**Программа для ЭВМ «Guardant OS»**

(функциональные характеристики)

В данном документе представлено описание функциональных характеристик программного обеспечения и информация, необходимая для установки и эксплуатации программного обеспечения.

**Содержание:**

[1. Описание Guardant OS 2](#_Toc76533023)

[1.1 Список доступных функций Guardant OS в зависимости от модели носителя 3](#_Toc76533024)

[2. Установка 4](#_Toc76533025)

[3. Настройка Guardant OS 4](#_Toc76533027)

[3.1 Инструменты 4](#_Toc76533028)

[3.1.1 Коды доступа 4](#_Toc76533029)

[3.1.2 Guardant SDK 4](#_Toc76533030)

[3.1.3 Mobile SDK 5](#_Toc76533031)

[3.1.4 ARM-компилятор (Yagarto) 5](#_Toc76533032)

[3.2 Настройка 6](#_Toc76533033)

[3.2.1 Запись маски 6](#_Toc76533034)

[3.2.2 Поля общего назначения маски настроек Guardant OS 6](#_Toc76533034)

[3.2.3 Поля свободного назначения маски настроек Guardant OS 6](#_Toc76533034)

[3.2.4 Запись маски настроек Guardant OS с помощью утилиты GrdUtil 6](#_Toc76533034)

[3.2.5 Загрузка кода на носители типа Code 9](#_Toc76533035)

[3.2.5.1 Добавление поля “Загружаемый код” 10](#_Toc76533036)

[3.2.5.2 Свойства загружаемого кода 11](#_Toc76533037)

[3.2.5.3 Временные зависимости загружаемого кода 11](#_Toc76533038)

[3.2.5.4 Запись загружаемого кода 12](#_Toc76533039)

[4. Эксплуатация 12](#_Toc76533040)

[4.1 Работа с данными и алгоритмами Guardant OS 12](#_Toc76533041)

[4.1.1 Работа с защищенной памятью Guardant OS 12](#_Toc76533042)

[4.1.2 Работа с аппаратными и программно-реализованными алгоритмами 13](#_Toc76533043)

[4.1.3 Работа с защищенными ячейками 13](#_Toc76533044)

[4.1.4 Лицензирование приложений по времени работы (для носителей Time) 14](#_Toc76533045)

[4.2 Работа с данными и алгоритмами Guardant OS из загруженного пользовательского кода 14](#_Toc76533046)

[4.2.1 Функция ОС Guardant OS - Guardant Code API 14](#_Toc76533047)

[4.3 Обновление памяти Guardant OS 15](#_Toc76533048)

[4.3.1 Удаленное обновление памяти Guardant OS (технология Trusted Remote Update) 15](#_Toc76533049)

[4.3.2 Удаленное обновление Guardant OS на носителе типа Time 16](#_Toc76533050)

[4.4 Обновление загружаемого кода 17](#_Toc76533051)

# Описание Guardant OS

Программа для ЭВМ «Guardant OS» – это операционная система, предназначенная для защиты стороннего программного обеспечения от нелегального копирования и использования. Поставляется на аппаратном носителе. Носитель – это устройство, представляющее собой независимую и безопасную среду для корректной работы Guardant OS. Носитель подключается к компьютеру или иному оборудованию, на котором работает защищаемое программное обеспечение, через USB-разъем, USB-шину или другие интерфейсы.

Встроенные механизмы Guardant OS:

* Туннельное шифрование трафика протокола обмена между Guardant OS и защищаемым программным обеспечением
* Чтение и запись произвольных бинарных данных в постоянную память по паролю
* Чтение и запись произвольных данных в постоянную память
* Запись произвольного программного кода на языке С или Java в постоянную память по паролю
* Выполнение записанного программного кода по паролю
* Работа с функциями и памятью Guardant OS из записанного кода
* Автоматический контроль количества единовременных сессий работы Guardant OS с экземплярами защищенного программного обеспечения

Поддержка криптографических алгоритмов:

* Электронная подпись на эллиптических кривых ECC160
  + Функция генерации подписи
  + Функция проверка подписи
* Симметричное шифрование AES-128
* Симметричное шифрование GSII64

Возможность устанавливать ограничения на работу криптографических алгоритмов:

* Общее количество использований (вызовов).
* Продолжительность работы в миллисекундах.
* Дата начала и окончания работы.

