ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на передачу неисключительных прав на программное обеспечение в сфере информационной безопасности для федеральных органов исполнительной власти

Перечень сокращений

Сокращения, а также термины, используемые в настоящем документе, и их определения приведены в таблице 1.

Таблица 1

Термин	**Определение**
ПО	Программное обеспечение
ФОИВ	Федеральный орган исполнительной власти
Вендор	Производитель ПО, обладатель исключительных прав на программное обеспечение в сфере информационной безопасности, включенное в единый реестр российских программ для электронных вычислительных машин и баз данных
Заказчик	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Получатель	ФОИВ
Пользователь	Работник ФОИВ, осуществляющий эксплуатацию ПО, неисключительные права на которые передаются
Эшелонированная защита	Под эшелонированной защитой понимается использование антивирусных продуктов разных вендоров на разных видах защищаемой вычислительной техники: АРМ, файловые серверы, почтовые шлюзы, интернет шлюзы
Категория	Признак количества передаваемых неисключительных прав, исходя из предполагаемого срока начала использования. Определяется механизмом сбора потребностей в соответствии с порядком, утвержденным приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 19.12.2018 № 725 «Об утверждении формы и порядка представления потребности, формирования потребности в осуществлении централизованных закупок офисного программного обеспечения и программного обеспечения в сфере информационной безопасности», и может быть «первичное» и «по заявкам».
Лицензия, неисключительная лицензия, неисключительные права	Право использования результата интеллектуальной деятельности или средства индивидуализации с сохранением за лицензиаром права выдачи лицензий другим лицам (простая (неисключительная) лицензия)
Ключ	Код активации для программного продукта. Лицензионный ключ является кодом доступа к использованию программных продуктов.

Раздел I. Спецификация ПО

Таблица 2

СПЕЦИФИКАЦИЯ
программного обеспечения в сфере информационной безопасности для федеральных органов исполнительной власти с указанием пределов прав и способов его использования

№ п/п	Наименование ПО	Основные технические характеристики ПО	Ссылка на нормативный документ, который устанавливает технические требования	Комплектность	Единица измерения	Коли-чество	Срок исполнения	Место исполнения	Период, на который передаются неисключительные права
1	2	3	4	5	6	7	8	9	10
1	Права на использование (неисключительных лицензий) антивирусного программного обеспечения по защите автоматизированного рабочего места (АРМ)	Обеспечение антивирусной защиты автоматизированных рабочих мест согласно пункту 10 Раздела III настоящего технического задания	Постановление Правительства Российской Федерации от 23.03.2017 № 325 «Об утверждении дополнительных требований к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, и внесении изменений в Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных»	Установочный файл + ключ	Комплект	274 881 (согласно разбивке в таблице 3)	В течение 10 (Десяти) рабочих дней с даты заключения Контракта, но не позднее 22 декабря 2019 года.	Адрес: 125039, г. Москва, Пресненская наб., д.10, стр.2, IQ-квартал	Срок действия неисключительных прав (период, на который передаются неисключительные права) – 12 месяцев
2	Права на использование	Обеспечение антивирусной	Постановление Правительства Российской	Установочный файл +	Комплект	32 935 (согласно	В течение 10 (Десяти)	Адрес: 125039, г.	Срок действия неисключительных

№ п/п	Наименование ПО	Основные технические характеристики ПО	Ссылка на нормативный документ, который устанавливает технические требования	Комплектность	Единица измерения	Коли-чество	Срок исполнения	Место исполнения	Период, на который передаются неисключительные права
	(неисключительных лицензий) антивирусного программного обеспечения **по защите серверов**	защиты серверов согласно пункту 11 Раздела III настоящего технического задания	Федерации от 23.03.2017 № 325 «Об утверждении дополнительных требований к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, и внесении изменений в Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных»	ключ		разбивке в таблице 3)	рабочих дней с даты заключения Контракта, но не позднее 22 декабря 2019 года.	Москва, Пресненская наб., д.10, стр.2, IQ-квартал	прав (период использования, на который передаются неисключительные права) – 12 месяцев.
3	Права на использование (неисключительных лицензий) антивирусного программного обеспечения **по защите почтовых шлюзов**	Обеспечение антивирусной защиты почтовых шлюзов согласно пункту 12 Раздела III настоящего технического задания	Постановление Правительства Российской Федерации от 23.03.2017 № 325 «Об утверждении дополнительных требований к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, и внесении изменений в Правила формирования и ведения	Установочный файл + ключ	Комплект	25 276 (согласно разбивке в таблице 3)	В течение 10 (Десяти) рабочих дней с даты заключения Контракта, но не позднее 22 декабря 2019 года.	Адрес: 125039, г. Москва, Пресненская наб., д.10, стр.2, IQ-квартал	Срок действия неисключительных прав (период использования, на который передаются неисключительные права) – 12 месяцев.

