ЭКСПЕРТНОЕ АГЕНТСТВО
ВИТТА

тел. (812) 9292574, (812) 9292547, www.vittaspb.ru, e-mail: vitta.spb@mail.ru,
191025, Санкт-Петербург, Невский пр. д55, Лит.А., 3 этаж.

ЗАКЛЮЧЕНИЕ СПЕЦИАЛИСТА
№037-13
Компьютерно – техническое исследование

Исполнитель **ООО «Экспертное агентство «ВИТТА»**

Санкт-Петербург 2013 г.

ЭКСПЕРТНОЕ АГЕНТСТВО
ВИТТА

тел. (812) 9292574, (812)9292547, www.vittaspb.ru, e-mail: vitta.spb@mail.ru,
191025, Санкт-Петербург, Невский пр. д.55, Лит.А., 3 этаж.

Производство заключения начато в 11 ч.00 мин. 06.06.2013 г.
окончено в 15 ч.00 мин. 13.06.2013 г

ЗАКЛЮЧЕНИЕ СПЕЦИАЛИСТА

№037-13 **от «13» июня 2013г.**

Специалист ООО «Экспертное агентство «ВИТТА» ПОСТОВАЛОВ Иван Вадимович, имеющий высшее механико-математическое образование, (диплом Бакалавра математики и механики №ВБА 0204940 от 06.06.2007г., выданный Государственной аттестационной комиссией Санкт-Петербургского государственного университета, диплом Магистра математики и механики №ВМА 0077004 от 02.06.2009г., выданный Государственной аттестационной комиссией Санкт-Петербургского государственного университета) стаж экспертной работы с 2007 года, на основании договора №06/06/13-38 от «06» июня 2013 года, произвел компьютерно-техническое исследование.

НА ИССЛЕДОВАНИЕ ПРЕДСТАВЛЕНО:

1. Прибор ПРЭМ, зарегистрирован в Государственном реестре средств измерений РФ под № 17858-11, серийный номер №495595, документы прилагаются
2. Адаптер USB–COM Gembird UAS111 http://gmb-online.nl/item.aspx?id=1326
3. USB ключ, переданный руководством ЗАО «Взлет» для проведения экспертизы
4. ПО Pult01-P, находилось в свободном доступе до 2007 года
5. ПО Pult01 Архив, передано в ООО «СКБ Взлет» [redacted]
6. ПО «**pultkey»,** ПО разработки ООО «СКБ Взлет» для работы с USB ключами фирмы Алладин, передано на экспертизу с исходными кодами для анализа.

ПЕРЕД СПЕЦИАЛИСТОМ ПОСТАВЛЕНЫ ВОПРОСЫ:

1. «Имеется ли в приборе ПРЭМ, фирмы «Теплоком», недокументированная возможность (НДВ), позволяющая переводить прибор в режим доступа, превышающий описанный в технической документации»?

2. «Имеется ли возможность в режиме НДВ изменять защищенные параметры прибора, в частности, калибровочные коэффициенты без фиксации проведенных изменений в архиве событий прибора ПРЭМ»?

При производстве исследования использовалось следующее оборудование:

- Цифровая фотокамера SONY DSC-H5;
- Компьютер "SONY VPCF13S1R" с программным обеспечением "Windows 7", текстовым редактором "Microsoft Office Word 2007";
- Многофункциональное устройство "Epson Stylus TX550W".

ИССЛЕДОВАНИЕ

Объекты поступили на исследование без упаковки (см. иллюстрацию №1 в таблице иллюстраций к заключению специалиста №037-13 от 13.06.2013г.).

Преобразователь расхода электромагнитный ПРЭМ поступил на исследование в заводской таре – картонной коробке. Коробка не опечатана (см. иллюстрацию №2 в таблице иллюстраций к заключению специалиста №037-13 от 13.06.2013г.)

При вскрытии коробки из нее извлечены (см. иллюстрацию №3):

1. Преобразователь расхода электромагнитный ПРЭМ серийный номер №495595, номер версии ПО «21»;
2. Паспорт;
3. Инструкция по монтажу;
4. Руководство по эксплуатации;
5. Акт рекламации;
6. Прокладки – 2 шт.
7. Блок питания;
8. Клеммник – розетка.

Преобразователь расхода электромагнитный ПРЭМ осмотрен специалистом.

Следов эксплуатации и внешних повреждений не имеет. Заводской номер ПРЭМ указан на шильде корпуса – 495595 (см. иллюстрацию №4). Совпадает с номером, указанным в Паспорте и на наклейке заводской тары.

Для дальнейшего исследования Специалистом снята лицевая панель измерительного блока (см. иллюстрации №5, №6, №7).

Описание ключей eToken

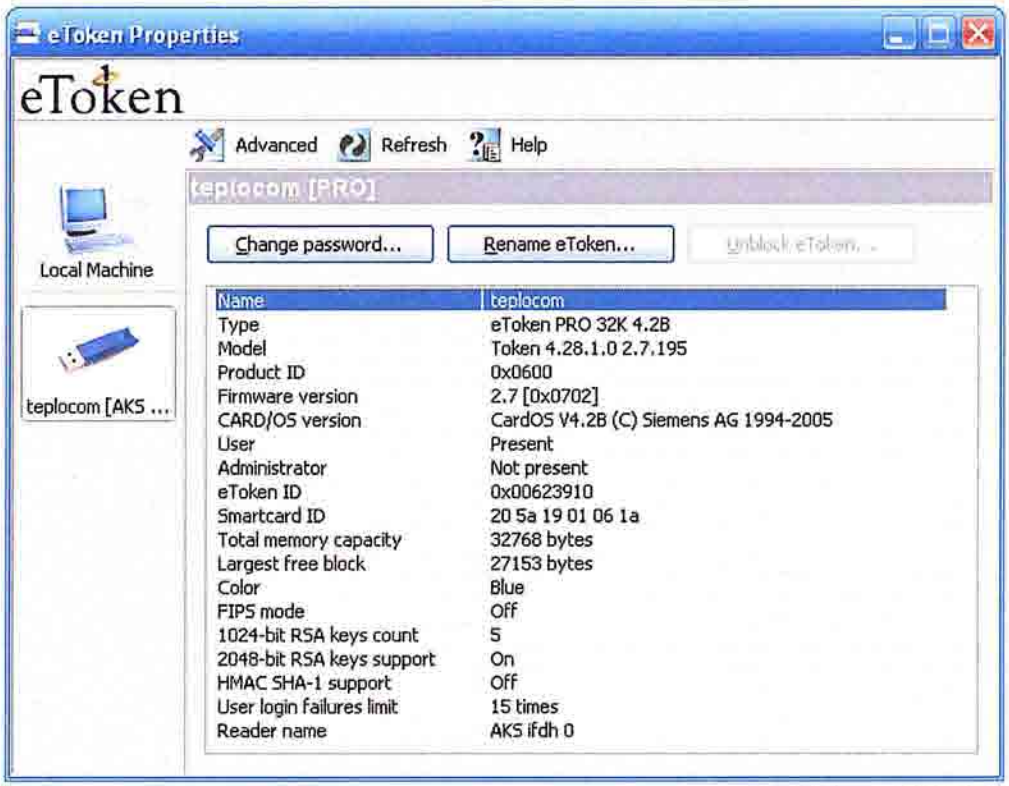
Электронные USB-ключи и смарт-карты eToken представляют собой компактные устройства, предназначенные для обеспечения информационной безопасности корпоративных заказчиков и частных пользователей. Данные **USB-ключи производятся компанией** «Аладдин Р.Д.» – ведущим российским

разработчиком и поставщиком средств аутентификации, продуктов и решений для обеспечения информационной безопасности и защиты конфиденциальных данных.

USB-ключи и смарт-карты eToken «базируются на высокозащищенной платформе, разработанной для производства смарт-карт — области, в которой традиционно предъявляют повышенные требования к информационной безопасности. Поэтому **USB-ключи eToken** фактически являются миниатюрным компьютером, обеспечивающим безопасное хранение Ваших персональных данных и надежно защищенным от несанкционированного вмешательства. Данные ключи обладают функциями смарт-карт: одно- и двухфакторная аутентификация пользователей, хранение ключевой информации и проведение криптографических операций в доверенной среде. В ключах аппаратно реализованы алгоритмы шифрования: RSA 1024 / 2048, DES, 3DES, SHA-1. Поддерживаются следующие интерфейсы и стандарты: PKCS#11 версии 2.01, Microsoft CryptoAPI, PC/SC, Сертификаты X.509 v3, SSL v3, IPSec/IKE, Microsoft CCID».

http://www.aladdin-rd.ru/catalog/etoken/

http://www.aladdin-rd.ru/catalog/etoken/java/ details.php?sphrase_id=131629



Информация о ключе, предоставляемая программой eToken PKI Client (http://www.aladdin-rd.ru/support/downloads/27418/)

Краткое описание прибора ПРЭМ

ПРЭМ – преобразователи расхода электромагнитные, производства компании Теплоком. Преобразователи предназначены для измерений и преобразований в выходные электрические сигналы объемного расхода и объема электропроводящих

жидкостей. Преобразователи могут быть применены для контроля и учета, в том числе при учетно-расчетных операциях, объемного расхода и объема жидкостей на объектах теплоэнергетического комплекса, на промышленных предприятиях и в жилищно-коммунальном хозяйстве. (Руководство по эксплуатации ПРЭМ стр.3 http://www.teplocom.spb.ru/upload/iblock/968/PREM_operating_manual_v5.14.pdf).

Система безопасности ПРЭМ. Для предотвращения несанкционированного вмешательства в работу ПРЭМ существует три уровня защиты, которые блокируют:

- изменение метрологических характеристик;
- внесение изменений в электронный модуль;
- отключение соединительных линий и демонтаж преобразователя.

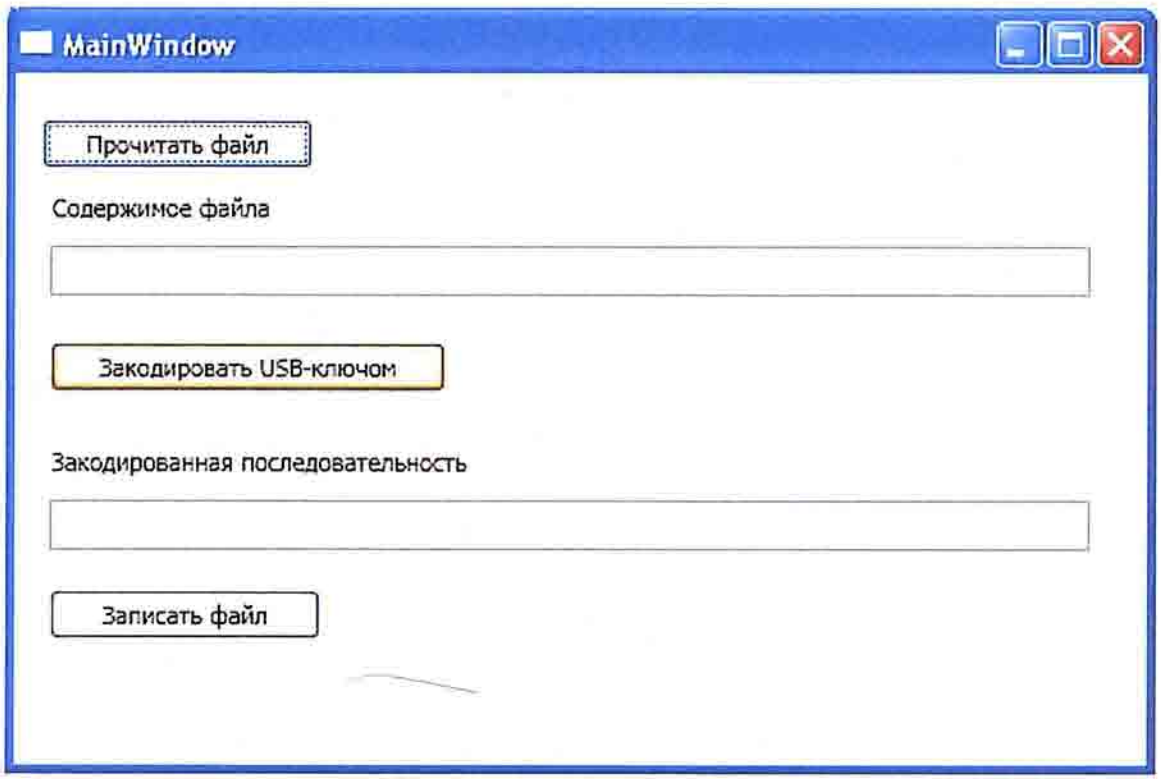
Защита от внесения изменений в электронный модуль ПРЭМ выполняется нанесением оттиска клейма изготовителя и клейма госповерителя на мастике в чашке. Возможность отключения соединительных линий обеспечивается пломбированием ПРЭМ навесной пломбой инспектора теплоснабжающей организации. Возможность демонтажа ПРЭМ обеспечивается пломбированием крепежных элементов преобразователя навесной пломбой инспектора теплоснабжающей организации.

В ПРЭМ имеется независимый архив диагностируемых событий, в котором отражаются все изменения, внесенные в ПО и параметры настройки. Просмотр параметров настройки, а также версии и цифрового идентификатора ПО, возможен с помощью программы «PULT 01» или PULT-01(Service). Просмотр архива событий возможен с помощью программы «Pult 01 Архив».
(Руководство по эксплуатации ПРЭМ стр.10)
http://www.teplocom.spb.ru/upload/iblock/968/PREM_operating_manual_v5.14.pdf).

Описание и алгоритм работы программы «pultkey»

Программное обеспечение «pultkey» предназначено для работы с USB ключами фирмы Алладин, ПО использует в своей работе стандартную библиотеку, предоставляемую данной компанией.

Программное обеспечение «pultkey» выполняет шифрование случайной цифровой байтовой последовательности, передаваемой в USB ключ, алгоритмами и методами, примененными непосредственно в ключе. ПО «pultkey» не вносит дополнительных преобразований в методы шифрования, выполняемые ключом фирмы Алладин.



Главное окно программы

Программа может работать как на одном ПК с Pult01-P, так и на любом другом ПК, никак физически не связанным с прибором ПРЭМ и Pult01-P (байтовые последовательности в этом случае можно передавать с компьютера на компьютер устным способом, по сети или с помощью сменных носителей). Таким образом можно гарантировать полную изоляцию USB-ключа от прибора ПРЭМ и программы Pult01-P.

