

**R301 ФОРОС USB, смарт-карта ФОРОС для
Windows
Руководство администратора**

Оглавление

1	Общее описание	3
2	Установка драйвера для Форос Windows	4
2.1	Автоматическая установка драйвера	4
2.2	Ручная установка драйвера	4
3	Совместимость с КриптоПро CSP	6
4	Режимы доступа к Форос Windows	7
4.1	Режим администратора	7
4.2	Режим пользователя	7
4.3	Режим гостя	8
5	Использование центра сертификации	8
6	Утилита администрирования Форос Windows	11
6.1	Общее описание утилиты	11
6.2	Начало работы с утилитой	11
6.3	Управление ПИНом пользователя	11
6.4	Управление паролем администратора	12

1 Общее описание

Носитель R301 ФОРОС USB/смарт-карта ФОРОС для Windows (далее - Форос-Windows) предназначен для применения в качестве персонального электронного идентификатора в ОС Windows (7, 8.1, 10) в рамках информационной технологии компании Microsoft.

Аутентификация при помощи Форос-Windows позволяет кардинально повысить безопасность системы, снижает риск несанкционированного доступа. Использование Форос-Windows позволяет внедрить двухфакторную аутентификацию в следующие сценарии использования:

- аутентификация при входе в ОС Windows (winlogon);
- аутентификация в VPN-соединениях;
- аутентификация при доступе к удаленному рабочему столу по протоколу RDP;
- аутентификация при доступе к интернет ресурсам.

Также Форос-Windows можно использовать для:

- защиты электронной почты в Microsoft Outlook;
- подписи документов Microsoft Office;
- подписи pdf документов;
- шифрования отдельных файлов и целиком разделов жестких дисков (EFS, BitLocker).

Подробно каждое применение Форос-Windows описано в «Руководстве пользователя Форос-Windows».

Для внедрения и управления электронными ключами Форос требуется квалифицированный системный администратор, обладающий навыками администрирования Windows Server (2008, 2012, 2016) и рабочих станции Windows (7, 8.1, 10).

Для применения Форос-Windows требуется, чтобы компьютер, на котором применяется Форос-Windows, был членом домена. Перед применением Форос-Windows необходимо персонализировать – записать на него ключевую пару и сертификат пользователя. Это можно сделать на сервере с установленной ролью центра сертификации.

Соответственно в сетевой инфраструктуре использования Форос-Windows должны присутствовать сервер являющийся контроллером домена, сервер являющийся центром сертификации, конечные персональные компьютеры пользователей.

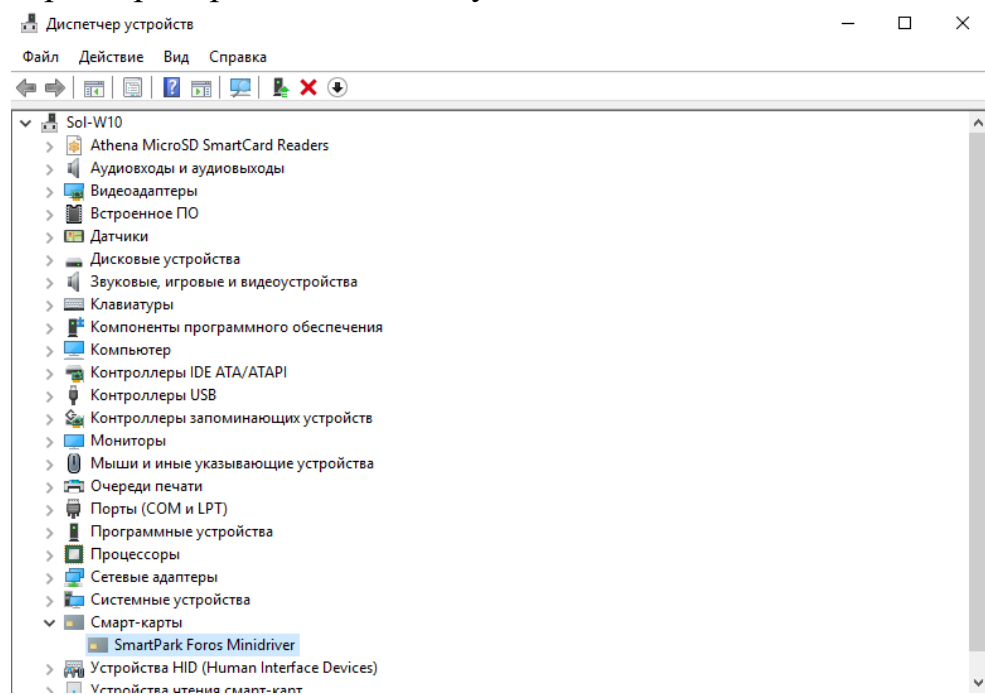
Установка службы сертификатов и ActiveDirectory в данном документе не рассматривается.

