

Hideez Key



РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Версия 1.3.5

Прошивка устройства 1.2
Приложение Hideez Safe для Windows 1.16
Приложение Hideez Safe для Android 2.7
Приложение Hideez Safe для iOS 1.1
Приложение Hideez Safe для Mac 1.2

© Hideez Group Inc, 2018

Оглавление

1. Общая информация	5
1.1. Декларация соответствия	5
1.2. Охрана окружающей среды	5
1.3. Ответственность	5
1.4. Изменения	5
1.5. Торговые марки	5
1.6. Обновления и исправления	5
1.7. Меры предосторожности	5
2. Технические характеристики	6
3. Системные требования	6
4. Гарантийные обязательства производителя	8
5. Соответствие стандартам	8
5.1. Заявление о соответствии требованиям Федеральной комиссии по связи (FCC)	8
5.2. Заявление о соблюдении FCC в области радиационного воздействия	8
6. Назначение Hideez Key	8
7. Принципы функционирования	9
8. Приступая к работе	10
8.1. Внешний вид и элементы управления	10
8.2. Замена батареи	10
8.3. Могут ли мои устройства работать с Hideez Key?	11
8.4. Режимы работы и меню управления Hideez Key	12
Hideez Key может находиться в одном из трех режимов:	12
В каждом из режимов нажатия на кнопку обрабатываются следующим образом.	12
8.5. Установка управляющей программы Hideez Safe	13
8.6. Регистрация аккаунта My Hideez	13
8.7. Сопряжение и инициализация Hideez Key	13
8.8. Сопряжение со следующим устройством	14
8.9. Поддержка постоянного соединения	15
8.10. Переключение между сопряженными устройствами	15
8.11. Отключение и стирание персональных данных Hideez Key	16

8.12. Обновление клиентского приложения Hideez Safe	16
8.13. Обновление микропрограммы Hideez Key	16
8.14. Обновление микропрограммы Hideez Key из режима загрузчика	17
9. Практическое применение Hideez Key	18
9.1. Контроль доступа к компьютеру	18
9.3. Настройка «Доверенные места» для Android и iOS устройств	20
9.4. Защита ПК Windows	20
9.5. Менеджер паролей	23
9.5.1. Работа с паролями в системе Android I iOS	23
Добавление паролей	24
Добавление уже существующего пароля приложению Android.	24
Применение паролей в iOS	25
Применение паролей в Android	25
Изменение и удаление аккаунтов менеджера паролей	26
9.5.2. Работа с паролями на компьютере Windows или Mac	26
Добавление и ввод паролей в интернет браузерах	26
Автоматическая генерация пароля	27
Смена пароля	27
Добавление и ввод паролей в десктоп-приложениях	28
Добавление паролей вручную	28
Выбор из нескольких подходящих аккаунтов	29
Импорт паролей	29
Экспорт паролей	29
Использование пароля по умолчанию	30
Настройка горячих клавиш	30
Удаление записей из Менеджера паролей	30
9.6. Одноразовые пароли (OTP) и двухфакторная авторизация	30
9.7. Резервное копирование и восстановление пользовательских данных	31
9.8. Охрана предметов и поиск Hideez Key со смартфона	33
9.8.1. Поиск брелока со смартфона	33
9.8.2. Координаты брелока на карте Google Maps в смартфоне.	34

9.9. Биометрическая идентификация пользователя Android	34
9.10. Использование RFID датчика	34
9.11. Датчик прикосновения (только для Android)	35
9.12. Действия по нажатию на кнопку (Android, Windows, Mac)	35
Windows	36
10. Веб-сервис my.hideez.com	37
Приложение 1. Возможные неисправности и их устранение	38
Приложение 2. Рекомендации по безопасной работе	39
Приложение 3. Сигналы и состояние Hideez Key	40
Приложение 4. Частые вопросы и ответы	41

1. Общая информация

1.1. Декларация соответствия

Компания Hideez Group Inc. заявляет, что данное изделие соответствует основным требованиям и другим положениям 199/5/WE.

1.2. Охрана окружающей среды

Устройство соответствует требованиям директивы WEEE 2002/96/EC. Символ  рядом с параметром означает, что продукт должен быть утилизирован отдельно и должен быть отправлен в соответствующие коллекторы. Это позволяет ограничить загрязнение окружающей среды и влияние на здоровье человека.

1.3. Ответственность

Компания Hideez Group Inc. и ее лицензиары не несут ответственности за потерю данных, информации, прибыли или получения других косвенных убытков вследствие использования нашего оборудования, если это не противоречит закону.

Компания Hideez Group Inc. не несет ответственности за любые проблемы, связанные с неправильной работой операционной системы и программ, работающих под ее контролем.

1.4. Изменения

Компания Hideez Group Inc. оставляет за собой право изменить этот документ или характеристики без предварительного уведомления. Функциональные возможности и изображения могут варьироваться в зависимости от услуг и версии установленного программного обеспечения. Снимки экранов в документе могут не совпадать с реальными. Внешний вид устройств может отличаться от реальных образцов.

1.5. Торговые марки

© Hideez являются зарегистрированными торговыми марками Hideez Group Inc. Bluetooth является зарегистрированной торговой маркой Bluetooth SIG, Microsoft® Windows™ – зарегистрированная торговая марка Microsoft Corporation. Google, Android и YouTube — товарные знаки Google, Inc. Все остальные упоминаемые продукты, торговые знаки и марки могут быть собственностью их уважаемых владельцев.

1.6. Обновления и исправления

Последняя версия программного обеспечения и Руководства пользователя находится на сайте: www.hideez.com/download

Онлайн-версия Лицензионного соглашения с пользователем может быть найдена на www.hideez.com/legal

1.7. Меры предосторожности

Прежде чем начать работу с устройством, пожалуйста, прочитайте этот раздел. Следующие советы помогут обеспечить безопасность Ваших данных и продлить срок службы устройства.

Не подвергайте устройство воздействию чрезмерно высоких или низких температур. Оберегайте его от попадания прямых солнечных лучей. Батарея внутри устройства не должна подвергаться сильному нагреву или охлаждению. Помните: рабочая температура устройства составляет от -10°C до 40°C.

Оберегайте устройство от воздействия открытого пламени или дыма (зажженная сигарета, зажигалка, костер и др.).

Не подвергайте устройство воздействию сильных электромагнитных полей.

Не роняйте устройство и не пытайтесь изогнуть. В случаях повреждения устройства обращайтесь в сервисный центр.

Данное устройство нельзя использовать под водой. При попадании устройства в воду незамедлительно выньте батарею и обращайтесь в сервисный центр.

Устройство принимает и излучает радиочастоты по стандарту Bluetooth® на небольшое расстояние, и не требует выключения на борту самолета, согласно указаниям FAA от 31.10.2013. При использовании личных медицинских устройств (таких как кардиостимуляторы и слуховые аппараты) проконсультируйтесь с врачом или производителем, чтобы узнать, защищены ли они от внешних радиочастотных сигналов.

Храните устройство в месте, недоступном для детей.

2. Технические характеристики

Процессор	Nordic nRF52 серия
Связь	Bluetooth 4.0 Low Energy
Питание	один элемент питания CR2032
Срок работы от одной батареи	до 6 месяцев
Габариты	32,5 x 32,5 x 9,5 мм
Вес	8 гр.
Рабочая температура	от -10 °С до +40°С
Кнопка	одна многофункциональная
Светодиодный индикатор (LED)	два (красный и зеленый)
RFID	125 КГц, стандарт HID и Em-Marine
Объем пользовательской памяти	72 Кб
Звук	70 Дб
Одноразовые пароли (OTP)	RFC 6238
Шифрование	AES-128, RSA-1024, ECC

3. Системные требования

Hideez Key предназначен для совместной работы с устройствами, отвечающим требованиям:

- Android 4.4 и выше
- iOS 9.3 и выше
- Windows 7, 8* (с применением внешнего USB Bluetooth адаптера), Windows 8.1 и выше
- MacOS 10.11 и выше

Устройство должно быть оснащено адаптером **Bluetooth версии 4.0** и выше с поддержкой режима Low Energy (Bluetooth Smart). Смотрите «[Могут ли мои устройства работать с Hideez Key?](#)».

*Операционные системы Windows до версии 8.1 могут не работать корректно с устройствами Bluetooth 4.0. Для работы на таких системах необходимо применение USB Bluetooth адаптера на базе чипа CSR 8510. Компания Hideez рекомендует использовать [Hideez Dongle](#). Разработчики Hideez Key не гарантируют корректную работу устройства с использованием непроверенных Bluetooth адаптеров.

Функция биометрической аутентификации (распознавание по отпечаткам пальцев) – TouchID работает только на операционной системе Android. Эта функция может быть использована, как для доступа к программе Hideez Safe, так и для входа на само Android устройство.

Программа Hideez Safe для **Windows** умеет работать с последними версиями наиболее популярных интернет браузеров – **Chrome, Firefox, Opera, Internet Explorer, Edge, Vivaldi**. В этих браузерах программа определяет доменное имя сайта с текущей вкладки и использует его для добавления или подстановки пароля. С остальными браузерами система работает как с обычным десктоп-приложением и вместо адреса домена использует заголовок открытой вкладки.

В системе **Android** программа Hideez Safe может вводить пароли в программы и веб сайты. Это работает для большинства программ, а также для браузеров **Chrome, Opera и Javelin**. Остальные браузеры не поддерживаются, так как не позволяют получить доступ к элементам ввода на своих страницах. Также автоматический ввод паролей может не работать с некоторыми Android приложениями, которые используют нестандартные элементы пользовательского интерфейса. В этом случае стоит обратиться в техподдержку с указанием названия и версии такого приложения для поддержки его в будущих версиях Hideez Safe.

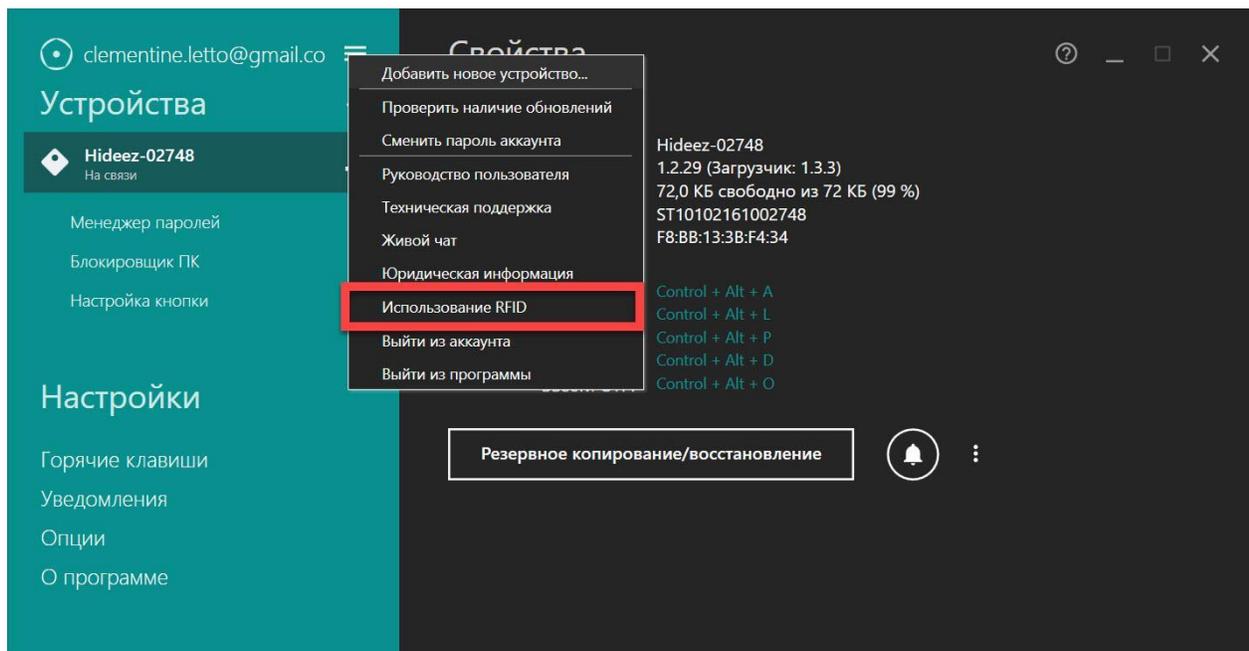
В iOS Hideez Safe работает только с браузером Safari и не может вводить пароли в приложения.

В MacOS Hideez Safe работает с браузерами Safari и Chrome, а также с приложениями для MacOS.

[Модуль RFID](#) работает в двух стандартах – HID или Em-Marine и является **НЕ совместимым с модулями NFC**, установленными в смартфонах и планшетах.

Работа модуля RFID не связана с приложением Hideez Safe.

Информацию по использованию RFID можно посмотреть в статье из блога на сайте либо перейти в приложении Hideez Safe, выбрав соответствующий пункт меню (Использование RFID):



Примечание: программное обеспечение Hideez Key и Hideez Safe постоянно совершенствуется, список поддерживаемых операционных систем будет со временем расширяться, следите за обновлениями.

4. Гарантийные обязательства производителя

Гарантийный срок эксплуатации 12 месяцев со дня продажи устройства при наличии гарантийного талона, чека и соблюдения условий хранения и использования.

5. Соответствие стандартам

5.1. Заявление о соответствии требованиям Федеральной комиссии по связи (FCC)

Устройство соответствует требованиям части 15 правил FCC. При эксплуатации устройства необходимо учитывать следующие два обстоятельства: (1) данное устройство не является источником неблагоприятного воздействия; (2) данное устройство должно принимать любые сигналы помех, в том числе сигналы, которые могут привести к его неправильному функционированию.

5.2. Заявление о соблюдении FCC в области радиационного воздействия

Оборудование соответствует нормам FCC по радиочастотному излучению в неконтролируемой среде. Передатчик не должен располагаться рядом с другой антенной или передатчиком, а также не должен принимать от них сигналов.

6. Назначение Hideez Key

Электронный ключ Hideez Key (метка) предназначен для идентификации пользователя на электронных устройствах - компьютер, планшет, смартфон; хранения ключей шифрования, паролей, логинов и прочих пользовательских данных; выполнения операций шифрования, хеширования и электронной подписи; генерации одноразовых паролей (OTP); идентификации пользователя по протоколу RFID (125 кГц стандарт HID и Em- Marine).

Для использования Hideez Key требуется установка дополнительного программного обеспечения «Hideez Safe» которое позволяет:

- Блокировать/разблокировать доступ к компьютеру, планшету основываясь на оценке расстояния по уровню принимаемого сигнала Bluetooth (RSSI).
- Хранить пользовательские пароли и логины для программ и веб-сервисов.
- Генерировать одноразовые пароли для сервисов, использующих двухфакторную аутентификацию по спецификации RFC 6238, (например, сервисы Google, Microsoft, Dropbox, Facebook).
- Выполнять внутри Hideez Key операции шифрования и цифровой подписи данных по стандартам AES-128, RSA-1024, ECC.
- Обновлять программное обеспечение внутри Hideez Key (прошивку) по каналу Bluetooth;
- Дистанционно (по Bluetooth) выключать компьютер;
- Запускать исполняемый файл.