**Комплект поставки:**

* Операционная система Guardant OS на носителе (часть функций Guardant OS работают только на носителях определенной модели)
* Коды доступов к настройкам Guardant OS (уникальные для каждого вендора защищаемого программного обеспечения)
* Драйвер для работы с носителем (Guardant или HID или WinUSB)

## 1.1 Список доступных функций Guardant OS в зависимости от модели носителя

|  |  |
| --- | --- |
| **Носитель** | **Доступные функции Guardant OS** |
| Guardant Sign | * Туннельное шифрование трафика протокола обмена. * Электронная подпись на эллиптических кривых ECC160 * Симметричное шифрование AES-128 и GSII64 |
| Guardant Time | * Все функции Guardant Sign * Возможность ограничения времени работы криптографических алгоритмов для лицензирования защищаемого приложения по времени |
| Guardant Sign Micro | * Все функции Guardant Sign |
| Guardant Sign SD | * Все функции Guardant Sign |
| Guardant Code | * Электронная подпись на эллиптических кривых ECC160 * Симметричное шифрование AES-128 * Загрузка и исполнение до 20 000 строк кода в постоянной памяти Guardant OS * Поддержка Guardant Mobile API |
| Guardant Stealth II | * Симметричный алгоритм GSII64 с длиной носителя 128 или 256 бит * Алгоритмы шифрования Stealth 1: Autoprotect, Fast, Random |
| Guardant SD | * Поддержка Guardant Mobile API * Загрузка и исполнение апплетов на Java * Ассиметричное шифрование и подпись RSA * Симметричное шифрование AES-128 * Хэширование на базе SHA-1 и SHA-256 |

# Установка

# 

Guardant OS записывается на носитель при предпродажной подготовке, отдельно не поставляется. Каждый экземпляр Guardant OS имеет уникальную конфигурацию для каждого клиента, основанную на персональных кодах доступа.

# Настройка Guardant OS

## 3.1 Инструменты

## 3.1.1 Коды доступа

Коды доступа – набор уникальных идентификаторов для каждого покупателя Guardant OS, единожды генерируются при первой покупке и записываются в память Guardant OS на носителе.

Далее коды доступа вводятся в процессе инсталляции специального ПО для настройки Guardant OS и задаются в исходных кодах приложения, если оно защищается при помощи API.

Все коды доступа (за исключением Public) должны храниться в тайне от третьих лиц.

Существует несколько видов кодов доступа в зависимости от их назначения:

|  |  |
| --- | --- |
| **Вид кода** | **Назначение** |
| Public | Избежать конфликта ПО разных разработчиков на одном компьютере. Используется при поиске носителя/лицензии. |
| Private Read | Защитить выполнение основных операций Guardant OS. Используется при чтении данных из памяти Guardant OS и выполнении алгоритмов. |
| Private Write | Защитить память Guardant OS от перезаписи. Используется при записи данных/лицензии в память Guardant OS. |
| Private Master | Защитить алгоритмы носителя от перезаписи. Требуется при выполнении специальных операций. |

Коды доступа вводятся в процессе инсталляции специализированного ПО для настройки Guardant OS.

Также коды доступа нужно указывать в исходных кодах приложения, если оно защищается при помощи встроенных в Guardant OS функций API.

## 3.1.2 Guardant SDK

Комплект разработчика Guardant SDK – это набор инструментов, который необходим для взаимодействия со всеми функциями операционной системы Guardant OS. Утилиты и библиотеки, входящие в состав комплекта, позволяют настроить Guardant OS и построить защиту ПО разработчика разного уровня сложности и стойкости.

Установка Guardant SDK и драйвера должна производиться пользователем с правами администратора. Guardant SDK доступен для свободной загрузки на странице сайта <https://www.guardant.ru/support/download/sdk/>

1. Необходимо скачать и запустить msi-файл
2. Ввести коды доступа и контрольное число
3. После установки перезагрузить компьютер

В процессе установки ПО на диске в рабочем каталоге Guardant будет создан файл nvcodes.dat с информацией о кодах доступа. Этот файл необходим для настройки Guardant OS.

## 3.1.3 Mobile SDK

Mobile SDK – набор API, примеров и документации для работы с Guardant OS на носителе Guardant SD и носителях семейства Guardant Code, разработки защиты приложений под Android и другие операционные системы.

Mobile SDK доступен для свободной загрузки на странице сайта <https://www.guardant.ru/support/download/mobile/>

1. Необходимо скачать архив
2. Разархивировать и запустить msi-файл
3. Пройти стандартный диалог установки
4. После установки перезагрузить компьютер

## 3.1.4 ARM-компилятор (Yagarto)

Yagarto - это компилятор, который используется для сборки пользовательского исполняемого кода на языке С для последующей записи в постоянную память носителей семейства Guardant Code и исполнения операционной системой Guardant OS.

Yagarto доступен для свободной загрузки на странице сайта <https://www.guardant.ru/support/download/sdk/>

1. Необходимо скачать архив Yagarto.zip
2. Разархивировать и запустить exe-файл Yagarto
3. Пройти стандартный диалог установки
4. Разархивировать и запустить exe-файл Yagarto-tools
5. Пройти стандартный диалог установки
6. Если используется операционная система Windows 8 или более поздняя версия, то из архива с набором утилит необходимо в директорию ..\yagarto-tools\bin скопировать с заменой файл msys-1.0.dll.
7. После установки перезагрузить компьютер

После выполнения этих шагов компилятор полностью готов к работе. Дальнейшая работа с ним будет выполняться посредством вызова утилиты make на заранее созданных и настроенных makefile.

