

## 1 ЗАГАЛЬНІ ВІДОМОСТІ ЩОДО ОБ'ЄКТА ЕКСПЕРТИЗИ

1.1 Найменування об'єкта експертизи: Комплекс засобів захисту (КЗЗ) Web-ресурсів від несанкціонованого доступу «Тайфун-Web» версії 1.xx (далі – КЗЗ «Тайфун-Web»).

1.2 Розробник об'єкта експертизи: ТОВ "Інститут комп'ютерних технологій" (ліцензія на право провадження господарської діяльності в галузі технічного захисту інформації № 617984 серії АВ від 05.06.2012, код ЄДРПОУ 21541987), адреса: 03151, м. Київ, пр-т Повітрофлотський, 54.

1.3 Роботи з проведення додаткової експертизи КЗЗ «Тайфун-Web» проводяться з метою оцінювання відповідності реалізованих в об'єкті експертизи функціональних послуг безпеки (далі – ФПБ) та рівня гарантій коректності їх реалізації вимогам НД ТЗІ 2.5-004-99 та технічного завдання, з урахуванням порядку реалізації цих вимог, викладеного у проектній документації.

КЗЗ «Тайфун-Web» в 2011 році пройшов державну експертизу в сфері ТЗІ, за результатами якої отримав експертний висновок № 336 від 29.12.2011. За час дії зазначеного експертного висновку розробником КЗЗ «Тайфун-Web» було доопрацьовано бібліотеку процедур КЗІ «Тайфун-РКІ PKCS#11», а саме окрім 32-бітної версії, додатково розроблено 64-у бітну версію. Оновлена бібліотека процедур КЗІ «Тайфун-РКІ PKCS#11» версії 1.02 пройшла державну експертизу в сфері КЗІ, за результатами якої отримала відповідний позитивний експертний висновок (№ 05/02/02-550 від 18.02.2014).

1.4 Додаткова державна експертиза в сфері технічного захисту інформації КЗЗ «Тайфун-Web» проводиться Інститутом спеціального зв'язку та захисту інформації НТУУ «КПІ» на виконання рішення Експертної ради з питань державної експертизи в сфері технічного захисту інформації Адміністрації Держспецзв'язку (протокол засідання від 29.12.2014 № 18-2014).

1.5 Замовник експертизи: ТОВ "Інститут комп'ютерних технологій", 03151, м. Київ, пр-т Повітрофлотський, 54.

1.6 Організатор експертизи: Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ», 01011, м. Київ, вул. Московська, 45/1.

## 2 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОБ'ЄКТА ЕКСПЕРТИЗИ

2.1 КЗЗ «Тайфун-Web» призначений для захисту інформаційних ресурсів (що містять як відкриту інформацію, так і інформацію з обмеженим доступом), оброблюваних у розподілених інформаційно-телекомунікаційних системах (ІТС), побудованих за клієнт-серверною архітектурою з використанням Web-технологій, у яких для взаємодії між серверними та клієнтськими застосуваннями використовується протокол HTTP.

2.2 КЗЗ «Тайфун-Web» реалізує такі основні функції захисту:

- ідентифікацію та автентифікацію користувачів комплексу на основі атрибутів, отриманих від операційної системи (ОС), що дозволяє однозначно встановити певного користувача та у подальшому коректно оброблювати його запити на доступ до захищеної інформації або до засобів адміністрування;

- виділення, на підставі результатів виконаної автентифікації, користувачів-адміністраторів, яким надані повноваження із керування засобами комплексу;

- взаємну автентифікацію клієнтської та серверної компонентів комплексу та їхніх користувачів з використанням відповідних протоколів, у яких використовується механізм вироблення/ перевірки електронного цифрового підпису за алгоритмом, установленим ДСТУ 4145-2002, з використанням відповідних атрибутів (особистих ключів (ОК) та сертифікатів відкритих ключів (ВК) відповідних користувачів);

- керування доступом користувачів до захищених **Web**-ресурсів (окремих **Web**-сторінок та їх сукупностей), представлених відповідними **URL**-адресами, на основі атрибутів доступу, призначених спеціально вповноваженими адміністраторами;

- зашифрування/розшифрування інформації, що передається між **Web**-браузером (або **Web**-застосуванням), який функціонує на робочій станції (PC) користувача, та захищеним **Web**-сервером (**Proxy**-сервером), що забезпечує захист конфіденційності інформації на всьому шляху її передачі по каналах мережі **Internet**;

- контроль цілісності інформації, що передається між **Web**-браузером (**Web**-застосуванням), яке функціонує на PC користувача, та захищеним **Web**-сервером (**Proxy**-сервером), що забезпечує захист від її несанкціонованої модифікації на всьому шляху її передачі по мережі **Internet**;

- контроль цілісності та самотестування програмних засобів комплексу при старті та в процесі функціонування, що дозволяє забезпечити стійке функціонування засобів захисту та не допустити обробки повідомлень у випадку порушення працездатності;

- протоколювання критичних з погляду захищеності оброблюваної інформації подій у захищеному журналі ОС із забезпеченням можливості аналізу зареєстрованих даних аудита вповноваженими адміністраторами.