Использование Hideez Key совместно с телефоном/планшетом на операционной системе Android дополнительно позволяет:

- Предотвращать забывание и утерю самого Hideez Key, а также личных вещей к которым он может крепиться, контролируя наличие связи по Bluetooth;
- Для входа в программу использовать аутентификацию пользователя по технологии сканирования отпечатков пальцев (TouchID);
- Делать фотографии нарушителя в случае попытки доступа к смартфону без присутствия Hideez Key;
- По нажатию кнопки выполнять заранее запрограммированные действия и их последовательности (скрипты), такие как: включение аудио или видеозаписи, отправка СМС, инициализация телефонного вызова, включение звукового сигнала, включение фонарика, фотосъемка (селфи);

- Отправлять на заданный номер телефона текущие географические координаты (режим "тревожная кнопка");
- Запоминать и отображать в приложении на смартфоне координаты места, где в последний раз была связь с меткой.

Примечание: программное обеспечение Hideez Key и Hideez Safe постоянно совершенствуется, список возможностей расширяется, следите за обновлениями.

7. Принципы функционирования

Электронное устройство Hideez Key взаимодействует со смартфонами, планшетами и компьютерами с помощью радиосвязи по стандарту Bluetooth 4.0 Low Energy на частоте 2.4 ГГц.

Указанный стандарт обеспечивает минимальные затраты электроэнергии на поддержание связи, а также обладает криптографической защитой канала передачи данных.

Дальность стабильной связи в условиях прямой видимости двух устройств до 100 метров, в помещении – до 25 метров. Фактический уровень сигнала зависит от расстояния, окружающих предметов, наличия на пути преград, в том числе человеческого тела, что влияет на расстояние связи и выполнение заявленных функций.

Устройство может измерять уровень принимаемого сигнала (RSSI), и таким образом приблизительно оценивать расстояние между подключенными устройствами. Эта возможность положена в основу значительной части охранной и сигнализирующей функциональности.

Параметры установленного соединения с другим Bluetooth устройством хранятся внутри Hideez Key. Набор таких параметров далее называется бонд (bond). Hideez Key может помнить восемь бондов, что составляет список из восьми «знакомых» устройств. Установление соединения с девятым и следующими устройствами вызывает удаление из списка наиболее старого.

Также Hideez Key оборудован радио модулем RFID, работающем на частоте 125 КГц. Подробнее о работе RFID смотрите [здесь](#).

Для работы с Hideez Key по протоколу Bluetooth требуется установка на сопряженное устройство программного обеспечения Hideez Safe. Подробные инструкции по установке смотрите далее в этом руководстве. Для работы RFID дополнительное ПО не требуется.

Замечание: для нормальной работы Bluetooth может понадобиться отключить некоторые функции энергосбережения на смартфонах и планшетах, так как эти режимы могут отключать Bluetooth или блокировать выполнение фоновых сервисов.

8. Приступая к работе

8.1. Внешний вид и элементы управления

Устройство Hideez Key выполнено в форме брелока и имеет многофункциональную кнопку, под которой находятся зеленый и красный светодиодные индикаторы.

Внутри корпуса находится источник звука (buzzer) который используется для подачи звуковых сигналов и предупреждений.

На основной плате находится Bluetooth антенна.

Под верхней крышкой корпуса находится RFID антенна с модулем управления. Этот модуль не связан с основной платой.

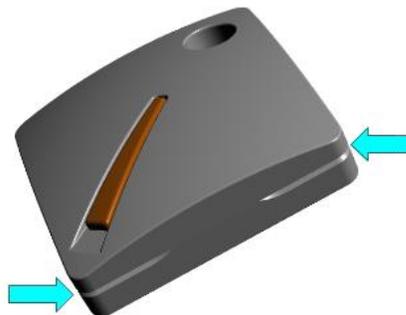


Внешний вид:

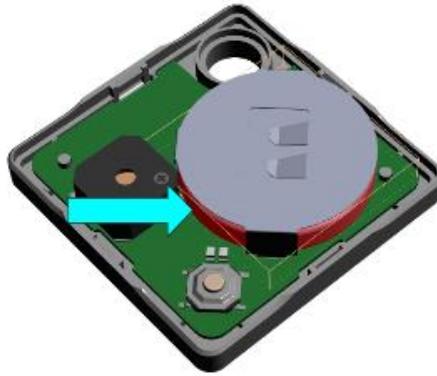
1. Многофункциональная кнопка
2. Зеленый и Красный LED индикатор
3. Отверстие для крепления брелока

8.2. Замена батареи

Устройство поставляется в собранном виде с установленной батареей. Корпус устройства состоит из двух половинок, которые крепятся защелками. Для замены батареи - раскройте корпус, поддев щель между половинками ногтем или пластиковой карточкой (не используйте металлические предметы). Извлеките старую батарею, нажав на нее с внутренней стороны узким пластиковым предметом. Установите новую батарею CR2032 узкой стороной (минусовой контакт) к плате. Hideez Key выдаст звуковой сигнал, после чего будет готов к работе.



Вскрытие корпуса



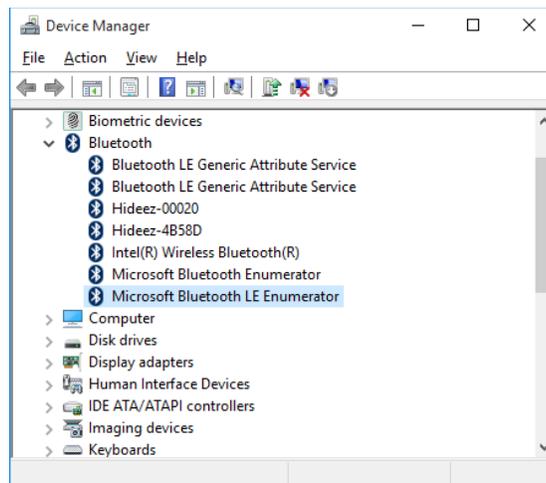
Извлечение батареи

Примечание: если вы не хотите менять батарею самостоятельно, то можете воспользоваться услугами сервисных точек по замене батареек в часах и прочих электронных устройствах.

8.3. Могут ли мои устройства работать с Hideez Key?

Перед приобретением Hideez Key необходимо убедиться, что ваш телефон, компьютер и планшет сможет с ним работать.

Для этого в **системе Windows** откройте Диспетчер Устройств, затем закладку Bluetooth и убедитесь, что там присутствует элемент под названием Microsoft Bluetooth LE Enumerator.



Если в системе нет Microsoft Bluetooth LE Enumerator, значит ваша система не поддерживает режим Low Energy. Если нет закладки Bluetooth, значит в вашей системе вообще не установлен Bluetooth адаптер. В обоих случаях вы можете приобрести внешний адаптер, который подключается по USB. (Рекомендуется [Hideez Smart Bluetooth dongle](#)). Обратите внимание, что некоторые производители Bluetooth адаптеров заявляют поддержку режима Low Energy, но работают через свое собственное ПО и Windows не распознает такие устройства как Bluetooth адаптер (в списке устройств не появится Microsoft Bluetooth LE Enumerator). В этом случае Hideez Safe работать не сможет.

На устройстве с Android можно скачать из Google Play приложение для проверки поддержки режима Bluetooth Low Energy, например, [BLE Checker](#). Если после запуска программы появится надпись “BLE Supported”, значит ваша система поддерживается.

8.4. Режимы работы и меню управления Hideez Key

Hideez Key может находиться в одном из трех режимов:

Режим 1 – Подключено

Hideez Key на связи с центральным устройством (Windows, Android) посредством Bluetooth.

Один раз в 4 секунды мигает зеленый светодиод.

Если устройство подключено и один раз в 4 секунды мигает красный светодиод, это означает необходимость замены батареи.

Режим 2 – Не подключено

Существует два варианта этого режима:

- a) Устройство выполняет поиск по списку «знакомых» устройств для того чтобы установить соединение.
- b) Устройство выполняет поиск всех окружающих Bluetooth устройств, при этом является видимым и открытым для сопряжения с каждым из них.

Режим 3 - Выключено

В каждом из режимов нажатия на кнопку обрабатываются следующим образом.

Режим 1 – Подключено

- короткие нажатия от одного до восьми отправляют событие с соответствующим номером на подключенное устройство (телефон, планшет или компьютер). Там это событие обрабатывается в приложении Hideez Safe, которое выполняет заранее назначенное для такого события действие.
- длинное нажатие 2-4 секунды (с удерживанием кнопки) отключает Hideez Key от текущего устройства (телефона, планшета или компьютера) и подключает к другому из списка известных. Если известных устройств нет рядом, то Hideez Key через 30 секунд восстановит соединение с первоначальным устройством.
- Более 9 коротких нажатий – выполняет вход в системное меню Hideez Key (зеленый светодиод горит постоянно). В этом режиме короткие нажатия на кнопку выполняет действия из списка:
 - 3 нажатия - удаление текущего набора параметров связи и отключение связи.
 - 4 нажатия – сообщает количество сохраненных бондов с помощью коротких звуковых сигналов (используется для целей отладки)
 - 5 нажатий - переход в режим загрузчика (bootloader).
- Длинное нажатие (10 секунд) выключает Hideez Key.

Режим 2 - Не подключено

- Одно короткое нажатие на кнопку делает устройство доступным для подключения.
- Более 9 коротких нажатий – вход в системное меню, как в пункте 1 (Подключено). Пункты меню аналогичны описанным в этом пункте, кроме следующего:
 - 3 нажатия – удаляет не просто текущее соединения, а вообще все связи с известными устройствами.
- Длинное нажатие (10 секунд) выключает Hideez Key.

Режим 3 – Выключено

- Одно короткое нажатие включает Hideez Key, который сразу начинает поиск устройств для подключения.
- Длинное нажатие (10 секунд) включает устройство в режиме загрузчика (bootloader).

8.5. Установка управляющей программы Hideez Safe

Для смартфона: установите приложение Hideez Safe из [Google Play](#) или [AppStore](#). После установки на экране уведомлений появится иконка .

Для Windows ПК или Mac: загрузите инсталляционный пакет Hideez Safe с сайта <http://hideez.com/download>, запустите его и следуйте пошаговым инструкциям установки. Для установки понадобятся права администратора. Смотрите видеоролик [по установке программы](#) на канале <youtube.com/hideez>.

Программа предусматривает загрузку и установку обновлений с сайта [Hideez.com](#). Некоторые антивирусы считают такую возможность вредоносной и предупреждают об опасности. Если Ваша антивирусная программа не позволяет установить Hideez Safe, отключите ее на время установки, затем включите снова.

После установки на системной панели появится значок . По нажатию на этот значок откроется основное окно программы.

8.6. Регистрация аккаунта My Hideez

Система Hideez является критически важным компонентом информационной инфраструктуры пользователя, поскольку является беспроводным средством аутентификации пользователя, беспроводным аппаратным менеджером паролей, средством генерации одноразовых паролей, а также средством шифрования и электронной подписи. Важным элементом системы защиты данных пользователя является облачный сервис My Hideez. Обратите внимание, что этот сервис не хранит данные пользователя (логины, пароли). Он используется исключительно в целях верификации аппаратных устройств Hideez Key, микропрограмм, прикладного ПО, обеспечения зашифрованных каналов передачи данных и т.п.

Более полная информация о мерах защиты информации содержится в отдельном документе Hideez Security White Paper.

Для начала использования Hideez Key Вам необходимо пройти регистрацию в онлайн-системе <my.hideez.com> и привязать Hideez Key к своему аккаунту. После этого им можно будет пользоваться без подключения к Интернет. Такая привязка не позволит подключить Hideez Key к любому другому компьютеру/телефону без знания пароля вашего аккаунта. Смотрите видеоролик [по регистрации пользователя](#) на канале <youtube.com/hideez>.

Указать аккаунт и пароль необходимо при первом запуске программы. Если такой аккаунт еще не создан, его можно создать. Выберите «Зарегистрируйтесь сейчас». В открывшейся веб-странице укажите адрес своей электронной почты в качестве логина и создайте новый пароль. На указанный адрес будет отправлено письмо-подтверждение. После перехода по ссылке, указанной в нем, регистрация будет завершена.

Примечание: если Вы забудете пароль к вашему аккаунту его можно восстановить с помощью email через сервис <my.hideez.com>. Если же вы потеряете и доступ к почте, тогда вы потеряете возможность зарегистрировать и использовать Hideez Key с другими устройствами.

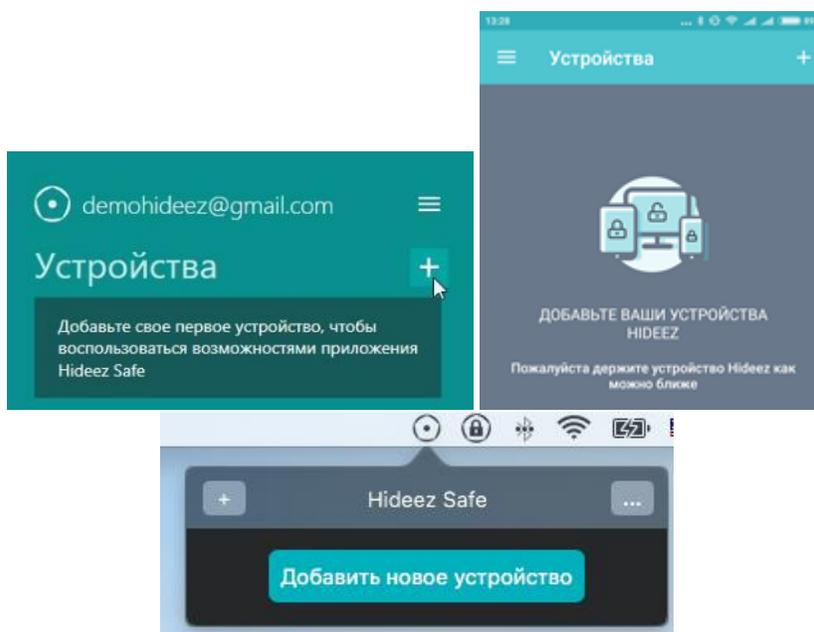
8.7. Сопряжение и инициализация Hideez Key

Инициализация устройства – это процедура обмена ключами шифрования канала Bluetooth, а также загрузка ключа шифрования пользователя. Ключ пользователя передается в зашифрованном виде с веб-сервиса Hideez и не может быть перехвачен. Напротив, ключи шифрования канала Bluetooth потенциально могут быть перехвачены и использованы для последующей расшифровки обмена

данными. Поэтому эту процедуру следует выполнять в безопасном окружении, где исключена возможность использования подслушивающего оборудования. Для минимизации риска мощность радиопередатчика занижается в момент инициализации подключения, поэтому Hideez Key нужно расположить как можно ближе к ПК/телефону. После инициализации канал связи будет зашифрован и защищён от перехвата.

