АО «Лаборатория Касперского»

УТВЕРЖДЕН
643.46856491.01-2021-ЛУ

Программное изделие

KASPERSKY ENDPOINT SECURITY 11 ДЛЯ LINUX

Формуляр

643.46856491.00049-09 30 01

Листов 18

2021

Литера

Инв. N подл.	Подп. и дата	Взам. инв. N	Инв. N дубл.	Подп. и дата

СОДЕРЖАНИЕ

1. ОБЩИЕ УКАЗАНИЯ

1.1. Настоящий формуляр удостоверяет комплектность, гарантированное изготовителем качество программного изделия и содержит указания по его эксплуатации.

1.2. Программное изделие может поставляться в виде физического медиапака (физическая поставка) либо в электронном виде по сетям передачи данных (электронная поставка).

1.3. Перед эксплуатацией необходимо ознакомиться с документацией к программному изделию, перечисленной в разделе «Комплектность».

1.4. При электронной поставке программного изделия лицо, ответственное за эксплуатацию программного изделия, распечатывает твердую копию формуляра и производит необходимые записи в разделах.

1.5. Формуляр должен находиться в подразделении, ответственном за эксплуатацию программного изделия.

1.6. Все записи в формуляре производят только чернилами, отчетливо и аккуратно. Подчистки, помарки и незаверенные исправления не допускаются.

2. ОБЩИЕ СВЕДЕНИЯ

2.1. Сведения о программном изделии:

Наименование: «Kaspersky Endpoint Security 11 для Linux»

Версия: 11.1.0.3013

Обозначение: 643.46856491.00049-09

Дата изготовления (заполняется при физической поставке): 3 июня 2021 г.

Наименование изготовителя: АО «Лаборатория Касперского»

Адрес: 125212, г. Москва, Ленинградское ш., 39А, стр. 2, тел. (495) 797-8700.

Серийный номер (заполняется при физической поставке): **СМП8067-51112**

Тип носителя (при физической поставке): лазерный диск.

2.2. Сведения о применимом сертификате соответствия:

Наименование и номер сертификата	Срок начала действия	Срок окончания действия	Идентификатор
Сертификат соответствия № 2534, выдан ФСТЭК России	27.12.2011 г.	27.12.2025 г. .	РОСС RU.01.2534.000766

2.3. Программное изделие является средством антивирусной защиты и предназначено для защиты от вредоносных компьютерных программ, в том числе в системах обработки данных и государственных информационных системах.

2.4. В соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, введенными в действие приказом ФСТЭК России № 17 от 11 февраля 2013 г., и Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, введенными в действие приказом ФСТЭК России № 21 от 18 февраля 2013 г., программное изделие может использоваться в информационных системах 1 и 2 класса защищенности и для обеспечения защищенности персональных данных до 1 уровня включительно.

3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1. Контрольные суммы файлов инсталляционного комплекта программного изделия приведены в настоящем формуляре в таблице 1.

3.2. Контрольные суммы исполняемых файлов программного изделия после установки приведены в Приложении 1 к настоящему формуляру.

Таблица 1 – Контрольные суммы файлов инсталляционного комплекта программного изделия

