Руководство пользователя
Системы «Интернет-Банкинг» по установке ПО Kaspersky Fraud Prevention for Endpoints

(для Microsoft Windows)

Содержание:

Оглавление

1. Термины

1.1. Internet Explorer, Google Chrome, Mozilla Firefox, (бра́узер) – это программное обеспечение используемое для просмотра и работы с Web страницами.

1.2. Апплет– программное обеспечение e-Security Client разработанное компанией ТОО "Ak Kamal Security".

1.3. Прокси-Сервер - служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, файл), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кеша (в случаях, если прокси имеет свой кеш). В некоторых случаях запрос клиента или ответ сервера может быть изменен прокси-сервером в определенных целях.

1.4. Руткит - Программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в операционной системе.

В операционных системах Windows под руткитом принято подразумевать программу, которая внедряется в операционную систему и перехватывает системные функции (Windows API). Перехват и модификация низкоуровневых API-функций, в первую очередь, позволяет такой программе достаточно качественно маскировать свое присутствие в операционной системе. Кроме того, как правило, руткит может маскировать присутствие в операционной системе любых описанных в его конфигурации процессов, каталогов и файлов на диске, ключей в реестре. Многие руткиты устанавливают в операционную систему свои драйверы и службы (они также являются «невидимыми»)

2. О Kaspersky Fraud Prevention For Endpoints

Kaspersky Fraud Prevention for Endpoints предназначен для защиты конфиденциальных данных, которые Вы вводите на защищаемых веб-сайтах (например, номера банковской карты, пароля для доступа к сервисам интернет-банкинга), а также для предотвращения кражи платежных средств при проведении платежей онлайн.

Для безопасной работы с веб-сайтами используется Защищенный браузер – специальный режим работы браузера, который используется для защиты ваших данных при работе на веб-сайтах банков или платежных систем. Защищенный браузер запускается в изолированной среде, чтобы другие программы не могли внедриться в процесс Защищенного браузера.

Kaspersky Fraud Prevention for Endpoints создает специальные профили браузеров Mozilla Firefox и Google Chrome, чтобы установленные сторонние расширения не могли повлиять на работу Защищенного браузера. Программа не влияет на ваши данные, которые браузеры могут сохранять в созданных профилях.

Для работы в режиме Защищенного браузера в веб-браузерах должно быть установлено и включено расширение Kaspersky Protection. Веб-браузеры Mozilla Firefox и Google Chrome предлагают установить это расширение при первом запуске в режиме Защищенного браузера. Если вы отказались от установки расширения, вы можете установить его позднее вручную. В веб-браузере Internet Explorer® расширение Kaspersky Protection устанавливается и включается по умолчанию.

С помощью расширения Kaspersky Protection программа Kaspersky Fraud Prevention for Endpoints внедряет на веб-страницу, открытую в Защищенном браузере, скрипт. Программа использует этот скрипт для взаимодействия с веб-страницей.

При работе в Защищенном браузере программа предоставляет защиту от следующих видов угроз:

- Недоверенные исполняемые модули. Программа выполняет проверку на недоверенные исполняемые модули при запуске Защищенного браузера и далее с заданным интервалом во время работы Защищенного браузера.
- Руткиты. Проверка на наличие руткитов выполняется при запуске Защищенного браузера.
- Известные уязвимости операционной системы. Проверка на наличие уязвимостей операционной системы выполняется при запуске Защищенного браузера.
- Недействительные сертификаты веб-сайтов банков или платежных систем. Проверка сертификатов выполняется при переходе на веб-сайт банка или платежной системы. Проверка сертификатов выполняется по базе скомпрометированных сертификатов.

Kaspersky Fraud Prevention for Endpoints защищает конфиденциальные данные пользователя только на веб-страницах банков, предустановленных в программе. Программа не обеспечивает защиту конфиденциальных данных пользователя на веб-сайтах других банков.

