

Guardant S P

Руководство пользователя



Содержание

1. Общая информация	3
1.1. Введение	3
1.2. О ключе Guardant SP	3
1.3. Принцип работы Guardant SP	4
1.4. Быстрый старт	5
1.5. Технические характеристики Guardant SP	5
1.6. Демонстрационные ключи Guardant SP	6
2. Подготовка к защите	7
2.1. Регистрация и установка Guardant SDK	7
2.2. Настройка продуктов и серийных номеров	7
3. Защита при помощи Guardant SP	8
3.1. Автоматическая защита	8
3.2. Создание шаблона программного ключа в GrdUtil	11
3.3. Защита с использованием Guardant API	12
3.4. Использование ключей в Linux	12
4. Лицензирование по времени работы	13
4.1. Принцип работы	13
4.2. Установка ограничений по времени работы	13
4.3. Механизмы ограничения времени	15
4.4. Особенности использования	15
5. Лицензирование по сети	16
5.1. Принцип работы	16
5.2. Создание и подготовка ключа	16
5.3. Активация и использование ключа	17
6. Распространение защищенного ПО	17
6.1. Комплект поставки защищенного приложения	17
6.2. Активация Guardant SP у конечного пользователя	18

1. Общая информация

1.1. Введение

Софтверный ключ Guardant SP объединяет в себе преимущества технологий защиты Guardant и удобство распространения и активации через Интернет. Приобретение и управление ключами Guardant SP осуществляется на сервере активации, расположенном по адресу <https://sp.guardant.ru>.

Guardant SP используется для привязки программы к копии ключа и предотвращения пиратского распространения этой программы. Защитные технологии ключа не позволят пользователю скопировать его и использовать на другом компьютере. А без ключа защищенное приложение останется неработоспособным.

Для обеспечения надежной защиты инфраструктура софтверных ключей включает в себя сервер активации — доверенную сторону, позволяющую активировать ключи конечных пользователей.

1.2. О ключе Guardant SP

Guardant SP — это софтверная реализация современных электронных ключей Guardant, предоставляющая клиенту практически все возможности защиты, что и аппаратные ключи. Особенностью Guardant SP является криптографическая привязка к оборудованию. Т.е. защищенное приложение может отслеживать изменения в конфигурации оборудования конечного пользователя.

Приложение защищается и работает с таким ключом по тем же принципам, что и с аппаратными ключами Guardant. Главным отличием является то, что вся логика софтверного ключа расположена в защищенной псевдокодом части драйвера Guardant и выполняется непосредственно на компьютере пользователя.

При проведении автозащиты (или использовании Guardant API) защищаемое приложение надежно привязывается к экземпляру софтверного ключа, где используются симметричный алгоритм шифрования AES128 и алгоритм электронной цифровой подписи ECC160.

Получившийся ключ защиты остается неработоспособным до его активации на компьютере конечного пользователя с использованием уникального серийного номера. При активации ключ криптографически привязывается к составляющим компьютера, защищая программу от несанкционированного копирования.

Начиная с драйверов Guardant версии 6.2, софтверный ключ поддерживает функциональность Guardant Time (лицензирование по времени работы с использованием механизмов ограничения времени) и Guardant Net (создание и активация ключа на несколько лицензий с возможностью раздачи этих лицензий по сети).

Guardant SP поддерживает все современные операционные системы Windows. Софтверные ключи также работают в операционных системах семейства Linux. Однако в этом случае недоступна автоматическая защита (привязка к ключу осуществляется только через API), функционал Time и Net.

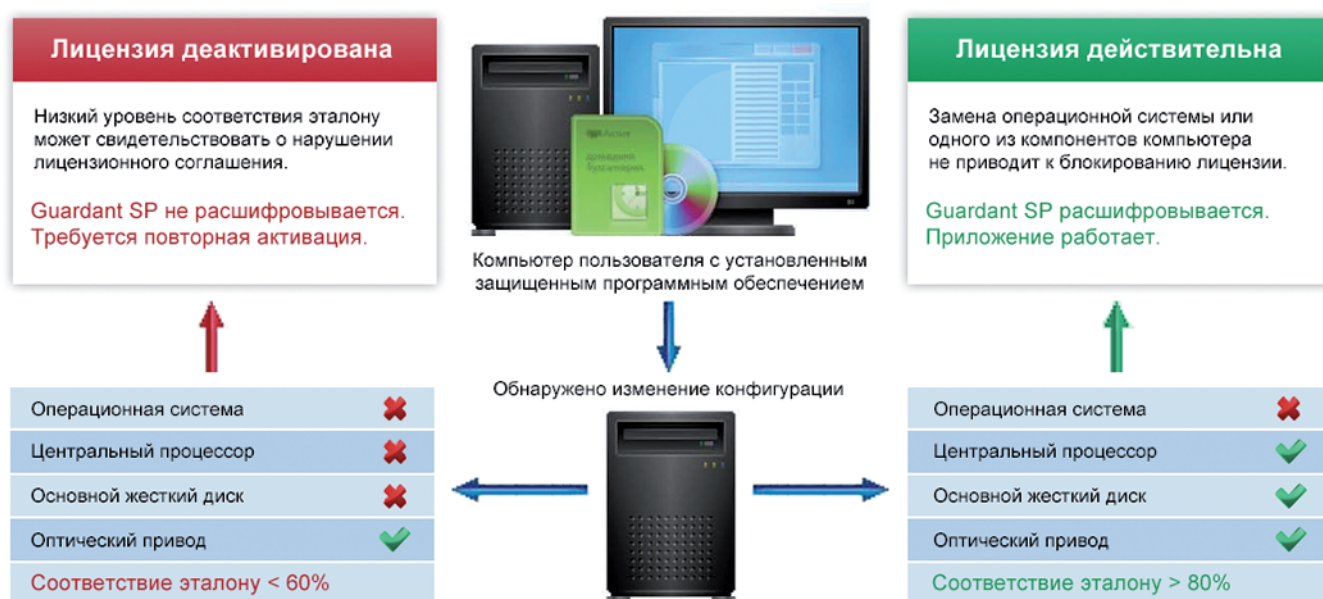
1.3. Принцип работы Guardant SP

Организация защиты приложения при помощи Guardant SP состоит из двух этапов:

