**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
15 февраля 2011 г.

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

Срок действия
с 15.02.2011 по 15.02.2013

15.02.2010 № 240

на программное средство гарантированной защищенной передачи данных «BelHard Security Transport v1.0» (РБ.КМАС.00052-01)

1 Введение

1.1 Государственная экспертиза программного средства гарантированной защищенной передачи данных «BelHard Security Transport v1.0» (РБ.КМАС.00052-01), производства ЗАО «БелХард Групп» (далее – Продукт), проведена на основании договора от 18.11.2010 № 2-76/2010 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 раздела 1.2.1 документа «Средство гарантированной защищенной передачи данных «BelHard Security Transport v1.0». Руководство системного программиста» (РБ.КМАС.00052-01 32).

1.5 Экспертное заключение выдано на основании результатов испытаний – экспертное заключение испытательной лаборатории НИИ прикладных проблем математики и информатики БГУ от 31.01.2011 № 444/1.

2 Состав представленных материалов

На экспертизу представлен Продукт в соответствии с актом отбора образцов от 08.02.2011 № 8/43/1-10, включающий:

2.1 Основные исполняемые модули:

Имя файла	Контрольная характеристика*
BHAuthPlugin.dll	A9216B73A97B2C2F57024749B7AB1927 2B348DD3F27B2FBACDE380F75B11299B
BHMCMFNET.dll	BCDE8442C86F5AB9F3F105FD2927C570 6C8DD3C7BA13246B65D98ED752EF81B5
BHMCertAPINET.dll	AC9E0E18ABC33F67F7375FAAAECD5843 D3992D737BF647E3D90CF0A61D56D4DB
BHTCommonData.dll	4978DAA9FF8D3CF30C87F6656C162E8A 3CDD5C1D2A77F2691C507C786E88035B
BHTransport.dll	CC6F47A64DCC93759E9CD9BD619B8AD8 D1667D167435666A66F69F6D337DFBF9
CompressPlugin.dll	52B641702D3A2363EC6C8C741C4B259B D6DA70141933BC66DE956BF77077C488
EdsPlugin.dll	54B37796E38339260EEC9D9C093C81EB 52A84095A17B2CDC8D1C17B1746E7EC4
EncryptPlugin.dll	2A1BD129AC32347C8E6C489D4BA21533 48BC0D1E58C8BD7137526D05C84C37AE
HashPlugin.dll	A3B389D5556FF2ADC8395C777EA4F316 F90BED9E57569A7881E309C8C4422407
Configurator.exe	729AD5A88C0A73CE1B910F756017C92A 8F880A416E17AC1D98D30860779F72C4
ConsoleServer.exe	EDB3D6CA4A091C947C6421DE344C3E0D 3C021FB286F6859EB998FB1AB40A5EF1
TransmitClient.exe	34CA3CB4915E7591D61BC30BAD5AEB8E AC68F2CE635205519FACDFF3E464A4DC
BHMCMF.dll	5D426D201629018A769BF6E4CEA50F7E 825EEC519A1B9491AA21A7A8E8874C27
BHMCrypt32v2.dll	C1987CC3853EE84A3171DB2D58021275 C7130CC1E13C53F124D796318EA1B13A

(*) 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 … xAA* (32 байта – *10101010*) (шестнадцатеричная запись байтов контрольной характеристики осуществляется справа налево).

2.2 программную документацию на CD-R *N 1280C291D800087C1*.

3 Результаты исследований

В результате исследований установлено:

3.1 В Продукте для выполнения криптографических алгоритмов согласно ГОСТ 28147-89, СТБ 1176.1-99, СТБ 1176.2-99, РД РБ 07040.1202-2003 и протокола согласно проекту РД РБ «Банковские технологии.

Протоколы формирования общего ключа» используется библиотека «BHMCrypt32v2.dll» (РБ.УАСР.00013-01), соответствующая сертификату соответствия № BY/112 03/07/036 0081, экспертному заключению Оперативно-аналитического центра при Президенте Республики Беларусь от 22.10.2009 г. № 167.

3.2 В Продукте вызов функций библиотеки «BHMCrypt32v2.dll» (РБ.УАСР.00013-01), реализующих криптографические алгоритмы согласно ГОСТ 28147-89, СТБ 1176.1-99, СТБ 1176.2-99, РД РБ 07040.1202-2003 и протокол согласно проекту РД РБ «Банковские технологии. Протоколы формирования общего ключа», осуществляется через вызов функций библиотеки «BHMCMF.dll» (РБ.УАСР.00014-01), соответствующей экспертному заключению Оперативно-аналитического центра при Президенте Республики Беларусь от 23.10.2009 г. № 169.