Поскольку для инициализации Hideez Key используется веб-сервис, требуется подключение к сети Интернет. После окончания инициализации, работа с устройством возможна без подключения к сети.

В главном окне приложения Hideez Safe нажмите кнопку [+] (добавление нового устройства).



Добавление нового устройства на Windows, Android, MacOS

Затем нажмите кнопку Hideez Key. Устройство включится на 60 секунд и станет видимой для программы Hideez Safe. При этом устройство медленно мигает зеленым цветом.

На телефоне или компьютере Hideez Key виден в Bluetooth-окружении под именем Hideez-XXXXX, где XXXXX – последние цифры серийного номера.

После обнаружения Hideez Key, выберите его из списка и следуйте экранным инструкциям Помощника добавления. На одном из этапов потребуется ввести пароль вашего My Hideez аккаунта.

Если регистрация по какой-то причине не завершилась, Hideez Key отключится через 60 секунд. Его нужно удалить из списка устройств и выполнить всю процедуру заново.

После завершения регистрации Hideez Key остается включенным. Батареи должно хватить на период до 6 месяцев работы, в зависимости от интенсивности использования и качества самой батареи. Наибольший расход энергии происходит при использовании звуковых сигналов.

8.8. Сопряжение со следующим устройством

При установлении связи между двумя Bluetooth устройствами одно из них является ведущим, второе – ведомым. Обычно Hideez Key выступает в качестве «ведомого», и согласно спецификации Bluetooth может быть подключено только к одному ведущему устройству в один момент времени. Кроме того, когда Hideez Key подключен, он не виден для обнаружения третьими устройствами.

Для создания нового подключения, необходимо отключить Hideez Key от предыдущего устройства, (удалить устройство за пределы действия сигнала или же просто выключить в нем Bluetooth).

Подключение нового устройства выполняется аналогично тому, как описано в предыдущем пункте.

Хотя возможно только одно активное подключение, Hideez Key может хранить набор параметров связи для 8 устройств и может переключаться между ними. Если выполняется подключение к 9-му устройству, то наиболее старое удаляется из списка.

8.9. Поддержка постоянного соединения

Hideez Key рассчитан на круглосуточный режим соединения со своим ведущим устройством. Если связь разрывается вследствие большого расстояния между устройствами, она восстанавливается автоматически при их сближении. Если с Hideez Key было сопряжено несколько устройств, то он подключится к тому из них, кто первый его «обнаружит».

Для того чтобы обнаружить Hideez Key телефон или ПК должны выполнять периодическое сканирование Bluetooth канала. Постоянное сканирование нецелесообразно по нескольким причинам:

- В момент сканирования Bluetooth антенна не может использоваться для связи с другими устройствами.
- Сканирование потребляет больше энергии, что может сказаться на продолжительности работы от аккумулятора.
- Многие адаптеры совмещают модули Bluetooth и Wi-Fi и используют единую антенну. Поскольку сканирование Bluetooth окружение полностью занимает антенну, она не может использоваться для связи с Wi-Fi и скорость работы в сети падает.

Алгоритм сканирования Bluetooth в ПО Hideez Safe постоянно подстраивается исходя из использования программы и времени с момента последней потери связи. Однако, при подключении Hideez Key, могут возникать задержки в 10-15 секунд.

Примечание: Драйвера Bluetooth адаптеров в операционных системах не всегда работают стабильно. При интенсивном использовании, особенно когда часто выполняется переподключение различных устройств, адаптер может «зависать». Выражается это в невозможности подключить или просканировать Bluetooth устройства. Часто при этом помогает программное выключение и последующее включение адаптера. Иногда требуется перезагрузить компьютер.

8.10. Переключение между сопряженными устройствами

Hideez Key может переключаться между несколькими известными устройствами. Для этого нужно выполнить долгое (от 2 до 4 секунд) нажатие на кнопку. При этом Hideez Key отключается от текущего устройства и отправляет приглашение остальным устройствам из своего списка. То устройство, которое первое обнаружит Hideez Key, выполнит подключение.

Если эти устройства не отзываются, или в списке только одно устройство, Hideez Key снова подключается к первоначальному устройству.

Возможно, в силу разных мощностей блютуз передатчика и приемника, какое-либо из находящихся в списке подключенных устройств будет быстрее обнаруживаться и чаще подключаться при переключении. Тогда, на устройстве, которое чаще подключается, но на данный момент не используется, следует временно отключить Bluetooth.

При переключении между устройствами возможна задержка до 10 секунд по причинам, описанным в предыдущем разделе.

8.11. Отключение и стирание персональных данных Hideez Key

Для передачи Hideez Key другому лицу, необходимо выполнить команду «Отвязать от аккаунта». По этой команде из Hideez Key стираются все пользовательские данные, включая пароли и ключи шифрования. После этого Hideez Key становится «чистым» и его можно привязать к другому аккаунту.

Для выполнения этой команды необходимо наличие Интернет соединения. В процессе удаления необходимо будет ввести пароль от аккаунта My Hideez.

Если передать Hideez Key другому лицу, не отвязав ее от своего аккаунта, то при попытке подключения новый пользователь получит сообщение об ошибке: «Устройство зарегистрировано на другого пользователя». Он не сможет инициализировать устройство или прочитать данные. В этом случае нужно «отвязать» устройство от аккаунта удаленно, воспользовавшись [сервисом my.hideez.com](http://сервисом.my.hideez.com). Когда Hideez Key будет отвязан на веб-сервере, клиентская программа на телефоне/ПК вначале выполнит команду полного сброса и очистки метки, а затем ее можно будет использовать.

Примечание: если Вы потеряли Hideez Key, не удаляйте его из своего аккаунта. Никто не сможет его использовать или прочитать данные, если не знает пароль от вашего аккаунта. Если же вы удалите Hideez Key из своего аккаунта, то таким образом вы просто разрешите его сбросить и использовать как чистое устройство.

8.12. Обновление клиентского приложения Hideez Safe

Клиентское ПО Hideez Safe регулярно обновляется – добавляются новые функции, локализации на другие языки, исправляются ошибки и повышается удобство и стабильность работы.

Для приложения Hideez Safe для смартфона обновление выполняется так же, как и для любого другого ПО, установленного через Google Play или AppStore.

Приложение Hideez Safe для ПК самостоятельно проверяет наличие обновлений. Пользователь может также инициировать проверку по команде «Проверить наличие обновлений». Уведомление о наличии новой версии будет показано на главном экране приложения. Нажав кнопку [Обновить], вы запустите процесс скачивания и установки.

8.13. Обновление микропрограммы Hideez Key

Встроенное программное обеспечение (далее - прошивка или firmware) Hideez Key постоянно совершенствуется. Пользователь может получить новые возможности, обновив прошивку через клиентское приложение Hideez Safe. Регулярная проверка обновлений выполняется автоматически. Пользователь может также инициировать ее самостоятельно по команде «Проверить наличие обновлений» в меню программы Hideez Safe.

Перед обновлением прошивки рекомендуется обновить клиентское приложение Hideez Safe.

В процессе обновления расположите Hideez Key как можно ближе к сопряженному устройству для достижения наиболее быстрого и устойчивого соединения.

Микропрограмма состоит из двух компонент – загрузчика (bootloader) и, собственно, прошивки. Загрузчик выполняет функцию загрузки микропрограммы по Bluetooth и последующей ее замены внутри Hideez Key. Прошивка содержит всю прикладную логику работы. Загрузчик также может быть обновлен, но выполняется это значительно реже, чем обновление прошивки.

Чтобы выполнить обновление микропрограммы, нужно:

- Подключить Hideez Key к планшету или ПК с установленной программой Hideez Safe.
- Убедиться, что батарея Hideez Key заряжена (нет уведомления о низком заряде).
- Подключить планшет или ПК к Интернет
- В программе Hideez Safe выбрать пункт меню «Проверить наличие обновлений» и следовать указаниям на экране

Обновление микропрограммы из ОС Windows происходит сложнее, чем обновление из Android, поскольку Windows не позволяет программно подключать и отключать Bluetooth устройства. В процессе обновления пользователю будет предложено несколько раз добавлять и удалять Bluetooth устройства в системном окне настроек Bluetooth. Обратите внимание, что всегда нужно добавлять или удалять устройство с именем, которое начинается на “v23”, например, “v23-Hideez-12345”.

В случае, если обновления не устанавливались долгое время, может потребоваться обновление в несколько этапов. Например, сначала установить последнюю версию прошивки 1.1, затем последнюю версию прошивки 1.2 и т.д.

Примечание: образ микропрограммы, который загружается с сайта Hideez, подписан и зашифрован приватным ключом Hideez. Это исключает подмену прошивки и внедрение вредоносного кода внутрь Hideez Key.

8.14. Обновление микропрограммы Hideez Key из режима загрузчика

Если по каким-то причинам произойдет сбой в процессе обновления микропрограммы, то Hideez Key может остаться в режиме загрузчика – постоянно горит зеленый светодиод, когда устройство не подключено или красный, когда подключено.

В этом режиме Hideez Key виден для обнаружения под именем “v23-Hideez-XXXXX”, где XXXXX – последние пять цифр серийного номера.

Подключите Hideez Key как обычно, используя функцию добавления нового устройства в Hideez Safe. Такое устройство будет иметь ограниченный функционал: только возможность обновить прошивку или удалить устройство. Выполните команду проверки наличия обновлений, а затем само обновление. Следуйте пошаговым инструкциям.

Частой причиной сбоя при обновлении прошивки является разряженная батарея. В этом случае замените ее на новую. Рекомендуется во время обновления не использовать Wi-Fi на сопряженном телефоне/компьютере, чтобы не ухудшить качество Bluetooth соединения.

Примечание: в режиме загрузчика батарея расходует намного сильнее, чем в обычном режиме работы. Не оставляйте включенную Hideez Key в этом режиме надолго. Если по каким-то причинам не удастся обновить прошивку, выньте батарею и обратитесь в службу техподдержки.

9. Практическое применение Hideez Key

9.1. Контроль доступа к компьютеру

Сегодня существует множество способов аутентификации пользователя - с помощью пароля, смарт-карты и ПИН-кода или биометрической аутентификации. Hideez предоставляет еще один способ – с помощью физического присутствия ключа рядом с устройством, к которому нужно получить доступ. Это дает максимальное удобство и высокий уровень безопасности, но предъявляет высокие требования к надёжному хранению самого Hideez Key.

Вы можете использовать функцию контроля доступа с помощью Hideez Key к Windows ПК или Mac

9.2. Настройки программы

Основные настройки программы доступны во вкладке боковой панели - **Опции**

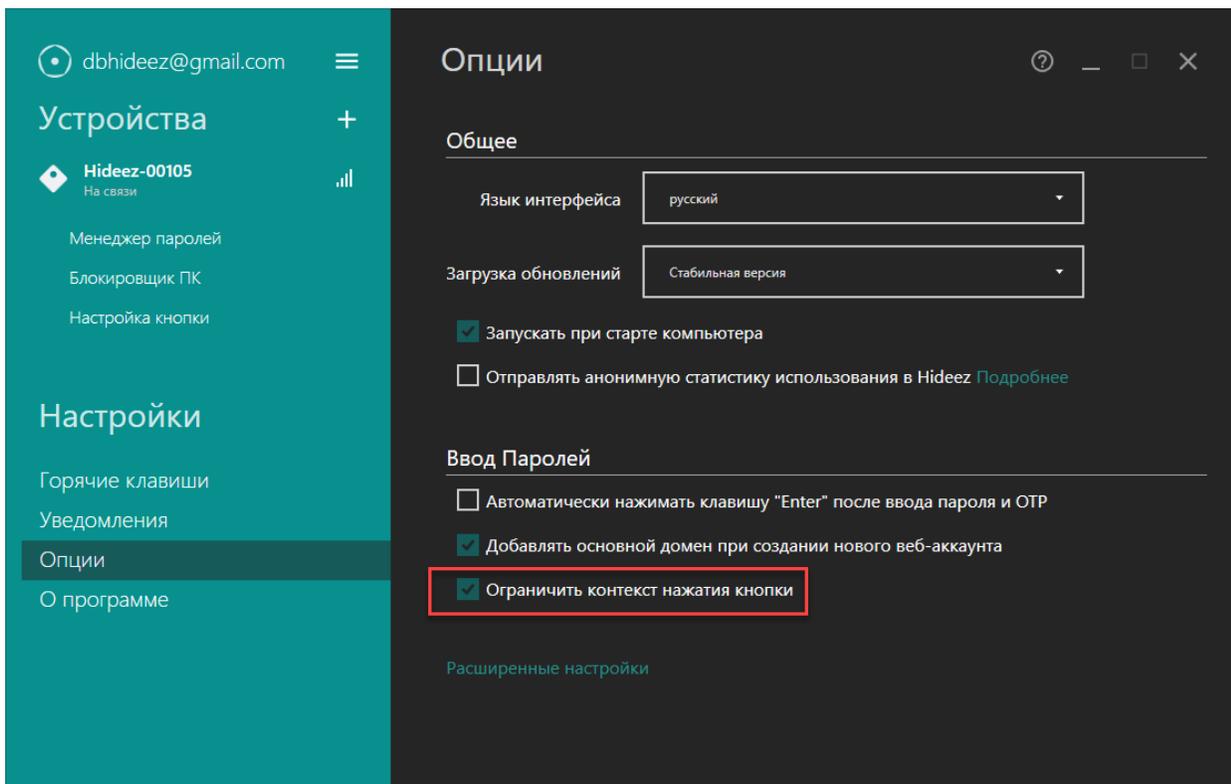
В меню **Опции** вы можете:

- выбрать язык интерфейса - доступны: English, Українська, Русский,
- выбрать ветку загрузки обновлений- Стабильная версия, Бета версия
- убрать (поставить) флажок запуска программы при старте компьютера (По умолчанию программа запустится автоматически после запуска (перезагрузки) вашего компьютера, ноутбука, планшета)
- поставить (убрать) флажок - Отправлять анонимную статистику использования в Hideez и ознакомиться с правилами сбора статистики Подробнее (<https://hideez.com/legal>)
- поставить (убрать) флажок - Автоматически нажимать клавишу “Enter” после ввода пароля и OTP
- убрать (поставить) флажок - Добавлять основной домен при создании нового веб-аккаунта
- поставить (убрать) флажок - Ограничить контекст нажатия кнопки