1. Привязка защищаемого приложения к шаблону программного ключа посредством автоматической защиты или Guardant API;
2. Активация шаблона программного ключа серийным номером и привязка ключа к компьютеру конечного пользователя.

Шаблон программного ключа — это файл с расширением .grdvd, содержащий набор полей, алгоритмов шифрования и подписи. После активации серийным номером он преобразуется в полностью работоспособный ключ Guardant SP.

Шаблон уникально определяет содержимое ключа и его криптографические возможности. Он создается разработчиком софта при проектировании системы защиты приложения и надежно зашифрован и подписан ключами разработчика. Шаблон может быть переподписан и перешифрован только на сервере активации компании «Актив» таким образом, чтобы он стал работоспособен лишь на том компьютере, где проводилась активация.



Важно: все программные ключи равноправны, не существует понятия «ключ разработчика» или «мастер-ключ». Если необходимо протестировать работу защищенного приложения при помощи ключа с нужной маской, такой ключ необходимо создать и активировать на компьютере разработчика. Также произвольную маску можно записать в уже активированный ключ. Таким образом для выполнения защиты и отладки на компьютере разработчика необходимо создать один работоспособный отладочный ключ Guardant SP. Активировать более одного ключа на компьютере разработчика обычно не требуется.

1.4. Быстрый старт

При регистрации на сервере активации или приобретении Комплекта Разработчика Guardant клиент бесплатно получает комплект ключей Guardant SP. Для того чтобы воспользоваться софтверным ключом и защитить приложение, достаточно совершить несколько шагов:

1. Зарегистрироваться на сервере активации по адресу <https://sp.guardant.ru>;
2. Скачать Guardant SDK с сайта www.guardant.ru;
3. Дождаться завершения регистрации на сервере активации (1-3 рабочих дня). В письме-оповещении будет приложен файл nvcodes.dat, содержащий коды доступа. Его нужно скопировать в папку установки Guardant SDK, подпапку Bin;
4. На сервере активации через несколько минут после завершения регистрации появится комплект серийных номеров Guardant SP. Нужно задать список продуктов, которые планируется защищать, и провести назначение серийным номерам этих продуктов (чтобы конкретным серийным номером можно было активировать ключ только для определенного продукта);
5. Запустить Мастер лицензирования и автоматической защиты (входит в состав Guardant SDK) и произвести защиту, указав любой серийный номер с соответствующим продуктом и статусом «Готов к активации».

После выполнения описанных шагов в директории с проектом автозащиты будет сформирован шаблон софтверного ключа (файл с расширением .grdvd), который необходимо распространять вместе с защищенной программой. Активация шаблона производится при помощи серийного номера и утилиты Мастер активации.

1.5. Технические характеристики Guardant SP

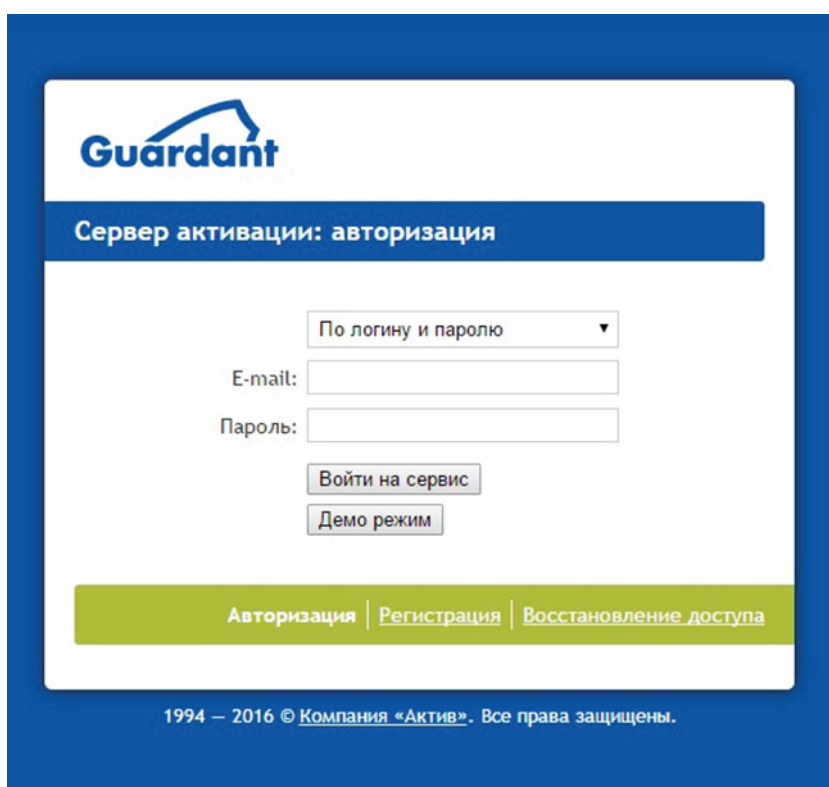
Доступная память	4096 байт эмулируемой EEPROM
Поддерживаемые аппаратные алгоритмы	AES-128 (симметричное шифрование)
	ECC160 (электронная цифровая подпись)
	SHA-256 (хеширование)
Функциональные возможности	Шифрование трафика протокола обмена
	Поддержка Linux
	Автоматическая защита Native и .NET-приложений
	Псевдокод и обфускация компонентов защиты
	Часы реального времени
	Лицензирование по сети
	Оффлайн активация
Привязка к оборудованию	Операционная система
	Процессор (для Linux дополнительно привязка к материнской плате и MAC)
	Жесткий диск
	Оптический привод

