусной сети
         2. контроля неактивных станций антивирусной сети
         3. просмотра сессий пользователей антивирусной сети
         4. замены системного DNS
         5. использования как внутренней СУБД (поставляемой в составе дистрибутива антивирусного сервера), так и внешней (устанавливаемой отдельно до или после развертывания антивирусного сервера). При использовании внешней СУБД Система должна иметь возможность работы с ней как без установки дополнительное ПО (с СУБД MS SQL, Oracle), так и с помощью драйверов ODBC для операционных систем Windows и Linux (в том числе с СУБД PostgreSQL). Система должна иметь возможность замены типа используемой СУБД после установки серверной части – без необходимости переустановки серверной части Системы
         6. управления базой данных средствами системы управления, в том числе возможности очистки базы данных, ее анализа, выполнения произвольных SQL-запросов
         7. экспорта и импорта базы данных антивирусного сервера в XML-файл.
         8. создания иерархической сети антивирусных серверов. В случае реализации иерархической сети Система должна иметь возможность:
            1. объединения информации от нескольких серверов на одном.
            2. распределения рабочих станций между серверами для получения обновлений в целях снижения общей нагрузки на сеть.
            3. обмена статистикой в рамках одной иерархической сети между антивирусными серверами различных версий
            4. контроля отсутствия связанных серверов в расписании антивирусного сервера.
         9. построения многоуровневой системы управления с возможностью настройки ролей администраторов и пользователей, а также форм предоставляемой отчетности на каждом уровне;
         10. установки антивирусных агентов в сети, не использующей единого пароля доступа к рабочим станциям;
         11. централизованной настройки параметров защиты, уникальных для различных групп, в том числе для рабочих станций, находящихся в режиме off-line.
         12. централизованного сбора и просмотра статистической информации и создания отчетов о состоянии антивирусной защиты и их консолидации;
         13. интеграции в системы управления и информационные системы с помощью встроенного в систему API
         14. наличия множественных путей уведомления пользователей и администраторов путем посылки почтового сообщения, звукового оповещения, всплывающего окна, записи в журнал событий, SNMP-trap;
         15. оповещения о возникновении эпидемий (множественных инфекций)
         16. оповещения о наличии обновлений сервера
         17. отправки информационных сообщений пользователям по сети в режиме реального времени через Web-интерфейс Системы;
         18. обеспечения связи антивирусного сервера и клиентских частей через встроенный модуль в случае, когда они расположены в различных сетях, работающих по протоколам TCP/IP (в т.ч. IPv6), между которыми отсутствует маршрутизация пакетов
         19. самостоятельного написания обработчиков событий на языке Lua, а также выполнения произвольных Lua-скриптов с помощью средств системы управления.
      10. В случае интеграции с внешними подсистемами с помощью встроенного Web API, должна иметься возможность аудита действий, произведенных с помощью функций данного Web API
      11. Вне зависимости от типа антивирусного агента и защищаемой системы, Система должна обеспечивать реализацию следующих функциональных возможностей
          1. экспорта, импорта и распространения конфигураций групп, станций антивирусной сети или компонентов антивирусной защиты на другие группы, станции и компоненты, в том числе в целях изменения политик, применения их к определенным группам
          2. скачивания конфигурационных файлов с настройками подключения антивирусных агентов для ОС Android, Mac OS X и ОС семейства UNIX
          3. восстановления рабочих станций, случайно удаленных из системы защиты;
          4. централизованного обновления антивирусных баз на всех защищенных рабочих станциях, в том числе мобильных и находящихся в режиме off-line. Доставки обновлений на рабочие места пользователей как по расписанию, так сразу после их получения;
          5. обновления программных средств и антивирусных баз из разных источников, доставляемые как автоматически по каналам связи в пределах антивирусной сети, так и на отчуждаемых машинных носителях информации – путем ручной синхронизации информации между серверами и рабочими станциями
          6. обновления программных средств и антивирусных баз с помощью мобильного сервера обновлений, представляющего собой Сервер управления, развернутый на flash-диске;
          7. управления ревизиями обновлений продуктов, находящихся в репозитории антивирусного сервера, включая откат обновлений
          8. контроля результатов обновления антивирусного ПО на станциях антивирусной сети.
          9. организации межсерверного обмена согласно расписанию
          10. ограничения канала связи по группам
          11. наличия возможности групповых обновлений
          12. обновлений по защищенному каналу с использованием SSL-сертификатов
          13. организации отложенного обновления
          14. проверки обновлений на выбранных администратором компьютерах/группах перед распространением их на все клиентские компьютеры
          15. автоматического перехода установленного ПО на более новые версии, в том числе с возможностью выбора обновляемых компонентов;
      12. Программные средства управления для всех защищаемых ресурсов, реализованных на платформах ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:
          1. централизованной удаленной установки и деинсталляции программных средств, антивирусных баз и антивирусного ядра на защищаемые узлы сети – в том числе на станции, находящиеся в разных доменах.
          2. создания инсталляционных пакетов для конкретных защищаемых рабочих станций;
          3. выбора и настройки устанавливаемых компонентов до начала установки антивирусного пакета на клиентские части;
      13. Система должна обладать специальной политикой для мобильных пользователей (ноутбуки), при применении которой, мобильные пользователи должны иметь возможность редактирования настроек антивирусного пакета и обновления через Интернет при отсутствии доступа к антивирусному серверу. Применение политики должно происходить через Web-интерфейс, без необходимости использования файлов конфигурации типа \*.xml.
      14. Система управления должна поддерживать возможность:
          1. создания точки восстановления перед установкой антивирусного пакета на защищаемые рабочие станции и сервера;
          2. восстановления удаленных станций.
      15. Система должна поддерживать множественную возможность установки своих компонентов на защищаемые рабочие станции – в том числе с помощью:
          1. прямого их указания в системе управления в результате сканирования локальной сети, Microsoft Active Directory,
          2. политик Microsoft Active Directory
          3. установки с помощью дистрибутива, содержащего все компоненты защиты
          4. рассылки инсталляционных файлов из системы управления по электронной почте
          5. возможностей службы распределенной файловой системы (DFS).
      16. Система должна поддерживать возможность настройки правил автоматического распределения станций по пользовательским группам, а также возможность изменения первичной группы при автоматическом подтверждении доступа станций к антивирусному серверу
      17. Система управления должна обладать возможностью встроенного автоматического резервного копирования критически важных данных и конфигурации антивирусного сервера по заранее заданному расписанию, а также опцию восстановления сервера из резервной копии без использования файлов конфигурации типа \*.xml.
      18. Система должна иметь возможность минимизации трафика:
          1. за счет применения специальных алгоритмов сжатия;
          2. ограничения трафика по пропускной способности и по времени в определенных IP-подсетях.
      19. Система должна иметь возможность интеграции с платформой Microsoft® Network Access Protection (NAP), обеспечивающей автоматическую систему реагирования на инциденты безопасности.
      20. Система должна иметь возможность выбора уровня подробности протоколирования своих компонентов. cистема управления должна иметь возможность загрузки архивированных файлов журнала работы всех антивирусных серверов иерархической сети
      21. В целях ограничения использования серверного пространства должна иметься возможность ротации файлов журнала антивирусного сервера по времени (час, день, неделя)
      22. Система управления должна обеспечивать защиту от несанкционированного доступа. Авторизация должна обеспечиваться парой логин/пароль.
      23. Администраторы Системы должны иметь возможность авторизации с помощью ActiveDirectory, LDAP, RADIUS, PAM. Система управления должна иметь возможность предварительного тестирования настроек авторизации внешних администраторов Active Directory, LDAP и RADIUS
      24. Система должна иметь журнал аудита действий администраторов Системы, позволяющий просматривать журнал событий и изменений, осуществленных администраторами при помощи системы управления.
      25. Система должна обеспечивать:
          1. возможность экспорта выбранных файлов из карантина рабочей станции и/или файлового сервера на антивирусный сервер для дальнейшего анализа;
          2. возможность задания групповых политик в зависимости от группы IP-адресов.
          3. возможность просмотра новостей безопасности, в том числе информирующих об актуальных угрозах
      26. В случае включения какого-либо компонента Системы в единую систему управления антивирусной защиты локальной сети:
          1. обновления компонента Системы должны происходить через сервер обновления системы управления антивирусной защиты;
          2. статистика работы компонентов Системы должна:
             1. собираться на сервере системы управления антивирусной защиты;
             2. быть доступной с любой операционной системы, поддерживающей браузеры Mozilla Firefox, Internet Explorer, Safari, Opera без ограничений на использование последних версий браузеров и без доустановки какого-либо программного обеспечения за исключением устанавливаемого автоматически с антивирусного сервера модуля, необходимого для отображения статистики.
             3. Иметь возможность экспорта в формат PDF
             4. Иметь возможность отправки по по электронной почте согласно расписанию работы антивирусного сервера
      27. Система должна обеспечивать реализацию следующих функциональных возможностей по обновлению:
          1. получения ежедневных обновлений вирусных баз не менее 10 раз в сутки независимо от того, рабочий, либо выходной день, что должно подтверждаться созданным Системой отчетом (файлом протокола). Система также должна поддерживать возможность получения экстренных обновлений, связанных с выходом новых типов вредоносного ПО, а также возможность мгновенного распространения этих обновлений;
          2. возможность множественности путей обновления, в том числе по каналам связи и на съемных электронных носителях информации;
          3. возможность обновления через прокси-серверы, в том числе прокси-серверы MS ISA/TMG.
          4. проверка целостности и подлинности обновлений средствами электронной цифровой подписи.
          5. обновления компонентов и вирусных баз по защищенному каналу, с использованием протокола HTTPS.
      28. В случае размещения антивирусных серверов во внутренней сети без доступа к сети Интернет получение обновлений должно быть возможно с помощью специальной утилиты автономной загрузки репозитория;
      29. Система должна иметь возможность перезагрузки защищаемой станции через систему управления
      30. Система должна иметь возможность шифрования трафика между серверами и защищаемыми рабочими станциями в целях предотвращения утечки конфиденциальной информации.
   3. **Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows**
      1. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
         1. осуществление антивирусной (включая постоянную защиту от руткит-технологий) и антиспам защиты на рабочих станциях.
      2. Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов:
      3. Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию ПО должна обеспечивать защиту рабочих станций под управлением операционных систем:
         1. Microsoft Windows XP Professional;
         2. Microsoft Windows Vista;
         3. Microsoft Windows 7;
         4. Microsoft Windows 8;
         5. Microsoft Windows 8.1;
         6. Microsoft Windows 10.
      4. Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки. Компоненты системы должны поддерживать механизм динамического выделения оперативной памяти, учитывающий производительность системы, а также потребности в ресурсах задач, выполняемых пользователем и операционной системой во время проверки.
