Общество с ограниченной ответственностью «Софт Билдинг» (ООО «Софт Билдинг»)
Адрес для документов: 191015, г. Санкт-Петербург, ул. Шпалерная, д. 51, лит. А, офис 528 (БЦ «Таврический»)
ИНН 7839399170 КПП 783901001
E-mail: mail@softb.ru, pravotdel@softb.ru

05.09.2019 № 1
на № _____ от _____

В Управление Федеральной антимонопольной службы по городу Москве

Адрес: 107078, г. Москва, Мясницкий проезд, дом 4, стр. 1

to77@fas.gov.ru

Жалоба на действия организатора аукциона

Жалоба на неправомерные действия аукционной комиссии организатора аукциона

Организатор аукциона
Акционерное общество «Атомкомплект» (АО «Атомкомплект»).
Место нахождения и почтовый адрес: 119180, г. Москва, ул. Большая Полянка, д.25, стр.1.
Контактное лицо: Дробижев Владимир Сергеевич
тел.(499) 949-47-40 доб. 30-20, факс (499) 949-47-36,
E-mail: info@atomkomplekt.org

Инициатор аукциона
Департамент информационных технологий Госкорпорации «Росатом».
Место нахождения: 119017, г. Москва, ул. Большая Ордынка, д. 24.
Почтовый адрес: 119017, г. Москва, ул. Большая Ордынка, д. 24.
тел. (495) 949-45-35, факс (499) 949-46-79, e-mail: info@rosatom.ru

Заказчик аукциона
В соответствии с п. 4 раздела 1 «Извещение о проведении аукциона» Аукционной документации.

Извещение по проведению открытого аукциона в электронной форме без предварительного квалификационного отбора на право заключения договоров на предоставление прав использования антивирусного программного обеспечения, установочных комплектов и сертификата технической поддержки для нужд организаций Госкорпорации «Росатом» 1 группы. Реестровый номер извещения в ЕИС - № **31908118670.**

Заявитель
ООО «Софт Билдинг»;
Адрес места нахождения: 190121, г. Санкт-Петербург, пр. Римского-Корсакова, д. 83-85, оф. 40;
Почтовый адрес: 191015, г. Санкт-Петербург, ул. Шпалерная, д. 51, лит. А, офис 528 (БЦ «Таврический»);
Контактное лицо: Савин Кирилл Сергеевич
Телефон: (812) 416-47-57, 8-800-333-2350
Электронный адрес: mail@softb.ru; K.Savin@softb.ru

Реквизиты закупки
Номер извещения на общероссийском официальном сайте: 31908118670;

Форма торгов: Открытый аукцион в электронной форме (по 94-ФЗ) (до 01.07.18);
Наименование закупки: Право заключения договоров на предоставление прав использования антивирусного программного обеспечения, установочных комплектов и сертификата технической поддержки для нужд организаций Госкорпорации «Росатом» 1 группы;
Начальная максимальная цена контракта: 68 441 984,44 руб.;
Дата публикации извещения: 02.08.2019 г;
Дата подведения итогов: 29.08.2019 г.

Доводы Жалобы

Организатор аукциона, АО «Атомкомплект», опубликовал 02.08.2019 г., извещение о проведении закупки, формой которой является **открытый аукцион в электронной форме (по 94-ФЗ) (до 01.07.18)**, объект закупки «Право заключения договоров на предоставление прав использования антивирусного программного обеспечения, установочных комплектов и сертификата технической поддержки для нужд организаций Госкорпорации «Росатом» 1 группы».

ООО «Софт Билдинг» является заинтересованным в участии в данной закупке лицом, а также в исполнении договора, в связи с чем подало заявку на участие в закупке, а также на основании статьи 18.1 Федерального закона от 26.07.2006 N 135-ФЗ «О защите конкуренции», подает настоящую Жалобу на незаконные действия организатора аукциона.

Согласно части 1 статьи 3 Федерального закона от 18.07.2011 N 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» (Далее – Закон), при закупке товаров, работ, услуг заказчики руководствуются в том числе следующими принципами: равноправие, справедливость, **отсутствие дискриминации и необоснованных ограничений конкуренции по отношению к участникам закупки**.

Согласно статьям 1.1. и 1.2 «Единого отраслевого стандарта закупок (Положение о закупке) государственной корпорации по атомной энергии «Росатом»» (Далее – Положение о закупке) целью осуществления закупочной деятельности корпорации является в том числе обеспечение единства экономического пространства, расширения возможностей участия юридических и физических лиц в закупках продукции для нужд заказчиков и стимулирования такого участия, развития добросовестной конкуренции, а принципом является конкурентность, равноправие, справедливость, отсутствие дискриминации и необоснованных ограничений по отношению к участникам закупки.

Согласно частям 9 и 10 статьи 4 Закона, в извещении об осуществлении конкурентной закупки должны быть указаны, в том числе предмет договора с указанием количества поставляемого товара, объема выполняемой работы, оказываемой услуги, а также краткое описание предмета закупки в соответствии с частью 6.1 статьи 3 настоящего Федерального закона (при необходимости). В документации о закупе должны быть указаны в том числе **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 Российской Федерации о техническом регулировании, документами, разрабатываемыми и применяемыми в национальной системе стандартизации, принятыми в соответствии с законодательством Российской Федерации о стандартизации, иные требования, связанные с определением соответствия поставляемого товара, выполняемой работы, оказываемой услуги потребностям заказчика. Если заказчиком в документации о закупке не используются установленные в соответствии с законодательством Российской Федерации о техническом регулировании, законодательством Российской Федерации о стандартизации требования к безопасности, качеству, техническим характеристикам, функциональным характеристикам (потребительским свойствам) товара, работы, услуги, к размерам, упаковке, отгрузке товара, к результатам работы, в документации о закупке должно содержаться обоснование необходимости использования иных требований,

связанных с определением соответствия поставляемого товара, выполняемой работы, оказываемой услуги потребностям заказчика.

Согласно условиям технического задания, требуется поставка **антивирусных решений правообладателя АО «Лаборатория Касперского» или аналог**. При этом в техническом задании не указаны характеристики эквивалентности, которым должен соответствовать аналог. Вместо этого указаны конкретные парт-номера программного обеспечения. Таким образом, исходя из требований технического задания, единственным возможным программным продуктом является антивирус правообладателя АО «Лаборатория Касперского».

На участие в закупке было подано три заявки, победителем признано ООО «ПФП Сервис» с ценой предложения 68 099 774, 52 рубля, что значительно ниже минимальных цен на требуемые лицензии данного правообладателя. Правообладатель не продает требуемых лицензий на таких условиях, что вызывает сомнения в соответствии предложения ООО «ПФП Сервис» техническому заданию.

На основании вышеизложенного, считаю, что организатор аукциона необоснованно и в нарушение установленных Положением и Законом требований, существенно ограничивает круг участников закупки, а также грубо нарушает основные принципы, установленные статьей 3 Закона.

Кроме того, закупка осуществляется с нарушением требований части 10 статьи 3 Закона, а именно нарушается порядок проведения Закупки в части установления требований к безопасности, качеству, техническим характеристикам, функциональным характеристикам (потребительским свойствам) требуемых товаров, что привело к невозможности поставки эквивалентного товара.

Организатор аукциона действует в нарушение требований статьи 3 Федерального закона от 18.07.2011 N 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц», а также части 1 статьи 17 Федерального закона от 26.07.2006 N 135-ФЗ «О защите конкуренции».

Прошу приостановить осуществление закупки в части подписания договора до рассмотрения Жалобы по существу, провести проверку законности действий организатора аукциона, а также правомерность допуска заявки ООО «ПФП Сервис» и выдать предписание об устранении нарушений.

Приложения к Жалобе.

1. Техническое задание.

2. Протокол № 3/1907191065261 от 29.08.2019 г..

3. Полномочия руководителя.

Приложение № 1 к Жалобе

УТВЕРЖДЕНО

Заместитель директора департамента
информационных технологий
Госкорпорации «Росатом»

_____/ И.Н. Холкин/

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Предмет закупки:

Предоставление прав использования антивирусного программного обеспечения, установочных комплектов и сертификата технической поддержки для нужд организаций Госкорпорации «Росатом» 1 группы (закупки которых регулируются Федеральным законом от 18 июля 2011 г. № 223-ФЗ)

Оглавление

РАЗДЕЛ 1. НАИМЕНОВАНИЕ

Предоставление прав использования антивирусного программного обеспечения, установочных комплектов и сертификата технической поддержки для нужд организаций Госкорпорации «Росатом»

РАЗДЕЛ 2. ОПИСАНИЕ

Подраздел 2.1. Состав (перечень) передаваемых прав использования ПО, поставляемых установочных комплектов и сертификата технической поддержки*

№ п/п	Заказчик по договору	Конечный заказчик	Полное наименование продукции	Партномер (серийный номер)	Кол-во, шт	Срок действия	Место поставки
	АО "Атомредметзолото"						
1	АО "Атомредметзолото"	АО "Атомредметзолото"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	300	1 год	-
2	АО "Атомредметзолото"	АО "Атомредметзолото"	Комплект установочный Kaspersky Стартовый Certified Media Pack Russian Edition KL8066RMZZZ или аналог	KL8066RMZZZ	1	-	109004, г. Москва, Б. Дровяной пер., д. 22
	АО ИК "АСЭ"						
3	АО ИК "АСЭ"	АО ИК "АСЭ"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	5200	3 года	
4	АО ИК "АСЭ"	АО ИК "АСЭ"	Комплект установочный Kaspersky Certified Media Pack Russian Edition KL8069RMZZZ или аналог	KL8069RMZZZ	1	-	603006, г. Нижний Новгород, пл. Свободы, д. 3
	АО "АТОМПРОЕКТ"						
5	АО "АТОМПРОЕКТ"	АО "АТОМПРОЕКТ"	Лицензия Endpoint Security для бизнеса Расширенный Russian Edition 5000 Node 3 year Renewal License KL4867RAYTR Kaspersky или аналог	KL4867RAYTR	2850	3 года	
6	АО "АТОМПРОЕКТ"	АО "АТОМПРОЕКТ"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	KL8067RMZZZ	3	-	197183, г. Санкт-Петербург, ул. Савушкина, д. 82, лит. А
	АО «Атомспецтранс»						
7	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	150	3 года	
8	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	50	3 года	
9	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year	KL4863RAYTR	40	3 года	

			Renewal License KL4863RAYTR Kaspersky или аналог				
10	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	50	3 года	
11	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	30	3 года	
12	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	25	3 года	
13	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	65	3 года	
14	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	30	3 года	
15	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	30	3 года	
16	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	100	3 года	
17	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	50	3 года	
18	АО «Атомспецтранс»	АО «Атомспецтранс»	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	KL8067RMZZZ	1	-	129085, г. Москва, проспект Мира, д. 81Б
	ФГУП "Атомфлот"						
19	ФГУП "Атомфлот"	ФГУП "Атомфлот"	Лицензия Endpoint Security для бизнеса Стандартный KL4863RAYDW Kaspersky Russian Edition Cross-grade на 2года (5000+ узлов) или аналог	KL4863RAYDW	740	2 года	
20	ФГУП "Атомфлот"	ФГУП "Атомфлот"	Лицензия Security для почтовых серверов KL4313RAYDW Kaspersky Russian Edition Cross-grade на 2года (5000+ адресов) или аналог	KL4313RAYDW	100	2 года	
	АО "Атомэнергомаш"						
21	АО "Атомэнергомаш"	АО "Атомэнергомаш"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year	KL4863RAYFR	479	1 год	

			Renewal License KL4863RAYFR Kaspersky или аналог				
22	АО "Атомэнергомаш"	АО "Атомэнергомаш"	Комплект установочный Kaspersky Certified Media Pack Russian Edition KL8069RMZZZ или аналог	KL8069RMZZZ	1	-	115184, г. Москва, Озерковская наб., д. 28, стр. 3
	АО "Гринатом"						
23	АО "Гринатом"	АО "Гринатом"	Лицензия KL4867RAYTR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 3 year Renewal License Kaspersky или аналог	KL4867RAYTR	5900	3 года	
24	АО "Гринатом"	АО "Гринатом"	Лицензия Security для виртуальных и облачных сред Server KL4255RATTR Kaspersky Russian Edition Renewal на 3года (250-499 вирт.серверов) или аналог	KL4255RATTR	43	3 года	
25	АО "Гринатом"	АО "Гринатом"	Лицензия KL4313RAYTR Kaspersky Security для почтовых серверов Russian Edition. 5000+ MailAddress 3 year Renewal License Kaspersky или аналог	KL4313RAYTR	20300	3 года	
26	АО "Гринатом"	АО "Гринатом"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	KL8067RMZZZ	12	-	115230, г. Москва, 1-й Нагатинский проезд, д. 10, стр. 1
27	АО "Гринатом"	АО "Гринатом"	Сертификат Maintenance Service Agreement Enterprise Russian Edition KL7157RLZTZ СрокДейств=3год Kaspersky Security или аналог	KL7157RLZTZ	1	3 года	115230, г. Москва, 1-й Нагатинский проезд, д. 10, стр. 1
28	АО "Гринатом"	АО "Гринатом"	Лицензия Endpoint Security для бизнеса Расширенный KL4867RAYFS Kaspersky Russian Edition Base на 1год (5000+ узлов) --KL4867RA Kaspersky или аналог	KL4867RAYFS	80	1 год	
	АО "ДЕЗ"						
29	АО "ДЕЗ"	АО "ДЕЗ"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	100	3 года	
	АО "НИКИМТ-Атомстрой "						
30	АО "НИКИМТ-Атомстрой"	АО "НИКИМТ-Атомстрой"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	1222	1 год	
31	АО "НИКИМТ-Атомстрой"	АО "НИКИМТ-Атомстрой"	Лицензия Kaspersky Security для почтовых серверов Russian Edition от 5000 адресов 1 год продление KL4313RAYFR Kaspersky Lab или аналог	KL4313RAYFR	1000	1 год	
	АО "НИКИЭТ"						

32	АО "НИКИЭТ"	АО "НИКИЭТ"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	KL8067RMZZZ	1	-	107140, г. Москва, ул. Красносельская М., 2/8
33	АО "НИКИЭТ"	АО "НИКИЭТ"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	1300	3 года	
34	АО "НИКИЭТ"	АО "НИКИЭТ"	Лицензия KL4313RAYTR Kaspersky Security для почтовых серверов Russian Edition. 5000+ MailAddress 3 year Renewal License Kaspersky или аналог	KL4313RAYTR	1300	3 года	
35	АО "НИКИЭТ"	АО "НИКИЭТ"	Лицензия Anti-Spam для Linux KL4713RAVTR Kaspersky Russian Edition Renewal на 3года (1000-1499 почт.ящиков) или аналог	KL4713RAVTR	1300	3 года	
	АО "Русатом Сервис"						
36	АО "Русатом Сервис"	АО "Русатом Сервис"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	346	1 год	
	ФГУП «РФЯЦ ВНИИТФ им. академ. Е.И. Забабахина»						
37	ФГУП «РФЯЦ ВНИИТФ им. академ. Е.И. Забабахина»	ФГУП «РФЯЦ ВНИИТФ им. академ. Е.И. Забабахина»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	7403	1 год	
	АО "В/О "Изотоп"						
38	АО "В/О "Изотоп"	АО "В/О "Изотоп"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	170	1 год	
	АО "СХК"						
39	АО "СХК"	АО "СХК"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	1900	3 года	
40	АО "СХК"	АО "СХК"	Лицензия Endpoint Security для бизнеса Расширенный KL4867RAYFS Kaspersky Russian Edition Base на 1год (5000+ узлов) --KL4867RA Kaspersky или аналог	KL4867RAYFS	85	1 год	
41	АО "СХК"	АО "СХК"	Комплект установочный Kaspersky Certified Media Pack Russian Edition KL8069RMZZZ или аналог	KL8069RMZZZ	2	-	636039, Томская обл., г. Северск, ул. Курчатова, д. 1
42	АО "СХК"	АО "СХК"	Дистрибутив для виртуальных сред KL8072RMZZZ Kaspersky или аналог	KL8072RMZZZ	1	Не применимо	636039, Томская обл., г. Северск, ул. Курчатова, д. 1
43	АО "СХК"	АО "СХК"	Лицензия Security для почтовых серверов KL4313RAYTS Kaspersky Russian Edition Base на 3года (5000+ адресов) или аналог	KL4313RAYTS	150	3 года	