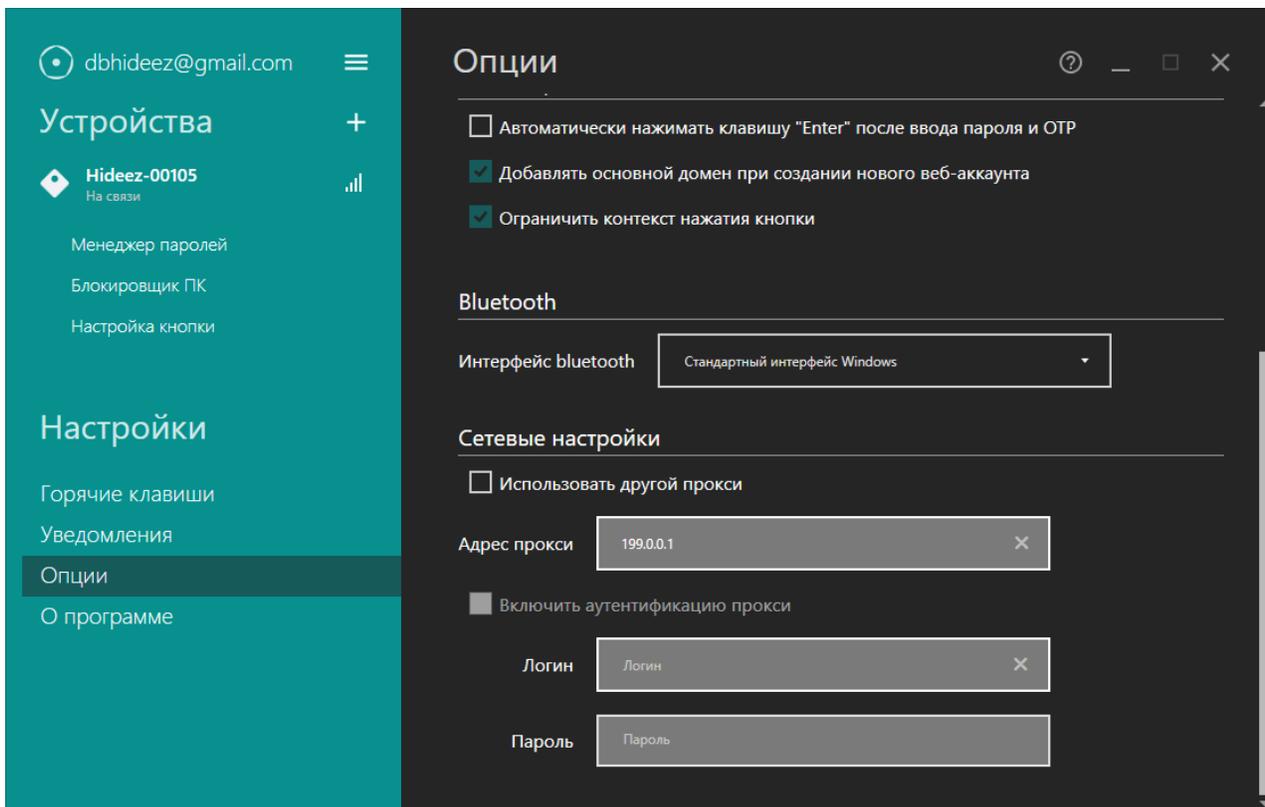
Ограничение контекста нажатия кнопки устройства для ввода паролей (только для Windows)

По умолчанию, при добавленных в приложении нескольких Hideez Key в одном аккаунте, данные, сохраненные в менеджере паролей доступны к использованию любым из добавленных Hideez Key. Поэтому, если у пользователя, например, есть одна запись, сохраненного логина и пароля в менеджере паролей устройства 001 для сайта facebook.com, а также одна запись, сохраненная для facebook.com в менеджере паролей устройства 002, то, независимо от того, с какого из подключенных устройств отправляется запрос на подстановку данных логина и пароля, пользователю будут предоставляться для выбора обе записи подходящих аккаунтов из двух устройств - 001 и 002.

Выбор в меню Опции варианта - поставить флажок “Ограничить контекст нажатия кнопки” позволит избежать объединения данных менеджеров паролей всех подключенных устройств и по запросу будут использоваться сохраненные записи только из того устройства, на котором нажимается кнопка с командой вставить логин и пароль.



Внизу экрана Опции, пользователь может кликнуть Расширенные настройки, после чего появится возможность настроить интерфейс Bluetooth, а также произвести Сетевые настройки - Использовать другой прокси, Включить аутентификацию прокси, добавить Логин и Пароль прокси сервера.



9.3. Настройка «Доверенные места» для Android и iOS устройств

«Доверенные места» позволяют настроить функционал Hideez Safe в зависимости от месторасположения, в частности Датчик прикосновений и Охрана предметов.

Программа Hideez Safe определяет местоположение по географическим координатам (адресу) или по данным GPS телефона. Для добавления критерия нужно нажать кнопку (+) на соответствующем профиле. Запустится помощник настройки, на первом шаге которого можно выбрать один из вариантов:

1. **Точка на местности** – на открывшейся карте нужно нажать и удерживать точку до появления окружности вокруг нее. Затем можно изменить радиус окружности используя регулятор в нижней части окна. Для изменения положения окружности нужно нажать и удерживать другую точку на карте. Критерий будет срабатывать, когда координаты телефона будут попадать внутрь окружности.
2. **Район расположения** – По данным GPS телефона на карте появится точка с окружностью - место Вашего расположения в данный момент. Затем можно изменить радиус окружности используя регулятор в нижней части окна.
3. **Wi-Fi** (только для Android) – из открывшегося списка нужно выбрать название сети Wi-Fi, по наличию которой в зоне видимости будет срабатывать критерий.

На последнем шаге пошаговой инструкции можно при желании изменить имя критерия, созданное автоматически.

Впоследствии критерий можно отредактировать. Удалить критерий из списка можно выбрав справа от сохраненного доверенного места пункт “Удалить” в скрытом меню для Android или кликнув на сохраненное доверенное место в открывшемся окне с местом на карте кликнуть на “Удалить место” внизу окна для iOS.

Профиль можно переключить вручную, с помощью иконки, расположенной в верхней части главного окна. Если профиль переключен вручную, он действует до тех пор, пока не переключится автоматически по какому-либо критерию.

Примечание: для более точной работы функционала *Доверенные места* необходимо разрешить программе использовать GPS на телефоне, соответствующая опция есть в окне Настроек. Следует учитывать, что это может увеличить расход батареи.

9.4. Защита ПК Windows

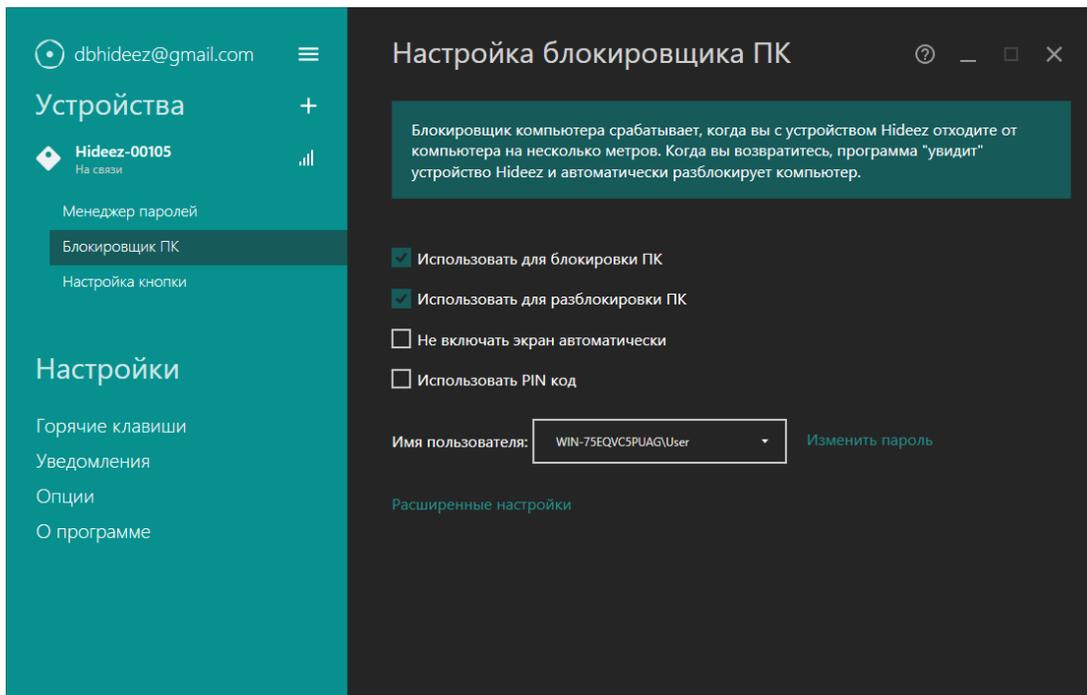
При установке программы Hideez Safe на ПК добавляется еще один способ входа – с помощью присутствия Hideez Key. Полный список возможных способов входа на компьютере можно посмотреть, нажав на ссылку «Опции входа» (Sign-in options) на экране блокировки ПК:



Например, на приведенном рисунке доступны четыре способа входа: по Hideez Key, сканеру отпечатков пальцев, ПИН-коду и паролю.

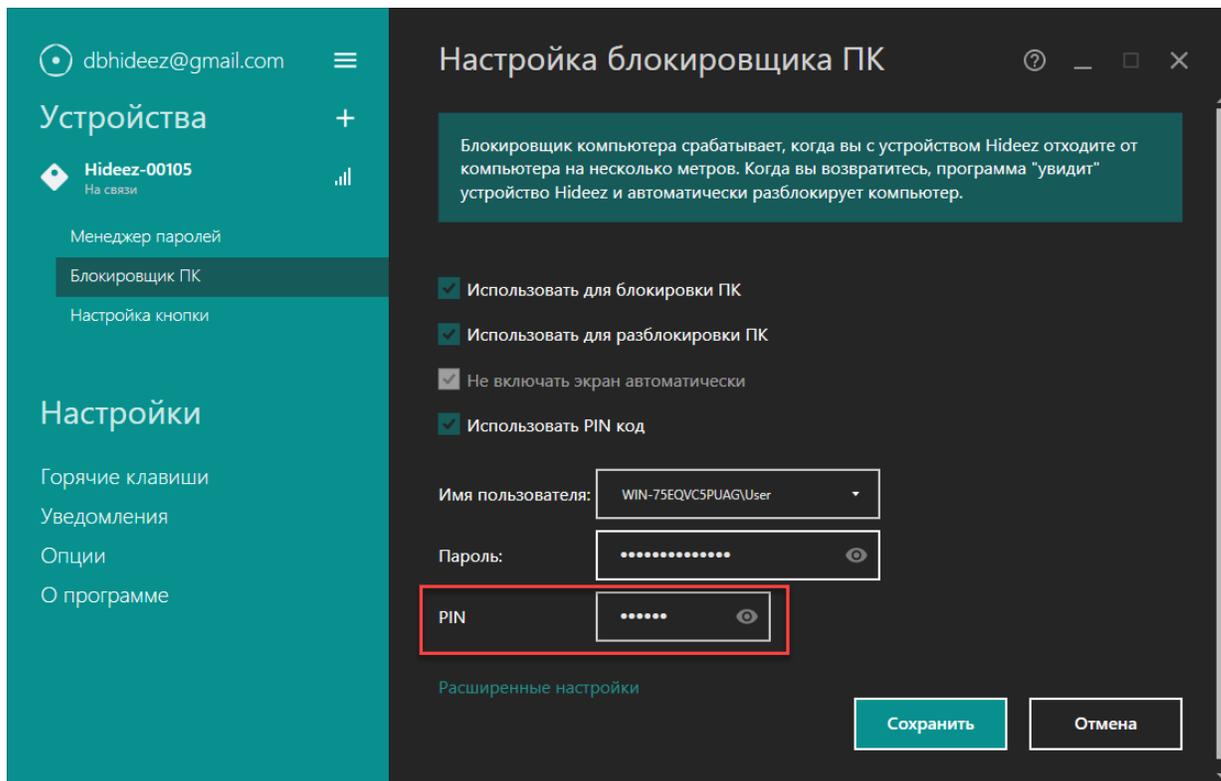
При выборе Hideez Key компьютер будет автоматически разблокирован, если ваш ключ находится достаточно близко, либо необходимо будет вручную ввести PIN код для разблокировки, если будет активирована в приложении соответствующая функция.

Предварительно нужно настроить опции входа в программе Hideez Safe, на закладке «Блокировщик ПК», как указано на рисунке ниже:



- Установите флажок "Использовать для блокировки ПК".
- Установите флажок "Использовать для разблокировки ПК".
- Установите флажок "Использовать PIN код"
- Укажите имя учетной записи. Для выбора из имеющихся локальных пользователей используйте выпадающий список.
- Введите пароль к учетной записи. Этот пароль сохраняется в Hideez Key и не хранится на компьютере.
- Введите PIN код (В случае выбора данной функции)*
- Сохраните изменения.

* PIN код при входе в систему вводится исключительно вручную, связан только с приложением Hideez Safe и не имеет отношения к системному ПИН коду для входа в Windows



Расширенные настройки позволяют задать уровни сигнала Bluetooth по достижению которых компьютер будет заблокирован или разблокирован. Слева отображается уровень сигнала блокировки. Когда уровень упадет ниже этого порога, компьютер заблокируется. В программе сделана задержка на несколько секунд, чтобы убедиться, что уровень сигнала действительно понизился. Это уменьшает ложные блокировки при случайных сбоях в радиоканале.

Справа отображается уровень сигнала разблокировки. Как только уровень превысит этот порог, компьютер может быть разблокирован автоматически или вручную.

Над полями ввода уровней расположен *индикатор текущего уровня сигнала*. Используйте этот индикатор для справки, чтобы оценить уровень в тех положениях, когда вы хотите заблокировать и разблокировать ваш компьютер. Нижний порог установите с запасом процентов в 20, чтобы избежать блокировок от случайных падений сигнала.

Опция «Не включать экран автоматически» по умолчанию не включена. Это означает что, когда вы подходите к компьютеру и уровень сигнала достигает верхнего порога, экран включается, блокировка снимается и вы сразу попадаете на рабочий стол даже не прикоснувшись к компьютеру. Если же эта опция включена, то нужно будет нажать Enter или провести пальцем по экрану устройства с сенсорным экраном.

Примечание: все ваши прежние способы входа остаются доступными для использования.

Защита Mac осуществляется подобным образом.

9.5. Менеджер паролей

Hideez Key может хранить пароли и логины, количество которых ограничено только объемом доступной внутренней памяти (72 КБ). Пароли вводятся в приложениях и веб-браузерах по нажатию на кнопку Hideez Key или по нажатию комбинации клавиш (на компьютере).

Менеджер паролей Hideez оперирует понятием аккаунта (учетной записи) - это совокупность логина, пароля, секретного ключа OTP и названия аккаунта. Понятие одноразового пароля рассматривается в разделе «Одноразовые пароли (OTP) и двухфакторная авторизация». Название аккаунта – это произвольное имя, которое вы даете, чтобы отличать один аккаунт от другого в общем списке. Имена должны быть уникальными, либо содержать различные логины. По умолчанию имя аккаунта соответствует домену веб сайта, названию приложения в Android или заголовку окна для Windows приложения.