Kaspersky Fraud Prevention for Endpoints выполняет следующие функции:

- защищает веб-адрес интернет-банкинга от изменения вредоносными программами;
- проверяет подлинность защищаемой веб-страницы с помощью службы проверки сертификата веб-сайта;
- защищает от атак на DNS-запросы;
- выполняет поиск, лечение и удаление активных и неактивных вредоносных программ;

- проверяет ваш компьютер на наличие уязвимостей в операционной системе, которые могут быть использованы для кражи персональных данных;
- защищает от перехвата персональные данные, которые вы вводите на веб-страницах, с помощью средств защиты ввода с аппаратной клавиатуры;

- проверяет веб-страницы, на которые вы переходите, на принадлежность к фишинговым веб-сайтам, как в обычном режиме работы веб-браузера, так и в Защищенном браузере;
- осуществляет поиск руткитов в памяти ядра операционной системы при запуске Защищенного браузера;
- предотвращает несанкционированное получение снимков экрана программами-шпионами;

Kaspersky Fraud Prevention for Endpoints не предотвращает получение снимков экрана с помощью нажатия на клавишу Print Screen.

- предотвращает копирование между незащищенными процессами.

Kaspersky Fraud Prevention блокирует несанкционированный доступ программ к буферу обмена во время проведения платежных операций, предотвращая кражу данных злоумышленниками. Блокировка действует только в случае попыток недоверенных программ получить несанкционированный доступ к буферу обмена. Если вы вручную копируете данные из окна одной программы в окно другой программы (например, из Блокнота в окно текстового редактора), доступ к буферу обмена разрешен. Если источником данных для копирования является браузер Internet Explorer, открытый в обычном режиме, в буфер обмена могут быть помещены только данные из адресной строки браузера.

Функциональность программы зависит от банка, который предоставил вам Kaspersky Fraud Prevention for Endpoints. В зависимости от указанных банком параметров установки программы в интерфейсе Kaspersky Fraud Prevention for Endpoints могут отсутствовать следующие окна:

- окно настройки параметров программы;
- окно отчетов;

3. Установка Kaspersky Fraud Prevention for Endpoints.

3.1. Для начала процесса, необходимо скачать ПО Kaspersky Fraud Prevention for Endpoints с сайта https://ib.bcc.kz/index_kav.html, во вкладке «Помощь и консультация» в форме «Полезные ссылки» (Рис.1)