# 3.2 Настройка

## 3.2.1 Запись маски

Совокупность всех полей памяти, доступной для хранения настроек Guardant OS составляют так называемый образ – маску памяти. Она хранится в специальном файле.

Чтобы записать настройки Guardant OS, предварительно их необходимо занести в заранее созданное поле.

3.2.2 Поля общего назначения маски настроек Guardant OS  
 Группа полей, назначение которых предопределено. Для этих полей «закреплено» фиксированное место в памяти Guardant OS. Поэтому возможно только редактирование содержимого полей, но не удаление.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Адрес (UAM)** | **Название и тип поля** | **Диапазон значений, DEC** | **Назначение** | **Работа с полем из приложения** | |
| **Авто-защита** | **API** |
| 0000 | Номер программы, беззнаковое целое | 0 – 255 | «Привязка» копии приложения к Guardant OS для поддержки нескольких программных продуктов | [**/UN[=[0x]...]**](https://dev.guardant.ru/pages/viewpage.action?pageId=1279030) | [**GrdSetFindMode**](https://dev.guardant.ru/display/DOC/GrdSetFindMode)**,** [**GrdGetInfo**](https://dev.guardant.ru/display/DOC/GrdGetInfo)**,** [**GrdRead**](https://dev.guardant.ru/display/DOC/GrdRead)**,** [**GrdWrite**](https://dev.guardant.ru/display/DOC/GrdWrite) |
| 0001 | Версия, беззнаковое целое | 0 – 255 | «Привязка» копии приложения к Guardant OS для поддержки новых версий программы | [**/UV[=[0x]...]**](https://dev.guardant.ru/pages/viewpage.action?pageId=1279021) |
| 0002 | Серийный №, счетчик | 0 – 65535 | «Привязка» конкретной копии приложения к Guardant OS | [**/US[=[0x]...]**](https://dev.guardant.ru/pages/viewpage.action?pageId=1279011) |
| 0004 | Битовая маска, беззнаковое целое | 0 – 65535 | Разрешение/запрет на работу с отдельными, независимыми модулями программного комплекса | [**/UM[=[0x]..]**](https://dev.guardant.ru/pages/viewpage.action?pageId=1279024) |
| 0006 | Счетчик №1 (GP), беззнаковое целое | 0 – 65535 | Устаревшая технология. Теперь для ограничения числа запусков приложения необходимо использовать счетчики аппаратных алгоритмов | - | - |
| 0008 | Счетчик №2, беззнаковое целое | 0 - 65535 | Отображение реального ресурса лицензий Guardant OS для сетевых носителей (в современных сетевых носителях сетевой ресурс хранится в таблице лицензий, а в счетчике №2 только отображается) | [**/GN2** **/GN3** **/GN3S**](https://dev.guardant.ru/pages/viewpage.action?pageId=1279267) | [**GrdSetFindMode**](https://dev.guardant.ru/display/DOC/GrdSetFindMode)**,** [**GrdGetInfo**](https://dev.guardant.ru/display/DOC/GrdGetInfo)**,** [**GrdRead**](https://dev.guardant.ru/display/DOC/GrdRead)**,** [**GrdWrite**](https://dev.guardant.ru/display/DOC/GrdWrite) |
| 0010 | Индекс, беззнаковое целое | - | Предназначено для дистанционного программирования носителя.  Нельзя использовать для хранения данных. | - | - |

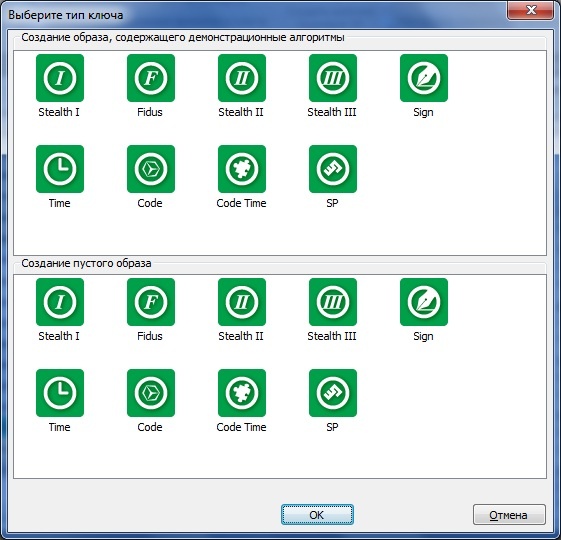
3.2.3 Поля свободного назначения маски настроек Guardant OS