№ п/п	Наименование ПО	Основные технические характеристики ПО	Ссылка на нормативный документ, который устанавливает технические требования	Комплектность	Единица измерения	Коли-чество	Срок исполнения	Место исполнения	Период, на который передаются неисключительные права
			единого реестра российских программ для электронных вычислительных машин и баз данных»						
4	Права на использование (неисключительных лицензий) антивирусного программного обеспечения **по защите Интернет шлюзов**	Обеспечение антивирусной защиты Интернет шлюзов согласно пункту 13 Раздела III настоящего технического задания	Постановление Правительства Российской Федерации от 23.03.2017 № 325 «Об утверждении дополнительных требований к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, и внесении изменений в Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных»	Установочный файл + ключ	Комплект	1 055 (согласно разбивке в таблице 3)	В течение 10 (Десяти) рабочих дней с даты заключения Контракта, но не позднее 22 декабря 2019 года.	Адрес: 125039, г. Москва, Пресненская наб., д.10, стр.2, IQ-квартал	Срок действия неисключительных прав (период использования, на который передаются неисключительные права) – 12 месяцев.

Таблица 3

Объем неисключительных прав на программное обеспечение в сфере информационной безопасности для федеральных органов исполнительной власти

№ п/п	ФОИВ	Количество неисключительных прав на антивирусное программное обеспечение по видам защищаемой техники										
		Категория: «Первичное»					Категория: «По заявкам»					Общее количество
		АРМ	Сервер	Почта	Интернет	Итого	АРМ	Сервер	Почта	Интернет	Итого	
		(п. 10 ТЗ)	(п. 11 ТЗ)	(п. 12 ТЗ)	(п. 13 ТЗ)	(3 + 4 + 5 + 6)	(п. 10 ТЗ)	(п. 11 ТЗ)	(п. 12 ТЗ)	(п. 13 ТЗ)	(8 + 9 + 10 + 11)	(7 + 12)
1	2	3	4	5	6	7	8	9	10	11	12	13
1.	Федеральная служба по надзору в сфере здравоохранения	1843	154	-	-	1997	-	-	-	-	-	1997
2.	Федеральное медико-биологическое агентство	940	40	-	-	980	213	57	-	-	270	1250
3.	Министерство культуры Российской Федерации	740	898	-	-	1638	228	79	-	-	307	1945
4.	Министерство науки и высшего образования Российской Федерации	688	219	678	678	2263	396	128	376	376	1276	3539
5.	Федеральная служба по гидрометеорологии и мониторингу окружающей среды	158	-	-	-	158	135	-	-	-	135	293
6.	Федеральное агентство водных ресурсов	865	260	190	1	1316	-	-	-	-	-	1316

№ п/п	ФОИВ	Количество неисключительных прав на антивирусное программное обеспечение по видам защищаемой техники										
		Категория: «Первичное»					Категория: «По заявкам»					Общее количество
		АРМ	Сервер	Почта	Интернет	Итого	АРМ	Сервер	Почта	Интернет	Итого	
		(п. 10 ТЗ)	(п. 11 ТЗ)	(п. 12 ТЗ)	(п. 13 ТЗ)	(3 + 4 + 5 + 6)	(п. 10 ТЗ)	(п. 11 ТЗ)	(п. 12 ТЗ)	(п. 13 ТЗ)	(8 + 9 + 10 + 11)	(7 + 12)
1	2	3	4	5	6	7	8	9	10	11	12	13
7.	Федеральное агентство лесного хозяйства	318	5	-	-	323	655	2	-	-	657	980
8.	Федеральное агентство по недропользованию	853	58	-	-	911	-	-	-	-	-	911
9.	Министерство промышленности и торговли Российской Федерации	1200	69	-	-	1269	-	-	-	-	-	1269
10.	Федеральное агентство по техническому регулированию и метрологии	287	29	3	-	319	-	2	-	-	2	321
11.	Министерство просвещения Российской Федерации	1265	59	-	-	1324	1086	2	-	-	1088	2412
12.	Министерство сельского хозяйства Российской Федерации	900	153	-	-	1053	-	-	-	-	-	1053
13.	Федеральная служба по ветеринарному и фитосанитарному надзору	7478	37	-	-	7515	-	-	-	-	-	7515