Помимо вышеперечисленных полей, в аккаунт добавляется информации о том, как его использовать. Для веб-сайтов добавляется корневое имя домена, для приложений Android – их идентификатор (package name) в Google Play, для приложений Windows – заголовок окна программы. Информация о веб-сайтах является общей для всех операционных систем и будет видна на любом вашем устройстве. Специфическая информация о приложениях Android или Windows отображается только в соответствующих ОС.

Вся информация сохраняется только в Hideez Key и не хранится на компьютере/телефоне. Аккаунты, которые вы сохраняете на различных устройствах являются общими. Таким образом, решена проблема синхронизации данных между устройствами и нет необходимости задействования облачных хранилищ.

К одному аккаунту менеджера паролей можно привязать несколько приложений, в том числе на разных ОС, а также несколько веб-сайтов. При смене пароля в аккаунте, все привязанные приложения и сайты автоматически станут использовать новый пароль.

9.5.1. Работа с паролями в системе Android I iOS

Работа Hideez Key со смартфонами на базе Android и iOS имеет различия.

Ввод паролей в iOS возможен только в Safari.

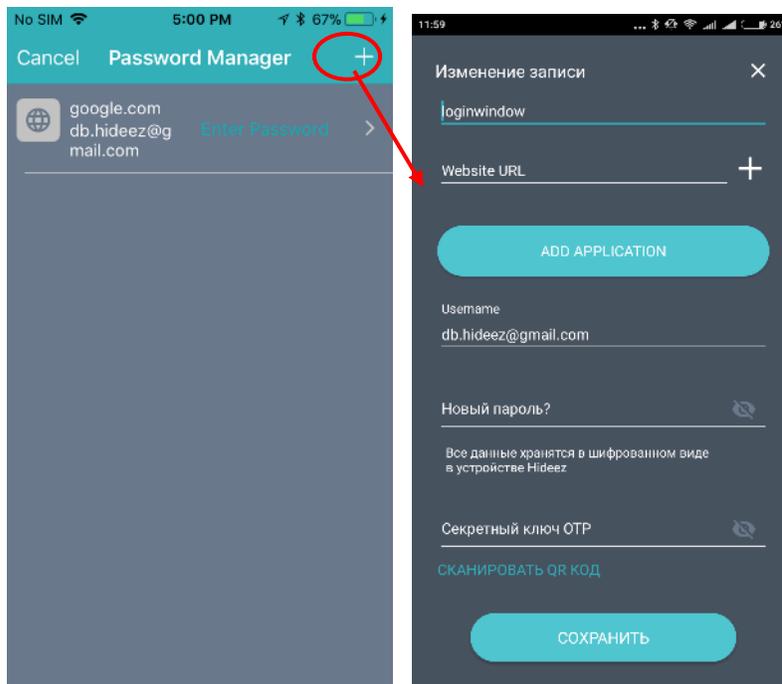
Для Android пароли вводятся в веб-страницы (только браузеры Chrome, Opera), а также в большинство установленных на смартфон приложений (это зависит от реализации приложения). Если Вы обнаружили программу, в которой ввод пароля не срабатывает – сообщите об этом в службу техподдержки Hideez. Когда решение проблемы будет найдено, оно будет включено в следующие обновления программы Hideez Safe.

Для iOS ввод логинов и паролей в приложениях пока не доступен.

Добавление паролей

Запустите менеджер паролей из главного окна приложения для Android. При первом запуске программа запросит разрешение на автоматический ввод паролей и откроет окно настроек Android. Разрешите доступ для Hideez Safe, включив соответствующий переключатель, затем вернитесь в окно Hideez Safe.

Для добавления пароля нажмите знак «+» в верхней части окна. Откроется окно добавления аккаунта.



При выборе «Добавить приложение» программа откроет список приложений, зарегистрированных в Android (на момент написания руководства эта возможность отсутствует для iOS). Выберите нужное и заполните поля Логин и Пароль.

При выборе веб-сайта (http//...) можно указать домен, для которого будет действителен пароль, при этом пароль будет действителен также для его под-доменов.

Обратите внимание, логин может быть пустой для некоторых сайтов или приложений.

Если программа использует PIN-код (4 цифры) – введите его в поле пароля.

Сохраните запись кнопкой «Сохранить».

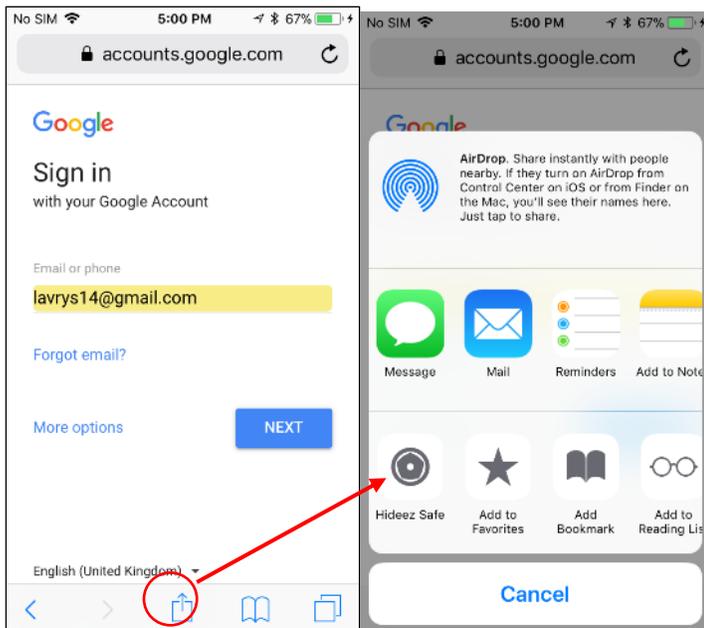
Добавление уже существующего пароля приложению Android.

Часто веб-приложения имеют «нативные» приложения на смартфонах. В этом случае удобно использовать единую запись менеджера паролей. Уже созданную на компьютере запись можно «привязать» к мобильному приложению на смартфоне. Для этого после установки «целевого» приложения нужно открыть менеджер паролей Hideez Safe, выбрать нужный аккаунт, открыть его для редактирования и «добавить приложение».

Запустите выбранное приложение – поля логина и пароля теперь могут быть заполнены по двойному (по умолчанию) нажатию кнопки Hideez Key.

Применение паролей в iOS

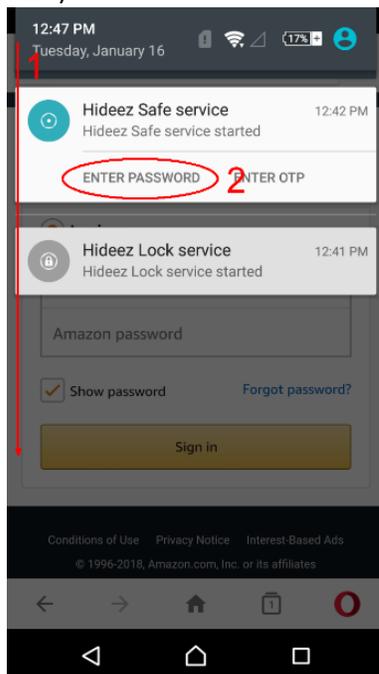
Пароль можно ввести в веб-форму, открытую в Safari, с помощью кнопки Hideez Safe на панели расширений (см рисунок ниже)



Применение паролей в Android

Применить пароль можно двумя вариантами:

- Откройте выбранное приложение или веб-страницу и нажмите кнопку Hideez Key два раза. Поля логина и пароля будут автоматически заполнены.
- В версиях Android 6.0 и выше, логин и пароль можно ввести из строки сообщений Android (вызывается жестом «сверху вниз»)



Изменение и удаление аккаунтов менеджера паролей

Для редактирования аккаунта, нажмите на нужную строку в списке. Удалить аккаунт можно «смахнув» его из списка в сторону и подтвердив операцию в всплывающем окне.

Сохранённые пароли нельзя посмотреть, можно только изменить. (Для просмотра паролей используйте функцию “Экспорт” в приложении на Mac и Windows)

Смотрите видео Добавление паролей в Hideez Safe для [Android](#) и [iOS](#)

9.5.2. Работа с паролями на компьютере Windows или Mac

В системе Windows для ввода паролей нужно использовать либо комбинации «горячих» клавиш, либо кнопку Hideez Key. По умолчанию в программе установлены следующие комбинации клавиш:

Команда	Windows	MacOS
Ввести логин	Control + Alt + L	^↑L
Ввести пароль	Control + Alt + P	^↑P
Ввести пароль по умолчанию	Control + Alt + D	^↑D
Добавить новую запись в менеджер паролей	Control + Alt + A	^↑A
Ввести OTP	Control + Alt + O	^↑O

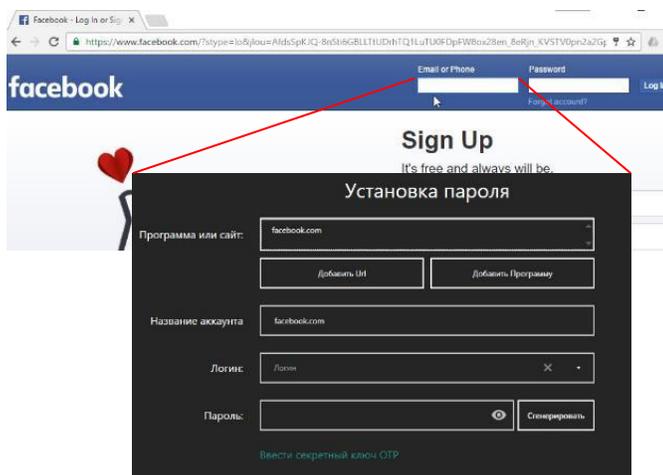
Действия кнопки Hideez Key по умолчанию настроены следующим образом:

Тип нажатия	Действие
1 нажатие	Заблокировать компьютер
2 нажатия	Ввести пароль
3 нажатия	Ввести логин
4 нажатия	Ввести OTP

Эти настройки могут быть изменены.

Добавление и ввод паролей в интернет браузерах

Добавить новый пароль (аккаунт) проще всего из того приложения, где его нужно ввести. Например, откройте интернет браузер, зайдите на любой сайт, где требуется пароль и установите курсор ввода на поле пароля. Нажмите кнопку Hideez Key два раза или комбинацию клавиш для ввода пароля. Поскольку пароля для этого сайта еще нет в списке, откроется окно приложения Hideez Safe с предложением добавить новый аккаунт, как на рисунке.



Поле «*Программа или сайт*» будет автоматически заполнено названием домена открытого сайта. Это поле в дальнейшем будет использоваться для поиска аккаунта, менять его не рекомендуется, за исключением того, что можно удалить под-домен. Например, вместо «my.hideez.com» ввести «hideez.com» – в этом случае действие аккаунта будет распространяться на все поддомены. В этом поле можно ввести несколько доменов, каждый из которых должен быть в отдельной строке.

Поле «*Название аккаунта*» также автоматически заполнено названием домена. Вы можете ввести сюда произвольное имя.

Поле «*Логин*» нужно заполнить вручную. Если ранее такой логин уже вводился, его можно выбрать из выпадающего списка. Логин удаляется из списка автоматически, если он больше не используется.

Поле «*Пароль*» нужно заполнить вручную.

После заполнения всех полей нажмите кнопку [Сохранить], после чего вернитесь в окно браузера в поле ввода пароля и снова нажмите комбинацию клавиш. Пароль будет введен автоматически. Аналогичным образом можно ввести логин и OTP (подробнее об OTP см. [Одноразовые пароли](#)).

Примечание: программа Hideez Safe умеет работать с последними версиями наиболее популярных интернет браузеров – Chrome, Firefox, Opera, Internet Explorer, Edge (Windows), Safari, Chrome (MacOS), Chrome, Opera (Android), Safari (iOS). Другие браузеры рассматриваются программой как обычное десктоп-приложение и вместо адреса домена будет определяться заголовок окна.

Совет: Обновите браузер, если он входит в перечень поддерживаемых и при этом адрес домена не определяется программой.

Совет: Если Вы зарегистрированы на одном и том же ресурсе под несколькими логинами, то при первой попытке автоматического ввода пароля программа предложит добавить аккаунт и далее будет его использовать. Чтобы добавить еще один аккаунт под другим логином стоит воспользоваться комбинацией клавиш для добавления нового пароля (по умолчанию Control + Alt + A).

Автоматическая генерация пароля

Когда вы регистрируетесь на новом веб сервисе, удобно воспользоваться функцией автоматической генерации пароля. Сгенерированный уникальный пароль будет обладать очень высокой надежностью. Для этого в окне редактирования аккаунта нажмите кнопку [Сгенерировать]. Сгенерированный пароль можно посмотреть, кликнув на значок . После сохранения аккаунта, можно вернуться на страницу регистрации и применить сохраненный пароль в обоих полях - ввода и подтверждения пароля.

Доступно в приложении для Windows, Mac, iOS.

Совет: Создавайте уникальные пароли для разных сервисов. В случае взлома или компрометации одного из сервисов ваши остальные пароли не пострадают.

Смена пароля

Часто возникает необходимость сменить пароль на каком-нибудь из веб-ресурсов. Обычно эта процедура включает ввод старого пароля и ввод нового с подтверждением. Воспользуйтесь Hideez Key для ввода старого пароля. Затем откройте окно Hideez Safe, перейдите в менеджер паролей, найдите требуемый аккаунт и откройте его для редактирования. В окне редактирования нажмите ссылку [Сменить пароль], а затем нажмите кнопку [Сгенерировать] или введите новый пароль вручную. После этого сохраните аккаунт, перейдите в браузер и используйте новый пароль.

Совет: Если по каким-то причинам смена пароля на веб-ресурсе не завершится, воспользуйтесь резервной копией данных Hideez Key чтобы восстановить первоначальный пароль и попробовать процедуру заново. Однако, следует помнить, что резервная копия заменит содержимое всей памяти Hideez Key, в том числе и другие записи менеджера паролей.

Добавление и ввод паролей в десктоп-приложениях

Программа Hideez Safe может вводить логины и пароли не только на интернет страницах, но и в любое приложение. Для этого нужно установить курсор ввода на поле логина или пароля и нажать соответствующую комбинацию клавиш или кнопку Hideez Key. Программа определит текущее активное окно, получит заголовок окна и имя процесса и попытается найти по этой информации подходящий аккаунт. Так же, как и при работе с интернет сайтами, если подходящего аккаунта нет, будет предложено создать новый.

Поле «*Программа или сайт*» будет автоматически заполнено заголовком окна. Это поле в дальнейшем будет использоваться для поиска аккаунта. Можно убрать из этого поля несущественные слова. При поиске будет использоваться следующий алгоритм – аккаунт считается подходящим, если каждое слово из этого поля встречается в заголовке окна в которое вводится логин/пароль. Это поле может состоять из нескольких строк, каждая из которых обрабатывается независимо от остальных. Таким образом вы можете назначить аккаунт нескольким программам.

