**ОПЕРАТИВНО-АНАЛИТИЧЕСКИЙ ЦЕНТР
ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ**

220004 г. Минск, ул. Кальварийская, 17, тел. (017) 203 59 67, факс 306 08 10

УТВЕРЖДАЮ
Заместитель начальника Центра-
начальник управления защиты
информации

..... С.Н. Капариха

29 марта 2011 г.

Срок действия
с 29.03.2011 по 29.03.2013

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

29.03.2011 № 247

на программное средство
криптографической защиты
информации BelIPSec v 2.0
(РБ.КМАС.00023-02)

1 Введение

1.1 Экспертиза программного средства криптографической защиты информации BelIPSec v 2.0 (РБ.КМАС.00023-02) (далее - Продукт), производства Закрытого акционерного общества «БелХард Групп», проведена на основании договора от 10.08.2010 № 2-47/2010 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 в целях подтверждения соответствия Продукта требованиям раздела 5 документа «Комплекс средств обеспечения безопасности объекта программного средства криптографической защиты информации BelIPSec v 2.0. Общее описание».

1.5 Экспертное заключение выдано на основании результатов испытаний проведенных НИИ прикладных проблем математики и информатики (экспертное заключение от 28.02.2011 № 444/2, протокол

результатов проверки идентичности от 28.02.2011 № 444/2/1П, протокол результатов анализа изменений от 28.02.2011 № 444/2/2П, протокол результатов анализа исходных текстов от 28.02.2011 № 444/2/3П, протокол контрольной компиляции от 28.02.2011 № 444/2, методика испытаний программного средства криптографической защиты информации BelIPSec v 2.0 (РБ.КМАС.00023-02) МИ.190159829.444.02).

2 Состав представленных материалов

На экспертизу представлен Продукт в соответствии с актом отбора образцов от 28.03.2011 № 8/26/1-10, включающий:

2.1 Основные исполняемые модули:

Имя файла	Контрольная характеристика*
IPSecVPN.sys для ОС Windows 2000	290B206D E27D24CB 6937432B 0B4C67C1 88DD6075 6A2B524D 81F7FB3B 1CB839AC
IPSecVPN.sys для ОС Windows XP	A4DDABE7 8013DF32 6748410F B10B7919 3FC7AF1D A6C155E4 349655E8 84B9099E
AdminCli.exe	93829451 FE7313EE 97F7888A 28682985 A8CBF76E 0286D1B8 185E3968 E979109C
AdminSrv.exe	2E6E64FB 90CFECF6 D2F43702 5B8876C6 48CB7BBD 67A19D4D 129E238D 6D8B76A0
IKEServer.exe	A2FAC342 F78029D7 50180C04 0D3AFC19 5B493076 E96C0652 5BBE5863 F35F4A88
BHLogging.dll	CC4FEBA3 472C9A65 3168DF63 D79C17FF D1089EBA CC3D6562 EBE3A302 90931BE2
BHSettings.dll	2E44B969 212E7739 1A9986A8 38AB5722 9D7CA746 B5F8C5B4 CE59998E 7A443511
IKEExchangeInfo.dll	1F5D908E 1E48CD5E F7338CA5 6E17551F A116872E DA1AE275 549B3F88 B35E436D
PKIWorker.dll	92D99609 5D321268 BEEA8E98 92250334 F532B1B1 6EFE6C9E 4A592893 8E9C7A82
VpnComm.dll	822F64B9 8BBCC55C 5BBCC0E3 16B7C3F8 FB5DB82A 52CA4139 05ED5734 CA3D8323
VPNCommunication.dll	3C0267E0 75E1A9CF E7967F89 724D1B33 B93288BF 4756093A A6E4C170 61FBA7AB

(*) 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 NI280C297D800098A2.