№ п/п	ФОИВ	Количество неисключительных прав на антивирусное программное обеспечение по видам защищаемой техники										
		Категория: «Первичное»					Категория: «По заявкам»					Общее количество
		АРМ	Сервер	Почта	Интернет	Итого	АРМ	Сервер	Почта	Интернет	Итого	
		(п. 10 ТЗ)	(п. 11 ТЗ)	(п. 12 ТЗ)	(п. 13 ТЗ)	(3 + 4 + 5 + 6)	(п. 10 ТЗ)	(п. 11 ТЗ)	(п. 12 ТЗ)	(п. 13 ТЗ)	(8 + 9 + 10 + 11)	(7 + 12)
1	2	3	4	5	6	7	8	9	10	11	12	13
14.	Федеральное агентство по рыболовству	-	-	-	-	-	1852	23	1	-	1876	1876
15.	Министерство спорта Российской Федерации	367	30	360	-	757	-	-	-	-	-	757
16.	Министерство строительства и жилищно-коммунального хозяйства Российской Федерации	60	30	450	-	540	-	-	-	-	-	540
17.	Министерство транспорта Российской Федерации	695	-	800	-	1495	-	-	-	-	-	1495
18.	Федеральная служба по надзору в сфере транспорта	2801	54	-	-	2855	96	-	-	-	96	2951
19.	Федеральное агентство воздушного транспорта	1592	62	600	-	2254	-	-	-	-	-	2254
20.	Федеральное дорожное агентство	230	142	-	-	372	-	-	-	-	-	372
21.	Федеральное агентство железнодорожного транспорта	-	-	-		-	366	40	-	-	406	406

№ п/п	ФОИВ	Количество неисключительных прав на антивирусное программное обеспечение по видам защищаемой техники										
		Категория: «Первичное»					Категория: «По заявкам»					Общее количество
		АРМ	Сервер	Почта	Интернет	Итого	АРМ	Сервер	Почта	Интернет	Итого	
		(п. 10 ТЗ)	(п. 11 ТЗ)	(п. 12 ТЗ)	(п. 13 ТЗ)	(3 + 4 + 5 + 6)	(п. 10 ТЗ)	(п. 11 ТЗ)	(п. 12 ТЗ)	(п. 13 ТЗ)	(8 + 9 + 10 + 11)	(7 + 12)
1	2	3	4	5	6	7	8	9	10	11	12	13
22.	Федеральное агентство морского и речного транспорта	300	15	-	-	315	-	-	-	-	-	315
23.	Министерство труда и социальной защиты Российской Федерации	522	78	-	-	600	110	-	-	-	110	710
24.	Федеральная служба по труду и занятости	2977	-	-	-	2977	-	-	-	-	-	2977
25.	Федеральная налоговая служба	-	-	-	-	-	144772	2928	-	-	147700	147700
26.	Федеральная служба по регулированию алкогольного рынка	1292	55	1000	-	2347	-	-	-	-	-	2347
27.	Федеральная таможенная служба	38500	25000	-	-	63500	4977	-	-	-	4977	68477
28.	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций	3505	-	-	-	3505	-	-	-	-	-	3505

№ п/п	ФОИВ	Количество неисключительных прав на антивирусное программное обеспечение по видам защищаемой техники										
		Категория: «Первичное»					Категория: «По заявкам»					Общее количество
		АРМ	Сервер	Почта	Интернет	Итого	АРМ	Сервер	Почта	Интернет	Итого	
		(п. 10 ТЗ)	(п. 11 ТЗ)	(п. 12 ТЗ)	(п. 13 ТЗ)	(3 + 4 + 5 + 6)	(п. 10 ТЗ)	(п. 11 ТЗ)	(п. 12 ТЗ)	(п. 13 ТЗ)	(8 + 9 + 10 + 11)	(7 + 12)
1	2	3	4	5	6	7	8	9	10	11	12	13
29.	Федеральное агентство по печати и массовым коммуникациям	210	17	-	-	227	-	-	-	-	-	227
30.	Федеральное агентство связи	140	20	-	-	160	-	-	-	-	-	160
31.	Федеральная служба по аккредитации	270	150	-	-	420	-	-	-	-	-	420
32.	Федеральная служба государственной статистики	20000	-	20000	-	40000	3 738	-	-	-	3738	43738
33.	Федеральная служба по интеллектуальной собственности	104	4	-	-	108	-	-	-	-	-	108
34.	Федеральное агентство по туризму	90	-	-	-	90	30	-	-	-	30	120
35.	Федеральное агентство по управлению государственным имуществом	3232	1038	-	-	4270	-	-	-	-	-	4270
36.	Министерство энергетики Российской Федерации	816	96	816	-	1728	-	-	-	-	-	1728