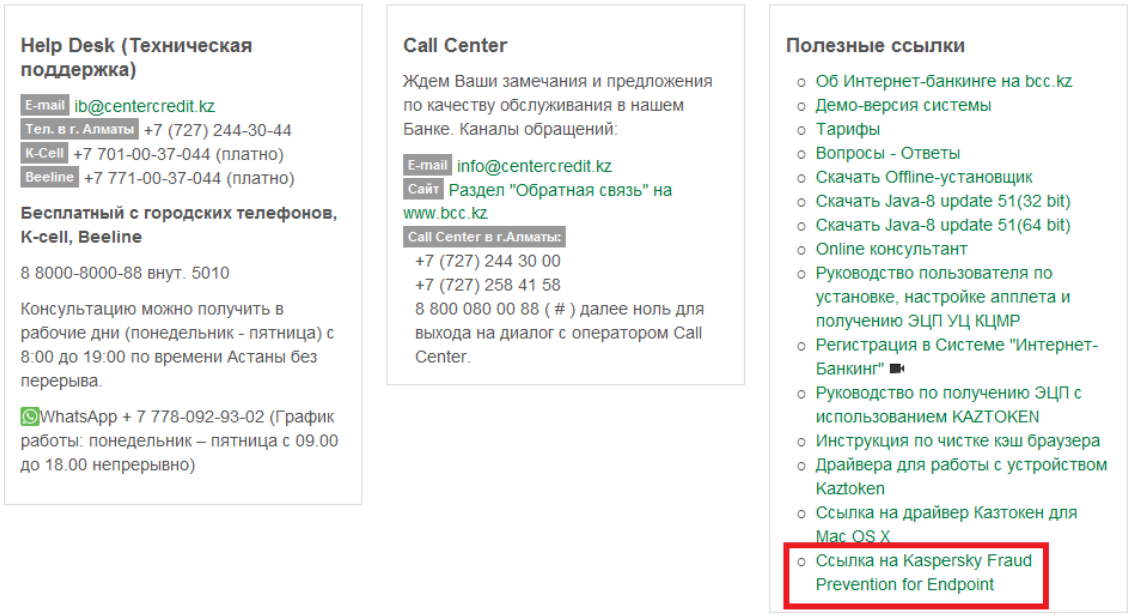

Рис. 1 - Ссылка на Kaspersky Fraud Prevention for Endpoint

3.2. После скачивания ПО, начать процесс установки (Рис. 2-5)

Рис. 2 – Нажать два раза на скачанный файл ПО Kaspersky Fraud Prevention for Endpoint.

Рис. 3 – Начало установки ПО Kaspersky Fraud Prevention for Endpoint, нажать на «Install and choose to participate in KSN» (выделено красным).