Весь процесс состоит из трёх последовательных этапов:

Считывание байтовой последовательности, полученной из прибора посредством программы Pult01-P. Кнопка «Прочитать файл»

Шифрование байтовой последовательности (полученной из этапа 1) посредством USB-ключа eToken. Кнопка «Закодировать USB-ключом».

Запись зашифрованной байтовой последовательности (полученной из этапа 2) в файл. Кнопка «Записать файл»

На этапе 1 вызывается диалоговое окно выбора входного файла, после чего содержимое выбранного файла сохраняется в байтовый массив inputBytes и выводится на визуальную форму с помощью метода bytesToHex.

На этапе 2 происходит шифрование массива inputBytes (используется метод encodeByETоken) с сохранением результата в массив encodedBytes и выводом его на визуальную форму с помощью метода bytesToHex. Порядок работы с библиотекой etoken.dll в методе encodeByEToken:

etInitialize (инициализация работы с библиотекой eToken.dll)

etCreateTalker (создаёт и возвращает объект talker – необходим для последующей работы. В качестве первого параметра lpszReaderName используется строка “AKS ifdh 0”)

etLockReader (блокирует работу USB-ключа для предотвращения доступа к нему из других потоков/процессов)

os4ApduMSERestore (подгружает криптографическую среду, находящуюся в ключе под номером 0xDD)

os4ApduPSOEnc (осуществляет непосредственное шифрование байтовой последовательности)

etUnlockReader (снимает полученную ранее блокировку USB-ключа)

etDestroyTalker (освобождает созданный ранее объект talker)

etFinalize (завершение работы с библиотекой)

На этапе 3 вызывается диалоговое окно выбора выходного файла, после чего содержимое массива encodedBytes сохраняется в выбранном файле (с перезаписью).

Сборка программы pultkey

Вместе с проектом программы идёт библиотека etoken.dll, идущая в пакете RTE_3.66.msi (библиотека инсталлируется в папку %Windows%\System32). Проект настроен на Net Framework 4.0, но можно перенастроить и на 3.0, 3.5. Собирается через файл решения «pultkey.sln» без дополнительной настройки.

Для показа формы используется технология WPF. Весь рабочий код находится в MainWindow.xaml.cs. Для вызова процедур библиотеки eToken.dll используется DllImport и маршаллинг параметров. Весь процесс работы с USB-ключом располагается в методе usbKeyEncode. Все используемые функции библиотеки etoken.dll подробно описаны в вышеуказанном Developers Guide. Метод bytesToHex используется только для отображения байтовых последовательностей на форме.

Исходные коды ПО «pultkey» проанализированы специалистом, выполнена компиляция проекта ПО «pultkey».

ПО «pultkey» не содержит алгоритмов и методов с признаками вредоносного программного обеспечения.

В ходе исследования использовано ПО «pultkey», скомпилированное непосредственно специалистом.

Для проведения исследования представлены исходные коды ПО pultkey.

```
using System;
using System.Text;
using System.Windows;
using Microsoft.Win32;
using System.IO;
using System.Runtime.InteropServices;

namespace pultkey
{
  /// <summary>
  /// Логика взаимодействия для MainWindow.xaml
  /// </summary>
  public partial class MainWindow : Window
  {
    // считанный из файла байты
    byte[] inputBytes = new byte[] {};
    // байты, закодированные с помощью USB-ключа
    byte[] encodedBytes = new byte[] { };

    [DllImport("eToken.dll")]
    public static extern uint etCreateTalker(String lpszReaderName, out uint phTalker, uint
dwFlags);

    [DllImport("eToken.dll")]
    public static extern uint etDestroyTalker(uint hTalker);

    [DllImport("eToken.dll")]
    public static extern uint etInitialize(IntPtr lpReserved);

    [DllImport("eToken.dll")]
    public static extern uint etFinalize();

    [DllImport("eToken.dll")]
    public static extern uint etLockReader(uint hTalker);

    [DllImport("eToken.dll")]
    public static extern uint etUnlockReader(uint hTalker);
```

```
[DllImport("eToken.dll")]
public static extern uint etStartListen(IntPtr hDest, uint dwType, IntPtr lpEt, uint dwFlags);

[DllImport("eToken.dll")]
public static extern uint os4ApduMSERestore(uint hTalker, byte nObjectId);

[DllImport("eToken.dll")]
public static extern uint os4ApduPSOEnc(uint hTalker, IntPtr lpData, byte cbData, ref IntPtr
ppReply, ref byte lpcbReply, ref byte lpnPadding);

/// <summary>
/// Возвращает шестнадцатеричное представление байтового массива
/// </summary>
/// <param name="bytes"></param>
/// <returns></returns>
static string bytesToHex(byte[] bytes)
{
  StringBuilder stringBuilder = new StringBuilder(bytes.Length * 2);

  foreach (byte b in bytes)
    stringBuilder.Append(Convert.ToString(b, 16).PadLeft(2, '0').ToUpper());

  return stringBuilder.ToString();
}

public MainWindow()
{
  InitializeComponent();
}
/// <summary>
/// Вызывает диалоговое окно выбора входного файла. Читает содержимое файла в
массив inputBytes
/// </summary>
private void bReadFile_Click(object sender, RoutedEventArgs e)
{
  OpenFileDialog dialog = new OpenFileDialog();
  if (dialog.ShowDialog() == true)
  {
    inputBytes = File.ReadAllBytes(dialog.FileName);

    tbInput.Text = bytesToHex(inputBytes);
  }
```

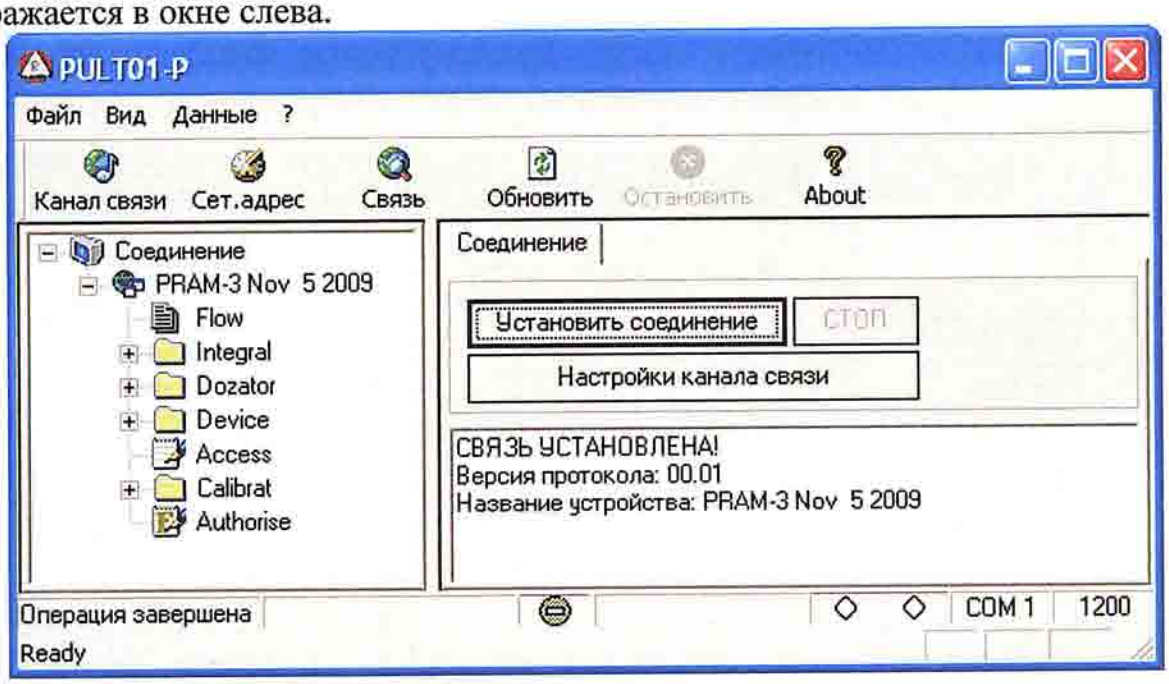
```
}

byte[] encodeByEToken(byte[] bytes)
{
  if (etInitialize(new IntPtr(0)) != 0)
    throw new Exception("eToken error");

  try
  {
    uint talker = 0;
    uint result = etCreateTalker("AKS ifdh 0", out talker, 0);

    if (result != 0)
      throw new Exception("eToken error");

    try
    {
      if (etLockReader(talker) != 0)
        throw new Exception("eToken error");
      try
      {
        if (os4ApduMSERestore(talker, 0xDD) != 0)
          throw new Exception("eToken error");

        IntPtr outBytesPtr = new IntPtr();
        byte outLength = 0;
        byte outPadding = 0;

        IntPtr bytesPtr = Marshal.AllocHGlobal(bytes.Length);
        try
        {
          Marshal.Copy(bytes, 0, bytesPtr, bytes.Length);

          if (os4ApduPSOEnc(talker, bytesPtr, (byte)bytes.Length, ref outBytesPtr, ref
outLength, ref outPadding) != 0)
            throw new Exception("eToken error");

          byte[] outBytes = new byte[outLength];

          Marshal.Copy(outBytesPtr, outBytes, 0, outBytes.Length);

          if (outBytes.Length > bytes.Length)
```

```
                Array.Resize(ref outBytes, bytes.Length);

              if (outBytes.Length != bytes.Length)
                throw new Exception("eToken error");

              return outBytes;
            }
            finally
            {
              Marshal.FreeHGlobal(bytesPtr);
            }
          }
          finally
          {
            if (etUnlockReader(talker) != 0)
              throw new Exception("eToken error");
          }
        }
        finally
        {
          etDestroyTalker(talker);
        }
      }
      finally
      {
        etFinalize();
      }
    }
    /// <summary>
    /// Кодирует массив inputBytes в encodedBytes с помощью USB-ключа
    /// </summary>
    private void bEncode_Click(object sender, RoutedEventArgs e)
    {
      try
      {
        encodedBytes = encodeByEToken(inputBytes);
      }
      catch (Exception ex)
      {
        MessageBox.Show(ex.ToString());
      }
      tbEncoded.Text = bytesToHex(encodedBytes);
```

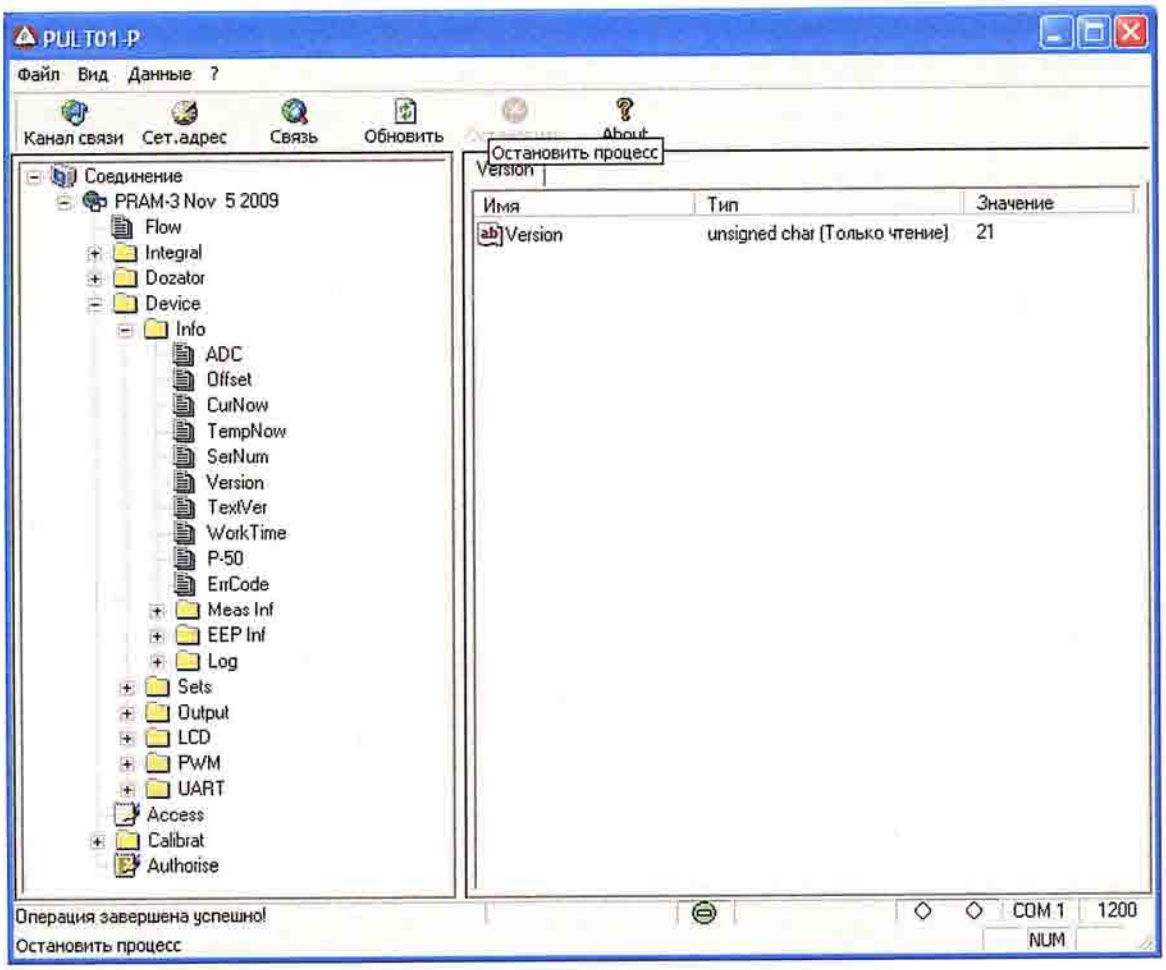
```
        }
        /// <summary>
        /// Вызывает диалоговое окно выбора выходного файла. Записывает в файл массив
    encodedBytes
        /// </summary>
        private void bWriteFile_Click(object sender, RoutedEventArgs e)
        {
          SaveFileDialog dialog = new SaveFileDialog();
          if (dialog.ShowDialog() == true)
          {
            File.Delete(dialog.FileName);
            File.WriteAllBytes(dialog.FileName, encodedBytes);
          }
        }
      }
    }
```