№ п/п	ФОИВ	Количество неисключительных прав на антивирусное программное обеспечение по видам защищаемой техники										
		Категория: «Первичное»					Категория: «По заявкам»					Общее количество
		АРМ	Сервер	Почта	Интернет	Итого	АРМ	Сервер	Почта	Интернет	Итого	
		(п. 10 ТЗ)	(п. 11 ТЗ)	(п. 12 ТЗ)	(п. 13 ТЗ)	(3 + 4 + 5 + 6)	(п. 10 ТЗ)	(п. 11 ТЗ)	(п. 12 ТЗ)	(п. 13 ТЗ)	(8 + 9 + 10 + 11)	(7 + 12)
1	2	3	4	5	6	7	8	9	10	11	12	13
37.	Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека	-	-	-	-	-	15306	-	-	-	15306	15306
38.	Федеральная служба по надзору в сфере образования и науки	4365	196	-	-	4561	-	-	-	-	-	4561
39.	Федеральная служба по экологическому, технологическому и атомному надзору	-	597	2	-	599	-	30	-	-	30	629
40.	Федеральное агентство по государственным резервам	1198	64	-	-	1262	-	-	-	-	-	1262
41.	Федеральное агентство по делам молодежи	120	7	-	-	127	-	8	-	-	8	135
	ИТОГО:	**100921**	**29636**	**24899**	**679**	**156135**	**173960**	**3299**	**377**	**376**	**178012**	**334147**

Раздел II. Общие положения

2. Общее описание закупаемого программного обеспечения

Наименование программного обеспечения: неисключительные права на программное обеспечение (ПО) в сфере информационной безопасности (далее – неисключительные права); неисключительные права передаются для использования на территории всего мира.

Срок действия неисключительных прав (период использования, на который передаются неисключительные права) – 12 месяцев:

– для неисключительных прав с категорией «первичные» – начинается не позднее 10 (Десяти) рабочих дней с даты подписания акта приема-передачи неисключительных прав;

– для неисключительных прав с категорией «по заявкам» — начинается не позднее 01.01.2020.

2.1. Закупка осуществляется в рамках исполнения постановления Правительства Российской Федерации от 08.06.2018 № 658 «О централизованных закупках офисного программного обеспечения, программного обеспечения для ведения бюджетного учета, а также программного обеспечения в сфере информационной безопасности».

2.2. К разрешенным способам использования ПО относятся:

для Заказчика – право осуществлять действия, необходимые для функционирования ПО, включая воспроизведение, инсталляцию, и запуск ПО, хранение ПО в памяти ЭВМ и/или серверов, резервное копирование, активация ПО, обновление и использование актуальных версий ПО, с возможностью последующей передачи права на использование программного обеспечения в сфере информационной безопасности федеральным органам исполнительной власти;

для Получателей, пользователей – осуществление действий, необходимых для функционирования ПО, включая воспроизведение, инсталляцию, и запуск ПО; хранение ПО в памяти ЭВМ и (или) серверов; резервное копирование; активация ПО; обновление и использование актуальных версий ПО.

3. Цели осуществления закупки

Целью закупки является централизованное обеспечение Получателей, пользователей правами пользования программным обеспечением антивирусной защиты.