В полях свободного назначения могут храниться любые данные, необходимые для защиты приложений: в том числе, дескрипторы аппаратных алгоритмов, таблицы лицензий, ключевые слова, наборы данных, константы и проч.  
 Здесь можно создавать поля различных типов, редактировать их содержимое и удалять эти поля.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Тип поля** | | **Размер, байтов** | **Содержимое** | **Аппаратные запреты** | **Работа с полем из приложения (**[**Guardant API**](https://dev.guardant.ru/pages/viewpage.action?pageId=1278128)**)** |
| Алгоритм | | Размер поля определяется размером дескриптора алгоритма | Дескриптор аппаратного алгоритма | Обязательные запреты на запись и чтение | [GrdTransform](https://dev.guardant.ru/display/DOC/GrdTransform), [GrdCrypt](https://dev.guardant.ru/display/DOC/GrdCrypt), [GrdHash](https://dev.guardant.ru/display/DOC/GrdHash), [GrdCodeInit](https://dev.guardant.ru/display/DOC/GrdCodeInit)  [GrdPI\_Activate](https://dev.guardant.ru/display/DOC/GrdPI_Activate), [GrdPI\_Deactivate](https://dev.guardant.ru/display/DOC/GrdPI_Deactivate), [GrdPI\_Read](https://dev.guardant.ru/display/DOC/GrdPI_Read), [GrdPI\_Update](https://dev.guardant.ru/display/DOC/GrdPI_Update)  [GrdTRU\_DecryptQuestion](https://dev.guardant.ru/display/DOC/GrdTRU_DecryptQuestion), [GrdTRU\_EncryptAnswer](https://dev.guardant.ru/display/DOC/GrdTRU_EncryptAnswer), [GrdTRU\_ApplyAnswer](https://dev.guardant.ru/display/DOC/GrdTRU_ApplyAnswer) |
| Защищенная ячейка | | В новых носителях произвольный размер.  В старых:1 – 255 Б+ служебные поля | Дескриптор защищенной ячейки | Обязательные запреты на запись и чтение | [GrdPI\_Activate](https://dev.guardant.ru/display/DOC/GrdPI_Activate), [GrdPI\_Deactivate](https://dev.guardant.ru/display/DOC/GrdPI_Deactivate), [GrdPI\_Read](https://dev.guardant.ru/display/DOC/GrdPI_Read), [GrdPI\_Update](https://dev.guardant.ru/display/DOC/GrdPI_Update) |
| Таблица лицензий | Носитель Guardant Sign Net/ Time Net/ Net III | Длина каждого модуля=1 или 2 Б Максимум - 254 байта +служебные поля | 1. Реальный сетевой ресурс  2. Количество модулей программного комплекса и их ресурсы лицензий | Обязательные запреты на запись и чтение | [GrdPI\_Activate](https://dev.guardant.ru/display/DOC/GrdPI_Activate), [GrdPI\_Deactivate](https://dev.guardant.ru/display/DOC/GrdPI_Deactivate), [GrdPI\_Read](https://dev.guardant.ru/display/DOC/GrdPI_Read), [GrdPI\_Update](https://dev.guardant.ru/display/DOC/GrdPI_Update) |
| Носитель Guardant Net II / Net | Длина каждого модуля=1 или 2 Б Максимум – 127 модулей | Количество модулей программного комплекса и их ресурс лицензий | Обязательный запрет на запись | [GrdRead](https://dev.guardant.ru/display/DOC/GrdRead) |
| Целое число | | 1, 2, 4, 8 | Целое число со знаком или без знака | Запрет на запись (при необходимости) | [GrdRead](https://dev.guardant.ru/display/DOC/GrdRead), [GrdWrite](https://dev.guardant.ru/display/DOC/GrdWrite) |
| Загружаемый код | |  |  |  |  |
| Строка | | Произвольный размер | Последовательность символов в кодировке ANSI или Unicode | Запрет на запись (при необходимости) | [GrdRead](https://dev.guardant.ru/display/DOC/GrdRead), [GrdWrite](https://dev.guardant.ru/display/DOC/GrdWrite) |
| Счетчик | | 1, 2, 4, 8 | Беззнаковое целое число. Автоматически увеличивается на 1 после каждой записи образа в память Guardant OS | Запрет на запись (при необходимости) | [GrdRead](https://dev.guardant.ru/display/DOC/GrdRead), [GrdWrite](https://dev.guardant.ru/display/DOC/GrdWrite) |
| Дамп памяти | | Произвольный размер | Двоичный дамп | Запрет на запись (при необходимости) | [GrdRead](https://dev.guardant.ru/display/DOC/GrdRead), [GrdWrite](https://dev.guardant.ru/display/DOC/GrdWrite) |

3.2.4 Запись маски настроек Guardant OS с помощью утилиты GrdUtil

Создание и редактирование масок выполняется в программе GrdUtil, входящей в Guardant SDK.  
 Чтобы создать новую маску, запустите GrdUtil и выполните команду меню “Меню приложения | Создать образ”. В появившемся диалоге выберите тип образа для работы с определенным типом носителей:

  
  
 При первом запуске утилиты появляется диалог создания новой маски.

Тип создаваемой маски должен соответствовать модели носителя, который на данный момент подсоединен к порту.

После нажатия кнопки [ОК] новая маска загружается в Редактор маски и ей присваивается имя формата <модель носителя><год>\_<месяц>\_<число>.nsd, которое потом можно изменить. Имя маски отображается в заголовке главного окна утилиты.

