

Памятка новому пользователю Подсистемы «Интернет-Клиент»

Термины и сокращения

ИК – подсистема «Интернет-Клиент» (клиентская часть СДБО), которая предоставляет Клиентам возможность банковского обслуживания по сети интернет в режиме онлайн.

ЭЦП – электронная цифровая подпись.

СКЗИ – средство криптографической защиты информации.

НКИ – носитель ключевой информации - малогабаритное USB-устройство, предназначенное для защищенного хранения личных ключей пользователей (абонентов).



ПО – программное обеспечение.

Для работы в Подсистеме ИК зарегистрированному пользователю следует осуществить:

- [запуск Подсистемы ИК](#);
- [установка ПО для работы с ЭЦП «Avest»](#);
- [создание запроса на выпуск сертификата](#);
- [импорт личного сертификата](#) (файл с расширением *p7b*);
- [программное обеспечение для работы с СКЗИ \(ldd-server\)](#);
- авторизацию с помощью ЭЦП.

Запуск Подсистемы ИК

Для запуска Подсистемы ИК необходимо:

- запустить Web-браузер (Google Chrome 37 и выше , Opera 13 и выше ,

Mozilla 33 и выше , Explorer 8 и выше );

- указать в адресной строке ввода Web-браузера <https://eparitet.by/signin> и нажать на клавишу ВВОД (Enter);
- на экране появится стартовая страница Интернет-Клиента (Рис.1).

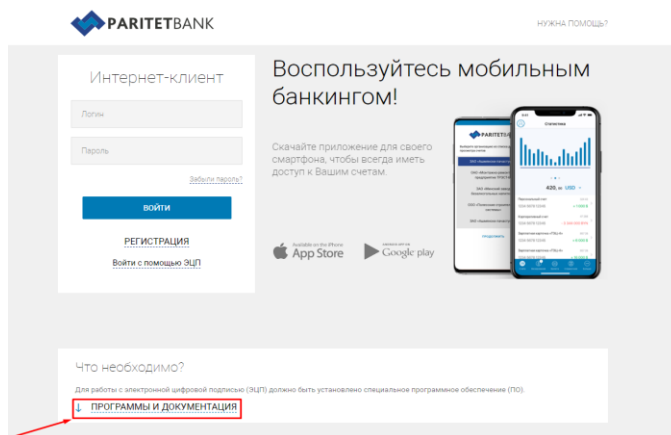


Рис. 1

Со стартовой страницы ИК следует нажать на кнопку «Программы и документация» (см. Рис.1), после нажатия откроется страница (см. Рис.2), с которой необходимо скачать ПО для работы с СКЗИ (ldd-server)

[ldd_server_crypt_installer.exe](#) и скачать объединённый инсталлятор ПО «Авест для ПаритетБанка» – [Пакет установочных файлов ПО Авест AvPKISetup_base_Paritet](#). (см. Рис.2).

Если используете **ключ налоговой организации** - достаточно будет скачать и установить [программное обеспечение для работы с СКЗИ \(ldd-server\)](#). При этом на компьютере должно быть установлено налоговое программное обеспечение. При возникновении проблем с установкой налоговых программ, необходимо обратиться в *службу технической поддержки ГосСУОК (+3751731130 00)*.

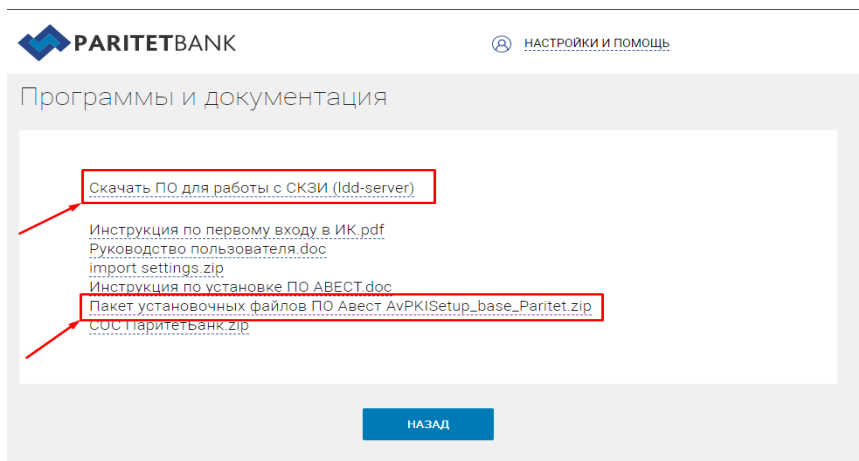


Рис. 2

Установка ПО для работы с ЭЦП «Avest»

После загрузки (сохранения файла) объединённого инсталлятора ПО «Авест для ПаритетБанка» ([Пакет установочных файлов ПО Авест AvPKISetup_base_Paritet](#)). распаковать архив и выполнить запуск файла **AvPKISetup2.exe** (см. рис. 3), произведя следующие действия:

Имя	Дата изменения	Тип	Размер
data	17.03.2017 15:39	Папка с файлами	
docs	14.03.2017 10:49	Папка с файлами	
autorun.inf	18.02.2009 14:50	Сведения для уст...	1 КБ
AvBelCert.dll	17.01.2006 15:17	Расширение при...	400 КБ
AvBelCert2.dll	22.04.2014 11:32	Расширение при...	1 136 КБ
AvCertStoreUtl.dll	23.07.2014 16:56	Расширение при...	124 КБ
AvPkiSetup.cfg	17.05.2016 10:59	Файл configura...	27 КБ
AvPKISetup2.exe	15.03.2016 15:01	Приложение	923 КБ
AvPKISetup2ResRu.dll	11.08.2006 10:58	Расширение при...	375 КБ

Рис. 3

- В появившемся окне нажимаем «Далее» (см. рис. 4).
- Выбираем тип инсталляции «Установка» и нажимаем «Далее» (см. рис. 5).