2 Установка драйвера для Форос Windows

2.1 Автоматическая установка драйвера

В большинстве операционных систем Windows драйвер Форос Windows устанавливается автоматически из Windows Update при подключении Форос Windows к компьютеру.

Проверить установился ли драйвер на вашем компьютере можно подключив Форос Windows к нему и посмотрев в "Диспетчер устройств". В разделе Смарт-карты в деспетчере устройств должно отображаться имя «SmartPark Foros Minidriver». Если же там отображается имя «Неизвестная карта», то драйвер Форос Windows не установлен.



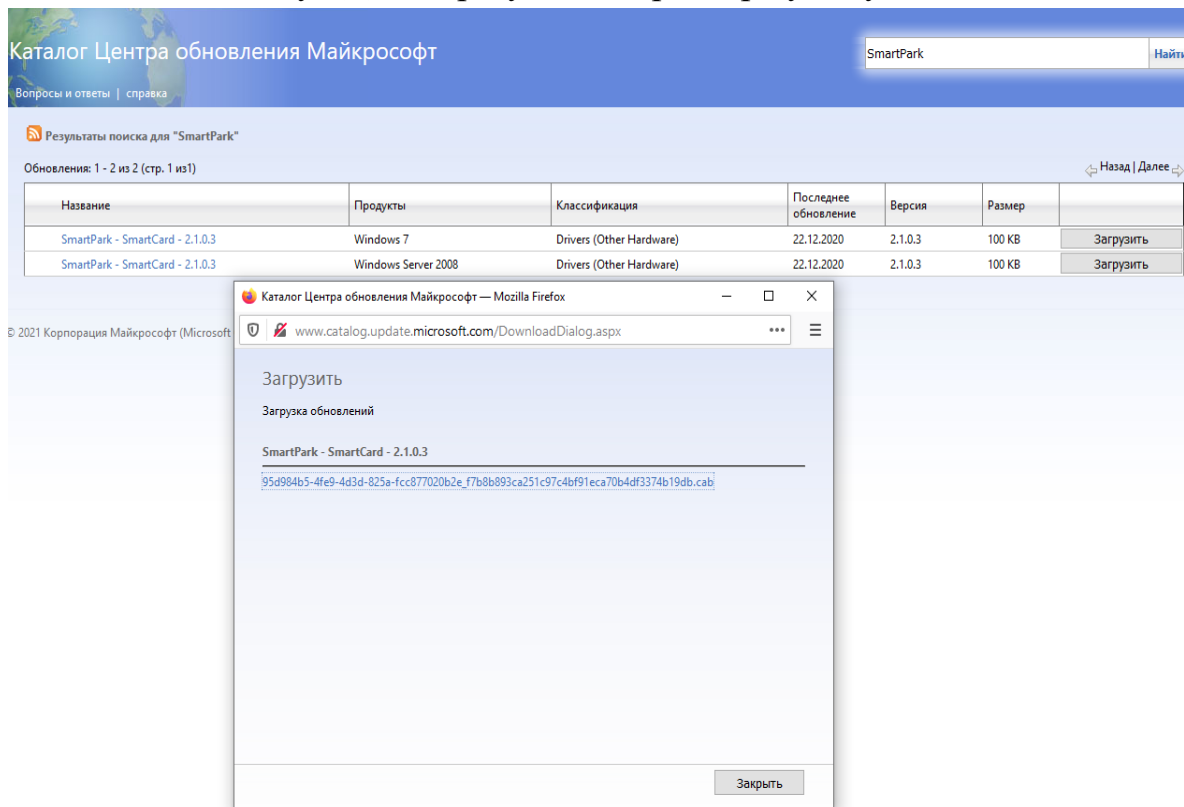
2.2 Ручная установка драйвера

Есть несколько вариантов установить драйвер Форос Windows вручную:
Установка с помощью пакета msi с сайта СмартПарк

1. Пройдите по ссылке:
2. <http://smart-park.ru/index.php/support/driver.html>
3. Найдите установщик (msi файл), соответствующий архитектуре вашего компьютера.
4. Загрузите соответствующий установщик
5. Запустите загруженный установщик
6. Следуя подсказкам установщика, пройдите процедуру установки драйвера
7. В результате драйвер будет добавлен в хранилище Windows.
8. Подключите Форос Windows к компьютеру. Автоматический установщик ОС Windows завершит процедуру установки.