	АО "Техснабэкспорт"						
44	АО "Техснабэкспорт"	АО "Техснабэкспорт"	Лицензия Total Security для бизнеса Russian Edition 500-999узлов на 1год KL4869RAUFR Kaspersky или аналог	KL4869RAUFR	600	1 год	
45	АО "Техснабэкспорт"	АО "Техснабэкспорт"	Лицензия Security для виртуальных и облачных сред Core Russian Edition KL4555RAPFR Renewal License СрокДейств=1год КолРабСтанц=25-49 Kaspersky Security или аналог	KL4555RAPFR	40	1 год	
	АО ФНПЦ "ПО "Старт" им. М.В. Проценко"						
46	АО ФНПЦ "ПО "Старт" им. М.В. Проценко"	АО ФНПЦ "ПО "Старт" им. М.В. Проценко"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	2100	1 год	
	АО ФНПЦ "ПО "Старт" им. М.В. Проценко" НИКИРЭТ - филиал АО "ФНПЦ "ПО "Старт" им. М.В. Проценко"						
47	АО ФНПЦ "ПО "Старт" им. М.В. Проценко" НИКИРЭТ - филиал АО "ФНПЦ "ПО "Старт" им. М.В. Проценко"	АО ФНПЦ "ПО "Старт" им. М.В. Проценко" НИКИРЭТ - филиал АО "ФНПЦ "ПО "Старт" им. М.В. Проценко"	Лицензия KL4867RAYFR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 1 year Renewal License Kaspersky или аналог	KL4867RAYFR	600	1 год	
	АО "НПК "Химпроминжиниринг "						
48	АО "НПК "Химпроминжиниринг"	АО "НПК "Химпроминжиниринг"	Лицензия KL4867RAYTR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 3 year Renewal License Kaspersky или аналог	KL4867RAYTR	200	3 года	
49	АО "НПК "Химпроминжиниринг"	АО "НПК "Химпроминжиниринг"	Лицензия KL4313RAYTR Kaspersky Security для почтовых серверов Russian Edition. 5000+ MailAddress 3 year Renewal License Kaspersky или аналог	KL4313RAYTR	400	3 года	
50	АО "НПК "Химпроминжиниринг"	АО "НПК "Химпроминжиниринг"	Комплект установочный Kaspersky Certified Media Pack Russian Edition KL8069RMZZZ или аналог	KL8069RMZZZ	1	-	109316, г. Москва, Волгоградский просп., д. 42, корп. 13
	ФГУП "Комбинат "Электрохимприбор"						
51	ФГУП "Комбинат "Электрохимприбор"	ФГУП "Комбинат "Электрохимприбор"	Лицензия KL4867RAYTR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 3 year Renewal License Kaspersky или аналог	KL4867RAYTR	4000	3 года	

	ВНИИХТ						
52	ВНИИХТ	ВНИИХТ	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	200	1 год	
	Радиевый институт им. Хлопина						
53	Радиевый институт им. Хлопина	Радиевый институт им. Хлопина	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	100	3 года	
	Госкорпорация "Росатом"						
54	Госкорпорация "Росатом"	Госкорпорация "Росатом"	Лицензия KL4867RAYTR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 3 year Renewal License Kaspersky или аналог	KL4867RAYTR	1400	3 года	
55	Госкорпорация "Росатом"	Госкорпорация "Росатом"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	KL8067RMZZZ	1	-	119017, г. Москва, ул. Большая Ордынка, д. 24
	АО "НТЦ "ЯФИ"						
56	АО "НТЦ "ЯФИ"	АО "НТЦ "ЯФИ"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	100	3 года	
57	АО "НТЦ "ЯФИ"	АО "НТЦ "ЯФИ"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	KL8067RMZZZ	1	-	194021, г. Санкт-Петербург, 2-й Муринский пр., д. 28
	АО "ФЦНИВТ "СНПО "Элерон"						
58	АО "ФЦНИВТ "СНПО "Элерон"	АО "ФЦНИВТ "СНПО "Элерон"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	3500	3 года	
	АО "НИИЭФА"						
59	АО "НИИЭФА"	АО "НИИЭФА"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	280	3 года	
	АО "ОТЭК"						
60	АО "ОТЭК"	АО "ОТЭК"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	630	3 года	

61	АО "ОТЭК"	АО "ОТЭК"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	KL8067RMZZZ	1	-	119017, г. Москва, Погорельский пер., д. 7, стр. 2
	ООО «НИИАР-ГЕНЕРАЦИЯ»						
62	ООО «НИИАР-ГЕНЕРАЦИЯ»	ООО «НИИАР-ГЕНЕРАЦИЯ»	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	KL8067RMZZZ	1	3 года	433504, Ульяновская обл., г. Димитровград, ул. Юнг Северного Флота, д. 20
63	ООО «НИИАР-ГЕНЕРАЦИЯ»	ООО «НИИАР-ГЕНЕРАЦИЯ»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	60	3 года	
	АО "НИИТФА"						
64	АО "НИИТФА"	АО "НИИТФА"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	112	3 года	
	АО "ОДЦ УГР"						
65	АО "ОДЦ УГР"	АО "ОДЦ УГР"	Лицензия Endpoint Security для бизнеса Стандартный KL4863RAYDR Kaspersky Russian Edition Renewal на 2года (5000+ узлов) или аналог	KL4863RAYDR	180	2 года	
66	АО "ОДЦ УГР"	АО "ОДЦ УГР"	Лицензия Endpoint Security для бизнеса Стандартный KL4863RAYDR Kaspersky Russian Edition Renewal на 2года (5000+ узлов) или аналог	KL4863RAYDR	20	2 года	
	ФГУП "ПО "Маяк"						
67	ФГУП "ПО "Маяк"	ФГУП "ПО "Маяк"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	4100	1 год	
68	ФГУП "ПО "Маяк"	ФГУП "ПО "Маяк"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky (для мобильных устройств) или аналог	KL4863RAYFR	10	1 год	
	АО "Концерн Росэнергоатом"						
69	АО "Концерн Росэнергоатом"	Курская АЭС-2 филиал АО "Концерн Росэнергоатом"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	270	3 года	
70	АО "Концерн Росэнергоатом"	Курская АЭС филиал АО "Концерн Росэнергоатом"	Лицензия Endpoint Security для бизнеса Расширенный KL4867RAYFS Kaspersky Russian Edition Base на 1год (5000+ узлов) или аналог	KL4867RAYFS	15	1 год	
71	АО "Концерн Росэнергоатом"	Курская АЭС филиал АО "Концерн Росэнергоатом"	Лицензия Endpoint Security для бизнеса Расширенный KL4867RAYFS Kaspersky Russian Edition Base на 1год (5000+ узлов) или аналог	KL4867RAYFS	15	1 год	

72	АО "Концерн Росэнергоатом"	Курская АЭС филиал АО "Концерн Росэнергоатом"	Лицензия Endpoint Security для бизнеса Расширенный KL4867RAYFS Kaspersky Russian Edition Base на 1год (5000+ узлов) или аналог	KL4867RAYFS	15	1 год	
73	АО "Концерн Росэнергоатом"	Курская АЭС филиал АО "Концерн Росэнергоатом"	Лицензия Endpoint Security для бизнеса Расширенный KL4867RAYFS Kaspersky Russian Edition Base на 1год (5000+ узлов) или аналог	KL4867RAYFS	15	1 год	
74	АО "Концерн Росэнергоатом"	Филиал по реализации капитальных проектов АО "Концерн Росэнергоатом"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	310	1 год	
75	АО "Концерн Росэнергоатом"	Технологический филиал АО "Концерн Росэнергоатом"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	125	3 года	
76	АО "Концерн Росэнергоатом"	Балаковская атомная станция АО "Концерн Росэнергоатом"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	KL8067RMZZZ	6	-	413801, г. Балаково, Саратовская область, филиал АО «Концерн Росэнергоатом» «Балаковская атомная станция»
77	АО "Концерн Росэнергоатом"	Нововоронежская атомная станция АО "Концерн Росэнергоатом"	Лицензия Kaspersky Endpoint Security для бизнеса–Расширенный Russian Edition 5000+ Node 2 year Renewal License KL4867RAYDR Kaspersky или аналог	KL4867RAYDR	3000	2 года	
	АО "НИЦ АЭС"						
78	АО "НИЦ АЭС"	АО "НИЦ АЭС"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	40	1 год	
	АО "Электрогорский научно-исследовательский центр по безопасности атомных станций"						
79	АО "Электрогорский научно-исследовательский центр по безопасности атомных станций"	АО "Электрогорский научно-исследовательский центр по безопасности атомных станций"	Лицензия KL4867RAYFR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 1 year Renewal License Kaspersky или аналог	KL4867RAYFR	32	1 год	
80	АО "Электрогорский научно-исследовательский центр по безопасности атомных станций"	АО "Электрогорский научно-исследовательский центр по безопасности атомных станций"	Лицензия KL4867RAYFR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 1 year Renewal License Kaspersky или аналог	KL4867RAYFR	210	1 год	
	АО "Атомтранс"						
81	АО "Атомтранс"	АО "Атомтранс"	Лицензия Endpoint Security для бизнеса Стандартный KL4863RAYDR Kaspersky Russian Edition Renewal на 2года (5000+ узлов) или аналог	KL4863RAYDR	65	2 года	

82	АО "Атомтранс"	АО "Атомтранс"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	KL8067RMZZZ	1	-	216400, Смоленская обл., г. Десногорск
	ООО "Балаковская АЭС-Авто"						
83	ООО "Балаковская АЭС-Авто"	ООО "Балаковская АЭС-Авто"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	65	1 год	
	ООО «Белоярская АЭС-Авто»						
84	ООО «Белоярская АЭС-Авто»	ООО «Белоярская АЭС-Авто»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	100	1 год	
	ООО "Волгодонская АЭС-Сервис»						
85	ООО "Волгодонская АЭС-Сервис»	ООО "Волгодонская АЭС-Сервис»	Лицензия KL4867RAYFR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 1 year Renewal License Kaspersky или аналог	KL4867RAYFR	100	1 год	
86	ООО "Волгодонская АЭС-Сервис»	ООО "Волгодонская АЭС-Сервис»	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	KL8067RMZZZ	1	-	347388, Ростовская область, г. Волгодонск, д.28
	ООО «Калининская АЭС - Сервис»						
87	ООО «Калининская АЭС - Сервис»	ООО «Калининская АЭС - Сервис»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	150	1 год	
	ООО "Нововоронежская АЭС-Авто"						
88	ООО "Нововоронежская АЭС-Авто"	ООО "Нововоронежская АЭС-Авто"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	180	1 год	
	ООО "Смоленская АЭС-Сервис"						
89	ООО "Смоленская АЭС-Сервис"	ООО "Смоленская АЭС-Сервис"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	KL8067RMZZZ	1	-	216400, Смоленская область, г. Десногорск, 3-й микрорайон, здание ИАЦ
	ООО "Энергоатоминвест"						
90	ООО "Энергоатоминвест"	ООО "Энергоатоминвест"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	KL4863RAYFR	60	1 год	

	АО "НИФХИ"						
91	АО "НИФХИ"	АО "НИФХИ"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	KL4863RAYTR	330	3 года	
92	АО "НИФХИ"	АО "НИФХИ"	Лицензия Kaspersky Security для почтовых серверов Russian Edition от 5000 адресов 3 год продление KL4313RAYTR Kaspersky Lab или аналог	KL4313RAYTR	280	3 года	

**На момент заключения договора, в случае возникшей необходимости, заказчик может внести корректировки в подраздел 2.1. настоящего Технического задания и оставить в данном подразделе информацию, относящуюся только непосредственно к его индивидуальным потребностям, исключив при этом потребности других предприятий.*

Подраздел 2.2. Описание передаваемых прав использования ПО, поставляемых установочных комплектов и сертификата технической поддержки**

№ п/п	Наименование	Требования к продукции
1	Лицензия Security для виртуальных и облачных сред Server KL4255RATTR Kaspersky Russian Edition Renewal на 3года (250-499 вирт.серверов) или аналог	В соответствии с Приложением № 1 к Техническому заданию
2	Лицензия Security для почтовых серверов KL4313RAYDW Kaspersky Russian Edition Cross-grade на 2года (5000+ адресов) или аналог	В соответствии с Приложением № 1 к Техническому заданию
3	Лицензия Kaspersky Security для почтовых серверов Russian Edition от 5000 адресов 1 год продление KL4313RAYFR Kaspersky Lab или аналог	В соответствии с Приложением № 1 к Техническому заданию
4	Лицензия KL4313RAYTR Kaspersky Security для почтовых серверов Russian Edition. 5000+ MailAddress 3 year Renewal License Kaspersky или аналог	В соответствии с Приложением № 1 к Техническому заданию
5	Лицензия Security для почтовых серверов KL4313RAYTS Kaspersky Russian Edition Base на 3года (5000+ адресов) или аналог	В соответствии с Приложением № 1 к Техническому заданию
6	Лицензия Security для виртуальных и облачных сред Core Russian Edition KL4555RAPFR Renewal License СрокДейств=1год КолРабСтанц=25-49 Kaspersky Security или аналог	В соответствии с Приложением № 1 к Техническому заданию

7	Лицензия Anti-Spam для Linux KL4713RAXTR Kaspersky Russian Edition Renewal на 3года (2500-2499 почт.ящиков) или аналог	В соответствии с Приложением № 1 к Техническому заданию
8	Лицензия Endpoint Security для бизнеса Стандартный KL4863RAYDR Kaspersky Russian Edition Renewal на 2года (5000+ узлов) или аналог	В соответствии с Приложением № 1 к Техническому заданию
9	Лицензия Endpoint Security для бизнеса Стандартный KL4863RAYDW Kaspersky Russian Edition Cross-grade на 2года (5000+ узлов) или аналог	В соответствии с Приложением № 1 к Техническому заданию
10	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	В соответствии с Приложением № 1 к Техническому заданию
11	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	В соответствии с Приложением № 1 к Техническому заданию
12	Лицензия Kaspersky Endpoint Security для бизнеса–Расширенный Russian Edition 5000+ Node 2 year Renewal License KL4867RAYDR Kaspersky или аналог	В соответствии с Приложением № 1 к Техническому заданию
13	Лицензия KL4867RAYFR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 1 year Renewal License Kaspersky или аналог	В соответствии с Приложением № 1 к Техническому заданию
14	Лицензия Endpoint Security для бизнеса Расширенный KL4867RAYFS Kaspersky Russian Edition Base на 1год (5000+ узлов) Kaspersky или аналог	В соответствии с Приложением № 1 к Техническому заданию
15	Лицензия KL4867RAYTR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 3 year Renewal License Kaspersky или аналог	В соответствии с Приложением № 1 к Техническому заданию
16	Лицензия Total Security для бизнеса Russian Edition 500-999узлов на 1год KL4869RAUFR Kaspersky или аналог	В соответствии с Приложением № 1 к Техническому заданию
17	Сертификат Maintenance Service Agreement Enterprise Russian Edition KL7157RLZTZ СрокДейств=3год Kaspersky Security или аналог	В соответствии с Приложением № 1 к Техническому заданию

18	Комплект установочный Kaspersky Стартовый Certified Media Pack Russian Edition KL8066RMZZZ или аналог	В соответствии с Приложением № 1 к Техническому заданию
19	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	В соответствии с Приложением № 1 к Техническому заданию
20	Комплект установочный Kaspersky Certified Media Pack Russian Edition KL8069RMZZZ или аналог	В соответствии с Приложением № 1 к Техническому заданию
21	Дистрибутив для виртуальных сред KL8072RMZZZ Kaspersky или аналог	В соответствии с Приложением № 1 к Техническому заданию