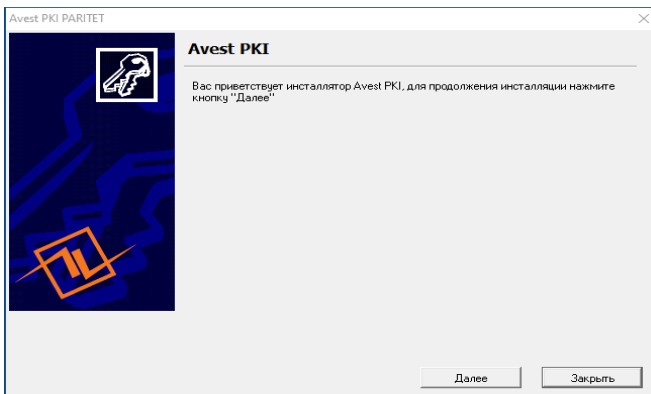


Рис. 4

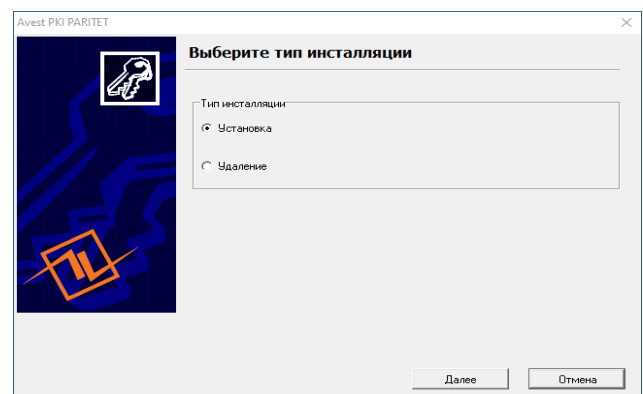


Рис. 5

- При выборе компонентов, ничего не изменяя, нажимаем «Далее» (см. рис. 6). В случае наличия установленных на компьютере криптопровайдеров Avest CSP 6.3.0.800 и Avest CSP Bel 6.3.0.800 галочки напротив этих пунктов будут отсутствовать.
- В пределах главного окна нужно подвигать мышью до окончания сбора случайности (до 100%) (см. рис. 7).

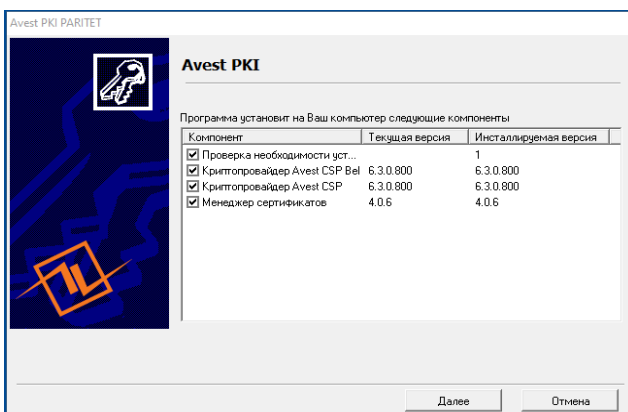


Рис. 6

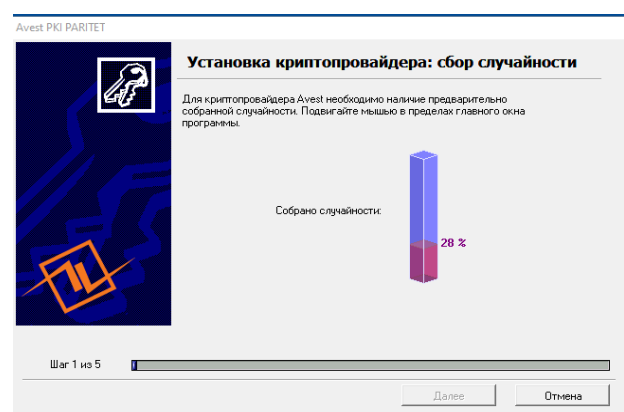


Рис. 7

- По завершению установки ПО «Авест для Паритетбанк» появится результат работы программы объединённого инсталлятора (см. рис. 8).

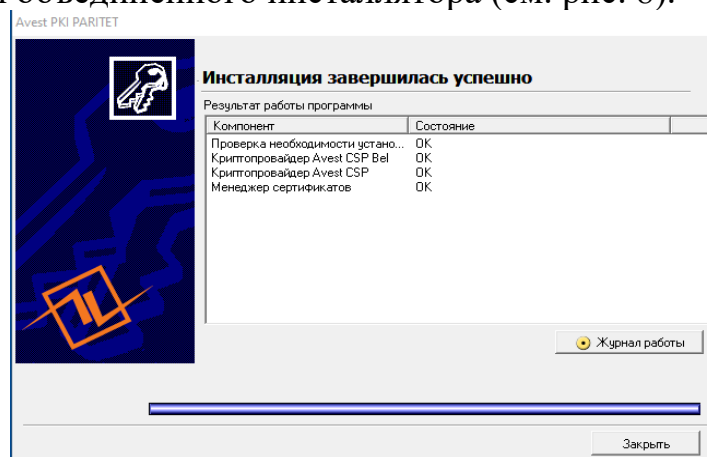
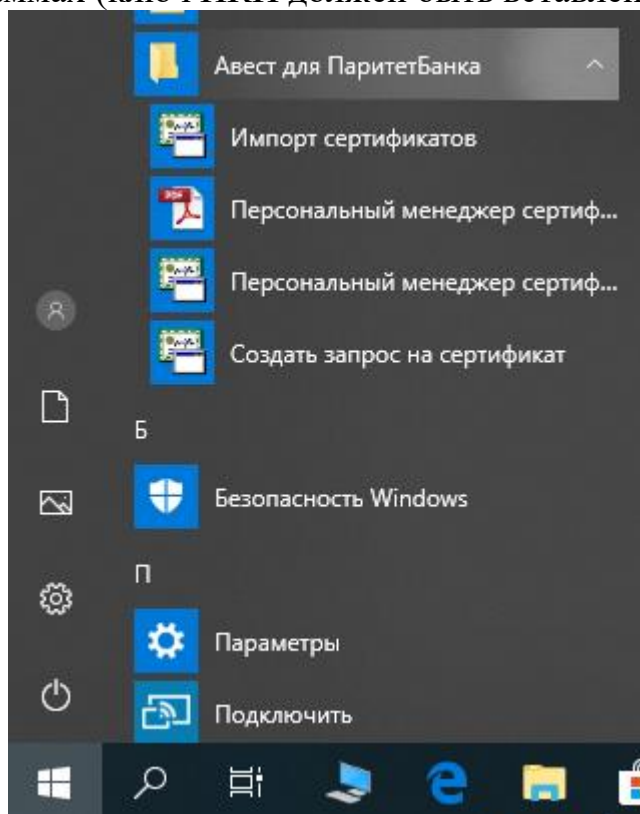


