УТВЕРЖДЕНО
М. Чайкин
Генеральный директор

Вступает в силу
с 01.03.2026

ТЕХНИЧЕСКИЙ РЕГЛАМЕНТ
Системы «ИНГ Бизнес»
для клиентов-юридических лиц

(Редакция № 3.0)

ИНГ БАНК (ЕВРАЗИЯ) АКЦИОНЕРНОЕ ОБЩЕСТВО предоставляет доступ к Системе «ИНГ Бизнес» в соответствии с настоящим Техническим регламентом (далее – «**Регламент**»). Настоящий Регламент является неотъемлемой частью Условий расчетного обслуживания Клиентов-юридических лиц с использованием Системы «ИНГ Бизнес».

Для целей Регламента указанные ниже термины будут иметь соответствующее значение, если иное не предусмотрено контекстом.

1. Определения

Авторизация означает Процедуру проверки предоставленных прав на выполнение определенных действий, а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий. Работать в системе могут только зарегистрированные в ней и успешно авторизованные (то есть подтвердившие свое право работать под данным системным именем) Пользователи. Авторизация происходит при входе Пользователя в систему. Успешно авторизованным Пользователям предоставляется индивидуальный набор прав на выполнение операций в Системе и доступов к объектам Системы на основании Заявления Клиента.

Аутентификация означает процедуру опознания Пользователя Системой, путем проверки соответствия (сопоставления) указанных Пользователем данных, используемых для входа Пользователя в Систему.

Двухфакторная Аутентификация означает процедуру опознания Пользователя Системой, путем проверки Банком соответствия (сопоставления) указанных Пользователем данных логина и пароля Системы «ИНГ Бизнес», используемых для входа Пользователя в Систему, а также проверки введенного кода из PUSH-уведомления/СМС, используемых в качестве второго фактора аутентификации.

Банк означает ИНГ БАНК (ЕВРАЗИЯ) АКЦИОНЕРНОЕ ОБЩЕСТВО.

Удостоверяющий центр (УЦ) означает ООО «КРИПТО-ПРО», осуществляющее выполнение целевых функций удостоверяющего центра по изготовлению и управлению неквалифицированными сертификатами ключей проверки электронной подписи в соответствии с Федеральным законом «Об электронной подписи» в целях обеспечения применения участниками Информационной Системы неквалифицированной усиленной электронной подписи.

Оператор УЦ означает ИНГ БАНК (ЕВРАЗИЯ) АКЦИОНЕРНОЕ ОБЩЕСТВО, наделенное Удостоверяющим центром ООО «КРИПТО-ПРО» правами по осуществлению действий по регистрации и управлению сертификатами ключей подписей Пользователей Удостоверяющего центра в соответствии с Регламентом Оператора УЦ.

Регламент Оператора УЦ означает Регламент предоставления услуг Оператора Удостоверяющего центра ООО «КРИПТО-ПРО».

Клиент означает юридическое лицо, присоединившееся к Условиям расчетного обслуживания Клиентов- юридических лиц с использованием Системы «ИНГ Бизнес».

Канал Банка означает Мобильное приложение «ИНГ Бизнес» или Систему дистанционного

банковского обслуживания «ИНГ Бизнес».

Токен означает электронный носитель информации модели «РУТОКЕН ЭЦП 3.0», используемый для авторизации Клиента в Канале Банке и подписания Распоряжений Клиента в Системе, предоставляемый Банком Клиенту. Электронный носитель информации содержит Аналог собственноручной подписи. Это устройство USB-токен (USB-брелок), являющееся разновидностью сменного носителя криптографических ключей, а именно электронным персональным устройством хранения ключевой информации Электронной подписи в защищенном на аппаратном уровне виде.
Подробная информация по работе с Токеном, в том числе с ПИН-кодом Токена, доступна по ссылке: https://dev.rutoken.ru/pages/viewpage.action?pageId=72450129

Электронный документ означает любой электронный документ, в том числе Электронные платежные инструкции, Электронные выписки, Электронные статусы по платежным инструкциям, Документы произвольного формата, предусмотренные Системой «ИНГ Бизнес».

Электронная подпись (ЭП) означает информацию в электронной форме, которая присоединена к Электронному документу или иным образом связана с Электронным документом, полученная в результате криптографического преобразования с использованием Ключа ЭП, позволяющая идентифицировать Владельца сертификата ключа подписи, а также установить целостность и неизменность информации в Электронном документе, при этом Владелец сертификата ключа подписи должен быть уполномочен Клиентом подписывать документы.

Закрытый ключ электронной подписи (Ключ ЭП) означает уникальную последовательность символов, известной Владельцу сертификата ключа подписи и предназначенной для создания в Электронных документах Электронной подписи с использованием средств Электронной подписи.

Открытый ключ электронной цифровой подписи (Ключ Проверки ЭП) означает уникальную последовательность символов, предназначенную для подтверждения с использованием средств Электронной подписи подлинности Электронной подписи в Электронном документе.

Сертификат Ключа ЭП (Ключ ЭП) означает электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра, и подтверждающий принадлежность Ключа Проверки ЭП Владельцу сертификата ключа подписи.

Владелец сертификата ключа подписи (Владелец/Держатель) означает лицо, на имя которого аккредитованным удостоверяющим центром выдан Сертификат Ключа ЭП и которое владеет соответствующим Закрытым ключом электронной подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою Электронную подпись в Электронных документах (подписывать Электронные документы).

Пользователь означает физическое лицо, назначенное Клиентом, зарегистрированное в Системе «ИНГ Бизнес», и использующее Систему «ИНГ Бизнес» и Мобильное приложение «ИНГ Бизнес».

Комплекс программно-аппаратных средств означает программно-аппаратный комплекс Клиента, который должен соответствовать действующим требованиям к системе, программному обеспечению и иным параметрам, установленным Банком. Требования к конфигурации: Поддержка латинских и кириллических системных шрифтов; доступ в интернет.

Мобильное приложение «ИНГ Бизнес» (Мобильное приложение) означает программное обеспечение для операционных систем Android и iOS, используемое для Двухфакторной Аутентификации Пользователя.

Компрометация Токена и/или Электронной подписи, и/или доступа к Каналам Банка, означает утрату доверия к способности используемых Токенов и/или Электронной подписи, и/или доступа к Каналам Банка, обеспечить подлинность, защиту и безопасность документов, передаваемых сторонами по Каналу Банка. События, связанные с Компрометацией Токена и/или Электронной подписи, и/или доступа к Каналам Банка, включают в себя, без каких-либо ограничений, следующее:

- потеря Пользователем Токена –независимо от того, будет ли он найден впоследствии, или Пользователь не сможет его найти;
- потеря мобильного устройства, используемого для доступа к ИНГ Бизнес через Мобильное приложение;
- потеря данных авторизации (логин и/или ПИН);
- удаление или отключение Пользователя;
- возникающие подозрения в утечке или искажении информации при передаче документов по Каналу Банка.

2. Доступ к Системе «ИНГ Бизнес»

Для получения доступа к Системе «ИНГ Бизнес» и к Мобильному приложению «ИНГ Бизнес» Клиент должен предоставить в Банк надлежащим образом оформленное и подписанное Заявление Клиента на подключение к Системе «ИНГ Бизнес» в соответствии с Условиями расчетного обслуживания Клиентов-юридических лиц с использованием Системы «ИНГ Бизнес», в котором содержатся данные всех конечных Пользователей, а также параметры доступа к Системе.