Авторизация с использованием ключа, переданного для исследования

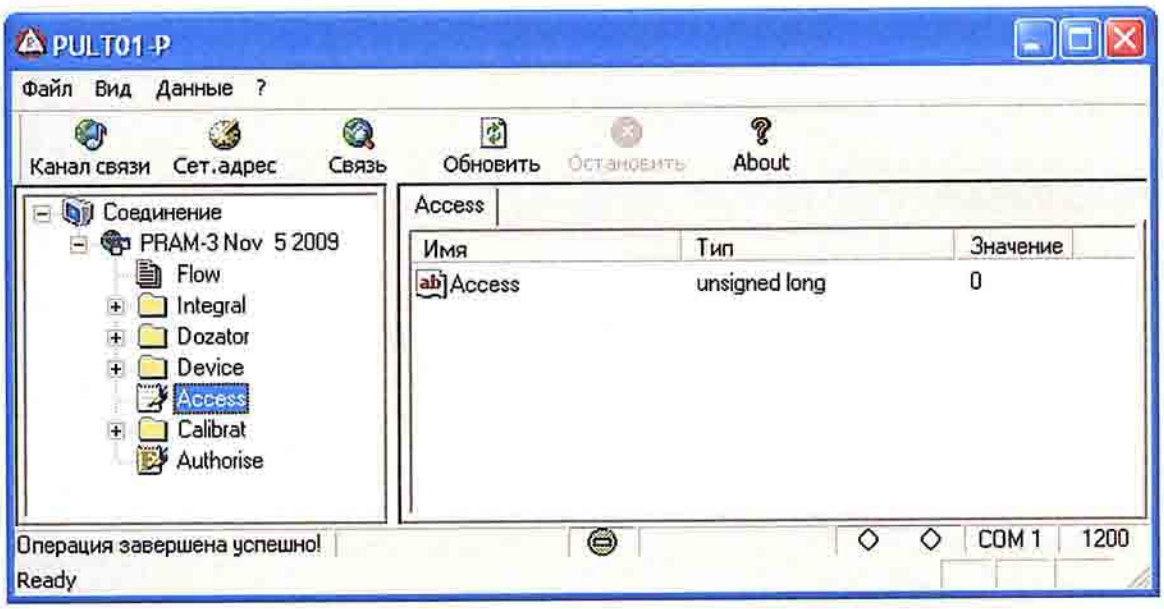
Установим в приборе ПРЭМ протокол ПРЭМ-3, установив джампер J4.
Запустим Pult01-P.
Установим связь с прибором нажатием на кнопку «Установить соединение».
После установления связи с прибора считывается дерево параметров и отображается в окне слева.



Считаем версию прибора ПРЭМ – версия ПО «21».



Прочитаем параметр уровень доступа Access (значение = 0).

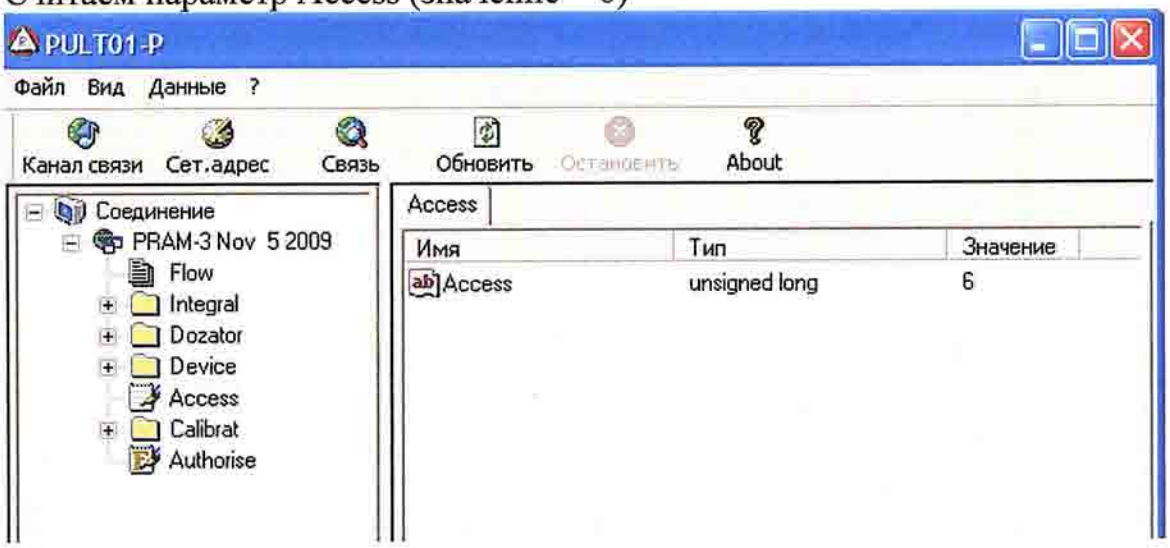


Примечание: согласно руководству по эксплуатации ПРЭМ сервисный ключ переводит прибор в уровень доступа 5. Данные получены из документации на программное обеспечение Pult01 Service, стр. 18, файл Описание программы Pult01 Service.pdf

Определим уровень доступа при нажатой кнопке «Калибровка», стр.10 Руководства по эксплуатации, файл PREM_operating_manual_v5.14

Обновим дерево параметров, нажав в верхнем меню Pult01-P кнопку «Связь» (либо просто перезапустим программу)

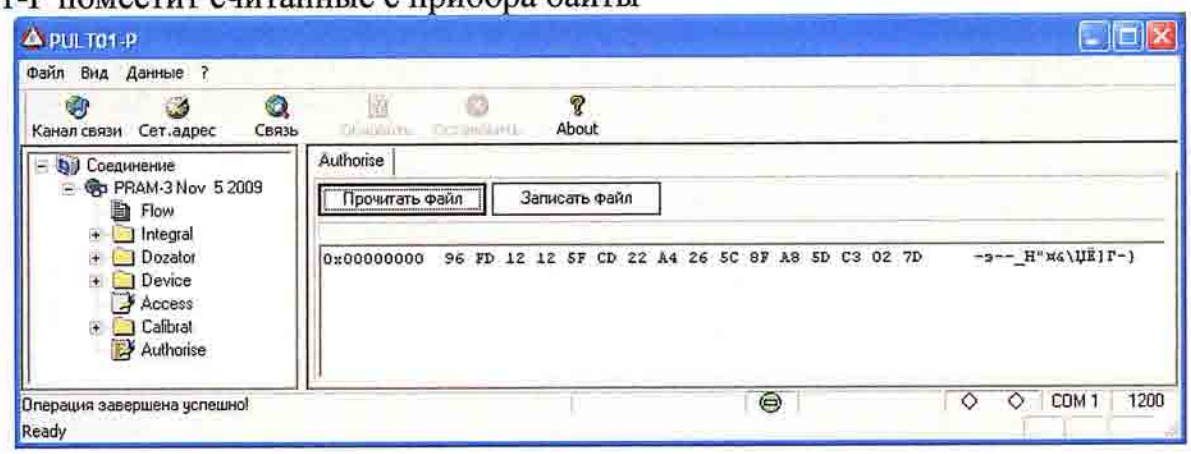
Считаем параметр Access (значение = 6)



Проверим наличие дополнительных уровней доступа в приборе ПРЭМ

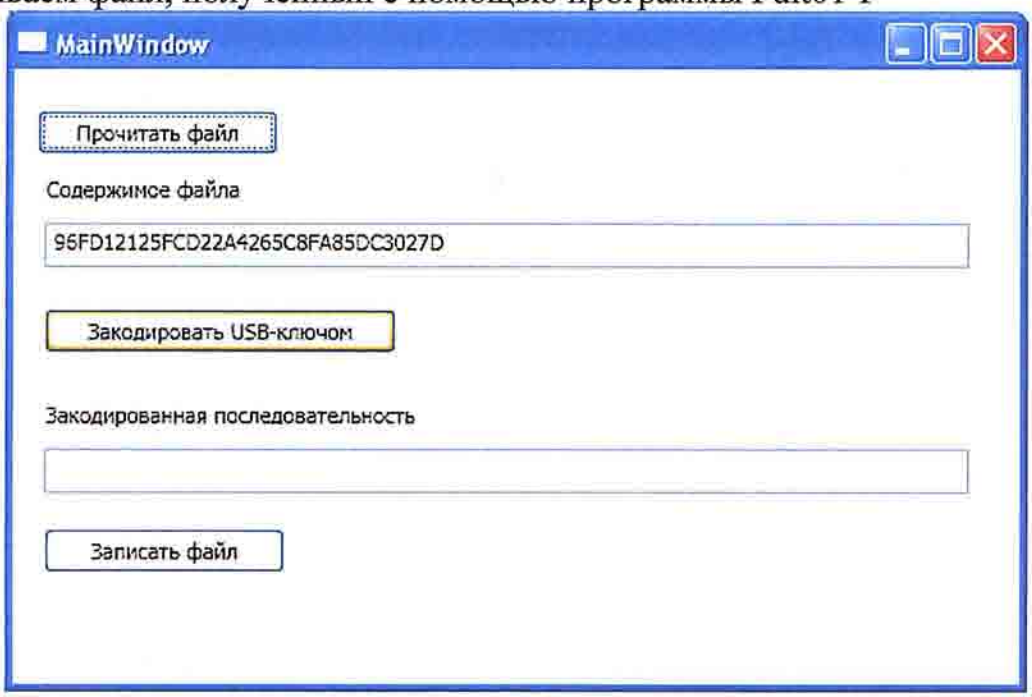
Выделяем в дереве ветку под названием «Authorize»

В окне справа нажимаем кнопку «Прочитать файл» и выбираем файл, куда Pult01-P поместит считанные с прибора байты

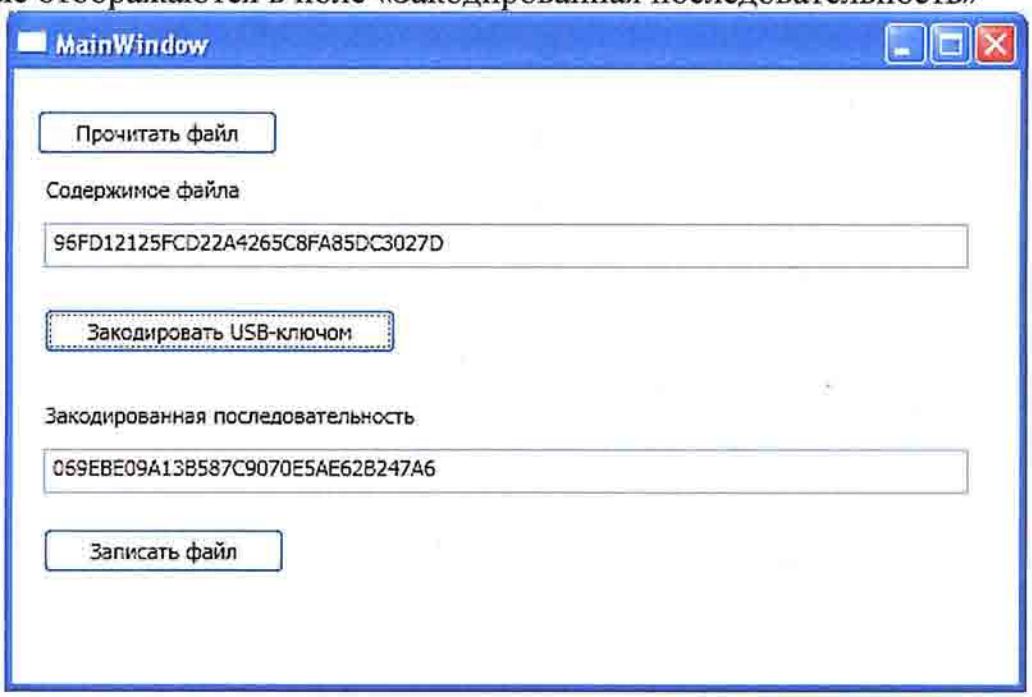


В окне отобразится считанная с прибора байтовая последовательность (16 байт), она же запишется в указанный нами файл

Запускаем программу pultkey и с помощью кнопки «Прочитать файл» указываем файл, полученный с помощью программы Pult01-P



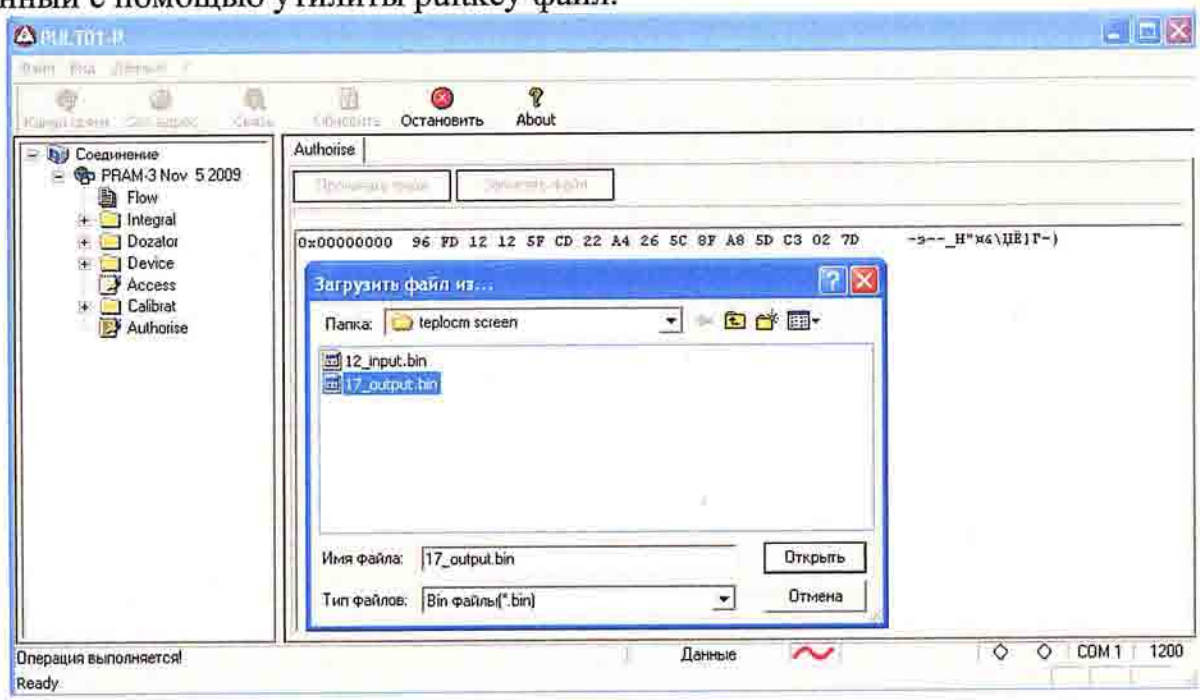
Вставляем ключ eToken в USB разъём ПК и нажимаем кнопку «Закодировать USB-ключом». При этом осуществляется передача считанной16 байтной последовательности из прибора в ключ фирмы Аладдин. Переданные из USB ключа данные отображаются в поле «Закодированная последовательность»