Установка из inf файла с сайта Microsoft Update

1. Пройдите по ссылке:
2. <http://www.catalog.update.microsoft.com/Search.aspx?q=SmartPark>
3. Найдите соответствующую вашей версии ОС строку.
4. В этой строке нажмите на кнопку «Загрузить»
5. Появится окно со ссылкой на архив для загрузки.
6. Сохраните этот архив на компьютере.
7. Распакуйте этот архив.
8. Щелкните правой кнопкой мыши по названию файла sminidriver.inf и выберите пункт «Установить».
9. В открывшемся окне для подтверждения внесения изменений нажмите на кнопку «Да». В результате драйвер будет установлен.



Установка с помощью диспетчера устройств

1. Выполните пункты 1-6 из предыдущей инструкции
2. Подключите Форос Windows к компьютеру
3. Откройте диспетчер устройств
4. Найдите в диспетчере устройств вкладку «Смарт-карты»
5. Во вкладке «Смарт-карты» найдите устройство «Неизвестная смарт-карта»
6. Щелкните правой кнопкой мыши по данному устройству и выберите пункт «Обновить драйвер»

7. В открывшемся меню выберите «Выполнить поиск драйверов на этом компьютере»
8. Укажите директорию, в которую вы распаковали скачанный архив
9. Нажмите «Далее»
10. В результате драйвер будет установлен

3 Совместимость с КриптоПро CSP

Носитель Форос Windows поставляется в формате:

- специализированного носителя R301 ФОРОС USB ♦ Смарт карта ФОРОС для Windows (далее ФОРОС для Windows);
- функционального приложения носителя R301 ФОРОС USB ♦ Смарт карта ФОРОС для ЭП с расширенной функциональностью (далее ФОРОС для ЭП с расширенной функциональностью).

Носители «ФОРОС для ЭП с расширенной функциональностью», без ограничений можно применять как носитель ключа и сертификата для криптопровайдеров КриптоПро CSP и VipNet CSP, а также Может применяться в качестве персонального электронного идентификатора пользователей ОС Windows (7, 8.1, 10) в рамках информационной технологии компании Microsoft.

Носитель ФОРОС для Windows может применяться только в качестве персонального электронного идентификатора пользователей ОС Windows (7, 8.1, 10) в рамках информационной технологии компании Microsoft. При этом доступная Пользователю область энергонезависимой памяти носителя существенно больше.

Если носитель ФОРОС для ЭП с расширенной функциональностью планируется применять также и как носитель ФОРОС-Windows, то необходимо учитывать возможность возникновения конфликта с КриптоПро CSP так как КриптоПро CSP в таком случае будет пытаться использовать Форос Windows для входа в учетную запись Windows через собственный криптопровайдер.

Чтобы избежать данной ситуации, возможны следующие решения:

1. Сначала на компьютер установить Форос Windows (см. п. 2 данного документа), а затем КриптоПро CSP. В таком случае конфликтов не должно возникнуть.
2. В панели управления КриптоПро CSP открыть вкладку Winlogon и нажать «Удалить регистрации носителей». В этом случае все носители КриптоПро будут удалены из списка возможных для входа в учетную запись Windows.
3. Устанавливать КриптоПро CSP с ключом NOTRUSTWL=1
4. Открыть редактор реестра (команда regedit.exe). Открыть путь
«\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\C

alais\SmartCards\»

и там удалить запись «CP_Trust_Default».

В случае ОС x64 аналогично сделать в пути

«\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Calais\SmartCards»

4 Режимы доступа к Форос Windows

В Форос Windows существуют 3 режима доступа:

1. режим администратора
2. режим пользователя
3. режим гостя

4.1 Режим администратора

Режим администратора позволяет разблокировать ПИН пользователя и сменить ПИН пользователя.

Для входа в режим администратора необходимо предъявить пароль администратора.