      5. Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства, в том числе за счет возможности отложенной проверки файлов, открываемых «на чтение», а также использования особенностей современных архитектур.
      6. Система должна поставляться в конфигурации, обеспечивающей антивирусную защиту при работе в локальной сети и в Интернет с Web-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции, как от вредоносных программ, так и от спама. Должно обеспечиваться обнаружение и удаление вирусов всех типов, как из тела сообщения, так и, если это возможно, из вложенных файлов.
      7. В случае наличия системы централизованного управления права доступа к настройкам компонентов антивирусного пакета для пользователей должны определяться администратором Системы с возможностью самостоятельной настройки пользователями только в пределах делегированных администратором прав и без применения пароля.
      8. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек пользователями и администраторами Системы в рамках имеющихся у них прав.
      9. В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.
      10. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения с последующим лечением системы.
      11. Дополнительно к вышеперечисленному система должна обеспечивать на рабочих станциях:
          1. поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;
          2. непрерывное фоновое сканирование в целях нейтрализации активных угроз
          3. проверку любых объектов на защищаемых рабочих станциях, в том числе внутри архивов без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора;
          4. проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;
          5. блокировку опасных макросов VBA в реальном времени;
          6. защиту от вредоносных сценариев, загружаемых с Web-страниц;
          7. защиту от проникновения вредоносных программ и использования уязвимостей за счет использования персонального межсетевого экрана;
          8. проверку трафика как до получения его программными клиентами, так и после, с целью исключения использования уязвимостей прикладного ПО;
          9. защиту от намеренных/непреднамеренных действий пользователей посредством блокировки доступа к локальным и сетевым ресурсам. В том числе отдельным типам сменных носителей информации, локальным файлам и каталогам, сайтам в сети Интернет;
          10. ограничения доступа к сети Интернет или к компьютеру в определенный момент времени по расписанию
          11. помещение найденных зараженных файлов в специальное место на жестком диске - «карантин»;
          12. просмотр местоположения станций и серверов на карте, если заданы географические координаты станции
          13. автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
          14. запуск задач по расписанию и/или сразу после загрузки операционной системы;
          15. возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке.
      12. Система защиты рабочих станций должна обеспечивать проверку протоколов:
      13. HTTP;
      14. IMAP, SMTP, POP3 независимо от используемого почтового клиента;
      15. NNTP (только проверка на вирусы), независимо от почтового клиента.
      16. Система должна обеспечивать проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов (компьютерных вирусов, троянских программ, Интернет-червей, макро-вирусов, опасных Java-апплетов, ActiveX и др.) посредством:
      17. антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;
      18. проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.
      19. В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.
      20. Система должна обеспечивать защиту от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе шифровальщиков, а также блокировщиков экрана) с помощью превентивной защиты, отслеживающей попытки внедрения вредоносных файлов
      21. В Системе должна быть реализована защита работы собственных модулей от сбоев и случайного изменения.
   4. **Требования к программным средствам антивирусной защиты рабочих станций и домашних компьютеров под управлением ОС семейства Microsoft Windows, не входящих в систему централизованного управления**
      1. Программные средства системы защиты (далее Системы) должны обеспечивать реализацию следующих функциональных возможностей:
         1. осуществление антивирусной (включая постоянную защиту от руткит-технологий) и антиспам защиты на рабочих станциях;
      2. Система используя актуальную на момент проведения тендера версию ПО должна обеспечивать защиту рабочих станций под управлением операционных систем:
         1. Microsoft Windows XP;
         2. Microsoft Windows Vista;
         3. Microsoft Windows 7;
         4. Microsoft Windows 8.1;
         5. Microsoft Windows 8;
         6. Microsoft Windows 10.
      3. В целях противодействия вредоносным программам, блокирующим запуск известного ПО - для установки системы защиты не должна требоваться установка стороннего инсталлятора - включая Microsoft Windows Installer, либо использование служб, дополнительных к ранее используемым.
      4. В связи с необходимостью автоматизации развертывания системы защиты установка должна быть возможна в том числе в режиме командной строки - указанием необходимых параметров установки. В том числе установки в фоновом режиме, необходимости перезагрузки и состава устанавливаемых компонент;
      5. В связи с возможными ограничениями канала доступа в сеть Интернет установка системы защиты должна быть возможной без доступа в сеть Интернет - дистрибутив должен содержать все компоненты системы защиты, а также базы данных признаков вредоносных программ и вредоносных ресурсов сети Интернет, доступ к которым может регулироваться системой защиты.
      6. Для работы системы защиты не должны использоваться внешние библиотеки, а также среда .Net Framework, целостность которых не находится под контролем системы самозащиты и компрометация которых может привести к ошибкам отображения информации системы защиты или иным проблемам, связанным с интерфейсом системы защиты
      7. С целью противодействия вредоносным программам, запущенным на компьютере, система установки должна быть интегрирована с антируткитом - обнаружение и удаление угроз должно быть доступно во время установки.
      8. Система установки должна поддерживать импорт настроек и содержания карантина, сохраненных после удаления ранее установленного антивируса - в случае наличия совместимости версий.
      9. Дистрибутив, использованный для установки, должен после завершения установки использоваться для автоматического восстановления работы сервисов. В целях поддержания дистрибутива в актуальном состоянии должно быть реализовано инкрементированное обновление установочного пакета. В целях исключения неправомерного доступа к дистрибутиву в целях удаления или изменения доступ должен контролироваться системой самозащиты антивирусной Системы.
      10. Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки. Компоненты системы должны поддерживать механизм динамического выделения оперативной памяти, учитывающий производительность системы, а также потребности в ресурсах задач, выполняемых пользователем и операционной системой во время проверки.
      11. Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства, в том числе за счет возможности отложенной проверки файлов, открываемых «на чтение», а также использования особенностей современных архитектур.
      12. Система должна поставляться в конфигурации, обеспечивающей антивирусную защиту при работе в локальной сети и в Интернет с Web-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции, как от вредоносных программ, так и от спама. Должно обеспечиваться обнаружение и удаление вирусов всех типов, как из тела сообщения, так и, если это возможно, из вложенных файлов.
      13. В случае наличия системы централизованного управления права доступа к настройкам компонентов антивирусного пакета для пользователей должны определяться администратором Системы с возможностью самостоятельной настройки пользователями только в пределах делегированных администратором прав и без применения пароля.
      14. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек пользователями и администраторами Системы в рамках имеющихся у них прав.
      15. Обновление системы защиты должно быть возможно (по выбору администратора системы защиты) с серверов компании поставщика системы защиты, размещенных в сети Интернет, локальной или сетевой папки, компьютеров локальной сети, на которых установлена аналогичная система защиты и создано зеркало обновлений;
      16. В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.
      17. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения с последующим лечением системы.
      18. По умолчанию система защиты должна работать в так называемом пользовательском (ограниченном) режиме. Пользователю системы, не являющемуся администратором защиты, не должны быть доступны настройки компонентов системы защиты, а также возможность отключения системы защиты. При работе в данном режиме в интерфейсе системы защиты не должны показываться пункт меню или иконка, нажатие на которые открывает окно или раздел интерфейса с настройками системы защиты. Администратор должен иметь возможность ограничить доступ к настройкам с помощью пароля;
      19. Дополнительно к вышеперечисленному система должна обеспечивать на рабочих станциях:
          1. поиск и удаление вредоносных программ всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;
          2. обнаружение вредоносных программ, не обнаруживаемых средствами антивирусного ядра, с помощью превентивной защиты, отслеживающей поведение запущенных процессов, а также вредоносных объектов, внедренных в запущенные процессы;
          3. проверки ссылок на видоизменение, скрипты и фреймы;
          4. проверки файлов по ссылкам до скачивания из сети Интернет на локальный компьютер;
          5. проверку любых объектов на защищаемых рабочих станциях, в том числе внутри архивов без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора;
          6. выявления вредоносных объектов в HTML- и PDF-документах;
          7. выявления и анализа «невидимых» IFRAME-элементов на страницах сайтов и HTML-документах;
          8. проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;
          9. блокировку опасных макросов VBA в реальном времени;
          10. блокировку перехода по внешним ссылкам в социальных сетях;
          11. защиту от вредоносных сценариев, загружаемых с Web-страниц;
          12. защиту от проникновения вредоносных программ и использования уязвимостей за счет использования персонального межсетевого экрана;
          13. проверку трафика как до получения его программными клиентами, так и после, с целью исключения использования уязвимостей прикладного ПО;
          14. защиту от намеренных/непреднамеренных действий пользователей посредством блокировки доступа к локальным и сетевым ресурсам. В том числе отдельным типам сменных носителей информации, локальным файлам и каталогам, сайтам в сети Интернет;
          15. помещение найденных зараженных файлов, а также резервных копий объектов, к которым были применены действия, отличные от «Поместить в карантин», в специальное место на жестком диске -«карантин»;
          16. просмотр местоположения станций и серверов на карте, если заданы географические координаты станции;
          17. автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
          18. запуск задач по расписанию и/или сразу после загрузки операционной системы;
          19. возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке
          20. защиту возникновения претензий от правообладателей контента путем использования специальной базы данных признаков ресурсов, доступ к которым ограничен по требованию правообладателей.
      20. Администратор системы должен иметь возможность:
          1. настройки правил защиты от намеренных/непреднамеренных действий посредством блокировки доступа к локальным и сетевым ресурсам (локальным файлам и каталогам, сайтам в сети Интернет) для конкретных пользователей;
          2. копировать настройки между учетными записями пользователей;
          3. запрещать возможность отправки заданий на печать;
          4. запрещать возможность передачи данных по сети;
          5. запрещать возможностьизменения системного времени и часового пояса;
          6. отключать ранее заданные ограничения для конкретной учетной записи;
          7. назначать месторасположения карантина при обнаружении зараженных файлов на съемных носителей;
          8. используя возможности менеджера карантина, осуществлять повторную проверку объектов, помещенных в карантин;