4. Организация распространения средств антивирусной защиты

4.1 Исполнитель должен:

– предоставить неисключительные права (лицензии) на программные средства антивирусной защиты;

– обеспечить возможность использования Заказчиком, Получателями, пользователями самой последней актуальной версии программного продукта;

– обеспечить передачу прав на использование программного продукта в пределах, предусмотренных Спецификацией ПО (таблица 2 данного Технического задания), включенного в единый реестр российских программ для электронных вычислительных машин и баз данных и соответствующего настоящему Техническому заданию (при этом рекомендуется использовать **продукты разных вендоров для каждого вида защищаемой вычислительной техники** (эшелонированная защита));

– обеспечить получение Заказчиком доступа к средствам загрузки актуальных версий продуктов путем предоставления доступа для скачивания установочных файлов и с ресурса (сайта) в информационно-коммуникационной сети «Интернет» в течение 10 (Десяти) рабочих дней с даты заключения Контракта, но не позднее 22 декабря 2019 года;

– обеспечить передачу Заказчику обновленных версий программного обеспечения в период действия неисключительных лицензий путем предоставления доступа для скачивания установочных файлов обновленных версий продуктов с ресурса (сайта) в информационно-коммуникационной сети «Интернет» в течение 10 (десяти) рабочих дней после их выхода.

Предоставление прав пользования программными средствами антивирусной защиты осуществляется в объемах, указанных в таблице 3 данного Технического задания, путем передачи Заказчику данных для скачивания установочных файлов и ключей посредством электронной

почты либо путем предоставления доступа для скачивания установочных файлов и лицензионных ключей с ресурса (сайта) в сети «Интернет».

5. Общие требования к средствам антивирусной защиты

5.1. Предлагаемые к использованию программные средства антивирусной защиты должны входить в Единый реестр российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. Устанавливается запрет на допуск программных средств антивирусной защиты, происходящих из иностранных государств, в соответствии с постановлением Правительства от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

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

5.3. Программные средства антивирусной защиты должны иметь возможность установки как в режиме независимой (изолированной) установки на компьютеры, так и в режиме взаимодействия с программными средствами централизованного управления, мониторинга и обновления.

5.4. Программные средства должны иметь функцию автоматического запуска при запуске операционной системы.

6. Требования к программным средствам централизованного управления, мониторинга и обновления

6.1. Средства антивирусной защиты для программных средств централизованного управления, мониторинга и обновления должны быть сертифицированы уполномоченным органом (ФСТЭК России) в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20.03.2012 № 28, по типу А не ниже четвертого класса защиты.

6.2. Программные средства централизованного управления, мониторинга и обновления должны функционировать под управлением как минимум следующих операционных систем:

- Microsoft Windows Server 2008 SP1;
- Microsoft Windows Server 2012;
- Microsoft Windows 7.

6.3. Средства должны иметь функции создания иерархии серверов администрирования с возможностью иметь несколько подчиненных серверов администрирования.

6.4. Средства должны иметь функции распространения ключей активации лицензии (или иного механизма активации) на клиентские устройства и хранения информации о ключах.

6.5. Средства должны функционировать как минимум со следующими типами СУБД: SQL Server, MySQL.

6.6. Средства должны иметь возможность экспортировать отчеты как минимум в следующих форматах: HTML, PDF.

7. Требования к техподдержке и обновлению антивирусных баз

7.1. Техническая поддержка предоставляется в объеме стандартной поддержки, входящей в состав поставляемой в рамках Контракта простой (неисключительной) лицензии производителя программного обеспечения в течение срока действия неисключительных прав (лицензий).

7.2. Регламентное обновление антивирусных баз не реже 1 раза в течение календарных суток.

7.3. Обновляемые антивирусные базы данных должны поддерживать множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации.

7.4. Проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

7.5. В состав прав на использование простых (неисключительных) лицензий программного обеспечения в сфере информационной безопасности должны быть включены права

на все обновления программного обеспечения до актуальной версии ПО, выходящие в период действия лицензии.

8. Требования к эксплуатационной документации

8.1. Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы на русском языке, в том числе: руководство пользователя (администратора).

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

9. Дополнительные требования.

9.1. Средства антивирусной защиты должны быть сертифицированы уполномоченным органом (ФСТЭК России) в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК России от 20.03.2012 № 28 не ниже четвертого класса защиты.

Раздел III. Требования к программному обеспечению антивирусной защиты по видам защищаемой вычислительной техники

10. Программное обеспечение антивирусной защиты для рабочих станций (АРМ)

10.1. Требования к программным средствам антивирусной защиты для рабочих станций **Windows**.