1.6. Демонстрационные ключи Guardant SP

Уникальность ключей Guardant SP для каждого разработчика обеспечивается ключами шифрования AES128 и подписи ECC160, присваиваемыми разработчику при регистрации на сервере активации. Они позволяют перешифровать шаблон для привязки к компьютеру конечного пользователя.

Однако для удобства ознакомления с Guardant SP существуют демонстрационные софтверные ключи. Их криптографические ключи AES128 и ECC160 находятся в открытом доступе, поэтому демонстрационные ключи бесполезно использовать для защиты коммерческого программного обеспечения.

Для установки демонстрационных Guardant SP необходим специальный аккаунт на сервере активации и Мастер лицензирования и автоматической защиты (входит в состав Guardant SDK).



The screenshot shows the 'Сервер активации: авторизация' (Activation Server: Authorization) page. At the top is the Guardant logo. Below it is a blue header bar with the text 'Сервер активации: авторизация'. The main content area contains a dropdown menu labeled 'По логину и паролю' with a downward arrow. Below this are two input fields: 'E-mail:' and 'Пароль:'. Under the password field are two buttons: 'Войти на сервис' and 'Демо режим'. At the bottom of the form is a green bar with three links: 'Авторизация', 'Регистрация', and 'Восстановление доступа'. The footer of the page contains the text '1994 — 2016 © Компания «Актив». Все права защищены.'

Сервер активации располагается по адресу <https://sp.guardant.ru>. Для ознакомления с его возможностями можно воспользоваться демонстрационным режимом, нажав соответствующую кнопку на форме авторизации. Все софтверные ключи, представленные на сервере, полностью работоспособны и могут быть использованы для изучения Guardant SP и принципов работы с ним.

В демонстрационном режиме все возможности сервера активации доступны только для просмотра. Любые действия с ключами в этом режиме заблокированы.

2. Подготовка к защите

В данном разделе подробно описываются шаги 1–4 раздела «Быстрый старт» на примере Мастера лицензирования и автоматической защиты.

2.1. Регистрация и установка Guardant SDK

Для начала использования софтверных ключей необходимо подать заявку на регистрацию на сервере активации Guardant SP, который располагается по адресу <https://sp.guardant.ru>.

Обработка заявки занимает до 3 рабочих дней. После прохождения регистрации на адрес электронной почты, указанный в заявке, придет письмо с паролем для входа на сервер и кодами доступа для работы с софтверными ключами.

Файл с кодами доступа подходит для работы как с аппаратными ключами Guardant, так и с софтверными. Его необходимо скопировать в папку установки Guardant SDK, подпапку Bin, заменив существующий файл nvcodes.dat.

Эту процедуру необходимо повторять каждый раз при установке Guardant SDK. Файл nvcodes.dat является уникальным хранилищем ключей шифрования клиента и может быть сгенерирован только в компании «Актив». При утере файла его можно восстановить в личном кабинете на сервере активации.

После завершения регистрации необходимо установить Guardant SDK. Дистрибутив можно скачать с сайта www.guardant.ru. Если Guardant SDK устанавливается только для использования ключей Guardant SP, то можно произвести установку с демонстрационными кодами (они впоследствии будут заменены на файл nvcodes.dat, созданный на сервере).

Обращаем внимание, что Guardant SDK с демонстрационными кодами не поддерживает функцию удаленного обновления аппаратных электронных ключей (TRU).

2.2. Настройка продуктов и серийных номеров

Каждый новый пользователь после завершения регистрации на сервере получает бесплатный комплект Guardant SP. Их можно использовать как для отладки и создания защиты, так и для продажи продукта конечным пользователям. Все ключи идентичны, для работы можно использовать любой.

- На сервере активации серийный номер должен быть однозначно ассоциирован с программным продуктом. Это исключает возможность активации серийного номера с иным программным продуктом.
- Необходимо создать столько продуктов, сколько планируется защищать с помощью Guardant SP. Если продукт всего один, либо же все продукты распространяются по идентичной цене, можно оставить настройки по умолчанию и использовать единственный защищенный продукт с кодом 0.

- Также необходимо назначить нужные серийные номера защищаемому продукту. Для создания защиты и отладки с использованием программного ключа, хотя бы один ключ должен быть активирован на компьютере разработчика. Обратите внимание: для выполнения защиты и отладки триальных версий в 99% случаев достаточно использовать обычный серийный номер нетриального программного ключа. Сетевой программный ключ должен быть сформирован до его первой активации.
- После назначения продукту серийного номера, его нужно передать пользователю. Это будет означать, что выделенные серийные номера ушли в продажу и готовы к активации.

В итоге серийный номер для успешной активации у конечного пользователя должен обладать рядом свойств:

- Соответствовать защищаемому продукту (номер продукта указывается и при защите, и на сервере);
- Находиться в статусе «Готов к активации» или «Активирован» (для перевода в статус «Готов к активации» нужно провести операцию «Передать пользователю»);
- Если ключ «Активирован», счетчик активаций не должен быть исчерпан (исключением является повторная активация на той же конфигурации компьютера, на которой проводилась предыдущая активация; в этом случае счетчик активаций не уменьшается).