Рис. 8

- ПО «Авест для ПаритетБанка» будет полностью установлено только в случае появления результата работы программы (см. рис. 8). При установке возможна неоднократная перезагрузка компьютера. Если компьютер перезагрузился, а установка автоматически не продолжилась, то необходимо запустить файл **AvPKISetup2.exe** повторно (см. рис. 3).

Создание запроса на выпуск сертификата

1. Запустить ярлык «*Персональный менеджер сертификатов Авест*» на Рабочем столе компьютера или выбрать из основного меню *Windows* во *Всех программах* (ключ НКИ должен быть вставлен);



2. Далее «*Войти в систему без авторизации*» (см. Рис.13) и «*Подготовить запрос на сертификат*» (см. Рис.14);

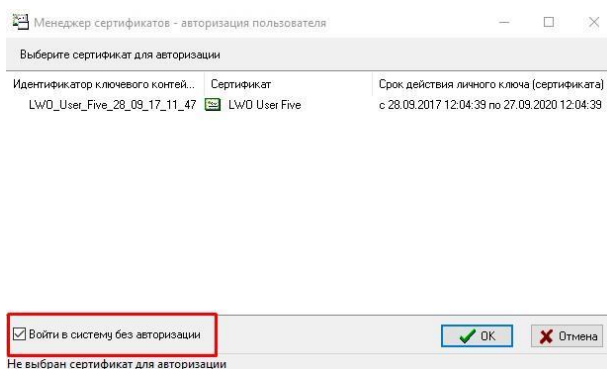


Рис. 13

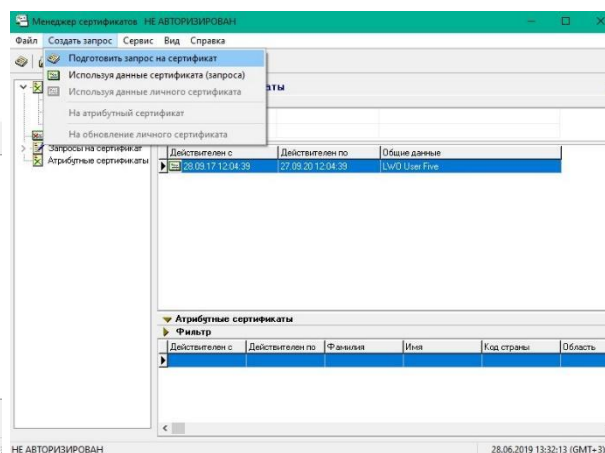


Рис. 14

3. В появившемся окне мастера создания запроса на сертификат выбрать шаблон для создания сертификата – «Сертификат абонента системы» (см. Рис.15);

4. В следующем диалоговом окне надо задать реквизиты будущего владельца сертификата для карточки открытого ключа, включаемые в запрос на сертификат (см. Рис.16) Обращаем Ваше **внимание**, что поле «Наименование организации» должно быть заполнено согласно Свидетельства о государственной регистрации. Индивидуальным предпринимателям в поле «Наименование организации» необходимо писать без сокращений (например: Индивидуальный предприниматель Иванов Иван Иванович). Поле «Подразделение» и «адрес электронной почты» являются не обязательными для заполнения. Все остальные поля **ОБЯЗАТЕЛЬНЫ** к заполнению. **В случае некорректности заполнения полей в параметрах сертификата запрос Банком обработан не будет.**

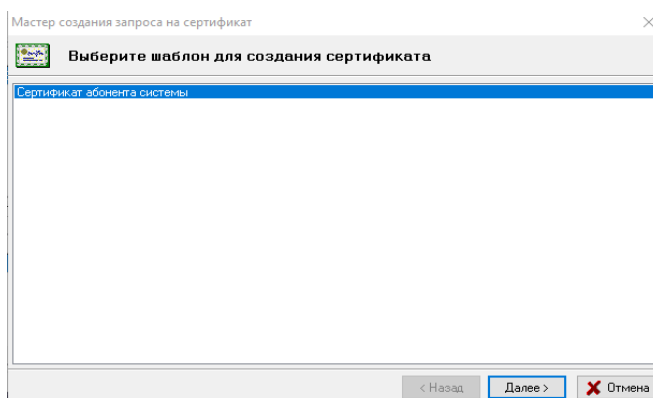


Рис. 15

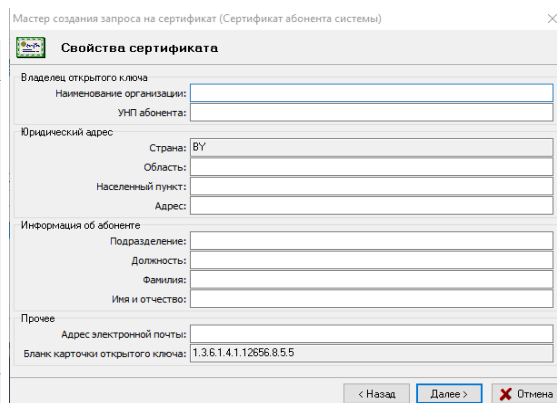


Рис. 16

Примечания:

В поле «адрес» ввести юридический адрес организации начиная с «ул.».