№ пп	Имя файла	Длина, байт	КС
Каталог D:\kesl			
1	kesl-11.1.0-3013.cert.i386.rpm	102127094	5de7ffd46cabb380a54713fd1bdcbb982576292fa1ae34fc0a6dc835d05f7db5
2	kesl-11.1.0-3013.cert.x86_64.rpm	98009213	72abb86831e90d416018155b094a927b0e11b2b01aab61c40c731f9efb8e08bb
3	kesl-astra_11.1.0-3013_amd64.deb	59419444	214791832f73269d1f315f4f8b9e37ca532e0e7af06679d0d64f1332cc1e7676
4	kesl_11.1.0-3013.cert_amd64.deb	59440162	d459fdeee0b487ad51bb7f65b33bc296bac2d563e4a345c850e10d67a46ce3f2
5	kesl_11.1.0-3013.cert_i386.deb	61696280	b4cf33f2ce151cffd8dfe4e50889f4e3d3c8da6ef99db6b3a23ecabcee09ef53
итого: файлов - 5		**380692193**	**6e9d18235c90030e530ac26922ba285c11439ae8565ddf93228e0342adaa0fd9**
Каталог D:\klnagent			
6	klnagent-11.0.1-19.i386.rpm	11880300	9950f93eecc181b031d4fa17274ae45d5189d771f42e81f3eb74461b6e4ba033
7	klnagent64-11.0.0-38.x86_64.rpm	11040330	497fc76974ff723463298d546ac589cd5eb2a1f82259afee2e79e6c74d439269
8	klnagent64-astra_11.0.0-38_amd64.deb	8013244	477a7314b74552293adfa1cd01de8b06c3d2f30847571540e24399a5fcfa22b6
9	klnagent64_11.0.0-38_amd64.deb	8008204	9a6a80fcba37b4f01412dac3587477eae8ef5a70a434584101b48cba86edf1e8
10	klnagent_11.0.1-19_i386.deb	8670064	81f9c92be9ca9a4a36a275404066dd8f7f7eb61029d4462f21ff00f6f5db52b7
итого: файлов - 5		**47612142**	**8cc604947c868f174a92790d54434cf35b7869e11cc025330705b535acc4b3b3**
Каталог D:\remote install			
11	kesl-11.1.0.3013.zip	494830	0a88bbd2ddc8b6ccaadfe097091683ad8a253772eac098ec4ba56ab7a25149ce
12	kesl-astra-11.1.0.3013.zip	494836	7fe858482f1b24efac6643d16a2724437e2290caa08190b46dc0a9049aa2274f
13	klnagent-11.0.1-19.i386.rpm.tgz	1559	46bb1041876fbef17f1bb32516d255827a08e79aec91da7ea2023a591836ad67
14	klnagent-amd64-deb.tgz	2718	8173f2f9e78b23cb09137b1bb29d1b95f9ce4576ad4ee2c8ddc5186076274b0c
15	klnagent-astra-amd64-deb.tgz	2729	666e21b91e6a4c4718dfacae90b5fbc7d94d79479d3112270e174f983ea1a848
16	klnagent-x86_64-rpm.tgz	2721	ecd11398f5c18738c3efa7541f44e11c16d735f586f144a7d6f77c94530014c6
17	klnagent_11.0.1-19_i386.deb.tgz	1556	3be5d21baed6eeb324a5bbf2a3dcf0fedf121de18587a7842bf8b7419f9feea7
итого: файлов - 7		**1000949**	**03f2e118d74a2ad58f24db70eb5303dc6749540795d9c1eaaaba65c7a4dcdac3**
Каталог D:\SCPlugin			
18	klcfginst.msi	11902976	2a540e30d4e91f2b6b3cdd1a44309ae1734de009c183e2456d76633844b7ce52
итого: файлов - 1		**11902976**	**2a540e30d4e91f2b6b3cdd1a44309ae1734de009c183e2456d76633844b7ce52**
ВСЕГО: файлов - 18		**441208260**	**cbfdf39f23b5b9e7fd80bd0ed99afd925e3f47071ec7d90fe247b088e105a8fb**
Конец			

Контрольные суммы рассчитаны с использованием средства фиксации исходного состояния программного комплекса «ФИКС» версии 2.0.2 (сертификат ФСТЭК России № 1548, техническая поддержка до 15.01.2025 г., лицензия № ЦС 50 – 7400 Л629640, знак соответствия № Л629640) по алгоритму «ГОСТ-34.11-94, программно».

4. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

4.1. В программном изделии реализованы следующие функции безопасности:

4.1.1. разграничение доступа к управлению САВЗ:
- а) поддержку определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности и администраторами серверов или пользователями ИС;

4.1.2. управление работой САВЗ:
- а) возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности САВЗ;

4.1.3. управление параметрами САВЗ:
- а) возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности САВЗ;

4.1.4. управление установкой обновлений (актуализации) БД ПКВ САВЗ:
- а) получение и установку обновлений БД ПКВ без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса; без применения средств автоматизации;

4.1.5. аудит безопасности САВЗ:
- а) генерацию записи аудита для событий, подвергаемых аудиту;
- б) чтение информации из записей аудита;
- в) ассоциацию событий аудита с идентификаторами субъектов;
- г) ограничение доступа к чтению записей аудита;
- д) поиск, сортировку, упорядочение данных аудита;