Двухфакторная Аутентификация

Для дополнительной защиты от входа в Систему неуполномоченных лиц, в соответствии с политикой безопасности Банка, используется Двухфакторная Аутентификация. В этом случае после того, как Пользователь введет правильный логин и пароль (первый фактор Аутентификации), система предложит ему дополнительно ввести полученный одноразовый пароль из PUSH-уведомления, полученного через Мобильное приложение, либо одноразовый СМС-пароль (второй фактор Аутентификации). Только после успешного прохождения Двухфакторной Аутентификации Пользователь будет авторизован и сможет работать в Системе. PUSH-уведомление является основным вторым фактором Двухфакторной Аутентификации. Для получения PUSH-уведомлений Пользователь обязан произвести необходимые настройки в соответствии с Руководством пользователя (Приложение 4 к Условиям расчетного обслуживания Клиентов – юридических лиц с использованием Системы «ИНГ Бизнес»).

Двухфакторное подтверждение подписания Распоряжений

Для дополнительной защиты от подписания Распоряжения неуполномоченными лицами, в соответствии с политикой безопасности Банка, используется двухфакторное подтверждение подписания Распоряжений.

Первым фактором подтверждения подписания Распоряжений является успешная Авторизация.

Вторым фактором подтверждения подписания Распоряжений является ПИН-код Токена.

Любой электронный документ, созданный в Канале Банка, признается сторонами эквивалентным бумажному документу с оригинальной собственноручной подписью, если Клиент получает доступ к этому Каналу посредством Двухфакторной Аутентификации. Электронный документ считается подписанным от имени Клиента Пользователем, который согласно внутреннему журналу Канала Банка, получил доступ к данному Каналу Банка.

Требования для работы с Системой

Клиент должен обладать Комплексом программно-аппаратных средств. Клиент должен использовать только надлежащий и исправный Комплекс программно-аппаратных средств и обеспечивать его техническое обслуживание.

Перед началом работы с Системой и/или Электронной подписью, если это применимо, Пользователю необходимо установить вспомогательное программное обеспечение:

- Плагин BSS;
- Драйвер Рутокена.

Для установки плагина BSS и драйвера Рутокен используйте порядок, указанный в Приложении 1 настоящего Технического регламента.

Для работы с Системой Клиенту необходимо использовать следующие браузеры:

- Chrome;
- Firefox;
- Edge;
- Safari;
- Яндекс.Браузер.

Мобильное приложение «ИНГ Бизнес»

Мобильное приложение для операционной системы iOS доступно для скачивания в AppStore, для операционной системы Android – в Системе «ИНГ Бизнес» после авторизации Пользователя. Мобильное приложение используется для получения PUSH-уведомления в качестве основного второго фактора Аутентификации. Пользователь может войти в Мобильное приложение с помощью логина и пароля, а также с помощью функции сканера отпечатка пальца Touch ID, идентифицирующей Пользователя или с помощью функции распознавания лица Face ID, если устройство, с которого осуществляется вход, поддерживает данные функции. Данныефункции доступны на некоторых мобильных устройствах и позволяет Пользователю получить доступ к Мобильному приложению «ИНГ Бизнес» без указания логина и пароля при входе в Мобильное приложение. Для получения возможности использования функции Touch ID/ Face ID необходимо активировать ее на мобильном устройстве, сохранить в памяти мобильного устройства индивидуальные отпечатки пальцев/ изображения лица, а также специально активировать функцию Touch ID/ Face ID в Мобильном приложении. Мобильное приложение не собирает, не хранит и не использует данные об отпечатках пальцев/ изображении лица Пользователя. Пользователь всегда может отключить функцию Touch ID/ Face ID и использовать Мобильное приложение с помощью своего логина и пароля.

3. Выпуск Электронной подписи

Для регистрации и изготовления Сертификата Ключа ЭП Пользователь должен предоставить электронную заявку через Систему и документы на бумажном носителе в соответствии с Регламентом Оператора УЦ.

Регистрация Пользователя в УЦ и изготовление Сертификата Ключа ЭП осуществляется только при условии принятия Банком к обработке запрашиваемых документов и завершения проверки в соответствии с Регламентом Оператора УЦ.

4. Использование и порядок проверки Электронной подписи

После нажатия кнопки «Подписать» Система просит ввести ПИН-код Токена, который Держатель должен ввести в специальном поле на экране. В случае успешной проверки введенного ПИН-кода Токена Распоряжение считается подписанным, и Система уведомляет Держателя об успешном подписании Распоряжения на экране «Результаты подписи» для дальнейшей отправки в Банк.

5. Безопасность и конфиденциальность

Клиент (Пользователи) обязаны обеспечить надлежащие условия для хранения Токенов, которые исключают возможность их повреждения, потери и какого-либо несанкционированного использования, а также несанкционированного использования Мобильного приложения. Передача Токена и/или данных для авторизации в Системе и/или Мобильном приложении любым иным лицам строго запрещена и будет рассматриваться Банком как существенное нарушение настоящего Регламента.
При первичном получении Токена такой Токен содержит предустановленный начальный ПИН-код (ПИН Токена), который Клиент (Пользователь) обязан изменить для дальнейшего использования. Порядок смены ПИН-кода Токена указан в Приложении 2 настоящего Технического регламента.

Каждый Пользователь обязан:
1. предоставлять Банку полную и достоверную информацию относительно всех и любых действий, связанных с использованием Системы, Токена, ЭП, Мобильного приложения;
2. действовать в соответствии с обязательствами, процедурами и правилами, установленными документацией к Системе, Токену, ЭП, Мобильному приложению;
3. при использовании Системы, Токена, ЭП, Мобильного приложения использовать приложения Банка, а также программное обеспечение,предоставленное Банком;
4. использовать только действующие Токены, ЭП и, насколько может бытьизвестно Пользователю, ЭП, которые не были отозваны;
5. незамедлительно информировать Банк в случае (а также при наличии сомнений) злоупотребления Токена или потери Токена, таким образом, чтобы Банк имел возможность отозвать ЭП;
6. незамедлительно информировать Банк о любых изменениях в данных (которые произошли), связанных с использованием ЭП;
7. использовать, хранить и обращаться с Токеном с должной осмотрительностью, осторожностью и необходимой степенью защиты, включая обязанность хранить Токен таким образом, чтобы исключить возможность его использования неуполномоченными лицами;
8. не осуществлять каких-либо действий, которые могут привести к нарушению конфиденциальности или принципа непрерывности деятельности Банка.

Пользователь Системы также обязан:
- Хранить в тайне личный Закрытый ключ электронной подписи, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

- Применять для формирования Электронной подписи только действующий личный Закрытый ключ электронной подписи;
- При наличии оснований полагать, что тайна Ключа ЭП нарушена (произошла Компрометация), прекратить использование этого Ключа ЭП и немедленно начать процедуру аннулирования сертификата ключа проверки ЭП согласно Регламенту Оператора УЦ;
- Обновлять сертификат ключа проверки ЭП в соответствии с Регламентом Оператора УЦ. Поддерживать в актуальном состоянии программное обеспечение и операционную систему автоматизированного рабочего места, с которого Пользователь будет заходить в Систему;
- Поддерживать в актуальном состоянии антивирусное программное обеспечение;
- Использовать автоматизированное рабочее место, с которого Пользователь будет заходить в Систему, только в рабочих целях;
- Обеспечивать безопасность и конфиденциальность своих учетных данных для Аутентификации в автоматизированном рабочем месте;
- Для подключения к Системе использовать только доверенные и безопасные сети.

6. Нарушение безопасности

В случае Компрометации Токена и/или Электронной подписи, и/или доступа к Системе, и/или доступа к Мобильному приложению, Клиент обязан незамедлительно письменно уведомить Банк об этом происшествии с подробным описаниемобстоятельств вышесказанного.

Подразумевается, что при наступлении событий, связанных с Компрометацией Токена и/или Электронной подписи, и/или доступа к Системе, и/или доступа к Мобильному приложению, соответствующие Токены, ЭП и/или данные авторизации не подлежат дальнейшему использованию Клиентом (Пользователем). Также предполагается, что при условии соответствующего уведомления Банка при наступлении таких событий Банк вправе прекратить доступ к Системе «ИНГ Бизнес» с использованием таких Токенов, ЭП и данных авторизации и/или доступ к Мобильному приложению с данными авторизации, которые были затронуты вышеуказанными событиями.