Пароль администратора имеет длину 16 символов и может содержать любые печатные символы.

Пароль администратора имеет 3 попытки ввода, то есть если ввести 3 раза подряд неверный пароль, то он заблокируется. При этом функции Форос Windows выполняться будут, но не будет возможности разблокировать ПИН пользователя. Если после нескольких попыток неверного ввода пароля администратора (меньше 3) ввести верный пароль, то счётчик возможных неверных вводов вновь установится в максимальное значение, то есть будет равен 3.

Пароль администратора по умолчанию ‘2222222222222222’, то есть шестнадцать двоек.

По сути, пароль администратора – это ключ алгоритма TDES. Для предъявления данного ключа необходимо выполнить аутентификацию, то есть получить случайное число с Форос Windows и зашифровать его.

Для выполнения функций администратора можно использовать утилиту UnblockForosWindows, описанную далее.

4.2 Режим пользователя

Режим пользователя позволяет выполнить все целевые функции Форос Windows. Также режим пользователя позволяет сменить ПИН пользователя.

Для входа в режим пользователя надо предъявить ПИН пользователя.

ПИН пользователя имеет длину от 4 до 8 символов и может содержать

любые печатные символы.

ПИН пользователя имеет 5 попыток ввода, то есть если ввести 5 раз подряд неверный ПИН, то он заблокируется, и функции Форос Windows выполняться не будут. Если после нескольких попыток неверного ввода ПИНа (меньше 5) ввести верный ПИН, то счётчик возможных неверных вводов вновь установится в максимальное значение, то есть будет равен 5.

ПИН пользователя по умолчанию '1111111', то есть восемь единиц.

4.3 Режим гостя

Режим гостя – это режим по умолчанию после подключения Форос Windows, то есть без предъявления каких-либо паролей. В режиме гостя доступен для чтения сертификат пользователя. Другие функции Форос Windows в режиме гостя не доступны.

5 Использование центра сертификации

Центр сертификации позволяет выпустить и записать сертификат и ключевую пару на Форос Windows.

Настройка центра сертификации состоит из следующих пунктов:

1. установка роли центр сертификации Active Directory (Active Directory Certificate Services);
2. настройка шаблонов выдачи сертификатов;
3. выпуск сертификатов на электронные ключи Форос Windows;

В этом разделе подразумевается, что у администратора есть компьютер под управлением ОС Windows Server. На данный компьютер предварительно был установлен центр сертификации.

Также данный компьютер является членом домена, соответственно настроен контроллер домена.

Установка Windows Server, установка и настройка контроллера домена и установка центра сертификации в данном документе не рассматриваются.

Для выпуска сертификатов на Форос Windows необходимо создать соответствующий шаблон выдачи сертификатов.

1. Выполните в командной строке команду mmc.
2. Нажмите Файл->Добавить оснастку, там выберите «Центр Сертификации». Нажмите «Добавить» и «ОК». В следующем окне выберите «Локальным компьютером» и нажмите «Готово». Откроется консоль «Центр Сертификации».
3. В консоли «Центр Сертификации» щелкните правой кнопкой мыши по «Шаблоны сертификатов» и выберите «Управление».
4. Появится список шаблонов. Щелкните правой кнопкой мыши по

«Пользователь со смарт-картой» и выберите «Скопировать шаблон».

5. Откроется окно со свойствами нового шаблона. Откройте вкладку «Общее». Здесь надо указать имя шаблона. Для примера «ForosWindows».

6. Откройте вкладку «Требования выдачи». Укажите политику применения - «Агент запроса сертификата».

7. Откройте вкладку «Имя субъекта». Выберите «Строится на основе данных Active Directory». Формат имени субъекта отметьте «Полное различающееся имя». Чтобы Форос Windows работал для защиты электронной почты надо также отметить «Имя электронной почты». При этом адрес электронной почты должен быть прописан в данных Active Directory.

8. Если Форос Windows планируется использовать в технологии шифрования дисков BitLocker, то необходимо перейти во вкладку «Расширения», выбрать «Политики применения» и нажать «Изменить». В открывшемся окне нажмите «Добавить». Выберите «Шифрование диска BitLocker» и нажмите «ОК». (До этого также необходимо на сервере добавить компоненту «Шифрование диска BitLocker». Данное действие выходит за рамки данного руководства.)

9. Нажмите «Применить» в окне свойств шаблона.

