Общество с ограниченной ответственностью
«**ДДОС-ГВАРД**»
Юридический адрес (почтовый адрес):
пр. Буденновский, 62/2, этаж 8
г. Ростов-на-Дону, 344000
Тел.: 8 (800) 333-17-63, +7 (495) 215-03-87

E-mail: sales@ddos-guard.net

https://ddos-guard.net

ОКПО: 00174243, ОГРН: 1149204010988

ИНН / КПП: 9204005780 / 616501001

01.06.2017г. № 0088/17

На №_____ от _____

Руководителю Московского УФАС России

г. Москва, Мясницкий проезд, дом 4, стр. 1 (вход со стороны Боярского переулка) 107078

от ООО «**ДДОС-ГВАРД**»

ЗАЯВЛЕНИЕ
о нарушении антимонопольного законодательства

Настоящее заявление подается в отношении **АКЦИОНЕРНОГО ОБЩЕСТВА «ЦЕНТРАЛЬНЫЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ЭКОНОМИКИ, ИНФОРМАТИКИ И СИСТЕМ УПРАВЛЕНИЯ» (АО «ЦНИИ ЭИСУ»)**, имеющего юридический адрес**:** 123104, Россия, г. Москва, ул. Малая Бронная, д. 2/7, стр. 1; тел.: +7 (495) 539-22-49. Руководителем АО «ЦНИИ ЭИСУ» является временный генеральный директор Вилков Сергей Валерьевич.

Нарушением антимонопольного законодательства со стороны АО «ЦНИИ ЭИСУ» явились следующие действия:

24 мая 2017 г. АО «ЦНИИ ЭИСУ» было размещено извещение № **31705148731** о проведении закупки: (http://zakupki.gov.ru/223/purchase/public/purchase/info/common-info.htmlnoticeId=5304715&epz=true&style44=false).

Наименование закупки: Открытый запрос котировок в электронной форме без квалификационного отбора на передачу права использования программного обеспечения на условиях простой (неисключительной) лицензии: «**Kaspersky DDoS Prevention (Ultimate) Russian Edition**».

ООО «ДДОС-ГВАРД» является участником данной закупки.

Номер заявки: 2 (https://opk.roseltorg.ru/#com/applic/view/id/12302/lot_id/9882).

Согласно п. 1.9 проекта договора (Приложение № 1 к документации о закупке от «24» мая 2017 г. № 37-ДПВ-2017) данный СУБЛИЦЕНЗИОННЫЙ ДОГОВОР заключается в рамках исполнения государственного контракта от 02 мая 2017 г. № **17171871480625925621945 96** (идентификатор государственного контракта 17171871480625925621945 96), заключенного между Министерством обороны Российской Федерации (Государственный заказчик) и АО «ЦНИИ ЭИСУ» (далее – Государственный контракт), в целях выполнения государственного оборонного заказа, а именно в рамках исполнения обязанности по передаче прав на использование следующего ПО: **Лицензия на право использования программного средства защиты от распределенных атак, направленных на отказ в обслуживании.** Код по ОКПД **58.29.50.000** (**Услуги** по предоставлению лицензий на право использовать компьютерное программное обеспечение).

Согласно п. 3 Спецификации, содержащейся в Приложении № 2 к документации об электронном аукционе, закупка № **0173100004517000153**; размещено: 13.03.2017 15:55; объект закупки — поставка комплекса средств защиты информации и мониторинга (по спецификации) (http://zakupki.gov.ru/epz/order/notice/ea44/view/common-info.html?regNumber=0173100004517000153), для указанного лота закупки Министерством обороны Российской Федерации (Государственным заказчиком) были установлены следующие требования (характеристики):

- Сведения о программном обеспечении должны быть включены в Единый реестр российских

программ для электронных вычислительных машин и баз данных.

- Срок действия права – не менее 1 года.
- Количество ресурсов, подлежащих защите от распределенных атак, направленных на отказ в обслуживании – не менее 8.

В комплект должно входить:

… лицензия на бумаге формата А4;
… дистрибутив и эксплуатационно-техническая документация на материальном носители информации;
… формуляр с отражением:
… сведений о разработчике;
… дате оказания услуги по предоставлению (передаче) прав на условиях простой (неисключительной) лицензии;
… перечня модулей, их назначение;
… контрольной суммы установочных файлов;
… копии сертификата соответствия по требованиям безопасности информации.