3 Результаты исследований

В результате исследований установлено:

3.1 В программной компоненте BHMCMF.dll (РБ.УАСР.00014-01) Продукта обращение к криптографическим функциям шифрования и выработки имитовставки в соответствии с ГОСТ 28147–89, хэширования в соответствии с СТБ 1176.1-99, выработки и проверки электронной цифровой подписи в соответствии с СТБ 1176.2-99, выработки псевдослучайных данных в соответствии с РД РБ 07040.1202-2003,

формирования общего ключа в соответствии с проектом РД РБ «Банковские технологии. Протоколы формирования общего ключа», реализованным в библиотеке BHMCrypt32v2.dll (РБ.УАСР.00013-01), производится корректно. При обращении к данным криптографическим функциям недокументированные возможности отсутствуют.

Программная компонента BHMCMF.dll (РБ.УАСР.00014-01) Продукта соответствует требованиям РД РБ 070040.1201-2003 «Банковские технологии. Средства электронной цифровой подписи программные. Общие требования» (разделы 6 – 9, 11 – 14).

Программная компонента BHMCMF.dll (РБ.УАСР.00014-01) Продукта соответствует требованиям проекта стандарта Республики Беларусь «Информационные технологии. Технология безопасности. Аутентификация объекта. Ч.3 Механизм использования технологии цифровой подписи» (проверка меток времени и порядковых номеров механизма аутентификации в компоненте BHMCMF.dll не реализована).

3.2 В программной компоненте BHMCMFNET.dll Продукта обращение к криптографическим функциям шифрования и выработки имитовставки в соответствии с ГОСТ 28147–89, хэширования в соответствии с СТБ 1176.1-99, выработки и проверки электронной цифровой подписи в соответствии с СТБ 1176.2-99, выработки псевдослучайных данных в соответствии с РД РБ 07040.1202-2003, формирования общего ключа в соответствии с проектом РД РБ «Банковские технологии. Протоколы формирования общего ключа», реализованным в библиотеке BHMCrypt32v2.dll (РБ.УАСР.00013-01), производится корректно. Обращение к данным криптографическим функциям осуществляется через вызов функций программной компоненты BHMCMF.dll (РБ.УАСР.00014-01). При обращении к данным криптографическим функциям недокументированные возможности отсутствуют.

3.3 В Продукте шифрование и вычисление имитовставки данных IP-пакетов в соответствии с ГОСТ 28147-89 производится программной компонентой IPSecVPN.sys (РБ.КМАС.00035-02), прошедшей сертификационные испытания (см. протокол испытаний испытательной лаборатории НИИ прикладных проблем математики и информатики № 38 от 28 февраля 2011 г.).

3.4 В Продукте в режиме работы с криптографическими библиотеками ЧПУП «Модуль-НП» (см. раздел 3 и подраздел 4.2 документа «Общее описание»), режиме ввода пароля к криптоконтейнеру «Ручной» и режиме аутентификации клиентов «ПФОК с аутентификацией» (см. пункты 4.1.4.1 и 4.1.4.2 документа

«Руководство системного программиста. РБ.КМАС.00023-02 32» соответственно):

3.4.1 Обращение к криптографическим функциям шифрования и выработки имитовставки в соответствии с ГОСТ 28147–89, хэширования в соответствии с СТБ 1176.1-99, выработки и проверки электронной цифровой подписи в соответствии с СТБ 1176.2-99, выработки псевдослучайных данных в соответствии с РД РБ 07040.1202-2003, формирования общего ключа в соответствии с проектом РД РБ «Банковские технологии. Протоколы формирования общего ключа», реализованным в библиотеке BHMCrypt32v2.dll (РБ.УАСР.00013-01), производится корректно. Обращение к данным криптографическим функциям осуществляется через вызов функций программной компоненты BHMCMFNET.dll. При обращении к данным криптографическим функциям недокументированные возможности отсутствуют. Используемая библиотека BHMCrypt32v2.dll (РБ.УАСР.00013-01) имеет сертификат соответствия BY/112 03.07.036 0081 и экспертное заключение Оперативно-аналитического центра при Президенте Республики Беларусь от 22.10.2009 г. № 167.