7. Прочие положения

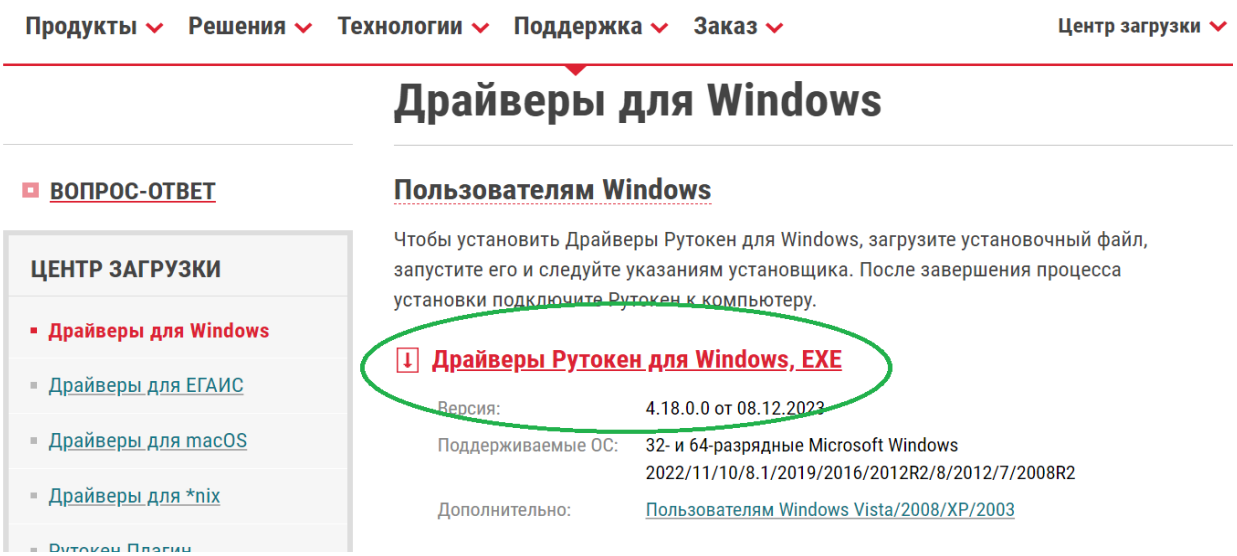
Банк вправе вносить изменения в настоящий Регламент в одностороннем порядке. Банк уведомляет Клиента об изменении Регламента путем публикации соответствующих сведений на своем Интернет-сайте, или иным способом по усмотрению Банка.
В случае перехода на новый способ Аутентификации Банк обязан письменно уведомить Клиента об этом за 30 (тридцать) календарных дней до подобного перехода.

Приложение 1
к Техническому регламенту
Системы «ИНГ Бизнес»

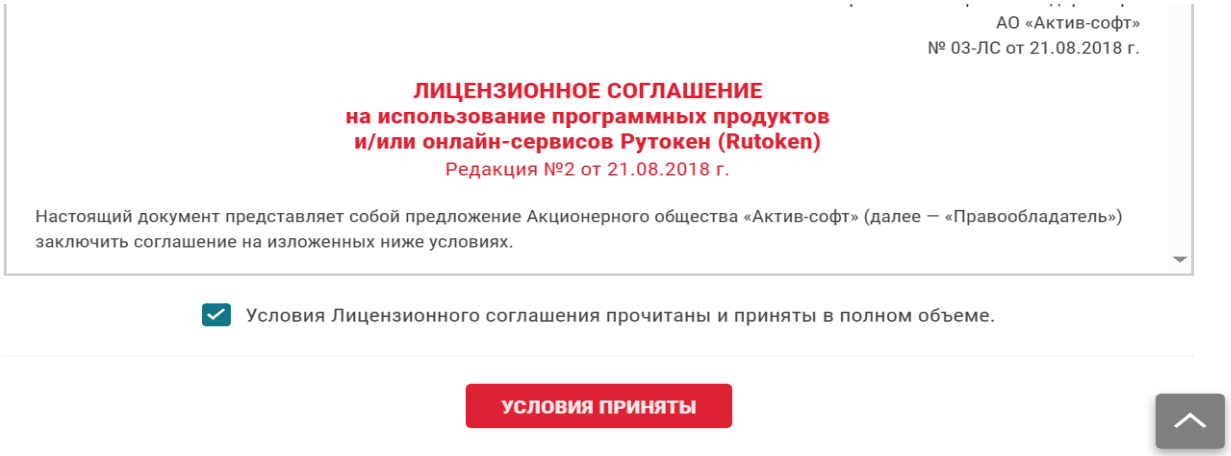
Инструкция по установке программного обеспечения
для работы с Системой «ИНГ Бизнес»

1. Установка драйвера Рутокен.

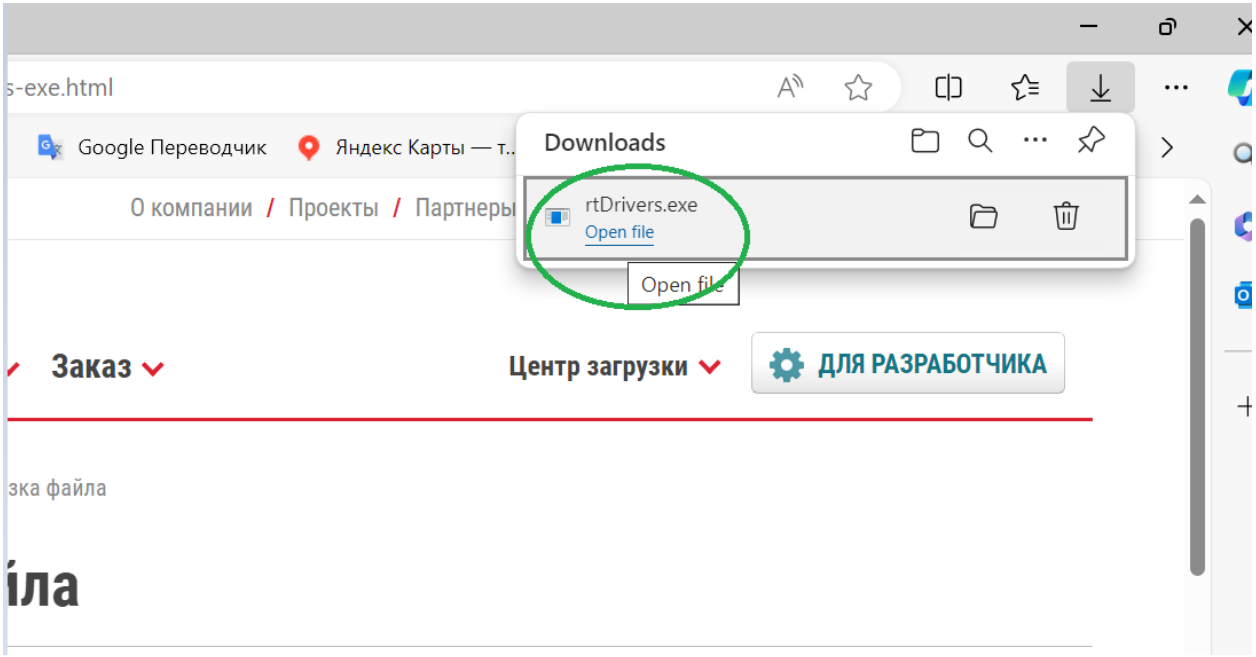
- Скачать драйвер Рутокен по ссылке Драйверы для Windows / Центр загрузки / Поддержка (rutoken.ru).



- Принять лицензионное соглашение и нажать «Условия приняты». На следующей страницы начнется автоматическое скачивание драйвера.