Программное средство защиты от распределенных атак, направленных на отказ в обслуживании должно отвечать следующим требованиям:

… иметь программный интерфейс и эксплуатационно-техническую документацию на русском языке;
… обеспечивать очистку (фильтрацию) трафика, направленную на снижение нагрузки на атакуемый ресурс, путем выявления и блокировки паразитного трафика, при этом:
… обеспечивать очистку трафика защищаемых ресурсов в не менее 98% случаев на основе следующего алгоритма:
… если IP адрес является вредоносным, то вероятность его блокировки равна указанному проценту по прошествии 5 минут после того, как IP адрес начал атаковать защищаемый ресурс;
… если IP адрес является адресом легитимного пользователя, то вероятность его прохождения равна указанному проценту по прошествии 5 минут после того как IP адрес начал обращаться к защищаемому ресурсу;
… обеспечивать очистку трафика в не менее 98% случаев при условии, что емкость атаки, направленной на защищаемые ресурсы, не превышает лимиты:

- **Тип атаки**

… Атаки, основанные на использовании протоколов UDP и ICMP (с большим размером пакетов)

- **Максимальная емкость атаки**

… 500 Гбит/с Атак на основе протоколов TCP, IPSEC, GRE и др. 20 Гбит/с или 25 млн пакетов/с
… приведение системы в «боевую» готовность к фильтрации трафика за время не более 15 минут;
… обеспечивать реализацию комплекса механизмов выявления паразитного трафика, при этом обеспечивать использование следующих механизмов фильтрации:
… фильтрацию на основании задаваемых через программный интерфейс черных и белых списков IP-адресов (в т.ч. формируемых администратором безопасности автоматически и передаваемых в программное средство через специализированный программный интерфейс API);
… фильтрацию по географическому признаку (месторасположение источника трафика) как с возможностью исключения определенных регионов, так и с возможностью приема трафика только от определенного списка регионов;
… фильтрацию на основании статистических параметров трафика, в т.ч. входящие и исходящие скорости трафика в пакетах и байтах в секунду, число устанавливаемых соединений (как на превышение установленных порогов, так и на их недостижение) и т.п.;
… фильтрацию на основании анализа сетевого обмена с защищаемыми ресурсами;
… сигнатурную фильтрацию трафика (на основании задаваемых шаблонов, встречающихся в сетевых пакетах);
… использование механизмов SYN-проксирования;
… пропуск трафика только по определенному администратором безопасности списку протоколов транспортного уровня;
… использование механизмов поведенческой фильтрации, в т.ч. с возможностью перенаправления трафика пользователя при помощи механизмов redirect, cookies.
… иметь возможность мониторинга трафика защищаемых ресурсов на предмет выявления

аномалий и иметь систему оповещения о выявленных аномалиях, при этом должно быть обеспечено выполнение следующих требований:

- время выявления и оповещения администратора безопасности о существенных превышениях статистических параметров в трафике защищаемого ресурса: не более 15 минут;
- администратор безопасности должен иметь возможность определять состав параметров, по которым будет производиться детектирование аномалий, в т.ч.:
- количество уникальных IP-адресов, взаимодействующих с ресурсом;
- входящее количество пакетов;
- входящий объем данных;
- количество попыток установить соединение с ресурсом;
- усредненное число байт/соединение;
- усредненное число пакетов/соединение;
- усредненное число соединений/IP;
- усредненное число Pps/IP;
- усредненное число Bps/IP;
- соотношение исходящего и входящего трафика;
- скорость входящего трафика в пакетах;
- скорость исходящего трафика в пакетах;
- скорость входящего трафика в байтах;
- скорость исходящего трафика в байтах;
- центры очистки должны иметь возможность доставки перенаправленного для очистки трафика до защищаемых ресурсов, в том числе с использованием механизмов туннелирования GRE и с использованием выделенного канала;
- обеспечивать сохранение конфиденциальности передаваемой информации на участке прохождения трафика через центры очистки;
- обладать возможностью предоставлять информацию о трафике защищаемого ресурса в едином пользовательском интерфейсе;
- формировать периодические отчеты: о состоянии защищаемого ресурса за период; о прошедших атаках; о «черных» и «белых» списках для защищаемого ресурса;
- иметь возможность сбора списка заблокированных в ходе атаки для расследования возможных инцидентов;
- обеспечивать аутентификацию при обращении к пользовательскому интерфейсу;
- функционировать в режиме «24 часа, 7 дней в неделю» без необходимости выделения технических специалистов для поддержания и обслуживания программного средства;
- техническая поддержка программного средства должна осуществляться в режиме «24 часа, 7 дней в неделю» (время реакции на обращения: не более 4 часа, время решения инцидентов, связанных с работоспособностью программного средства: не более 36 часов);
- время прохождения трафика через центры очистки во время атаки: без ограничений;
- время прохождения трафика через центры очистки после завершения Атаки: не менее 24 часов;
- предоставлять полосу пропускания легитимного трафика в объеме не менее 300 Мбит/сек.