ID	Серийный номер	Продукт	Сетевой ресурс	Статус	Кол-во активаций	Текущий лимит	Исходный лимит
8000B279	NNLh88-...-myAIBC	[12] Тестовая триальная программа		Активирован	2	13	100
8000AF33	gjCCaf-...-OvAIBC	[1] Триальная программа		Готов к активации	0	100	100000
8000BBC7	2US#6r-...-e7AIBC	[0] Защищённая программа	50	Готов к передаче	0	1	3
8000BBC6	97gnJA-...-a7AIBC	[0] Защищённая программа		Готов к передаче	0	3	3
8000BBC5	It#ZJ4-...-W7AIBC	[0] Защищённая программа	50	Готов к передаче	0	3	3
8000BBC4	AK2zd6-...-S7AIBC	[0] Защищённая программа	1	Готов к передаче	0	3	3
8000BBC3	9d6MKZ-...-O7AIBC	[10] Test SP	5	Готов к передаче	1	2	3

На приведенном скриншоте первые два серийных номера могут быть успешно активированы, т.к. назначены продукту, имеют нужный статус, и их счетчики активаций не исчерпаны.

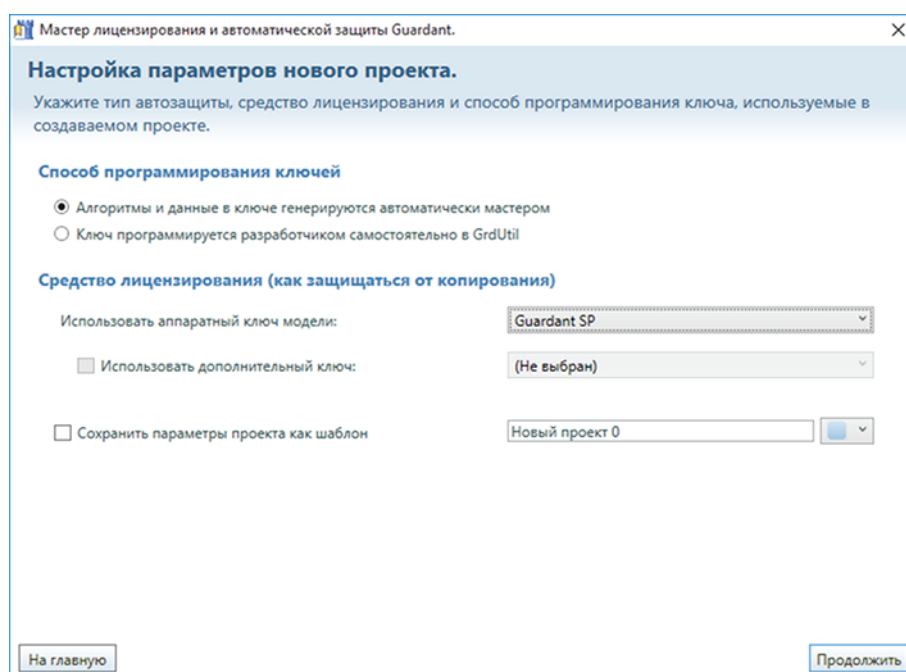
3. Защита при помощи Guardant SP

В процессе защиты программного обеспечения при помощи ключа Guardant SP происходит привязка копии защищенного приложения к Guardant SP. При этом задействуются технологии аналогичные электронным ключам Guardant: автозащита, симметричные алгоритмы шифрования, электронная цифровая подпись, Guardant API.

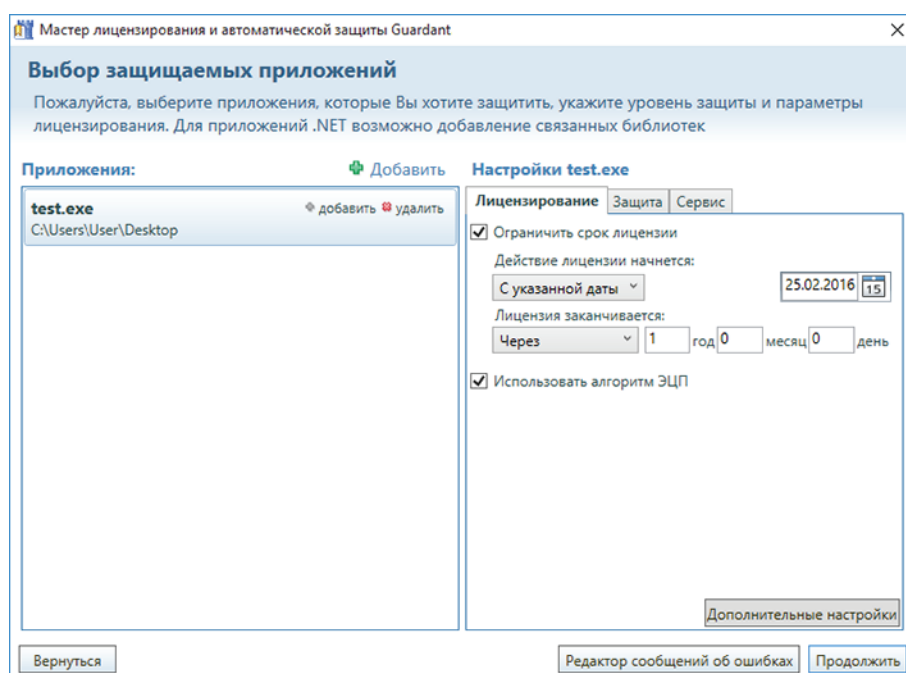
3.1. Автоматическая защита

Самый доступный вариант создания защиты при помощи программных ключей Guardant SP заключается в использовании Мастера лицензирования и автоматической защиты (входит в состав Guardant SDK).