Для ИП (Индивидуального предпринимателя) в поле «Должность» написать - Индивидуальный предприниматель.

Поле «Имя и отчество» должно быть заполнено согласно документа удостоверяющего личность, без сокращений (не инициалы).

Затем появится окно, в котором будет указано Применение личного ключа пользователя (см. Рис.17).

5. В следующем диалоговом окне определяется срок действия сертификата пользователя (см. Рис.18);

По умолчанию включен флажок «Срок действия сертификата задается удостоверяющим центром» и поля «действителен с» и «действителен по» заполнены значениями «0». Данные не редактируем.

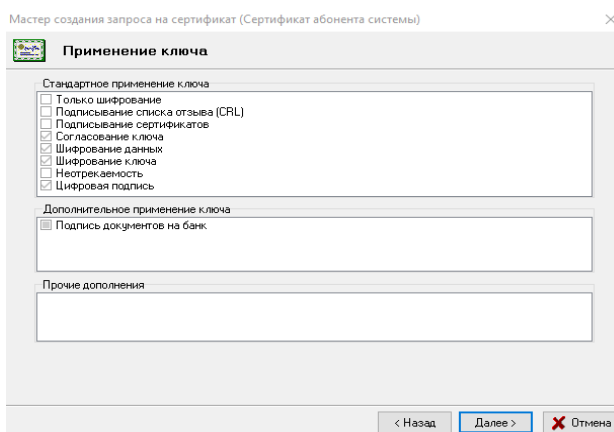


Рис. 17

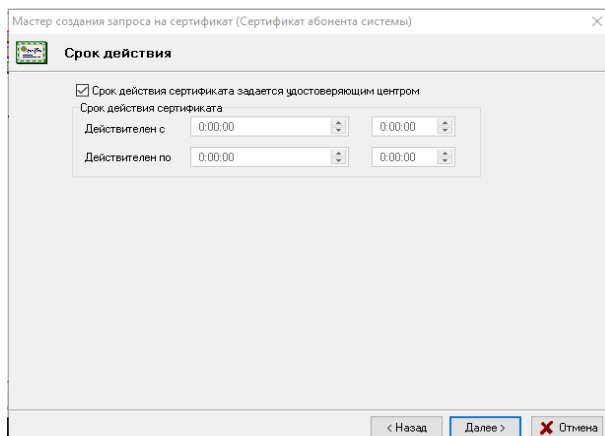


Рис. 18

6. Затем, в появившемся окне, надо задать имя контейнера, в который будет помещен Ваш личный ключ (см. Рис.19). По умолчанию программа создаст контейнер личных ключей с именем «**[Наименование организации владельца открытого ключа]_дд_мм_гг_чч_мм**», где «дд_мм_гг_чч_мм» – это дата и время генерации ключей.

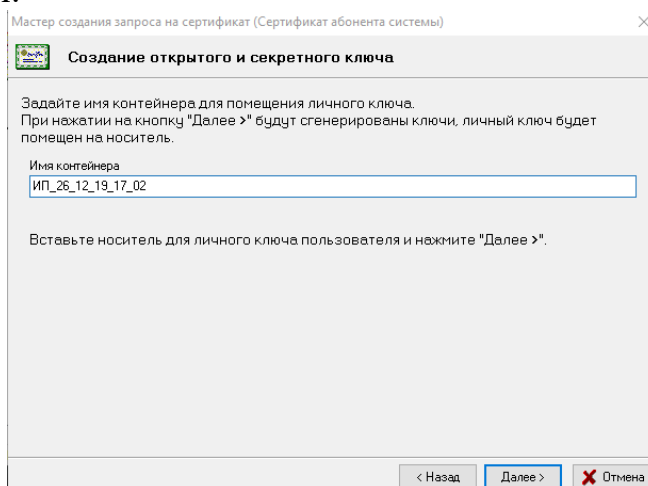


Рис. 19

7. Если на компьютере установлено несколько носителей личных ключей, в поле «Носитель» необходимо указать носитель, на который будут записан секретный ключ ЭЦП и шифрования, соответствующий СЕРТИФИКАТУ (запросу). Банк предоставляет пользователям систем ДБО носители типа Avest Token (AvToken). Проверить соответствие указанного в программе носителя можно по серийному номеру, который указан на корпусе USB-носителя и в соответствующем поле программы. ввести в соответствующих полях пароль и его подтверждение и нажать «ОК» (см. Рис.20);

Указанный (и подтвержденный) пароль доступа к контейнеру в дальнейшем будет использоваться для входа в ИК с помощью ЭЦП. Пароль должен быть не менее 8 символов и не должен состоять из одинаковых символов.

Внимание!

* Введенный Вами пароль невозможно восстановить. В случае «утери» пароля всю процедуру создания запроса и выдачи СЕРТИФИКАТА необходимо будет проходить повторно.