Предоставление права на указанное программное средство в течение срока действия лицензии включает:

- бесперебойную работоспособность всех компонентов программного средства;
- предоставление (с возможностью просмотра) журналов регистрации, в которых с интервалом не менее чем в 5 минут должны быть представлены характеристики входящего – исходящего трафика, параметров отклика ресурса и т.п., при этом срок хранения журналов составляет 2 месяца для ординарной информации и 1 год для информации об атаках;
- мониторинг наличия аномалий в трафике защищаемых ресурсов (круглосуточно без праздников и выходных в режиме – «24 часа, 7 дней в неделю»);
- оповещение Получателя о наличии устойчивых аномалий в трафике и приведение программного средства защиты от распределенных атак в готовность к фильтрации:

Характер Аномалии	Время и способ оповещения об Аномалиях, не более	% своевременного выполнения, не менее
Существенная аномалия (превышение профиля трафика более чем на 50%), свидетельствующая о возможной атаке на защищаемый ресурс	15 минут по электронной почте	95%
Атака на защищаемый ресурс	15 минут по телефону	95%
	30 минут по электронной почте	95%
Возвращение характеристик трафика защищаемого ресурса к норме (превышение профиля трафика менее чем на 50%), регистрируемое в течение не менее 30 минут, свидетельствующее о завершении атаки	15 минут по телефону	95%
	30 минут по электронной почте	95%
Отклонения характеристик трафика защищаемого ресурса от профиля трафика в остальных случаях	Не производится	-

- … запуск фильтрации (по решению Получателя при условии перенаправления трафика защищаемых ресурсов центров очистки) и контроль степени очистки трафика, корректировка настроек программного средства при необходимости (время защиты в месяц – без ограничений):
- … информирование Получателя о прекращении деструктивных воздействий на защищаемые ресурсы;
- … контроль качества работы системы очистки при включенном режиме фильтрации.

Программное средства защиты от распределенных атак, направленных на отказ в обслуживании должно быть сертифицировано по требованиям безопасности информации в системе сертификации федерального органа исполнительной власти не менее:

- … 4 уровня контроля отсутствия недекларированных возможностей согласно руководящему документу «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999г.);
- … и иметь действующий сертификат соответствия на момент передачи услуг по предоставлению (передаче) прав.

Однако, АО «ЦНИИ ЭИСУ» в своем извещении № **31705148731** о проведении закупки устанавливает иные требования (характеристики) к закупаемому ПО, а именно меняет наименование объекта закупки на следующее: **«Продукция на предоставление на условиях простой (неисключительной) лицензии права использования программного обеспечения антивирусной защиты (программ для ЭВМ) «Лицензия на право использования программного средства защиты от распределенных атак, направленных на отказ в обслуживании Kaspersky DDoS Prevention (Ultimate) Russian Edition»»**.

Изменив наименование объекта закупки путем включения фразы «**Kaspersky DDoS Prevention (Ultimate) Russian Edition**», АО «ЦНИИ ЭИСУ» установило дополнительную новую характеристику объекта закупки, которая не была предусмотрена Министерством обороны РФ.

Поскольку АО «ЦНИИ ЭИСУ» действует в интересах государственного Заказчика (Министерства обороны РФ), установление новых дополнительных требований к объекту закупки не является правомерным. **Такие условия закупки изначально влекут за собой ограничение количества участников среди других производителей аналогичных программных продуктов, нарушают требования государственного Заказчика (**СУБЛИЦЕНЗИОННЫЙ ДОГОВОР заключается в рамках исполнения государственного контракта от 02 мая 2017 г. № 17171871480625925621945 96**), а также приведут к неэффективному расходованию средств выделенных для Гособоронзаказа в дальнейшем**.