3.3 В Продукте при реализации механизмов безопасности производится корректное обращение к функциям библиотеки «BHMCMF.dll» (РБ.УАСР.00014-01), обеспечивающих:

шифрование в режиме гаммирования с обратной связью и выработку имитовставки согласно ГОСТ 28147-89;

хэширование согласно СТБ 1176.1-99;

выработку и проверку электронной цифровой подписи согласно СТБ 1176.2-99;

формирование общего ключа согласно проекту РД РБ «Банковские технологии. Протоколы формирования общего ключа»;

выработку псевдослучайных данных согласно РД РБ 07040.1202-2003;

аутентификацию согласно проекту стандарта Республики Беларусь «Информационные технологии. Аутентификация объекта. Часть 3. Механизм использования технологии цифровой подписи» (механизм трехшаговой аутентификации).

3.4 Продукт обеспечивает:

взаимную аутентификацию АРМ «Клиент» и АРМ «Сервер» путем выполнения механизма трехшаговой аутентификации согласно проекту стандарта Республики Беларусь «Информационные технологии. Аутентификация объекта. Часть 3. Механизм использования технологии цифровой подписи» при условии использования дополнительно подключаемого программного модуля «AuthPlugin» (согласно документу РБ.КМАС.00052-01 32);

конфиденциальность файлов, передаваемых от АРМ «Клиент» на АРМ «Сервер», путем шифрования в режиме гаммирования с обратной связью согласно ГОСТ 28147-89 при условии использования дополнительно подключаемого программного модуля «EncryptPlugin» (согласно документу РБ.КМАС.00052-01 32);

контроль целостности и подлинности файлов, передаваемых от АРМ «Клиент» на АРМ «Сервер», путем контроля имитовставки,

выработанной согласно ГОСТ 28147-89, при условии использования дополнительно подключаемого программного модуля «EncryptPlugin» (согласно документу РБ.КМАС.00052-01 32);

контроль целостности и подлинности файлов, передаваемых от АРМ «Клиент» на АРМ «Сервер», путем проверки электронной цифровой подписи, выработанной согласно СТБ 1176.2-99, при условии совместного использования дополнительно подключаемых программных модулей «EncryptPlugin» и «EDSPlugin» (согласно документу РБ.КМАС.00052-01 32);

контроль целостности файлов (при непреднамеренных ошибках в канале связи), передаваемых от АРМ «Клиент» на АРМ «Сервер», путем проверки хэш-значения, выработанного согласно СТБ 1176.1-99, при условии использования дополнительно подключаемого программного модуля «HashPlugin» (согласно документу РБ.КМАС.00052-01 32);

уничтожение в ОЗУ критических объектов после их использования и при возникновении ошибочных ситуаций.

4 Выводы

Программное средство гарантированной защищенной передачи данных «BelHard Security Transport v1.0» (РБ.КМАС.00052-01), изготовленное ЗАО «БелХард Групп» (г. Минск, ул. Мельникайте, 2-709), соответствует требованиям раздела 1.2.1 документа «Средство гарантированной защищенной передачи данных «BelHard Security Transport v1.0». Руководство системного программиста» (РБ.КМАС.00052-01 32).

5 Рекомендации по эксплуатации

Продукт должен эксплуатироваться:

в соответствии с требованиями программного документа «Средство гарантированной защищенной передачи данных «BelHard Security Transport v1.0». Руководство системного программиста» (РБ.КМАС.00052-01 32);

при использовании личных ключей и сертификатов открытых ключей электронной цифровой подписи СТБ 1176.2-99, секретных ключей идентификации и сертификатов открытых ключей проекта РД РБ «Банковские технологии. Протоколы формирования общего ключа», секретного параметра РД РБ 07040.1202-2003, сгенерированных с помощью средств криптографической защиты, имеющих сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы;

при организации безопасного управления списками отозванных сертификатов открытых ключей электронной цифровой подписи СТБ 1176.2-

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

при безопасном использовании пароля для доступа к криптоконтейнеру, который применяется объектом испытаний для хранения личного ключа СТБ 1176.2-99, секретного ключа идентификации проекта РД РБ «Банковские технологии. Протоколы формирования общего ключа» и секретного параметра РД РБ 07040.1202-2003.

Руководитель экспертной группы  Н.Д.Микулич