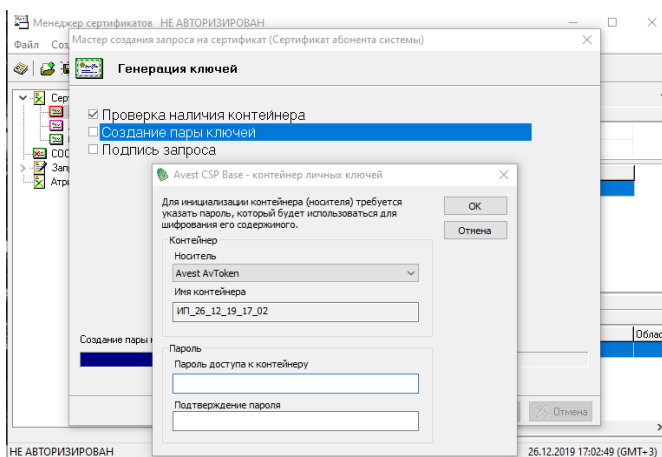


Рис. 20

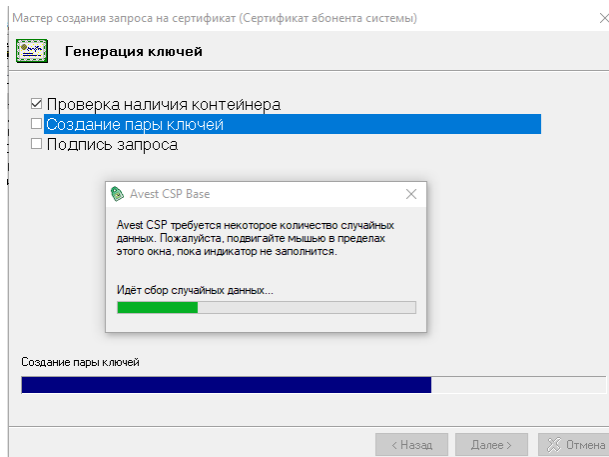


Рис. 21

8. Для создания личных ключей программе требуется некоторое количество случайных данных, поэтому «подвигайте» курсором мыши в пределах появившегося окна до полного заполнения полосы индикации (см. Рис.21);

9. После этого будет сформирована *карточка открытого ключа* (см. Рис.22), которую требуется распечатать в 2 экземплярах, подписать, поставить печать организации и передать в Банк 1 экземпляр карточки открытого ключа (без карточки открытого ключа запрос не может быть обработан). Выдача **СЕРТИФИКАТА** осуществляется банком не позднее следующего рабочего дня с момента предоставления клиентом корректно оформленной и удостоверенной карточки открытого ключа в обслуживающее подразделение банка.

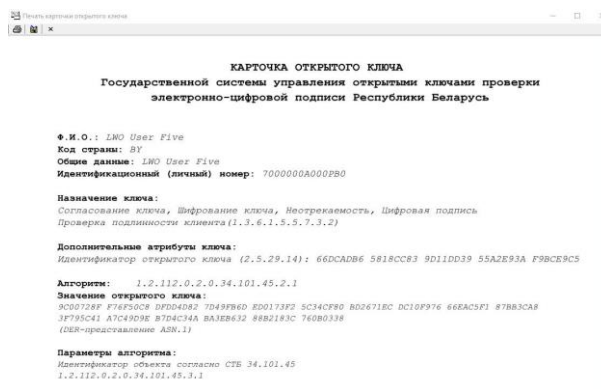


Рис. 22

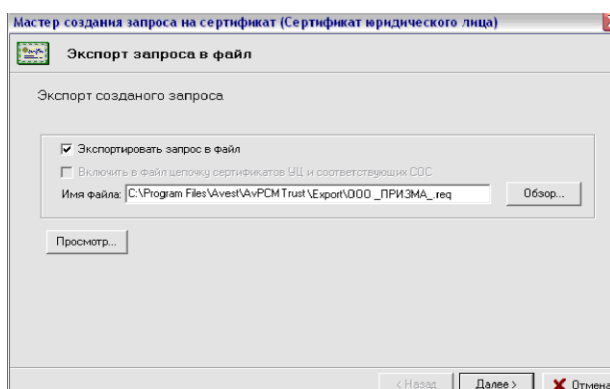


Рис. 23

10. Закройте карточку открытого ключа, и отметьте чек-бокс «Экспортировать запрос в файл» (см. Рис.23). С помощью кнопки «Обзор» можно изменить путь выгрузки файла.

Появится окно «Работа мастера завершена». Запрос создан.

Передача в Банк запроса на сертификат

Если ключ получен на стороне Банка

Зайдите *C:\ProgramFiles\Avest\AvPCM_Paritet\Export* (или по пути, по которому сохранили файл) и отправьте по электронной почте файл с расширением

.req (например, *ООО_КЛИЕНТ.req*) на адрес ib@paritetbank.by с заголовком письма «Запрос на сертификат Название организации» (согласно Свидетельства о государственной регистрации) и УНП. (см. Рис.24)

Далее !!! передайте в Банк карточку открытого ключа на бумажном носителе с подписью и печатью организации (без карточки открытого ключа запрос не может быть обработан).

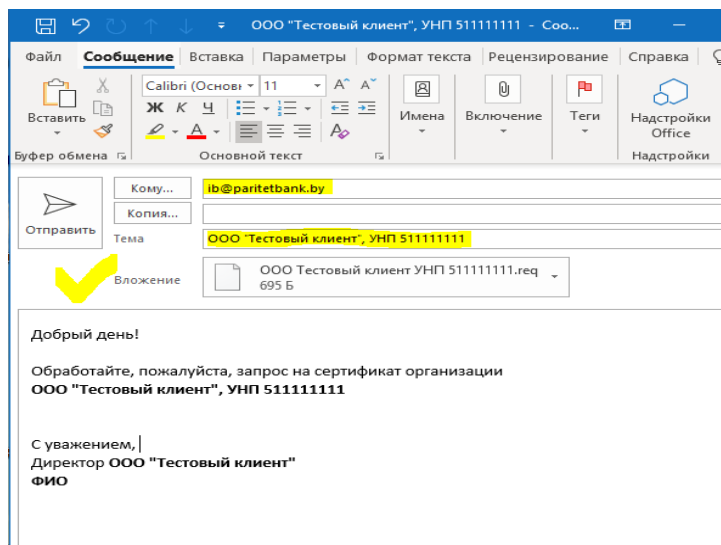


Рис.24

Если ключ получен в налоговой организации (ГосСУОК)

1. Запустить ярлык «Персональный менеджер сертификатов ГосСУОК» на Рабочем столе компьютера или выбрать из основного меню *Windows* во *Всех программах*;

2. Далее «Войти в систему без авторизации»;

3. Выбрать нужный сертификат, кликнуть правой кнопкой мыши – экспорт сертификата в файл (либо найти сертификат на компакт-диске с ПО ГосСУОК).

Важно! При сохранении сертификата выбрать тип файла: *p7b*.

4. Затем необходимо сформировать и отправить письмо с почтового адреса организации на ib@paritetbank.by, приложив сохранённый файл (по аналогии с ключом из Банка) и предоставив в банк карточку открытого ключа.