          9. иметь возможность очистки карантина для отдельного диска.
      21. Система защиты рабочих станций должна обеспечивать проверку протоколов:
          1. HTTP независимо от используемого браузера или иного приложения, получающего трафик;
          2. IMAP, SMTP, POP3 независимо от используемого почтового клиента;
          3. NNTP (только проверка на вирусы), независимо от почтового клиента.
      22. Система защиты рабочих станций должна обеспечивать проверку почтовых сообщений, передаваемых по протоколу MAPI для Microsoft Outlook 2000 (Outlook 9)/2002 (Outlook 10 или Outlook XP)/2003 (Outlook 11)/2007/2010/2013.
      23. Система защиты рабочих станций должна автоматически обеспечивать проверку трафика передаваемого по поддерживаемым системой защиты протоколам:
          1. вне зависимости от порта, через который передается трафик - без необходимости указания списка проверяемых портов для конкретных протоколов;
          2. включая проверку трафика, передаваемого по зашифрованному соединению SSL.
      24. Система защиты рабочих станций должна обеспечивать фильтрацию трафика в мгновенных сообщениях Mail.Ru Agent, ICQ, Jabber, QIP, Pidgin и другие, включая антивирусную проверку пересылаемых вложений, а также автоматическое удаление из сообщений ссылок, ведущих на вредоносные и фишинговые сайты.
      25. Система защиты рабочих станций должна обеспечивать фильтрацию выдачи результатов поисковых систем Google, Yandex, Yahoo!, Bing, Rambler с показом только безопасных с точки зрения поисковых систем и системы защиты ресурсов.
      26. Система должна обеспечивать проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов (компьютерных вирусов, троянских программ, Интернет-червей, макро-вирусов, опасных Java-апплетов, ActiveX и др.) посредством:
          1. антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;
          2. проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы;
          3. непрерывного фонового сканирования и нейтрализации активных угроз. В том числе в критических областях Windows, оперативной памяти, запущенных процессах, MBR/VBR дисков, BIOS;
          4. проверки ссылок и файлов с помощью репутационного сервиса облачной защиты - в том числе с помощью базы данных алгоритмов работы вредоносных программ.
      27. В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.
      28. С целью защиты от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе шифровальщиков, а также блокировщиков экрана) Система должна:
          1. обеспечивать защиту критически важных частей системы (в том числе папок и ветвей реестра) от модификаций вредоносными программами, в том числе блокировать попытки:
             1. изменения вредоносными программами загрузочных областей диска;
             2. изменения нежелательным образом пользовательских файлов (в том числе действия троянцев-шифровальщиков) ;
             3. изменения файла HOSTS;
             4. добавления новых задач в логику работы операционной системы;
             5. изменения правил запуска ранее установленных программ;
             6. измения параметров работы системных служб, в том числе процесса создания резервных копий файлов;
             7. загрузки новых или неизвестных драйверов без ведома пользователя, установки новых виртуальных устройств, загрузки в браузер вредоносных плагинов, в том числе блокировщиков браузера;
             8. автозапуска вредоносных программ;
             9. получения низкоуровневого доступа к диску;
             10. регистрации вредоносных программ в реестре для последующего запуска;
             11. отключения безопасного режима Windows путем блокировки изменения реестра;
             12. сокрытия присутствия троянской программы в контролируемой системе в виде руткита.
          2. блокировать попытки установления каналов связи между вредоносным ПО, ранее установленным на компьютер и удаленными серверами злоумышленников;
          3. с помощью превентивной защиты, отслеживающей работу всех процессов системы в поисках действий, характерных для процессов вредоносных программ и не позволяющей вредоносным объектам внедриться в процессы других программ или каким-либо способом разместить вредоносные файлы в защищаемой системе, выявлять и прекращать работу вредоносных, подозрительных или ненадежных сценариев и процессов;
          4. обеспечивать защиту от эксплойтов (программ, эксплуатирующих как уже известные, так и еще неизвестные уязвимости) путем внедрения специального модуля защиты в контролируемые процессы;
          5. ограничивать время работы конкретного сотрудника на защищаемом компьютере - с целью исключения доступа у компьютеру в остальное время неопределенного круга лиц. Система ограничения доступа должна позволять:
             1. задавать время работы на компьютере для выходных и будних дней для каждого сотрудника, а также ограничения по доступу в сеть Интернет;
             2. задавать суммарное время работы на компьютере для конкретного сотрудника;
             3. автоматически блокировать доступ к защищаемому компьютеру в ночное время.
          6. ограничивать доступ к определенным ресурсам сети Интернет - согласно белым и черным спискам ресурсов сети, предопределенным группам ресурсов;
          7. ограничивать доступ к определенным файлам и папкам - с указанием типа доступа объектам (блокировать доступ или разрешать только чтение);
          8. обеспечивать возможность использования на защищаемом компьютере только устройств, входящих список разрешенных. Администратор Системы должен иметь возможность:
             1. контроля доступа к таким типам устройств, как дисковые накопители, приводы DVD/CD-ROM, клавиатуры, компьютерные мыши, сетевые карты, игровые устройства, USB-устройства;
             2. импорта и экспорта правил использования устройств (в том числе с помощью функционала управления удаленными компьютерами антивирусной сети), а также формирования правил блокировки шин и классов устройств, создания списка разрешенных устройств для заблокированных шин и классов устройств;
             3. задать уровень доступа к устройству осуществляется в форме полного запрета доступа всем процессам операционной системы или в форме интерактивного режима, в котором пользователю выводится оповещение о попытке доступа к устройству. Для устройств. с файловой системой администратор Системы должен иметь возможность задать тип доступа - разрешать полный доступ к устройству или доступ только на чтение.
          9. обеспечивать возможность полного запрета использования USB-устройств и CD/DVD-приводов.
      29. модуль превентивной защиты должен:
          1. поддерживать возможность создания профилей - групп настроек, применяемых пользователем или администратором защищаемой системы - как для системы превентивной защиты в целом, так и для конкретных приложений с целью исключения потенциальных конфликтов при их работе.
      30. С целью ускорения проверки Система должна поддерживать возможность исключения из проверки различными компонентами системы защиты:
          1. данных, передаваемых по защищенным протоколам (в том числе HTTPS), а также трафика доверенных приложений (имеющих валидную цифровую подпись) ;
          2. файлов и папок;
          3. ресурсов сети Интернет;
          4. почтовых адресов;
          5. доверенных программ;
      31. С целью ускорения проверки Брандмауэр (файрвол) должен поддерживать **базу** доверенных приложений, а также позволять создавать правила работы для приложений.
      32. В случае отсутствия централизованного управления системой защиты Система защиты рабочей станции должна поддерживать возможность удаленного управления Системами защиты, установленными на компьютерах в пределах одной локальной сети.
      33. Подсистема показа статистики Системы защиты должна:
          1. отображать время возникновения (детектирования) угроз;
          2. списки запрещенных сайтов, доступ к которым был запрошен с защищаемого компьютера.
      34. Подсистема статистики должна иметь возможность отображения только необходимых для анализа сообщений - в том числе создания выборки сообщений отдельных компонентов системы защиты, сообщений с определенными кодами
      35. В Системе должна быть реализована защита работы собственных модулей от сбоев и случайного изменения.
   5. **Требования к программным средствам антивирусной защиты рабочих станций Linux**
      1. Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.
      2. Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов.
      3. Система, используя актуальную на момент проведения тендера версию ПОдолжна обеспечивать защиту ресурсов рабочих станций функционирующих под управлением операционных систем:
         1. Linux, имеющих версию ядра 2.6.37 и новее
      4. Установка модулей Системы в зависимости от типа используемой операционной системы должна происходить с помощью универсального пакета для UNIX систем, независимого от типа и версии используемой операционной системы, репозитория или пакета рассчитанного на работу с используемым в ОС менеджером пакетов
      5. Установка и обновление Системы должны быть возможны как через средства командной строки, так и с помощью графического инсталлятора.
      6. Система установки должна включать возможность автоматической установки модулей, необходимых для компонентов Системы.
      7. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности работы. При этом, в случае необходимости внесения изменений, Система должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователями в рамках имеющихся у них прав.
      8. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением заданных файловых областей.
      9. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
         1. поиск и удаление вирусов всех известных типов в файлах;
         2. антивирусного сканирования ресурсов сервера как по команде администратора, так и по расписанию, заключающегося в однократной полной или выборочной проверке на наличие угроз объектов;
         3. помещения найденных зараженных и подозрительных файлов в карантин для дальнейшего анализа;
         4. автоматического запуска антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
         5. запуска задач по расписанию и/или сразу после загрузки операционной системы;
         6. настройки расписания сканирования с указанием параметров запуска.
      10. Управление программой должно осуществляться как непосредственно через конфигурационные файлы, так и через графический интерфейс, реализованный для операционных систем типа Linux. Система управления должна поддерживать возможность настройки параметров антивирусного сканирования с указанием файлов и каталогов, подлежащих антивирусной проверке, действий по отношению к вредоносным объектам различных типов.
      11. Администратор системы должен иметь возможность:
          1. Определять необходимый уровень анализа, в том числе путем отключения эвристического анализа, ограничения размера файла и глубины проверки;
          2. определять типы проверяемых файлов, в том числе с использованием масок;
          3. задавать различные действия по отношению к различным типам вредоносных объектов в случае их обнаружения;
          4. управлять детализацией протоколов антивирусной проверки;
          5. просматривать информацию об используемом ключевом файле и его владельце;
          6. запускать периодическую проверку в приоритетном или в фоновом режиме;
   6. **Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Microsoft Windows**
      1. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
         1. Осуществление антивирусной защиты на серверах, включая защиту от руткит-технологий.
      2. Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов.
      3. Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию ПО должна обеспечивать защиту серверов под управлением операционных систем:
         1. Microsoft Windows Server 2003;
         2. Microsoft Windows Server 2008;
         3. Microsoft Windows Server 2012;
         4. Microsoft Windows Server 2016;
         5. Microsoft Windows Server 2019.
      4. Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.
      5. Антивирусное программное обеспечение должно по умолчанию иметь оптимальные настройки с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователями в рамках имеющихся у них прав.
      6. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением системы.
      7. В Системе должна быть реализована возможность выбора приоритета сканирования, а также остановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.
      8. Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.
      9. Система должна обеспечивать:
         1. поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;
         2. проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;