Помимо наименования объекта закупки АО «ЦНИИ ЭИСУ» самовольно изменило классификацию

товара по **ОКПД**: с кода **58.29.50.000** (**Услуги** по предоставлению лицензий на право использовать компьютерное программное обеспечение), указанного Министерством обороны РФ, на код **62.01.29** (**Оригиналы** программного обеспечения прочие).

Это означает, что АО «ЦНИИ ЭИСУ» действует в ущерб интересов Министерства обороны РФ, поскольку, **вместо услуги**, в которой нуждается основной заказчик, и от которой в случае неудовлетворения качеством ее оказания в любой момент может отказаться на основании ст. 782 **Гражданского кодекса РФ**, навязывает ему **программный продукт определенного товарного знака и технических характеристик**, который в дальнейшем обяжет Министерство обороны использовать лишь ПО данного производителя, а переход на другой программный продукт будет финансово- и ресурсо- затратным. **В этом случае односторонний отказ от приобретенного ПО законодательно не предусмотрен**.

В соответствии с частью 5 ст. 17 ФЗ № 135, положения части 1 ст. 17 ФЗ № 135 распространяются, в том числе на все закупки товаров, работ, услуг, осуществляемые в соответствии с Федеральным законом от 18 июля 2011 года N 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц".

Перечень действий, ограничивающих конкуренцию, приведенный в ч. 1 ст. 17 Закона N 135-ФЗ, не является исчерпывающим, и законом не дано исчерпывающего перечня таких действий.

Запрет по существу установлен на предварительный, до проведения торгов, запроса котировок, запроса предложений, выбор заказчиком в качестве контрагента одного лица или группы лиц, из которых может быть выбран контрагент, и обеспечение победы такому лицу или одному из лиц определенной группы при создании видимости равной конкуренции для всех обратившихся.

«Kaspersky DDoS Prevention (Ultimate) Russian Edition» является продуктом Акционерного общества «Лаборатория Касперского» (Россия, Москва, 125212, Ленинградское шоссе, д.39А, стр.3, БЦ «Олимпия Парк»).

То есть, своими действиями, АО «ЦНИИ ЭИСУ» фактически обеспечило победу данной коммерческой организации или ее реселлерам, заранее выбрало своего контрагента, что является грубейшим нарушением **конституционного принципа свободы конкуренции**.

АО «ЦНИИ ЭИСУ» сделало невозможным победу других участников закупки, при условии соблюдения ими всех требований, предъявляемых к участникам закупки, установленных государственным Заказчиком. И более того, сделает эти победы невозможными и в будущем, поскольку использование ПО определенного производителя в дальнейшем обяжет Государственного заказчика использовать товарные знаки, знаки обслуживания, фирменные наименования, патенты, полезные модели, промышленные образцы, наименования места происхождения товара или наименования производителя закупаемой продукции в своих дальнейших Гособоронзаказах, что в настоящий момент не представляется возможным для него, поскольку идет вразрез с требованиями части 1 ст. 33 Федерального закона от 5 апреля 2013 г. N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд".

На основании вышеизложенного, можно сделать вывод о том, что АО «ЦНИИ ЭИСУ» нарушает требования антимонопольного законодательства, а именно:

1) Ч. 1, 2 ст. 3 Федерального закона от 18 июля 2011 г. N 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц" в части необоснованного ограничения конкуренции по отношению к участникам закупки; равноправия, справедливости, отсутствия дискриминации и необоснованных ограничений конкуренции по отношению к участникам закупки;
2) Ч. 3 ст. 3 Федерального закона от 18 июля 2011 г. N 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц" в части нецелевого и экономически неэффективного расходования денежных средств на приобретение товаров, работ, услуг (с учетом при необходимости стоимости жизненного цикла закупаемой продукции) и реализации мер, направленных на сокращение издержек заказчика;
3) П. 1 ч. 10 ст. 4 Федерального закона от 18 июля 2011 г. N 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц", в соответствии с которым документация о закупке должна содержать требования к безопасности, качеству, техническим характеристикам,