При використанні КЗЗ «Тайфун-**Web**» забезпечується:

- взаємна автентифікація (підтвердження справжності) клієнта та сервера за протоколом, побудованим із використанням несиметричних криптографічних алгоритмів;

- захист конфіденційності та цілісності інформації, що передається між клієнтом та сервером, з використанням алгоритмів симетричного зашифрування/розшифрування інформації та вироблення/перевіряння кодів автентифікації повідомлень;

- розмежування доступу користувачів до інформаційних ресурсів, представлених у вигляді статичних або динамічних **Web**-сторінок, що зберігаються та оброблюються на відповідних **Web**-серверах та потребують захисту (захищених **Web**-ресурсів).

**2.3** До складу КЗЗ «Тайфун-**Web**» входять такі функціональні компоненти (модулі), установлювані на серверах та PC користувачів:

- модуль обробки мережевого трафіка, інтегрований у стек протоколів ОС, що реалізують функції **Winsock**;

- модуль обробки мережевого трафіка, що підключається до **MS IIS** через інтерфейс **ISAPI**;

- модуль ініціалізації параметрів захищених з'єднань;

- модуль реалізації криптографічних протоколів;

- модуль адміністрування.

Модуль обробки мережевого трафіка, інтегрований у стек протоколів ОС,

що реалізують функції **Winsock**, реалізований у вигляді динамічної бібліотеки та функціонує:

- на PC користувачів, з яких з використанням стандартних **Web**-браузерів або з використанням спеціально розроблених **Web**-застосувань здійснюється доступ до захищених **Web**-ресурсів;

- на серверах, на яких розміщуються захищені **Web**-ресурси або через які забезпечується доступ за протоколом **HTTP** до захищених **Web**-ресурсів (захищених серверах), та на яких для забезпечення доступу до **Web**-ресурсів застосовуються програмні засоби серверів застосувань (**Web**-серверів, **Proxy**-серверів), що використовують для взаємодії з **Web**-браузерами клієнтів функції **Winsock**.

Модуль обробки мережевого трафіка, що підключається до **MS IIS** через інтерфейс **ISAPI**, реалізований у вигляді динамічної бібліотеки та функціонує на захищених серверах, на яких для забезпечення доступу до захищених **Web**-ресурсів застосовуються програмні засоби **MS IIS** версії **6.0** та вище.

Модуль ініціалізації параметрів захищених з'єднань реалізований у вигляді системного сервісу та функціонує на всіх захищених серверах і PC користувачів.

Модуль реалізації криптографічних протоколів реалізований у вигляді динамічної бібліотеки та функціонує на всіх захищених серверах і PC користувачів.

Модуль адміністрування реалізований у вигляді інтерактивного багатовіконного застосування та функціонує на всіх захищених серверах і PC користувачів.

**2.4** Для виконання криптографічних перетворень у **K33 «Тайфун-Web»** (у модулі реалізації криптографічних протоколів) використовується бібліотека процедур криптографічного захисту інформації (**K3I**) «Тайфун-РКІ **PKCS#11**» версії **1.02**, яка має експертний висновок за результатами державної експертизи в сфері **K3I** щодо можливості використання з метою генерації ключів та шифрування інформації з обмеженим доступом (крім інформації, що становить державну таємницю, та службової інформації), а також інформації, вимогу щодо захисту якої встановлено законом (**№ 05/02/02-550** від **18.02.2014**).

Для керування ключовою інформацією (для вироблення **OK** та **BK** користувачів) у **K33 «Тайфун-Web»** (у модулі адміністрування) використовуються програмні засоби генерації ключів та обслуговування сертифікатів користувачів комплексу «Тайфун-РКІ» версії **1.02**, які мають експертний висновок за результатами державної експертизи в сфері **K3I** щодо можливості використання для побудови акредитованих центрів сертифікації ключів (**№ 05/02/02-4680** від **10.12.2014**).