10. Откройте окно консоли «Центр Сертификации». Щёлкните правой кнопкой по «Шаблоны сертификатов» и выберите Создать->Выдаваемый шаблон сертификата.

11. В появившемся окне выберите шаблон «ForosWindows» и «Агент регистрации». Нажмите «ОК». Выбранные шаблоны должны появиться в разделе «Шаблоны сертификатов» в консоли «Центр Сертификации».

После создания шаблонов можно выпускать сертификаты и записывать их в Форос Windows.

Для начала надо выпустить сертификат агента регистрации.

1. Выполните в командной строке команду mmc.

2. Нажмите Файл->Добавить оснастку, там выберите «Сертификаты». Нажмите «Добавить» и «ОК». В следующем окне выберите «моей учетной записи пользователя» и нажмите «Готово». Откроется консоль «Сертификаты».

3. В консоли «Сертификаты» щёлкните правой кнопкой по «Личное» и выберите «Все задачи->Запросить новый сертификат». В появившемся окне нажмите «Далее».

4. В следующем окне выберите «Агент регистрации» и нажмите «Заявка». В появившемся окне нажмите «Далее» и затем «Готово».

Теперь можно приступать к выпуску сертификатов пользователей Форос Windows.

1. Выполните в командной строке команду mmc.

2. Нажмите Файл->Добавить оснастку, там выберите «Сертификаты». Нажмите «Добавить» и «ОК». В следующем окне выберите «моей учетной записи пользователя» и нажмите «Готово». Откроется консоль «Сертификаты».
3. В консоли «Сертификаты» щёлкните правой кнопкой по «Личное» и выберите «Все задачи->Дополнительные операции->Зарегистрироваться от имени». В появившемся окне нажмите «Далее». И еще раз «Далее».
4. В следующем окне предложат выбрать сертификат подписи. Нажмите «Обзор». Выберите сертификат Агента регистрации и нажмите «ОК».
5. Выберите шаблон, который ранее создали для пользователей Форос Windows (в примере это шаблон ForosWindows). Нажмите «Далее».
6. В следующем окне предложат выбрать пользователя, для которого выпускается сертификат. Нажмите «Обзор». Выберите пользователя и нажмите «ОК». Затем нажмите «Заявка».
7. Далее система запросит вставить электронный ключ Форос Windows и ввести ПИН-код. Введите ПИН-код пользователя и нажмите «ОК».
8. Если всё прошло без ошибок, то отобразится состояние «Успешно» и далее можно завершить этот процесс или нажать «Следующий пользователь» для выдачи следующего сертификата.

Для каждого пользователя администратор опционально можно настроить автоматическую блокировку компьютера при отсоединении электронного ключа, а также совсем отключить стандартную парольную аутентификацию. Также данные настройки можно сделать в групповых политиках и применить ко всем пользователям сразу.

6 Утилита администрирования Форос Windows

6.1 Общее описание утилиты

Для управления паролями Форос Windows существует утилита UnblockForosWindows. Данная утилита позволяет изменить ПИН пользователя, изменить пароль администратора, разблокировать ПИН пользователя.

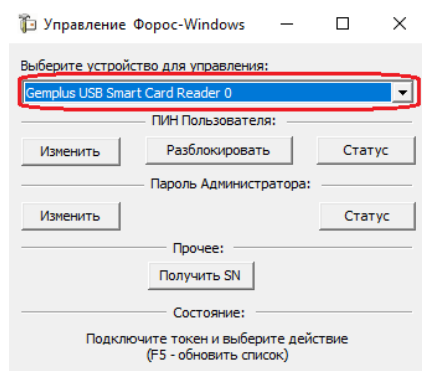
Утилита UnblockForosWindows предназначена для работы в ОС Windows.

Скачать утилиту UnblockForosWindows можно по ссылке:

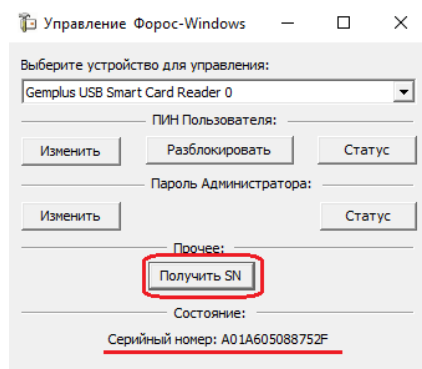
<http://smart-park.ru/index.php/support/driver.html>

6.2 Начало работы с утилитой

Сразу после запуска утилиты необходимо выбрать смарт-карт считыватель, в который вставлена смарт-карта Форос Windows.