10.1.1. Средства антивирусной защиты для рабочих станций Windows должны быть сертифицированы уполномоченным органом (ФСТЭК России) в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК России от 20 марта 2012 г. № 28, по типам «В» и «Г» не ниже четвертого класса защиты. Для рабочих станций Windows, предназначенных для хранения и обработки сведений, составляющих государственную тайну, должны быть предложены средства антивирусной защиты, сертифицированные ФСБ России в соответствии с требованиями к средствам антивирусной защиты, применяемым в государственных информационных системах, в том числе для защиты информации, содержащей сведения, составляющие государственную тайну.

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

- Microsoft Windows 7;
- Microsoft Windows 8;
- Microsoft Windows 8.1;
- Microsoft Windows 10.

10.1.3. Средства должны реализовывать, в том числе следующие функциональные возможности:

– возможность выполнять проверки с целью обнаружения зараженных объектов в файлах, (включая исполняемые), упакованных различными средствами архивации, в оперативной памяти, в файловых и системных областях носителей информации;

– возможность блокирования доступа и/или удаления (если возможно) кода вредоносных программ из оперативной памяти, удаления вредоносных или подозрительных файлов, возможность 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;

– 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;

– осуществление контроля работы пользователя с веб-ресурсами (разрешение или запрещение доступа).

10.1.4. Средства должны поддерживать различные пути установки:

– локальная установка (в интерактивном и тихом режиме);

– удаленная установка (с использованием сервера администрирования/сервера управления средства и редактором управления групповыми политиками Microsoft Windows).

10.2. Требования к программным средствам антивирусной защиты для рабочих станций **Linux.**

10.2.1. Средства антивирусной защиты для рабочих станций Linux должны быть сертифицированы уполномоченным органом (ФСТЭК России) в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК России от 20.03.2012 № 28, по типам «В» и «Г» не ниже четвертого класса защиты. Для рабочих станций Linux, предназначенных для хранения и обработки сведений, составляющих государственную тайну, должны быть предложены средства антивирусной защиты, сертифицированные ФСБ России в соответствии с требованиями к средствам антивирусной защиты, применяемым в государственных информационных системах, в том числе для защиты информации, содержащей сведения, составляющие государственную тайну.

10.2.2. Программное обеспечение антивирусной защиты для рабочих станций Linux должно функционировать на компьютерах, работающих под управлением как минимум следующих операционных систем следующих версий:

– Red Hat Enterprise Linux;
– CentOS;
– Debian GNU/Linux;
– Альт Линукс;
– Astra Linux.

10.2.3. Средства должны реализовывать, в том числе следующие функциональные возможности:

– обнаруживать и удалять различные типы вредоносных программ при помощи сигнатурного анализа: компьютерные вирусы, сетевые черви, троянские программы, рекламные программы и прочие вредоносные программы;

– обнаруживать и удалять вредоносные программы в архивах;

– обнаруживать ранее неизвестные вредоносные программы при помощи эвристического анализатора;

– осуществлять защиту в режиме реального времени и осуществлять проверку файлов при обращении к ним (включая SAMBA);

– проводить проверку по требованию и/или по расписанию и/или сразу после загрузки операционной системы с возможностью помещать подозрительные объекты в карантин;

– сохранять копии зараженного объекта в отдельном хранилище перед лечением и удалением в целях возможного восстановления объекта;

– возможность управления через пользовательский графический интерфейс.

11. Программное обеспечение антивирусной защиты для файловых серверов

11.1. Требования к программным средствам антивирусной защиты для файловых серверов **Windows**

11.1.1. Средства антивирусной защиты для файловых серверов Windows должны быть сертифицированы уполномоченным органом (ФСТЭК России) в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК России от 20.03.2012 № 28, по типам «Б» не ниже четвертого класса защиты. Для файловых серверов Windows, предназначенных для хранения и обработки сведений, составляющих государственную тайну, должны быть предложены средства антивирусной защиты, сертифицированные ФСБ России в соответствии с требованиями к средствам антивирусной защиты, применяемым в государственных информационных системах, в том числе для защиты информации, содержащей сведения, составляющие государственную тайну.

11.1.2. Средства антивирусной защиты для файловых серверов MS Windows должны функционировать на компьютерах, работающих под управлением как минимум следующих операционных систем:

– Microsoft Windows Server 2008;
– Microsoft Windows Server 2012;
– Microsoft Windows Server 2016.