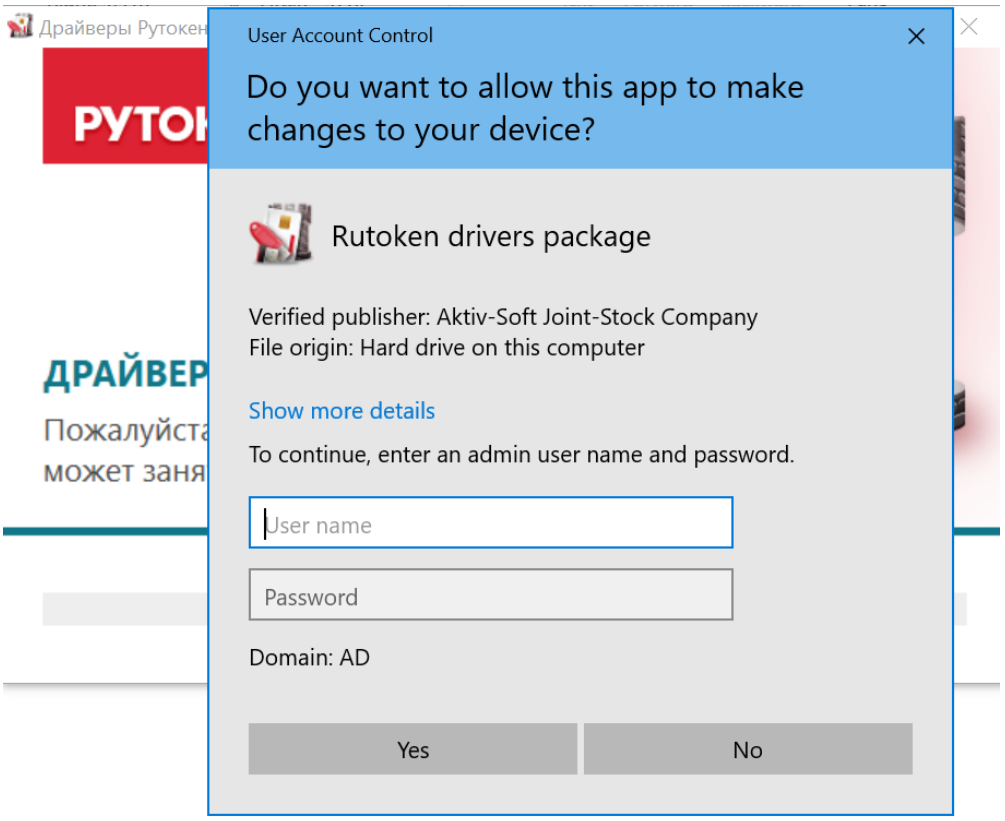


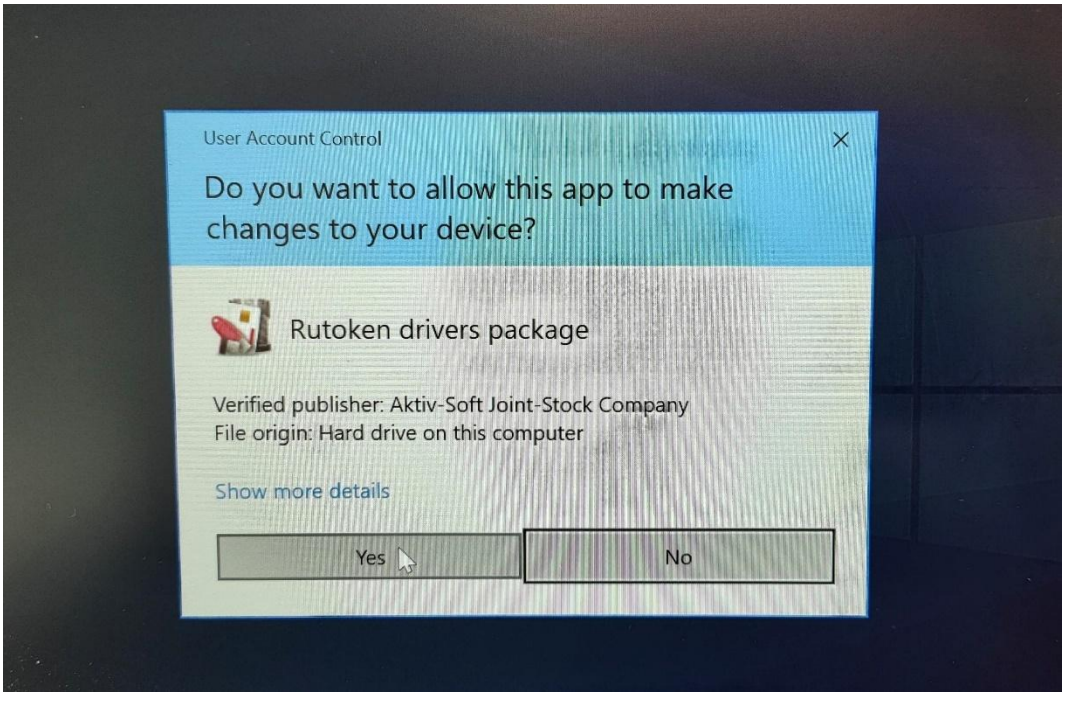
- Запустить скачанный файл прямо из браузера.



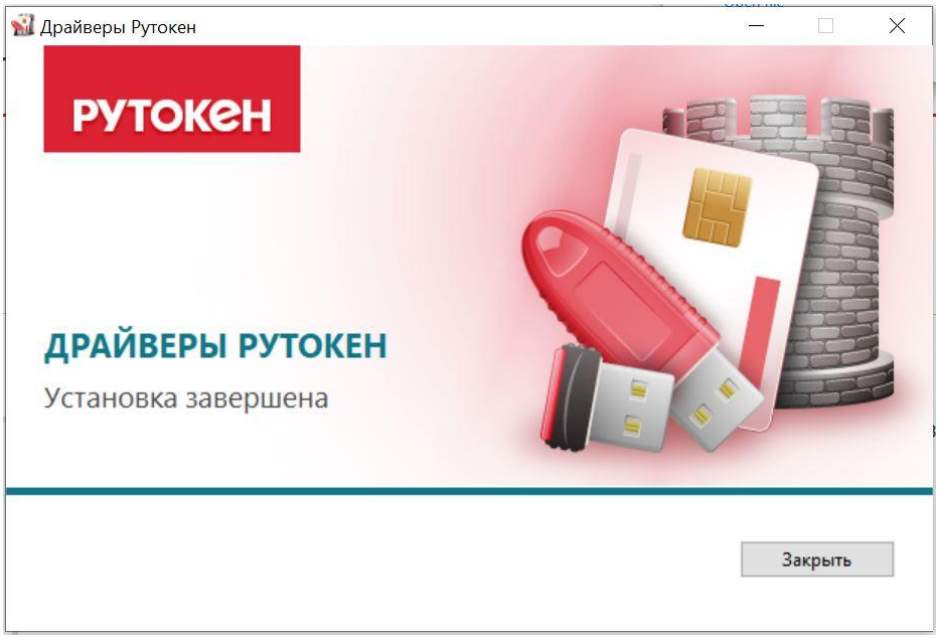
- Нажать «Установить».

- На данном этапе может потребоваться ввести логин и пароль Администратора, либо нажать “Да”(Yes) в окне контроля учетных записей.