         3. блокировку опасных макросов VBA в реальном времени;
         4. защиту от вредоносных сценариев, загружаемых с веб-страниц;
         5. помещение найденных зараженных файлов в специальное место на жестком диске —«карантин»;
         6. автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
         7. запуск задач по расписанию и/или сразу после загрузки операционной системы.
      10. Система защиты серверов под управлением семейства ОС Microsoft Windows должна обеспечивать реализацию следующих функциональных возможностей:
          1. проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов посредством:
             1. антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;
             2. проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.
      11. В Системе должна быть реализована самозащита для всех ее объектов, в том числе критических файлов, процессов, окон, ключей и прочего, от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.
   7. **Требования к программным средствам антивирусной защиты файловых серверов UNIX**
      1. Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.
      2. Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных файлов всех типов.
      3. Система, используя актуальную на момент проведения тендера версию ПО должна обеспечивать защиту ресурсов серверов, использующих Samba версий 3.0.x - 4.3.x, и функционирующих под управлением операционных систем:
         1. Linux, имеющих версию ядра 2.6.37 или новее, использующих библиотеку glibc 2.13 или новее;
         2. FreeBSD версии 10.3 или новее для платформы Intel x86 и amd64;
      4. Интеграция Системы с Samba должна осуществляться с помощью модуля VFS (Virtual File System).
      5. В случае использования версий Samba, отличных от вышеперечисленных, либо Samba для 64-битных платформ семейства Linux должна существовать возможность компиляции модулей интеграции из исходных кодов.
      6. Установка модулей Системы в зависимости от типа используемой операционной системы должна происходить с помощью универсального пакета для UNIX систем, независимого от типа и версии используемой операционной системы, репозитория или пакета рассчитанного на работу с используемым в ОС менеджером пакетов
      7. Установка и обновление Системы должны быть возможны как через средства командной строки, так и с помощью графического инсталлятора.
      8. Система установки системы должна включать возможность автоматической установки модулей, необходимых для установки необходимых компонентов.
      9. Компоненты системы должны иметь возможность управления использованием серверных ресурсов при выполнении сканирования файлового пространства.
      10. В Системе должна быть реализована возможность задания приоритета антивирусного сканирования.
      11. Система должна поддерживать возможность порождения нескольких одновременно действующих процессов проверки.
      12. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы настройки. При этом, в случае необходимости внесения изменений, Система должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователем в рамках имеющихся у них прав.
      13. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением заданных файловых областей.
      14. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
          1. поиск и удаление вирусов всех известных типов в файлах;
          2. антивирусного сканирования ресурсов сервера, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде администратора, так и по расписанию;
          3. антивирусной проверке «на лету» файлов, загружаемых как на сервер, так и с него;
          4. помещения найденных зараженных и подозрительных файлов в карантин для дальнейшего анализа;
          5. автоматического запуска антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
          6. запуска задач по расписанию и/или сразу после загрузки операционной системы;
          7. настройки расписания сканирования с указанием параметров запуска.
      15. Управление программой должно осуществляться как с помощью веб-интерфейса, так и непосредственно через конфигурационные файлы. Система управления должна поддерживать возможность настройки параметров антивирусного сканирования с указанием файлов и каталогов, подлежащих антивирусной проверке, и действий по отношению к вредоносным объектам различных типов.
      16. Администратор системы должен иметь возможность:
          1. определять необходимый уровень анализа, в том числе путем отключения эвристического анализа, ограничения размера файла и глубины проверки;
          2. определять типы проверяемых файлов, в том числе с использованием масок;
          3. задавать различные действия по отношению к различным типам вредоносных объектов в случае их обнаружения.
          4. управлять детализацией протоколов антивирусной проверки;
          5. просматривать результаты антивирусной проверки;
          6. просматривать информацию об используемом ключевом файле и его владельце;
          7. запускать периодическую проверку в приоритетном или в фоновом режиме;
          8. использовать альтернативные языковые файлы**.**
   8. **Требования к программным средствам антивирусной защиты почтовых систем на платформе Microsoft Exchange** 
      1. Программные средства Системы должны обеспечивать защиту всей входящей и исходящей электронной корреспонденции, поступающей для обработки на почтовый сервер, как от вредоносных программ, так и от спама. Должно обеспечиваться обнаружение и удаление вирусов всех типов из следующих элементов электронных писем:
         1. тело письма;
         2. прикрепленные файлы (включая архивированные и упакованные);
         3. вложенные OLE-объекты.
      2. В случае интеграции с почтовым сервером Microsoft Exchange с помощью интерфейса Microsoft Virus Scanning Application Interface (VSAPI) программные средства Системы должны обеспечивать возможность проверки документов, хранящихся в базе данных, а также проверки при доступе к письму.
      3. Система должна обеспечивать:
         1. проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе из сети Интернет;
      4. Система должна обеспечивать исключение из проверки отдельных типов объектов, в том числе потенциально опасных.
      5. Система должна обеспечивать возможность выбора желаемых действия для неизлечимых и подозрительных объектов. В качестве таких действий должны быть доступны удаление объекта или перемещение прикрепленных файлов в карантин. Для подозрительных объектов также должна быть доступна возможность пропуска.
      6. Система должна иметь возможность добавления к зараженному или отфильтрованному письму файла до того, как программа совершит над ним выбранное действие. Администратор системы должен иметь возможность редактирования содержания этого файла и использования в нем предопределенных макросов.
      7. Система должна обеспечивать возможность выбора желаемых действий для отфильтрованных спам-сообщений. В качестве таких действий должны быть доступны блокировка, пропуск или перемещение в специальную папку. Система должна иметь возможность модификации заголовка проверенных сообщений и добавления префикса к теме спам-сообщения.
      8. Система, используя актуальную на момент проведения тендера версию ПО должна функционировать на почтовых серверах:
         1. Microsoft Exchange Server 2007 x64 SP1
         2. Microsoft Exchange Server 2010 x64
         3. Microsoft Exchange Server 2013 SP1 CU5
         4. Microsoft Exchange Server 2016 CU3
         5. Microsoft Exchange Server 2019.
      9. Система должна поддерживать возможность ускорения процесса сканирования почтовых сообщений за счет пропуска объектов, проверенных ранее в транспортной системе организации через другие почтовые серверы MS Exchange.
      10. Система должна иметь возможность администрирования с помощью консоли управления.
      11. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. Система должна обеспечивать возможность автоматического определения параметров производительности – без необходимости тонкой настройки их администраторами Системы через интерфейс управления.
      12. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
          1. В случае интеграции с почтовым сервером Microsoft Exchange с помощью интерфейса Microsoft Virus Scanning Application Interface (VSAPI) - проверку всех почтовых ящиков, включая служебные почтовые ящики SystemMailbox, System Attendant;
          2. фильтрацию и блокировку сообщений в зависимости от вероятности принадлежности их к спаму – по категориям *спам,* *вероятно, спам и маловероятно спам*;
          3. обеспечение фильтрации почтового трафика на спам исключительно с использованием системы анализа на основе правил, не требующей постоянного обучения системы антиспама;
          4. фильтрацию по определенным типам сообщений и предотвращение массовых рассылок. Система должна поддерживать возможность создания правил фильтрации, в том числе фильтрацию по расширению, маске, размеру файла, максимальному количеству получателей писем.
          5. создание белых и черных списков адресов;
          6. исключения сообщений от доверенных отправителей из проверки на спам и вирусы
          7. запуск задания на фоновую проверку в целях обнаружения ранее неизвестных вредоносных программ;
          8. изоляцию инфицированных и подозрительных объектов в специальное место на жестком диске - «карантин»;
          9. разбиение клиентов на группы для упрощения администрирования и задание с помощью профилей защиты, реализующих применение различных правил для групп, включая приоритет обработки;
          10. обеспечение возможности управления работой Системы с разными уровнями доступа;
          11. уведомление о вирусных событиях;
          12. регистрацию ошибок и происходящих событий как в журнале регистрации событий операционной системы (Event Log), так и в текстовом журнале регистрации событий программы установки;
          13. ведение журнала событий, в том числе с указанием необходимой степени детализации для определенного типа событий;
          14. сбор статистики;
          15. автоматическое обновление вирусных баз.
      13. Система должна иметь возможность управления карантином, в том числе восстановления сохраненных объектов.
   9. **Требования к программным средствам антивирусной защиты почтовых систем на платформе UNIX**
      1. Программные средства Системы должны обеспечивать защиту всей входящей и исходящей электронной корреспонденции, поступающей для обработки на почтовый сервер. Должна обеспечиваться защита как от вредоносных программ, так и от спама. Все исходящие сообщения должны проверяться до того, как они передаются на удаленный сервер.
      2. Должна обеспечиваться проверка почтовых протоколов SMTP/LMTP/POP3/IMAP4.
      3. Должна обеспечиваться проверка защищенных версий протоколов POP3/IMAP4.
      4. Должно обеспечиваться обнаружение и удаление вирусов всех типов как из самого письма, так и из всех его компонентов, вне зависимости от их типа и уровня вложенности.
      5. Установка модулей Системы в зависимости от типа используемой операционной системы должна происходить с помощью универсального пакета для UNIX систем, независимого от типа и версии используемой операционной системы, репозитория или пакета рассчитанного на работу с используемым в ОС менеджером пакетов
      6. Система должна иметь возможность установки как в качестве дополнительного модуля фильтрации для используемого почтового сервера на платформе типа UNIX, так и самостоятельно — в качестве почтового шлюза, предназначенного для проверки входящего и исходящего почтового трафика.
      7. Система должна включать средства контроля работы собственных модулей, включая средства автоматического перезапуска модулей в случае возникновения проблем в их работе.
      8. Система должна поддерживать средства оптимизации загрузки почтового сервера, в том числе путем управления количеством одновременно проверяемых сообщений.
      9. Система должна поддерживать средства управления рабочей очередью приложения.
      10. Система должна иметь возможность работы с несколькими почтовыми системами с различными настройками.
      11. Система должна поддерживать средства контроля правильности настроек.
      12. Система должна иметь возможность расширения функционала, в том числе путем добавления новых модулей в соответствии с имеющимся программным интерфейсом.
      13. Система должна обеспечивать:
          1. поиск и удаление вирусов всех известных типов;
          2. помещение найденных зараженных файлов в специальное место на жестком диске — «карантин»;
          3. возможность управления карантином, в том числе восстановления сохраненных объектов.