Поле «*Название аккаунта*» также автоматически заполнено заголовком окна. Вы может ввести сюда произвольное имя.

Поле «*Логин*» нужно заполнить вручную. Если ранее такой логин уже вводился, его можно выбрать из выпадающего списка. Логины удаляются из списка автоматически, если они больше не используются.

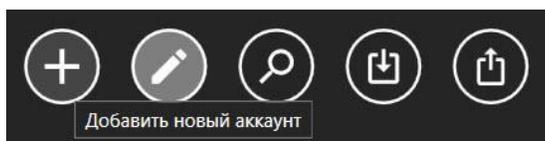
Поле «*Пароль*» нужно заполнить вручную.

После заполнения всех полей нажмите кнопку [Сохранить], после чего вернитесь в окно программы, где нужно ввести пароль и снова нажмите комбинацию клавиш. Пароль будет введен автоматически. Аналогично можно ввести логин или OTP.

Смотрите видео Как добавлять пароли в веб- и десктоп-приложениях для [Windows](#) и [Mac](#) на канале <http://youtube.com/hideez>.

Добавление паролей вручную

Новый аккаунт можно добавить в программу из интерфейса Hideez Safe. Для этого нажмите кнопку [+] в менеджере паролей, как указано на рисунке.



Для «*Программа или сайт*» есть кнопки [Добавить Url] и [Добавить программу]. «Добавить программу» открывает список заголовков окон всех открытых программ на компьютере. «Добавить Url» отображает доменное имя текущих закладок в открытых окнах браузеров. Выберите нужную запись из списка. Заполнение остальных параметров выполняется как описано в разделах выше [Добавление и ввод паролей в интернет браузерах](#) и [Добавление и ввод паролей в десктоп-приложениях](#).

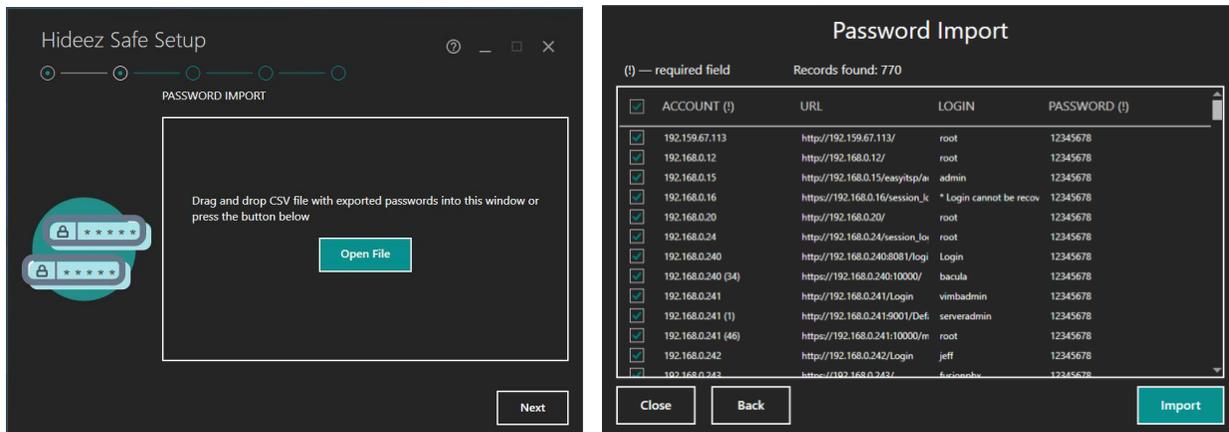
Выбор из нескольких подходящих аккаунтов

Часто случается, что регистрируется несколько аккаунтов на одном ресурсе, например, личный и корпоративный адрес в Google Mail. Программа Hideez Safe не может определить какой из логинов пользователь хочет использовать, поэтому предложит список подходящих вариантов. Этот список появится в углу экрана, возле иконки Hideez Safe.

Импорт паролей

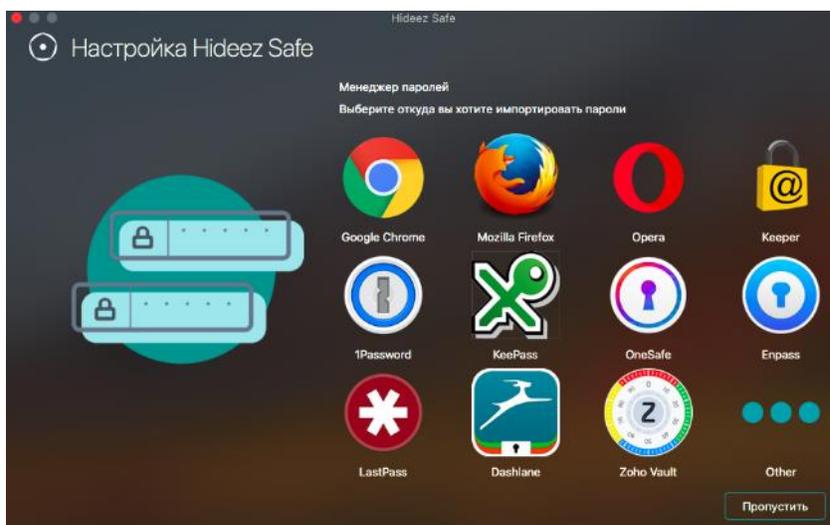
Hideez Safe предоставляет возможность импорта паролей из файла CSV в Hideez Key. Процедура импорта

запускается нажатием клавиши  в Менеджере паролей.



Среди найденных записей нужно отметить нужные и нажать кнопку [Импортировать].

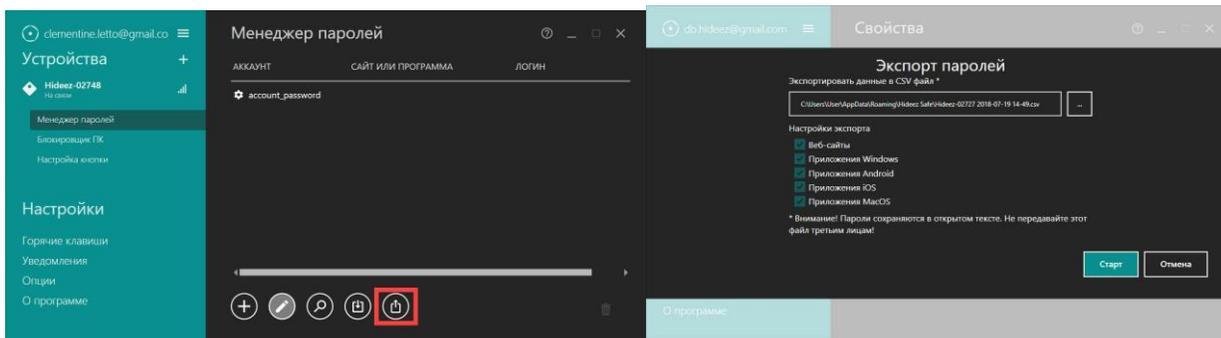
Импорт паролей в Hideez Safe для Mac работает аналогично.



Экспорт паролей

Hideez Safe предоставляет возможность экспорта паролей с Hideez Key в файл CSV. Процедура экспорта

запускается нажатием кнопки  в Свойствах Hideez Key.



Для осуществления экспорта нужно указать путь, куда будет сохранен CSV файл, либо оставить “по умолчанию” и настроить параметры экспорта (веб-сайты, приложения Windows, приложения Android, приложения iOS, приложения MacOS).

Внимание! Пароли сохраняются в открытом тексте. Не передавайте сохраненный файл третьим лицам!

Использование пароля по умолчанию

Один из имеющихся в списке паролей можно назначить паролем «по умолчанию». Такой пароль будет вводиться каждый раз, когда вы будете нажимать комбинацию клавиш для ввода пароля по умолчанию (в стандартных настройках это Control + Alt + D). Для настройки этого пароля откройте закладку *Горячие клавиши* и выберите его из списка.

Настройка горячих клавиш

Комбинации «горячих» клавиш значительно облегчают ввод логинов и паролей, стандартные настройки достаточно легко запомнить, но при необходимости вы можете изменить их в разделе *Горячие клавиши*. Поставьте курсор ввода в требуемое поле и нажмите комбинацию, которую вы хотите установить. Если это не срабатывает, значит такая комбинация уже занята операционной системой или другой запущенной программой – выберите другую комбинацию.

При запуске Hideez Safe регистрирует все комбинации клавиш в системе Windows, чтобы ими можно было воспользоваться в любой программе. Если другая программа уже зарегистрировала такую же комбинацию, то Hideez Safe выдаст об этом уведомление. В этом случае нужно выбрать другую комбинацию клавиш.

Удаление записей из Менеджера паролей

Для удаления записи откройте ее для редактирования и нажмите ссылку «Удалить аккаунт» в нижней части экрана. При этом из памяти Hideez Key также удалится логин, если он не используется для других аккаунтов.

Примечание: полностью очистить память Hideez Key можно выполнив команду «Отвязать от аккаунта» в настройках устройства.

9.6. Одноразовые пароли (OTP) и двухфакторная авторизация

Hideez Key поддерживает генерацию одноразовых паролей (time based one-time password, TOTP) согласно стандарту RFC 6238.

Общий принцип использования одноразовых паролей заключается в следующем – есть общий секрет, известный двум устройствам (секретный ключ). На основании этого ключа, используя криптографические преобразования, одно из устройств генерирует относительно небольшой (например, 6 цифр) одноразовый пароль. Этот пароль передается для проверки на второе устройство. Второе устройство по

томе же алгоритму, используя тот же секретный ключ, тоже генерирует одноразовый пароль и сверяет его с полученным паролем от первого устройства. Если пароли совпали – доступ разрешается. Одноразовыми такие пароли называются потому, что в алгоритме генерации, в дополнение к секретному ключу используется еще счетчик созданных одноразовых паролей, и каждый раз такой получается отличным от предыдущего. Естественно, что счётчики на обеих сторонах должны быть синхронизированы – если хоть один пароль пропустить, то они уже не будут совпадать и алгоритм нарушится. Более удобным вариантом генерации одноразовых паролей является синхронизация по времени. В этом случае алгоритм генерации использует не счетчик, а текущее время. Синхронизировав время между двумя устройствами, мы будем всегда получать одинаковые пароли с двух сторон. В реализации RFC 6238 время округляется до 30 секунд – т.е. каждые 30 сек. одноразовый пароль будет меняться.

В Hideez Key используется второй вариант – на основе текущего времени. Синхронизация времени между Hideez Key и компьютером/телефоном происходит при каждом установлении связи между ними. Для корректной работы на компьютере должно быть установлено точное время, иначе оно не совпадет с временем сервера, который будет проверять OTP и пароли не совпадут.

Секретный ключ OTP можно добавить в любой из аккаунтов в окне менеджера паролей.

В качестве примера, ниже приведена информация по использованию Hideez Key для двухфакторной аутентификации пользователей Google.

- Зайдите в настройки безопасности своего аккаунта <https://accounts.google.com/b/0/SmsAuthConfig>
- Включите для своего аккаунта двухфакторную аутентификацию (для корпоративных клиентов это потребует дополнительного разрешения администратора).
- Если Google потребует, подтвердите номер своего телефона и укажите присланный в СМС код.
- Выберите мобильное приложение как основной способ получения кодов (Get codes via our mobile app instead), укажите что планируете использовать приложение для Android.
- В окне "Настройка Google Authenticator" вы получите QR-код, в котором содержится секретный ключ, выберите ссылку "Не могу сканировать QR-код" (Can't scan the barcode?) и тогда тот же самый код будет отображен в текстовом виде.
- Скопируйте секретный ключ в буфер обмена.
- Откройте нужную запись Менеджера паролей Windows приложения и нажмите ссылку [Ввести секретный ключ OTP]. Вставьте скопированный код и сохраните изменения.
- После этого вернитесь в браузер и нажмите ОК, тем самым завершив настройку - Google сразу попросит ввести одноразовый пароль, чтобы убедиться, что вы все правильно настроили. Нажмите комбинацию клавиш для ввода OTP (по умолчанию это Control + Alt + O) – одноразовый пароль будет создан в метке и подставлен в поле ввода. До проверки OTP секретный ключ не будет применён и двухфакторная аутентификация не включится.

Смотрите видеоролик о настройке двухфакторной аутентификации Google для [Windows](#) и [Mac](#) на канале <http://youtube.com/hideez>.

Примечание: Генерирование нового секретного ключа Google-аккаунта делает предыдущий ключ недействительным, поэтому, для одновременной работы Hideez Key и Google Authenticator на другом устройстве нужно устанавливать ключ одновременно во всех устройствах.

9.7. Резервное копирование и восстановление пользовательских данных

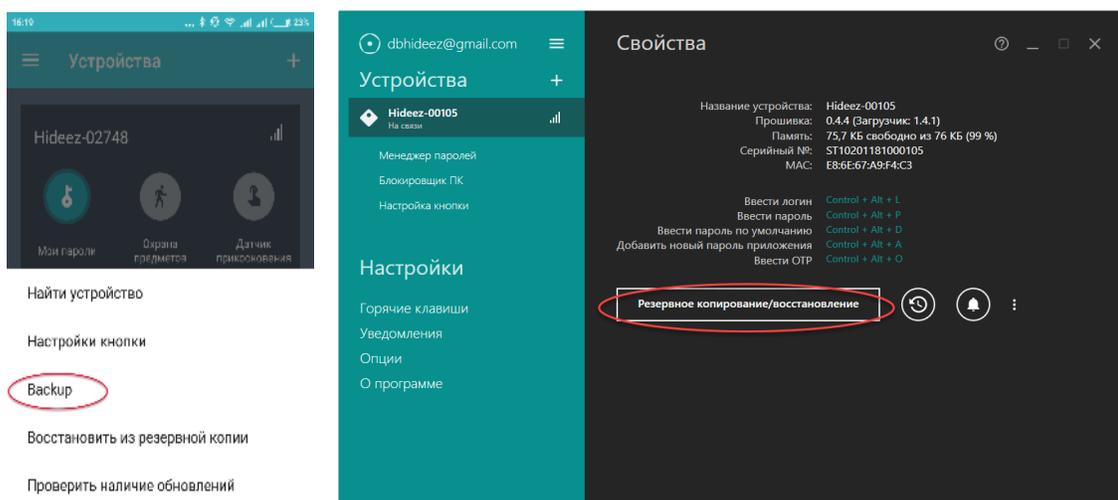
Устройство Hideez Key содержит 72 КБ пользовательской памяти и может хранить тысячи паролей, логинов, ключей и прочей информации. Рекомендуется периодически делать резервную копию этих данных, либо настроить функцию автоматического резервного копирования.

Резервная копия создается в локальном файле компьютера/телефона в зашифрованном виде и не передается на сервера Hideez. Для шифрования используется алгоритм AES-256 и пароль пользовательского аккаунта My Hideez.