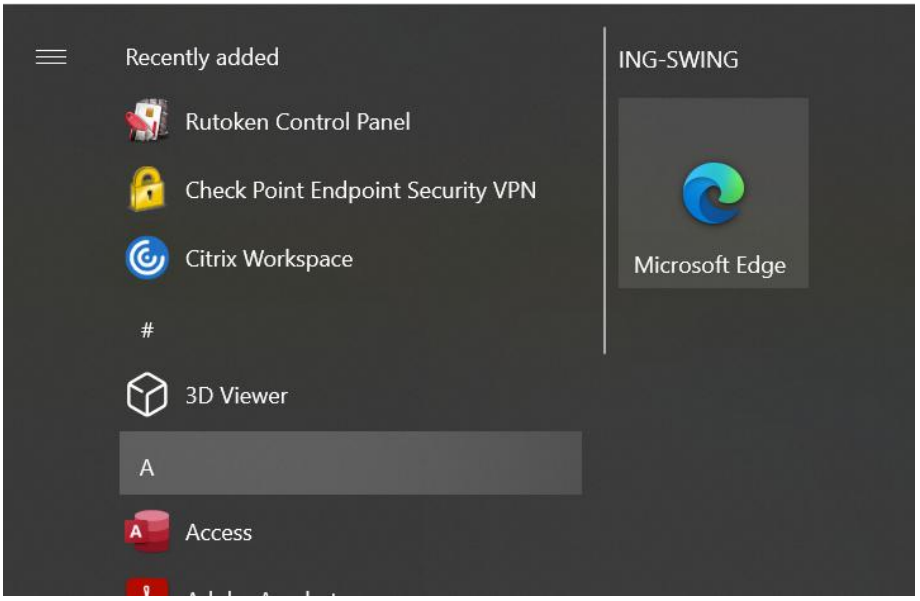




- По окончании установки нажать «Закрыть».

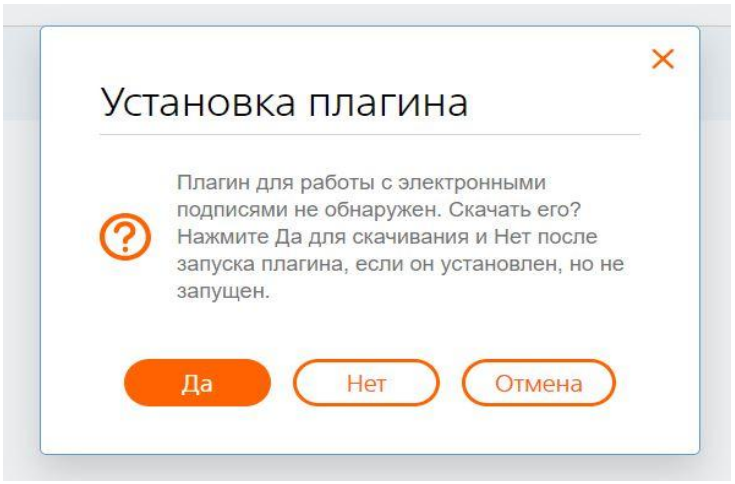


- По завершении установки Панель управления Рутокен появится в меню «Пуск».

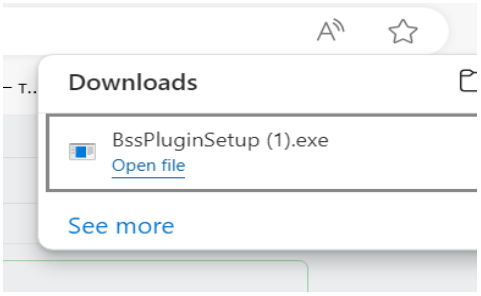


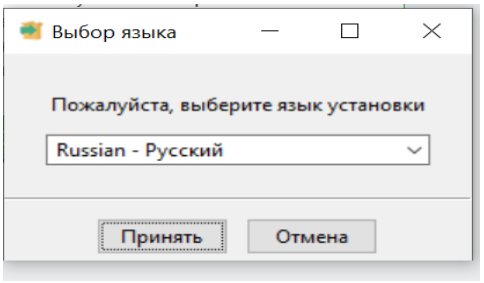
2. Установка плагина BSS

- При первом посещении портала ДБО https://business.ing.ru/ будет предложено скачать и установить плагин BSS. Нажать «Да». Нажимать кнопку «Скачать» в следующем окне не нужно.

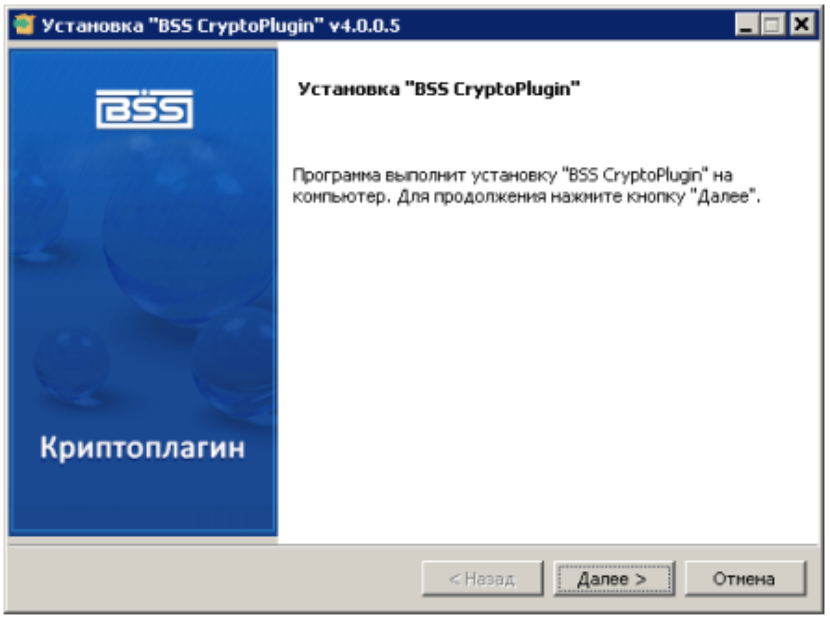


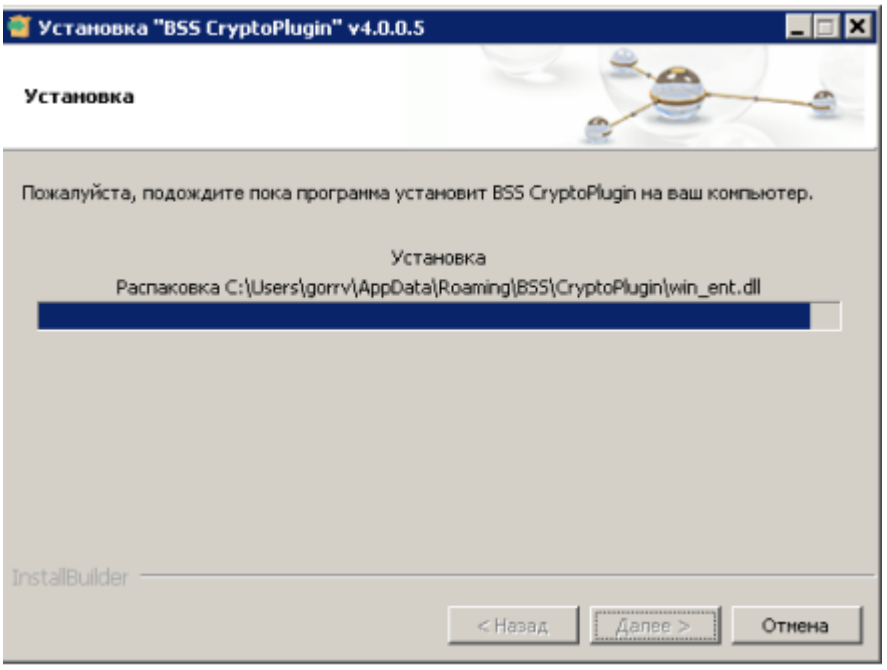
- Запустить скачанный файл. Нажать «Принять».