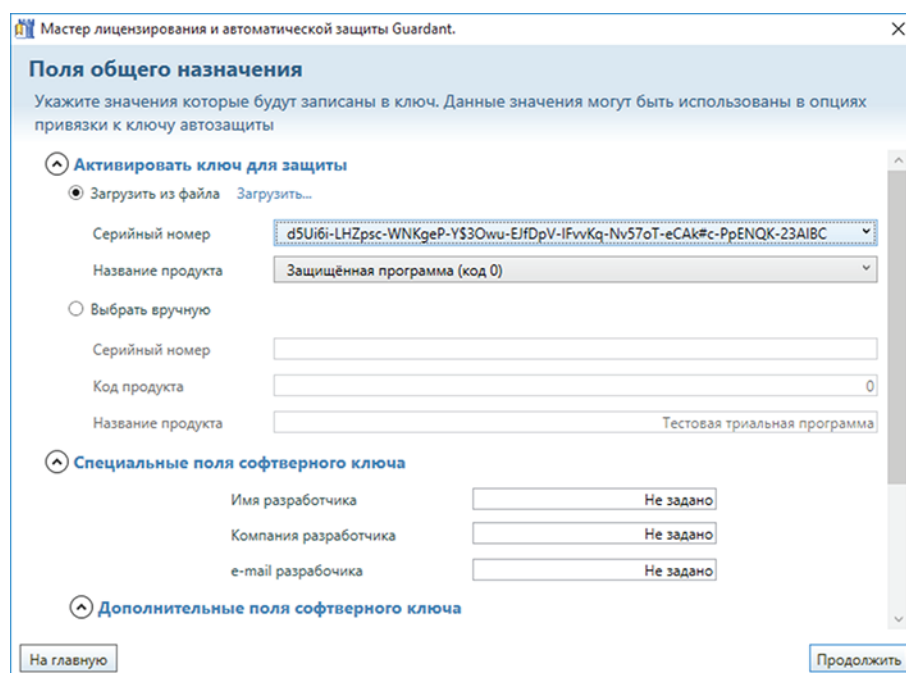
При запуске Мастера необходимо создать новый проект защиты и выбрать режим программирования ключа.



При необходимости создания временной лицензии нужно установить дату начала и продолжительность срока лицензирования.



Далее необходимо указать используемый для защиты серийный номер и прочие параметры. Код и название должны соответствовать продукту, ассоциированному с серийным номером на сервере активации. Для удобства можно использовать выгружаемый с сервера активации файл с расширением .gsr. Его использование упрощает выбор продукта и соответствующего ему серийного номера. При несоответствии защищаемого продукта активация завершится с ошибкой.



Следует обратить внимание, что для защиты подходит любой серийный номер, соответствующий защищаемому продукту и имеющий статус «Готов к активации» или «Активирован» с ненулевым счетчиком активаций.

Использованный серийный номер будет активирован на компьютере разработчика и более не сможет быть использован на другом компьютере. Именно этот серийный номер следует использовать для защиты и отладки новых версий. Однако если ключ Guardant SP рассчитан на несколько активаций, он может быть активирован на другом компьютере или конфигурации. В этом случае он потеряет возможность переактивации для изначальной конфигурации компьютера.

Подробнее об управлении серийными номерами можно прочитать в руководстве по серверу активации на портале документации по адресу developer.guardant.ru.

После выполнения описанных шагов защита проводится, как при использовании аппаратного ключа Guardant. На этапе вызова автозащиты Мастер самостоятельно активирует продукт на сервере активации, после чего ключ может быть обнаружен утилитой диагностики и доступен для использования.

Автозащита шифрует и подписывает массивы данных на алгоритмах ключа и использует получившийся результат для привязки программы к копии ключа – в процессе работы будет проводиться расшифровывание и проверка подписи данных.

В результате применения автозащиты формируется файл шаблона программного ключа (с расширением .grdvd), который необходимо распространять вместе с защищенным приложением, вакциной автозащиты и серийным номером для активации.

Этот шаблон зашифрован и подписан ключами разработчика и может быть превращен в рабочий программный ключ только на сервере активации, где шаблон будет перешифрован. Причем в качестве компонентов ключей шифрования будут использованы комплектующие конкретного компьютера конечного пользователя.

3.3. Защита с использованием Guardant API

Ключ Guardant SP полностью поддерживается Guardant API. Он обнаруживается функцией GrdFind при указании соответствующих кодов доступа и функционирует аналогично аппаратным ключам.

На портале документации по адресу developer.guardant.ru содержится подробная информация о функциях Guardant API и порядке работы с ними.

3.4. Использование ключей в Linux

Для софтверных ключей Guardant SP в Linux используются те же шаблоны, что и в Windows. Однако, т.к. в Linux отсутствует автоматическая защита, разработчику защищенного приложения доступен только Guardant API. При этом шаблон ключа нужно самостоятельно создать в GrdUtil.

Фоновая программа, утилита активации и API для ключей входят в состав установленного Guardant SDK (папка \Redistribute\Linux).