3.4.2 Общий ключ, вырабатываемый в соответствии с проектом РД РБ «Банковские технологии. Протоколы формирования общего ключа» (протокол с аутентификацией сторон) и используемый при шифровании и вычислении имитовставки данных IP-пакетов в соответствии с ГОСТ 28147–89, защищен от несанкционированного доступа (общий ключ вырабатывается при создании ассоциации безопасности, хранится только в оперативной памяти и уничтожается сразу после удаления ассоциации безопасности путем перезаписи фрагментов оперативной памяти).

3.5 В объекте испытаний «Программное средство криптографической защиты информации BelIPSec v 2.0 (РБ.КМАС.00023-02)» в режиме работы с криптопровайдером ЗАО «АВЕСТ» версии 5 (см. раздел 3 и подраздел 4.1 документа «Общее описание») при использовании отчуждаемых носителей ключевой информации AvToken и AvPass:

3.5.1 Обращение к криптографическим функциям шифрования в соответствии с ГОСТ 28147-89, хэширования в соответствии с СТБ П 34.101.31-2007, выработки и проверки электронной цифровой подписи в соответствии с СТБ 1176.2-99, выработки псевдослучайных данных в соответствии с РД РБ 07040.1202-2003, формирования общего ключа в соответствии с РД РБ «Банковские технологии. Протоколы формирования общего ключа» (протокол одностороннего формирования

ключа), реализованным в библиотеке «AvCrypt.dll ver 5.0» (РБ.ЮСКИ.09000-01), производится корректно. Обращение к данным криптографическим функциям осуществляется через вызов функций криптопровайдера «Avest CSP Base» программного средства «Криптопровайдер Avest CSP» (РБ.ЮСКИ.08000-01, версии 5.1.0.631 или 5.1.0.647). При обращении к данным криптографическим функциям недокументированные возможности отсутствуют. Особенностью использования функций, реализующих выработку и проверку электронной цифровой подписи, является то, что на входы алгоритмов СТБ 1176.2-99 подаются не электронные сообщения, а их хэш-значения, вычисленные в соответствии с СТБ П 34.101.31-2007. Используемая библиотека «AvCrypt.dll ver 5.0» (РБ.ЮСКИ.09000-01) имеет сертификат соответствия BY/112 03.06.036 0103 и экспертное заключение Оперативно-аналитического центра при Президенте Республики Беларусь от 27.07.2009 г. № 155.

3.5.2 Механизм локальной идентификации и аутентификации реализован корректно и в соответствии с пунктом 4.1.2.1 документа «Общее описание». Механизм построен на основе проверки пароля для доступа к отчуждаемому носителю ключевой информации AvToken или AvPass и реализован путем обращения к функциям криптопровайдера «Avest CSP Base» программного средства «Криптопровайдер Avest CSP» (РБ.ЮСКИ.08000-01, версии 5.1.0.631 или 5.1.0.647).

3.5.3 Механизм удаленной идентификации и аутентификации реализован корректно и в соответствии с пунктом 4.1.2.2 документа «Общее описание». При реализации механизма производится обращения к функциям криптопровайдера «Avest CSP Base» программного средства «Криптопровайдер Avest CSP» (РБ.ЮСКИ.08000-01, версии 5.1.0.631 или 5.1.0.647).

3.5.4 Механизм обеспечения конфиденциальности и контроля целостности криптографических критических объектов при их хранении реализован корректно. Хранятся следующие криптографические критические объекты: личный ключ алгоритма СТБ 1176.2-99, секретный ключ проекта РД РБ «Банковские технологии. Протоколы формирования общего ключа», секретный параметр алгоритма РД РБ 07040.1202-2003. Критические объекты хранятся на отчуждаемом носителе ключевой информации AvToken или AvPass. Конфиденциальность и контроль целостности данных объектов при их хранении обеспечивается средствами криптопровайдера «Avest CSP Base» программного средства «Криптопровайдер Avest CSP» (РБ.ЮСКИ.08000-01, версии 5.1.0.631 или 5.1.0.647).