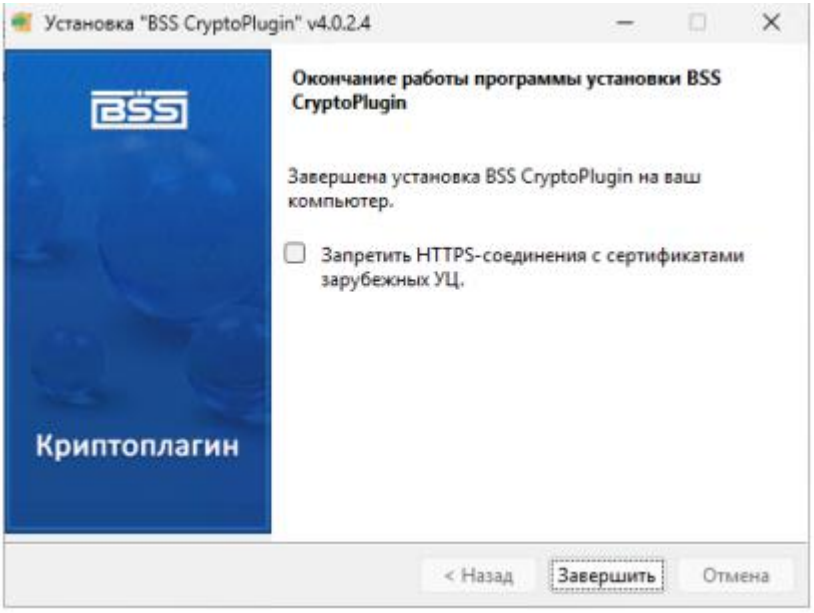


- Нажать «Далее».

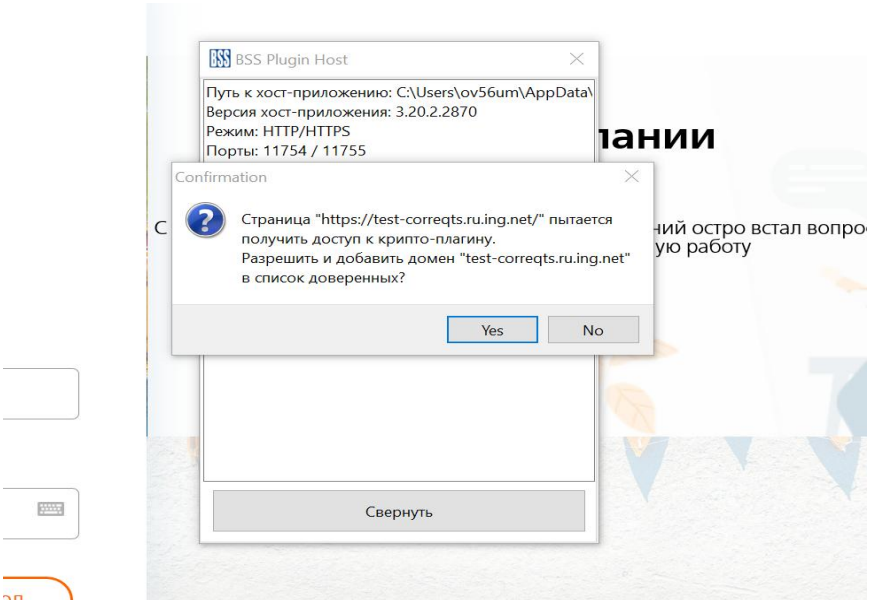




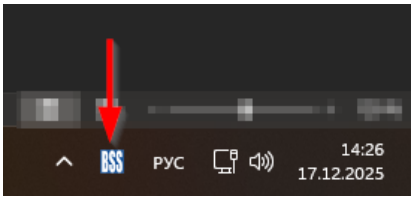
- По окончании установки нажать «Завершить».



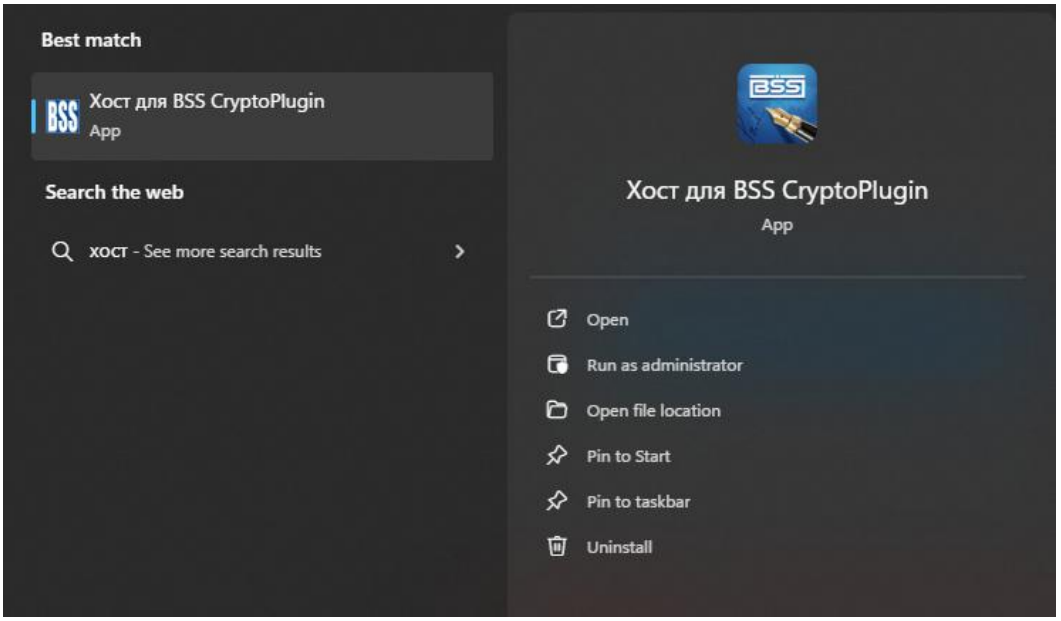
- Обновить страницу https://business.ing.ru/, появится уведомление от плагина на запрос доступа и добавление портала в список доверенных. Нажать “Yes”.



- Перед работой с сайтом ДБО убедитесь, что плагин запущен и отображается в трее:



- Если его там нет, плагин можно запустить из меню «Пуск»:

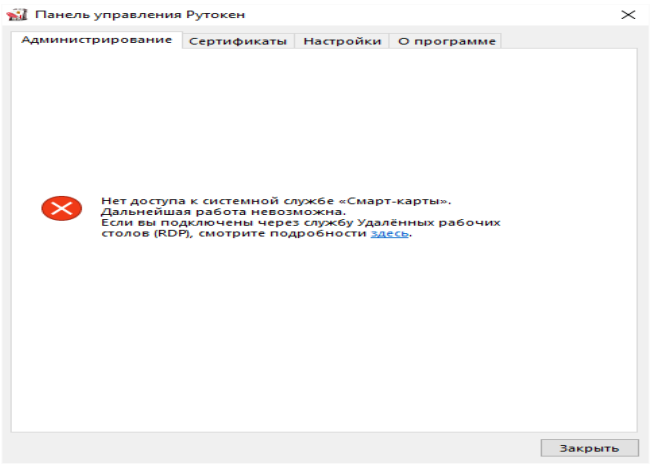


Установка и настройка программного обеспечения для работы с ДБО завершены!

Информация для технической поддержки Вашей организации

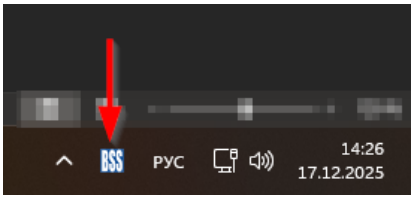
1. Рутокен

При возникновении проблем с драйвером Рутокен, например, «Нет доступа к системной службе «Смарт-карты». Дальнейшая работа невозможно», можно воспользоваться базой знаний PU1018 - База знаний - Сервер документации Рутокен (rutoken.ru).