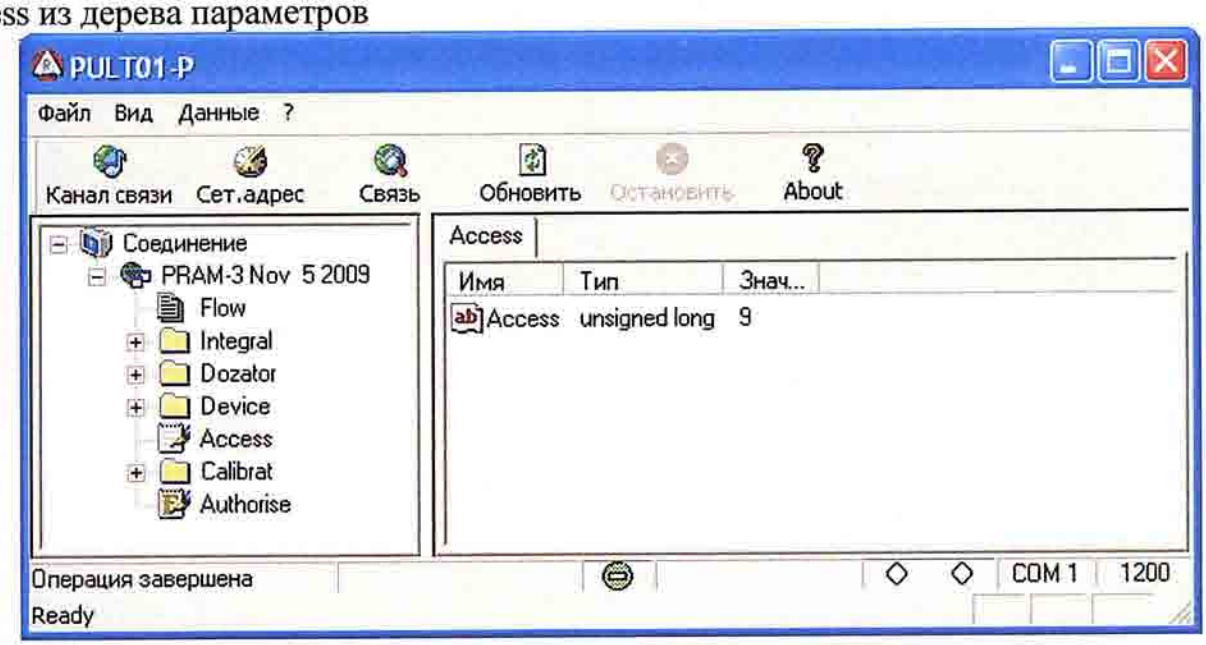
USB-ключ в ходе исследования был изъят из ПК в целях отсутствия дополнительного обмена.

Запишем закодированную последовательность (16 байт) в новый файл с помощью кнопки «Записать файл»

Осуществим запись закодированной последовательности в прибор с помощью ПО Pult01-P. Для этого нажмём в Pult01-P кнопку «Записать файл» и выберем созданный с помощью утилиты pultkey файл.



Прибор введён в режим доступа 9, о чём свидетельствует мигающий светодиод. Так же прочитать текущий уровень доступа можно, прочитав параметр Access из дерева параметров



Данное исследование свидетельствует о том, что в приборе ПРЭМ, фирмы Теплом имеется недокументированная возможность (НДВ), позволяющая переводить прибор в режим доступа, превышающий описанный в технической документации.

При использовании стандартного программного обеспечения фирмы Теплоком Pult01-P прибор может быть переведен в уровень доступа (Access = 9), не описанный в технической документации на прибор ПРЭМ.

Перевод прибора в режим уровня доступа 9 (Access = 9) был произведен без нарушения пломбы госповерителя.

Анализ уровней доступа показывает, что полученный уровень (Access =9) выше по значению, чем регламентированные в документации на прибор ПРЭМ уровни доступа:

- рабочий режим, Access = 0
- сервисный режим, Уровень доступа 5, согласно документации на ПО Pult01 Service, стр.18
- режим калибровки при нажатой кнопке аппаратного доступа, Access = 6

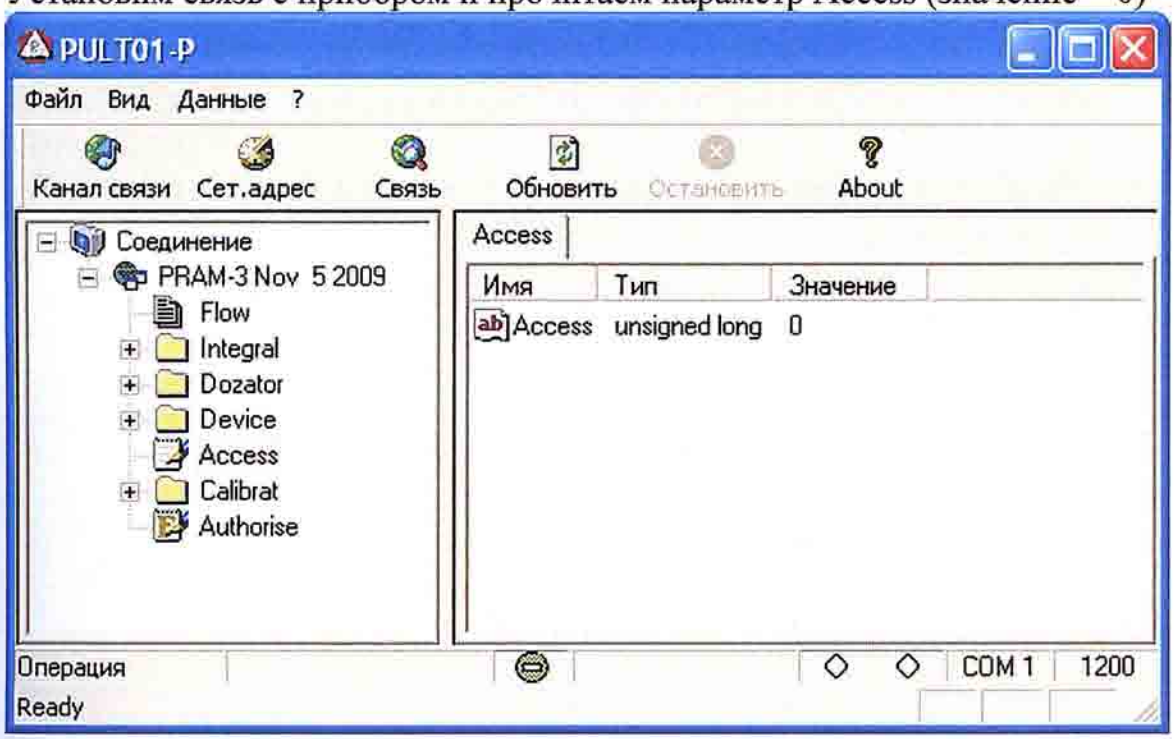
Обмен с прибором составляет 16 байт в рамках стандартного протокола обмена прибора ПРЭМ с использованием стандартного ПО Pult01-P.

Ключ фирмы Аладдин используется только для шифрования считанной из ПРЭМ последовательности в 16 байт и не участвует в активном обмене с прибором ПРЭМ. На момент записи зашифрованной ключом последовательности из 16 байт ключ был удален из ПК.

Исследование уровней доступа

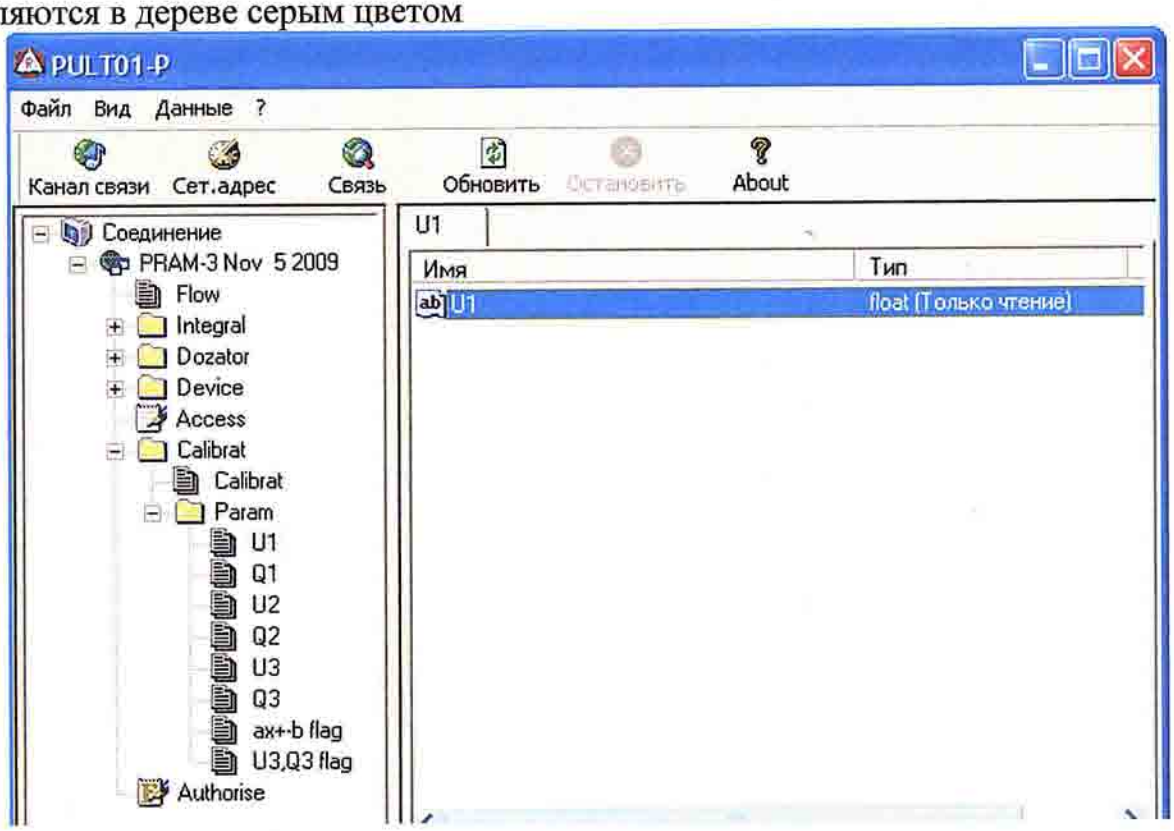
Запустим программное обеспечение Pult01-P

Установим связь с прибором и прочитаем параметр Access (значение = 0)



Примечание: согласно руководству по эксплуатации ПРЭМ сервисный ключ переводит прибор в уровень доступа 5.

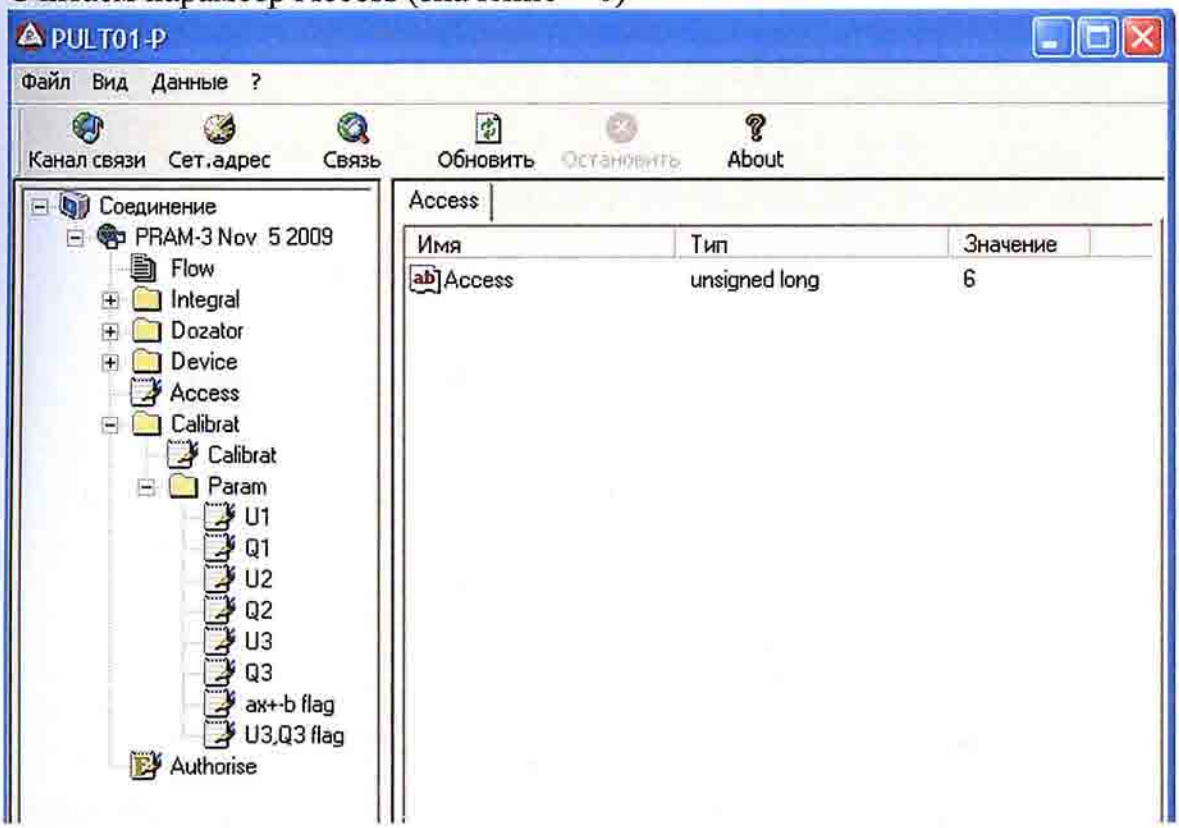
Откроем ветку Calibrat/Param и попытаемся изменить значение коэффициента U1 (правой кнопкой на строке с U1, во всплывающем меню пункт «Изменить…»). Это не получится, т.к. программа запрещает на данном уровне доступа (Access = 0) модификацию калибровочных коэффициентов. Запрещённые к записи параметры выделяются в дереве серым цветом