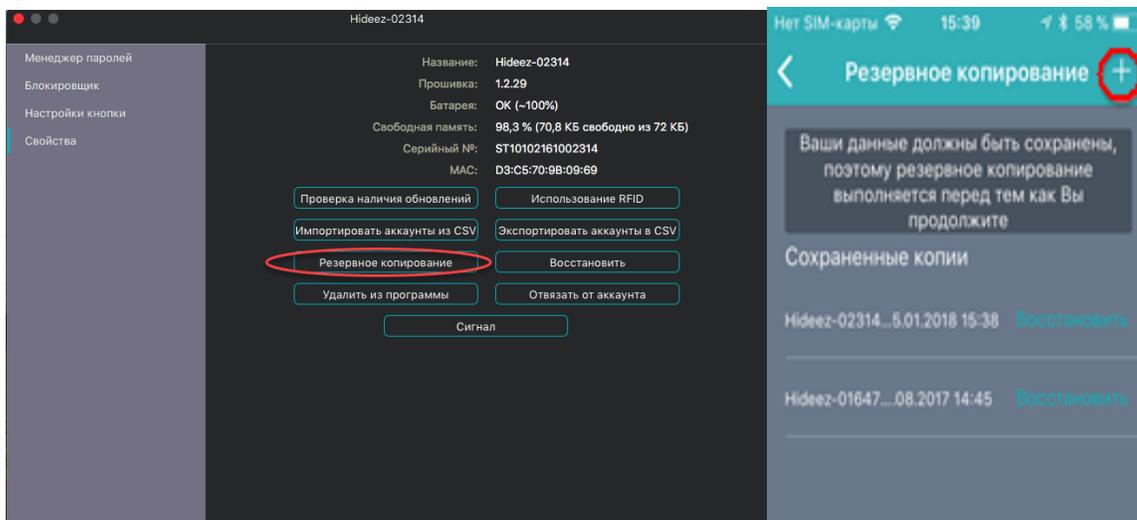
Имя файла содержит расширение *.hb, включает название устройства, а также дату и время последней модификации данных в памяти Hideez Key.

Для восстановления файла пароль необходимо ввести вручную. Обратите внимание, что если вы меняете пароль своего аккаунта, то при восстановлении из резервной копии нужно ввести тот пароль, который был актуален на момент ее создания.

Команда резервного копирования и восстановления находится в контекстном меню или свойствах Hideez Key и может отличаться в различных реализациях Hideez Safe (см. рисунок).



Резервное копирование в Hideez Safe для Android и Windows.



Резервное копирование в Hideez Safe для Mac и iOS.

Хотя файл резервной копии зашифрован, рекомендуется хранить его в надежном месте, т.к. как в случае его потери, любой локальный файл подвержен риску взлома методом прямого перебора пароля (brute force attack). Подробнее см. Приложение 2. Рекомендации по безопасной работе.

Настройка автоматического резервного копирования (только для Windows)

В приложении можно настроить запуск автоматического резервного копирования по расписанию.



Для этого необходимо кликнуть на значок настроек автоматического резервного копирования -

в Свойствах добавленного устройства. В открывшемся окне выбрать флажок “Включить автоматическое резервное копирование”, настроить “Частоту (дней)”, “Время начала” и сохранить выбранные настройки. В выбранное время и день будет произведено автоматическое резервное копирование данных с сохранение файла резервной копии в локальную папку по умолчанию.

Примечание: для выполнения резервного копирования или восстановления Hideez Key должен быть зарегистрирован и проинициализирован.

Совет: процедура сохранения/восстановления может быть использована как для переноса данных между двумя Hideez Key одного пользователя, так и для переноса данных между устройствами разных пользователей (при восстановлении необходимо будет ввести пароль, которым выполнялось шифрование).

9.8. Охрана предметов и поиск Hideez Key со смартфона

Благодаря постоянной радиосвязи, можно предотвратить случайную потерю брелока Hideez Key, а также личных вещей, к которым он может крепиться.

Если телефон покинул «Доверенное место» и брелок Hideez Key не находится на связи, он считается «забытым».

Hideez Key находится под угрозой потери/кражи, если устройство находится на связи, но уровень сигнала упал ниже установленного порога.

Когда телефон покидает «доверенное место», проверяется, что подключенный Hideez Key находится на связи. Если устройства на связи нет, звучит звуковое предупреждение и делается запись в журнале сообщений.

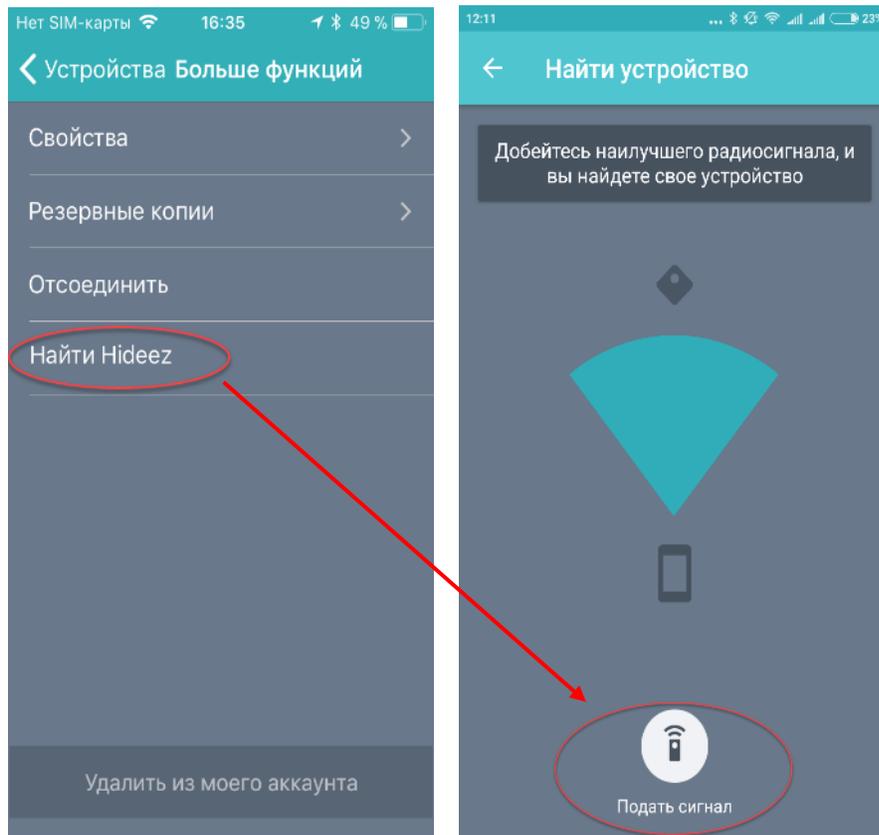
Режим «Охрана предметов» используется только на смартфоне (Android, iOS). Включить и настроить его можно в пункте меню «Охрана предметов»:

- Задайте мелодию сигнала, которая известит о потере.
- Установите высокую или низкую чувствительность для срабатывания сигнала.
- Укажите необходимость включения звука на Hideez Key. По умолчанию звук будет включаться только на.
- Укажите, включать ли сигнал в доверенных местах (по умолчанию выключено).

Примечание: использование звуковых сигналов сильно разряжает батарею Hideez Key, поэтому по умолчанию опция звука отключена.

9.8.1. Поиск брелока со смартфона

Если Hideez Key на связи, вы можете его найти с помощью звукового сигнала:



Если звук по каким-то причинам не слышен, можно ориентироваться на уровень сигнала, который напрямую зависит от расстояния между смартфоном и брелоком.

Примечание: телефон отображает только текущий уровень сигнала, а не его направление. Уровень сигнала сильно зависит от внешних причин: расположения антенны в телефоне, расположения телефона в руке, наличия преград, отражения сигнала и т.д.

9.8.2. Координаты брелока на карте Google Maps в смартфоне.

В момент потери связи с Hideez Key приложение запоминает текущие географические координаты. Соответствующий участок карты отображается на главном экране программы.

9.9. Биометрическая идентификация пользователя Android

Hideez Safe использует биометрическую идентификацию TouchID – распознавание отпечатков пальцев для упрощения аутентификации.

Для использования биометрической аутентификации TouchID - распознавание отпечатков пальцев, пожалуйста выполните:

1. Откройте “Настройки” из главного меню.
2. Убедитесь, что переключатель “Требовать PIN для входа в приложение” включен.
3. Включите “Активировать сканер отпечатка пальца”.
4. Настройка закончена, теперь Вы можете использовать TouchID с Hideez Key.

9.10. Использование RFID датчика

Hideez Key оборудован модулем радиочастотной идентификации (RFID) Atmel T5577, работающим на частоте 125 КГц. Этот модуль работает независимо от Bluetooth модуля и никак с ним не связан.

Модуль RFID также не связан с приложением Hideez Safe!

Модуль RFID обычно используется для идентификации в системах контроля доступа, например, электромагнитных дверных замках, турникетах и др.

RFID-модуль Hideez Key умеет работать по стандартам HID или Em-Marine, но только один из них может быть активен в каждый момент времени, то есть на Hideez Key может храниться только один уникальный RFID код. Изначально Hideez Key уже снабжен перезаписываемым уникальным кодом в стандарте Em-Marine.

Чтобы, заменить его на любой другой код в стандарте Em-Marine или HID необходимо специальное оборудование – программатор. Такое оборудование поставляется в составе коммерческих систем контроля доступа (СКД) либо его можно приобрести отдельно. Соответствующая информация подробно изложена в документации к СКД и здесь не рассматривается.

Смотрите видеоролик о [программировании RFID модуля](http://youtube.com/hideez) на канале <http://youtube.com/hideez>.

Примечание: модуль RFID Hideez Key модели ST101 **НЕ является совместимым с модулями NFC**, установленными в смартфонах и планшетах, так как работает на другой частоте.

9.11. Датчик прикосновения (только для Android)

Приложение Hideez Safe для Android позволяет незаметно для окружающих выполнить серию фотографий в момент, когда смартфон оставленный без присмотра, кто-то возьмет в руки. Фотографии будут сделаны при соблюдении следующих условий:

- Режим "Датчик прикосновения" включен и смартфон находится в режиме ожидания.
- К смартфону подключен Hideez Key и уровень его сигнала, меньше заданного в настройках.
- Акселерометр показывает активность (смартфон пришел в движение).

9.12. Действия по нажатию на кнопку (Android, Windows, Mac)

В настройках Hideez Safe для **Android** «Показать больше» предусматривается возможность настройки определенных действий на смартфоне по нажатию кнопки на Hideez Key. Для этого выберите «Настройки кнопки» в выпадающем списке и далее «НАСТРОЙКА». Доступны следующие настраиваемые действия:

- *Отправить СМС.* В настройках необходимо будет указать номер телефона и текст СМС.
- *Звукозапись старт/стоп.* Включение диктофона. Повторное нажатие на кнопку будет отключать запись. Прослушать запись можно из галереи Hideez Safe, файл записи не зашифрован.
- *Сделать исходящий звонок.* Инициировать исходящий звонок на указанный номер телефона.
- *Сделать снимок.* Фотографии создаются зашифрованными и посмотреть их можно только из галереи Hideez Safe.
- *Отправить координаты.* Отправить текущие координаты на указанный номер телефона.
- *Вкл/Выкл фонарик.* Включение фонарика. Повторное нажатие выключает фонарик.
- *Старт/стоп видеозапись.* Включение видеозаписи. Посмотреть запись также можно из галереи Hideez Safe, но файл создается не зашифрованным. Повторное нажатие на кнопку будет отключать запись.
- *Подать сигнал.* Включение звукового сигнала. В настройках можно указать тип сигнала.

Настройка действий выполняется с помощью пошагового помощника:

- Войдите в раздел «Действия» Нажмите кнопку [+] чтобы запустить пошаговую инструкцию.

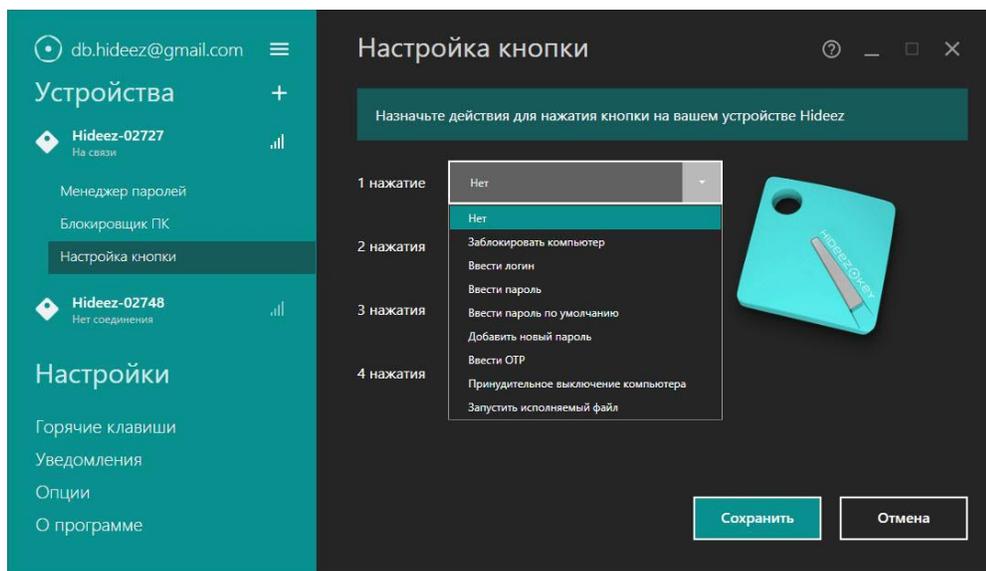
- Выберите тип нажатия (кол-во нажатий на кнопку). В списке будут доступны только те типы, которые еще не заняты.
- Выберите действие из списка.
- Введите дополнительные параметры для выбранного действия, например, тип камеры или номер телефона.