***На момент заключения договора, в случае возникшей необходимости, заказчик может внести корректировки в подраздел 2.2. настоящего Технического задания и оставить в данном подразделе информацию, относящуюся только непосредственно к его индивидуальным потребностям, исключив при этом потребности других предприятий.*

РАЗДЕЛ 3. ТРЕБОВАНИЯ К ПЕРЕДАВАЕМЫМ ПРАВАМ ИСПОЛЬЗОВАНИЯ ПО, ПОСТАВЛЯЕМЫМ УСТАНОВОЧНЫМ КОМПЛЕКТАМ И СЕРТИФИКАТАМ

Подраздел 3.1. Общие требования
Срок предоставления прав использования ПО, поставки установочных комплектов, сертификата технической поддержки – в течение 14 календарных дней с даты заключения договора. Право использования ПО предоставляется Сублицензиату посредством направления электронных ключей по электронной почте. Сроки действия лицензий: в соответствии с подразделом 2.1 Технического задания Место поставки установочных комплектов: в соответствии с подразделом 2.1 Технического задания. Сроки окончания и номера текущих лицензий, необходимость разбивки лицензий по диапазонам указана в Приложении № 2 к Техническому заданию.
Подраздел 3.2.Требования к качеству
Специальных требований к качеству не предъявляется.
Подраздел 3.3.Требования к гарантийным обязательствам
Специальных требований к гарантийным обязательствам не предъявляется.
Подраздел 3.4.Требования к конфиденциальности
Специальных требований к конфиденциальности не предъявляется
Подраздел 3.5 Требования к безопасности и безопасности результата
Специальных требований не предъявляется.
Подраздел 3.6 Требования по обучению персонала Сублицензиата
Требований к организации специального обучения персонала не предъявляется.
Подраздел 3.7 Требования к составу технического предложения Лицензиата
Требования не предъявляются
Подраздел 3.8 Специальные требования
Требования не предъявляются

РАЗДЕЛ 4. РЕЗУЛЬТАТ

Подраздел 4.1. Описание конечного результата
Возможность использования антивирусного программного обеспечения в соответствии со сроками, указанными в Подразделе 2.1 Технического задания
Подраздел 4.2. Требования по приемке
Факт предоставления права использования антивирусного программного обеспечения подтверждается подписанием Сторонами акта предоставления права использования ПО. Факт передачи установочных комплектов ПО и сертификатов на ТП Сублицензиату фиксируется подписанием товарной накладной (ТОРГ-12).
Подраздел 4.3. Требования по передаче Сублицензиату технических и иных документов (оформление результатов)
Требований к технической документации не предъявляется

РАЗДЕЛ 5. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОБУЧЕНИЮ ПЕРСОНАЛА СУБЛИЦЕНЗИАТА

Требований к техническому обучению персонала Сублицензиата не предъявляется

РАЗДЕЛ 6. ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

№ п/п	Сокращение	Расшифровка сокращения
1	ПО	*Программное обеспечение*

РАЗДЕЛ 7. ПЕРЕЧЕНЬ ПРИЛОЖЕНИЙ

№ п/п	Наименование
1	*Требования к функционалу программного обеспечения*
2	*Перечень продлеваемых лицензий, указание разбивки по диапазонам*

Требования к функционалу программного обеспечения

Kaspersky Endpoint Security для бизнеса – Стандартный (ФСТЭК) или аналог

Общие требования

Антивирусные средства должны включать:

- Программные средства антивирусной защиты для рабочих станций Windows.
- Программные средства антивирусной защиты для рабочих станций Linux.
- Программные средства антивирусной защиты для файловых серверов Windows.
- Программные средства антивирусной защиты для файловых серверов Linux.
- Программные средства централизованного управления, мониторинга и обновления.
- Обновляемые базы данных сигнатур вредоносных программ.
- Эксплуатационную документацию на русском языке.

Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке.

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

Требования к программным средствам антивирусной защиты для рабочих станций Windows

Средства антивирусной защиты для рабочих станций Windows должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), В и Г не ниже второго класса защиты.

Программные средства антивирусной защиты для рабочих станций Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows XP 32 bit
- Windows 7 Professional
- Windows 8 Pro/Enterprise
- Windows 10

Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей:

- возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;
- возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
- возможность читать информацию из записей аудита;
- ограничение доступа к чтению записей аудита;
- поиск, сортировка и упорядочение данных аудита;
- возможность уполномоченным пользователям (ролям) управлять данными (административными данными), используемыми функциями безопасности;
- возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;
- возможность выполнять проверки с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации;
- возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
- возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
- возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам;
- возможность выполнять проверки с целью обнаружения зараженных объектов путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
- возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из оперативной памяти, удаления файлов, в которых обнаружены вредоносная составляющая, а также подозрительных файлов, возможность перемещения и изолирования зараженных объектов;

- возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы;
- возможность отображения сигнала тревоги на рабочей станции пользователя или администратора безопасности;
- возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса;
- Антивирусное сканирование в режиме реального времени и по запросу.
- Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы.
- Антивирусное сканирование по расписанию.
- Запуск задач по расписанию и/или сразу после загрузки операционной системы.
- Антивирусная проверка в архивах форматов RAR, ARJ, ZIP, CAB.
- Защита электронной корреспонденции от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP — независимо от используемого почтового клиента;
- Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных сайтов.
- Блокировка баннеров и всплывающих окон, загружаемых с Web-страниц.
- Распознавание и блокировка фишинг-сайтов.
- Возможность определения аномального поведения приложения с помощью анализа последовательности действий этого приложения.
- Наличие механизмов защиты от атак типа BadUSB.
- Наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ.
- Осуществление контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory.
- Осуществление контроля работы пользователя с сетью Интернет, в том числе явный запрет или разрешение доступа к ресурсам определенного характера. Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory.
- Гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.
- Защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.
- Возможность установки только выбранных компонентов программного средства антивирусной защиты.
- Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для рабочих станций Linux

Средства антивирусной защиты для рабочих станций Linux должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу В и Г не ниже четвертого класса защиты.

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Debian GNU/Linux 7;
- RedHat Enterprise Linux 6;

- Ubuntu 14;
- CentOS 6;
- CentOS 7;
- AstraLinux 1.5;
- Альт 8 СП.

Программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей:

Обнаружение вредоносных программ и зараженных объектов:

• Обнаруживать и удалять следующие типы вредоносных программ при помощи сигнатурного анализа:

o компьютерные вирусы (загрузочные вирусы, макро-вирусы, файловые вирусы);

o сетевые черви (семейства Net-Worm, Email-Worm, IM-Worm, IRC-Worm, P2P-Worm, Worm);

o троянские программы (семейства Backdoor, Trojan-Ransom, Trojan-FakeAV, Trojan-ArcBomb, Trojan-Clicker, Trojan-DDoS, Trojan-Downloader, Trojan-Dropper, Trojan-IM, Trojan-Notifier, Trojan-Proxy, Trojan-SMS, Trojan-Spy, Trojan-Mailfinder, Trojan-GameThief, Trojan-PSW, Trojan-Banker, Trojan, Rootkit, Exploit);

• Вредоносные программы в архивах .zip, .rar, . arj;

• Ранее неизвестные вредоносные программы при помощи эвристического анализатора;

• Осуществлять защиту в режиме реального времени (осуществлять проверку файлов при обращении к ним со стороны ОС);

• Проводить проверку объектов по требованию;

• Проводить проверку объектов по расписанию;

• Помещать подозрительные объекты на карантин;

• Сохранять резервные копии файлов перед лечением и восстановление резервных копий;

• Обеспечивать возможность перехвата файловых операций на уровне SAMBA;

• Обеспечивать возможность просмотра отчетов о работе программного изделия через командную строку и сохранение их в файл;

• Обеспечивать возможность управления через графический интерфейс;

• Обеспечивать управление с помощью единой централизованной системы;

• Осуществлять обновления баз антивируса из заданного источника;

Кроме того, программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

• Резидентный антивирусный мониторинг.

• Проверка ресурсов доступных по SMB/NFS.

• Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы.

• Антивирусное сканирование по команде пользователя или администратора и по расписанию.

• Запуск задач по расписанию и/или сразу после загрузки операционной системы.

• Помещение подозрительных и поврежденных объектов на карантин.

• Возможность экспортировать и сохранять отчеты в форматах HTML и CSV.

• Гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.

• Сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность.

• Возможность управления через пользовательский графический интерфейс.

• Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для файловых серверов Windows

Средства антивирусной защиты для файловых серверов Windows должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу Б не ниже второго класса защиты.

Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows Server 2003 Standard Edition/Enterprise Edition x86
- Microsoft Windows Server 2008 Standard Edition/Enterprise Edition x86/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Server 2016

Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:

- возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;
- возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
- возможность читать информацию из записей аудита;
- ограничение доступа к чтению записей аудита;
- поиск, сортировка и упорядочение данных аудита;
- возможность уполномоченным пользователям (ролям) управлять данными (административными данными), используемыми функциями безопасности;
- возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;
- возможность выполнять проверки с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации;
- возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
- возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
- возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам;
- возможность выполнять проверки с целью обнаружения зараженных объектов путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
- возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из оперативной памяти, удаления файлов, в которых обнаружены вредоносная составляющая, а также подозрительных файлов, возможность перемещения и изолирования зараженных объектов;
- возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы;
- возможность отображения сигнала тревоги на рабочей станции пользователя или администратора безопасности;
- возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса;

Кроме того, программные средства антивирусной защиты для защиты файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

- Антивирусное сканирование в режиме реального времени и по запросу.
- Антивирусное сканирование по команде пользователя или администратора и по расписанию.
- Запуск задач по расписанию и/или сразу после загрузки операционной системы.
- Наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ
- Антивирусная проверка файлов в архивах форматов RAR, ARJ, ZIP, CAB.
- Настройки проверки критических областей сервера в качестве отдельной задачи.
- Регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме.

- Наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий).
- Защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.
- Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для файловых серверов Linux

Средства антивирусной защиты файловых серверов Linux должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу Б не ниже второго класса защиты.

Программные средства антивирусной защиты для файловых серверов Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
- Debian GNU/Linux 7;
- RedHat Enterprise Linux 6;
- Ubuntu 14;
- CentOS 6;
- CentOS 7;
- AstraLinux 1.5;
- Альт 8 СП.

Программные средства антивирусной защиты для файловых серверов Linux должны обеспечивать реализацию следующих функциональных возможностей:
- возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;
- возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
- возможность читать информацию из записей аудита;
- ограничение доступа к чтению записей аудита;
- упорядочение данных аудита;
- возможность уполномоченным пользователям (ролям) управлять данными (административными данными), используемыми функциями безопасности;
- возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;
- возможность выполнять проверки с целью обнаружения зараженных объектов;
- возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
- возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
- возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам;
- возможность выполнять проверки с целью обнаружения зараженных объектов путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
- возможность удаления (если технически возможно) файлов, в которых обнаружена вредоносная составляющая, а также подозрительных файлов, перемещение и изолирование объектов воздействия;
- возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций;
- возможность отображения сигнала тревоги на рабочей станции администратора безопасности;
- возможность восстановления функциональных свойств зараженных объектов;

• возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения;

Кроме того, программные средства антивирусной защиты для защиты файловых серверов Linux должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

• Резидентный антивирусный мониторинг.
• Антивирусное сканирование по команде пользователя или администратора и по расписанию.
• Проверка ресурсов доступных по SMB / NFS
• Антивирусная проверка и лечение файлов в архивах.
• Запуск задач по расписанию и/или сразу после загрузки операционной системы.
• Помещение подозрительных и поврежденных объектов на карантин.
• Формирование отчетов в форматах HTML, CSV, PDF и XLS.
• Возможность перехвата и проверки файловых операций на уровне SAMBA.
• Сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность.
• Удаленно через веб-браузер управлять антивирусом и настраивать его.
• Централизованно управляться с помощью единой системы управления.

Требования к программным средствам централизованного управления, мониторинга и обновления

Средства централизованного управления, мониторинга и обновления должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу А не ниже второго класса защиты.

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows Server 2003;
- Microsoft Windows Server 2008;
- Microsoft Windows 7;
- Microsoft Windows Server 2012;
- FreeBSD 10;
- Debian GNU/Linux 7;
- RedHat Enterprise Linux 6;
- Ubuntu 14;
- CentOS 6;
- CentOS 7;
- Astra Linux 1.5.

Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:

• Microsoft SQL Server
• MySQL
• PostgreSQL

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

• возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;
• возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
• возможность читать информацию из записей аудита;
• ограничение доступа к чтению записей аудита;
• поиск, сортировка данных аудита.
• возможность уполномоченным пользователям (ролям) управлять данными (административными данными), используемыми функциями безопасности;

- возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;
- поддержка определенных ролей и их ассоциации с конкретными администраторами безопасности.
- возможность отображения на рабочей станции администратора безопасности сигнала тревоги, идентифицирующего обнаруженные угрозы безопасности, рабочие станции и сервера, где они были обнаружены, и предпринятое антивирусным решением действие;
- возможность получения и установки обновлений антивирусных баз в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения.
- возможность централизованной установки компонентов антивирусной защиты на серверы и рабочие станции вычислительной сети.

Кроме того, программные средства централизованного управления, мониторинга и обновления должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:
- Установка системы управления антивирусной защиты из единого дистрибутива.
- Возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации.
- Возможность поиска и обнаружения компьютеров в сети по IP-адресу, имени хоста, имени домена, маске подсети.
- Автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети. Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD.
- Централизованные установка, обновление и удаление программных средств антивирусной защиты. Централизованная настройка, администрирование, просмотр отчетов и статистической информации по их работе.
- Сохранение истории изменений политик, возможность выполнить откат к предыдущим версиям;
- Наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки.
- Тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; доставка обновлений на рабочие места пользователей сразу после их получения.
- Построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне.
- Создание иерархии серверов администрирования произвольного уровня.
- Обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации.
- Автоматическое распространение лицензии на клиентские компьютеры.
- Инвентаризация установленного ПО и оборудования на компьютерах пользователей.
- Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них.
- Возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления.
- Возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления.
- Построение графических отчетов.
- Наличие преднастроенных стандартных отчетов о работе системы.
- Экспорт отчетов в файлы форматов PDF и XML.
- Централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение.
- Создание внутренних учетных записей для аутентификации на сервере управления.
- Создание резервной копии системы управления встроенными средствами системы управления.
- Наличие веб-консоли управления приложением.
- Наличие системы контроля возникновения вирусных эпидемий.

Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

- Регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток.
- Множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации.
- Проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Требования к эксплуатационной документации

Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:

- Руководство пользователя (администратора).

Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

Требования к технической поддержке

Техническая поддержка антивирусного программного обеспечения должна:

- Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации по телефону, электронной почте и через Интернет.
- Web-сайт производителя АПО должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продукт

Kaspersky Endpoint Security для бизнеса – Расширенный или аналог

Антивирусные средства должны включать:
- Программные средства антивирусной защиты для рабочих станций Windows.
- Программные средства антивирусной защиты для рабочих станций Linux.
- Программные средства антивирусной защиты для файловых серверов Windows.
- Программные средства антивирусной защиты для файловых серверов Linux.
- Программные средства централизованного управления, мониторинга и обновления.
- Обновляемые базы данных сигнатур вредоносных программ.
- Эксплуатационную документацию на русском языке.

Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке.
Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке.