4.1.6. выполнение проверок объектов воздействия:
- а) выполнение проверок с целью обнаружения зараженных КВ объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации, в Docker-контейнерах;
- б) выполнение проверок с целью обнаружения зараженных КВ объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
- в) выполнение проверок с целью обнаружения зараженных КВ объектов по команде; в режиме динамического обнаружения в процессе выполнения операций доступа к объектам; путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
- г) выполнение проверок с целью обнаружения зараженных КВ объектов сигнатурными и эвристическими методами;

4.1.7. обработка объектов воздействия:
- а) удаление (если удаление технически возможно) кода КВ из оперативной памяти, удаления файлов, в которых обнаружены КВ, а также файлов, подозрительных на наличие КВ, возможность перемещения и изолирования зараженных объектов, удаления кода КВ из файлов и системных областей носителей информации;
- б) блокирование доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных КВ;
- в) предоставление возможности блокирования сервера, на котором обнаружены зараженные файлы или блокирование АРМ, на котором обнаружены зараженные файлы;
- г) восстановление функциональных свойств зараженных объектов;

4.1.8. сигнализация САВЗ:
отображение сигнала тревоги об обнаружении КВ.

4.1.9. контроль целостности компонентов ОО:
- а) контроль целостности компонентов ОО.

Примечание — Функциональные возможности соответствуют следующим мерам защиты информации в информационных системах, согласно приказу №17 ФСТЭК России, и меры по обеспечению безопасности персональных данных, согласно приказу №21 ФСТЭК России: АВЗ.1 — Реализация антивирусной защиты; АВЗ.2 — Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

5. КОМПЛЕКТНОСТЬ

5.1. Сведения по комплектности при физической поставке представлены в таблице 2.

Таблица 2 – Сведения по комплектности программного изделия при физической поставке

Наименование изделия (составной части, документа)	Обозначение конструкторского документа	Кол-во	Порядковый учетный номер	Примечание
1. Kaspersky Endpoint Security 11 для Linux. Инсталляционный комплект	643.46856491.00049-09	1		На лазерном диске
2. Kaspersky Endpoint Security 11 для Linux. Формуляр	643.46856491.00049-09 30 01	1		В печатном виде
3. Kaspersky Endpoint Security 11 для Linux. Приложение 1 к формуляру	643.46856491.00049-09 30 02	1		На лазерном диске
4. Kaspersky Endpoint Security 11 для Linux. Подготовительные процедуры и руководство по эксплуатации	643.46856491.00049-09 90 01	1		На лазерном диске
5. Упаковка		1		
6. Заверенная копия выданного ФСТЭК России сертификата соответствия Системы сертификации средств защиты информации по требованиям безопасности информации		1		В печатном виде

5.2. Сведения по комплектности при электронной поставке представлены в таблице 3.

Таблица 3 – Сведения по комплектности программного изделия при электронной поставке

Наименование изделия (составной части, документа)	Обозначение конструкторского документа	Кол-во	Порядковый учетный номер	Примечание
1. Kaspersky Endpoint Security 11 для Linux. Инсталляционный комплект	643.46856491.00049-09	1		В электронном виде
2. Kaspersky Endpoint Security 11 для Linux. Формуляр	643.46856491.00049-09 30 01	1		В электронном виде
3. Kaspersky Endpoint Security 11 для Linux. Приложение 1 к формуляру	643.46856491.00049-09 30 02	1		В электронном виде
4. Kaspersky Endpoint Security 11 для Linux. Подготовительные процедуры и руководство по эксплуатации	643.46856491.00049-09 90 01	1		В электронном виде
5. Копия выданного ФСТЭК России сертификата соответствия Системы сертификации средств защиты информации по требованиям безопасности информации		1		В электронном виде

6. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

6.1. Программное изделие должно функционировать на компьютерах, имеющих следующие конфигурации вычислительной среды.

