АО «Лаборатория Касперского»

УТВЕРЖДЕН
643.46856491.00084-04 30 01-ЛУ

Программное изделие

KASPERSKY SECURITY 10.1.2 ДЛЯ WINDOWS SERVER

Формуляр

643.46856491.00084-04 30 01

Листов 15

Литера

2019

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

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 Security 10.1.2 для Windows Server»

Версия: 10.1.2.996

Обозначение: 643.46856491.00084-04

Дата изготовления (заполняется при физической поставке): _____

Наименование изготовителя: АО «Лаборатория Касперского»

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

Серийный номер (заполняется при физической поставке): _____

Тип носителя (при физической поставке): лазерный диск.

2.2. Сведения о применимых сертификатах соответствия и лицензиях:

Наименование и номер сертификата	Срок начала действия	Срок окончания действия	Знак соответствия (заполняется при физической поставке)

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	Дата создания	Длина, байт	КС
Каталог K:				
1	ks4ws_10.1.2.996_ru.exe	23.04.19 15-51	282686312	7dfca0b8e27f6fbf8baf20cd08de826b3bf01056676e611d63d735a5ac6c5057
итого: файлов - 1			**282686312**	**7dfca0b8e27f6fbf8baf20cd08de826b3bf01056676e611d63d735a5ac6c5057**
ВСЕГО: файлов - 1			**282686312**	**7dfca0b8e27f6fbf8baf20cd08de826b3bf01056676e611d63d735a5ac6c5057**
Конец				

Контрольные суммы рассчитаны с использованием средства фиксации исходного состояния программного комплекса «ФИКС» версии 2.0.2 (сертификат ФСТЭК России № 1548, действителен до 15.01.2020 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:

- 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 САВЗ;
- возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности САВЗ;
- поддержка определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности и администраторами сервера;
- возможность выполнять проверки с целью обнаружения зараженных КВ объектов;
- возможность выполнения проверок с целью обнаружения зараженных КВ объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
- возможность выполнять проверки с целью обнаружения зараженных КВ объектов сигнатурными и эвристическими методами;
- возможность выполнять проверки с целью обнаружения зараженных КВ объектов по команде и в режиме динамического обнаружения в процессе выполнения операций доступа к объектам;
- возможность выполнять проверки с целью обнаружения зараженных КВ объектов путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
- возможность удаления (если технически возможно) файлов, в которых обнаружены КВ, а также файлов, подозрительных на наличие КВ, перемещение и изолирование объектов воздействия;
- возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных КВ;
- возможность отображения сигнала тревоги на АРМ администратора, в том числе до подтверждения его получения или до завершения сеанса;
- возможность восстановления функциональных свойств зараженных объектов;
- возможность получения и установки обновлений БД ПКВ без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения;
- возможность мониторинга контроля выполнения файловых операций объектов;
- возможность проводить анализ журналов событий Windows;
- возможность выполнять проверки с целью обнаружения атаки эксплойтов в памяти процессов, в контейнерах Windows Server 2016;
- возможность при обнаружении признаков атаки эксплойтов на защищаемый процесс завершать процесс, сообщать о факте дискредитации уязвимости в процессе.

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 Security 10.1.2 для Windows Server. Инсталляционный комплект	643.46856491.00084-04	1		На лазерном диске
2. Kaspersky Security 10.1.2 для Windows Server. Формуляр	643.46856491.00084-04 30 01	1		В печатном виде
3. Kaspersky Security 10.1.2 для Windows Server. Приложение 1 к формуляру	643.46856491.00084-04 30 02	1		На лазерном диске
4. Kaspersky Security 10.1.2 для Windows Server. Подготовительные процедуры и руководство по эксплуатации	643.46856491.00084-04 90 01	1		На лазерном диске
5.Kaspersky Security 10.1.2 для Windows Server. Руководство пользователя	643.46856491.00084-04 90 02	1		В электронном виде
6.Kaspersky Security 10.1.2 для Windows Server. Руководство по эксплуатации для защиты сетевых хранилищ	643.46856491.00084-04 90 03	1		В электронном виде
7. Упаковка		1		
8. 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 Security 10.1.2 для Windows Server. Инсталляционный комплект	643.46856491.00084-04	1		В электронном виде
2. Kaspersky Security 10.1.2 для Windows Server. Формуляр	643.46856491.00084-04 30 01	1		В электронном виде
3. Kaspersky Security 10.1.2 для Windows Server. Приложение 1 к формуляру	643.46856491.00084-04 30 02	1		В электронном виде
4. Kaspersky Security 10.1.2 для Windows Server. Подготовительные процедуры и руководство по эксплуатации	643.46856491.00084-04 90 01	1		В электронном виде
5.Kaspersky Security 10.1.2 для Windows Server. Руководство пользователя	643.46856491.00084-04 90 02	1		В электронном виде
6.Kaspersky Security 10.1.2 для Windows Server. Руководство по эксплуатации для защиты сетевых хранилищ	643.46856491.00084-04 90 03	1		В электронном виде
7. 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. Требования к серверу, на который устанавливается Kaspersky Security:

Аппаратные требования к серверу

- x86-64-совместимые системы в однопроцессорной и многопроцессорной конфигурации;
- объем дискового пространства:
- для установки всех программных компонентов – 70 МБ;

- для загрузки и хранения антивирусных баз программы – 2 ГБ (рекомендуется);
- для хранения объектов на карантине и в резервном хранилище – 400 МБ (рекомендуется);
- для хранения журналов – 1 ГБ (рекомендуется).

Рекомендуемая конфигурация:

- процессор: четырехпроцессорный 2,4 ГГц.
- объем оперативной памяти: 2 ГБ.
- дисковая подсистема: 4 Гб доступного пространства.

Программные требования к серверу

Для установки и работы Kaspersky Security 10.1.2 для Windows Server требуется наличие на сервере Microsoft Windows Installer 3.1.

6.1.2. ОО может функционировать на одной из следующих 32-разрядных систем:

- Windows Server® 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1;
- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1.

6.1.3. ОО может функционировать на одной из следующих 64-разрядных систем:

- Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1;
- Microsoft Small Business Server 2008 Standard / Premium;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1;
- Windows Server 2008 R2 Core / Standard / Enterprise / Datacenter с пакетом обновлений SP1;
- Windows Hyper-V® Server 2008 R2 с пакетом обновлений SP1;
- Microsoft Small Business Server 2011 Essentials / Standard;
- Microsoft Windows MultiPoint™ Server 2011;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server;
- Windows Server 2012 Core Standard / Datacenter;
- Windows Storage Server 2012;
- Windows Hyper-V Server 2012;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Core Standard / Datacenter;
- Windows Storage Server 2012 R2;
- Windows Hyper-V Server 2012 R2;
- Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server;
- Windows Server 2016 Core Standard / Datacenter;
- Windows Storage Server 2016;
- Windows Hyper-V Server 2016;
- Windows Server 2019 all versions (including Core/Terminal/Hyper-V).

6.1.4. ОО функционирует на следующих типах терминальных серверов:

- Microsoft Remote Desktop Services на базе Windows 2008 Server;
- Microsoft Remote Desktop Services на базе Windows 2008 R2 Server;
- Microsoft Remote Desktop Services на базе Windows 2012 Server;
- Microsoft Remote Desktop Services на базе Windows 2012 Server R2;

- Microsoft Remote Desktop Services на базе Windows Server 2016;
- Windows Server 2019;
- Citrix XenApp 6.0, 6.5, 7.0, 7.5 - 7.9, 7.15;
- Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15.

6.1.5. Требования к защищаемому сетевому хранилищу:
Изделие может использоваться для защиты следующих сетевых хранилищ:

- NetApp® с одной из следующих операционных систем:
  - Data ONTAP® 7.x и Data ONTAP 8.x в режиме 7-mode;
  - Data ONTAP 8.2.1 или выше в режиме cluster-mode.
- Dell EMC™ Celerra™ / VNX™ со следующим программным обеспечением:
  - операционная система EMC DART 6.0.36;
  - Антивирусный агент Celerra (CAVA) 4.5.2.3.
- Dell EMC Isilon™ с операционной системой OneFS™ 7.0.
- Hitachi NAS на одной из следующих платформ:
  - HNAS 4100;
  - HNAS 4080;
  - HNAS 4060;
  - HNAS 4040;
  - HNAS 3090;
  - HNAS 3080.
- IBM® NAS серии IBM System Storage® N series.
- Oracle® NAS Systems семейства Oracle ZFS Storage Appliance.
- Dell™ NAS на платформе Dell Compellent™ FS8600.