В процессе записи данных GrdUtil автоматически переносит на носитель всю информацию из маски настроек, загруженного в Редактор, и корректирует границы аппаратных запретов в случае их изменения.

## 3.2.5 Загрузка кода на носители типа Code

Если Guardant OS использует носители семейства Guardant Code, есть возможность загружать и исполнять в памяти специально написанный код приложения.

Защитный механизм загружаемого кода основан на том, что запрограммированный разработчиком алгоритм обрабатывает полезные данные в памяти Guardant OS. Обработанные данные можно использовать в приложении напрямую, исключая проверки валидности, которые, как правило, сводятся к одной-двум ассемблерным командам.

Поток натуральных данных не постоянен и разнообразен, поэтому алгоритм загружаемого кода производит вычисления на постоянно меняющихся данных при условии оптимально подобранного и корректно реализованного алгоритма.

GrdUtil.exe предоставляет удобный сервис для работы с загружаемыми кодом, в том числе, его автоматическое преобразование из Bin-файла в формат, пригодный для записи память Guardant OS (GCEXE), и, собственно, запись GCEXE в память Guardant OS.

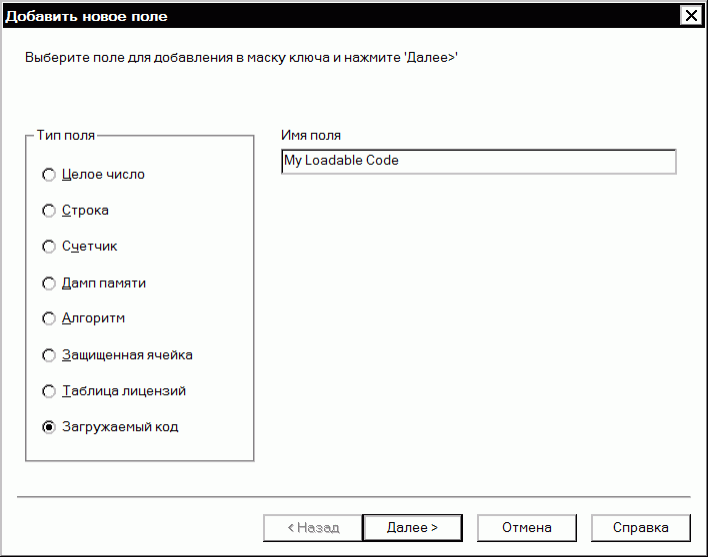
Работа с полем типа “Загружаемый код” происходит при помощи специальных функций API: [GrdCodeGetInfo](https://dev.guardant.ru/display/DOC/GrdCodeGetInfo), [GrdCodeLoad](https://dev.guardant.ru/display/DOC/GrdCodeLoad), [GrdCodeRun](https://dev.guardant.ru/display/DOC/GrdCodeRun).

Диалог создания поля выполнен в виде мастера, состоящего из нескольких страниц:

* Добавить загружаемый код
* Свойства загружаемого кода
* Временные зависимости (для Guardant Code Time)
* [Запись загружаемого кода](https://dev.guardant.ru/pages/viewpage.action?pageId=1279938)

## 3.2.5.1 Добавление поля “Загружаемый код”

Чтобы создать поле типа “Загружаемый код”, выполните команду “Образ ключа| (поле) Добавить поле.”

В появившемся диалоге выберите переключатель “Загружаемый код” и задайте имя поля:  
  
Ячейка “Загружаемый код” имеет фиксированный размер 160 байт.

## 3.2.5.2 Свойства загружаемого кода

Поле типа “Загружаемый код” представляет собой частный случай [защищенной ячейки](https://dev.guardant.ru/pages/viewpage.action?pageId=1048587), то есть, оно защищено аппаратными запретами на чтение и запись. И его состояние можно программировать и, в дальнейшем, управлять им из приложения.

Для загружаемого кода доступны только сервисы активации и деактивации, которые управляют состоянием защищенной ячейки и обеспечивают доступ к ее содержимому из приложения.

Работа с сервисами активации и деактивации загружаемого кода полностью идентична работе с сервисами защищенных ячеек и алгоритмов.

## 3.2.5.3 Временные зависимости загружаемого кода

В маске настроек для носителя Guardant Code Time, содержащего часы реального времени, за страницей “Свойства загружаемого кода” следует страница “Временные зависимости”, на которой расположены элементы, позволяющие ограничивать время работы защищенного приложения.

Смысл технологии ограничения времени заключается в том, что работоспособность ячейки “Загружаемый код” зависит от таймера (RTC), встроенного в носитель Guardant Code Time.

## 3.2.5.4 Запись загружаемого кода

После компиляции кода и получения Bin-файла разработчику необходимо передать бинарный код в GrdUtil.exe для его обработки и записи защищенную память Guardant OS. Для этого служит вкладка “Настройки загружаемого кода”.