11.1.3. Средства должны реализовывать, в том числе следующие функциональные возможности:

– выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами по команде и(или) в режиме динамического обнаружения в процессе доступа;

– включать и выключать компоненты защиты независимо друг от друга;

– настраивать параметры работы отдельных компонентов защиты;

– поиск, обнаружение и обезвреживание угроз в файлах, загрузочных секторах и оперативной памяти защищаемого устройства;

– периодически выполнять проверку сервера на присутствие вирусов и других программ, представляющих угрозу;

– наличие настраиваемого модуля превентивной защиты, позволяющего обеспечивать защиту как минимум следующих объектов: низкоуровневый доступ к диску, загрузку драйверов, критических областей Windows (в том числе файла hosts);

– наличие самозащиты объектов средства, в том числе критических файлов, процессов, окон, ключей от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусного средства;

– осуществление антивирусной проверки на серверах, выполняющих разные функции: Серверов терминалов и принт-серверов; Серверов приложений и контроллеров доменов; Файловых серверов;

– проверка следующих объектов защищаемого сервера при доступе к ним: Файлов при их записи и считывании; Альтернативных потоков файловых систем (NTFS-streams); Главной загрузочной записи и загрузочных секторов локальных жестких дисков и съемных носителей;

– непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting) или эквивалентным. Проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными;

– проверка по требованию, заключающаяся в однократной полной или выборочной проверке на наличие угроз объектов на сервере;

– помещение подозрительных и поврежденных объектов на карантин. Возможность восстановления файлов из карантина;

– балансировка загрузки путем регулирования распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: антивирусная проверка может продолжаться в фоновом режиме;

– выбор доверенных процессов путем исключения из проверки безопасных процессов, работа которых может замедляться при антивирусной проверке (процесс резервного копирования данных, программы дефрагментации жесткого диска и другие);

– централизованно управляться с помощью единой системы управления.

11.1.4. Средства должны поддерживать различные пути установки:

– локальная установка (в интерактивном и тихом режиме);

– удаленная установка (с использованием сервера администрирования/сервера управления системы и редактором управления групповыми политиками Microsoft Windows).

11.2. Требования к программным средствам антивирусной защиты для файловых серверов **Linux**.

11.2.1. Средства антивирусной защиты для файловых серверов Linux должны быть сертифицированы уполномоченным органом (ФСТЭК России) в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК России от 20.03.2012 № 28, по

типу «Б» не ниже четвертого класса защиты. Для файловых серверов Linux, предназначенных для хранения и обработки сведений, составляющих государственную тайну, должны быть предложены средства антивирусной защиты, сертифицированные ФСБ России в соответствии с требованиями к средствам антивирусной защиты, применяемым в государственных информационных системах, в том числе для защиты информации, содержащей сведения, составляющие государственную тайну.

11.2.2. Средства антивирусной защиты для файловых серверов Linux должно функционировать на компьютерах, работающих под управлением как минимум следующих операционных систем:

- Debian GNU/Linux;
- Red Hat Enterprise Linux;
- CentOS;
- Astra Linux;
- Альт Линукс;
- Ubuntu.

11.2.3. Средства должны реализовывать, в том числе следующие функциональные возможности:

– обнаруживать и удалять различные типы вредоносных программ при помощи сигнатурного анализа: компьютерные вирусы, сетевые черви, троянские программы и прочие вредоносные программы;

– обнаруживать ранее неизвестные вредоносные программы при помощи эвристического анализатора;

– осуществлять защиту в режиме реального времени и осуществлять проверку файлов при обращении к ним;

– проводить проверку по требованию и (или) по расписанию и (или) сразу после загрузки операционной системы с возможностью помещать подозрительные объекты в карантин;

– мониторинг обращений к файлам: в файловой системе, в разделяемых каталогах Samba (или эквивалент);

– изоляция инфицированных и (или) подозрительных объектов в специальном хранилище (карантине) для предохранения операционной системы от возможного ущерба;

– локальный сбор статистики по результатам проверок и инцидентам, ведение журнала угроз.

12. Программное обеспечение антивирусной защиты для почтовых шлюзов

12.1. Средства антивирусной защиты для почтовых шлюзов должны быть сертифицированы уполномоченным органом (ФСТЭК России) в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК России от 20.03.2012 № 28, по типу «Б» не ниже четвертого класса защиты.

