**Kaspersky Endpoint Security для Windows**

**Руководство пользователя**

Версия 12.8

Оглавление

[Введение 3](#_Toc193816871)

[1. О программе 4](#_Toc193816872)

[1.1 Минимальные системные требования 4](#_Toc193816873)

[2. Компоненты приложения 5](#_Toc193816874)

[2.1 Базовая защита 5](#_Toc193816875)

[2.2 Продвинутая защита 5](#_Toc193816876)

[2.3 Контроль безопасности 5](#_Toc193816877)

[2.4 Шифрование данных 6](#_Toc193816878)

[2.5 Detection and Response 6](#_Toc193816879)

[3. Установка, изменение и удаление программы 7](#_Toc193816880)

[3.1 Распаковка дистрибутива 7](#_Toc193816881)

[3.2 Установка с помощью мастера установки 7](#_Toc193816882)

[3.2.1 Приветственное окно 7](#_Toc193816883)

[3.2.2 Лицензионное соглашение и Политика конфиденциальности 8](#_Toc193816884)

[3.2.3 Выбор режима приложения 8](#_Toc193816885)

[3.2.4 Выбор компонентов программы 9](#_Toc193816886)

[3.2.5 Выбор папки для установки приложения 11](#_Toc193816887)

[3.2.6 Дополнительные настройки 11](#_Toc193816888)

[3.2.7 Подготовка к установке 12](#_Toc193816889)

[3.2.8 [Положение о Kaspersky Security Network 12](#_Toc193816891)](#_Toc193816890)

[3.3 Изменение компонентов 13](#_Toc193816892)

[3.4 Удаление программы 13](#_Toc193816893)

[3.4.1 Сохранение объектов 13](#_Toc193816894)

[3.4.2 Подтверждение удаления 14](#_Toc193816895)

[3.4.3 Завершение удаления 14](#_Toc193816896)

[4. Предварительная настройка 15](#_Toc193816897)

[4.1 Интерфейс программы 15](#_Toc193816898)

[4.1.1 Мониторинг 16](#_Toc193816899)

[4.1.2 Безопасность 16](#_Toc193816900)

[4.1.3 Обновление 17](#_Toc193816901)

[4.1.4 Задачи 17](#_Toc193816902)

[4.1.5 Лицензия 18](#_Toc193816903)

[4.2 Лицензирование 18](#_Toc193816904)

[4.2.1 Лицензия 18](#_Toc193816905)

[4.2.2 Активация лицензии 19](#_Toc193816906)

# Введение

Данное руководство описывает установку и предварительную настройку клиентской версии программы Kaspersky Endpoint Security в качестве локального решения. Руководство актуально для версии 12.8 от 19 февраля 2025 года.

**Условные обозначения**

|  |  |
| --- | --- |
| **Уровень безопасности** | Обозначение элементов или интерфейса программы |
| *setup\_kes.exe* | Пути к файлу, имя файла или ссылки в сети Интернет |

**Сокращения**

|  |  |
| --- | --- |
| **ЛКМ** | Левая кнопка мыши |
| **ОС** | Операционная система |
| **VDI** | Virtual Desktop Infrastructure |
| **ПКМ** | Правая кнопка мыши |

# О программе

Kaspersky Endpoint Security предлагает комплексную защиту компьютера от файловых и сетевых угроз, а также мошеннических и бесфайловых атак.

Для выявления угроз программа использует современные методы, среди которых машинное обучение и различные виды анализа: облачный, экспертный, поведенческий, автоматический.

Kaspersky Endpoint Security имеет три режима функционирования: Стандартный режим, Агент EDR (Endpoint Detection and Response) и Легкий агент для защиты виртуальных сред. Режимы включают в себя разные компоненты и выполняют разные функции.

### Минимальные системные требования

Перед установкой убедитесь, что компьютер соответствует следующим минимальным требованиям:

* Жесткий диск: 2 ГБ свободного пространства;
* Оперативная память:
  + 1 ГБ для Windows x32;
  + 2 ГБ для Windows x64;
* Процессор:
  + 1 ГГц;
  + Поддержка SSE2.