      14. Система должна обеспечивать возможность выбора желаемых действия для различных типов вредоносных объектов, в том числе неизлечимых и подозрительных. В качестве таких действий должны быть доступны удаление сообщения и/или перемещение в карантин. Для подозрительных объектов также должна быть доступна возможность пропуска и доставка без изменения. Должна иметься возможность реализации нескольких действий.
      15. Система должна иметь возможность модификации проверенных (в том числе зараженных и отфильтрованных) писем — в числе прочих: путем модификации заголовка или добавления подписи.
      16. Система, используя актуальную на момент проведения тендера версию ПО должна функционировать:
          1. на операционных системах Linux, имеющих версию ядра 2.6.37 или новее, а также библиотеку glibc версии 2.13 или новее;
          2. FreeBSD версии 10.3 или новее для платформы Intel x86 и amd64
      17. Система, используя актуальную на момент проведения тендера версию, должна функционировать в локальных сетях с поддержкой протоколов IPv4/IPv6.
      18. Система, используя актуальную на момент проведения тендера версию, должна функционировать на почтовых серверах Sendmail, Postfix, Courier, QMail, CommuniGate Pro, ZMailer, Exim.
          1. В состав поставки системы должен входить антивирусный сканер для периодической проверки системы.
          2. Компоненты Системы должны устойчиво функционировать на компьютерах с 32-битной и 64-битной архитектурой в условиях их минимальной и максимальной загрузки без существенного снижения производительности серверов, в том числе за счет управления приоритетами обработки сообщений.
      19. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы.
      20. Система должна иметь возможность сохранения отредактированных настроек в текстовый файл и использования их на этом же или другом компьютере.
      21. Система должна иметь возможность администрирования с помощью веб-консоли управления.
      22. Консоль управления Системой должна быть доступной из единой системы управления антивирусной защиты локальной сети.
      23. Система сбора статистики должна иметь возможность настройки уровня ее детализации, в том числе на уровне отдельных пользователей и групп;
      24. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
          1. настройка параметров сканирования для каждого почтового ящика;
          2. фильтрация по определенным типам сообщений и предотвращение массовых рассылок;
          3. фильтрация почтовых сообщений с помощью технологий репутационного анализа;
          4. анализ заголовков и тела по формальным признакам, в том числе на соответствие спецификации RFC-822;
          5. маршрутизация сообщений;
          6. балансировка нагрузки между несколькими узлами антивирусного анализа, в том числе удаленными;
          7. фильтрация и блокировка сообщений в зависимости от вероятности их принадлежности к спаму — по категориям спам и вероятно, спам;
          8. использование интеллектуальной системы анализа почтового трафика без необходимости постоянного обучения системы антиспама системным администратором;
          9. гарантированная доставка всех почтовых сообщений, в том числе в случае временной недоступности получателя;
          10. архивирование и регистрация сообщений;
          11. Использование различных типов баз данных;
          12. отправка уведомлений администратору;
          13. ведение журнала событий, в том числе для определенного типа объектов;
          14. автоматическое обновление вирусных баз и настройка расписания обновлений;
          15. откат обновлений;
          16. проверка адреса по черным спискам RBL/DNSBL.
      25. Система должна обеспечивать возможность выбора желаемых действия для отфильтрованных спам-сообщений. В качестве таких действий должны быть доступны удаление, пропуск или отказ от приема.
      26. Система должна поддерживать возможность создания правил фильтрации.
      27. Система должна обеспечивать регулировку распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач.
      28. Система должна позволять организовывать кластерное решение для распределения нагрузки по обработке почтовых сообщений на несколько серверов
   10. **Требования к программным средствам антивирусной защиты шлюзов сети Интернет, построенных на базе ОС UNIX**
       1. Программные средства Системы должны обеспечивать защиту интернет-трафика, поступающего по протоколам HTTP/FTP
       2. Все передаваемые по защищаемым протоколам объекты должны проверяться до момента передачи пользователям.
       3. Система должна обеспечивать возможность интеграции с прокси-серверами по протоколу ICAP
       4. Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.
       5. Программные средства Системы должны обеспечивать определение в проверяемых объектах вредоносных программ всех типов.
       6. Система, используя актуальную на момент проведения тендера версию ПО должна функционировать на:
          1. под управлением операционных систем Linux, имеющих версию ядра 2.6.37 или новее, а также библиотеку glibc версии 2.13 или новее,
          2. FreeBSD версии 10.3 или новее для платформы Intel x86 и amd64
          3. Установка и работа Системы должна быть возможна в операционных системах, использующих доверенную загрузку, реализуемую на основе анализа подписи файлов Системы, либо политики безопасности SELinux
       7. Установка модулей Системы в зависимости от типа используемой операционной системы должна происходить с помощью универсального пакета для UNIX систем, независимого от типа и версии используемой операционной системы, репозитория или пакета рассчитанного на работу с используемым в ОС менеджером пакетов
       8. Установка и обновление Системы должны быть возможны как через средства командной строки, так и с помощью графического инсталлятора.
       9. Система установки должна включать возможность автоматической установки модулей, необходимых для компонентов Системы.
       10. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователями в рамках имеющихся у них прав.
       11. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением заданных файловых областей.
       12. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
           1. выбора типа проверки (проверять все файлы, файлы по заданному списку масок);
           2. назначения различных действий для вредоносных объектов разного типа;
       13. фильтрации проверяемого трафика по ip-адресам или именам ресурсов, в том числе с помощью масок и регулярных выражений имен ресурсов;
       14. фильтрации проверяемого трафика по Mime-типам;
       15. фильтрации проверяемого трафика по размеру файлов;
       16. ограничения доступа к интернет-ресурсам благодаря использованию автоматически обновляемых тематических черных списков, а также формируемых вручную или с помощью веб-интерфейса черных и белых списков адресов;
       17. помещения найденных зараженных и подозрительных файлов в карантин для дальнейшего анализа;
           1. автоматического запуска антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
           2. запуска задач по расписанию и/или сразу после загрузки операционной системы;
       18. автоматической оптимизации количества проверяющих процессов и выбора приоритета сканирования;
       19. использование режима preview для ускорения проверки;
       20. ограничения времени проверки, включая время проверки отдельного файла;
       21. уведомления администратора о попытке открытия запрещенной страницы;
       22. регистрации времени события, объекта проверки и типа воздействия для реализации возможности проведения внутренних расследований;
       23. размещения статистической информации как публичном сервере статистики производителя Системы, так и на сервере централизованной защиты локальной сети
       24. получения статистической информации в форматах HTML и XML
       25. получения статистической информации как по одному серверу Системы, так и суммарно по всем серверам
       26. в случае использования ценрализованного управления:
       27. шифрования и/или сжатия трафика между сервером антивирусной защиты и Системой
       28. экспорта ранее сделанных настроек Системы на сервер антивирусной защиты в ходе первого подключения к серверу
       29. Управление программой должно осуществляться как непосредственно через конфигурационные файлы, так и через веб-интерфейс. Система управления должна поддерживать возможность настройки всех параметров антивирусной проверки трафика.
       30. Администратор системы должен иметь возможность:
       31. проверки корректности сделанных настроек средствами Системы до их применения;
       32. использования нескольких конфигурационных файлов Системы в зависимости от выполняемых задач;
       33. задавать индивидуальные настройки правил фильтрации с помощью логических выражений для групп пользователей, в том числе:
       34. правила работы с несколькими сканирующими сервисами, включая возможность и автоматического переключения между ними при необходимости - в целях повышения отказоустойчивости
       35. ограничения доступа к ресурсам по требованию, включая ограничения ip-адресам, сетям(подсетям), пользователям и группам
       36. ограничения доступа к определенным ресурсам в рабочее время либо в указанный промежуток времени
       37. ограничения доступа к определенным ресурсам для пользователей с определенным IP-адресом или пользователей локальной сети
       38. определять необходимый уровень анализа, в том числе путем отключения эвристического анализа, ограничения размера файла и глубины проверки;
           1. задавать место размещения отчетов - в текстовом файле или системном журнале, а также указывать степень подробности отчетов;
       39. задавать различные действия по отношению к различным типам вредоносных объектов в случае их обнаружения - в том числе возможности обрезать файл до нулевой длины перед передачей его пользователю;
       40. блокировать обновления для определенных компонентов Системы;
       41. восстанавливать компоненты к сохраненному состоянию, в том числе откатывать антивирусные базы
       42. управлять детализацией антивирусной проверки протоколов;
       43. запускать периодическую проверку файловой системы сервера
       44. получать уведомления о сроке действия лицензии и необходимости ее замены
       45. задавать уровни приоритета процессов Системы
       46. Защита работы Системы от сбоев должна обеспечиваться специально разработанным модулем
   11. **Требования по комплектности поставки**
       1. В состав Системы должны входить:
          1. программные средства антивирусной защиты, необходимые для выполнения требований данного технического задания;
          2. программные средства защиты пользователей от нежелательных массовых почтовых рассылок – спама;
          3. программные средства централизованного управления, мониторинга и обновления;
          4. обновляемые базы данных сигнатур всевозможных вредоносных программ.
       2. Комплект поставки должен содержать:
          1. необходимый набор серийных номеров либо ключевых файлов;
          2. дистрибутив Системы;
          3. файлы эксплуатационной документации в формате pdf (Adobe Acrobat Reader), в том числе руководство пользователя (администратора). Поставляемая документация должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.
   12. **Требования по технической поддержке Системы** 
       1. Техническая поддержка должна предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты на всей территории Российской Федерации круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет.
       2. Техническая поддержка должна включать возможность предоставления выделенного специалиста, доступного в режиме 5/8
       3. Техническая поддержка должна включать возможность проведения расследования компьютерных инцидентов
       4. Техническая поддержка должна включать возможность написания специального ПО, предназначенного для устранения последствий воздействия вредоносного ПО на зараженную систему. В том числе утилит расшифровки файлов, если данная операция является возможной
       5. Техническая поддержка должна обеспечивать возможность получения специалистами и пользователями Заказчика информационной помощи по установке Системы и ее компонентов, в том числе:
          1. ответов на вопросы, а также получение инструкций относительно процесса установки и применения программного обеспечения;
          2. ответов на вопросы о наличии проблем в работе программного обеспечения, а также помощи в определение того, является ли данная проблема результатом сбоя программного обеспечения, ошибок настройки или же она вызвана проблемами, связанными с внешними условиями существования или установкой программного обеспечения.
       6. Web-сайт производителя Системы должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов производителя.