Получение из Банка файлов сертификатов

После отправки запроса, ожидайте «ответное» письмо на Ваш электронный ящик, в котором будет содержаться сертификат в формате **.p7b* (например, *УНП_ООО_КЛИЕНТ.p7b*, обычно, как название запроса). Полученный сертификат необходимо скачать на компьютер (например, на рабочий стол) и проимпортировать в персональный менеджер сертификатов Авест.

Импорт сертификата

Зайдите в «Персональный менеджер сертификатов Авест», поставьте «галочку» в поле «Войти в систему без авторизации» и нажмите «ОК», ключ НКИ должен быть вставлен в ПК.

Затем нажмите «Файл»→ «Импорт сертификата/СОС» (см. Рис.25).

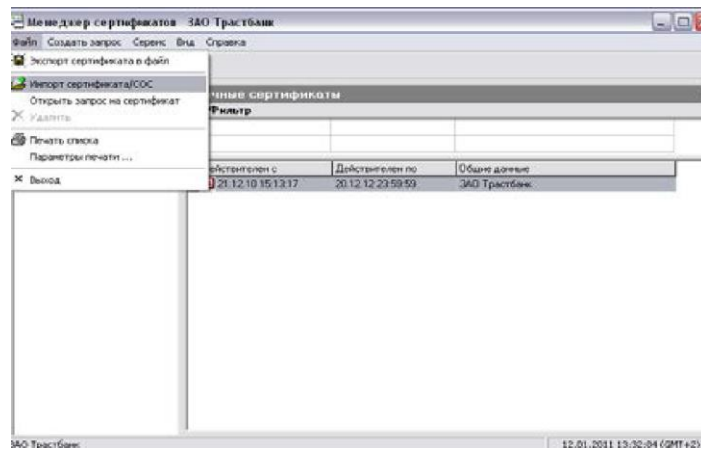


Рис. 25

В появившемся окне (см. Рис.26) нажмите «Обзор». В диалоговом окне мастера импорта сертификатов необходимо выбрать файл личного сертификата.

Для продолжения процедуры помещения личного сертификата в персональный справочник надо из списка выбрать контейнер личного ключа, который соответствует личному сертификату, отметить чек-бок «Поместить личный сертификат в контейнер» и нажать кнопку «Далее» (см. Рис. 27).

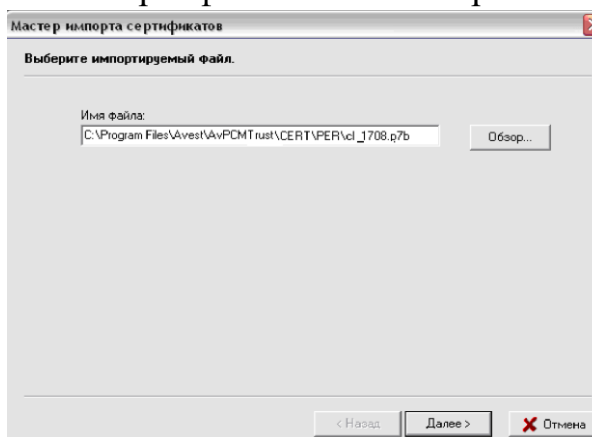


Рис. 26

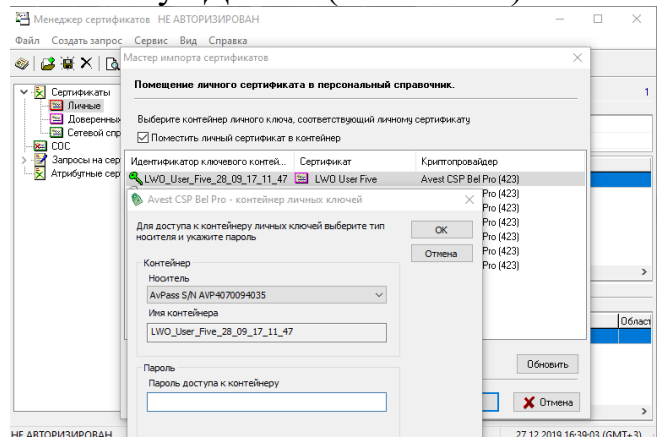


Рис. 27

Затем для доступа к ключевому контейнеру в поле «Пароль доступа к контейнеру» необходимо ввести пароль, который Вы вводили при создании запроса на сертификат (см. Рис.28). После успешного ввода пароля будет предложено установить сертификат центра сертификации, необходимо нажать «Да» (см. Рис.29).

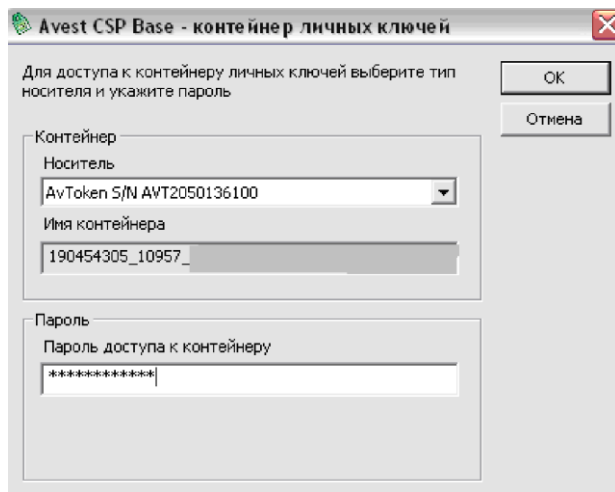


Рис. 28

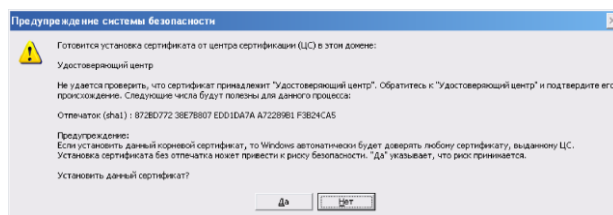


Рис. 29

Для полнофункциональной работы программы необходимо установить доверие к корневому сертификату УЦ. Для этого в следующем окне надо поставить чек-бокс «Установить доверие сертификату корневого УЦ» (см. Рис. 30).