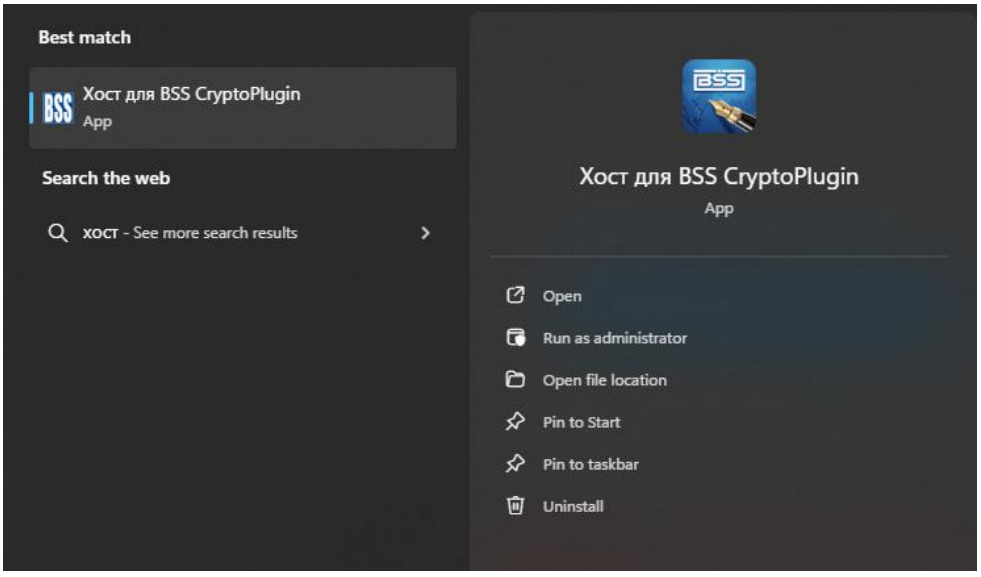


2. Плагин BSS

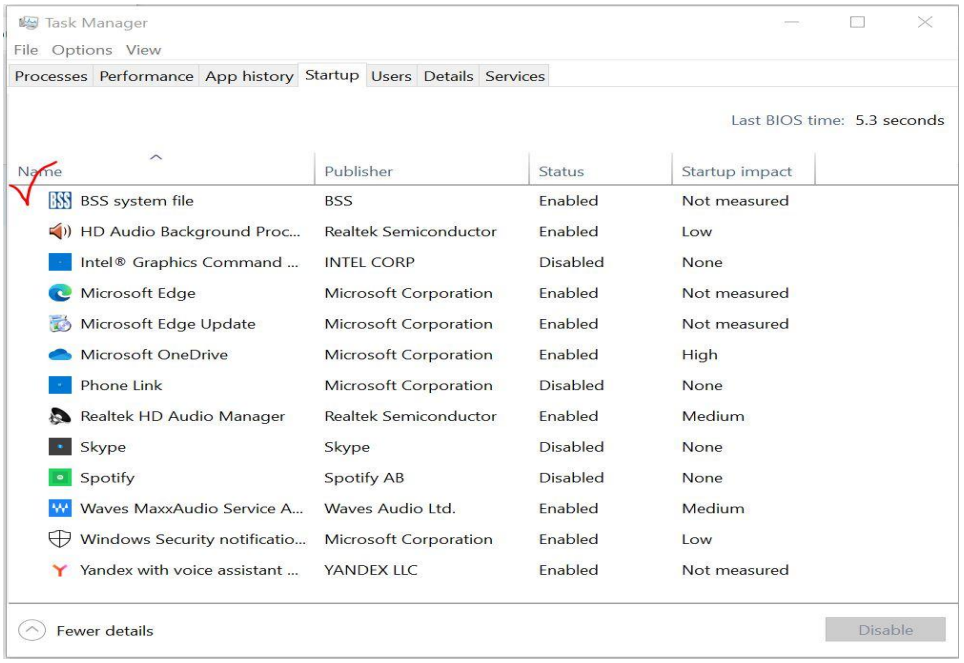
Если после установки плагина BSS сайт ДБО все равно предлагает скачать и установить плагин, убедитесь, что плагин запущен и отображается в трее:



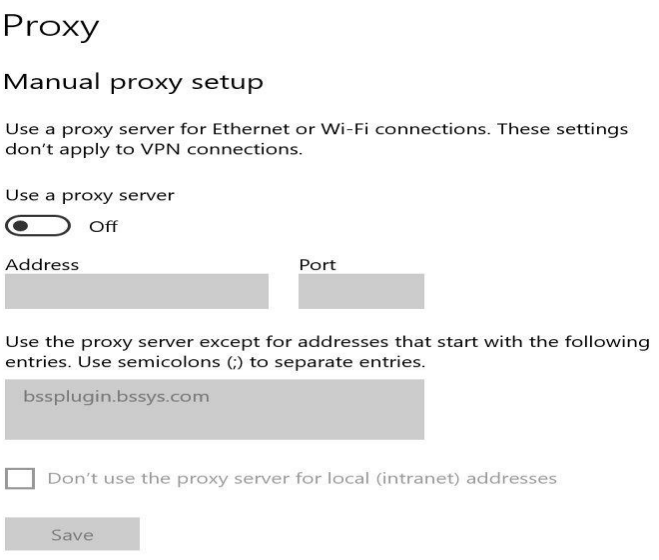
Если его там нет, плагин можно запустить из меню «Пуск»:



Также стоит проверить, есть ли плагин среди остального списка программного обеспечения автозагрузки:

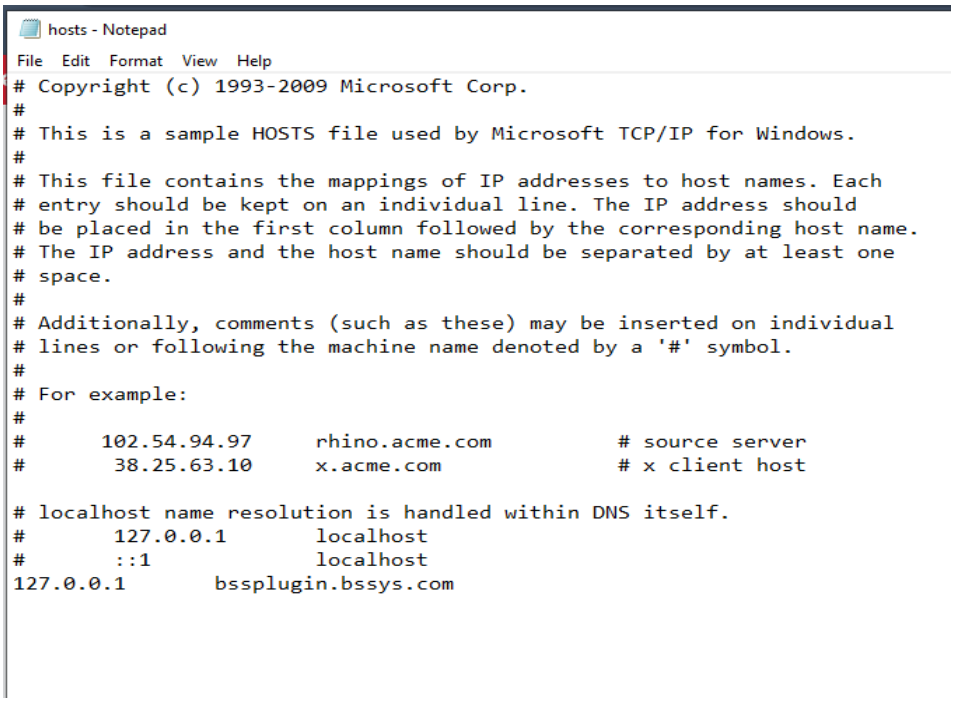


Проверьте, что адрес «bssplugin.bssys.com» включен в список исключения прокси (добавление должно происходить автоматически при установке плагина):



Возможно, вам потребуется добавить запись в файл Hosts (C:\Windows\System32\drivers\etc), если браузер все также не будет видеть установленный плагин.