Начальник ОИТ Тлеуов И.К.

**Приложение №5**

**СОГЛАСИЕ**

**на обработку персональных данных**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(фамилия, имя, отчество полностью)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(основной документ, удостоверяющий личность, номер основного документа, удостоверяющего его личность) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(сведения о дате выдачи, сведения о выдавшем указанный документ органе)

Зарегистрированный (ая) по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(адрес регистрации по месту жительства)

своей волей и в своем интересе выражаю согласие на обработку моих персональных данных Оператором - ООО «СЕВАСТОПОЛЬЭНЕРГО» (адрес – 299040, г. Севастополь, ул. Хрусталева, 44) для размещения в общедоступных источниках в информационно-телекоммуникационной сети "Интернет":

- в единой информационной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд;

- в единой информационной системе реестра договоров, заключенных заказчиками по результатам закупки;

- в реестре недобросовестных поставщиков;

- на сайте ООО «СЕВАСТОПОЛЬЭНЕРГО»;

включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), распространение (в том числе передачу) и уничтожение моих персональных данных, в следующем составе:

- фамилия, имя, отчество, номер основного документа, удостоверяющего мою личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- место жительства месте (страна, почтовый индекс, наименования единицы административно-территориального деления страны, муниципального образования, населенного пункта и улицы, номер дома (владения), корпуса (строения) и квартиры);

- идентификационный номер налогоплательщика, присваиваемый налоговым органом Российской Федерации, или в соответствии с законодательством соответствующего иностранного государства аналог идентификационного номера налогоплательщика;

Также выражаю согласие на получение и передачу моих персональных данных органам местного самоуправления, государственным органам и организациям для целей обеспечения соблюдения законов и иных нормативных правовых актов, контроля количества и качества выполняемой Услуги, прохождения отбора при проведении процедур закупок, в том числе проверки соответствия требованиям предъявляемых Оператором при проведении закупок.

Вышеприведенное согласие на обработку моих персональных данных представлено с учетом [п. 2 ст. 6](consultantplus://offline/ref=7AA42224394F273FB6C3D6FD89C033BAD66D0358F68E82E66EC65975D1E54120AC5BFB2E94F7C65En3x3I) и [п. 2 ст. 9](consultantplus://offline/ref=7AA42224394F273FB6C3D6FD89C033BAD66D0358F68E82E66EC65975D1E54120AC5BFB2E94F7C65Cn3x3I) Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в соответствии с которыми обработка персональных данных, осуществляемая на основе федерального закона либо для исполнения договора, стороной в котором я являюсь, может осуществляться Оператором без моего дополнительного согласия.

Настоящее согласие действует со дня его подписания до дня его отзыва мною путем подачи Оператору письменного заявления.

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись и фамилия, имя, отчество прописью полностью)

**Приложение №6**

**ПРОЕКТ**

**Сублицензионный договор**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,** именуемое в дальнейшем **Лицензиат**, в лице\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с одной стороны, и **ООО «Севастопольэнерго»,** именуемое в дальнейшем **Сублицензиат**, в лице\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, вместе именуемые — Стороны, а каждое по отдельности — Сторона, заключили настоящий Договор о нижеследующем.

**Термины и определения**

*Право использования* – разрешение на использование программ для ЭВМ, перечисленных в пункте 1 Приложения № 1 к настоящему Договору (далее именуется – «Спецификация»), способами, предусмотренными Договором, а также Типовым соглашением правообладателя с конечным пользователем, получаемое Сублицензиатом на условиях простой (неисключительной) лицензии.

*Типовое соглашение правообладателя с конечным пользователем* – декларируемые правообладателем программ для ЭВМ общие правила использования программ для ЭВМ, обязательные для исполнения Сублицензиатом. Типовое соглашение может быть размещено в инсталляционном файле программы для ЭВМ, отображаемом на экране монитора при установке программы, и/или размещено на официальном Интернет-сайте правообладателя программы для ЭВМ.

*Предоставление права использования программ для ЭВМ* – наступление установленного Сторонами в пункте 2.3. настоящего Договора срока, позволяющее Сублицензиату начать правомерное использование программ для ЭВМ способами, предусмотренными Договором, а также типовым соглашением правообладателя с конечным пользователем.