Чтобы убедиться, что устройство функционирует корректно можно нажать на кнопку «Получить SN». При нажатии на данную кнопку считывается серийный номер микроконтроллера устройства. Данный номер выводится в поле «Состояние» ниже.



В случае возникновения ошибки, сообщение об этом также будет выведено в поле «Состояние».

6.3 Управление ПИНом пользователя

ПИН пользователя даёт доступ к функциям Форос Windows. ПИН

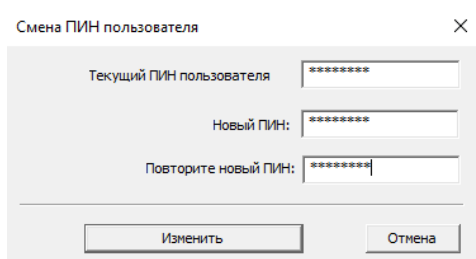
пользователя имеет длину от 4 до 8 символов и может содержать любые печатные символы.

ПИН пользователя имеет 5 попыток ввода, то есть если ввести 5 раз подряд неверный ПИН, то он заблокируется, и функции Форос Windows выполняться не будут. Если после нескольких попыток неверного ввода ПИНа (меньше 5) ввести верный ПИН, то счётчик возможных неверных вводов вновь установится в максимальное значение, то есть будет равен 5.

ПИН пользователя по умолчанию '1111111', то есть восемь единиц.

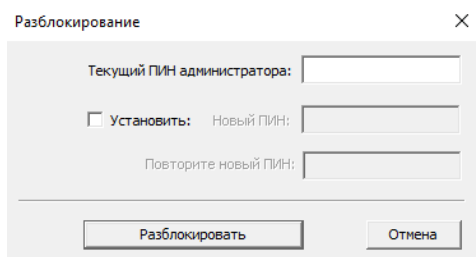
Для управления ПИНОм пользователя существует 3 кнопки.

1. Кнопка «Изменить». Позволяет изменить ПИН пользователя. Для этого необходимо ввести текущий ПИН пользователя и новый ПИН пользователя.



2. Кнопка «Разблокировать». Позволяет разблокировать ПИН пользователя. Для данного действия необходимо ввести пароль администратора.

По умолчанию происходит только разблокировка ПИНа пользователя, то есть значение ПИНа пользователя не изменяется. Но если поставить галочку в поле «Установить», то появится возможность ввести новое значение ПИНа пользователя, которое будет установлено одновременно с разблокированием.



3. Кнопка «Статус». Позволяет узнать оставшееся количество попыток ввода ПИНа. Данное значение выводится в поле «Состояние».

6.4 Управление паролем администратора

Пароль администратора позволяет разблокировать и менять ПИН пользователя Форос Windows. Пароль администратора имеет длину 16 символов и может содержать любые печатные символы.

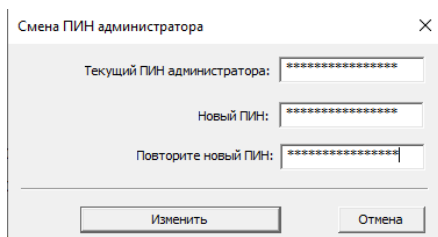
Пароль администратора имеет 3 попытки ввода, то есть если ввести 3 раза подряд неверный пароль, то он заблокируется. При этом функции Форос Windows выполняться будут, но не будет возможности разблокировать ПИН пользователя. Если после нескольких попыток неверного ввода пароля администратора (меньше 3) ввести верный пароль, то счётчик возможных неверных вводов вновь установится в максимальное значение, то есть будет равен 3.

Пароль администратора по умолчанию '2222222222222222', то есть шестнадцать двоек.

По требованиям безопасности перед началом использования Форос Windows необходимо обязательно сменить пароль администратора.

Для управления паролем администратора существует 2 кнопки.

1. Кнопка «Изменить». Позволяет изменить пароль администратора. Для этого необходимо ввести текущий пароль администратора и новый пароль администратора.



2. Кнопка «Статус». Позволяет узнать оставшееся количество попыток ввода пароля администратора. Данное значение выводится в поле «Состояние».