12.2. Средства антивирусной защиты для почтовых шлюзов должны функционировать как минимум на следующих платформах:

– средства для почтовых серверов на базе Microsoft Exchange: ОС Microsoft Windows Server 2008/2012/2016;

– средства для почтовых серверов на базе ОС Linux: Red Hat Enterprise Linux, CentOS, Ubuntu Server, Debian GNU / Linux, FreeBSD, Astra Linux SE, Alt Linux.

12.3. Средства должны функционировать совместно с почтовыми системами следующих типов:

– средства для почтовых серверов на базе Microsoft Exchange: Exchange Server 2010/2013/2016;

– средства для почтовых серверов на базе ОС Linux: Exim/Postfix/Sendmail/Qmail.

12.4. Средства для почтовых серверов Microsoft Exchange должны реализовывать, в том числе следующие функциональные возможности:

- совместимость с DAG в Microsoft Exchange;
- поддержка ролей MS Exchange 2010: Edge, Hub transport, Mailbox;

– поддержка ролей MS Exchange 2013: Mailbox, Edge Transport, Client Access Server (CAS);

– поддержка ролей MS Exchange 2016: Mailbox, Edge Transport;

– возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;

– 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, а также хранящихся на сервере Microsoft Exchange (в том числе в общих папках) сообщениях, включая вложения;

– 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;

– возможность обновления антивирусных баз, как с сайтов производителя, так и с внутренних сетевых ресурсов организации;

– интеграция с Active Directory.

12.5. Средства для почтовых серверов на базе ОС Linux должны реализовывать, в том числе следующие функциональные возможности:

– возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;

– 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;

– возможность удаления (если удаление технически возможно) файлов, в которых обнаружены вредоносные составляющие, а также подозрительных файлов, перемещение и изолирование объектов воздействия;

– контентная фильтрация почтовых сообщений по имени, типу и размеру вложений;

– интеграция со службами каталога Active Directory;

– использование регулярных выражений при создании правил фильтрации;

– возможность создания черного и белого списков;

– управление всеми функциями с помощью веб-интерфейса.

13. Программное обеспечение антивирусной защиты для Интернет шлюзов

13.1. Средства антивирусной защиты для Интернет шлюзов должны быть сертифицированы уполномоченным органом (ФСТЭК России) в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК России от 20.03.2012 № 28, по типу «Б» не ниже четвертого класса защиты.

13.2. Средства антивирусной защиты для сетевых шлюзов должны функционировать как минимум на следующих операционных системах:

– Debian GNU/Linux;

– RedHat Enterprise Linux;

– Ubuntu;

– CentOS;

– Альт Линукс.

13.3. Средства должны реализовывать, в том числе следующие функциональные возможности:

– обеспечивать защиту интернет-трафика, поступающего по протоколам HTTP/FTP;

– определение в проверяемых объектах вредоносных программ всех типов;

– выбор типа проверки (проверять все файлы, или по заданному списку масок);

– фильтрации проверяемого трафика по MIME-типам;

– фильтрации проверяемого трафика по размеру файлов;

– проверку всех передаваемых по защищаемым протоколам объектов до момента передачи

пользователю;

– фильтрацию проверяемого трафика по ip-адресам или именам ресурсов, в том числе с помощью масок и регулярных выражений имен ресурсов;

– регистрации времени события, объекта проверки и типа воздействия для реализации возможности проведения внутренних расследований;

– интеграции с прокси-серверами по протоколу ICAP;

– ограничения времени проверки, в том числе времени проверки отдельного файла;

– получения статистической информации как минимум в формате HTML;

– получения статистической информации как по одному серверу системы антивирусной защиты, так и суммарно по всем серверам;

– задание индивидуальных настроек правил фильтрации с помощью логических выражений для групп пользователей (ограничения доступа к ресурсам по требованию, в том числе ограничения по ip-адресам, сетям (подсетям), пользователям и группам);

– определять необходимый уровень анализа, в том числе путем отключения эвристического анализа, ограничения размера файла и глубины проверки;

– получать уведомления о сроке действия лицензии и необходимости ее обновления;

– управление программой должно осуществляться как непосредственно через конфигурационные файлы, так и через веб-интерфейс. Система управления должна поддерживать возможность настройки всех параметров антивирусной проверки трафика;

– антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, средство должно обеспечивать возможность простого и гибкого изменения настроек администраторами и пользователями в рамках имеющихся у них прав.