функциональным характеристикам (потребительским свойствам) товара, работы, услуги, к размерам, упаковке, отгрузке товара, к результатам работы, установленные заказчиком и предусмотренные техническими регламентами в соответствии с законодательством РФ о техническом регулировании, документами, разрабатываемыми и применяемыми в национальной системе стандартизации, принятыми в соответствии с законодательством РФ о стандартизации, иные требования, связанные с определением соответствия поставляемого товара, выполняемой работы, оказываемой услуги потребностям заказчика. **Должно содержаться обоснование необходимости использования иных требований, связанных с определением соответствия поставляемого товара, выполняемой работы, оказываемой услуги потребностям заказчика**. АО «ЦНИИ ЭИСУ» не представило обоснование выдвижения иных, дополнительных требований к объекту закупки, а также не раскрыло в документации о закупке критерии и порядок оценки и сопоставления заявок на участие в закупке.

4) Пп. 2 ч. 1 ст. 11, ч. 1 ст. 17 Федерального закона от 26 июля 2006 г. N 135-ФЗ "О защите конкуренции" (запрещаются соглашения между хозяйствующими субъектами или согласованные действия хозяйствующих субъектов на товарном рынке, если такие соглашения или согласованные действия приводят или могут привести к повышению, снижению или поддержанию цен на торгах либо к недопущению, ограничению или устранению конкуренции.) В рамках данного пункта акцентируем внимание на том, что другими участниками закупки были заявлены значительно более выгодные ценовые предложения на аналогичные товары (товары-субституты).

5) Статья 11.1. Федерального закона от 26 июля 2006 г. N 135-ФЗ "О защите конкуренции" в части запрета на согласованные действия хозяйствующих субъектов, ограничивающие конкуренцию.

6) Пп. 1, части 1 ст. 17 Федерального закона от 26 июля 2006 г. N 135-ФЗ "О защите конкуренции" в части ограничения конкуренции и (или) создания преимущественных условий для каких-либо участников;

7) Пп. 2, части 1 ст. 17 Федерального закона от 26 июля 2006 г. N 135-ФЗ "О защите конкуренции" в части создания участнику запроса котировок преимущественных условий.

8) Установление АО «ЦНИИ ЭИСУ» в Положении о закупках срока заключения договора по результатам закупки, не учитывает закрепленной в Законе о закупке и Законе о защите конкуренции процедуры административного контроля со стороны антимонопольного органа и фактически исключает применение оперативных мер, предусмотренных статьей 18.1 Закона о защите конкуренции, лишает право на обращение с жалобой какого-либо юридического смысла, **а потому направлено против прав участников закупки**. В нарушение положений ст. 18.1 Закона о защите конкуренции, Положение о закупках АО «ЦНИИ ЭИСУ» не предусматривает минимального срока заключения договора по результатам осуществления закупки, регламентировано допускающего возможность обжалования в административном порядке действий (бездействия) организатора торгов.

На основании протокола АО «ЦНИИ ЭИСУ» № **37-ДВП-2017/1** от 31 мая 2017 года, ООО ДДОС-ГВАРД, как участник запроса котировок, было признано несоответствующим требованиям закупки с формулировкой «**Отказать в допуске к участию в закупке**» Приложение № 1 к заявке на участие (Коммерческое предложение) не соответствует требованиям к продукции, установленным в Приложении № 2 к документации о закупке. **Заявка участника отклоняется на основании п. 4.12.9(3) документации о закупке**.

Настоящая формулировка также дана неверно, так как Приложение № 1 к заявке определяет соответствие критериям отнесения к субъектам малого и среднего предпринимательства, а не требования к продукции.

ООО «ДДОС-ГВАРД» обращается к Московскому УФАС РФ с заявлением о нарушении антимонопольного законодательства со стороны АО «ЦНИИ ЭИСУ», и требованием о проведении проверки описанных выше фактов, а также для установления направленности действий на ограничение конкуренции, нецелевое и экономически неэффективное расходование денежных средств, отменой

результатов проведенного запроса котировок и приведением закупки в соответствии с требованиями законодательства РФ.

К настоящему заявлению прилагаем:
1. Копия Приказа на Генерального директора;
2. Копия свидетельства ИНН;
3. Копия свидетельства ОГРН;
4. Копия заявки на участие в запросе котировок, с приложениями.

С уважением,
Генеральный директор
ООО «ДДОС-ГВАРД»

М.П.

Марченко Е.А.

DDOS-GUARD

Подписано цифровой подписью: Марченко Евгений Анатольевич
Дата: 2017.06.01 15:23:55 +03'00'