Программа поддерживает следующие ОС:

* Windows 7:
  + Home;
  + Professional;
  + Ultimate;
  + Enterprise Service Pack 1 и выше.
* Windows 8 и Windows 8.1:
  + Professional;
  + Enterprise.
* Windows 10 и Windows 11:
  + Home;
  + Pro;
  + Education;
  + Enterprise.

# Компоненты приложения

В данном разделе описываются основные блоки и компоненты защиты. Обязательными к установке и общими для всех режимов являются следующие компоненты:

* **Ядро приложения** обеспечивает работу основных компонентов;
* **Коннектор к Агенту администрирования** позволяет дистанционно управлять программой через Kaspersky Security Center.

Остальные компоненты зависят от выбранного режима приложения.

## Базовая защита

Сюда включены следующие виды защиты:

* **От сетевых угроз** предотвращает несанкционированный доступ к компьютеру и данным;
* **От файловых угроз** проверяет все файлы, с которыми взаимодействует пользователь;
* **От почтовых угроз** фильтрует электронные письма на наличие вредоносных программ;
* **От веб-угроз** контролирует передачу вредоносных файлов по HTTP-протоколу;
* **ASMI-защита** позволяет другим программам осуществлять проверку объектов через интерфейс ASMI;
* **От атак BadUSB** распознает и нейтрализует USB-устройства, которые имитируют клавиатуру или мышь;
* **От сетевых атак** фильтрует сетевую активность пользователя.

## Продвинутая защита

* **Анализ поведения** защищает компьютер от сложных угроз и вирусов-шифровальщиков;
* **Защита от эксплойтов** предотвращает угрозы, которые используют уязвимости в программном обеспечении;
* **Откат вредоносных действий** отменяет изменения, внесенные вредоносными программами;
* **Предотвращение вторжений** защищает систему от потенциально опасных действий.

## Контроль безопасности

* **Веб-Контроль** управляет доступом к Интернету;
* **Контроль приложений** обеспечивает настройку доступа к отдельным программам;
* **Контроль устройств** позволяет отслеживать подключение внешних устройств и носителей;
* **Адаптивный контроль** **аномалий** анализирует и контролирует нетипичные для компьютеров действия.

## Шифрование данных

* **Шифрование файлов** позволяет шифровать отдельные объекты;
* **Полнодисковое шифрование** позволяет шифровать жесткие и съемные диски;
* **Управление Bitlocker** позволяет шифровать жесткие диски с использованием технологии Bitlocker.

## Detection and Response

* **Интеграция с KUMA** (Kaspersky Unified Monitoring and Analysis Platform) обеспечивает подключение к платформе KUMA для сбора и анализа информации о безопасности в реальном времени;
* **Endpoint Detection and Response (KATA)** анализирует сетевой трафик на предмет сложных угроз, целевых атак и атак «нулевого дня»;
* **Network Detection and Response** входит в состав решения KATA;
* **Endpoint Detection and Response Optimum** обеспечивает защиту корпоративных мобильных устройств;
* **Endpoint Detection and Response Expert** контролирует сетевую безопасность;
* **Managed Detection and Response** обнаруживает и нейтрализует сетевые угрозы, которые способны обойти автоматические средства защиты;
* **Sandbox** позволяет запускать и проверять потенциально вредоносные программы в виртуальной машине.

# Установка, изменение и удаление программы

Перед установкой необходимо скачать и распаковать комплект установочных файлов с официального сайта [*https://www.kaspersky.ru/small-to-medium-business-security/downloads/endpoint*](https://www.kaspersky.ru/small-to-medium-business-security/downloads/endpoint).

Найдите и разверните панель **Kaspersky Endpoint Security для Windows** с помощью кнопки **Показать версии для загрузки**. Нажмите **Скачать**, чтобы загрузить необходимую версию дистрибутива под заголовком **Build**.

Вы также можете скачать:

* плагин контроля приложений;
* EULA (пользовательское соглашение);
* информацию о версии.

В конце списка вы можете найти ссылку на онлайн-справку.

После завершения скачивания запустите загруженный файл *keswin\_12.8.0.505\_ru\_aes56.exe*.