Порядок использования утилиты активации для Linux:

1. Утилита curl (или libcurl) с поддержкой OpenSSL, устанавливаемая с помощью автоматических систем обновления (например, Центр приложений Ubuntu / Ubuntu Software Center). Утилиту для нужной OS также можно вручную скачать с сайта <http://curl.haxx.se/download.html>, распаковать и прописать в путях поиска.
2. Демон grddaemon, предназначенный для активации контейнера и работы с софтверным ключом. Должен запускаться только с правами root.

Пример ручного запуска из текущей папки:

```
sudo ./grddaemon (имеет ключи stop, restart для остановки и перезапуска).
```

Для запуска также прилагаются скрипты.

3. Утилита активации GrdSPActivate, предназначенная для активации контейнера, генерируемого с помощью утилиты GrdUtil.

Входные параметры:

- Путь к контейнеру GrdVD_Template.grdvd;
- Путь к файлу с серийным номером, опция /serialfile=»/home/user1/Aktiv/Serial.txt».

Результат:

Активированный контейнер скопирован в папку «/var/guardant/Containers».

Примечание:

Удаление контейнера из папки «/var/guardant/Containers» равнозначно удалению софтверного ключа из системы.

Пример запуска:

```
./GrdSPActivate «/home/user1/Aktiv/GrdVD_Template.grdvd» /serialfile=»/home/user1/Aktiv/Serial.txt»
```

4. Утилита GrdSPActivate, предназначенная для активации контейнера, генерируемого с помощью утилиты GrdUtil.
5. После выполнения указанных операций в системе появляется активированный софтверный ключ с полноценной поддержкой Guardant API.

4. Лицензирование по времени работы

Все ключи Guardant SP позволяют осуществлять лицензирование по времени работы, что необходимо при сдаче ПО в аренду, продаже в рассрочку или выполнении других бизнес-сценариев.

4.1. Принцип работы

Ключ может содержать в себе несколько криптографических алгоритмов (шифрование AES128, подпись ECC160). При этом каждый из алгоритмов поддерживает установку на него временных ограничений, которые могут быть направлены как на включение алгоритма в определенный момент времени, так и на отключение его через определенный промежуток времени.

Каждый ключ отслеживает значение своих часов уникальным образом. Ключевой датой является **дата первой активации ключа** – именно при первой активации происходит создание виртуальных часов на компьютере, сравнение с временем на сервере и подготовка защитных механизмов для предотвращения манипуляций со временем.

В процессе работы ключ сверяет значения системного времени с его собственным, пристально следя за тем, чтобы пользователь не смог обмануть ограничения работы программы. При этом несколько часов разницы во времени не повлияют на работу ключа – он спроектирован таким образом, чтобы учитывать возможные переводы времени при путешествиях, часовые пояса, летнее/зимнее время и прочие подобные ситуации.

Предположим, в ключе есть алгоритм, ограниченный по времени работы. Если пользователь в любой момент времени переведет системные часы на несколько (<24) часов назад, то ключ не «заметит» этого. Однако если суммарное отклонение времени составит больше 24 часов, то таймер ключа инвалидируется и его восстановление станет невозможным.

Таким образом если пользователь пытается обмануть механизм ограничения времени в ключе переводом стрелок часов назад, time-функционал в ключе ломается и не подлежит восстановлению. При этом ключ можно перепрошить (или выслать другой шаблон) для использования без ограничений по времени работы.

4.2. Установка ограничений по времени работы

Важно понимать, что ограничение по времени работы устанавливается для конкретного алгоритма ключа. Именно к алгоритму ключа привязывается автоматическая защита Guardant, и им же пользуются функции Guardant API.

В арсенале Guardant присутствуют две программы, обладающие возможностью создания шаблона и программирования маски в ключе.

GrdUtil

Утилита редактирования ключей представляет из себя продвинутое средство работы с Guardant SP. Разработчик системы защиты самостоятельно может создать шаблон программного ключа, спроектировав его структуру данных и уникальный набор криптографических алгоритмов.

Для каждого алгоритма можно задать ограничения по времени работы. Для этого нужно дважды щелкнуть по алгоритму в редакторе образа главного окна GrdUtil и произвести настройки в отобразившемся окне.

Мастер лицензирования и автоматической защиты Guardant.

Настройка параметров нового проекта.
Укажите тип автозащиты, средство лицензирования и способ программирования ключа, используемые в создаваемом проекте.

Способ программирования ключей

- ☒ Алгоритмы и данные в ключе генерируются автоматически мастером
- ☐ Ключ программируется разработчиком самостоятельно в GrdUtil

Средство лицензирования (как защищаться от копирования)

Использовать аппаратный ключ модели: Guardant SP

☐ Использовать дополнительный ключ: (Не выбран)

☐ Сохранить параметры проекта как шаблон: Новый проект 0

На главную Продолжить

Мастер лицензирования и автоматической защиты

В Мастере на этапе выбора защищаемых приложений можно для каждого указать ограничения по времени.

Мастер лицензирования и автоматической защиты Guardant.

Выбор защищаемых приложений
Пожалуйста, выберите приложения, которые Вы хотите защитить, укажите уровень защиты и параметры лицензирования. Для приложений .NET возможно добавление связанных библиотек

Приложения: Добавить

test.exe добавить удалить
C:\Users\User\Desktop

Настройки test.exe

Лицензирование Защита Сервис

☒ Ограничить срок лицензии

Действие лицензии начнется:
С указанной даты 25.02.2016 15

Лицензия заканчивается:
Через 1 год 0 месяц 0 день

☒ Использовать алгоритм ЭЦП

Дополнительные настройки

Вернуться Редактор сообщений об ошибках Продолжить

4.3. Механизмы ограничения времени

В ключах Guardant SP механизмы ограничения времени аналогичны ключам Guardant Time.