Требования к программным средствам антивирусной защиты для рабочих станций Windows

Программные средства антивирусной защиты для рабочих станций Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
- Microsoft Windows XP SP3 32 bit
- Windows 7
- Windows 8/8.1
- Windows 10

Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей:
Антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
антивирусное сканирование по расписанию;
антивирусное сканирование подключаемых устройств;
эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
нейтрализация действий активного заражения;
анализ поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
блокирование действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
антивирусная проверка файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
защита электронной почты от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP;
Проверка трафика, поступающего на компьютер пользователя по протоколам HTTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов;
распознавание и блокировка фишинговых и небезопасных сайтов;
наличие встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ;
осуществление контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору;
осуществление контроля работы пользователя с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем. Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
наличие механизмов защиты от атак типа BadUSB;

Защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
возможность установки только выбранных компонентов программного средства антивирусной защиты;
централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
запуск задач по расписанию и/или сразу после загрузки операционной системы;
гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
возможность проверки целостности антивирусной программы;
возможность добавления исключений из антивирусной проверки;
наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;

Требования к программным средствам антивирусной защиты для рабочих станций Linux

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
- Linux для платформ Intel x86/amd64 на основе ядра с версией 2.6.37 или новее и библиотеку glibc версии 2.13 или новее, в т.ч.:
- Astra Linux Special Edition (Смоленск) 1.5/1.6
- CentOS 6.9, 7.4
- Debian 7.11, 8.10, 9.3
- Fedora 27
- Red Hat Enterprise Linux 7.4
- SUSE Linux Enterprise Server 11 SP4, 12 SP3
- Ubuntu 14.04, 16.04, 18.04

Программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей:
Резидентный антивирусный мониторинг;
проверка ресурсов доступных по SMB / NFS;
эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
антивирусное сканирование по команде пользователя или администратора и по расписанию;
антивирусная проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.;
наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла);
защита файлов в локальных директориях и с сетевым доступом по протоколам SMB / NFS;
помещение подозрительных и поврежденных объектов на карантин;
возможность перехвата и проверки файловых операций на уровне SAMBA;
запуск задач по расписанию и/или сразу после загрузки операционной системы;
возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
возможность управления через пользовательский графический интерфейс без root прав;
централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для файловых серверов Windows

- Microsoft Windows Server 2003 SP2 x86
- Microsoft Windows Server 2008/2008R2 x86/x64

- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Server 2016

Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:

Антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: Серверов терминалов и принт-серверов; Серверов приложений и контроллеров доменов; Файловых серверов;
антивирусное сканирование по команде пользователя или администратора и по расписанию;
запуск задач по расписанию и/или сразу после загрузки операционной системы;
антивирусная проверка в архивах форматов RAR, ARJ, ZIP, CAB;
защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting). Проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
Механизмы защиты от эксплуатирования уязвимостей в памяти процессов;
проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
настройки проверки критических областей сервера в качестве отдельной задачи;
регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме;
Наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);
ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;
возможность интеграции с SIEM системами;
возможность указания количества рабочих процессов антивируса вручную;
наличие удаленной и локальной консоли управления;
управления параметрами антивируса из командной строки;
централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

Требования к программным средствам антивирусной защиты для файловых серверов Linux.

Программные средства антивирусной защиты для файловых серверов Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Linux для платформ Intel x86/amd64 на основе ядра с версией 2.6.37 или новее и библиотеку glibc версии 2.13 или новее, в т.ч.:
- Astra Linux Special Edition 1.5/1.6
- CentOS 6.9, 7.4
- Debian 7.11, 8.10, 9.3
- Fedora 27
- Red Hat Enterprise Linux 7.4
- SUSE Linux Enterprise Server 11 SP4, 12 SP3
- Ubuntu 14.04, 16.04, 18.04

Программные средства антивирусной защиты для файловых серверов Linux должны обеспечивать реализацию следующих функциональных возможностей:
Резидентный антивирусный мониторинг;
проверка ресурсов доступных по SMB / NFS;
эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
антивирусное сканирование по команде пользователя или администратора и по расписанию;

антивирусная проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.;
проверка сообщений электронной почты в текстовом формате (Plain text);
наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла);
защита файлов в локальных директориях и с сетевым доступом по протоколам SMB / NFS;
помещение подозрительных и поврежденных объектов на карантин;
возможность перехвата и проверки файловых операций на уровне SAMBA;
запуск задач по расписанию и/или сразу после загрузки операционной системы;
возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам централизованного управления, мониторинга и обновления

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows Server 2003;
- Microsoft Windows Server 2008/2008R2;
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Server 2016;
- Microsoft Windows 7;
- Microsoft Windows 8/8.1
- Microsoft Windows 10
- FreeBSD 10/11;
- Debian GNU/Linux 7;
- RedHat Enterprise Linux 6/7;
- Ubuntu 14/16/18;
- CentOS 6/7;
- Astra Linux Special Edition (Смоленск) 1.5/1.6.

Программные средства централизованного управления, мониторинга и обновления должны функционировать со следующими СУБД:

- Microsoft SQL Server
- MySQL
- PostgreSQL

Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:
• Установка системы управления антивирусной защиты из единого дистрибутива.
• Возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации.
• Возможность поиска и обнаружения компьютеров в сети по IP-адресу, имени хоста, имени домена, маске подсети.
• Автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети. Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD.

- Централизованные установка, обновление и удаление программных средств антивирусной защиты. Централизованная настройка, администрирование, просмотр отчетов и статистической информации по их работе.
- Сохранение истории изменений политик, возможность выполнить откат к предыдущим версиям;
- Наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки.
- Тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; доставка обновлений на рабочие места пользователей сразу после их получения.
- Наличие преднастроенных ролей пользователей средств централизованного управления.
- Создание иерархии серверов администрирования произвольного уровня.
- Обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации.
- Автоматическое распространение лицензии на клиентские компьютеры.
- Инвентаризация установленного ПО и оборудования на компьютерах пользователей.
- Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них.
- Возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления.
- Возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления.
- Построение графических отчетов.
- Наличие преднастроенных стандартных отчетов о работе системы.
- Экспорт отчетов в файлы форматов PDF и XML.
- Централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение.
- Создание внутренних учетных записей для аутентификации на сервере управления.
- Создание резервной копии системы управления встроенными средствами системы управления.
- Наличие веб-консоли управления приложением.
- Наличие системы контроля возникновения вирусных эпидемий.

Kaspersky Total Security для бизнеса или аналог

Антивирусные средства должны включать:
- Программные средства антивирусной защиты для рабочих станций Windows.
- Программные средства антивирусной защиты для рабочих станций Linux.
- Программные средства антивирусной защиты для файловых серверов Windows.
- Программные средства антивирусной защиты для файловых серверов Linux.
- Программные средства централизованного управления, мониторинга и обновления.
- Обновляемые базы данных сигнатур вредоносных программ.
- Эксплуатационную документацию на русском языке.

Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке.
Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке.

Требования к программным средствам антивирусной защиты для рабочих станций Windows

Программные средства антивирусной защиты для рабочих станций Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
- Microsoft Windows XP SP3 32 bit
- Windows 7
- Windows 8/8.1
- Windows 10

Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей:
Антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
антивирусное сканирование по расписанию;
антивирусное сканирование подключаемых устройств;
эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
нейтрализация действий активного заражения;
анализ поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
блокирование действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
антивирусная проверка файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
защита электронной почты от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP;
Проверка трафика, поступающего на компьютер пользователя по протоколам HTTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов;
распознавание и блокировка фишинговых и небезопасных сайтов;
наличие встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ;
осуществление контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору;
осуществление контроля работы пользователя с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем. Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
наличие механизмов защиты от атак типа BadUSB;

Защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
возможность установки только выбранных компонентов программного средства антивирусной защиты;
централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
запуск задач по расписанию и/или сразу после загрузки операционной системы;
гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
возможность проверки целостности антивирусной программы;
возможность добавления исключений из антивирусной проверки;
наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;

Требования к программным средствам антивирусной защиты для рабочих станций Linux

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
- Linux для платформ Intel x86/amd64 на основе ядра с версией 2.6.37 или новее и библиотеку glibc версии 2.13 или новее, в т.ч.:
- Astra Linux Special Edition (Смоленск) 1.5/1.6
- CentOS 6.9, 7.4
- Debian 7.11, 8.10, 9.3
- Fedora 27
- Red Hat Enterprise Linux 7.4
- SUSE Linux Enterprise Server 11 SP4, 12 SP3
- Ubuntu 14.04, 16.04, 18.04

Программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей:
Резидентный антивирусный мониторинг;
проверка ресурсов доступных по SMB / NFS;
эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
антивирусное сканирование по команде пользователя или администратора и по расписанию;
антивирусная проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.;
наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла);
защита файлов в локальных директориях и с сетевым доступом по протоколам SMB / NFS;
помещение подозрительных и поврежденных объектов на карантин;
возможность перехвата и проверки файловых операций на уровне SAMBA;
запуск задач по расписанию и/или сразу после загрузки операционной системы;
возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
возможность управления через пользовательский графический интерфейс без root прав;
централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для файловых серверов Windows

Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows Server 2003 SP2 x86
- Microsoft Windows Server 2008/2008R2 x86/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Server 2016

Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:

Антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: Серверов терминалов и принт-серверов; Серверов приложений и контроллеров доменов; Файловых серверов;
антивирусное сканирование по команде пользователя или администратора и по расписанию;
запуск задач по расписанию и/или сразу после загрузки операционной системы;
антивирусная проверка в архивах форматов RAR, ARJ, ZIP, CAB;
защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting). Проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
Механизмы защиты от эксплуатирования уязвимостей в памяти процессов;
проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
настройки проверки критических областей сервера в качестве отдельной задачи;
регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме;
Наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);
ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;
возможность интеграции с SIEM системами;
возможность указания количества рабочих процессов антивируса вручную;
наличие удаленной и локальной консоли управления;
управления параметрами антивируса из командной строки;
централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

Требования к программным средствам антивирусной защиты для файловых серверов Linux.

Программные средства антивирусной защиты для файловых серверов Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Linux для платформ Intel x86/amd64 на основе ядра с версией 2.6.37 или новее и библиотеку glibc версии 2.13 или новее, в т.ч.:
- Astra Linux Special Edition 1.5/1.6
- CentOS 6.9, 7.4
- Debian 7.11, 8.10, 9.3
- Fedora 27
- Red Hat Enterprise Linux 7.4
- SUSE Linux Enterprise Server 11 SP4, 12 SP3
- Ubuntu 14.04, 16.04, 18.04

Программные средства антивирусной защиты для файловых серверов Linux должны обеспечивать реализацию следующих функциональных возможностей:

Резидентный антивирусный мониторинг;
проверка ресурсов доступных по SMB / NFS;
эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
антивирусное сканирование по команде пользователя или администратора и по расписанию;
антивирусная проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.;
проверка сообщений электронной почты в текстовом формате (Plain text);
наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла);
защита файлов в локальных директориях и с сетевым доступом по протоколам SMB / NFS;
помещение подозрительных и поврежденных объектов на карантин;
возможность перехвата и проверки файловых операций на уровне SAMBA;
запуск задач по расписанию и/или сразу после загрузки операционной системы;
возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам централизованного управления, мониторинга и обновления

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows Server 2003;
- Microsoft Windows Server 2008/2008R2;
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Server 2016;
- Microsoft Windows 7;
- Microsoft Windows 8/8.1
- Microsoft Windows 10
- FreeBSD 10/11;
- Debian GNU/Linux 7;
- RedHat Enterprise Linux 6/7;
- Ubuntu 14/16/18;
- CentOS 6/7;
- Astra Linux Special Edition (Смоленск) 1.5/1.6.

Программные средства централизованного управления, мониторинга и обновления должны функционировать со следующими СУБД:

- Microsoft SQL Server
- MySQL
- PostgreSQL

Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:
• Установка системы управления антивирусной защиты из единого дистрибутива.
• Возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации.
• Возможность поиска и обнаружения компьютеров в сети по IP-адресу, имени хоста, имени домена, маске подсети.

• Автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети. Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD.
• Централизованные установка, обновление и удаление программных средств антивирусной защиты. Централизованная настройка, администрирование, просмотр отчетов и статистической информации по их работе.
• Сохранение истории изменений политик, возможность выполнить откат к предыдущим версиям;
• Наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки.
• Тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; доставка обновлений на рабочие места пользователей сразу после их получения.
• Наличие преднастроенных ролей пользователей средств централизованного управления.
• Создание иерархии серверов администрирования произвольного уровня.
• Обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации.
• Автоматическое распространение лицензии на клиентские компьютеры.
• Инвентаризация установленного ПО и оборудования на компьютерах пользователей.
• Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них.
• Возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления.
• Возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления.
• Построение графических отчетов.
• Наличие преднастроенных стандартных отчетов о работе системы.
• Экспорт отчетов в файлы форматов PDF и XML.
• Централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение.
• Создание внутренних учетных записей для аутентификации на сервере управления.
• Создание резервной копии системы управления встроенными средствами системы управления.
• Наличие веб-консоли управления приложением.
• Наличие системы контроля возникновения вирусных эпидемий.

Kaspersky Security для виртуальных и облачных сред, Server & Desktop или аналог

Общие требования

Антивирусные средства защиты для гибридных сред должны защищать виртуальные машины, и серверы Windows и Linux и включать:

Антивирусные средства должны включать:

- Программные средства антивирусной защиты для рабочих станций Windows.
- Программные средства антивирусной защиты для рабочих станций Linux.
- Программные средства антивирусной защиты для файловых серверов Windows.
- Программные средства антивирусной защиты для файловых серверов Linux.
- Программные средства централизованного управления, мониторинга и обновления.
- Обновляемые базы данных сигнатур вредоносных программ и атак.
- Эксплуатационную документацию на русском языке.

Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке.

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

Требования к программным средствам антивирусной защиты для рабочих станций Windows

Программные средства антивирусной защиты для рабочих станций Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

Microsoft Windows XP SP3 32 bit

- Windows 7
- Windows 8/8.1
- Windows 10

Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей:

Антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;

антивирусное сканирование по расписанию;

антивирусное сканирование подключаемых устройств;

эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;

нейтрализация действий активного заражения;

анализ поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;

анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;

блокирование действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;

облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

антивирусная проверка файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;

защита электронной почты от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP;

Проверка трафика, поступающего на компьютер пользователя по протоколам HTTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов;

распознавание и блокировка фишинговых и небезопасных сайтов;

наличие встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ;

осуществление контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору;

осуществление контроля работы пользователя с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем. Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
наличие механизмов защиты от атак типа BadUSB;
Защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
возможность установки только выбранных компонентов программного средства антивирусной защиты;
централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
запуск задач по расписанию и/или сразу после загрузки операционной системы;
гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
возможность проверки целостности антивирусной программы;
возможность добавления исключений из антивирусной проверки;
наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;

Требования к программным средствам антивирусной защиты для рабочих станций Linux

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
- Linux для платформ Intel x86/amd64 на основе ядра с версией 2.6.37 или новее и библиотеку glibc версии 2.13 или новее, в т.ч.:
- Astra Linux Special Edition (Смоленск) 1.5/1.6
- CentOS 6.9, 7.4
- Debian 7.11, 8.10, 9.3
- Fedora 27
- Red Hat Enterprise Linux 7.4
- SUSE Linux Enterprise Server 11 SP4, 12 SP3
- Ubuntu 14.04, 16.04, 18.04

Программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей:
Резидентный антивирусный мониторинг;
проверка ресурсов доступных по SMB / NFS;
эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
антивирусное сканирование по команде пользователя или администратора и по расписанию;
антивирусная проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.;
наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла);
защита файлов в локальных директориях и с сетевым доступом по протоколам SMB / NFS;
помещение подозрительных и поврежденных объектов на карантин;
возможность перехвата и проверки файловых операций на уровне SAMBA;
запуск задач по расписанию и/или сразу после загрузки операционной системы;
возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
возможность управления через пользовательский графический интерфейс без root прав;
централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для файловых серверов Windows

Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows Server 2003 SP2 x86
- Microsoft Windows Server 2008/2008R2 x86/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Server 2016

Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:

Антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: Серверов терминалов и принт-серверов; Серверов приложений и контроллеров доменов; Файловых серверов;
антивирусное сканирование по команде пользователя или администратора и по расписанию;
запуск задач по расписанию и/или сразу после загрузки операционной системы;
антивирусная проверка в архивах форматов RAR, ARJ, ZIP, CAB;
защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting). Проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
Механизмы защиты от эксплуатирования уязвимостей в памяти процессов;
проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
настройки проверки критических областей сервера в качестве отдельной задачи;
регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме;
Наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);
ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;
возможность интеграции с SIEM системами;
возможность указания количества рабочих процессов антивируса вручную;
наличие удаленной и локальной консоли управления;
управления параметрами антивируса из командной строки;
централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

Требования к программным средствам антивирусной защиты для файловых серверов Linux.