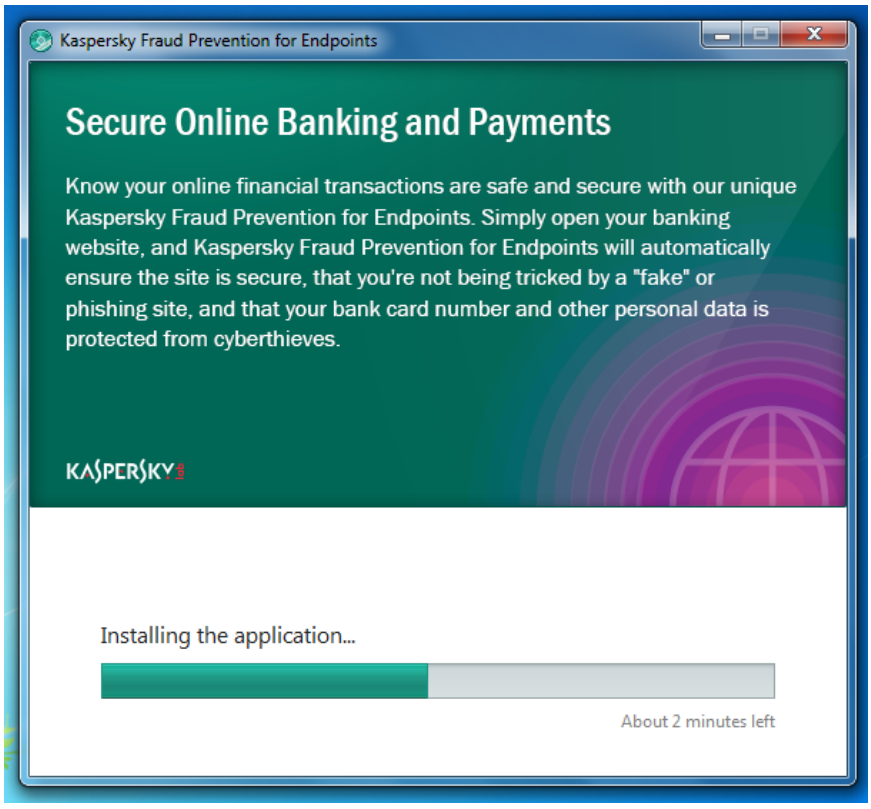

Рис. 4 – Процесс установки ПО Kaspersky Fraud Prevention for Endpoint

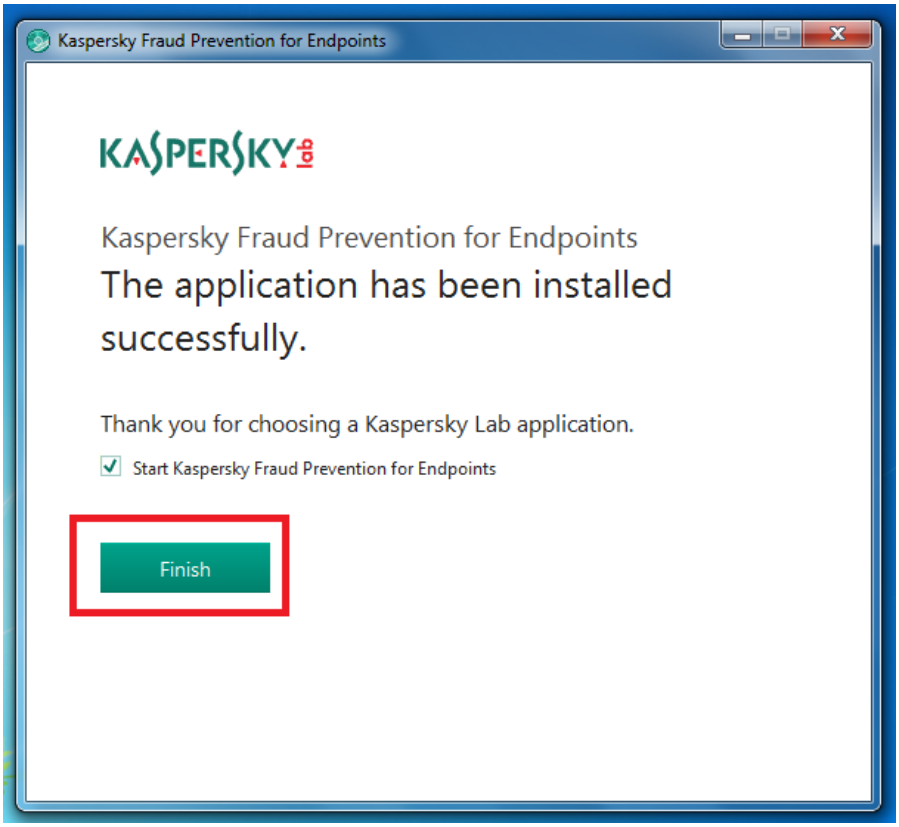

Рис. 5 – Завершение установки ПО Kaspersky Fraud Prevention for Endpoint

4. Вход в Систему «Интернет-Банкинг» с помощью ПО Kaspersky Fraud Prevention for Endpoints.

4.1. После установки ПО, на рабочем столе появиться ярлык по которому необходимо нажать два раза мышкой. (Рис.6)

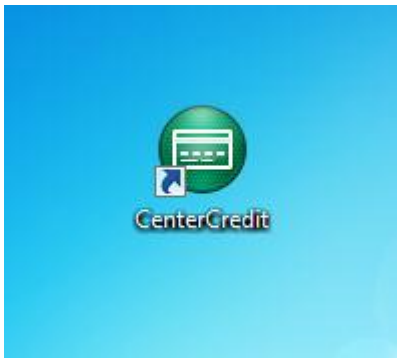

Рис. 6 – Ярлык на рабочем столе ПО Kaspersky Fraud Prevention for Endpoint

4.2. После запуска ярлыка в трее (в правом нижнем углу рабочего стола) появиться значок Kaspersky Fraud Prevention for Endpoint (выделено красным на Рис.7) а так же откроется защищенный браузер, где необходимо набрать в адресной строке адрес сайта https://ib.bcc.kz/index_kav.html, при этом в случае если Ваша операционная система не имеет последних обновлений, то может отобразиться сообщение о необходимости её обновления. Для

продолжения процесса Вам необходимо либо обновить ОС, либо нажать на «Ignore» (выделено красным на Рис. 8)