## Распаковка дистрибутива

Для извлечения необходимых для установки файлов следуйте следующим указаниям:

1. Приветственное окно информирует о функции данной программы. Для продолжения нажмите **Далее**.
2. Укажите путь к папке для распаковки дистрибутива. Для изменения воспользуйтесь кнопкой **Обзор**. В дальнейшем в этой папке будет находиться файл мастера установки. Для продолжения нажмите **Распаковать**.
3. Дождитесь окончания распаковки. По завершении нажмите **Готово**.

На любом этапе распаковки нажмите **Отмена**, чтобы прервать процесс.

## Установка с помощью мастера установки

Найдите указанную ранее папку с установочными файлами. Для запуска установки откройте файл *setup\_kes.exe*. Перед этим рекомендуется закрыть все приложения.

Для выполнения необходимо разрешение администратора компьютера.

Программа подготовит компьютер для дальнейшей установки.

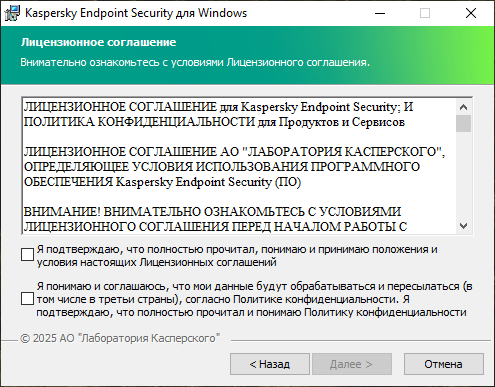
### Приветственное окно

Приветственное окно информирует о запущенном мастере установки.

Для продолжения нажмите **Далее**.

### Лицензионное соглашение и Политика конфиденциальности

Перед началом работы с мастером установки необходимо ознакомиться с пунктами Лицензионного соглашения и Политикой конфиденциальности. Полный текст приведен в открытом окне.



*Рис. 1 Лицензионное соглашение и Политика конфиденциальности*

В случае согласия установите следующие флажки:

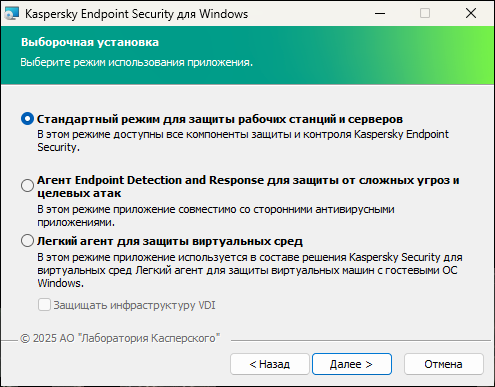
* Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящих Лицензионных соглашений.
* Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе и в третьи страны), согласно Политике конфиденциальности. Я подтверждаю, что полностью прочитал и принимаю Политику конфиденциальности.

Без вашего согласия со всеми пунктами мастер установки не позволит установить программу.

Для продолжения нажмите **Далее**, для возврата к предыдущему шагу — **Назад**, чтобы прервать процесс установки — **Отмена**. Данные действия доступны на любом этапе установки.

### Выбор режима использования приложения

По умолчанию установлен режим выборочной установки.



*Рис. 2 Выбор режима работы приложения*

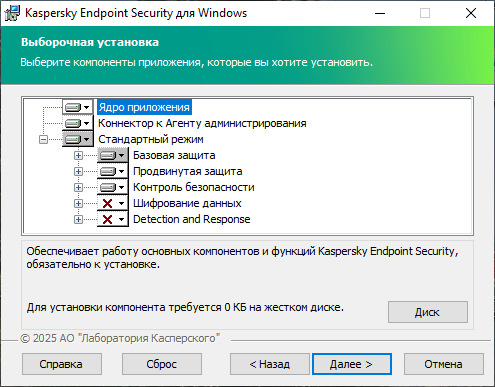
На данном этапе необходимо выбрать режим использования приложения:

* **Стандартный режим** предлагает все компоненты защиты и контроля Kaspersky Endpoint Security. Это основной режим работы приложения и режим работы по умолчанию.
* **Агент Endpoint Detection and Response** предназначен для защиты от сложных угроз и целевых атак и совместим со сторонними антивирусными приложениями.
* **Легкий агент для защиты виртуальных сред** доступен только при наличии Агента администрирования и предназначен для защиты виртуальных сред с гостевыми ОС. Чтобы включить защиту VDI, установите соответствующий флажок.