Программные средства антивирусной защиты для файловых серверов Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Linux для платформ Intel x86/amd64 на основе ядра с версией 2.6.37 или новее и библиотеку glibc версии 2.13 или новее, в т.ч.:
- Astra Linux Special Edition 1.5/1.6
- CentOS 6.9, 7.4
- Debian 7.11, 8.10, 9.3
- Fedora 27
- Red Hat Enterprise Linux 7.4

- SUSE Linux Enterprise Server 11 SP4, 12 SP3
- Ubuntu 14.04, 16.04, 18.04

Программные средства антивирусной защиты для файловых серверов Linux должны обеспечивать реализацию следующих функциональных возможностей:
Резидентный антивирусный мониторинг;
проверка ресурсов доступных по SMB / NFS;
эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
антивирусное сканирование по команде пользователя или администратора и по расписанию;
антивирусная проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj;
проверка сообщений электронной почты в текстовом формате (Plain text);
наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла);
защита файлов в локальных директориях и с сетевым доступом по протоколам SMB / NFS;
помещение подозрительных и поврежденных объектов на карантин;
возможность перехвата и проверки файловых операций на уровне SAMBA;
запуск задач по расписанию и/или сразу после загрузки операционной системы;
возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам централизованного управления, мониторинга и обновления

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows Server 2003;
- Microsoft Windows Server 2008/2008R2;
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Server 2016;
- Microsoft Windows 7;
- Microsoft Windows 8/8.1
- Microsoft Windows 10
- FreeBSD 10/11;
- Debian GNU/Linux 7;
- RedHat Enterprise Linux 6/7;
- Ubuntu 14/16/18;
- CentOS 6/7;
- Astra Linux Special Edition (Смоленск) 1.5/1.6.

Программные средства централизованного управления, мониторинга и обновления должны функционировать со следующими СУБД:

- Microsoft SQL Server
- MySQL
- PostgreSQL

Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:
- Установка системы управления антивирусной защиты из единого дистрибутива.

• Возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации.
• Возможность поиска и обнаружения компьютеров в сети по IP-адресу, имени хоста, имени домена, маске подсети.
• Автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети. Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD.
• Централизованные установка, обновление и удаление программных средств антивирусной защиты. Централизованная настройка, администрирование, просмотр отчетов и статистической информации по их работе.
• Сохранение истории изменений политик, возможность выполнить откат к предыдущим версиям;
• Наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки.
• Тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; доставка обновлений на рабочие места пользователей сразу после их получения.
• Наличие преднастроенных ролей пользователей средств централизованного управления.
• Создание иерархии серверов администрирования произвольного уровня.
• Обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации.
• Автоматическое распространение лицензии на клиентские компьютеры.
• Инвентаризация установленного ПО и оборудования на компьютерах пользователей.
• Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них.
• Возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления.
• Возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления.
• Построение графических отчетов.
• Наличие преднастроенных стандартных отчетов о работе системы.
• Экспорт отчетов в файлы форматов PDF и XML.
• Централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение.
• Создание внутренних учетных записей для аутентификации на сервере управления.
• Создание резервной копии системы управления встроенными средствами системы управления.
• Наличие веб-консоли управления приложением.
• Наличие системы контроля возникновения вирусных эпидемий.

Kaspersky Security для почтовых серверов или аналог

Требования к программным средствам антивирусной защиты и фильтрации спама для почтовых серверов Linux

Программные средства антивирусной защиты и фильтрации спама для почтовых серверов Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Linux для платформ Intel x86/amd64 на основе ядра с версией 2.6.37 или новее и библиотеку glibc версии 2.13 или новее, в т.ч.:
- Astra Linux Special Edition 1.5/1.6
- CentOS 6.9, 7.4
- Debian 7.11, 8.10, 9.3
- Fedora 27 - 29
- Red Hat Enterprise Linux 7.4
- SUSE Linux Enterprise Server 11 SP4, 12 SP3
- Ubuntu 14.04, 16.04, 18.04
- FreeBSD 10.3, 11.1

Программные средства антивирусной антивирусной защиты и фильтрации спама для почтовых серверов Linux должны функционировать совместно с почтовыми системами следующих версий:

- Exim-4.86 и выше;
- Postfix-2.6 и выше;
- Sendmail-8.14 и выше;
- Qmail-1.03.

Веб-интерфейс должен быть протестирован на совместимость со следующими версиями браузеров:

- Mozilla Firefox версии 59 и выше.
- Internet Explorer версии 11 и выше.
- Google Chrome версии 65 и выше.

Программные средства антивирусной защиты и фильтрации спама для почтовых серверов Linux должны обеспечивать реализацию следующих функциональных возможностей:

Поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;

Проверки входящего потока почтовых сообщений на наличие спама, потенциального спама, массовых рассылок (в том числе маркетинговые рассылки) удалять сообщения;

Детектирования вредоносных и фишинговых ссылок в теле письма;

Наличие эвристических методов детектирования;

Наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки ранее неизвестных угроз;

Обнаруживать, блокировать и лечить зараженные почтовые сообщения и зараженные вложения, удалять сообщения и вложения;

Обнаруживать и блокировать сообщения, содержащие макросы во вложении (например, файлы форматов Microsoft Office с макросами), удалять сообщения или вложения;

Обнаруживать и блокировать сообщения, содержащие зашифрованные объекты, удалять сообщения или вложения;

Обнаруживать и блокировать сообщения, содержащие архивы, распознавать типы файлов внутри архивов (например, файлы формата ZIP, RAR, TGZ, 7z, QZIP);

Выполнять контентную фильтрацию сообщений по имени, размеру и типу вложений, определять истинный формат и тип вложения, независимо от его расширения, удалять сообщения, содержащие вложения определенного формата или с определенным именем или сообщения, размер которых превышает допустимый;

Интеграции со службами каталогов Active Directory и Open LDAP;

Возможность отправки ловушек и уведомлений по протоколу SNMP;

Обрабатывать почтовые сообщения согласно правилам, заданным для групп отправителей и получателей;
Обновления баз с использованием протоколов HTTP, HTTPS;
Просматривать журнал событий, аудита в веб интерфейсе программы и загружать его на жесткий диск;
Фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
Проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
Выявление подозрительных, поврежденных и защищенных паролем файлов, а также файлов, в результате проверки которых произошла ошибка;
Организация дополнительной фильтрации почтового потока сообщений по именам и типам вложенных файлов и применение к отфильтрованным сообщениям отдельных правил обработки;
Использование регулярных выражений при создании правил фильтрации;
Возможность уведомления получателя и администратора сервера о почтовом сообщении, содержащем заражённые и подозрительные объекты;
Управление работой программы должно осуществлять как стандартными средствами операционной системы с помощью командной строки, так и через специальный веб-интерфейс, работающий на браузерах: Internet Explorer, Mozilla Firefox, Google Chrome;
Возможность выявления и удаления не только однозначно вредоносных, но и потенциально опасных приложений, таких как: рекламные программы, программы-сборщики информации, программы автоматического дозвона на платные сайты и другие утилиты, которые могут использоваться злоумышленниками в своих целях.

Требования к программным средствам антивирусной защиты и фильтрации спама для серверов Microsoft Exchange
Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows Server 2008/2008R2
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Server 2016

Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать с программным обеспечением Microsoft Exchange Server следующих версий:

- Microsoft Exchange Server 2010 SP3;
- Microsoft Exchange Server 2013 SP1;
- Microsoft Exchange Server 2016.

Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны обеспечивать реализацию следующих функциональных возможностей:
Проверять входящие, исходящие, а также хранящиеся на сервере Microsoft Exchange (в том числе и в общих папках) сообщения на присутствие вредоносных объектов.
Фильтровать почтовый трафик от нежелательной почты (спама).
Проверять почтовый поток на наличие фишинговых ссылок.
Сохранять резервные копии обнаруженных объектов и спам-сообщений перед лечением или удалением;
Уведомлять получателя и администратора антивирусной безопасности о сообщениях, содержащих вредоносные объекты.
Настраивать параметры проверки сообщений в соответствии с политикой безопасности компании, в частности формировать белые и черные списки отправителей и получателей;
Поддерживать базы Антивируса и Анти-Спама в актуальном состоянии с помощью обновления в автоматическом и ручном режимах;
Управлять лицензиями Серверов безопасности, в том числе централизованно;
Выполнять фильтрацию вложений;
Наличие эвристических методов детектирования.

Проверка почтовых хранилищ и общих папок на сервере, в фоновом режиме для гарантированной обработки всех объектов с использованием самой актуальной версии антивирусных баз без заметного увеличения нагрузки на сервер.
Возможность выявления и удаления не только однозначно вредоносных, но и потенциально опасных приложений, таких как: рекламные программы, программы-сборщики информации, программы автоматического дозвона на платные сайты и другие утилиты, которые могут использоваться злоумышленниками в своих целях.
Возможность детектирования вредоносных и фишинговых ссылок в теле письма.
Наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки ранее неизвестных угроз
Проверка различных параметров письма, таких как адреса отправителей и получателей, размер письма, а также поля заголовка сообщения.
Фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
Проверка графических вложений на совпадение с известными сигнатурами спам-сообщений.
Возможность обновления антивирусных баз как с сайтов производителя, так и с внутренних сетевых ресурсов организации.
Интеграция с Active Directory.
Возможность управления всеми серверами защиты с помощью одной консоли.

Kaspersky Security для интернет-шлюзов или аналог

Программные средства защиты для прокси-серверов (далее также "программа") должны обеспечивать:
- Защиту HTTP и HTTPS трафика, проходящего через прокси-сервер.
- Защиту пользователей корпоративной сети при работе с Интернет-ресурсами: удаление вредоносных и опасных программ из потока данных, поступающего в корпоративную сеть из интернета по протоколам HTTP(S), а также контроль доступа к Интернет-ресурсам на основании категорий веб-ссылок и типов контента.
- Поддержку масштабирования и кластеризации.
- Получение обновляемых базы данных сигнатур вредоносных программ и атак.

Программа должна иметь эксплуатационную документацию на русском языке.
Программный интерфейс должен быть на русском языке.
Программа должна обладать контекстной справочной системой на русском языке.

Требования к программным средствам защиты для прокси-серверов Linux
Программные средства защиты для прокси-серверов Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
- Linux для платформ Intel x86/amd64 на основе ядра с версией 2.6.37 или новее и библиотеку glibc версии 2.13 или новее, в т.ч.:
- Astra Linux Special Edition 1.5/1.6
- CentOS 6.9, 7.4
- Debian 7.11, 8.10, 9.3
- Fedora 27 - 29
- Red Hat Enterprise Linux 7.4
- SUSE Linux Enterprise Server 11 SP4, 12 SP3
- Ubuntu 14.04, 16.04, 18.04
- FreeBSD 10.3, 11.1

Программные средства защиты для прокси-серверов Linux должны обеспечивать реализацию следующих функциональных возможностей:
- Выполнять антивирусную проверку объектов, передаваемых через прокси-сервер.
- Лечить обнаруженные зараженные объекты и, если лечение невозможно, запрещать доступ к объекту.
- Обнаруживать и лечить вирусы в любых типах файлов и вложений.
- Использовать групповые настройки для определения различных параметров фильтрации применяемых в зависимости от адреса запрашиваемого объект пользователя и адреса (URL) объекта.
- Блокировать вредоносные и фишинговые веб-сайты.
- Осуществлять контроль и защиту SSL-шифрованного сетевого трафика.
- Выполнять контентную фильтрацию входящих и исходящих файлов.
- Выполнять контроль доступа пользователей к Интернет-ресурсам на основании категорий веб-ссылок и типов контента, определенных производителем средства защиты.
- Выполнять контроль доступа пользователей к Интернет-ресурсам на основании веб-ссылок, заданных администратором средства защиты. Поддержка «черных»/«белых» списков контроля доступа. Поддержка в качестве фильтра веб-ссылок масок и регулярных выражений.
- Вести статистику работы, включающую в себя помимо прочего информацию о выполнении и результатах антивирусной проверки, ошибках в работе приложения и предупреждениях.
- Позволять экспортировать журналы событий программы в форматы CSV, XML.
- Уведомлять администратора об обнаружении вредоносных программ.
- Обеспечивать возможность сбора диагностической информации о программе.
- Настраивать параметры программы и управлять программой через веб-интерфейс.
- Поддерживать возможность импортировать и экспортировать значения параметров программы.
- Получать статистику работы программы по протоколу SNMP, включать и отключать отправку SNMP-ловушек.
- Возможность масштабирования решения, поддержка кластеризации.
- Обновлять антивирусные базы, как с сайта компании – производителя, так и из настраиваемых ресурсов (HTTP- и FTP-серверов) по расписанию или по требованию.

Требования к обновлению антивирусных баз
Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:
• Регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток.
• Проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Требования к эксплуатационной документации
Эксплуатационная документация для программных продуктов защиты прокси-серверов должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:
• Руководство пользователя (администратора).
Документация, поставляемая со средствами защиты, должна детально описывать процесс установки, настройки и эксплуатации средства защиты.

Требования к технической поддержке
Техническая поддержка программного обеспечения должна:
• Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации по телефону, электронной почте и через Интернет.
• Web-сайт производителя АПО должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов.каталога.

7. Требования к программным средствам антивирусной защиты мобильных устройств

Программные средства для антивирусной защиты смартфонов должны функционировать под управлением следующих мобильных ОС:
• Android 4.4
• Android 5.0
• Android 5.1
• Android 6.0
• Android 7.0
• Android 7.1
• Android 8.0
Программные средства антивирусной защиты мобильных устройств должны обеспечивать реализацию следующих функциональных возможностей:
• Возможность выполнять проверки с целью обнаружения зараженных объектов.
• Возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных.
• Возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами.
• Возможность выполнять проверки с целью обнаружения зараженных объектов по команде и в режиме динамического обнаружения в процессе выполнения операций доступа к объектам.
• Возможность удаления (если технически возможно) файлов, в которых обнаружены компьютерные вирусы, а также файлов, подозрительных на наличие компьютерных вирусов, перемещение и изолирование объектов воздействия.
• Возможность получения и установки обновлений без применения средств автоматизации, автоматически через сетевые подключения.
• Мгновенная проверка устанавливаемых приложений.
• Проверка файловой системы устройства по требованию.
• Блокировка вредоносных и фишинговых сайтов. Поддержка белых списков разрешенных сайтов.
• Наличие хранилища для изолирования зараженных объектов.
• Обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию
• Блокирование нежелательных SMS сообщений.

• Возможность блокировки мобильного устройства, удаление данных, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset).

8. Требования к расширенной технической поддержки продуктов

1. Общие требования

Техническая поддержка антивирусного программного обеспечения должна:

- Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты на всей территории Российской Федерации по инцидентам;
- web-сайт производителя АПО должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов;
- предоставляться возможность использования персональной учетной записи пользователя для создания, обновления и мониторинга инцидентов;
- предоставлять техническую поддержку и консультации по решению инцидентов в процессе установки, конфигурирования и функционирования продукта, по лечению файлов, зараженных вредоносным ПО;
- определять приоритет запроса к службе технической поддержки на основе влияния проблемы на бизнес-процессы;
- запросам пользователей расширенной технической поддержки присвоить более высокий приоритет относительно стандартных запросов;
- регулярно информировать о промежуточных результатах и ходе решения запросов;
- осуществлять приоритетный выпуск антивирусных баз, в случае вирусных инцидентов;
- информировать пользователей о выходе новых версий продуктов по средствам почтовой рассылки;
- осуществлять выпуск программных коррекций для программного обеспечения.
- Возможность предъявления претензий и жалоб на качество обслуживания на уровень руководителя технический поддержки регионального офиса или менеджера по работе с корпоративными клиентами;
- предоставить персонального технического менеджера для организации единого канала взаимодействия

2. Требования к персональному техническому менеджеру

- Выделенный ПТМ должен:
- являться сотрудником компании-производителя
- заниматься обработкой всех инцидентов пользователя
- организовывать работы по технической поддержке для решения инцидентов
- информировать пользователя о текущем состоянии решения запросов
- предоставлять ежеквартальную отчетность
- поддерживать IT департамент пользователя в понимании и правильном использовании рекомендаций
- проводить регулярный анализ и согласование действий, необходимых для решения технических инцидентов
- быть гарантированно доступным в рабочие дни с 10:00 до 18:30 по телефону и электронной почте

3. Требования к срокам реагирования.