Нажмём на плате прибора кнопку «Калибровка» предварительно сняв пломбу (см. иллюстрацию №8)

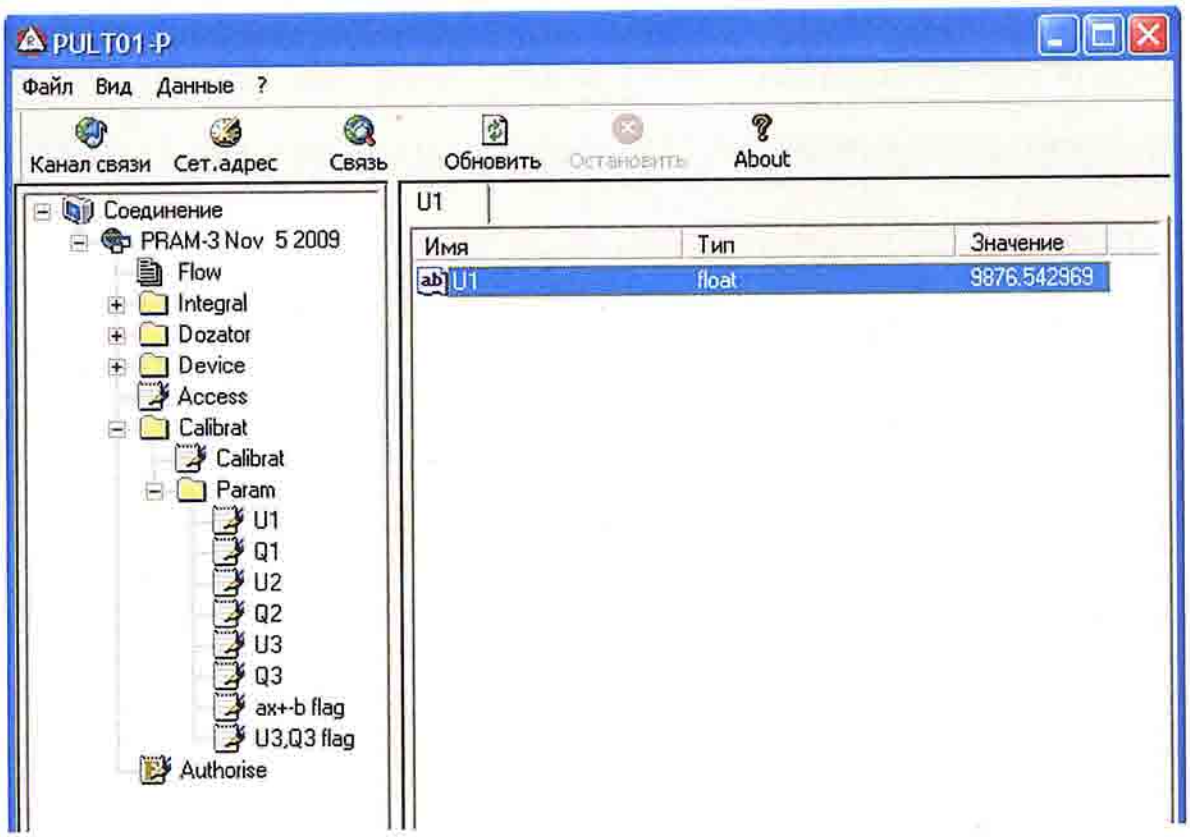
Обновим дерево параметров, нажав в верхнем меню Pult01-P кнопку «Связь» (либо просто перезапустим программу)

Считаем параметр Access (значение = 6)

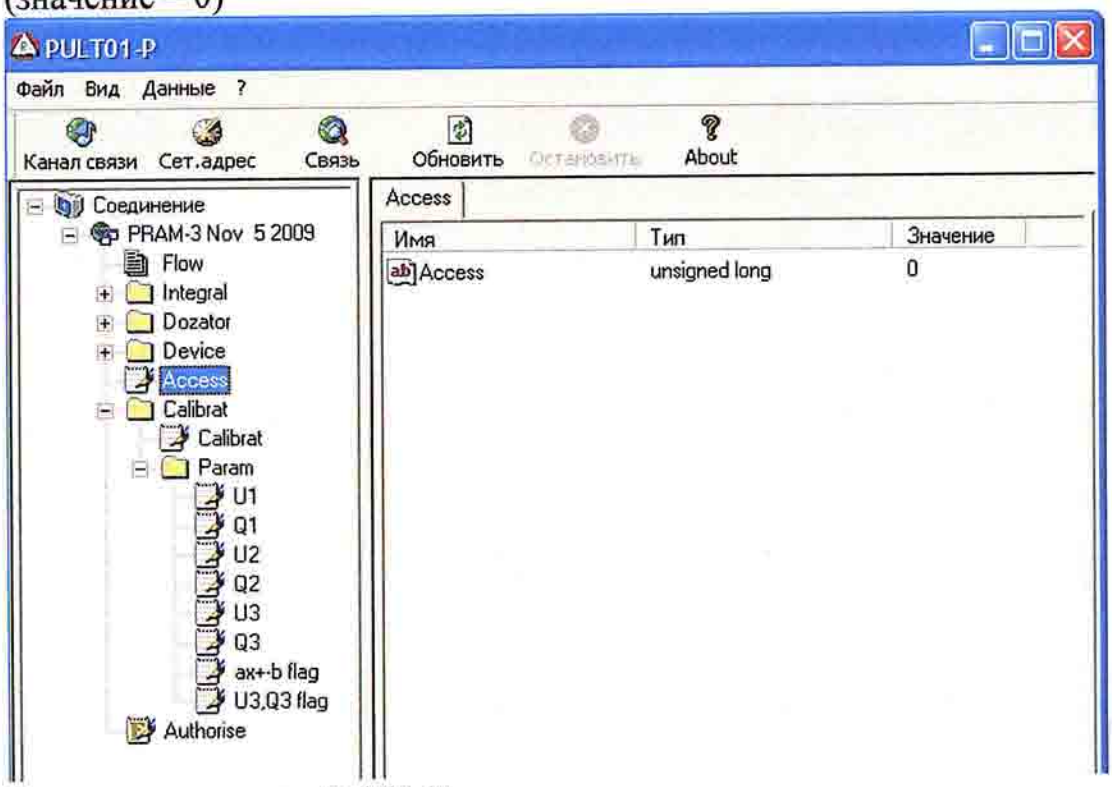


Изменим значение параметра U1

(в нашем случае текущее значение = 000.000000) на 9876.542969. Запись параметра прошла успешно.

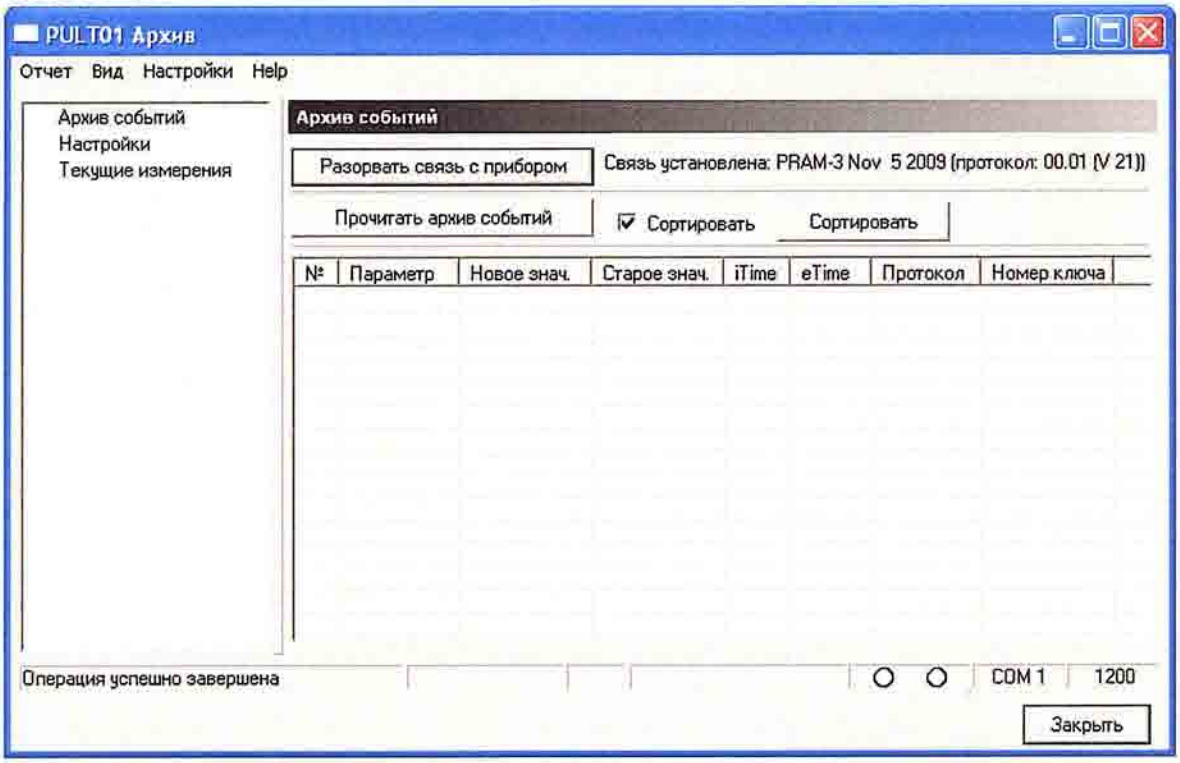


Перезагрузим прибор по питанию и считаем снова параметр Access (значение = 0)

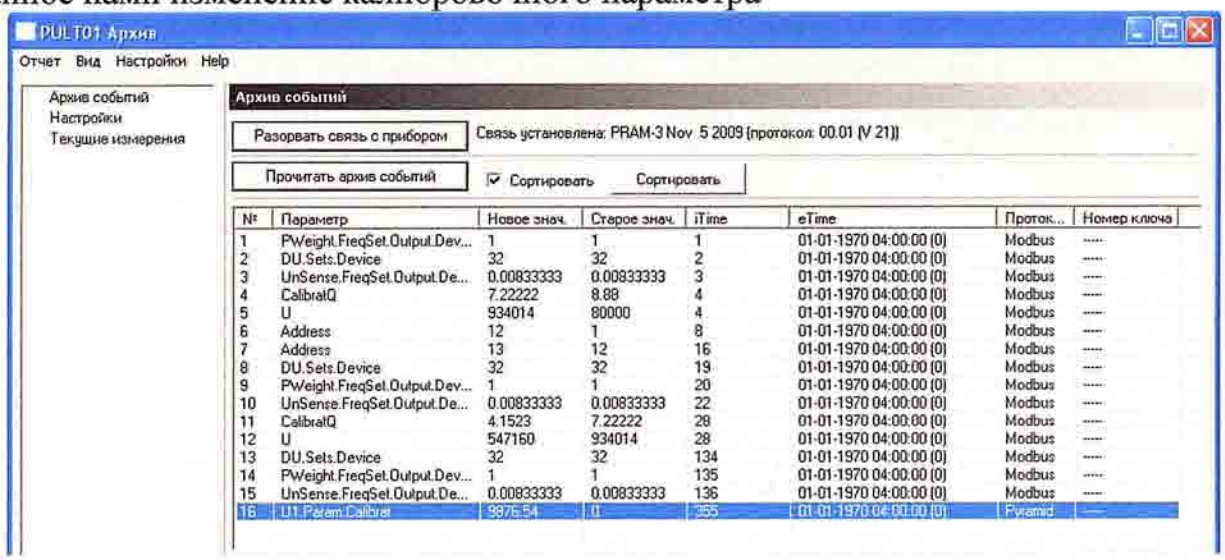


Закроем программу Pult01-P.