Для записи кода необходимо последовательно выполнить действия во вкладке:

1) Импортировать предварительно скомпилированный код из Bin-файла  
2) Преобразовывать импортированный код в формат GCEXE, пригодный для записи в память Guardant OS на носителе типа Guardant Code / Code Time  
3) После выполнения настроек загружаемого кода - завершить диалог и выполнить загрузку кода. При этом будут сформированы и записаны в память:

* Прошивка, содержащая дескриптор загружаемого кода (в числе прочих полей).
* Загружаемый код в формате GCEXE.

# 4. Эксплуатация

## 4.1 Работа с данными и алгоритмами Guardant OS

## 4.1.1 Работа с защищенной памятью Guardant OS

## 

Функции(методы) работы с защищенной памятью Guardant OS позволяют осуществлять сервисные операции, связанные с инициализацией и защитой памяти, а также выполнять операции, связанные с чтением информации из памяти и записью необходимых данных в память.

|  |  |  |
| --- | --- | --- |
| **Название функции(метода)** | **Код доступа** | **Краткое описание** |
| [GrdSetWorkMode](https://dev.guardant.ru/display/DOC/GrdSetWorkMode) | Не нужен | Установить режимы работы Guardant API |
| [GrdRead](https://dev.guardant.ru/display/DOC/GrdRead) | Private Read | Прочитать данные из памяти Guardant OS |
| [GrdWrite](https://dev.guardant.ru/display/DOC/GrdWrite) | Private Write | Записать данные в память Guardant OS |
| [GrdSeek](https://dev.guardant.ru/display/DOC/GrdSeek) | Не нужен | Переместить указатель на текущий адрес памяти Guardant OS |
| [GrdInit](https://dev.guardant.ru/display/DOC/GrdInit) | Private master | Инициализировать память Guardant OS |
| [GrdProtect](https://dev.guardant.ru/display/DOC/GrdProtect) | Private master | Установить аппаратные запреты чтения/записи и записать количество аппаратных алгоритмов и защищенных ячеек |

## 4.1.2 Работа с аппаратными и программно-реализованными алгоритмами

Функции(методы) работы этого раздела позволяют преобразовывать, кодировать и декодировать данные с помощью аппаратно- или программно-реализованных алгоритмов.

Они позволяют вычислить и проверить ЭЦП массива данных.

|  |  |  |
| --- | --- | --- |
| **Название функции(метода)** | **Код доступа** | **Краткое описание** |
| [GrdTransformEx](https://dev.guardant.ru/display/DOC/GrdTransformEx) | Private Read | Преобразовать данные аппаратно- или программно-реализованным алгоритмом |
| [GrdCryptEx](https://dev.guardant.ru/display/DOC/GrdCryptEx) | Private Read | Закодировать/раскодировать данные аппаратно или программно-реализованным алгоритмом |
| [GrdHashEx](https://dev.guardant.ru/display/DOC/GrdHashEx) | Private Read | Расширенный вариант [GrdHash](https://dev.guardant.ru/display/DOC/GrdHash) |
| [GrdSign](https://dev.guardant.ru/display/DOC/GrdSign) | Private Read | Вычислить ЭЦП массива данных |
| [GrdVerifySign](https://dev.guardant.ru/display/DOC/GrdVerifySign) | Не нужен | Проверить ЭЦП массива данных |
| [GrdCRC](https://dev.guardant.ru/display/DOC/GrdCRC) | не нужен | Вычислить CRC |

## 4.1.3 Работа с защищенными ячейками

Для работы с защищенными ячейками существуют специальные функции (методы) Guardant OS API:

|  |  |  |
| --- | --- | --- |
| **Название функции(метода)** | **Код доступа** | **Краткое описание** |
| [GrdPI\_Activate](https://dev.guardant.ru/display/DOC/GrdPI_Activate) | Private Read и пароль на данную операцию | Активировать алгоритм / защищенную ячейку |
| [GrdPI\_Deactivate](https://dev.guardant.ru/display/DOC/GrdPI_Deactivate) | Private Read и пароль на данную операцию | Деактивировать аппаратный алгоритм или защищенную ячейку |
| [GrdPI\_Read](https://dev.guardant.ru/display/DOC/GrdPI_Read) | Private Read и пароль на данную операцию | Прочитать данные из защищенной ячейки |
| [GrdPI\_Update](https://dev.guardant.ru/display/DOC/GrdPI_Update) | Private Read и пароль, на данную операцию | Обновить данные в защищенной ячейке |
| [GrdPI\_GetCounter](https://dev.guardant.ru/display/DOC/GrdPI_GetCounter) | Private Read | Получить значение счетчика запусков алгоритма |