Техническое консультирование по вопросам эксплуатации продукта и приём запросов на устранение негативных последствий инцидентов должно обеспечиваться посредством:

- Предоставления доступа Пользователю к Интернет-Порталу технической поддержки с возможностью размещения запросов в режиме 24x7x365 (круглосуточно, включая выходные и праздничные дни).

- Приёма запросов по телефону выделенной приоритетной линии в режиме 24x7x365

- Приёма запросов по электронной почте в режиме 24x7x365 (круглосуточно, включая выходные и праздничные дни) в случае невозможности создания запроса через Интернет-Портал
- Приёма запросов техническим менеджером в рабочие часы с 10:00 по 18:30 (время Московское) по рабочим дням

Время реакции должно обеспечиваться согласно уровню критичности:

Уровень критичности		**Время реакции не более:**
Критичный уровень	1	30 минут
Высокий уровень	2	4 рабочих часа
Средний уровень	3	6 рабочих часов
Низкий уровень	4	8 рабочих часов

УРОВНИ КРИТИЧНОСТИ ИНЦИДЕНТОВ, ОТНОСЯЩИХСЯ К ПРОДУКТУ

«**Критический уровень**»- вся локальная сеть (или критичная часть сети) не работает, что прерывает основные бизнес-процессы.

« Высокий уровень»- продукт полностью выведен из строя, но непрерывность основных бизнес процессов не нарушается.

«Средний уровень» - продукт частично выведен из строя (работает несоответствующим образом), но другое программное обеспечение пользователя не выведено из строя в результате работы продукта.

«Низкий уровень» - означает другие некритичные запросы на обслуживание. Все инциденты, не упомянутые выше, относятся к этому уровню критичности.

9. Требования к установочным комплектам (медиа-пакам)

Комплект поставки медиа-пака включает:
- CD в конверте с записанными сертифицированными приложениями
- Формуляр – документ, подтверждающий, что данный(е) CD действительно содержат сертифицированные приложения
- Заверенные копии сертификатов, подтверждающие, что предоставленные приложения действительно прошли сертификацию
- *Знак соответствия системы сертификации средств защиты информации по требованиям безопасности
информации (свидетельство № РОСС RU.0001.01БИ00) - только для сертификатов ФСТЭК

Приложение № 2 к Техническому заданию***

№ п/п	Заказчик по договору	Конечный заказчик	Полное наименование продукции	№ текущей лицензии	Срок окончания текущей лицензии	Необходимость разбивки по диапазонам
	АО "Атомредметзолото"					
1	АО "Атомредметзолото"	АО "Атомредметзолото"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	1894-181218-105411-237-774	действует до 26.12.19	
2	АО "Атомредметзолото"	АО "Атомредметзолото"	Комплект установочный Kaspersky Стартовый Certified Media Pack Russian Edition KL8066RMZZZ или аналог	-	-	
	АО ИК "АСЭ"					
3	АО ИК "АСЭ"	АО ИК "АСЭ"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	26FE-181109-152134-4-7023	действует до 30.11.19	
4	АО ИК "АСЭ	АО ИК "АСЭ	Комплект установочный Kaspersky Certified Media Pack Russian Edition KL8069RMZZZ или аналог	-	-	
	АО "АТОМПРОЕКТ"					
5	АО "АТОМПРОЕКТ"	АО "АТОМПРОЕКТ"	Лицензия Endpoint Security для бизнеса Расширенный Russian Edition 5000 Node 3 year Renewal License KL4867RAYTR Kaspersky или аналог	13C8-171010-113959-760-239; 13C8-171010-115359-877-433; 13C8-171010-133311-990-904	действует до 20.11.19	
6	АО "АТОМПРОЕКТ"	АО "АТОМПРОЕКТ"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	-	-	
	АО «Атомспецтранс»					
7	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	1688-181025-142639-497-1789	действует до 23.12.19	
8	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	1688-181025-142744-530-665	действует до 23.12.19	
9	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	1688-181025-142536-527-224	действует до 23.12.19	

10	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	1688-181025-143009-850-1411	действует до 23.12.19	
11	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	1688-181025-143301-750-1789	действует до 23.12.19	
12	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	1688-181025-143208-590-1240	действует до 23.12.19	
13	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	1688-181025-142846-440-665	действует до 23.12.19	
14	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	1688-181025-143506-617-196	действует до 23.12.19	
15	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	1688-181025-143415-380-1240	действует до 23.12.19	
16	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	1688-181025-142356-423-1789	действует до 23.12.19	
17	АО «Атомспецтранс»	АО «Атомспецтранс»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	1688-181025-142216-857-126	действует до 23.12.19	
18	АО «Атомспецтранс»	АО «Атомспецтранс»	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	-	-	
	ФГУП "Атомфлот"					
19	ФГУП "Атомфлот"	ФГУП "Атомфлот"	Лицензия Endpoint Security для бизнеса Стандартный KL4863RAYDW Kaspersky Russian Edition Cross-grade на 2года (5000+ узлов) или аналог	17E0-180314-085704-280-1495	действует до 29.03.2020	
20	ФГУП "Атомфлот"	ФГУП "Атомфлот"	Лицензия Security для почтовых серверов KL4313RAYDW Kaspersky Russian Edition Cross-grade на 2года (5000+ адресов) или аналог	17E0-180314-085837-003-1467	действует до 29.03.2020	
	АО "Атомэнергомаш"					
21	АО "Атомэнергомаш"	АО "Атомэнергомаш"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	26FE-181101-080318-7-9680	действует до 10.11.19	

22	АО "Атомэнергомаш"	АО "Атомэнергомаш"	Комплект установочный Kaspersky Certified Media Pack Russian Edition KL8069RMZZZ или аналог	-	-	
	АО "Гринатом"					
23	АО "Гринатом"	АО "Гринатом"	Лицензия KL4867RAYTR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 3 year Renewal License Kaspersky или аналог	17E0-181026-083539-180-1145	действует до 24.11.19	
24	АО "Гринатом"	АО "Гринатом"	Лицензия Security для виртуальных и облачных сред Server KL4255RATTR Kaspersky Russian Edition Renewal на 3года (250-499 вирт.серверов) или аналог	17E0-181026-084731-827-215	действует до 24.11.19	
25	АО "Гринатом"	АО "Гринатом"	Лицензия KL4313RAYTR Kaspersky Security для почтовых серверов Russian Edition. 5000+ MailAddress 3 year Renewal License Kaspersky или аналог	17E0-181026-083916-997-215	действует до 15.01.2020	Разбивка по диапазонам: 20000,300
26	АО "Гринатом"	АО "Гринатом"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	-	-	
27	АО "Гринатом"	АО "Гринатом"	Сертификат Maintenance Service Agreement Enterprise Russian Edition KL7157RLZTZ СрокДейств=3год Kaspersky Security или аналог	013E-181026-091447-400-1913	действует до 27.10.19	
28	АО "Гринатом"	АО "Гринатом"	Лицензия Endpoint Security для бизнеса Расширенный KL4867RAYFS Kaspersky Russian Edition Base на 1год (5000+ узлов) --KL4867RA Kaspersky или аналог	новый продукт	новый продукт	
	АО "ДЕЗ"					
29	АО "ДЕЗ"	АО "ДЕЗ"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	13C8-180719-141443-973-1159	действует до 27.07.19	разбивка по диапазонам: 74,26
	АО "НИКИМТ-Атомстрой "					
30	АО "НИКИМТ-Атомстрой"	АО "НИКИМТ-Атомстрой"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	13C8-180110-075207-813-1033 13C8-180110-075409-400-1560 13C8-180110-075708-730-482 13C8-180110-075855-830-482 13C8-180110-080120-327-889 13C8-180110-080239-500-889 13C8-180110-080654-940-1560 13C8-180110-080654-940-1560	действует до 05.03.2020	

31	АО "НИКИМТ-Атомстрой"	АО "НИКИМТ-Атомстрой"	Лицензия Kaspersky Security для почтовых серверов Russian Edition от 5000 адресов 1 год продление KL4313RAYFR Kaspersky Lab или аналог	-	-	
	АО "НИКИЭТ"					
32	АО "НИКИЭТ"	АО "НИКИЭТ"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	-	-	
33	АО "НИКИЭТ"	АО "НИКИЭТ"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	013E-160916-135947-210-80	действует до 29.10.19	
34	АО "НИКИЭТ"	АО "НИКИЭТ"	Лицензия KL4313RAYTR Kaspersky Security для почтовых серверов Russian Edition. 5000+ MailAddress 3 year Renewal License Kaspersky или аналог	013E-160916-135948-367-576	действует до 29.10.19	
35	АО "НИКИЭТ"	АО "НИКИЭТ"	Лицензия Anti-Spam для Linux KL4713RAXTR Kaspersky Russian Edition Renewal на 3года (2500-2499 почт.ящиков) или аналог	013E-160916-135949-237-535	действует до 29.10.19	
	АО "Русатом Сервис"					
36	АО "Русатом Сервис"	АО "Русатом Сервис"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	1688-190111-092420-947-1200	действует до 23.01.20	
	ФГУП «РФЯЦ ВНИИТФ им. академ. Е.И. Забабахина»					
37	ФГУП «РФЯЦ ВНИИТФ им. академ. Е.И. Забабахина»	ФГУП «РФЯЦ ВНИИТФ им. академ. Е.И. Забабахина»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	1AF6-181109-080448-260-129, 1AF6-181109-080449-213-129, 1AF6-181109-080450-260-129, 1AF6-181109-080451-260-604, 1AF6-181109-080452-200-604, 1AF6-181109-080453-107-1802, 1AF6-181109-080454-043-604, 1AF6-181109-080454-950-604, 1AF6-181109-080455-870-129, 1AF6-181109-080456-823-604, 1AF6-181109-080457-713-604, 1AF6-181109-080458-760-129	действуют до 20.12.2019, последняя до 15.03.2020	С разбивкой по диапазонам: 3000,507, 505, 800, 10, 4, 40, 300, 100, 21, 70, 700, 70, 25, 130, 9, 12, 1100 (расширение)
	АО "В/О "Изотоп"					

38	АО "В/О "Изотоп"	АО "В/О "Изотоп"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	1894-181010-124501-380-861	действуют до 18.10.19	
	АО "СХК"					
39	АО "СХК"	АО "СХК"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	17E0-180627-124720-373-558, 17E0-170718-080700-407-351, 17E0-170718-080836-643-528, 17E0-170718-081006-350-138, 17E0-170718-081158-590-138, 17E0-181122-083926-763-637, 17E0-181122-084051-063-637, 17E0-181122-084202-380-462, 17E0-181122-084310-303-1545	до июля 2019, до декабря 2019	
40	АО "СХК"	АО "СХК"	Лицензия Endpoint Security для бизнеса Расширенный KL4867RAYFS Kaspersky Russian Edition Base на 1год (5000+ узлов) --KL4867RA Kaspersky или аналог	новый продукт	-	
41	АО "СХК"	АО "СХК"	Комплект установочный Kaspersky Certified Media Pack Russian Edition KL8069RMZZZ или аналог	-	-	
42	АО "СХК"	АО "СХК"	Дистрибутив для виртуальных сред KL8072RMZZZ Kaspersky или аналог	-	-	
43	АО "СХК"	АО "СХК"	Лицензия Security для почтовых серверов KL4313RAYTS Kaspersky Russian Edition Base на 3года (5000+ адресов) или аналог	новый продукт	-	
	АО "Техснабэкспорт"					
44	АО "Техснабэкспорт"	АО "Техснабэкспорт"	Лицензия Total Security для бизнеса Russian Edition 500-999узлов на 1год KL4869RAUFR Kaspersky или аналог	13C8-180925-064343-770-1123	действует до 14.10.19	
45	АО "Техснабэкспорт"	АО "Техснабэкспорт"	Лицензия Security для виртуальных и облачных сред Core Russian Edition KL4555RAPFR Renewal License СрокДейств=1год КолРабСтанц=25-49 Kaspersky Security или аналог	13C8-180925-064802-300-784	действует до 22.10.19	
	АО ФНПЦ "ПО "Старт" им. М.В. Проценко"					
46	АО ФНПЦ "ПО "Старт" им. М.В. Проценко"	АО ФНПЦ "ПО "Старт" им. М.В. Проценко"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	1150-180910-115340-717-1029	действует до 23.11.19	

	АО ФНПЦ "ПО "Старт" им. М.В. Проценко" НИКИРЭТ - филиал АО "ФНПЦ "ПО "Старт" им. М.В. Проценко"					
47	АО ФНПЦ "ПО "Старт" им. М.В. Проценко" НИКИРЭТ - филиал АО "ФНПЦ "ПО "Старт" им. М.В. Проценко"	АО ФНПЦ "ПО "Старт" им. М.В. Проценко" НИКИРЭТ - филиал АО "ФНПЦ "ПО "Старт" им. М.В. Проценко"	Лицензия KL4867RAYFR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 1 year Renewal License Kaspersky или аналог	17E0-181026-123430-907-181	действует до 3.11.19	
	АО "НПК "Химпроминжиниринг"					
48	АО "НПК "Химпроминжиниринг"	АО "НПК "Химпроминжиниринг"	Лицензия KL4867RAYTR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 3 year Renewal License Kaspersky или аналог	0E26-181016-133154-557-817	действует до 1.11.19	
49	АО "НПК "Химпроминжиниринг"	АО "НПК "Химпроминжиниринг"	Лицензия KL4313RAYTR Kaspersky Security для почтовых серверов Russian Edition. 5000+ MailAddress 3 year Renewal License Kaspersky или аналог			
50	АО "НПК "Химпроминжиниринг"	АО "НПК "Химпроминжиниринг"	Комплект установочный Kaspersky Certified Media Pack Russian Edition KL8069RMZZZ или аналог	-	-	
	ФГУП "Комбинат "Электрохимприбор"					
51	ФГУП "Комбинат "Электрохимприбор"	ФГУП "Комбинат "Электрохимприбор"	Лицензия KL4867RAYTR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 3 year Renewal License Kaspersky или аналог	13C8-171031-082710-900-239	действует до 31.12.19	
	ВНИИХТ					
52	ВНИИХТ	ВНИИХТ	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	26FE-181107-081818-3-10	действует до 24.11.19	
	Радиевый институт им. Хлопина					
53	Радиевый институт им. Хлопина	Радиевый институт им. Хлопина	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	17E0-170803-123351-650-701	действует до 25.08.19	
	Госкорпорация "Росатом"					
54	Госкорпорация "Росатом"	Госкорпорация "Росатом"	Лицензия KL4867RAYTR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node	2922-181204-135914-207-88	действует до 17.12.19	