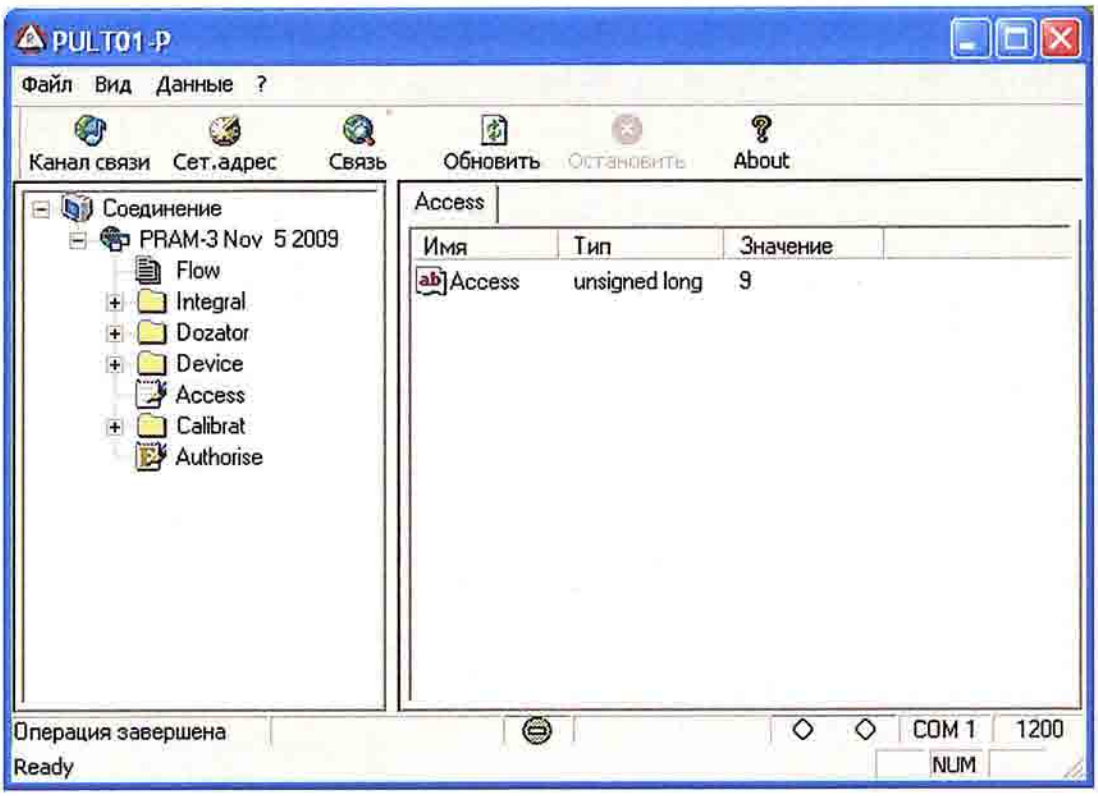
Запустим программу Pult01-Архив. Нажмём Кнопку «Установить связь». После успешной установки связи считаем архив с помощью кнопки «Прочитать архив событий»



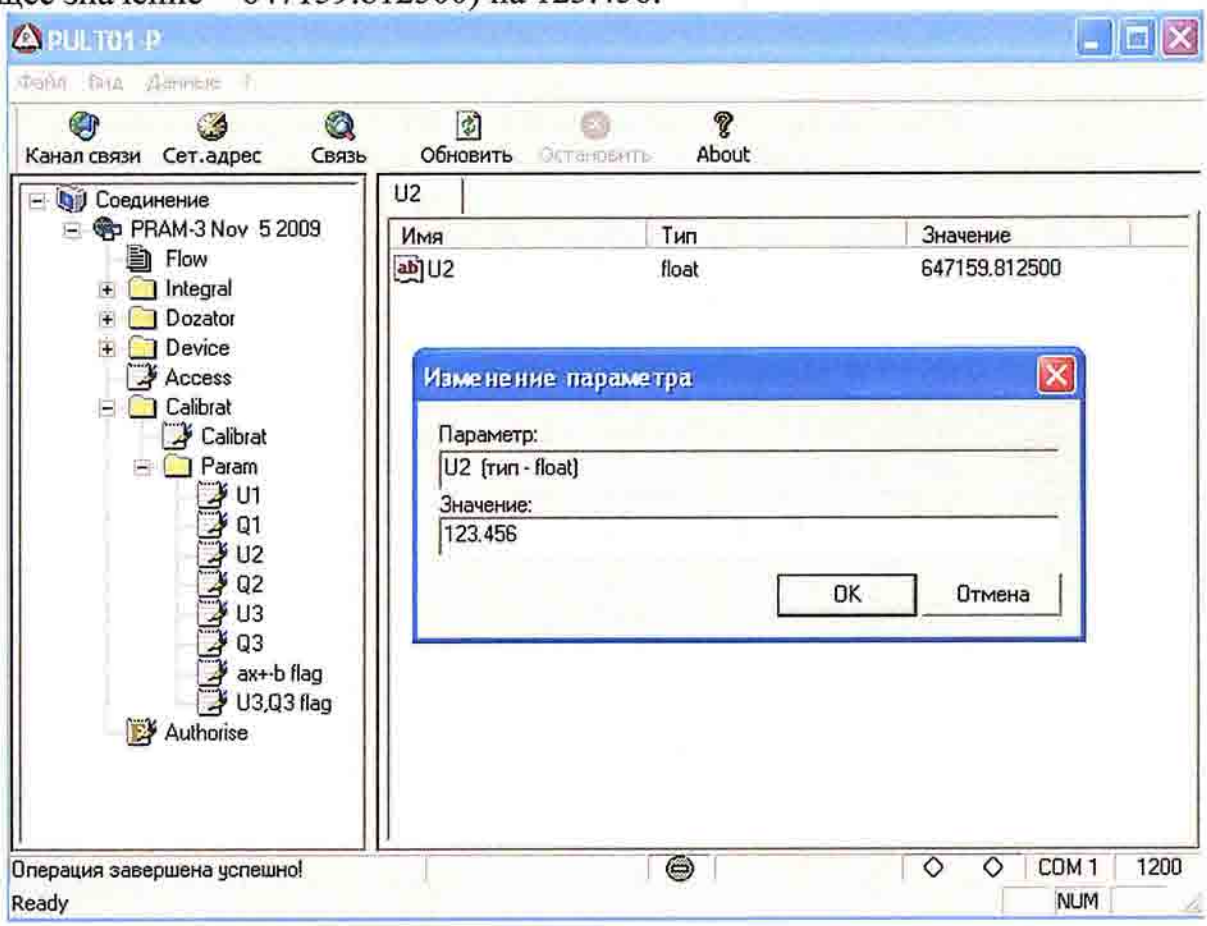
В считанном архиве (всего 16 записей), последней записью мы можем увидеть сделанное нами изменение калибровочного параметра



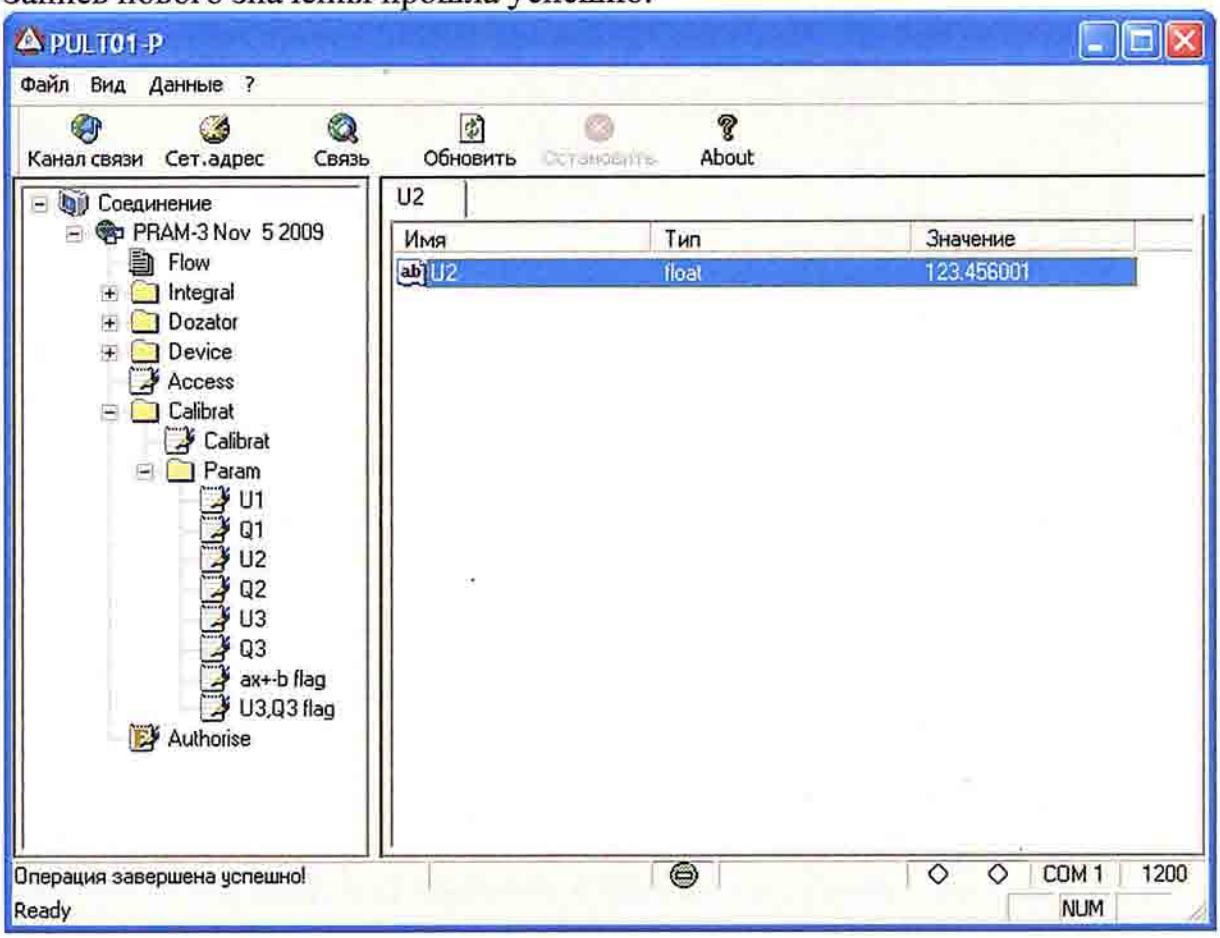
Авторизуем прибор по описанному выше алгоритму до уровня 9. Прочитаем параметр Access (значение = 9)



С помощью программы Pult01-P изменим калибровочный параметр U2 (текущее значение = 647159.812500) на 123.456.

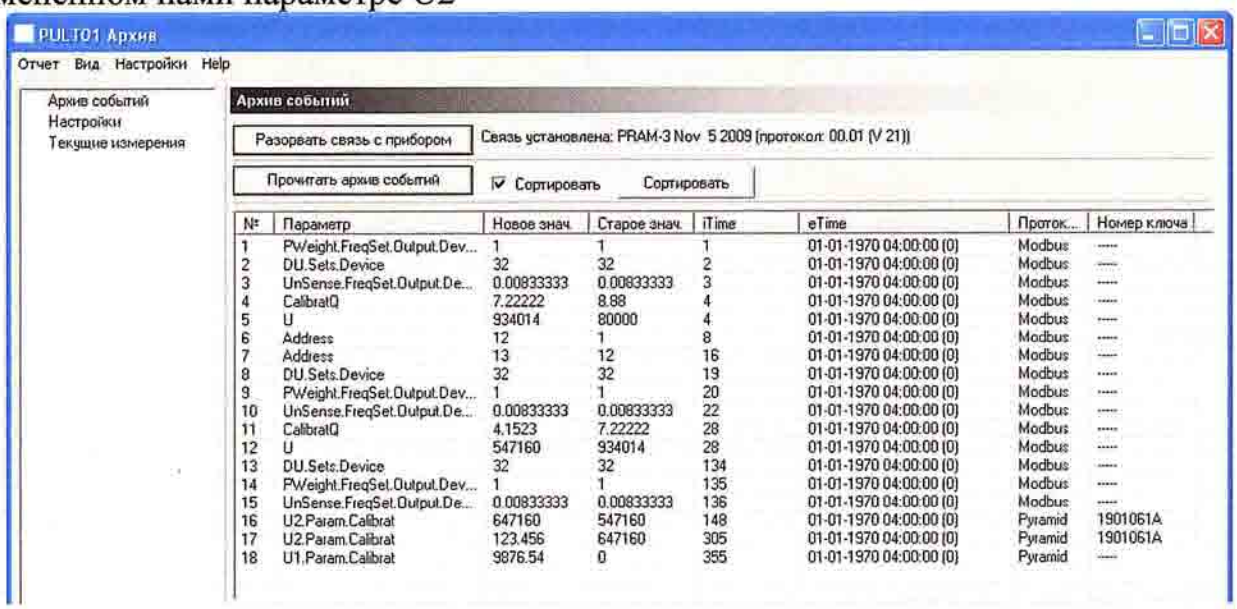


Запись нового значения прошла успешно.



С помощью программы Pult01-Архив считаем архив событий

В считанном архиве обнаружено 18 записей, под номером 17 имеется запись об изменённом нами параметре U2



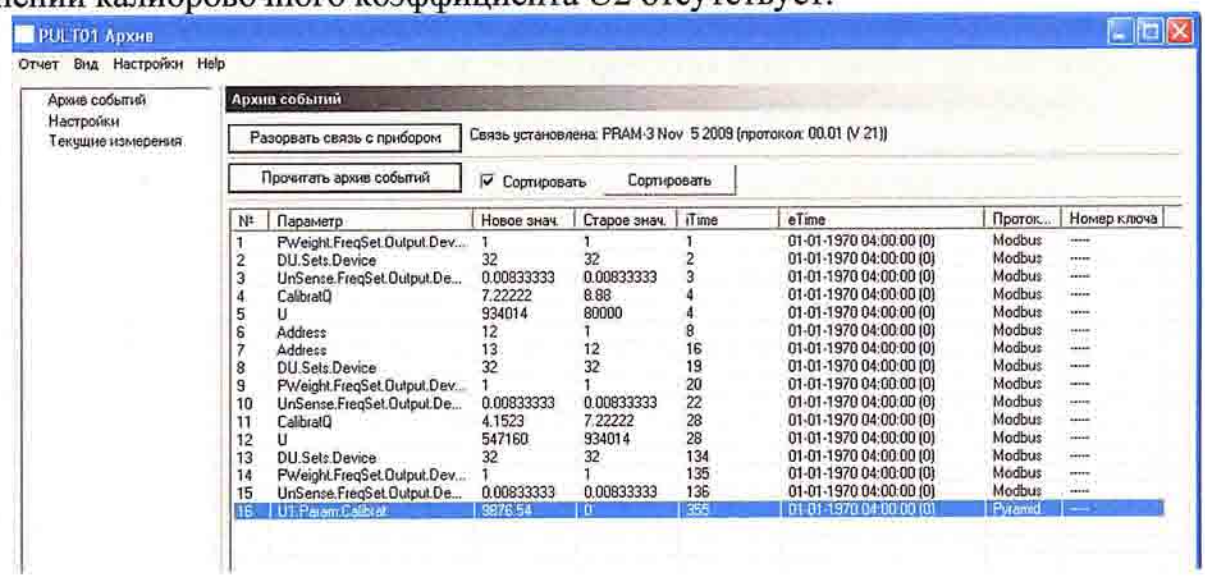
№	Параметр	Новое знач.	Старое знач.	iTime	eTime	Протак...	Номер ключа
1	PWeight.FreqSet.Output.Dev...	1	1	1	01-01-1970 04:00:00 (0)	Modbus	-----
2	DU.Sets.Device	32	32	2	01-01-1970 04:00:00 (0)	Modbus	-----
3	UnSense.FreqSet.Output.De...	0.00833333	0.00833333	3	01-01-1970 04:00:00 (0)	Modbus	-----
4	CalibratQ	7.22222	8.88	4	01-01-1970 04:00:00 (0)	Modbus	-----
5	U	934014	80000	4	01-01-1970 04:00:00 (0)	Modbus	-----
6	Address	12	1	8	01-01-1970 04:00:00 (0)	Modbus	-----
7	Address	13	12	16	01-01-1970 04:00:00 (0)	Modbus	-----
8	DU.Sets.Device	32	32	19	01-01-1970 04:00:00 (0)	Modbus	-----
9	PWeight.FreqSet.Output.Dev...	1	1	20	01-01-1970 04:00:00 (0)	Modbus	-----
10	UnSense.FreqSet.Output.De...	0.00833333	0.00833333	22	01-01-1970 04:00:00 (0)	Modbus	-----
11	CalibratQ	4.1523	7.22222	28	01-01-1970 04:00:00 (0)	Modbus	-----
12	U	547160	934014	28	01-01-1970 04:00:00 (0)	Modbus	-----
13	DU.Sets.Device	32	32	134	01-01-1970 04:00:00 (0)	Modbus	-----
14	PWeight.FreqSet.Output.Dev...	1	1	135	01-01-1970 04:00:00 (0)	Modbus	-----
15	UnSense.FreqSet.Output.De...	0.00833333	0.00833333	136	01-01-1970 04:00:00 (0)	Modbus	-----
16	U2.Param.Calibrat	647160	547160	148	01-01-1970 04:00:00 (0)	Pyramid	1901061A
17	U2.Param.Calibrat	123.456	647160	305	01-01-1970 04:00:00 (0)	Pyramid	1901061A
18	U1.Param.Calibrat	9876.54	0	355	01-01-1970 04:00:00 (0)	Pyramid	-----