Для выбора **Стандартного режима** установите соответствующий флажок.

### Выбор компонентов программы

На данном этапе вы можете выбрать компоненты для установки. Их набор различается для каждого режима приложения. Для ознакомления с функциями всех доступных компонентов перейдите в раздел [1.2](#_Компоненты_приложения).



*Рис. 3 Окно выбора компонентов для установки*

В открытом окне доступны следующие кнопки:

* **Диск** для просмотра доступного пространства на жестком диске;
* **Сброс** для возврата к выбору компонентов по умолчанию;
* **Справка** для получения советов по установке.

Чтобы развернуть список доступных подкомпонентов, нажмите .

Нажмите на название компонента, чтобы узнать основные сведения о нем. В окне под списком вы можете ознакомиться с его основной функцией и необходимым количеством пространства на жестком диске.

Каждый компонент и подкомпонент имеет свой **статус установки**. Чтобы его изменить, щелкните ЛКМ по значку рядом с названием компонента и выберите один из следующих статусов:

|  |  |
| --- | --- |
|  | Компонент будет полностью установлен на локальный жесткий диск. |
|  | Компонент и некоторые его подкомпоненты будут установлены. |
|  | Компонент не будет установлен. |

**Стандартный режим**

Данный режим обеспечивает комплексную защиту компьютера и включает в себя обязательные компоненты:

* Ядро приложения;
* Коннектор к Агенту администрирования.

Кроме того, он включает в себя необязательные компоненты по выбору. Следующие компоненты выбраны для установки по умолчанию:

* Базовая защита:
  + От сетевых угроз;
  + От файловых угроз;
  + От почтовых угроз;
  + От веб-угроз;
  + ASMI-защита;
  + От сетевых атак.
* Продвинутая защита:
  + Анализ поведения;
  + Защита от эксплойтов;
  + Откат вредоносных действий;
  + Предотвращение вторжений.
* Контроль безопасности:
  + Веб-Контроль;
  + Контроль приложений;
  + Контроль устройств;
  + Адаптивный контроль аномалий.

Следующие компоненты не выбраны по умолчанию, но вы можете их установить:

* Базовая защита:
  + От атак BadUSB.
* Шифрование данных:
  + Шифрование файлов;
  + Полнодисковое шифрование;
  + Управление Bitlocker.
* Detection and Response:
  + Интеграция с KUMA;
  + Endpoint Detection and Response (KATA);
  + Endpoint Detection and Response Optimum;
  + Endpoint Detection and Response Expert;
  + Managed Detection and Response;
  + Sandbox;
  + Network Detection and Response (KATA).

**Агент Endpoint Detection and Response**

Данный режим включает в себя обязательные компоненты:

* Ядро приложения;
* Коннектор к Агенту администрирования.

А также компонент и подкомпоненты по выбору:

* Агент Endpoint Detection and Response:
* Интеграция с KUMA;
* Endpoint Detection and Response (KATA);
* Network Detection and Response (KATA);
* Managed Detection and Response.

### Выбор папки для установки приложения

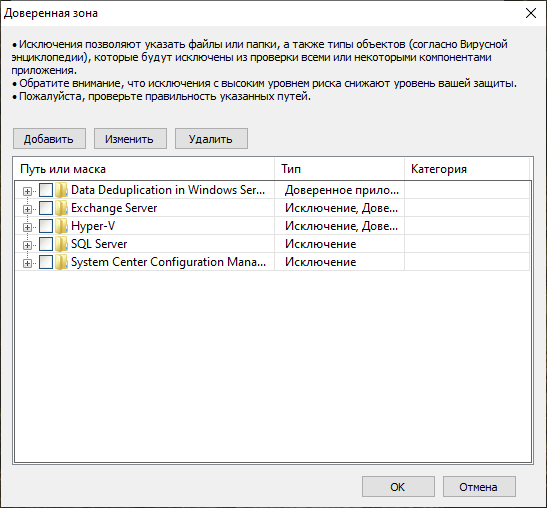
Укажите путь к папке для установки приложения. По умолчанию приложение устанавливается по пути *C:\Program Files (x86)\Kaspersky Lab\KES.12.8.0\.*

Для выбора папки воспользуйтесь кнопкой **Обзор**.