Рис. 7

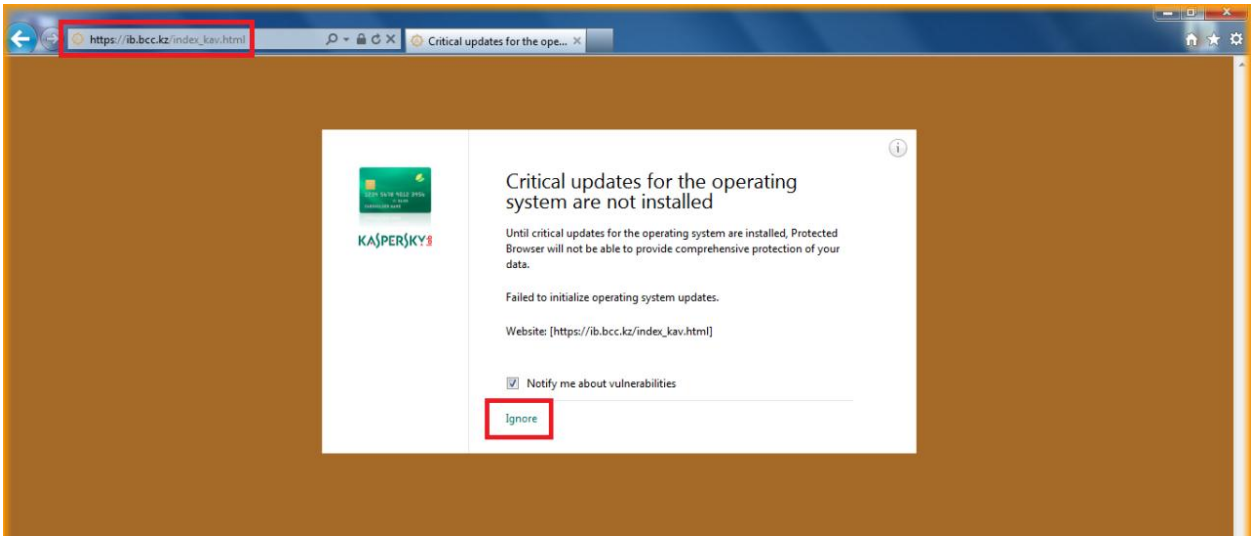

Рис. 8

4.3. После откроется сайт Системы «Интернет-Банкинг» ib.bcc.kz/index_kav.html, где надо нажать на «Войти в систему» (Рис. 9), в открывшемся апплете Ak Kamal e-Security Client авторизоваться (Рис. 10) и войти в систему (Рис. 11).