6.1.1. Минимальные общие требования:

- процессор Core™ 2 Duo 1.86 ГГц;
- 1 ГБ оперативной памяти для 32-битных операционных систем;
- 2 ГБ оперативной памяти для 64-битных операционных систем;
- раздел подкачки не менее 1 ГБ;
- 1 ГБ свободного места на жестком диске

6.1.2. Поддерживаемые 32-битные операционные системы:

- Ubuntu 16.04 LTS, 16.04.1 LTS, 16.04.2 LTS, 16.04.3 LTS, 16.04.4 LTS, 16.04.5 LTS, 16.04.6 LTS;
- Red Hat® Enterprise Linux® 6.7, 6.8, 6.9, 6.10;
- CentOS 6.7, 6.8, 6.9, 6.10;
- Debian GNU / Linux 9.4, 9.5, 9.6, 9.7, 9.8, 9.9, 9.10, 9.11, 9.12;

- Debian GNU / Linux 10.1, 10.2, 10.3;
- Linux Mint 18.2, 18.3;
- Linux Mint 19, 19.1, 19.2, 19.3;
- Альт 8 СП Рабочая Станция;
- Альт 8 СП Сервер;
- Альт Рабочая Станция 8;
- Альт Рабочая Станция К 8;
- Альт Рабочая Станция 9;
- Альт Сервер 8;
- Альт Сервер 9;
- Альт Образование 8;
- Альт Образование 9;
- Гослинукс 6.6;
- Операционная система Лотос (редакция для серверов и рабочих станций);
- Mageia 4.

6.1.3. Поддерживаемые 64-битные операционные системы:

- Ubuntu 16.04 LTS, 16.04.1 LTS, 16.04.2 LTS, 16.04.3 LTS, 16.04.4 LTS, 16.04.5 LTS, 16.04.6 LTS;
- Ubuntu 18.04 LTS, 18.04.1 LTS, 18.04.2 LTS, 18.04.3 LTS, 18.04.4 LTS;
- Red Hat® Enterprise Linux® 6.7, 6.8. 6.9. 6.10;
- Red Hat Enterprise Linux 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8;
- Red Hat Enterprise Linux 8.0, 8.1;
- CentOS 6.7, 6.8, 6.9, 6.10;
- CentOS 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8;
- CentOS 8.0, 8.1;
- Debian GNU / Linux 9.4, 9.5, 9.6, 9.7, 9.8, 9.9, 9.10, 9.11, 9.12;
- Debian GNU / Linux 10.1, 10.2, 10.3;
- OracleLinux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8;
- OracleLinux 8.0, 8.1;
- SUSE® Linux Enterprise Server 15, 15 SP 1;
- openSUSE® Leap 15.0, 15.1;
- Альт 8 СП Рабочая Станция.
- Альт 8 СП Сервер.
- Альт Рабочая Станция 8.
- Альт Рабочая Станция К 8.
- Альт Рабочая Станция 9.
- Альт Сервер 8.
- Альт Сервер 9.
- Альт Образование 8.
- Альт Образование 9.
- Amazon Linux AMI;
- Linux Mint 18.2, 18.3;
- Linux Mint 19, 19.1, 19.2, 19.3;

- Astra Linux Special Edition 1.5;
- Astra Linux Special Edition 1.6;
- Astra Linux Common Edition «Орел» 2.12;
- Гослинукс 6.6;
- Гослинукс 7.2;
- Операционная система Лотос (редакция для серверов и рабочих станций);
- РЕД ОС 7.1;
- РЕД ОС 7.2;
- AlterOS 7.5;
- Pardus OS 19.1.

6.1.4. Прочие программные требования:

- Интерпретатор языка Perl версии 5.10;
- Установленная утилита which;
- Установленные пакеты для компиляции программ (gcc, binutils, glibc, glibc-devel, make, ld, rpcbind).
- Заголовки исходного кода ядра операционной системы – для компиляции модулей Kaspersky Endpoint Security на операционных системах, не поддерживающих технологию fanotify.
- До установки программы и Агента администрирования на операционной системе SUSE Linux Enterprise Server 15 SP1 должен быть установлен пакет insserv-compat.
- Для операционных систем Red Hat® Enterprise Linux® 8.0 и CentOS 8.0 требуется установить пакет perl-Getopt-Long.
- Для работы плагина управления Kaspersky Endpoint Security должен быть установлен Microsoft® Visual C++ 2015 Redistributable Update 3 RC (https://www.microsoft.com/ru-ru/download/details.aspx?id=52685).
- Kaspersky Endpoint Security 11.1.0 для Linux совместим с Kaspersky Security Center следующих версий:
    - Kaspersky Security Center 10 Service Pack 3,
    - Kaspersky Security Center 11,
    - Kaspersky Security Center 12.