Существует три режима работы:

- **По времени активации алгоритма**

Можно указать точную дату и время активации алгоритма, указав при этом продолжительность его работы. Например, алгоритм ключа активируется в полночь 31 января 2026 года и проработает 12 месяцев.

- **По времени деактивации алгоритма**

Можно поставлять ключ с уже активированным алгоритмом, но с указанной датой автоматической деактивации. Например, можно поставлять софтверный ключ, в котором указанный алгоритм отключится 31 декабря 2026 года.

- **По времени жизни алгоритма**

Можно указать только продолжительность времени работы ключа. Например, программа продается на 1 год. В таком случае время жизни алгоритма будет отсчитываться от даты первой активации ключа.

4.4. Особенности использования

У ключей Guardant SP существует ряд особенностей, которые необходимо учитывать:

- Функциональность Time доступна только с драйвером Guardant 6.2 и выше;
- Ключи, созданные с помощью Guardant SDK, будут работоспособны только с драйвером такой же версии, что и SDK, или выше;
- При наличии нескольких алгоритмов в ключе с заданным для каждого из них временем жизни алгоритма нужно учитывать, что отсчет времени жизни происходит от **даты первой активации ключа для всех алгоритмов**;
- Если производилась попытка мошенничества со временем на компьютере, ключ полностью утрачивает работоспособность time-функционала. Все алгоритмы, ограниченные по времени, становятся неработоспособны, и восстановление ключа невозможно. Однако его можно использовать без time-функционала.

5. Лицензирование по сети

Для клиентов, ценящих удобство сетевого лицензирования, существует уникальный механизм формирования сетевых ключей Guardant SP Net. Ключ на нужное количество лицензий создается разработчиком прямо на сервере из свободных локальных ключей Guardant SP. Возможно даже сформировать сетевой софтверный ключ с максимальным сетевым ресурсом лишь в одну лицензию.

Удобство сетевых ключей Guardant SP Net заключается в том, что активация и привязка ключа к компьютеру необходима только на одной рабочей станции. На ней будет запущен сервер сетевых ключей и создан ключ Guardant SP Net. Защищенное программное обеспечение может быть запущено с любого компьютера сети при условии наличия свободных лицензий. При этом установка драйверов Guardant и права администратора не требуются.

5.1. Принцип работы

Сетевой софтверный ключ может нести в себе 1 и более лицензий и предназначен для использования на выделенном компьютере. С помощью специальной программы (сервера сетевых ключей) происходит раздача лицензий по сети.

Сервер сетевых ключей поддерживает как аппаратные, так и программные ключи.

Подробная документация по работе сервера сетевых ключей расположена на портале документации по адресу developer.guardant.ru.

5.2. Создание и подготовка ключа

Сетевые ключи создаются непосредственно на сервере активации по адресу <https://sp.guardant.ru>. Для создания ключа необходим 1 или более серийных номера со статусом «Готов к передаче», назначенных одному и тому же продукту. Если номер уже передан пользователю и находится в статусе «Готов к активации», предполагается, что он будет использован в качестве локального.

Для создания сетевого ключа необходимо нажать на любой серийный номер в статусе «Готов к передаче» и в появившемся окне указать нужное количество лицензий.

Просмотр записи #800010A2

Закрыть окно

Параметр	Значение
ID	800010A2
Серийный номер	vn4ye9-sg(TxA-3uQUhA-pvlqPw-fiV+Zi-Sr7r9Q-tvnK+E-4j_Fad-Yi1+l6-IQAIBC
Статус	Готов к передаче
Дата приобретения	10.12.2012
Номер заказа	139
Лимит активаций	5
Исходный лимит активаций	5
Выполнено активаций	0
Продукт	[5] Продукт №5
Создать сетевой ключ	Количество лицензий Создание сетевого ключа

После создания сетевого ключа он становится доступен на вкладке «Сетевые ключи». Его можно расформировать и использовать, как локальные Guardant SP, до момента первой активации. После активации он останется сетевым ключом навсегда.

Просмотр номеров	Назначение продукту	Передача пользователю	Сетевые ключи	Ограничение активаций	Блокировка	Разблокировка	Возврат/отмена	История	
Расформировать								Выбрано: 0 из 1	
☐	ID	Серийный номер	Продукт	Сетевой ресурс	Статус	Кол-во активаций	Текущий лимит	Исходный лимит	Комментарий
☐	800010A2	vn4ye9-...-lQAIBC	[5] Продукт №5	2	Готов к передаче	0	5	5	-

5.3. Активация и использование ключа

Сетевой ключ активируется таким же образом, как и локальный. Необходимо учитывать, что активировать сетевой ключ нужно только один раз на том компьютере, где будет расположен сервер сетевых ключей.

Для автоматической защиты с ключом Guardant SP Net необходимо использовать Мастер лицензирования (входит в состав Guardant SDK) или Guardant API.

В командной строке новый тип ключа обозначается как /GSPN. Остальные параметры аналогичны использованию аппаратных сетевых ключей и подробно описаны в документации.

6. Распространение защищенного ПО

После осуществления защиты приложения и его привязки к софтверному ключу Guardant SP можно распространять приложение среди конечных пользователей.