			3 year Renewal License Kaspersky или аналог			
55	Госкорпорация "Росатом"	Госкорпорация "Росатом"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	-	-	
	АО "НТЦ "ЯФИ"					
56	АО "НТЦ "ЯФИ"	АО "НТЦ "ЯФИ"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	13C8-181019-151914-623-237	действует до 21.12.19	
57	АО "НТЦ "ЯФИ"	АО "НТЦ "ЯФИ"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	-	-	
	АО "ФЦНИВТ "СНПО "Элерон"					
58	АО "ФЦНИВТ "СНПО "Элерон"	АО "ФЦНИВТ "СНПО "Элерон"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	17E0-180824-143006-753-130, 17E0-180824-143309-870-1272, 17E0-180824-143517-697-1431	действует до 4.09.19	разбивка по диапазонам: 2500+700+200+90+10
	АО "НИИЭФА"					
59	АО "НИИЭФА"	АО "НИИЭФА"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	0AFE-190116-130247-907-139	действует до 13.03.20	
	АО "ОТЭК"					
60	АО "ОТЭК"	АО "ОТЭК"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	13C8-170412-132514-430-128 13C8-170926-132207-903-138 13C8-161222-080053-413-201 13C8-170412-130701-610-684	До 20.04.2019 до 4.10.2019 до 6.01.19 До 20.04.2019	
61	АО "ОТЭК"	АО "ОТЭК"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	-	-	
	ООО «НИИАР-ГЕНЕРАЦИЯ»					
62	ООО «НИИАР-ГЕНЕРАЦИЯ»	ООО «НИИАР-ГЕНЕРАЦИЯ»	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	-	-	
63	ООО «НИИАР-ГЕНЕРАЦИЯ»	ООО «НИИАР-ГЕНЕРАЦИЯ»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	2304-180618-082150-437-1348	действует до 26.06.2019	
	АО "НИИТФА"					

64	АО "НИИТФА"	АО "НИИТФА"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	0B00-170927-131043-753-145, 2304-180122-082907-190-1304, 26FE-181127-094442-7-15238, 0B00-170915-105327-503-63	до 09.2019	разбивка по диапазонам: 89,23
	АО "ОДЦ УГР"					
65	АО "ОДЦ УГР"	АО "ОДЦ УГР"	Лицензия Endpoint Security для бизнеса Стандартный KL4863RAYDR Kaspersky Russian Edition Renewal на 2года (5000+ узлов) или аналог	2304-171023-134219-047-838	до 31.10.2019	
66	АО "ОДЦ УГР"	АО "ОДЦ УГР"	Лицензия Endpoint Security для бизнеса Стандартный KL4863RAYDR Kaspersky Russian Edition Renewal на 2года (5000+ узлов) или аналог	расширение		
	ФГУП "ПО "Маяк"					
67	ФГУП "ПО "Маяк"	ФГУП "ПО "Маяк"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	1AF6-180807-074547-257-697; 1AF6-180807-074545-767-751; 1AF6-180807-074544-273-1458; 1AF6-180807-074548-377-1458; 1AF6-180807-074549-467-1458; 1AF6-180807-074550-703-697; 1AF6-180807-074552-510-751; 1AF6-180807-074553-697-1458; 1AF6-180807-074554-910-335; 1AF6-180807-074556-290-1458; 1AF6-180807-074557-567-335; 1AF6-180807-074559-010-697; 1AF6-180807-074600-737-335;	до 10.08.2019	
68	ФГУП "ПО "Маяк"	ФГУП "ПО "Маяк"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky (для мобильных устройств) или аналог	13C8-180807-071106-147-397	до 10.08.2019	
	АО "Концерн Росэнергоатом"					
69	АО "Концерн Росэнергоатом"	Курская АЭС-2 филиал АО "Концерн Росэнергоатом"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	013E-151111-092536 013E-151111-092535	до 11.12.2019	
70	АО "Концерн Росэнергоатом"	Курская АЭС филиал АО "Концерн Росэнергоатом"	Лицензия Endpoint Security для бизнеса Расширенный KL4867RAYFS Kaspersky	Новый продукт	-	

			Russian Edition Base на 1год (5000+ узлов) или аналог			
71	АО "Концерн Росэнергоатом"	Курская АЭС филиал АО "Концерн Росэнергоатом"	Лицензия Endpoint Security для бизнеса Расширенный KL4867RAYFS Kaspersky Russian Edition Base на 1год (5000+ узлов) или аналог	Новый продукт	-	
72	АО "Концерн Росэнергоатом"	Курская АЭС филиал АО "Концерн Росэнергоатом"	Лицензия Endpoint Security для бизнеса Расширенный KL4867RAYFS Kaspersky Russian Edition Base на 1год (5000+ узлов) или аналог	Новый продукт	-	
73	АО "Концерн Росэнергоатом"	Курская АЭС филиал АО "Концерн Росэнергоатом"	Лицензия Endpoint Security для бизнеса Расширенный KL4867RAYFS Kaspersky Russian Edition Base на 1год (5000+ узлов) или аналог	Новый продукт	-	
74	АО "Концерн Росэнергоатом"	Филиал по реализации капитальных проектов АО "Концерн Росэнергоатом"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	013E-181228-132253-250-998	До 30.12.2019	
75	АО "Концерн Росэнергоатом"	Технологический филиал АО "Концерн Росэнергоатом"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000 Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	013E-181228-132251-810-998	До 30.12.2019	
76	АО "Концерн Росэнергоатом"	Балаковская атомная станция АО "Концерн Росэнергоатом"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	-	-	
77	АО "Концерн Росэнергоатом"	Нововоронежская атомная станция АО "Концерн Росэнергоатом"	Лицензия Kaspersky Endpoint Security для бизнеса–Расширенный Russian Edition 5000+ Node 2 year Renewal License KL4867RAYDR Kaspersky или аналог	013E-181228-132940-817-1485	До 29.12.2019	
	АО "НИЦ АЭС"					
78	АО "НИЦ АЭС"	АО "НИЦ АЭС"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	1FB6-180622-143411-1-2673	До 01.09.2019	
	АО "Электрогорский научно-исследовательский центр по безопасности атомных станций"					
79	АО "Электрогорский научно-исследовательский центр по безопасности атомных станций"	АО "Электрогорский научно-исследовательский центр по безопасности атомных станций"	Лицензия KL4867RAYFR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 1 year Renewal License Kaspersky или аналог	013E-181228-132034-430-995	До 07.01.2020	

80	АО "Электрогорский научно-исследовательский центр по безопасности атомных станций"	АО "Электрогорский научно-исследовательский центр по безопасности атомных станций"	Лицензия KL4867RAYFR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 1 year Renewal License Kaspersky или аналог	013E-181228-132035-617-1282	До 07.01.2020	
	АО "Атомтранс"					
81	АО "Атомтранс"	АО "Атомтранс"	Лицензия Endpoint Security для бизнеса Стандартный KL4863RAYDR Kaspersky Russian Edition Renewal на 2года (5000+ узлов) или аналог	13C8-171005-090327-707-680	До 14.10.2019	
82	АО "Атомтранс"	АО "Атомтранс"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	-	-	
	ООО "Балаковская АЭС-Авто"					
83	ООО "Балаковская АЭС-Авто"	ООО "Балаковская АЭС-Авто"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	013E-181228-132249-280-696	До 01.01.2020	
	ООО «Белоярская АЭС-Авто»					
84	ООО «Белоярская АЭС-Авто»	ООО «Белоярская АЭС-Авто»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	13C8-171004-144040-243-666	До 12.12.2019	
	ООО "Волгодонская АЭС-Сервис»					
85	ООО "Волгодонская АЭС-Сервис»	ООО "Волгодонская АЭС-Сервис»	Лицензия KL4867RAYFR Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 5000+ Node 1 year Renewal License Kaspersky или аналог	13C8-171004-144040-243-666	До 20.12.2019	
86	ООО "Волгодонская АЭС-Сервис»	ООО "Волгодонская АЭС-Сервис»	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	нет	-	
	ООО «Калининская АЭС - Сервис»					
87	ООО «Калининская АЭС - Сервис»	ООО «Калининская АЭС - Сервис»	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	13C8-171004-144040-243-666	До 01.05.2019	
	ООО "Нововоронежская АЭС-Авто"					
88	ООО "Нововоронежская АЭС-Авто"	ООО "Нововоронежская АЭС-Авто"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	13C8-171004-144040-243-666	До 12.12.2019	

	ООО "Смоленская АЭС-Сервис"					
89	ООО "Смоленская АЭС-Сервис"	ООО "Смоленская АЭС-Сервис"	Комплект установочный Kaspersky Стандартный Certified Media Pack Russian Edition KL8067RMZZZ или аналог	нет	-	
	ООО "Энергоатоминвест"					
90	ООО "Энергоатоминвест"	ООО "Энергоатоминвест"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 1 year Renewal License KL4863RAYFR Kaspersky или аналог	13C8-171004-144040-243-666	До 07.12.2019	
	АО "НИФХИ"					
91	АО "НИФХИ"	АО "НИФХИ"	Лицензия Endpoint Security для бизнеса Стандартный Russian Edition 5000+Node 3 year Renewal License KL4863RAYTR Kaspersky или аналог	1688-190117-100534-490-555; 1688-190117-100625-697-555	действуют до 25.01.20	С разбивкой по диапазонам: 280, 50
92	АО "НИФХИ"	АО "НИФХИ"	Лицензия Kaspersky Security для почтовых серверов Russian Edition от 5000 адресов 3 год продление KL4313RAYTR Kaspersky Lab или аналог	1688-190117-100433-567-174	действуют до 25.01.20	

****На момент заключения договора, в случае возникшей необходимости, заказчик может внести корректировки в Приложение № 2 настоящего Технического задания и оставить в данном приложении информацию, относящуюся только непосредственно к его индивидуальным потребностям, исключив при этом потребности других предприятий.*

ПРОТОКОЛ № 3/1907191065261
заседания аукционной комиссии по рассмотрению вторых частей заявок и подведению итогов по аукциону на право заключения договоров на предоставление прав использования антивирусного программного обеспечения, установочных комплектов и сертификата технической поддержки для нужд организаций Госкорпорации «Росатом» 1 группы

г. Москва дата подписания протокола «29» августа 2019 года.

Аукцион проводится в соответствии с Единым отраслевым стандартом закупок (Положением о закупке) Государственной корпорации по атомной энергии «Росатом», утвержденным решением наблюдательного совета Госкорпорации «Росатом» (протокол от 07.02.2012 № 37) (далее – ЕОСЗ) в редакции, указанной в аукционной документации, с использованием функционала ЭТП «Фабрикант» согласно регламенту ее работы.

Информация о закупке:
Заказчики:

1. АО "Гринатом"
2. АО "Атомредметзолото"
3. АО "НИКИМТ-Атомстрой"
4. АО "СХК"
5. АО "Концерн Росэнергоатом"
6. АО ИК "АСЭ"
7. ФГУП «ПО «Маяк»
8. АО "НИКИЭТ"
9. АО "АТОМПРОЕКТ",
10. АО «Атомспецтранс»,
11. ФГУП "Атомфлот"
12. АО «Атомэнергомаш»,
13. АО "ДЕЗ"
14. АО "Русатом Сервис"
15. ФГУП «РФЯЦ ВНИИТФ им. академ. Е.И. Забабахина»
16. АО "В/О "Изотоп"
17. АО «Техснабэкспорт»
18. АО ФНПЦ «ПО «Старт» им. М.В. Проценко»
19. АО ФНПЦ «ПО «Старт» им. М.В. Проценко» НИКИРЭТ - филиал АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»
20. АО "НПК "Химпроминжиниринг"
21. ФГУП «Комбинат «Электрохимприбор»
22. АО «ВНИИХТ»
23. Радиевый институт им. Хлопина
24. Госкорпорация "Росатом"

25. АО «НТЦ «ЯФИ»
26. АО «ФЦНИВТ «СНПО «Элерон»
27. АО "НИИЭФА"
28. АО "ОТЭК"
29. ООО «НИИАР-ГЕНЕРАЦИЯ»
30. АО «НИИТФА»
31. АО «ОДЦ УГР»
32. АО «НИЦ АЭС»
33. АО «Электрогорский научно-исследовательский центр по безопасности атомных станций»
34. АО «Атомтранс»
35. ООО «Балаковская АЭС-Авто»
36. ООО «Белоярская АЭС-Авто»,
37. ООО «Волгодонская АЭС-Сервис»,
38. ООО «Калининская АЭС - Сервис»
39. ООО «Нововоронежская АЭС-Авто»,
40. ООО «Смоленская АЭС-Сервис»,
41. ООО «Энергоатоминвест»,
42. АО «НИФХИ»,

Наименование инициатора: Департамент информационных технологий Госкорпорациям «Росатом».
Организатор аукциона: Акционерное общество «Атомкомплект» (АО «Атомкомплект»).

Наименование аукциона: открытый аукцион в электронной форме без предварительного квалификационного отбора на право заключения договоров на предоставление прав использования антивирусного программного обеспечения, установочных комплектов и сертификата технической поддержки для нужд организаций Госкорпорации «Росатом» 1 группы

Предмет договоров: предоставление прав использования антивирусного программного обеспечения, установочных комплектов и сертификата технической поддержки.

Срок выполнения поставок, оказания услуг: с Томом 2 «Техническая часть» аукционной документации
Место выполнения поставок, оказания услуг: в соответствии с Томом 2 «Техническая часть» аукционной документации
Состав и объем поставок, услуг: все необходимые сведения приведены в Томе 2 «Техническая часть» аукционной документации
Предложение частичного выполнения поставок, оказания услуг не допускается.

Начальная (максимальная) цена договора:

- 68 441 984,44 руб., включая НДС.

№ п/п	Заказчик	НМЦ, руб. с НДС
1	АО «Атомредметзолото»	104 788,92
2	АО ИК «АСЭ»	3 905 908,50
3	АО «АТОМПРОЕКТ»	4 317 776,59
4	АО «Атомспецтранс»	466 269,86
5	ФГУП «Атомфлот»	581 588,00
6	АО «Атомэнергомаш»	167 973,19
7	АО «Гринатом»	31 431 075,37
8	АО «ДЕЗ»	75 090,00
9	АО «НИКИМТ-Атомстрой»	588 250,42
10	АО «НИКИЭТ»	1 964 907,86
11	АО «Русатом Сервис»	120 446,06
12	ФГУП «РФЯЦ ВНИИТФ им. академ. Е.И. Забабахина»	2 577 058,33
13	АО «В/О «Изотоп»	59 178,70
14	АО «СХК»	1 679 520,59
15	АО «Техснабэкспорт»	1 129 672,00
16	АО ФНПЦ «ПО «Старт» им. М.В. Проценко»	731 031,00
17	АО ФНПЦ «ПО «Старт» им. М.В. Проценко» НИКИРЭТ - филиал АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»	302 850,00
18	АО «НПК «Химпроминжиниринг»	499 168,50
19	ФГУП «Комбинат «Электрохимприбор»	6 057 040,00
20	АО «ВНИИХТ»	69 622,00
21	Радиевый институт им. Хлопина	75 090,00
22	ГК «Росатом»	2 120 675,86
23	АО «НТЦ «ЯФИ»	75 801,86
24	АО «ФЦНИВТ «СНПО «Элерон»	2 628 150,00
25	АО «НИИЭФА»	210 252,00
26	АО «ОТЭК»	473 778,86
27	ООО «НИИАР-ГЕНЕРАЦИЯ»	45 765,86
28	АО «НИИТФА»	84 100,80
29	АО «ОДЦ УГР»	139 244,00
30	ФГУП «ПО «Маяк»	1 430 732,10
31	АО «Российский концерн по производству электрической и тепловой энергии на атомных станциях «Росэнергоатом»	3 517 678,78
32	АО «НИЦ АЭС»	13 924,40
33	АО «Электрогорский научно-исследовательский центр по безопасности атомных станций»	122 149,50
34	АО «Атомтранс»	45 966,16
35	ООО «Балаковская АЭС-Авто»	22 627,15
36	ООО «Белоярская АЭС-Авто»	34 811,00
37	ООО «Волгодонская АЭС-Сервис»	51 186,86
38	ООО «Калининская АЭС - Сервис»	52 216,50
39	ООО «Нововоронежская АЭС-Авто»	62 659,80
40	ООО «Смоленская АЭС-Сервис»	711,86

41	ООО «Энергоатоминвест»	20 886,60
42	АО «НИФХИ»	384 358,60

Извещение о проведении аукциона и аукционная документация опубликованы 19.07.2019 в сети «Интернет» на официальном сайте http://zakupki.gov.ru № 31908118670, официальном сайте по закупкам атомной отрасли http://zakupki.rosatom.ru закупка № 190719/1065/261 и на ЭТП «Фабрикант» http://fabrikant.ru закупка № 2574010.