6.1.6. Требования к компьютеру, на который устанавливается Консоль Kaspersky Security
Аппаратные требования к компьютеру

- Рекомендуемый объем оперативной памяти – 128 МБ или более.
- Свободное дисковое пространство: 30 МБ.

Программные требования к компьютеру

Для установки и работы Консоли ОО требуется наличие на компьютере Microsoft Windows Installer 3.1.
Консоль ОО может функционировать на одной из следующих 32-разрядных систем:

- Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1;
- Microsoft Windows XP Professional с пакетом обновлений SP2;
- Microsoft Windows Vista®;
- Microsoft Windows 7;
- Microsoft Windows 8;
- Microsoft Windows 8.1;
- Microsoft Windows 10.

ОО может функционировать на одной из следующих 64-разрядных систем:

- Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1;
- Microsoft Small Business Server 2008 Standard / Premium;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1;
- Microsoft Small Business Server 2011 Essentials / Standard;

- Microsoft Windows MultiPoint™ Server 2011;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server;
- Windows Storage Server 2012;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Storage Server 2012 R2;
- Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server;
- Windows Storage Server 2016;
- Microsoft Windows XP Professional Edition с пакетом обновлений SP2;
- Microsoft Windows Vista;
- Microsoft Windows 7;
- Microsoft Windows 8;
- Microsoft Windows 8.1;
- Microsoft Windows 10.

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

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

6.4. Для сохранения бинарной целостности запрещается устанавливать обновления версии сертифицированного программного изделия, не прошедшие сертификационные испытания. Порядок получения обновлений, прошедших сертификационные испытания, изложен в разделе 17 настоящего формуляра.

6.5. 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.

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

6.7. 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					
Наименование измерения	Величина	20__ г.		20__ г.		20__ г.	
		Фактическая величина	Замерил (должность, подпись)	Фактическая величина	Замерил (должность, подпись)	Фактическая величина	Замерил (должность, подпись)

8. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Программное изделие «Kaspersky Security 10.1.2 для Windows Server» — 643.46856491.00084-04

(наименование программного изделия) — (обозначение)

соответствует техническим условиям (стандарту) — ТУ 643.46856491.00084-04

(номер технических условий или стандарта)

и признано годным для эксплуатации.

Дата выпуска _____

М.П. Подпись лиц, ответственных за приемку

9. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ

9.1. Раздел заполняется при физической поставке изделия.

Kaspersky Security 10.1.2 для Windows Server ***(643.46856491.00084-04)***

наименование обозначение

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

наименование или код предприятия (организации)

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

Маркировано знаком соответствия №_____ системы сертификации средств защиты информации по требованиям безопасности информации (свидетельство № РОСС RU.0001.01БИ00). Наклеивается в разделе 2 настоящего формуляра в соответствующее место.

Контрольная сумма: `7dfca0b8e27f6fbf8baf20cd08de826b3bf01056676e611d63d735a5ac6c5057`

Серийный номер: _____

Наименование пользователя: _____

№ сборки (РО): _____

Дата упаковки _____

Упаковку произвел _____ (подпись)

Изделие после упаковки принял _____ (подпись)

М.П.

Примечание. Форму заполняют на предприятии, производившем упаковку.

9.2. При электронной поставке маркирование программного изделия осуществляется 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 разделе 11 настоящего формуляра.

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

11. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

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

11.2. 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.

11.3. 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.

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

11.5. 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.

12. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

12.1. 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.

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

12.3. Сведения о рекламациях заносятся в таблицу 5.

Таблица 5 – Сведения о рекламациях

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

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 разделе 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). Записать установочный комплект на физический носитель (лазерный диск).

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 обновлений программного изделия.

Получение обновлений версии программного изделия или обновлений, направленных на устранение уязвимостей, осуществляется путем загрузки соответствующего дистрибутива с комплектом измененной эксплуатационной документации с веб-сайта АО «Лаборатория Касперского» (https://support.kaspersky.ru/common/certificates). Подлинность и целостность обновлений обеспечивается применением электронной подписи.

17.4. Порядок применения обновлений программного изделия.

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). Записать инсталляционный комплект на физический носитель (лазерный диск).

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 643.46856491.00084-04 30 02 в электронном виде.