6.1. Комплект поставки защищенного приложения

Для работы приложения, защищенного софтверным ключом, пользователю необходимо:

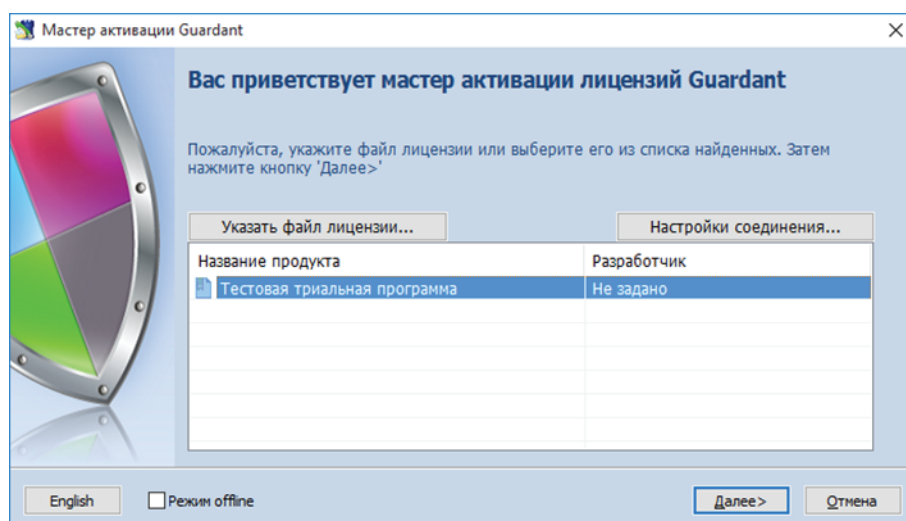
- Установить Драйвер Guardant;
- Получить комплект ПО, содержащий:
 - Защищенную программу;
 - Если использовалась автоматическая защита – вакцину (GrdVkc32.dll);
 - Шаблон софтверного ключа (файл с расширением .grdvd);
 - Мастер активации (GuardantActivationWizard.exe);
- Получить уникальный серийный номер.

6.2. Активация Guardant SP у конечного пользователя

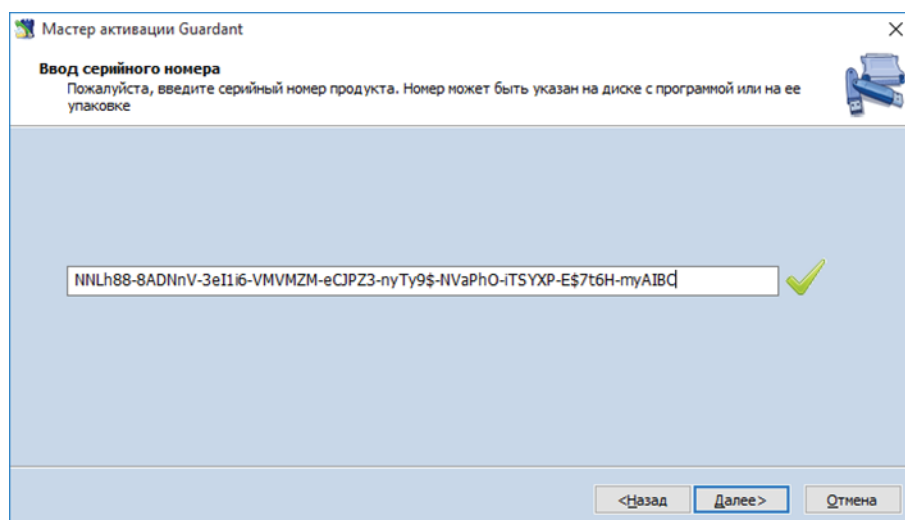
Активация ключей возможна только через интернет и требует от пользователя наличия корректного серийного номера и шаблона программного ключа.



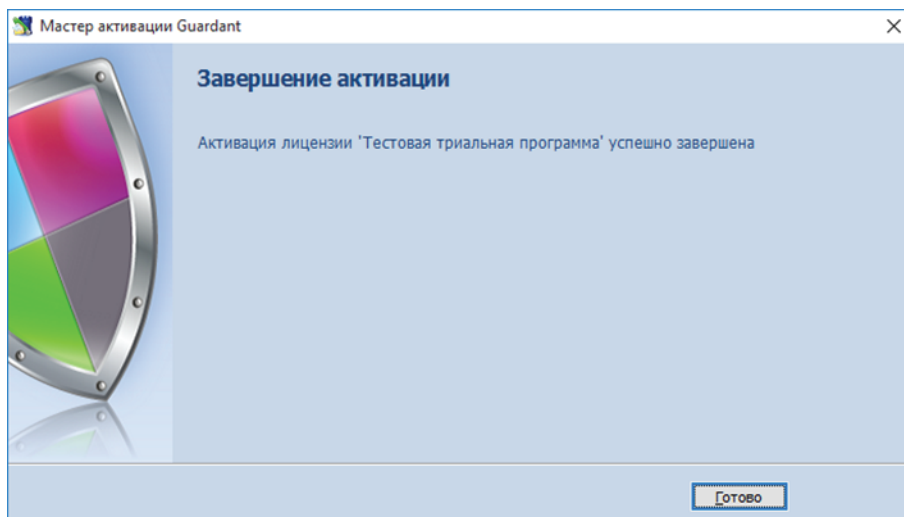
Если в списке Мастера активации отсутствует защищенный продукт, необходимо указать путь к файлу с расширением .grdvd, нажав на кнопку «Указать файл лицензии».



Далее необходимо ввести серийный номер.



После нажатия на кнопку «Далее» Мастер сообщит об успешной активации.



После завершения активации ключ Guardant SP полностью готов к работе. Клиент может использовать его повторно, если оборудование компьютера не изменилось.

Стоит отметить, что Guardant API предоставляет набор функций, позволяющих реализовать собственную утилиту активации и/или интерфейс активации программного ключа прямо в защищенном приложении.