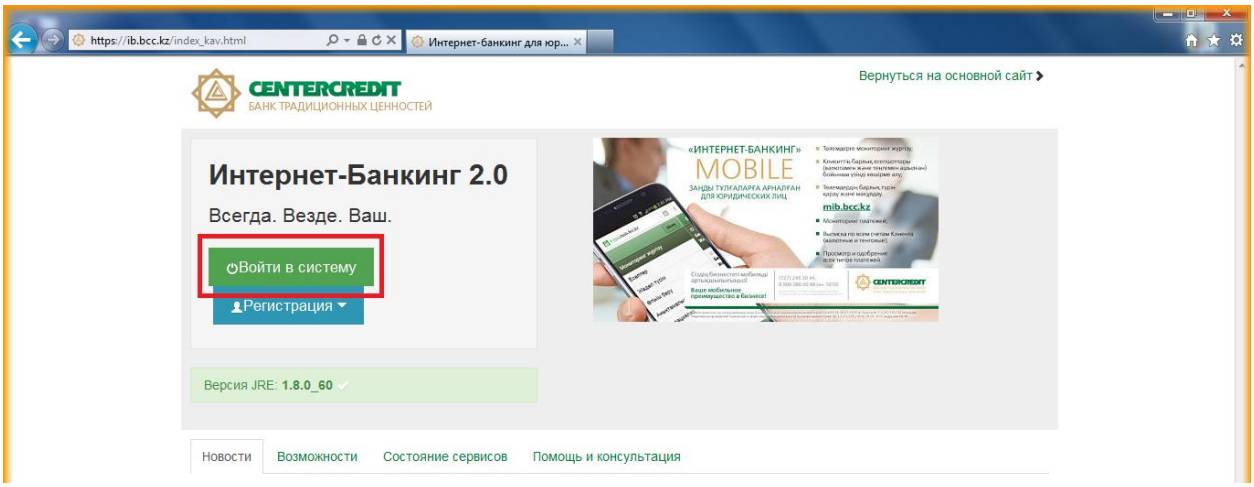

Рис. 9

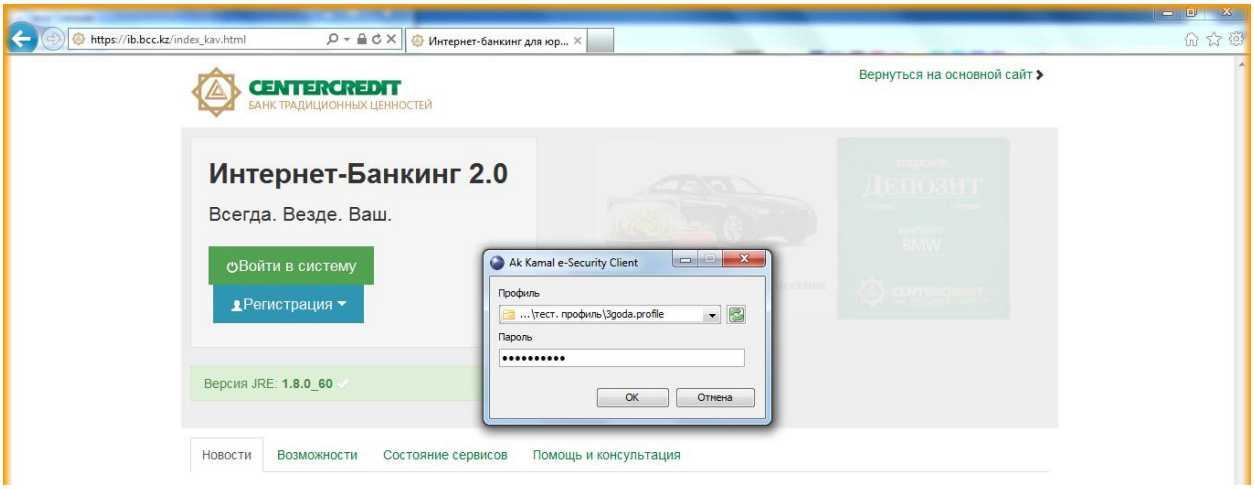
https://ib.bcc.kz/index_kav.html
Интернет-банкинг для юр...
CENTERCREDIT
БАНК ТРАДИЦИОННЫХ ЦЕННОСТЕЙ
Вернуться на основной сайт
Интернет-Банкинг 2.0
Всегда. Везде. Ваш.
Войти в систему
Регистрация
Ak Kamal e-Security Client
Профиль
...\тест. профиль\3goda.profile
Пароль
OK
Отмена
Версия JRE: 1.8.0_60
Новости
Возможности
Состояние сервисов
Помощь и консультация

Рис. 10

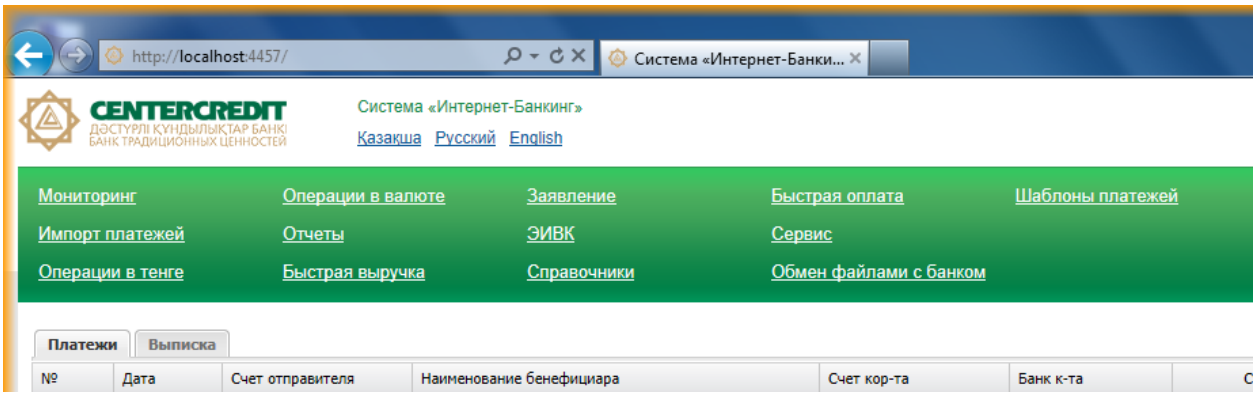
http://localhost:4457/
Система «Интернет-Банки...
CENTERCREDIT
ДӘСТҮРЛІ ҚҰНДЫЛЫҚТАР БАНКІ
БАНК ТРАДИЦИОННЫХ ЦЕННОСТЕЙ
Система «Интернет-Банкинг»
Қазақша Русский English
Мониторинг
Операции в валюте
Заявление
Быстрая оплата
Шаблоны платежей
Импорт платежей
Отчеты
ЭИВК
Сервис
Операции в тенге
Быстрая выручка
Справочники
Обмен файлами с банком
Платежи
Выписка
№
Дата
Счет отправителя
Наименование бенефициара
Счет кор-та
Банк к-та