### Дополнительные настройки

На данном этапе вы можете выбрать папки и файлы, которые будут исключены из области защиты и проверки. В открытом окне отображаются группы файлов, которые исключены по умолчанию.

Для настройки доверенной зоны нажмите **Настроить**.



*Рис. 4 Настройка доверенной зоны*

Нажмите  для просмотра списка файлов внутри группы.

Для добавления одного или нескольких файлов в область Доверенной зоны, нажмите **Добавить** и выберите тип объекта:

* Группа;
* Исключение;
* Доверенное приложение.

В строке введите путь к объекту. Чтобы редактировать путь, нажмите **Изменить**; чтобы исключить объект из списка — **Удалить**.

Чтобы включить/исключить объект из области защиты и проверки, поставьте/уберите флажок слева от наименования объекта. Нажмите **ОК/Отмена** для сохранения/сброса параметров Доверенной зоны.

### Подготовка к установке

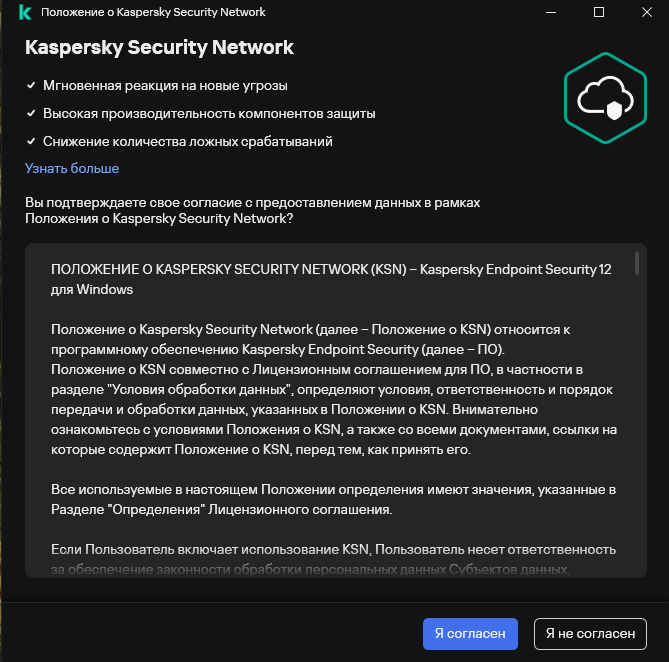
На данном этапе вы можете выбрать дополнительные настройки из следующих:

* обеспечить совместимость с Citrix PVS (Citrix Provisioning Services) для загрузки ОС по сети на выбранных машинах;
* защитить процесс установки приложения (рекомендованный параметр);
* добавить путь к файлу avp.com в системную переменную %PATH%.

Чтобы начать установку с выбранными настройками, нажмите **Установить** и дождитесь завершения установки.

### Положение о Kaspersky Security Network

По завершении установки появится окно с Положением о Kaspersky Security Network (KSN). С подробными условиями обработки данных при использовании KSN вы можете ознакомиться в открытом окне.



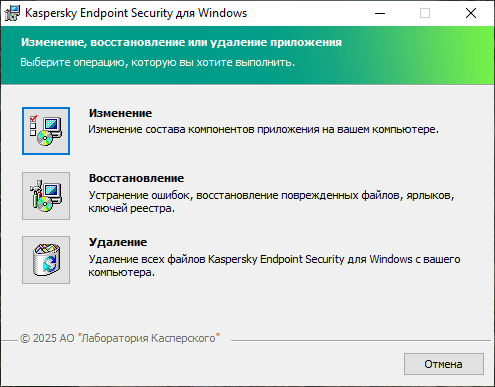
*Рис. 5 Положение о KSN*

Нажмите **Я согласен**, если вы принимаете данное Положение, или **Я не согласен**, если вы его не принимаете. Программа попросит вас подтвердить свой выбор.