Сбросим прибор по питанию

Прочитаем в программе Pult01-P текущий уровень доступа (значение = 0)

В программе Pult01-Архив снова считаем архив событий

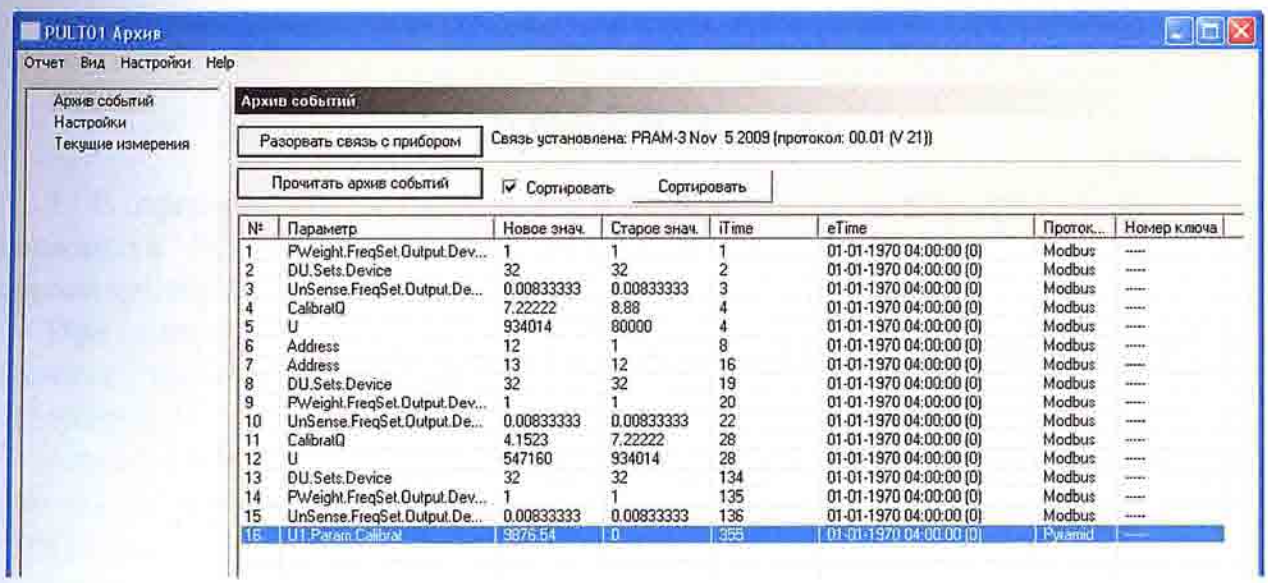
В считанном архиве прочитано только 16 записей. Видим, что записи об изменении калибровочного коэффициента U2 отсутствует.



№	Параметр	Новое знач.	Старое знач.	iTime	eTime	Протоко...	Номер ключа
1	PWeight.FreqSet.Output.Dev...	1	1	1	01-01-1970 04:00:00 (0)	Modbus	----
2	DU.Sets.Device	32	32	2	01-01-1970 04:00:00 (0)	Modbus	----
3	UnSense.FreqSet.Output.De...	0.00833333	0.00833333	3	01-01-1970 04:00:00 (0)	Modbus	----
4	CalibratQ	7.22222	8.88	4	01-01-1970 04:00:00 (0)	Modbus	----
5	U	934014	80000	4	01-01-1970 04:00:00 (0)	Modbus	----
6	Address	12	1	8	01-01-1970 04:00:00 (0)	Modbus	----
7	Address	13	12	16	01-01-1970 04:00:00 (0)	Modbus	----
8	DU.Sets.Device	32	32	19	01-01-1970 04:00:00 (0)	Modbus	----
9	PWeight.FreqSet.Output.Dev...	1	1	20	01-01-1970 04:00:00 (0)	Modbus	----
10	UnSense.FreqSet.Output.De...	0.00833333	0.00833333	22	01-01-1970 04:00:00 (0)	Modbus	----
11	CalibratQ	4.1523	7.22222	28	01-01-1970 04:00:00 (0)	Modbus	----
12	U	547160	934014	28	01-01-1970 04:00:00 (0)	Modbus	----
13	DU.Sets.Device	32	32	134	01-01-1970 04:00:00 (0)	Modbus	----
14	PWeight.FreqSet.Output.Dev...	1	1	135	01-01-1970 04:00:00 (0)	Modbus	----
15	UnSense.FreqSet.Output.De...	0.00833333	0.00833333	136	01-01-1970 04:00:00 (0)	Modbus	----
16	UI.Param.Calibrat	9876.54	0	355	01-01-1970 04:00:00 (0)	Pyramid	----

Нажмём на плате кнопку «Калибровка», прибор переходит в режим калибровка, считаем в Pult01-P параметр Access (значение = 6)

Ещё раз в программе Pult01-Архив считаем архив событий. При считывании архива отображается также лишь 16 записей, среди которых нет записи об изменении коэффициента U2



№	Параметр	Новое знач.	Старое знач.	iTime	eTime	Проток...	Номер ключа
1	PWeight.FreqSet.Output.Dev...	1	1	1	01-01-1970 04:00:00 (0)	Modbus	-----
2	DU.Sets.Device	32	32	2	01-01-1970 04:00:00 (0)	Modbus	-----
3	UnSense.FreqSet.Output.De...	0.00833333	0.00833333	3	01-01-1970 04:00:00 (0)	Modbus	-----
4	CalibratQ	7.22222	8.88	4	01-01-1970 04:00:00 (0)	Modbus	-----
5	U	934014	80000	4	01-01-1970 04:00:00 (0)	Modbus	-----
6	Address	12	1	8	01-01-1970 04:00:00 (0)	Modbus	-----
7	Address	13	12	16	01-01-1970 04:00:00 (0)	Modbus	-----
8	DU.Sets.Device	32	32	19	01-01-1970 04:00:00 (0)	Modbus	-----
9	PWeight.FreqSet.Output.Dev...	1	1	20	01-01-1970 04:00:00 (0)	Modbus	-----
10	UnSense.FreqSet.Output.De...	0.00833333	0.00833333	22	01-01-1970 04:00:00 (0)	Modbus	-----
11	CalibratQ	4.1523	7.22222	28	01-01-1970 04:00:00 (0)	Modbus	-----
12	U	547160	934014	28	01-01-1970 04:00:00 (0)	Modbus	-----
13	DU.Sets.Device	32	32	134	01-01-1970 04:00:00 (0)	Modbus	-----
14	PWeight.FreqSet.Output.Dev...	1	1	135	01-01-1970 04:00:00 (0)	Modbus	-----
15	UnSense.FreqSet.Output.De...	0.00833333	0.00833333	136	01-01-1970 04:00:00 (0)	Modbus	-----
16	U1.Param.Calibrat	9876.54	0	355	01-01-1970 04:00:00 (0)	Pyramid	-----

Данное исследование свидетельствует о том, что в режиме доступа уровня 9, превышающем уровни доступа, описанные в технической документации прибора ПРЭМ фирмы Теплоком, возможно изменение защищенных параметров прибора, в частности, калибровочных коэффициентов без отображения проведенных изменений в архиве событий прибора ПРЭМ фирмы Теплоком.

Изменения калибровочных параметров прибора ПРЭМ фирмы Теплоком, выполненные при уровне доступа 9 (авторизация при использовании шифрования ключом) не отображаются в архиве событий прибора ПРЭМ в рабочем режиме (Уровень /Access =0) и в режиме калибровка (Уровень/Access =6), т.е. при уровнях доступа, описанных в технической документации прибора ПРЭМ фирмы Теплоком.

Источники информации

Общая информация
http://www.teplocom-sale.ru/catalogue/?ELEMENT_ID=2110&SECTION_ID=142
Руководство по эксплуатации
http://www.teplocom-ale.ru/upload/iblock/968/PREM_operating_manual_v5.14.pdf
Описание типа
http://www.teplocom-sale.ru/upload/iblock/041/lcofnoww_lkhw_exxg_170611.pdf
Сертификат
http://www.teplocom-sale.ru/upload/iblock/a6d/_new_xvkx.jpg
Общедоступная программа для просмотра настроек ПРЭМ
http://www.teplocom.msk.ru/data/support/software/PULT01.exe
Часто задаваемые вопросы по ПРЭМ
http://www.teplocom.spb.ru/support/index.php?SECTION_ID=175#7185

В Ы В О Д Ы :

1. В приборе ПРЭМ, фирмы Теплоком имеется недокументированная возможность (НДВ), позволяющая переводить прибор в режим доступа, превышающий описанный в технической документации.

При использовании стандартного программного обеспечения фирмы Теплоком Pult01-P прибор может быть переведен в уровень доступа (Access = 9), не описанный в технической документации на прибор ПРЭМ.

Анализ уровней доступа показывает, что полученный уровень (Access =9) выше по значению, чем регламентированные в документации на прибор ПРЭМ уровни доступа:

- рабочий режим, Access = 0

- сервисный режим, Уровень доступа 5, согласно документации на ПО Pult01 Service, стр.18

- режим калибровки при нажатой кнопке аппаратного доступа, Access = 6

Обмен с прибором составляет 16 байт в рамках стандартного протокола обмена прибора ПРЭМ с использованием стандартного ПО Pult01-P.

Ключ фирмы Аладдин используется только для шифрования считанной из ПРЭМ последовательности в 16 байт и не участвует в активном обмене с прибором ПРЭМ. На момент записи зашифрованной ключом последовательности из 16 байт ключ был удален из ПК.

2. В режиме доступа уровня 9, превышающем уровни доступа, описанные в технической документации прибора ПРЭМ фирмы Теплоком, возможно изменение защищенных параметров прибора без нарушения пломбы госповерителя.

Изменения калибровочных параметров прибора ПРЭМ фирмы Теплоком, выполненные при уровне доступа 9 (авторизация при использовании шифрования ключом) не отображаются в архиве событий прибора ПРЭМ в рабочем режиме (Уровень /Access =0) и в режиме калибровка (Уровень/Access =6), т.е. при уровнях доступа, описанных в технической документации прибора ПРЭМ фирмы Теплоком.

ПРИЛОЖЕНИЕ:

- таблица иллюстраций к заключению специалиста №037-13 от 13 июня 2013 года на 2 листах;
- копии дипломов на 2-х листах;
- копия свидетельства о государственной регистрации юридического лица на 1 листе.

Специалист ООО Экспертное агентство VIIA ***Постовалов И.В.***

ЭКСПЕРТНОЕ АГЕНТСТВО
ВИТА

ТАБЛИЦА ИЛЛЮСТРАЦИЙ

к заключению специалиста №037-13 от «13» июня 2013 года.

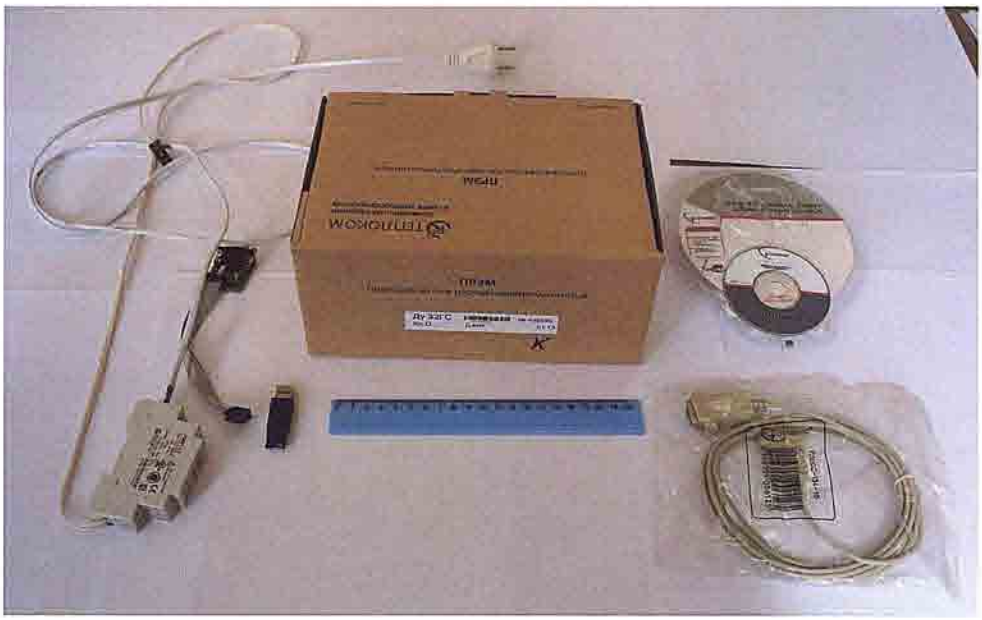


Иллюстрация №1. Вид объектов, предоставленных на исследование.