## 4.1.4 Лицензирование приложений по времени работы (для носителей Time)

Носители Guardant Time/Time Net/Code Time обладают встроенными часами реального времени (Real-Time Clock, RTC), что позволяет ограничивать астрономическое время работы приложения с помощью установки временных зависимостей от аппаратных алгоритмов, используемых Guardant OS. Для работы с возможностями, которые присущи только носителям с RTC, существуют специальные функции Guardant OS API:

|  |  |  |
| --- | --- | --- |
| **Название функции(метода)** | **Код доступа** | **Краткое описание** |
| [GrdSetTime](https://dev.guardant.ru/display/DOC/GrdSetTime) | Private Master | Установить время микросхемы таймера носителя |
| [GrdGetTime](https://dev.guardant.ru/display/DOC/GrdGetTime) | Private Read | Получить время таймера носителя |
| [GrdPI\_GetTimeLimit](https://dev.guardant.ru/display/DOC/GrdPI_GetTimeLimit) | Private Read | Получить оставшееся время работы алгоритма |
| [GrdMakeSystemTime](https://dev.guardant.ru/display/DOC/GrdMakeSystemTime) | Не нужен | Заполнить поля структуры TgrdSystemTime |
| [GrdSplitSystemTime](https://dev.guardant.ru/display/DOC/GrdSplitSystemTime) | Не нужен | Получить значение полей структуры TgrdSystemTime |

## 4.2 Работа с данными и алгоритмами Guardant OS из загруженного пользовательского кода

## 4.2.1 Функция ОС Guardant OS - Guardant Code API

Технология Guardant Code API позволяет использовать сервисы операционной системы Guardant OS на носителе семейства Code, вызывая их при помощи загружаемого кода (операционная система предоставляет свои сервисы пользовательской программе посредством API). При желании разработчики могут встраивать поддержку этой технологии непосредственно в свои приложения, используя набор предназначенных для этой цели функций:

|  |  |  |
| --- | --- | --- |
| **Название функции** | **Код доступа** | **Краткое описание** |
| [GcaRead](https://dev.guardant.ru/display/DOC/GcaRead) | - | Считать данные из памяти Guardant OS |
| [GcaWrite](https://dev.guardant.ru/display/DOC/GcaWrite) | - | Записать данные в память Guardant OS |
| [GcaPI\_Read](https://dev.guardant.ru/display/DOC/GcaPI_Read) | - | Считать данные защищенной ячейки |
| [GcaPI\_Update](https://dev.guardant.ru/display/DOC/GcaPI_Update) | - | Изменить данные защищенной ячейки или определителя алгоритма |
| [GcaGetTime](https://dev.guardant.ru/display/DOC/GcaGetTime) | - | Получить время таймера носителя |
| [GcaPI\_GetTimeLimit](https://dev.guardant.ru/display/DOC/GcaPI_GetTimeLimit) | - | Получить оставшееся время работы алгоритма |
| [GcaPI\_GetCounter](https://dev.guardant.ru/display/DOC/GcaPI_GetCounter) | - | Получить значение счетчика запусков алгоритма |
| [GcaGetLastError](https://dev.guardant.ru/display/DOC/GcaGetLastError) | - | Получить код последней ошибки |
| [GcaGetRTCQuality](https://dev.guardant.ru/display/DOC/GcaGetRTCQuality) | - | Выполнить тест часов реального времени - RTC |
| [GcaLedOn](https://dev.guardant.ru/display/DOC/GcaLedOn) | - | Включить светодиод |
| [GcaLedOff](https://dev.guardant.ru/display/DOC/GcaLedOff) | - | Выключить светодиод |
| [GcaExit](https://dev.guardant.ru/display/DOC/GcaExit) | - | Завершить выполнение загруженного кода |
| [GccaCryptEx](https://dev.guardant.ru/display/DOC/GccaCryptEx) | - | Зашифровать/расшифровать блок данных |
| [GccaSign](https://dev.guardant.ru/display/DOC/GccaSign) | - | Вычислить ЭЦП массива данных |
| [GccaVerifySign](https://dev.guardant.ru/display/DOC/GccaVerifySign) | - | Проверить ЭЦП массива данных |
| [GcaCodeRun](https://dev.guardant.ru/display/DOC/GcaCodeRun) | - | Выполнить загружаемый код из другого участка загружаемого кода |
| [GccaGenerateKeyPair](https://dev.guardant.ru/display/DOC/GccaGenerateKeyPair) | - | Создать пару ключей |
| [GccaHash](https://dev.guardant.ru/display/DOC/GccaHash) | - | Вычислить хэш-функцию блока данных |
| [GccaGetRandom](https://dev.guardant.ru/display/DOC/GccaGetRandom) | - | Сгенерировать случайное число |
| [GcaSetTimeout](https://dev.guardant.ru/display/DOC/GcaSetTimeout) | - | Установить максимально разрешенное время работы загружаемого кода |
| [GcaCodeGetInfo](https://dev.guardant.ru/display/DOC/GcaCodeGetInfo) | - | Запросить информацию из дескриптора загружаемого кода |