6.2. Запрещается использование программного изделия в среде функционирования, ядро которой скомпилировано с включенной опцией "CONFIG_MMAP_ALLOW_UNINITIALIZED (по умолчанию отключена в поддерживаемых операционных системах).

6.3. Установка, предварительная настройка и эксплуатация программного изделия должны осуществляться в соответствии с эксплуатационной документацией, входящей в комплект поставки.

6.4. Активация программного изделия должна осуществляться только с использованием файла ключа.

6.5. Для сохранения бинарной целостности запрещается устанавливать обновления сертифицированного программного изделия, не прошедшие сертификационные испытания (только для типа 3). Порядок получения обновлений, прошедших сертификационные испытания, изложен в разделе 17 настоящего формуляра.

6.6. Предприятие, осуществляющее эксплуатацию программного изделия, должно периодически (не реже одного раза в 6 месяцев) проверять отсутствие обнаруженных уязвимостей в программном изделии, используя сайт предприятия-изготовителя (https://support.kaspersky.ru/vulnerability), базу данных уязвимостей ФСТЭК России (www.bdu.fstec.ru) и иные общедоступные источники.

6.7. Перед началом эксплуатации программного изделия необходимо установить все доступные обновления используемых версий ПО среды функционирования.

6.8. Применение механизма облачной защиты KSN при использовании программного изделия для защиты информации ограниченного доступа (информация, содержащая сведения, составляющие государственную тайну, конфиденциальная информация) допускается только при условии совместного использования с сертифицированным программным комплексом «Kaspersky Security Center совместно

с Kaspersky Private Security Network» (643.46856491.00082). В остальных случаях механизм облачной защиты KSN должен быть гарантировано отключен.

7. ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОСНОВНЫХ ХАРАКТЕРИСТИК ПРИ ЭКСПЛУАТАЦИИ И ХРАНЕНИИ

7.1. Периодический контроль основных характеристик при эксплуатации и хранении программного изделия состоит в проверке сохранности исполняемого кода, записанного на носителях информации.

7.2. Проверка сохранности программного изделия осуществляется путем подсчета контрольных сумм файлов программного изделия после установки и сравнения их с контрольными суммами, указанными в таблице КС исполняемых модулей, приведенными в Приложении 1 к настоящему формуляру.

7.3. Контроль основных характеристик программного изделия проводится при первичном закреплении за ответственным лицом.

7.4. Результаты периодического контроля основных характеристик программного изделия фиксируются в таблице 4.

Таблица 4 – Периодический контроль основных характеристик при эксплуатации и хранении

Проверяемая характеристика		Дата проведения измерения					
		20__ г.		20__ г.		20__ г.	
Наименование измерения	Величина	Фактическая величина	Замерил (должность, подпись)	Фактическая величина	Замерил (должность, подпись)	Фактическая величина	Замерил (должность, подпись)

8. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Программное изделие «Kaspersky Endpoint Security 11 для Linux» — 643.46856491.00049-09

(наименование программного изделия) — (обозначение)

соответствует техническим условиям (стандарту) — ТУ 643.46856491.00049-09

(номер технических условий или стандарта)

и признано годным для эксплуатации.

Дата выпуска 3 июня 2021 г.

_____ М. А. Сухачева

М.П.

9. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ

9.1. Раздел заполняется при физической поставке изделия.

Kaspersky Endpoint Security 11 для Linux ***(643.46856491.00049-09)***

наименование — обозначение

упакован (о) ***АО «Лаборатория Касперского»***

наименование или код предприятия (организации)

согласно требованиям, предусмотренным инструкцией ***ЯМДИ.460649.003***.