Иллюстрация №2. Преобразователь расхода электромагнитный ПРЭМ серийный номер №495595 в заводской таре.

Специалист ООО Экспертное агентство ВИТА Постовалов И.В.

Иллюстрация №3. Исследуемый ПРЭМ с принадлежностями.

Иллюстрация №4. Увеличенное изображение ПРЭМ с заводским номером.

Специалист

ООО
Экспертное агентство
ВПА

Постовалов И.В.

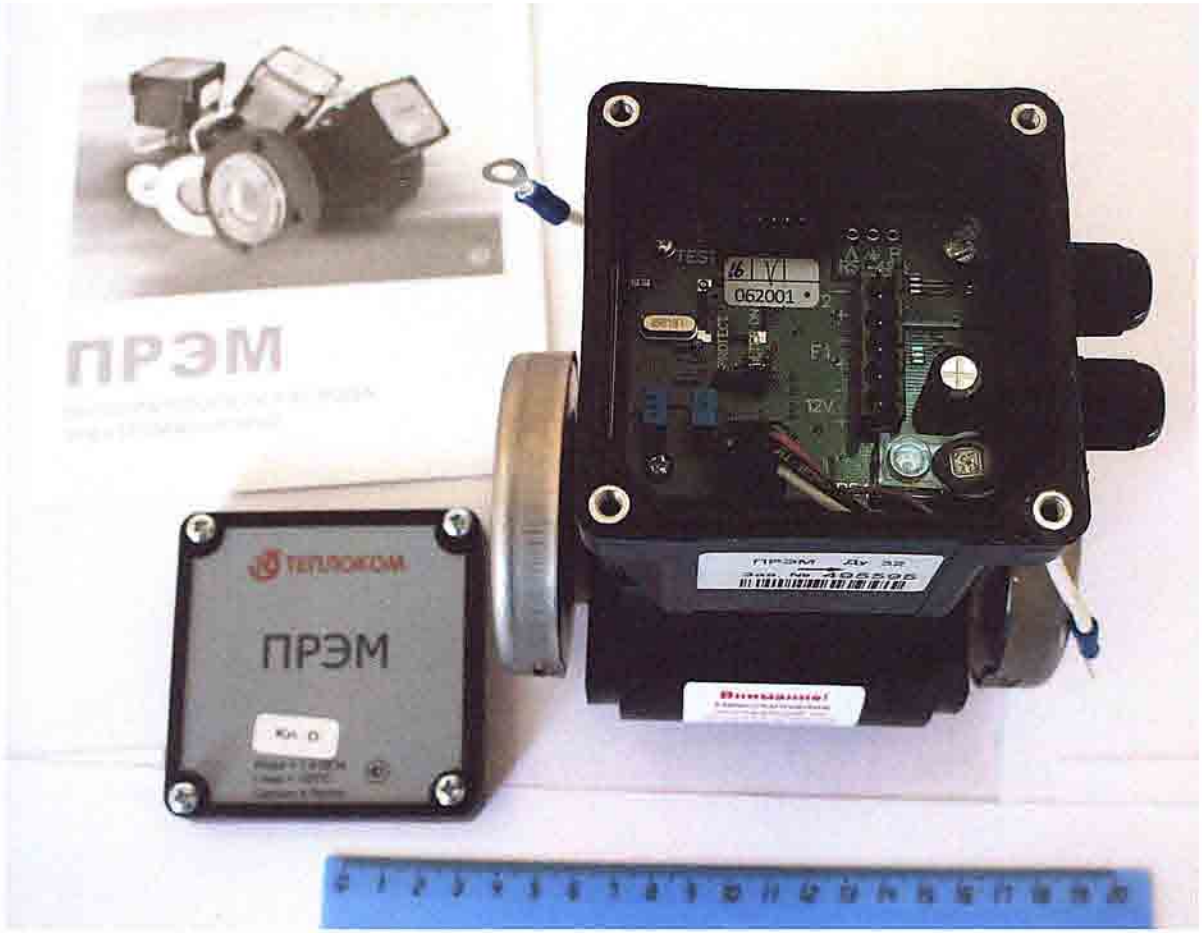


Иллюстрация №5. Увеличенное изображение ПРЭМ со снятой лицевой панелью измерительного блока.

Иллюстрация №6. Увеличенное изображение ПРЭМ со снятой лицевой панелью измерительного блока.

Специалист ООО Экспертное агентство Постовалов И.В.

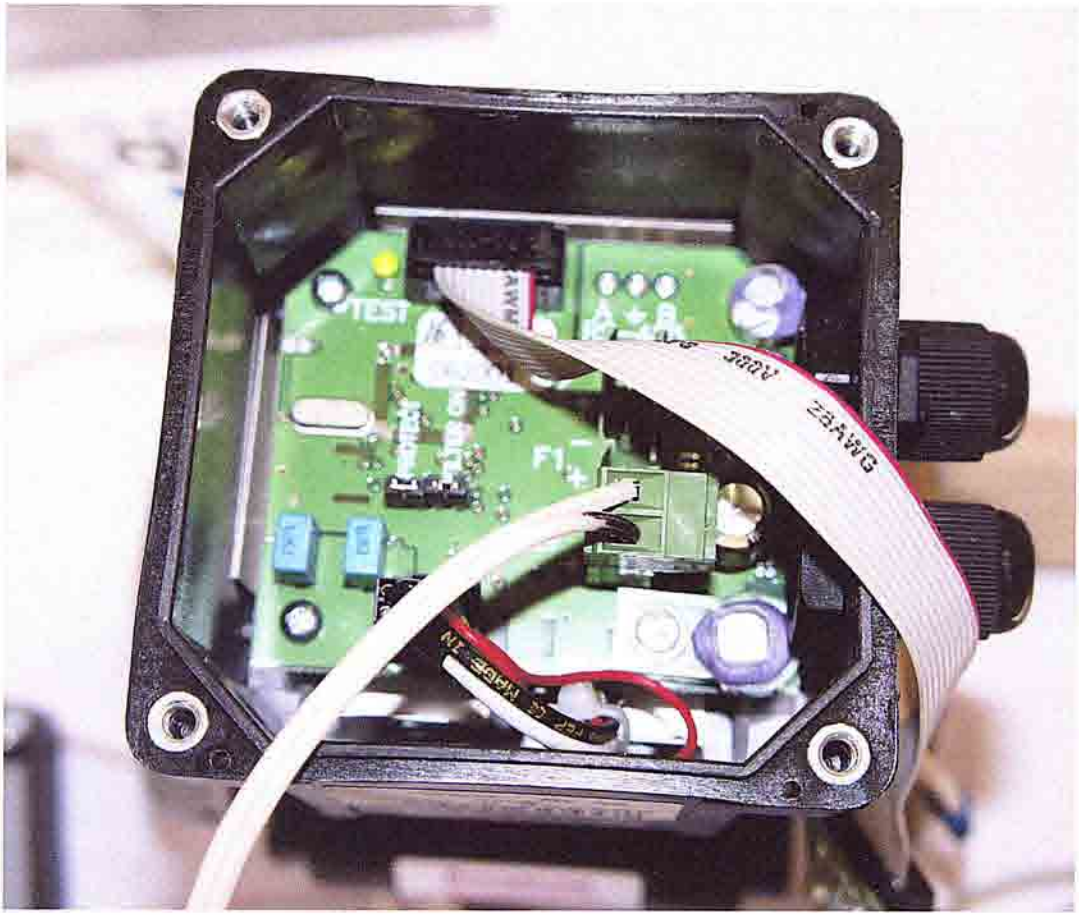


Иллюстрация №7. Увеличенное изображение ПРЭМ со снятой лицевой панелью.

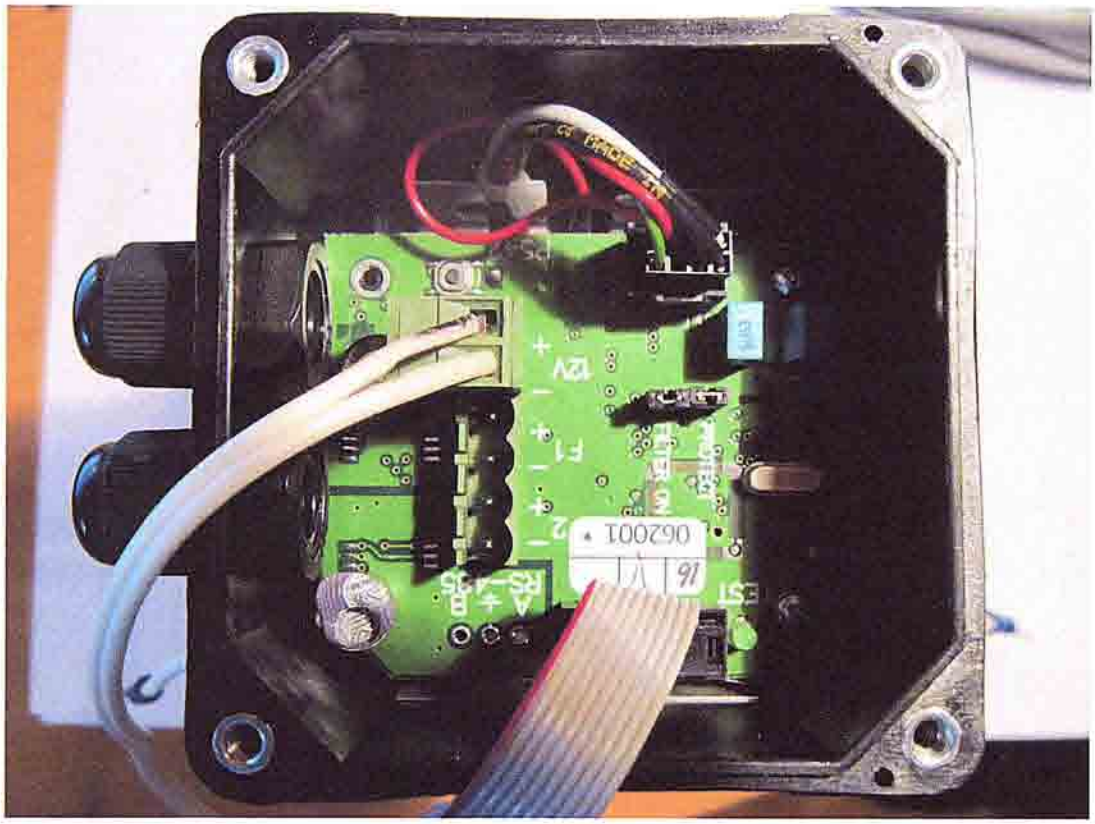


Иллюстрация №8. Увеличенное изображение ПРЭМ с удаленной пломбой для перевода ПРЕМ в режим «Калибровка» (уровень доступа 6).

Специалист

ООО
Экспертное агентство
Эксперт-Вита

Постовалов И.В.

ДИПЛОМ ЯВЛЯЕТСЯ
ГОСУДАРСТВЕННЫМ ДОКУМЕНТОМ
О ВЫСШЕМ ОБРАЗОВАНИИ

Регистрационный номер 2040 "02" июля 2007 г.

РОССИЙСКАЯ ФЕДЕРАЦИЯ
г. Санкт-Петербург
Федеральное государственное образовательное учреждение
высшего профессионального образования
"Санкт-Петербургский государственный университет"

ДИПЛОМ

ВБА 0204940

Решением
Государственной аттестационной комиссии
от 06 июня 2007 года
Постовалову
Ивану Вадимовичу

ПРИСУЖДЕНА СТЕПЕНЬ
БАКАЛАВРА
МАТЕМАТИКИ И МЕХАНИКИ
по направлению
"Механика, прикладная математика"

Председатель Государственной
аттестационной комиссии
Ректор
М.П.

ДИПЛОМ ЯВЛЯЕТСЯ
ГОСУДАРСТВЕННЫМ ДОКУМЕНТОМ
О ВЫСШЕМ ОБРАЗОВАНИИ

ООО Экспертное агентство ВИТТА КОПИЯ ВЕРНА
Ген. директор

Регистрационный номер 2506 01 июля 2009 года

РОССИЙСКАЯ ФЕДЕРАЦИЯ
г. Санкт-Петербург
Федеральное государственное образовательное учреждение
высшего профессионального образования
"Санкт-Петербургский государственный университет"

ДИПЛОМ

ВМА 0077004

Решением
Государственной аттестационной комиссии

от 02 июня 2009 года

ПОСТОВАЛОВУ
Ивану Вадимовичу

ПРИСУЖДЕНА СТЕПЕНЬ
МАГИСТРА
МАТЕМАТИКИ И МЕХАНИКИ
по направлению
"Механика. Прикладная математика"

Председатель Государственной
аттестационной комиссии
Ректор

М. П.

Форма № | Р | 5 | 1 | 0 | 0 | 1 |

Федеральная налоговая служба

СВИДЕТЕЛЬСТВО

о государственной регистрации юридического лица

Настоящим подтверждается, что в соответствии с Федеральным законом «О государственной регистрации юридических лиц» в единый государственный реестр юридических лиц внесена запись о создании юридического лица

Общество с ограниченной ответственностью "ЭКСПЕРТНОЕ АГЕНТСТВО "ВИТТА"
(полное наименование юридического лица с указанием организационно-правовой формы)

ООО "ЭКСПЕРТНОЕ АГЕНТСТВО "ВИТТА"
(сокращенное наименование юридического лица)

Общество с ограниченной ответственностью "ЭКСПЕРТНОЕ АГЕНТСТВО "ВИТТА"
(фирменное наименование)

11 (дата) мая (месяц прописью) 2007 (год) **за основным государственным регистрационным номером**

1	0	7	7	8	4	7	3	9	3	5	3	5

Межрайонная инспекция Федеральной налоговой службы №15 по Санкт-Петербургу
(Наименование регистрирующего органа)

Зам. начальника Межрайонной инспекции ФНС России _____ Г.Г.Рутковский
(подпись, ФИО)

МП

ООО Экспертное агентство ВИТТА КОПИЯ ВЕРНА Ген. директор

серия 78 №006087198

Прошито 31 листов
Генеральный директор
ООО «Экспертное агентство» «ВИТТА»

Меньшиков П.В.

Общество с ограниченной ответственностью * Экспертное агентство ВИТТА * Санкт-Петерб...