# 4.3 Обновление памяти Guardant OS

## 4.3.1 Удаленное обновление памяти Guardant OS (технология Trusted Remote Update)

Технология удаленного обновления Trusted Remote Update может быть реализована не только при помощи утилит, входящих в Комплект разработчика. При желании разработчики могут встраивать поддержку этой технологии непосредственно в свои приложения, используя набор предназначенных для этой цели функций:

|  |  |  |
| --- | --- | --- |
| **Название функции(метода)** | **Код доступа** | **Краткое описание** |
| [GrdTRU\_SetKey](https://dev.guardant.ru/display/DOC/GrdTRU_SetKey) | Private Master | Инициализировать память Guardant OS и записать секретный ключ TRU |
| [GrdTRU\_GenerateQuestion](https://dev.guardant.ru/display/DOC/GrdTRU_GenerateQuestion) | Private Read | Сгенерировать число-вопрос |
| [GrdTRU\_GenerateQuestionEx](https://dev.guardant.ru/display/DOC/GrdTRU_GenerateQuestionEx) | Private Read | Расширенная версия [GrdTRU\_GenerateQuestion](https://dev.guardant.ru/display/DOC/GrdTRU_GenerateQuestion) |
| [GrdTRU\_DecryptQuestion](https://dev.guardant.ru/display/DOC/GrdTRU_DecryptQuestion) | Private Read | Декодировать и проверить подлинность числа-вопроса |
| [GrdTRU\_DecryptQuestionEx](https://dev.guardant.ru/display/DOC/GrdTRU_DecryptQuestionEx) | Private Read | Расширенная версия [GrdTRU\_DecryptQuestion](https://dev.guardant.ru/display/DOC/GrdTRU_DecryptQuestion) |
| [GrdTRU\_SetAnswerProperties](https://dev.guardant.ru/display/DOC/GrdTRU_SetAnswerProperties) | Не нужен | Установить параметры числа-ответа |
| [GrdTRU\_EncryptAnswer](https://dev.guardant.ru/display/DOC/GrdTRU_EncryptAnswer) | Private Read | Сгенерировать и кодировать число-ответ |
| [GrdTRU\_EncryptAnswerEx](https://dev.guardant.ru/display/DOC/GrdTRU_EncryptAnswerEx) | Private Read | Расширенная версия [GrdTRU\_EncryptAnswer](https://dev.guardant.ru/display/DOC/GrdTRU_EncryptAnswer) |
| [GrdTRU\_ApplyAnswer](https://dev.guardant.ru/display/DOC/GrdTRU_ApplyAnswer) | Private Read | Записать число-ответ в носитель Guardant |

## 4.3.2 Удаленное обновление Guardant OS на носителе типа Time

Функции, реализующие технологию Trusted Remote Update для носителей с часами реального времени (Guardant Time, Guardant Time Net, Guardant Code Time) имеют некоторые отличия от своих [аналогов для других носителей](http://developer.guardant.ru/pages/viewpage.action?pageId=1278396) и поэтому выделяются в особую подгруппу:

|  |  |  |
| --- | --- | --- |
| **Название функции(метода)** | **Код доступа** | **Краткое описание** |
| [GrdTRU\_GenerateQuestionTime](https://dev.guardant.ru/display/DOC/GrdTRU_GenerateQuestionTime) | Private Read | Сгенерировать зашифрованное число-вопрос |
| [GrdTRU\_DecryptQuestionTimeEx](https://dev.guardant.ru/display/DOC/GrdTRU_DecryptQuestionTimeEx) | Private Read | Расширенная версия [GrdTRU\_GenerateQuestionTime](https://dev.guardant.ru/display/DOC/GrdTRU_GenerateQuestionTime) |
| [GrdTRU\_DecryptQuestionTime](https://dev.guardant.ru/display/DOC/GrdTRU_DecryptQuestionTime) | Private Read | Расшифровать и проверить подлинность числа-вопроса |
| [GrdTRU\_GenerateQuestionTimeEx](https://dev.guardant.ru/display/DOC/GrdTRU_GenerateQuestionTimeEx) | Private Read | Расширенная версия [GrdTRU\_DecryptQuestionTime](https://dev.guardant.ru/display/DOC/GrdTRU_DecryptQuestionTime) |

# 4.4 Обновление загружаемого кода

Если в защищенной памяти Guardant OS находится загруженный код, то для его обновления необходимо выполнение следующих условий:

* У разработчика должен храниться файл маски, содержащий ключевые пары для шифрования и подписи загружаемого кода.
* У конечного пользователя должна находиться Guardant OS на носителе семейства Guardant Code, содержащая дескриптор алгоритма с загружаемым кодом, а также закрытый ключ для расшифрования кода и открытый ключ для проверки ЭЦП.
* Ключевые пары в маске и носителе должны быть идентичны.
* Для обновления загружаемого кода необходимо сгенерировать новый GCEXE -файл с обновленным кодом, зашифрованным и подписанным на соответствующих ключах.
* Само обновление может производиться как при помощи технологии TRU, так и прямой загрузкой GCEXE-файла из защищаемого приложения функцией GrdCodeLoad().

При желании можно сделать процедуру обновления загружаемого кода «прозрачной» для пользователя. Тогда от него потребуется только получить обновление, поместить его рядом с исполняемым файлом приложения (или в специально для этого предназначенную директорию) и запустить приложение.