1. **Предмет Договора**
   1. Лицензиат в соответствии с условиями настоящего Договора обязуется предоставить Сублицензиату Право использования программ для ЭВМ, предусмотренных Спецификацией, а Сублицензиат обязуется принять и оплатить право использования программ для ЭВМ на условиях настоящего Договора.
2. **Порядок предоставления права использования программ для ЭВМ**
   1. Право использования программ для ЭВМ включает в себя право на воспроизведение соответствующих программ для ЭВМ на территории Российской Федерации, ограниченное инсталляцией, копированием и запуском. Право использования предоставляется на срок, предусмотренный типовым соглашением правообладателя с конечным пользователем, и с ограничениями, включая способы использования программ для ЭВМ, установленными указанным соглашением.
   2. Размер лицензионного вознаграждения Лицензиата за предоставление Сублицензиату права использования программ для ЭВМ и дистрибутива Медиа-комплект указывается в пункте 3.1. настоящего Договора и в Спецификации. Выплата лицензионного вознаграждения осуществляется Сублицензиатом в соответствии с разделом 3 настоящего Договора.
   3. Право использования программ для ЭВМ считается предоставленным Сублицензиату, и Сублицензиат вправе начать использование программ для ЭВМ по истечении 10 (десять) рабочих дней с даты подписания Сторонами настоящего Договора (далее – «дата предоставления права использования программ для ЭВМ»).
   4. Не позднее 5 (пяти) рабочих дней с даты предоставления права использования программ для ЭВМ и дистрибутива Медиа-комплект по настоящему Договору Лицензиат направляет Сублицензиату Акт предоставления права и УПД. Сублицензиат в течение 5 (пяти) рабочих дней с момента получения Акта предоставления права и УПД подписывает и направляет Лицензиату один экземпляр Акта и УПД или направляет мотивированный отказ от его подписания. В случае если в установленный настоящим пунктом срок Сублицензиат не направит Лицензиату подписанный Акт предоставления права и УПД или мотивированный отказ от его подписания, Акт и УПД считается подписанным Сублицензиатом без замечаний в последний день срока, установленного для его подписания. Стороны соглашаются с тем, что Акт предоставления прав не является подтверждением факта передачи права использования соответствующих программ для ЭВМ и не подписание Акта не является признаком непредоставления права использования Лицензиатом.
   5. В случае использования правообладателем программ для ЭВМ технических средств защиты использования программ для ЭВМ, Лицензиат обязуется не позднее 1 (одного) дня с даты предоставления права использования программ для ЭВМ обеспечить Сублицензиату возможность использования соответствующих программ для ЭВМ, в том числе путём сообщения ему необходимых ключей доступа и паролей.
   6. Лицензиат гарантирует, что он обладает всеми законными основаниями для предоставления Сублицензиату права использования программ для ЭВМ по настоящему Договору.
   7. Сублицензиату известны важнейшие функциональные свойства программ для ЭВМ, предусмотренных настоящим Договором, Сублицензиат несет риск соответствия указанных программ для ЭВМ своим пожеланиям и потребностям. Лицензиат не несет ответственности за какие-либо убытки, возникшие вследствие ненадлежащего использования или невозможности использования программы для ЭВМ, возникших по вине Сублицензиата.
3. **Порядок расчётов**
   1. Общая цена настоящего Договора, подлежащая уплате Сублицензиатом, составляет \_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_) рублей 00копеек, в том числе:  
        вознаграждение Лицензиата за предоставление права использования программ для ЭВМ составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_  (\_\_\_\_\_\_\_\_\_\_\_\_) рублей 00 копеек, НДС не облагается;  
        вознаграждение Лицензиата за предоставление дистрибутива Медиа-комплект составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_  (\_\_\_\_\_\_\_\_\_\_\_\_) рублей 00 копеек, НДС \_\_\_ % .
   2. Оплата Сублицензиатом цены настоящего Договора производится в течение 7 (семи) рабочих дней с даты начала действия настоящего Договора - в полном размере. При несоблюдении предусмотренных настоящим Договором сроков оплаты Сублицензиат уплачивает Лицензиату пеню в размере 0,1 % (ноль целых одна десятая процента) от неоплаченной в срок суммы за каждый день просрочки.
   3. Все платежи по настоящему Договору осуществляются в безналичной форме в рублях Российской Федерации путём перечисления денежных средств на расчётный счёт Лицензиата.
   4. Датой оплаты признаётся дата списания денежных средств с корреспондентского счёта банка, обслуживающего расчётный счёт Сублицензиата, в адрес расчётного счёта и иных реквизитов Лицензиата. По требованию Лицензиата Сублицензиат предоставляет ему копию платёжного поручения с отметкой банка о принятии к исполнению.
4. **Ответственность Сторон**
   1. При несоблюдении Лицензиатом предусмотренных настоящим Договором сроков исполнения обязательств Сублицензиат вправе потребовать уплаты Лицензиатом неустойки в размере 0,1 % (ноль целых одна десятая процента) от стоимости неисполненных обязательств за каждый день просрочки, но не более 10 % (десяти процентов) от суммы неисполненных обязательств в совокупности.
   2. В случае неисполнения и/или ненадлежащего исполнения обязательств по настоящему Договору одной из Сторон, другая Сторона вправе потребовать возмещения убытков исключительно в размере реального ущерба.
   3. Все штрафные санкции, предусмотренные настоящим Договором, начисляются за весь период просрочки. Право на получение штрафных санкций за нарушение обязательств возникает у стороны договора после признания должником выставленной ему претензии и счета на уплату неустойки, либо после вступления в силу решения суда о присуждении неустойки или иных штрафных санкций.
   4. Штрафные санкции не подлежат взысканию, если неисполнение Стороной своих обязательств по настоящему Договору вызвано нарушением обязательств другой Стороной.
   5. Лицензиат не несёт ответственности за неисполнение или либо ненадлежащее исполнение своих обязательств по настоящему Договору, допущенное ввиду приостановления, ограничения или прекращения распространения программ для ЭВМ, связанного, в том числе, с решением правообладателя о снятии программ для ЭВМ с производства (распространения) их модификацией или модернизацией, либо с установлением экспортных запретов и ограничений законодательством какой-либо юрисдикции, применимой к программам для ЭВМ, подтверждённое официальным письмом вышеуказанного правообладателя. В таком случае Лицензиат, по согласованию с Сублицензиатом, имеет право в части исполнить настоящий Договор в отношении аналогичных программ для ЭВМ либо не исполнять в соответствующей части Договор и осуществить возврат соответствующей суммы денежных средств Сублицензиату.
   6. В случае если настоящий Договор или соответствующая Спецификация к нему предусматривает оплату цены настоящего Договора (Спецификации) на условиях полной или частичной предварительной оплаты, то при нарушении Сублицензиатом сроков внесения такой предоплаты, Лицензиат вправе в одностороннем порядке отказаться от исполнения настоящего Договора или соответствующей Спецификации к нему в срок не позднее 10 (десяти) рабочих дней с даты фактического поступления денежных средств на расчётный счёт Лицензиата. В случае принятия Лицензиатом решения об одностороннем отказе от исполнения настоящего Договора Лицензиат уведомляет Сублицензиата в письменной форме и осуществляет возврат фактически поступивших от Сублицензиата денежных средств (если применимо) в срок не позднее 5 (пяти) рабочих дней с даты отправки Сублицензиату вышеуказанного уведомления.
5. **Техническая поддержка**
   1. Базовая техническая поддержка в отношении использования программ для ЭВМ, предусмотренных настоящим Договором, осуществляется Лицензиатом в течение 3 (трех) месяцев, с момента предоставления права использования. Под базовой технической поддержкой понимается предоставляемая по выделенной линии службы приема и разрешения технических запросов (телефон, e-mail, HelpDesk) специалистами Лицензиата консультационная помощь, включающая в себя: предоставление информации о новых версиях и исправлениях программ для ЭВМ, а также о базовых функциях программ для ЭВМ. Время предоставления поддержки и приема заявок осуществляется с понедельника по пятницу с 9:00 до 18:00 по Московскому времени. По запросу Сублицензиата Лицензиат обязуется предоставить адреса центров технической поддержки Правообладателей.
   2. Расширенная техническая поддержка и иные сопутствующие услуги могут быть оказаны на основании дополнительный Приложений к настоящему Договору или отдельно заключаемых с Сублицензиатом соглашений.
6. **Обстоятельства непреодолимой силы**
   1. Стороны по настоящему Договору освобождаются от ответственности за полное или частичное неисполнение либо ненадлежащее исполнение своих обязательств в случае, если такое неисполнение явилось следствием обстоятельств непреодолимой силы, то есть событий, которые нельзя было предвидеть или предотвратить. К таким событиям относятся: стихийные бедствия, военные действия, принятие государственными органами или органами местного самоуправления нормативных или правоприменительных актов и иные действия, находящиеся вне разумного предвидения и контроля Сторон.
   2. При наступлении обстоятельств непреодолимой силы каждая Сторона должна не позднее 5 (пяти) рабочих дней с момента наступления таких обстоятельств известить о них в письменном виде другую Сторону. Извещение должно содержать данные о характере обстоятельств, оценку их влияния на возможность исполнения Стороной своих обязательств по данному Договору, а также предполагаемые сроки их действия.
   3. В случае наступления обстоятельств непреодолимой силы срок выполнения Стороной обязательств по настоящему Договору отодвигается соразмерно времени, в течение которого действуют эти обстоятельства и их последствия.
   4. Если действие обстоятельств непреодолимой силы продолжается свыше одного месяца, Стороны проводят дополнительные переговоры для выявления приемлемых альтернативных способов исполнения настоящего Договора либо настоящий Договор подлежит расторжению в установленном порядке.
7. **Конфиденциальность**
   1. Стороны в течение срока действия настоящего Договора, а также в течение 3 (трёх) лет по окончании его действия, обязуются обеспечить конфиденциальность условий Договора, а также любой иной информации и данных, получаемых друг от друга в связи с исполнением настоящего Договора (в том числе персональных данных), за исключением информации и данных, являющихся общедоступными (далее – конфиденциальная информация). Каждая из Сторон обязуется не разглашать конфиденциальную информацию третьим лицам без получения предварительного письменного согласия Стороны, являющейся владельцем конфиденциальной информации.
   2. Стороны обязуются принимать все разумные меры для защиты конфиденциальной информации друг друга от несанкционированного доступа третьих лиц, в том числе:

— хранить конфиденциальную информацию исключительно в предназначенных для этого местах, исключающих доступ к ней третьих лиц;

— ограничивать доступ к конфиденциальной информации, в том числе для сотрудников, не имеющих служебной необходимости в ознакомлении с данной информацией.