3.5.5 Механизм контроля целостности криптографических открытых объектов при их хранении реализован корректно. Хранятся следующие криптографические открытые объекты: открытый ключ и параметры алгоритма СТБ 1176.2-99, открытый ключ и параметры проекта РД РБ «Банковские технологии. Протоколы формирования общего ключа», инициализирующее значение алгоритма РД РБ 07040.1202-2003 (хранится на отчуждаемом носителе ключевой информации AvToken или AvPass), блок подстановки алгоритма ГОСТ 28147-89, списки отозванных сертификатов, сертификат открытого ключа удостоверяющего центра. Контроль целостности криптографических открытых объектов при их хранении обеспечивается средствами криптопровайдера «Avest CSP Base» программного средства «Криптопровайдер Avest CSP» (РБ.ЮСКИ.08000-01, версии 5.1.0.631 или 5.1.0.647).

3.5.6 Отчуждаемые носители ключевой информации AvToken и AvPass используется корректно. Для доступа к криптографическим объектам, хранящимся на отчуждаемом носителе ключевой информации, оператор должен успешно пройти аутентификацию. Личный ключ алгоритма СТБ 1176.2-99, секретный ключ проекта РД РБ «Банковские технологии. Протоколы формирования общего ключа», секретный параметр и инициализирующее значение алгоритма РД РБ 07040.1202-2003 хранятся на носителе в защищенном виде. Обращение к носителю обеспечивается средствами криптопровайдера «Avest CSP Base» программного средства «Криптопровайдер Avest CSP» (РБ.ЮСКИ.08000-01, версии 5.1.0.631 или 5.1.0.647).

3.5.7 Механизм уничтожения в ОЗУ критических объектов реализован корректно. Уничтожение информационного содержания в ОЗУ сеансового ключа вычисления имитовставки и шифрования данных IP-пакетов, псевдослучайных данных, используемых при формировании сеансового ключа, производится после их использования перезаписыванием константной строкой. Уничтожение информационного содержания в ОЗУ личного ключа алгоритма СТБ 1176.2-99, секретного ключа проекта РД РБ «Банковские технологии. Протоколы формирования общего ключа», секретного параметра РД РБ 07040.1202-2003 и ключа шифрования сеансового ключа обеспечивается средствами криптопровайдера «Avest CSP Base» программного средства «Криптопровайдер Avest CSP» (РБ.ЮСКИ.08000-01, версии 5.1.0.631 или 5.1.0.647).

4 Выводы

Программное средство криптографической защиты информации BelIPSec v 2.0 (РБ.КМАС.00023-02), производства Закрытого акционерного общества «БелХард Групп», соответствует требованиям раздела 5 документа «Комплекс средств обеспечения безопасности объекта программного средства криптографической защиты информации BelIPSec v 2.0. Общее описание».

5 Рекомендации по эксплуатации

Программное средство криптографической защиты информации BelIPSec v 2.0 (РБ.КМАС.00023-02) необходимо использовать при:

5.1 Соблюдении условий применения программного средства, описанных в документах «Программное средство криптографической защиты информации «BHMCMF.DLL». Руководство программиста. РБ.УАСР.00014-01-33-01» и «Программное средство криптографической защиты информации «BHMCMF.DLL». Описание программы. РБ.УАСР.00014-01-13-01».

5.2 Обеспечении надлежащего качества пароля, используемого для обеспечения конфиденциальности и контроля целостности личного ключа подписи (см. СТБ 1176.2-99), а также секретного параметра и инициализирующего значения процедуры выработки псевдослучайных данных (см. РД РБ 07040.1202-2003).

5.3 Обеспечении контроля целостности открытого ключа проверки подписи и параметров p, q, a, l, r, L и H (см. СТБ 1176.1-99 и СТБ 1176.2-99) средой эксплуатации и (или) организационными мероприятиями;

5.4 Использовании для генерации секретного параметра процедуры выработки псевдослучайных данных (см. РД РБ 07040.1202-2003) физического датчика случайных чисел, удовлетворяющего нормативным документам, действующим в Республике Беларусь.

Руководитель экспертной группы  Н.Д. Микулич