По завершении установки нажмите **Готово**, чтобы закрыть мастер установки.

## Изменение компонентов

Для изменения компонентов воспользуйтесь мастером установки. Запустите файл *setup\_kes.exe*.



*Рис. 6 Окно мастера установки*

В меню мастера установки нажмите **Изменение**.

Чтобы добавить или удалить компонент, воспользуйтесь советами из пунктов [2.2.3](#_heading=h.26in1rg) и [2.2.4](#_heading=h.lnxbz9).

В меню также доступны опции:

* **Восстановление**, в случае если один из компонентов поврежден;
* **Удаление**, в случае если вы хотите удалить программу с компьютера.

Для отмены изменений нажмите **Отмена**.

## Удаление программы

Для удаления воспользуйтесь мастером установки. Запустите файл *setup\_kes.exe*.

В меню мастера установки нажмите **Удаление**.

### Сохранение объектов

Перед удалением вы можете указать объекты, которые сохранятся на компьютере и будут использованы при повторной установке. Для сохранения доступны:

* **Информация об активации**

Информация о вашей лицензии сохранится до повторной установки. Программа автоматически активирует лицензию, если вы сохраните эти данные.

* **Файлы резервного хранилища**

Копии объектов, которые были удалены или изменены в процессе лечения, сохранятся и восстановятся после повторной установки.

* **Настройки работы приложения**

Заданные вами параметры сохранятся и автоматически установятся после повторной установки.

* **Локальное хранилище ключей шифрования**

Данные о зашифрованных объектах сохранятся до повторной установки.

Для сохранения данных установите соответствующий флажок.

### Подтверждение удаления

Чтобы окончательно удалить программу, нажмите **Удалить**.

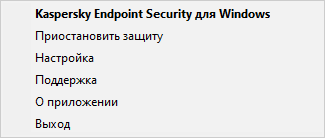
### Завершение удаления

Дождитесь завершения удаления. По завершении нажмите **Готово**. Для полного завершения удаления перезагрузите компьютер.

# Предварительная настройка

После установки вы можете найти значок приложения  на панели задач в **Скрытых значках**. Нажмите ЛКМ на значок, чтобы развернуть окно приложения.

Нажмите ПКМ, чтобы развернуть контекстное меню.