Рис. 11

5. Аппаратные и программные требования

Для функционирования Kaspersky Fraud Prevention for Endpoints компьютер должен удовлетворять следующим требованиям:
Общие требования:

- 480 МБ свободного места на жестком диске.
- Подключение к интернету (для активации программы, а также обновления баз и программных модулей).
- Internet Explorer 8.0 или выше.
- Microsoft® Windows® Installer 3.0 или выше.
- Microsoft .NET Framework 4 или выше.

Требования для операционных систем Microsoft Windows XP Home Edition (Service Pack 3 или выше), Microsoft Windows XP Professional (Service Pack 3 или выше), Microsoft Windows XP Professional x64 Edition (Service Pack 2 или выше):

- процессор Intel® Pentium® 800 МГц 32-разрядный (x86) / 64-разрядный (x64) или выше (или совместимый аналог);
- 512 МБ свободной оперативной памяти.

Поддерживаемые браузеры:

- Microsoft Internet Explorer версий 8 - 11
- Mozilla Firefox версий 31.x – 38.x
- Google Chrome версий 36.x – 39.x

Браузеры Internet Explorer 10 в стиле Modern UI и Internet Explorer 11 в стиле нового интерфейса Windows не поддерживаются.

6. Совместимость Kaspersky Fraud Prevention for Endpoints с другими программами

Следующие программы «Лаборатории Касперского» совместимы с Kaspersky Fraud Prevention for Endpoints:

- Kaspersky Anti-Virus (2013, 2014, 2015)
- Kaspersky AVPTool (2011, 2012)
- Kaspersky Internet Security (2013, 2014, 2015)
- Kaspersky CRYSTAL 3.0
- Kaspersky Password Manager
- Kaspersky Small Office Security 4.0
- Kaspersky Endpoint Security 10 SP1 для Windows
- Kaspersky Total Security 4.0

Работа следующих компонентов программ Kaspersky Internet Security, Kaspersky Small Office Security и Kaspersky Total Security при совместной установке программ с Kaspersky Fraud Prevention for Endpoints ограничивается в Защищенном браузере:

- Веб-Антивирус, кроме Анти-Фишинга;
- Родительский контроль (для Kaspersky Internet Security и Kaspersky Total Security);
- Веб-контроль (для Kaspersky Small Office Security);
- Модуль проверки ссылок;
- Анти-Баннер.

Следующие программы сторонних производителей антивирусного программного обеспечения совместимы с Kaspersky Fraud Prevention for Endpoints:

- Norton Antivirus
- Norton Internet Security
- Norton 360™
- AVG Internet Security 2014
- AVG Antivirus 2014
- AVG Antivirus FREE 2014
- Avira Free Antivirus
- McAfee Internet Security
- McAfee AntiVirus Plus
- McAfee Total Protection™
- Microsoft Security Essentials 4.4 (or later)
- ESET NOD32 Antivirus 5
- ESET NOD32 Smart Security
- Avast! Free Antivirus
- Avast! Internet Security 2014
- Avast! Premier 2014
- Avast! Endpoint Protection Suite
- Avast! Endpoint Protection Suite Plus
- Trend Micro Titanium Internet Security
- DeviceLock DLP