По умолчанию для Hideez Key уже настроены некоторые действия:

<i>Тип нажатия</i>	<i>Действие</i>
<i>1 нажатие</i>	Ввести OTP на смартфоне
<i>2 нажатия</i>	Ввести пароль и логин на смартфоне
<i>Длинное нажатие (2-4 секунды)</i>	Переключиться на другой ПК/смартфон
<i>Длинное нажатие (10 секунд)</i>	Выключить брелок

В настройках Hideez Safe для **Windows** в пункте меню «Настройка кнопки» предусматривается возможность настройки определенных действий на компьютере по нажатию кнопки на Hideez Key. Для этого выберите и назначьте на экране «Настройка кнопки» в выпадающем списке действия для выполнения устройством по нажатию на кнопку. Доступны следующие настраиваемые действия:

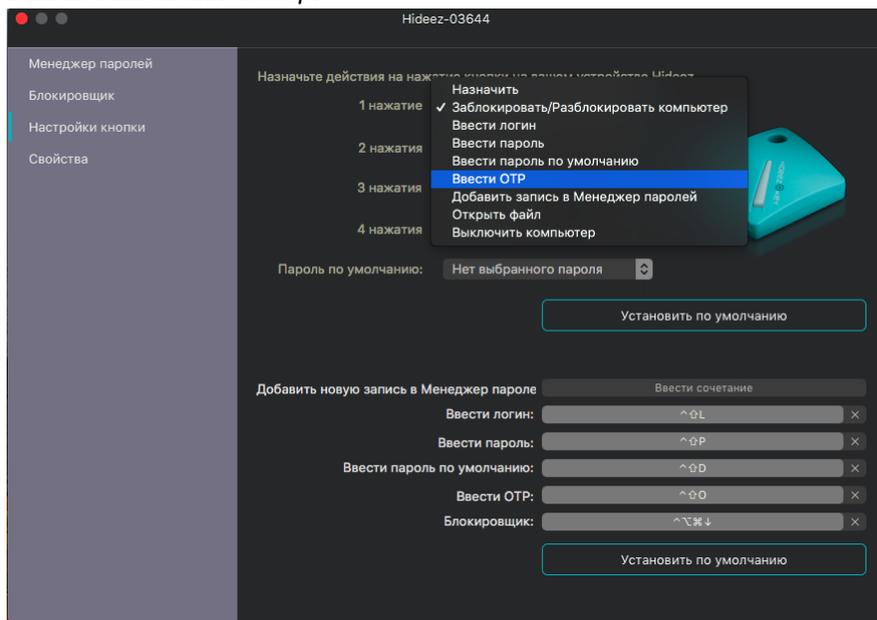
- *Заблокировать компьютер.*
- *Ввести логин;*
- *Ввести пароль;*
- *Ввести пароль по умолчанию;*
- *Добавить новый пароль;*
- *Ввести OTP;*
- *Принудительное выключение компьютера;*
- *Запустить исполняемый файл.*



Windows

В настройках Hideez Safe для **Mac** в пункте меню «Настройки кнопки» предусматривается возможность настройки определенных действий на компьютере по нажатию кнопки на Hideez Key. Для этого выберите и назначьте на экране в выпадающем списке действия для выполнения устройством по нажатию на кнопку. Доступны следующие настраиваемые действия:

- *Заблокировать/Разблокировать компьютер;*
- *Ввести логин;*
- *Ввести пароль;*
- *Ввести пароль по умолчанию;*
- *Ввести ОТР;*
- *Добавить запись в Менеджер паролей;*
- *Открыть файл;*
- *Выключить компьютер.*



Mac

10. Веб-сервис my.hideez.com

Личный кабинет My Hideez позволяет просмотреть список ваших Hideez Key. Отображается модель устройства, серийный номер и дата первой регистрации.

Через веб-сервис вы можете **удалить** Hideez Key из своего аккаунта, если вы передали ее другому лицу, но забыли отвязать от своего аккаунта. В этом случае новый пользователь при подключении Hideez Key получит сообщение об ошибке – «Устройство зарегистрировано на другого пользователя». Он не сможет пользоваться Hideez Key или прочитать ваши данные из устройства. Когда Hideez Key будет отвязана на веб-сервере, клиентская программа на телефоне/ПК выполнит команду полного сброса и очистки Hideez Key, после чего брелок можно будет использовать.

Примечание: если Вы потеряли Hideez Key, не удаляйте ее из своего аккаунта. Никто не сможет ее использовать или прочитать данные, если не знает пароль от вашего аккаунта. Если же вы ее удалите, то таким образом вы просто разрешите ее сбросить и использовать как чистое устройство.

С помощью веб-сервиса также выполняется операция **смены пароля** к вашему аккаунту. Необходимо будет указать старый и новый пароль. После смены пароля потребуется заново войти в аккаунт Hideez Safe на каждом ПК/телефоне, поскольку старый пароль перестанет работать.

Если забыли пароль к аккаунту, его можно сбросить через веб-сервис. Письмо с подтверждением сброса пароля будет отправлено на email.

Приложение 1. Возможные неисправности и их устранение

Hideez Key не работает, не реагирует на нажатие кнопок

Необходимо заменить батарею, как указано в разделе «Приступая к работе».

Невозможно обнаружить Hideez Key через Bluetooth-окружение

Для того, чтобы сделать Hideez Key доступным для подключения, нужно нажать один раз кнопку. Если Hideez Key соединен с другим устройством, то вначале нужно разорвать связь отключив Bluetooth на этом устройстве или вынести его за пределы действия сигнала.

Примечание. На некоторых Android устройствах обнаружение не работает при выключенных настройках геолокации. Необходимо включить эту настройку на период установления связи.

Устройство упало в воду и перестало работать

Попадание воды внутрь корпуса может привести к порче устройства. Следует как можно быстрее извлечь устройство из воды, вскрыть корпус, удалить батарею и просушить плату, например, бытовым феном для сушки волос.

После просушки необходимо установить новую батарею и проверить работоспособность.

Hideez Key перестал издавать звуки

Подача звуковых сообщений на Hideez Key отключается в случае истощения батареи. При этом остальной функционал остается работоспособным, что позволит вам пользоваться устройством до замены батареи.

Не могу удалить программу Hideez Safe для Android – удаление заблокировано

Если вы используете функцию Smart Lock, то возникает необходимость добавить Hideez Safe в список администраторов вашего устройства. Для удаления программы нужно сначала убрать программу из этого списка. Для этого перейдите в Настройки – Безопасность – Администраторы устройства.

Не могу добавить устройство – компьютер (телефон) не видит его.

При возникновении проблем с обнаружением Hideez Key в программе Hideez Safe, может помочь выполнение следующих действий:

- отключить и повторно включить Bluetooth на устройстве
- отключить и включить геолокацию
- при использовании Bluetooth Dongle (Windows 7) принудительно установить Драйвер Bluetooth из папки с установленным на компьютер приложением Hideez Safe (см [видео](#)).
- удалить с устройства Hideez Key бонды - информацию о ранее подключенных устройствах (нажмите кнопку устройства 9 раз - устройство подаст звуковой сигнал и через секунду загорится постоянным светом (режим инженерного меню), затем нажмите кнопку устройства 3 раза - бонды будут стерты, устройство вернется в обычный режим, после этого можно будет выполнить соединение). При этом нужно учитывать, что ранее подключенные устройства будут необходимо подключать заново.
- для успешного подключения Hideez Key к телефону может понадобиться предварительно произвести сопряжение устройства Hideez Key с телефоном в настройках Bluetooth (добавление Bluetooth устройства).

Приложение 2. Рекомендации по безопасной работе

1. Используйте надежный пароль для аккаунта Hideez - этот пароль, в отличие от всех остальных, вам нужно будет помнить и вводить вручную. При составлении этого пароля следуйте общим рекомендациям:
 - Пароль должен содержать не менее шести символов.
 - В состав пароля могут входить цифры, латинские буквы, пробелы и специальные символы («.», «,», «?», «!», «<», «>». «”» и другие).
 - Рекомендуется составлять пароль из смешанного набора цифровых и буквенных (прописных и строчных) символов.

Не используйте в качестве пароля:

- Общеупотребительные слова и устойчивые словосочетания.
 - Наборы символов, представляющие собой комбинации клавиш, расположенных подряд на клавиатуре, такие как: “qwerty”, “123456789”, “qazxsw” и т. п.
 - Персональные данные: имена и фамилии, адреса, номера паспортов, страховых свидетельств и т. п., пароли, созданные для доступа к другим программам (электронная почта, базы данных и пр.).
2. Создавайте новый, уникальный пароль для каждого сервиса, которым вы пользуетесь.
 3. По возможности используйте функцию автоматической генерации пароля – такой пароль обладает очень высокой стойкостью.
 4. Надежно храните файлы резервных копий, так как любой локальный файл подвержен риску взлома методом прямого перебора пароля (brute force attack). Лучше всего хранить копию на втором устройстве Hideez Key – в случае попытки подобрать ключ доступа устройство будет заблокировано навсегда после 1000 неуспешных попыток. Аналогичной защитой обладает веб-сервис my.hideez.com. Также резервную копию можно хранить на защищенных флэш-накопителях, либо же поместить сам накопитель в надежное место, например, сейф.
 5. Пользуйтесь антивирусным программным обеспечением, не посещайте подозрительные сайты, не устанавливайте ПО из ненадежных источников, не открывайте почтовые вложения с расширениями .exe или .apk.

Приложение 3. Сигналы и состояние Hideez Key

Перечень звуковых сигналов:

1. Alarm - попеременное звучание на частотах 6000 Гц, 2680 Гц, 1080 Гц на протяжении около 5 с
2. Single beep - короткий бип 480 Гц, 80 мс
3. Double beep - два коротких бипа 2680 Гц 80 мс
4. Roger beep - два коротких бипа 480 Гц 80 мс
5. Error beep - три бипа 200 Гц по 200 мс
6. Connected beep - 960 Гц 80 мс, 1360 Гц 80 мс
7. Disconnected beep - 960 Гц 80 мс, 800 Гц 80 мс, 800 Гц 80 мс
8. Peripheral beep - 3400 Гц 160 мс, 3600 Гц 80 мс, 3800 Гц 160 мс
9. Roger beep in menu - 1480 Гц 80 мс, 1880 Гц 80 мс, 3200 Гц 160 мс

Внимание! В случае, если батарея разряжена до 30 %, звуковой сигнал отключается, чтобы замедлить разряд батареи.

Перечень световых сигналов:

1. Connected - индикатор активного подключения по BT, 100 мс горит, 3900 мс пауза. (непрерывно)
2. Fast blink - 100 мс горит, 100 мс пауза. (непрерывно)
3. Slow blink - 500 мс горит, 500 мс пауза. (непрерывно)
4. Double blink - 100 мс горит, 100 мс пауза, 100 мс горит, 800 мс пауза. (однократно)
5. Single Blink - 100 мс горит, 100 мс пауза. (однократно)
6. Constant – непрерывный сигнал

Использование сигналов:

Сигнал		Событие, состояние	
Звук	Свет		
Single beep	Single зеленый	Blink Сопровождение одиночного нажатия на кнопку; отсчет секунд при удерживании кнопки	
Double beep	Double зеленый	blink Готов к работе после включения питания	
Roger beep	Double зеленый	blink Подтверждает принятие команды с кнопки; Подтверждение выполнения команды из инженерного меню	
Error beep	Double красный	blink Ошибка выполнения запрошенной команды	
Connected beep	Double зеленый	blink В момент подключения к устройству	
Disconnected beep	Double красный	blink В момент отключения от устройства	
	Connected зеленый		Hideez Key подключен к устройству
Peripheral beep	Fast красный	blink Вход в режим инженерного меню	
	Slow зеленый	blink Hideez Key находится в широковещательном режиме (advertisement)	
	Constant зеленый		Hideez Key находится в режиме bootloader, не подключен к устройству
	Constant красный		Hideez Key находится в режиме bootloader, подключен к устройству

Приложение 4. Частые вопросы и ответы

Насколько хватает батарей для Hideez Key?

Батареи должно хватить на период до 6 месяцев работы, в зависимости от интенсивности использования и качества самой батареи. Наибольший расход энергии происходит при использовании звуковых сигналов Hideez Key.

Как сменить батарею? Будут ли утеряны данные?

Все пользовательские данные хранятся в энергонезависимой памяти, при выключении питания они сохраняются.

Если я хочу отдать мой Hideez Key, как стереть все мои данные?

Каждое устройство Hideez при первом подключении привязывается к аккаунту My Hideez владельца. Чтобы передать устройство другому человеку, нужно на планшете или компьютере выполнить команду «удалить из аккаунта». Если вы забыли отвязать Hideez Key от аккаунта до того, как отдали ее, можно сделать это удаленно. Для этого нужно войти в свой кабинет на my.hideez.com и выполнить команду «удалить устройство».

Какие физические условия являются опасными для функционирования Hideez Key? Электромагнитное излучение? Солнечный свет? Магнитное поле?

Hideez Key выполнен из пластика и не обеспечивает высокой защиты от пыли и влаги. Электронные компоненты сохраняют свои характеристики при бытовых условиях (прямой солнечный свет, электромагнитное излучение) безопасных для человека. Не рекомендуется подвергать устройство длительному солнечному свету, чтобы избежать старения пластика корпуса.

Возможно ли использование Hideez Key в самолете?

Да, возможно. Устройство принимает и излучает радиочастоты по стандарту Bluetooth 4.0 на небольшое расстояние, и не требует выключения на борту самолета, согласно указаниям FAA от 31.10.2013. При использовании личных медицинских устройств (таких как кардиостимуляторы и слуховые аппараты) проконсультируйтесь с врачом или производителем, чтобы узнать, защищены ли они от внешних радиочастотных сигналов.

Что делать, если мой Hideez Key украли?

Если украли только Hideez Key, а ваш компьютер и телефон остались при вас – удалите Hideez Key из программ Hideez Safe. Не выполняйте команду «Удалить из моего аккаунта», так как там самым вы разрешите использовать ваш Hideez Key как новое устройство. Подключить и использовать ваш Hideez Key никто не сможет, если не знает пароль от вашего аккаунта. Веб-сервер и Hideez Key защищены от попыток подобрать пароль.

Если же украли Hideez Key вместе с устройством, к которому он привязан, то нужно сменить пароль от аккаунта Hideez - после перезапуска программ Hideez Safe они не смогут авторизоваться на сервере и соответственно не смогут использовать Hideez Key.

Если в моем ПК нет адаптера Bluetooth 4.0, могу я использовать Hideez Key?

Да, можно приобрести отдельный адаптер, подключаемый через USB. Подробнее см. [Могут ли мои устройства работать с Hideez Key?](#)

Где физически хранятся мои пароли? Копируются ли они на компьютер/телефон или в облако?

Пароли хранятся только внутри Hideez Key. В момент, когда пароль нужен для использования на компьютере или телефоне, программа Hideez Safe запрашивает его с Hideez Key, вводит и сразу удаляет из памяти. В облако пароли не передаются, но вы можете сделать копию данных с Hideez Key в зашифрованный локальный файл.

Можно ли сделать резервную копию данных с Hideez Key?

Да, клиентское ПО Hideez Safe предусматривает создание резервной копии данных в локальный файл. Весь файл шифруется паролем вашего аккаунта (в который пользователь использует при запуске программы). Файл попадает на диск в уже зашифрованном виде. Используется шифрование по алгоритму AES 256 в режиме CBC.

Следует иметь в виду, что Hideez Key и веб сервис защищены от взлома методом прямого перебора ключей (brute force attack), но файл с резервными данными такой защиты не может иметь в принципе. Поэтому рекомендуется хранить резервную копию данных на внешнем накопителе (например, USB-flash), но не на жестком диске или в облаке.

Оптимально сразу записать резервную копию данных на другой Hideez Key и положить в сейф.

Есть ли какие-то учебные материалы по использованию Hideez Key?

На канале <http://youtube.com/hideez> выложены короткие видеоролики, объединенные в учебные курсы по использованию устройства и работе с программами Hideez.

Смотрите их в плейлистах по использованию для [Android](#), [iOS](#), [Mac](#) и [Windows](#).