Маркировано идентификатором № **РОСС RU.01.2534.000766**, где:

- первая группа знаков указывает на систему сертификации ФСТЭК России РОСС RU.01.
- вторая группа знаков указывает на номер сертификата соответствия средства защиты информации.
- третья группа знаков указывает на уникальный порядковый номер идентификатора сертифицированного средства защиты информации.

Контрольная сумма: cbfdf39f23b5b9e7fd80bd0ed99afd925e3f47071ec7d90fe247b088e105a8fb

Серийный номер: **СМП8067-51112**

Наименование пользователя: **ГКУ ТО "ЦИТТО"**

№ сборки (РО): **Ax000407370-MP**

Дата упаковки **3 июня 2021 г.**

Упаковку произвел _____ А. А. Наумов

Изделие после упаковки принял _____ М. А. Сухачева

М.П.

Примечание. Форму заполняют на предприятии, производившем упаковку.

При электронной поставке программное изделие дополнительно маркируется с применением электронной подписи. Описание процедуры проверки электронной подписи приведено в разделе 16 настоящего формуляра.

10. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

10.1. В период гарантийного обслуживания предприятие-разработчик оказывает техническую поддержку в объеме, указанном в пункте 12 настоящего формуляра.

10.2. Гарантийное и послегарантийное обслуживание программного изделия осуществляется: АО «Лаборатория Касперского» (125212, г. Москва, Ленинградское шоссе, д. 39А, стр. 2).

11. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

11.1. Рекламации предъявляются в адрес АО «Лаборатория Касперского» (125212, г. Москва, Ленинградское шоссе, 39А, стр. 2) в письменном виде с указанием даты обнаружения неисправности, содержания и условий возникновения неисправности.

11.2. Рекламации подписываются руководителем подразделения, принимающего и эксплуатирующего программное изделие.

11.3. Сведения о рекламациях заносятся в таблицу 5.

Таблица 5 – Сведения о рекламациях

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

12. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

12.1. Изготовитель принимает на себя обязательства по технической поддержке программного изделия в объеме, указанном на странице https://support.kaspersky.ru/support/rules веб-сайта изготовителя.

12.2. В период оказания технической поддержки изготовитель гарантирует осуществление программным изделием функциональных возможностей, изложенных в настоящем формуляре, при соблюдении пользователем требований по эксплуатации, изложенных в эксплуатационной документации.

12.3. Срок оказания технической поддержки для программного изделия указан на странице https://support.kaspersky.ru/support/lifecycle веб-сайта изготовителя. Потребитель самостоятельно контролирует статус поддержки программного изделия.

12.4. Программное изделие, используемое после прекращения технической поддержки, не является сертифицированным.

12.5. Изготовитель принимает на себя обязательства по поиску ошибок реализации и уязвимостей в программном изделии на протяжении срока действия технической поддержки, а также обязательства по своевременному информированию потребителя о найденных ошибках и уязвимостях путем рассылки электронной почты, а также публикации на странице https://support.kaspersky.ru/support.

13. СВЕДЕНИЯ О ХРАНЕНИИ

13.1. При физической поставке программное изделие должно допускать пересылку заказчику (потребителю) в тарной упаковке на любое расстояние.

13.2. При электронной поставке программное изделие распространяется по сетям связи. Процедура получения программного изделия описана в пункте 16 настоящего формуляра.

13.3. Носители информации в упаковке должны храниться в отапливаемом помещении с температурой воздуха от 10 до 40°С) и максимальной относительной влажностью не более 80% при 25°С без конденсации влаги внутри помещения, при отсутствии в воздухе паров кислот, щелочей и других агрессивных примесей.

13.4. Условия хранения должны исключать резкие изменения температуры (не более 10°С/час) и влажности окружающего воздуха (не более 10%/час).

13.5. Сведения о хранении носителей информации с программным изделием заносятся в таблицу 6.

Таблица 6 – Сведения о хранении

Дата		Условия хранения	Должность, фамилия и подпись лица, ответственного за хранение
установки на хранение	снятия с хранения		

14. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ

14.1. Сведения о закреплении программного изделия при эксплуатации заносятся в таблицу 7.

14.2. При первичном закреплении необходимо провести контроль комплектности программного изделия (см. раздел 5).