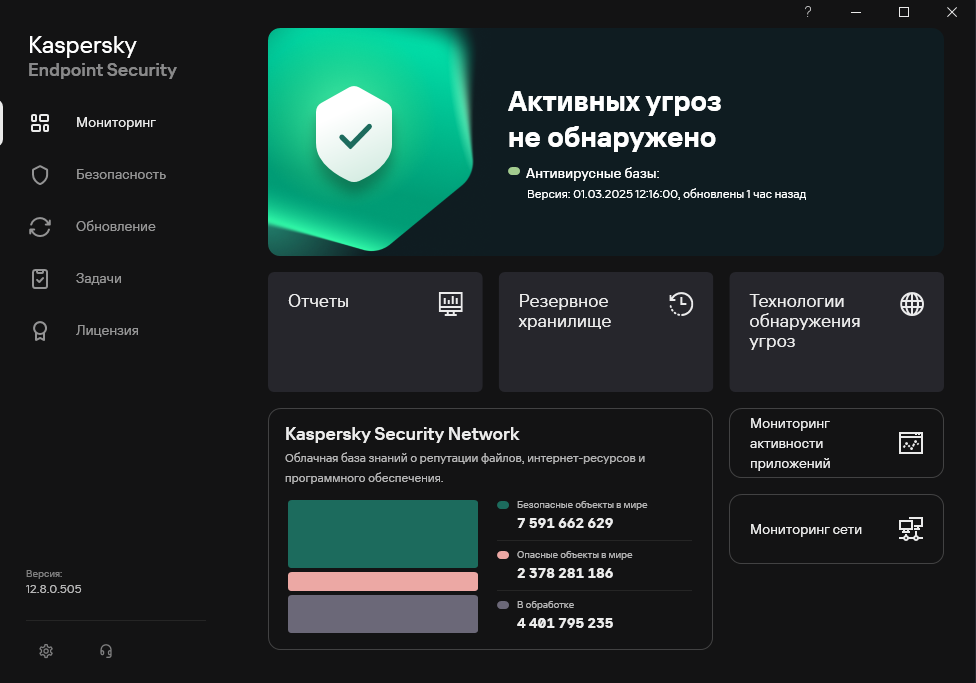


*Рис. 7 Контекстное меню значка*

В меню вам доступны следующие кнопки:

* **Kaspersky Endpoint Security для Windows** разворачивает окно программы;
* **Приостановить защиту** позволяет остановить работу приложения, но не закрывает его;
* **Настройки** открывает окно настроек параметров приложения;
* **Поддержка** открывает окно поддержки;
* **О приложении** открывает окно с основной информацией о приложении;
* **Выход** прекращает работу приложения.

## Интерфейс программы



*Рис. 8 Главное окно приложения*

Перед запуском программа подготовит компьютер к работе.

В правом верхнем углу находится панель управления окном. Вам доступны следующие действия:

*  закрывает окно;
*  разворачивает окно на полный экран;
*  сворачивает окно;
*  открывает онлайн-руководство в сети Интернет.

Слева находится панель **Меню**, в которой располагаются следующие разделы:

* **Мониторинг** позволяет просматривать отчеты о действиях программы и резервное хранилище, предоставляет информацию о технологиях обнаружения угроз, позволяет осуществлять мониторинг активности приложений и сети.
* **Безопасность** позволяет просмотреть список установленных компонентов, осуществлять их настройку и просматривать отчеты.
* **Обновление** позволяет настраивать и управлять процессом обновления модулей и баз данных приложения.
* **Задачи** позволяет управлять задачами приложения и запускать проверки на наличие вредоносных программ.
* **Лицензия** предоставляет доступ к информации о лицензиях и позволяет управлять актуальной лицензией.

В левом нижнем углу указана актуальная версия приложения. Там же доступны действия:

1.  открывает настройки приложения;
2.  открывает окно поддержки.

### Мониторинг

В данном разделе доступны следующие блоки:

* **Отчеты** позволяет просматривать журнал действий программы.
* **Резервное хранилище** хранит резервные копии файлов, которые были изменены или удалены в процессе лечения. Копии файлов не представляют угрозы для компьютера.
* **Технологии обнаружения угроз** описывает используемые методы распознавания и лечения вредоносных программам;
* **Мониторинг активности приложений** позволяет просматривать активность приложений.
* **Мониторинг сети** позволяет отслеживать сетевую активность пользователя.

### Безопасность

Данный раздел отображает установленные компоненты из блоков **Базовая защита**, **Продвинутая защита** и **Контроль безопасности**. Если компонент активен, он отмечен зелёным флажком , если нет — белым .

Вам доступны следующие кнопки:

1.  для взаимодействия с компонентом;
2. **Открыть отчет** для просмотра журнала действий компонента;
3. **Настройки** для изменения параметров компонента.

### Обновление

Данный раздел информирует об обновлениях модулей и баз данных. Программа отображает время последнего обновления.

Вам доступны следующие действия:

1. **Обновить** позволяет вручную обновлять модули и базы данных.
2. **Откатить** позволяет отменить обновления и вернуться к предыдущей версии.

Чтобы настроить параметры обновлений, нажмите . Параметры позволяют изменить:

* **Расписание обновления**

Нажмите для изменения режима запуска обновлений. По умолчанию установлен автоматический запуск.

* **Источники обновлений**

Источниками обновления по умолчанию установлены серверы обновлений «Лаборатории Касперского» и Kaspersky Security Center. Измените переключатель **Включено/Выключено** в графе **Статус**, чтобы изменить источник обновлений. Для добавления источника нажмите **Добавить**, для изменения — **Изменить**, для удаления — **Удалить**.

Источники по умолчанию не могут быть удалены.