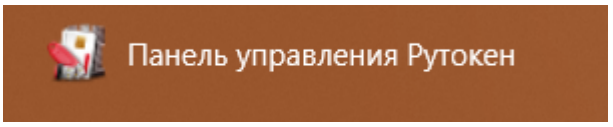
Запись: 127.0.0.1 bssplugin.bssys.com


hosts - Notepad
File Edit Format View Help
Copyright (c) 1993-2009 Microsoft Corp.
#
This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
This file contains the mappings of IP addresses to host names. Each
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding host name.
The IP address and the host name should be separated by at least one
space.
#
Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a '#' symbol.
#
For example:
#
102.54.94.97   rhino.acme.com   # source server
38.25.63.10   x.acme.com   # x client host
localhost name resolution is handled within DNS itself.
127.0.0.1   localhost
::1   localhost
127.0.0.1   bssplugin.bssys.com

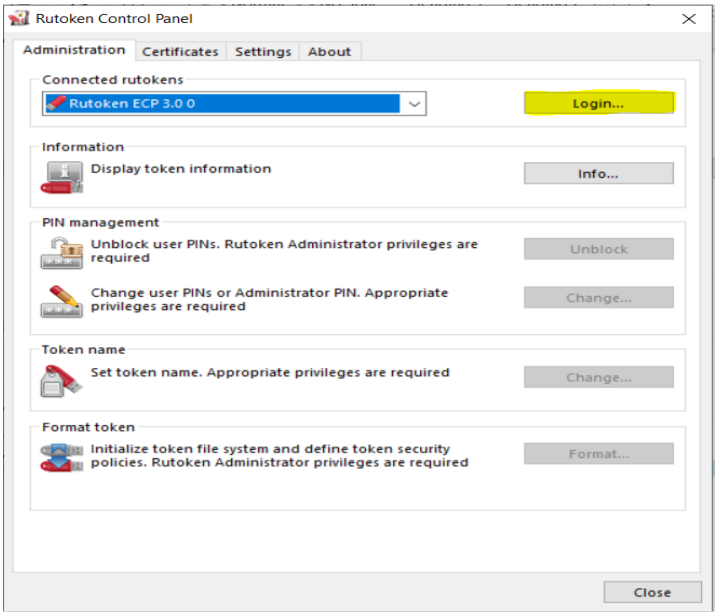
Приложение 2
к Техническому регламенту
Системы «ИНГ Бизнес»

Порядок смены ПИН-кода Токена (в том числе предустановленного)

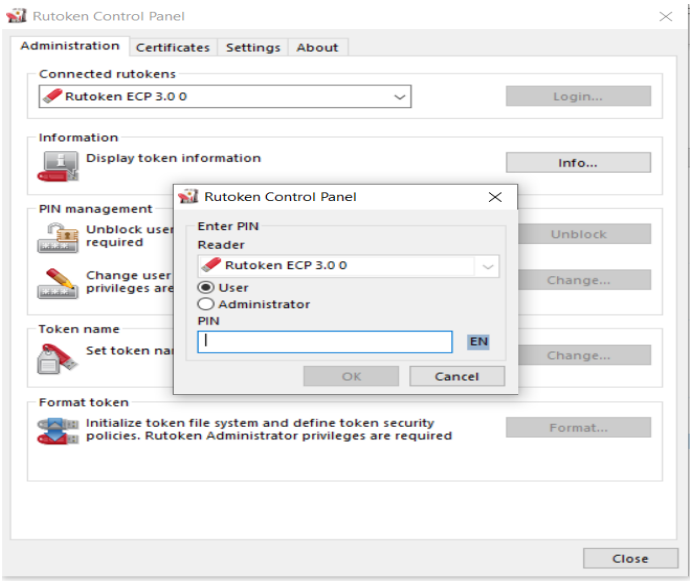
- Запустить приложение «Панель управления Рутокен»



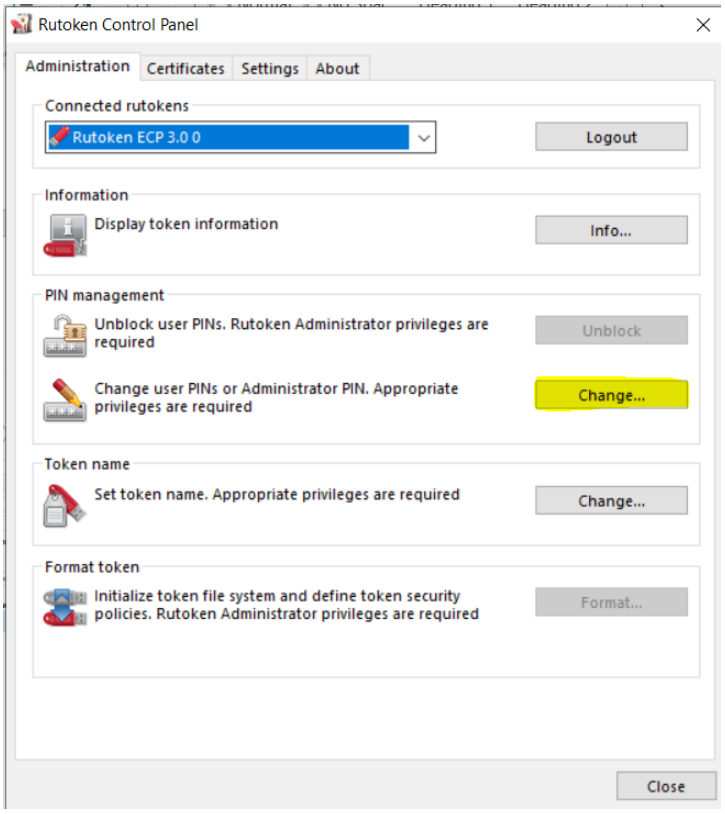
В открывшемся окне нажать “Login”



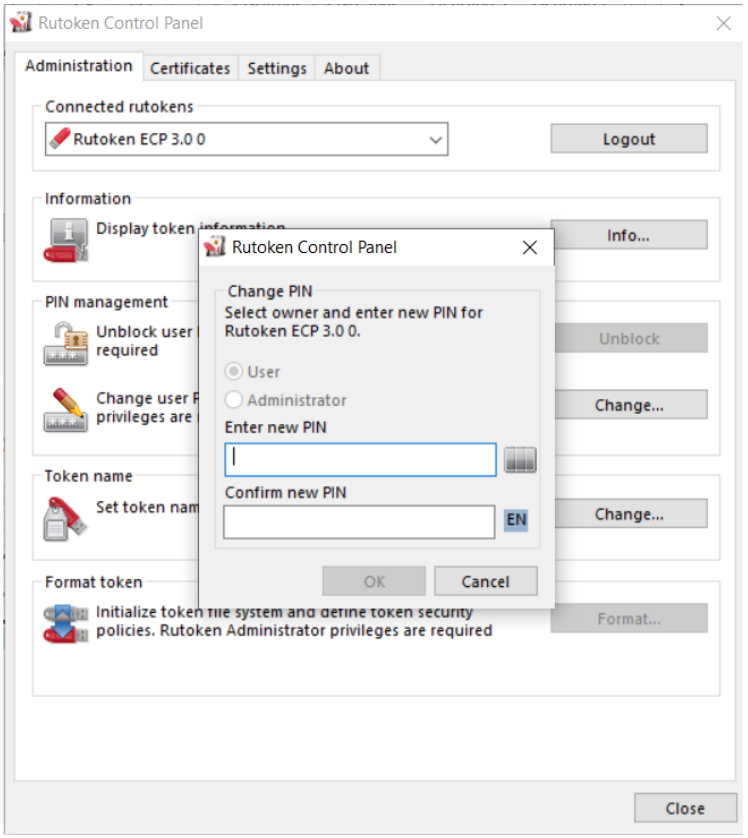
- Далее ввести текущий (или предустановленный 12345678) ПИН-код Пользователя (User) и нажать ОК



- В открывшемся окне нажать “Change”:



По умолчанию можно сменить только пароль Пользователя (User).



- Ввести и подтвердить новый ПИН-код Пользователя (User), далее нажать «ОК».