* 1. Стороны гарантируют полное соблюдение всех условий обработки, хранения и использования полученных персональных данных, согласно ФЗ «О персональных данных» № 152‑ФЗ от 27.07.2006.
  2. Стороны обязаны незамедлительно сообщить друг другу о допущенных ими либо ставшим им известным фактах разглашения или угрозы разглашения, незаконном получении или незаконном использовании конфиденциальной информации третьими лицами.
  3. Стороны не вправе в одностороннем порядке прекращать охрану конфиденциальной информации, предусмотренной настоящим Договором, в том числе в случае своей реорганизации или ликвидации в соответствии с гражданским законодательством.
  4. Под разглашением конфиденциальной информации в рамках настоящего Договора понимается действие или бездействие одной из Сторон договора, в результате которого конфиденциальная информация становится известной третьим лицам в отсутствие согласия на это владельца конфиденциальной информации. При этом форма разглашения конфиденциальной информации третьим лицам (устная, письменная, с использованием технических средств и др.) не имеет значения.
  5. Не является нарушением конфиденциальности предоставление конфиденциальной информации по законному требованию правоохранительных и иных уполномоченных государственных органов и должностных лиц в случаях и в порядке, предусмотренных применимым законодательством, а также предоставление Лицензиатом конфиденциальной информации третьим лицам в целях подтверждения опыта и квалификации Лицензиата для участия в закупочных процедурах, не противоречащих законодательству Российской Федерации.
  6. В случае раскрытия конфиденциальной информации указанным органам и/или лицам Сторона, раскрывшая конфиденциальную информацию, письменно уведомляет владельца конфиденциальной информации о факте предоставления такой информации, ее содержании и органе, которому предоставлена конфиденциальная информация, не позднее двух рабочих дней с момента раскрытия конфиденциальной информации.
  7. Стороны вправе передавать информацию о факте заключения настоящего Договора и о его условиях, за исключением финансовых, а также о сделках и соглашениях, согласно которым заключен настоящий Договор, партнерам, клиентам и иным лицам при условии подписания с указанными лицами соглашения о конфиденциальности (в качестве отдельного документа или в составе иного договора), гарантирующего предоставление соответствующими лицами защиты конфиденциальной информации на условиях не худших, чем содержатся в настоящем Договоре.
  8. В случае неисполнения Сторонами обязательств, предусмотренных настоящим разделом, Сторона, допустившее такое нарушение, обязуется возместить причиненный этим реальный ущерб в течение 5 (пяти) рабочих дней после получения соответствующего письменного требования пострадавшей Стороны.

1. **Порядок разрешения споров**
   1. В случае возникновения разногласий между Сторонами при исполнении настоящего Договора, Стороны обязуются решать их в претензионном порядке. Срок ответа на претензию составляет 10 (десять) рабочих дней с даты её получения Стороной.
   2. Если стороны не урегулировали возникшие разногласия в претензионном порядке любая из Сторон вправе обратиться в Арбитражный суд города Севастополя за защитой своих законных прав и интересов вне зависимости от встречного исполнения обязательства другой Стороной.
2. **Действие Договора. Иные условия**
   1. Настоящий Договор вступает в силу **с \_\_\_\_\_\_\_\_\_\_ и действует до 01.07.2026 г.**, в части финансовых расчетов – до полного исполнения Сторонами всех своих обязательств по нему.
   2. Настоящий Договор составлен в форме электронного документа, подписан Сторонами с помощью усиленной квалифицированной электронной подписи лица, уполномоченного на подписание Договора каждой из Сторон, в соответствии с требованиями нормативных правовых актов Российской Федерации.

При необходимости подписанный электронной подписью Договор может быть продублирован на бумажном носителе с проставлением подписей и печатей (в случае наличия) Сторон.

* 1. Если иное не установлено Договором или законом, ни одна из сторон не вправе в одностороннем порядке отказываться от исполнения Договора.
  2. В случае если для предоставления права использования программ для ЭВМ по настоящему Договору правообладателем предусмотрено заполнение регистрационных форм либо предоставление иной информации о Сублицензиате, Сублицензиат обязуется обеспечить заполнение указанных форм и предоставление надлежащей информации (далее – Регистрационная документация) в течение 3 (трёх) рабочих дней с момента получения соответствующего запроса Лицензиата, если иной срок не будет согласован Сторонами дополнительно. В случае нарушения Сублицензиатом вышеуказанного срока предоставления Регистрационной документации, Лицензиат вправе отказаться от исполнения настоящего Договора полностью или частично либо отодвинуть срок передачи права использования соразмерно времени предоставления надлежащим образом оформленной Регистрационной документации без применения каких-либо штрафных санкций и/или иных ограничений к Лицензиату.
  3. В случае подписания Сторонами дополнительных спецификаций к настоящему Договору, на указанные спецификации распространяются все применимые условия настоящего Договора.
  4. Вся переписка и переговоры, ранее имевшие место между Сторонами и относящиеся к предмету настоящего Договора, после вступления настоящего Договора в силу теряют силу. Настоящий Договор представляет собой окончательное и полное соглашение Сторон относительно его предмета. После вступления в силу настоящего Договора условия счетов и заказов, *противоречащих* настоящему Договору, не будут иметь юридической силы, если они не совершены в письменной форме и не подписаны надлежаще уполномоченными представителями обеих Сторон.
  5. Лицензиат обязуется предоставлять Сублицензиату информацию о вопросах функционирования и структуры, а также дополнительных услугах и компетенциях Лицензиата.
  6. Все изменения и дополнения к настоящему Договору имеют силу только если они совершены в письменной форме и подписаны надлежаще уполномоченными представителями Сторон.
  7. Стороны имеют право на односторонний отказ от Договора исключительно в части обязательств, срок которых не наступил на момент отказа, по следующим обстоятельствам:
  + в случае просрочки другой Стороной срока исполнения своего обязательства более чем на 60 (шестьдесят) календарных дней;
  + в случае прекращения хозяйственной деятельности другой Стороной, ее ликвидации или банкротства.
  1. Под рабочими днями в целях исполнения Сторонами обязательств по настоящему Договору понимаются рабочие дни исходя из пятидневной рабочей недели (все дни недели, кроме субботы и воскресенья), не являющиеся праздничными нерабочими днями в соответствии с действующим законодательством Российской Федерации.
  2. В случае изменения адресов и/или расчётных реквизитов Сторон, Сторона, чьи реквизиты изменились, обязана уведомить об этом другую Сторону в течение 5 (пять) рабочих дней с момента вступления в силу таких изменений. При этом заключения между Сторонами какого-либо дополнительного соглашения не требуется. Выставление счета с соответствующими реквизитами Стороны согласились считать надлежащим уведомлением.

1. **Реквизиты Сторон**

|  |  |
| --- | --- |
| **Лицензиат:** | **Сублицензиат:**  **ООО «Севастопольэнерго»** |
| **Подпись:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / /  М.П. | **Подпись:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ /  М.П. |

**Приложение №1**

*к Сублицензионному договору*

**Спецификация**

\_\_\_\_\_\_\_\_\_,именуемое в дальнейшем **Лицензиат**, в лице\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с одной стороны, и **ООО «Севастопольэнерго»,** именуемое в дальнейшем **Сублицензиат**, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_, с другой стороны, вместе именуемые — Стороны, а каждое по отдельности — Сторона, подписали настоящую Спецификацию к Договору о нижеследующем:

1. Лицензиат обязуется предоставить, а Сублицензиат оплатить лицензионное вознаграждение за предоставление права использования следующих программ для ЭВМ (*НДС не облагается*):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Правообладатель | Наименование программы для ЭВМ, право использования которой предоставляется Сублицензиату | Кол-во  лицензий**\* (шт)** | Цена,  руб.РФ | Сумма,  руб.РФ |
|  | DrWeb | Неисключительное право на использование ПО Dr.Web Desktop Security Suite (LBW-BC-12M-340:340-D3), Неисключительное право на использование ПО Dr.Web Server Security Suite (LBS-AC-12M-35:30-D3), Неисключительное право на использование ПО Dr.Web Mail Security Suite (LBP-AAC-12M-250:250-D3), Неисключительное право на использование ПО Dr.Web Gateway Security Suite (LBG-AC-12M-130:130-D3) | 1 |  |  |
|  | DrWeb | Дистрибутив Медиа-комплект «Dr.Web для бизнеса сертифицированный» ФСТЭК России (сертификат №3509 действует до 27.01.2029г.) | 2 |  |  |
| **Итого общий размер лицензионного вознаграждения:** | | | |  | |

**\***Под одной лицензией понимается одна ЭВМ на которой возможно использование соответствующей программ для ЭВМ, если иное не предусмотрено Типовым соглашением правообладателя с конечным пользователем.

1. Общая стоимость предоставления права использования программ для ЭВМ (вознаграждение Лицензиата), подлежащая уплате Сублицензиатом, составляет \_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_) рублей 00 копеек, НДС не облагается.

|  |  |
| --- | --- |
| **Лицензиат:** | **Сублицензиат:**  **ООО «Севастопольэнерго»** |
| **Подпись:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /  М.П. | **Подпись:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/  М.П. |

**Лист согласования**

**Запрос котировок в электронной форме по выбору организации на право заключения договора на** Предоставление на условиях простой (неисключительной) лицензии права на использование программы: антивирус DrWeb

Версия 3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *№ п/п* | *Должность* | *ФИО* | *Подпись* | *Дата* |
| 1 | Начальник ОИТ ООО «Севастопольэнерго» *(Инициатор)* | Тлеуов И.К. |  |  |
| 2 | Директор по капитальному строительству ООО «Севастопольэнерго» | Киктенко Д.П. |  |  |
| 3 | Заместитель главного инженера по оперативно - технологическому управлению  ООО «Севастопольэнерго» | Иваненко СА. |  |  |
| 4 | Главный бухгалтер  ООО «Севастопольэнерго» | Скрябина Е.А. |  |  |
| 5 | Начальник правового отдела  ООО «Севастопольэнерго» | Агапова И.В. |  |  |
| 6 | Заместитель генерального директора по безопасности  ООО «Севастопольэнерго» | Радченко В.Б. |  |  |
| 7 | Начальник ПЭО  ООО «Севастопольэнерго» | Плетнёва О.Е. |  |  |