* **Запуск обновлений с правами текущего пользователя**

Измените флажок, чтобы запускать обновления с правами другого пользователя.

* **Загрузку и установку обновлений модулей**

Установите флажок, чтобы включить обновление модулей. По умолчанию программа устанавливает только одобренные обновления. Измените флажок, чтобы разрешить установку критических и одобренных обновлений.

* **Копирование обновлений**

Установите флажок, чтобы включить копирование файлов обновления. Нажмите **Обзор**, чтобы указать путь к папке для копирования файлов.

* **Прокси-сервер для обновлений**

Нажмите **Настроить** для изменения настроек прокси-сервера.

Для сохранения изменений нажмите **Сохранить**, иначе — **Отмена**.

### Задачи

Задачи разделены на **Задачи проверки** и **Проверку целостности приложения**.

Измените переключатель **Показывать только запущенные задачи** в верхнем правом углу экрана, чтобы увидеть только запущенные проверки.

В Задачи проверки входят следующие задачи:

* Полная проверка;
* Проверка важных областей;
* Выборочная проверка;
* Проверка съемных дисков;
* Проверка из контекстного меню;
* Фоновая проверка.

Вам также доступны кнопки:

*  для изменения параметров;
*  для просмотра отчетов.

### Лицензия

Данный раздел информирует вас о действующих лицензиях. Вы можете узнать следующие сведения:

* Тип лицензии;
* Основные функции, которые предоставляет лицензия;
* Дата активации лицензии;
* Дата истечения срока лицензии;
* Ключ.

Чтобы удалить текущую лицензию, нажмите **Удалить**.

Вам доступны действия:

* **Купить лицензию** открывает интернет-магазин Kaspersky для приобретения новой лицензии:
* **Активировать приложение по коммерческой лицензии** запускает мастер активации для вашей программы.

## Лицензирование

Лицензирование заключается в выдаче пользователю лицензии на использование программного обеспечения. Лицензионное соглашение заключается между пользователем и АО «Лаборатория Касперского» как обладателем авторского права.

Вы можете ознакомиться с Лицензионным соглашением:

1. при установке с помощью мастера установки;
2. прочитав файл *license.txt*, который вы можете найти в папке с дистрибутивом.

Лицензионное соглашение содержит информацию о порядке предоставления, использования и активации лицензии, а также об условиях обработки данных и ограничениях для пользователей.

### Лицензия

Благодаря лицензии пользователь имеет право пользоваться приложением. Лицензия обладает ограниченным сроком и разным набором функций в зависимости от типа.

Для настоящей программы существует два вида лицензии:

* **Пробная лицензия** является бесплатной и предоставляется на месяц. По окончании срока программа приостановит свою работу.

Пробную лицензию можно получить только один раз при первичной установке.

* **Коммерческая лицензия** является платной и предоставляется на год. По окончании срока программа приостановит свою работу.

Для приобретения лицензии посетите [официальный сайт Kaspersky](https://www.kaspersky.ru/small-to-medium-business-security?campaign=kl-ru_buybutton_att_ona_inp_tri_onl_b2b_inp_inp-lnk___lnk-b_kes_21.20.8.505__&inp=0:kes:21.20.8.505:ru:2:1:32:26::LicenseManager&THRU&referer1=kl-ru_buybutton&referer2=kl-ru_buybutton_att_ona_inp_tri_onl_b2b_inp_inp-lnk___lnk-b_kes_21.20.8.505__).

Для активации перейдите в раздел **Активация лицензии**.

### Активация лицензии

Откройте главное окно приложения. Перейдите в раздел **Лицензия** и нажмите **Активировать приложение по коммерческой лицензии.** Откроется окно мастера активации.

Вы можете активировать лицензию двумя способами:

1. **С помощью кода активации**.

Код активации является уникальным и имеет следующий формат: XXXX-XXXX-XXXX-XXXX. Он указан в письме, которое вы получаете на электронную почту после приобретения лицензии. Скопируйте код в поле ввода и нажмите **Активировать**.

1. **С помощью файла ключа.**

Нажмите **Выбрать файл ключа**. В открывшемся окне выберите **Обзор** и укажите путь к файлу.