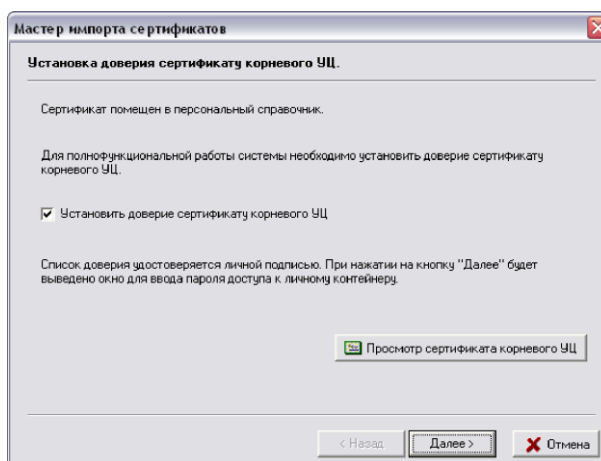


Рис. 30

После этого будет выведено сообщение о том, что корневой сертификат УЦ помещен в список доверия и мастер импорта сертификатов завершил работу.

Программное обеспечение для работы с СКЗИ

Для полноценного доступа к функционалу в Подсистеме ИК (с использованием ЭЦП) необходимо установить ПО для работы с СКЗИ (ldd-server).

Для этого запустите, ранее скаченное ПО и в каждом окне мастера установки нажмите кнопку «Далее» (см. Рис.31 – Рис.34) и «Установить».

Важно! Обязательно отметить чек-бокс «Автоматическая загрузка при старте».

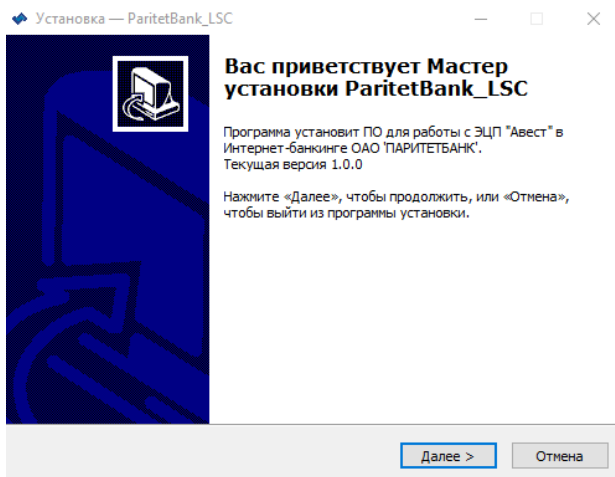


Рис. 31

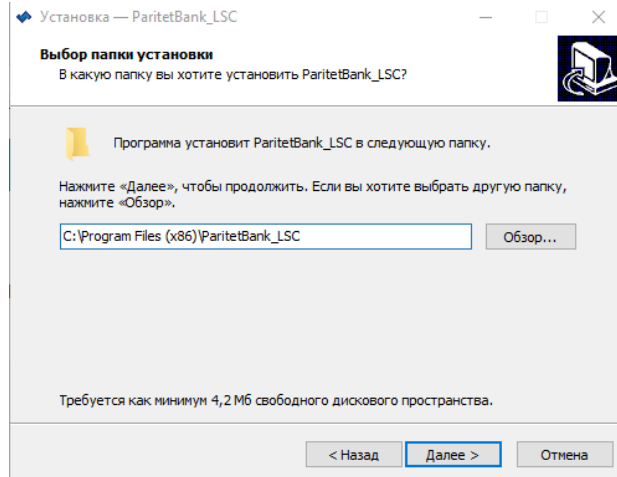


Рис. 32

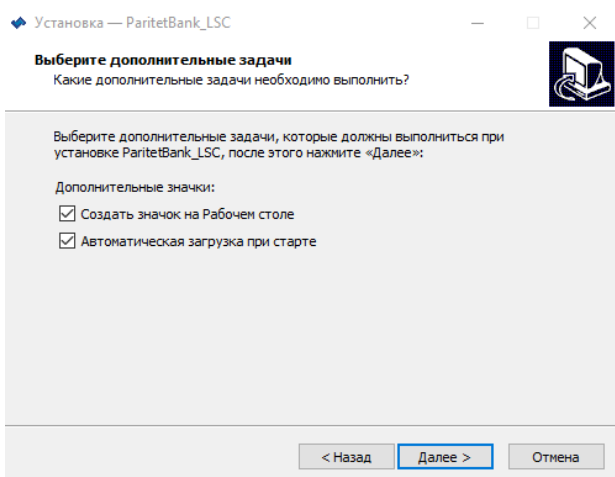


Рис. 33

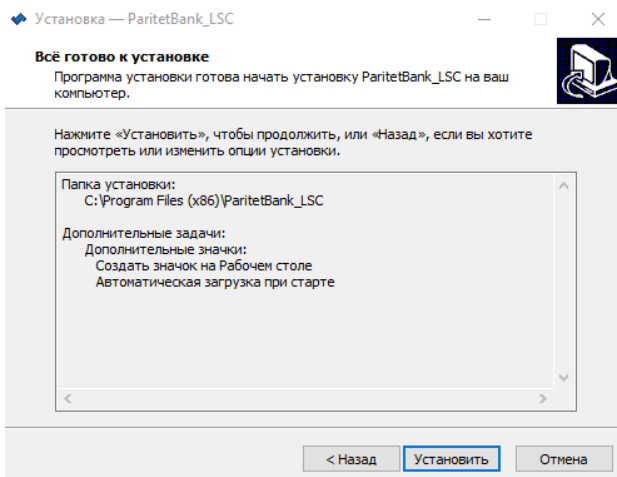


Рис. 34

Первый вход в ИК с помощью ЭЦП

При входе пользователя с помощью ЭЦП необходимо установить НКИ в порт USB и запустить Подсистему ИК. Далее на стартовой странице ИК нажать на кнопку «ВОЙТИ С ПОМОЩЬЮ ЭЦП» (см. Рис. 35).