Заседание аукционной комиссии проводится в очной форме в 12:55 (время московское) «28» августа 2019 года, по адресу: 119180, Москва, ул. Большая Ордынка д. 24, каб. 1011.

Заседание проводится в присутствии 3 из 6 членов аукционной комиссии. Кворум имеется.

1. Согласно результатам открытия доступа к первым частям заявок на участие в аукционе «12» августа 2019, при подаче заявки на участие в аукционе посредством программных и технических средств ЭТП «Фабрикант» в рамках данного аукциона участникам аукциона присвоены следующие уникальные идентификационные номера:
   - Организация № 1 (Идентификационный номер 2574010-1-1);
   - Организация № 2 (Идентификационный номер 2574010-1-2);
   - Организация № 4 (Идентификационный номер 2574010-1-4).

2. Согласно протоколу № 1/1907191065261 от «16» августа 2019 года по результатам рассмотрения первых частей заявок на участие в аукционе аукционной комиссией были приняты следующие решения:

2.1. Допустить к дальнейшему участию в аукционе участников, которым присвоены следующие уникальные идентификационные номера:
2.1.1. Организация № 4 (Идентификационный номер 2574010-1-4);

2.2. В соответствии с пунктом 8.2 раздела 2 Приложения 12 ЕОСЗ и пунктом 8.1 Части 2 Тома 1 аукционной документации направить запросы по уточнению заявок на участие в аукционе, а именно:
2.2.1. направить участнику аукциона Организация № 1 (Идентификационный номер 2574010-1-1) запрос о разъяснении положений заявки в связи с наличием положений, подразумевающих двойное трактование (разночтение).
2.2.2. направить участнику аукциона Организация № 2 (Идентификационный номер 2574010-1-2) запрос о разъяснении положений заявки в связи с наличием положений, подразумевающих двойное трактование (разночтение).

3. Согласно протоколу № 2/1907191065261 от «23» августа 2019 года по

результатам повторного рассмотрения первых частей заявок на участие в аукционе с учетом, в том числе, документов, дополнительно представленных участниками аукциона в ответ на направленные запросы по уточнению заявок на участие в аукционе, аукционной комиссией были приняты следующие решения:

3.1. Допустить к дальнейшему участию в аукционе участника, которому присвоен следующий уникальный идентификационный номер:
3.1.1. Организация № 1 (Идентификационный номер 2574010-1-1)
3.2. Учитывая непредставление ответа на запрос в установленные сроки в порядке, предусмотренном пунктом 10.11 Части 2 Тома 1 аукционной документации, отказать в допуске к участию в аукционе участнику, которому присвоен следующий уникальный идентификационный номер Организация № 2 (Идентификационный номер 2574010-1-2) на основании подпункта а) пункта 8.11 раздела 2 Приложения 12 ЕОСЗ и подпункта а) пункта 8.10 Части 2 Тома 1 аукционной документации.

4. Согласно результатам хода аукциона от «26» августа 2019 года на ЭТП «Фабрикант» было сделано предложение о цене договора следующим участником аукциона:

№ п/п	Идентификационный номер участника аукциона	Предложение о цене договора, руб. с учетом НДС	Дата и время поступления предложения
1	Организация № 1 (Идентификационный номер 2574010-1-1)	68 099 774,52	«26» августа 2019 года 10:08 (время московское)

5. По результатам рассмотрения вторых частей заявок на участие в аукционе аукционной комиссией были приняты следующие решения:
5.1. Признать соответствующим требованиям аукционной документации следующего участника аукциона и его заявку в целом:
5.1.1. Организация № 1 (Идентификационный номер 2574010-1-1) (ООО «ПФП Сервис», место нахождения: РФ, 107564, г. Москва, ул. Краснобогатырская, д. 2, стр. 16)

Результаты голосования членов аукционной комиссии:
«за» – 3 (три) голоса;
«против» – 0 (Ноль) голосов;
«воздержался» – 0 (Ноль) голосов.

6. Места, присвоенные аукционной комиссией участникам, соответствующим требованиям аукционной документации, подавшим заявки на участие в аукционе, соответствующие требованиям аукционной документации (первое место

присваивается участнику, который предложил минимальную цену договора):

Место	Участник аукциона	Сведения о предложении участника аукциона
1	Организация № 1 ООО «ПФП Сервис»	68 099 774,52

7. По результатам ранжирования заявок на участие в аукционе аукционной комиссией принято решение признать победителем аукциона ООО «ПФП Сервис» (РФ, 107564, г. Москва, ул. Краснобогатырская, д. 2, стр. 16) с ценой заявки 68 099 774 рубля 52 копейки, включая НДС.

Результаты голосования членов аукционной комиссии:
«за» – 3 (Три) голоса;
«против» – 0 (Ноль) голосов;
«воздержался» – 0 (Ноль) голосов.

Количество заявок на участие в закупке, которые отклонены: 1 (Одна) заявка на участие в закупке.

Секретарь аукционной комиссии (без права голоса):		
Штыкова Светлана Юрьевна	Начальник отдела по организации закупок для ПАО АО «Атомкомплект»	

РЕШЕНИЕ №1
ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«Софт Билдинг»

г. Санкт-Петербург **«22» января 2009 г.**

Я, гражданин Российской Федерации, Молотов Алексей Анатольевич, паспорт серии 40 03 243835, выдан 11 отделом милиции Фрунзенского района Санкт-Петербурга 22.11.2002 г., зарегистрированный по адресу: 190121, Санкт-Петербург, пр-кт Римского-Корсакова, д.83-85, кв.40, **решил**:

1. Создать общество с ограниченной ответственностью «Софт Билдинг», далее по тексту Общество.
2. Общество создано с целью извлечения прибыли. Общество создано без ограничения срока деятельности.
3. Общество является юридическим лицом, коммерческой организацией, имеет обособленное имущество на праве собственности и отвечает по своим обязательствам всем принадлежащим ему имуществом, может от своего имени заключать сделки, приобретать и осуществлять имущественные и личные неимущественные права, выступать истцом или ответчиком в суде, арбитражном суде.
4. Общество имеет самостоятельный баланс, расчетный и иные счета. Общество имеет круглую печать, содержащую его полное фирменное наименование на русском языке и указание на его место нахождения. Общество вправе иметь штампы и бланки со своим фирменным наименованием, собственную эмблему, а также зарегистрированный в установленном порядке товарный знак и другие средства индивидуализации.
5. Общество приобретает права юридического лица с момента его государственной регистрации.
6. Полное фирменное наименование Общества:

Общество с ограниченной ответственностью «Софт Билдинг»

Сокращенное фирменное наименование: **ООО «Софт Билдинг»**

Полное фирменное наименование на английском языке:

"Soft Building" Company Limited

Сокращенное фирменное наименование на английском языке:

"Soft Building " Co. Ltd.

7. Место нахождения Общества:

190121, Российская Федерация, Санкт-Петербург, пр.Римского-Корсакова, д.83-85, кв.40.

8. Имущество Общества принадлежит ему на праве собственности и образуется из:
-- вкладов учредителей (участников) в уставный капитал;
-- продукции, произведенной Обществом в процессе его деятельности;
-- полученных доходов;
--иного имущества, приобретенного Обществом по иным основаниям, допускаемым законодательством.

В связи с участием в образовании имущества Общества Участники имеют обязательственные права в отношении Общества, в том числе: право на участие в управлении, на долю в чистой прибыли, распределяемой среди участников и долю в имуществе при ликвидации Общества (после всех расчетов, установленных законодательством), иные права, установленные действующим законодательством и настоящим Уставом.

9. Уставный капитал Общества определяет минимальный размер имущества Общества, гарантирующего интересы его кредиторов.

Уставный капитал Общества составляется из номинальной стоимости долей его участников и на момент учреждения составляет 11500,00 руб. (одиннадцать тысяч пятьсот рублей 00 коп.), разделен на одну долю.

10. Размер и номинальная стоимость доли каждого участника составляют:

10.1. Размер доли участника Молотова Алексея Анатольевича составляет 100% от уставного капитала. Номинальная стоимость принадлежащей ему доли равна 11500,00 руб. (одиннадцать тысяч пятьсот рублей 00 коп.). Названный участник вносит вклад путем передачи Обществу на момент государственной регистрации следующего имущества, принадлежащего ему на праве собственности:

- Письменный стол «Директор», производство Польша, инв.№001, в количестве 1 шт., стоимостью 11500,00 руб. (одиннадцать тысяч пятьсот рублей 00 коп.).

Вещевые вклады передаются Обществу на праве собственности по акту приема-передачи и учитываются на балансе в соответствии с законодательством о бухгалтерском учете.

Право собственности на имущество, переданное в качестве вклада на момент государственной регистрации возникает у Общества в момент его государственной регистрации, за исключением случаев, предусмотренных законом.

10.2. На момент регистрации настоящего Решения о создании общества, уставный капитал оплачен на 100% имуществом.

11. В случае прекращения у Общества права пользования имуществом до истечения срока, на который такое имущество было передано в пользование Обществу в качестве вклада в уставный капитал. участник Общества, передавший имущество в пользование, обязан предоставить Обществу по его требованию денежную компенсацию, равную плате за пользование таким же имуществом на подобных условиях в течение оставшегося срока единовременно в срок не позднее пяти дней с момента предъявления Обществом требования о ее предоставлении. По истечении срока предоставления компенсации часть доли, пропорциональная неоплаченной части суммы компенсации переходит к Обществу.

Имущество, переданное исключенным или вышедшим участником в пользование Обществу в качестве вклада в уставны й капитал, остается в пользовании Общества в течение срока, на который оно было передано.

12. Участники имеют право:

- участвовать в управлении делами Общества в порядке, установленном Законом и Уставом;
- получать полную информацию о деятельности Общества и знакомиться с его бухгалтерскими книгами и иной документацией в порядке, предусмотренном Уставом;
- принимать участие в распределении прибыли;
- произвести отчуждение принадлежащих им долей в уставном капитале другим участникам или третьим лицам в порядке, предусмотренным Законом и учредительными документами;
- выйти в любое время из Общества независимо от согласия других участников, направив об этом извещение всем участникам Общества и директору Общества. При этом ему должна быть в течение шести месяце с момента окончания финансового года, в течение которого подано заявление о выходе,

выплачена действительная стоимость его доли или выдано имущество в натуре, такой же стоимости;

- получать в случае ликвидации Общества часть имущества, оставшегося после расчетов с кредиторами, или его стоимость.

Участники имеют также и другие права, предусмотренные Законом.

13. Участники обязаны:

- вносить вклады в порядке, в размерах, в составе и в сроки, которые предусмотрены учредительными документами Общества;
- не разглашать конфиденциальную информацию о деятельности Общества (перечень такой информации и порядок доступа к ней определяется Генеральным директором Общества).

Участники Общества несут так же и другие обязанности, вытекающие из Закона

14. Участники Общества, доли которых в совокупности составляют не менее чем 10% уставного капитала, вправе требовать в судебном порядке исключения из Общества участника, который грубо нарушает свои обязанности либо своими действиями (бездействием) делает невозможной деятельность Общества или существенно ее затрудняет.

Доля участника, исключенного из Общества, переходит к Обществу в момент вступления в законную илу решения суда об исключении участника из Общества. При этом Общество обязано выплатить исключенному участнику действительную стоимость его доли, которая определяется в порядке, установленном ст. 23 Закона.

15. Участники не отвечают по обязательствам Общества и несут риск убытков, связанных с деятельностью Общества в пределах стоимости внесенных ими вкладов в Уставный капитал.

Общество не отвечает по обязательствам своих участников.

16. Общество вправе раз в год принимать решение о распределении своей чистой прибыли между участниками Общества, получаемой Обществом после уплаты налогов и других обязательных платежей в государственные внебюджетные фонды, формирования фондов Общества.

Решение об определении части прибыли Общества, распределяемой между его участниками, принимается общим собранием участников Общества.

Часть прибыли Общества, предназначенная для распределения между его участниками, распределяется пропорционально их долям в уставном капитале Общества.

Дата выплаты определяется общим собранием участников Общества.

Общество обязано соблюдать установленные ст. 29 Закона ограничения на распределение прибыли Общества между его участниками и ограничения выплаты прибыли Общества его участникам.

17. Высшим органом Общества является общее собрание его участников.

Все участники общества имеют право присутствовать на общем собрании участников, принимать участие в обсуждении вопросов повестки дня и голосовать при принятии решений.

Каждый участник Общества имеет на общем собрании участников число голосов, равное размеру его доли в уставном капитале Общества, за исключением случаев, предусмотренных Законом и Уставом.

18. Текущее руководство деятельностью Общества осуществляет единоличный исполнительный орган - Генеральный Директор, избираемый общим собранием участников.

19. Компетенция, порядок формирования, порядок деятельности и принятия решений органами управления определяется Законом и Уставом Общества, а также внутренними документами Общества.

20. Общество может быть реорганизовано или ликвидировано добровольно по решению общего собрания участников, принятому единогласно.

Иные основания реорганизации и ликвидации, а также порядок его реорганизации и ликвидации определяются ГК РФ и другими законами.

21. Назначить Генеральным директором Общества Молотова Алексея Анатольевича.

22. Неурегулированные настоящим Решением вопросы деятельности Общества регулируются его Уставом и действующим законодательством.

23. Настоящее Решение вступает в силу со дня его подписания.

24. Настоящее Решение составлено и подписано в двух экземплярах.

25. Общество создается без ограничения срока деятельности.

Подпись Учредителя: _____ Молотов Алексей Анатольевич

РЕШЕНИЕ №1/18
единственного участника
Общества с ограниченной ответственностью
«СОФТ БИЛДИНГ»

г. Санкт-Петербург **«28» мая 2018 г.**

Я, Молотов Алексей Анатольевич, паспорт 40 13 886671, выдан ТП №1 отдела УФМС России по Санкт-Петербургу и Ленинградской обл. в Адмиралтейском р-не г. Санкт-Петербурга, дата выдачи: 19.02.2014 г. к/п 780-001, зарегистрирован по адресу: 190121, г. Санкт-Петербурга, пр-т Римского-Корсакова, 83-85, кв. 40, ИНН 781662674564, единственный участник Общества с ограниченной ответственностью «Софт Билдинг» (далее-Общество),

ПРИНЯЛ РЕШЕНИЕ:

1. Освободить Молотова Алексея Анатольевича от занимаемой должности Генерального директора Общества с ограниченной ответственностью «Софт Билдинг» 05 июня 2018 г.
2. Назначить Савина Кирилла Сергеевича, паспорт серия 94 05 № 624667, выдан Отделом Внутренних дел Ленинского района г. Ижевска. 2005г., код подразделения 182-003, зарегистрирован: Ленинградская область, поселок Мурино, улица Новая, дом 7, квартира 614 Генеральным директором Общества с ограниченной ответственностью «Софт Билдинг» с 05 июня 2018 г.
3. Осуществить государственную регистрацию изменений в сведения об Обществе с ограниченной ответственностью «Софт Билдинг» в Единый государственный реестр юридических лиц, не связанных с внесением изменений в учредительные документы в Инспекции Федеральной налоговой службы №15 по г. Санкт-Петербург.
4. Поручить представление документов и получение листа записи о внесении изменений в сведения об Обществе с ограниченной ответственностью «Софт билдинг» в Единый государственный реестр юридических лиц, не связанных с внесением изменений в учредительные документы в Инспекции Федеральной налоговой службы №15 по г. Санкт-Петербург Генеральному директору Общества Савину Кириллу Сергеевичу.
5. Также с 05 июня 2018 г. снимаю с себя обязанности Главного бухгалтера.

УЧАСТНИК ОБЩЕСТВА: _____ **А.А. Молотов**

Общество с ограниченной ответственностью

«Софт Билдинг»

Г. Санкт-Петербург 05 июня 2018 г.

ПРИКАЗ №4

Я, Савин Кирилл Сергеевич, вступаю в должность Генерального директора с 05 июня 2018 года на основании Решения №1/18 от 28 мая 2018 г.

Генеральный директор  Савин К.С.