Таблица 7 – Сведения о закреплении программного изделия при эксплуатации

Должность ответственного лица	Фамилия ответственного лица	Номер и дата приказа		Подпись ответственного лица
		о назначении	об освобождении	

15. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ

15.1. Сведения об изменениях заносятся в таблицу 8.

Таблица 8 – Сведения об изменениях

Основание (входящий номер сопроводительного документа и дата)	Дата проведения изменения	Содержание изменения	Порядковый номер изменения	Должность, фамилия и подпись ответственного лица за проведения изменения	Подпись лица, ответственного за эксплуатацию программного изделия

16. ПОЛУЧЕНИЕ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭЛЕКТРОННОЙ ПОСТАВКЕ

16.1. Порядок получения программного изделия:

Получение программного изделия осуществляется путем загрузки дистрибутива с веб-сайта АО «Лаборатория Касперского» (https://support.kaspersky.ru/common/certificates). Подлинность и целостность программного изделия обеспечивается применением электронной подписи.

16.2. Порядок эксплуатации программного изделия:

1). После загрузки дистрибутива программного изделия с комплектом эксплуатационной документации необходимо произвести проверку его подлинности и целостности путем проверки электронной подписи. Порядок проверки подлинности электронной подписи изложен в статье https://support.kaspersky.ru/15257.

2). При необходимости записать инсталляционный комплект на физический носитель и промаркировать его идентификатором, указанным в п.2.2.

3). Производить эксплуатацию обновленного программного изделия в соответствии с эксплуатационной документацией.

17. ОБНОВЛЕНИЕ ПРОГРАММНОГО ИЗДЕЛИЯ

17.1. Типы обновлений программного изделия.

Рассматриваются следующие типы обновлений программного изделия:

- обновление баз данных, необходимых для реализации функций безопасности (обновление БД ПКВ);
- обновление, направленное на устранение уязвимостей;
- обновление, направленное на добавление и/или совершенствование реализации функций безопасности, на расширение числа поддерживаемых программных и аппаратных платформ (обновление версии программного изделия).

17.2. Уведомления об обновлениях программного изделия.

Уведомления об обновлении БД ПКВ реализованы на программном уровне.

Уведомления об обнаруженных уязвимостях, обновлениях, направленных на устранение уязвимостей, и обновлениях версии программного изделия доводятся до потребителей путем отправки сообщений на адреса электронной почты, указанные при заказе программного изделия или подписке на рассылку «Новости о сертифицированных продуктах» (https://support.kaspersky.ru/email_subscriptions/form).

17.3. Порядок получения обновления программного изделия.

Обновление, направленное на устранение уязвимостей, можно получить на веб-сайте АО «Лаборатория Касперского» (https://support.kaspersky.ru/common/certificates). Подлинность и целостность обновлений обеспечивается применением электронной подписи.

Обновление версии программного изделия можно получить следующими способами.

Открыть статью о соответствующем продукте на веб-сайте АО «Лаборатория Касперского» (https://support.kaspersky.ru/common/certificates) и скачать дистрибутив обновления программного изделия с комплектом измененной эксплуатационной документации.

17.4. Порядок применения обновлений.

1). После загрузки файлов обновления программного изделия и комплекта измененной эксплуатационной документации произвести проверку подлинности и целостности загруженных файлов путем проверки электронной подписи. Порядок проверки подлинности электронной подписи изложен в статье https://support.kaspersky.ru/15257.

2). При необходимости записать инсталляционный комплект на физический носитель и промаркировать его идентификатором, указанным в п.2.2.

3). Внести изменения в эксплуатационную документацию, руководствуясь инструкциями в бюллетене. При необходимости заменить используемые эксплуатационные документы новыми редакциями.

4). При необходимости внести изменения в настройки программного изделия, руководствуясь инструкциями в бюллетене.

5). Производить эксплуатацию обновленного программного изделия в соответствии с обновленной эксплуатационной документацией.

6). При необходимости промаркировать замененные версии эксплуатационных документов,

дистрибутива, копии сертификата соответствия как замененные и хранить вместе с актуальными версиями.

18. ОСОБЫЕ ОТМЕТКИ

18.1. Приложение 1 выполнено в виде отдельного документа 643.46856491.00049-09 30 02 в электронном виде.