



ОПЕРАТИВНО-АНАЛИТИЧЕСКИЙ ЦЕНТР ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ

220004 г. Минск, ул. Кальварийская, 17, тел. (0172) 203 59 67, факс 306 08 10

УТВЕРЖДАЮ
Заместитель начальника Центра-
начальник управления защиты
информации

..... С.Н. Капариха

22 июля 2011 г.

Срок действия
с 22.07.2011 по 21.07.2013

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

22.07.2011 № 269

на программное средство
криптографической защиты
информации ВНСryptoCore
(РБ.КМАС.00082-01)

1 Введение

1.1 Государственная экспертиза программного средства криптографической защиты информации ВНСryptoCore (РБ.КМАС.00082-01), производства ЗАО «БелХард Групп» (далее – Продукт), проведена на основании договора от 28.04.2011 № 2-33/2011 между Оперативно-аналитическим центром при Президенте Республики Беларусь и ЗАО «БелХард Групп».

1.2 Экспертиза проведена Оперативно-аналитическим центром при Президенте Республики Беларусь, г. Минск, ул. Кальварийская, 17.

1.3 Материалы для проведения экспертизы представлены ЗАО «БелХард Групп», г. Минск, ул. Мельникайте, 2-709.

1.4 Экспертиза проведена на соответствие требованиям РД РБ 07040.1202-2003 «Банковские технологии. Процедура выработки псевдослучайных данных с использованием секретного параметра» и проекта Руководящего документа Республики Беларусь «Банковские технологии. Протоколы формирования общего ключа».

1.5 Экспертное заключение выдано на основании результатов испытаний – экспертное заключение испытательной лаборатории НИИ прикладных проблем математики и информатики БГУ от 07.07.2011 № 444/4.

2 Состав представленных материалов

На экспертизу представлен Продукт в соответствии с актом отбора образцов от 15.07.2011 № 27/2-11-1, включающий:

2.1 Основные исполняемые модули:

Имя файла	Контрольная характеристика*
BHCryptoCore_x86.dll	0F8937E8FAC452193A502ECABE9BE58F5A9ABA9E832EB3AC1FB7CD7F9B9D3994
BHCryptoCore_x86.lib	9617FA24D91C7DDBE2E3ED73DF1233D2AB81A60BCA2474BC9CDB21799628AC73
BHCryptoCore_x64.dll	3DA3DA8C3FC0E89A6171E282BB2FFDB53DD28671F8FDA7310FA5734E30C24048
BHCryptoCore_x64.lib	E02B29E56CE9ACD29E7CBD25AC6156D20716E7DDD01DD8A1B82BFBE78DEC05DA
libBHCryptoCore_x86-1.0.so.1.0.0	080EF5BCF8CA7A5190DCF4054E6A484F7BD042A04F1B1774AE397E31E7E1D5C9
libBHCryptoCore_x64-1.0.so.1.0.0	9617FA24D91C7DDBE2E3ED73DF1233D2AB81A60BCA2474BC9CDB21799628AC73

(*) Контрольная характеристика - значение функции хэширования файла, вычисленное в соответствии с алгоритмом, приведенным в СТБ 1176.1-99 со стартовым вектором хэширования в шестнадцатеричном виде $H = xAA\ xAA\ \dots\ xAA$ (32 байта – 10101010) (шестнадцатеричная запись байтов контрольной характеристики осуществляется справа налево).

2.2 программную документацию на CD-R № 252 170 MD 43739.

3 Результаты исследований

В результате исследований установлено:

3.1 Продукт соответствует требованиям:

РД РБ 07040.1202-2003 «Банковские технологии. Процедура выработки псевдослучайных данных с использованием секретного параметра»;

проекта РД РБ «Банковские технологии. Протоколы формирования общего ключа».

3.2 Исходные файлы Продукта скомпилированы в следующие исполняемые модули для выполнения в среде операционных систем (далее – ОС):

BHCryptoCore_x86.dll – динамическая библиотека для 32-х разрядных ОС семейства Windows;

BHCryptoCore_x86.lib – статическая библиотека экспортируемых символов для 32-х разрядных ОС семейства Windows;

BHCryptoCore_x64.dll – динамическая библиотека для 64-х разрядных ОС семейства Windows;

BHCryptoCore_x64.lib – статическая библиотека экспортируемых символов для 64-х разрядных ОС семейства Windows;

libBHCryptoCore_x86-1.0.so.1.0.0 – динамическая библиотека для 32-х разрядных ОС семейства Linux;

libBNCryptoCore_x64-1.0.so.1.0.0 – динамическая библиотека для 64-х разрядных ОС семейства Linux.

4 Выводы

Программное средство криптографической защиты информации BNCryptoCore (РБ.КМАС.00082-01), изготовленное ЗАО «БелХард Групп» (г. Минск, ул. Мельникайте, 2-709), соответствует требованиям РД РБ 07040.1202-2003 «Банковские технологии. Процедура выработки псевдослучайных данных с использованием секретного параметра» и проекта Руководящего документа Республики Беларусь «Банковские технологии. Протоколы формирования общего ключа».

5 Рекомендации по эксплуатации

Продукт должен эксплуатироваться в соответствии с требованиями эксплуатационной документации.

Руководитель экспертной группы



Н.Д.Микулич