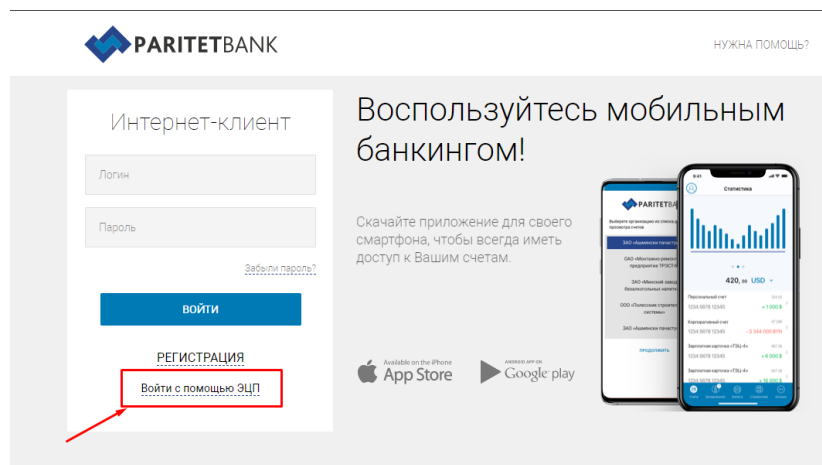


Рис. 35

Необходимо ввести пароль на ключ и нажать на кнопку «ОК» (Рис. 36).

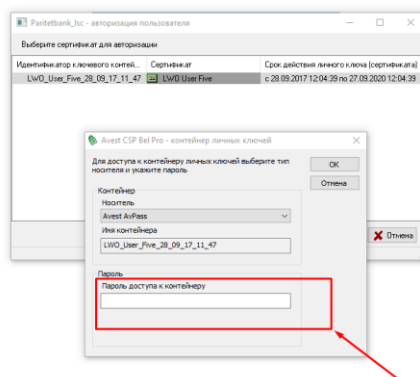


Рис. 36

Вам будет предложено сменить пароль (Рис. 37).

Имя пользователя – логин присваивается банком и уже указан на странице.

ВАЖНО! Обязательно зафиксируйте себе данный логин.

Старый пароль - это технический пароль, при первом входе Aa12345678 (латинские буквы). Новый пароль задается согласно правилам, указанным справа.

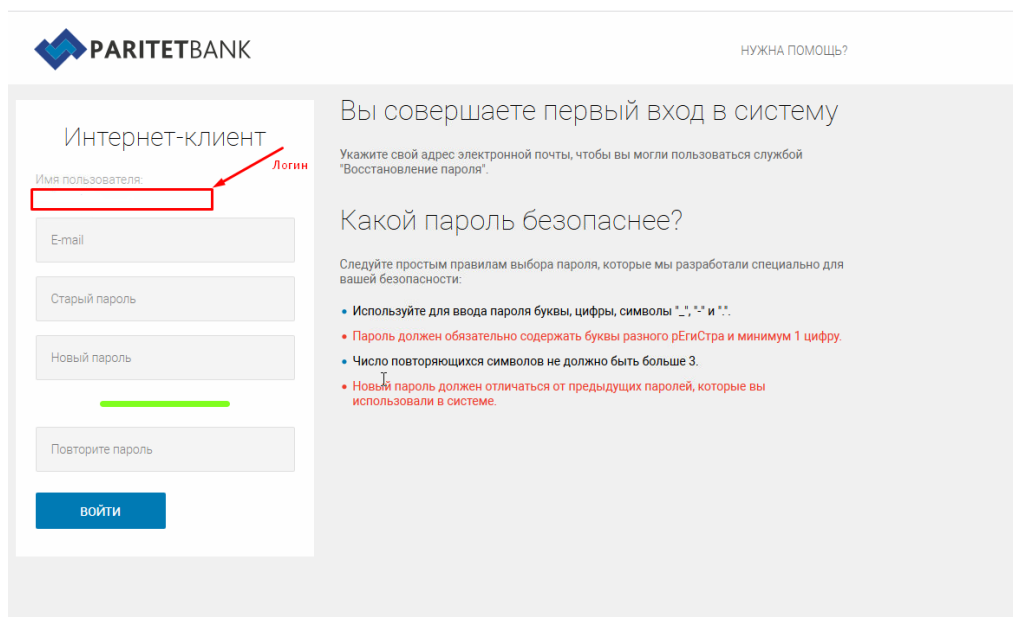


Рис. 37

При правильной авторизации отображается корпоративная страница раздела «Счета» (Рис. 38).

С дальнейшими действиями можно ознакомиться в ["Руководстве пользователя"](#).

Счета

- Бронирование
- Картотека
- Импорт документов
- Выписка по всем счетам
- Документы
- Подтверждение остатков
- Управление зарплатным проектом
- Онлайн-заявки
- Торговая площадка
- Эквайринг
- Cash Pooling
- Справочники
- Курсы валют
- Шаблоны
- Переписка
- Документы клиента

Сменить

Список счетов

^Текущий (расчетный)

Дата последней операции
Номер счета
Остаток на счете
Валюта счета

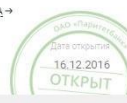
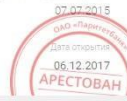

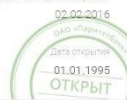
Текущий (расчетный)			
Открыт	0.00 EUR	Выписка →	
+ ДОКУМЕНТ	Код банка: BARBVY2X	Ставка: 0%	
Арестован	1.00 BYN	Выписка →	
+ ДОКУМЕНТ	Код банка: BARBVY2X	Ставка: 0%	
Арестован	0.00 USD	Выписка →	
+ ДОКУМЕНТ	Код банка: BARBVY2X	Ставка: 0%	
Открыт	0.00 BYN	Выписка →	
+ ДОКУМЕНТ	Код банка: BARBVY2X	Ставка: 0%	

Рис. 38