Як зовнішні засоби керування ключовою інформацією комплексу «Тайфун-**Web**», у яких здійснюється вироблення сертифікатів **BK** користувачів, можуть використовуватися програмні засоби автоматизованих робочих місць центра реєстрації та центра сертифікації комплексу «Тайфун-РКІ» версії **1.02** або будь-які інші засоби керування сертифікатами, що реалізують чинні технічні вимоги до форматів представлення базових об'єктів національної системи електронного цифрового підпису.

**2.5** Програмні засоби **K33 «Тайфун-Web»** функціонують на **IBM**-сумісних комп'ютерах (робочих станціях користувачів, **Web**-серверах, **Proxy**-серверах) в операційних системах (ОС) **Windows 2000 / XP / 2003 / Vista / 7 / 8 / Server 2008 /**

**Server 2012.** Програмні засоби комплексу сумісні з **MS Internet Information Services (IIS)** версії **6.0** та вище. При використанні засобів комплексу на **Proху-серверах**, жодних обмежень щодо ОС **Web-серверів**, на яких зберігаються та оброблюються захищені **Web-ресурси**, не висувається.

**2.6** КЗЗ «Тайфун-Web» реалізує такий функціональний профіль захищеності: {КА-2, КВ-2, ЦА-1, ЦВ-2, ДС-1, ДЗ-1, ДВ-1, НР-1, НИ-1, НО-1, НЦ-1, НТ-2, НВ-2}. Позначення та зміст послуг та їх рівнів відповідають НД ТЗІ 2.5-004-99.

**2.7** Деталізовані вимоги щодо політики функціональних послуг безпеки та механізмів захисту, реалізованих у КЗЗ «Тайфун-Web», визначені в документі «Технічні вимоги, на відповідність яким здійснюватиметься експертиза комплексу засобів захисту **Web-ресурсів** від несанкціонованого доступу «Тайфун-Web» версії 1» (№ 25/3-2580 від 09.11.2011).

### **3 ВИМОГИ НОРМАТИВНИХ ДОКУМЕНТІВ З ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, НА ВІДПОВІДНІСТЬ ЯКИМ ЗДІЙСНЮЄТЬСЯ ОЦІНКА ОБ'ЄКТА ЕКСПЕРТИЗИ**

Експертні роботи здійснювалися на відповідність наступним нормативним документам із технічного захисту інформації:

- Комплекс засобів захисту **Web-ресурсів** від несанкціонованого доступу «Тайфун-Web». Версія 1. Технічне завдання UA.21541987.00019-01 90 01, погоджене із Адміністрацією Держспецзв'язку;

- Технічні вимоги, на відповідність яким здійснюватиметься експертиза комплексу засобів захисту **Web-ресурсів** від несанкціонованого доступу «Тайфун-Web» версії 1 (№ 25/3-2580 від 09.11.2011);

- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

- НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

### **4 НАЗВА ОКРЕМОЇ МЕТОДИКИ, ЗГІДНО З ЯКОЮ ЗДІЙСНЮВАЛАСЯ ОЦІНКА ОБ'ЄКТА ЕКСПЕРТИЗИ, КИМ РОЗРОБЛЕНА ТА ЗАТВЕРДЖЕНА, РЕЄСТРАЦІЙНИЙ НОМЕР ТА ДАТА ЗАТВЕРДЖЕННЯ**

КЗЗ «Тайфун-Web» в 2011 році проходив державну експертизу в сфері ТЗІ, за результатами якої отримав експертний висновок № 336 від 29.12.2011. За час дії зазначеного експертного висновку розробником КЗЗ «Тайфун-Web» було доопрацьовано бібліотеку процедур КЗІ «Тайфун-РКІ РКCS#11», а саме окрім 32-бітної версії, додатково розроблено 64-у бітну версію. Оновлена бібліотека процедур КЗІ «Тайфун-РКІ РКCS#11» версії 1.02 пройшла державну експертизу в сфері КЗІ, за результатами якої отримала відповідний позитивний експертний висновок (№ 05/02/02-550 від 18.02.2014). Враховуючи, що інших змін до складу КЗЗ «Тайфун-Web» внесено не було, експертні випробування КЗЗ «Тайфун-Web» проводились згідно розроблених під час первинної експертизи «Програми державної експертизи у сфері технічного захисту інформації комплексу засобів

захисту Web-ресурсів від несанкціонованого доступу «Тайфун-Web» (№ 25/3-2175 від 19.09.2011) та «Методики державної експертизи у сфері технічного захисту інформації комплексу засобів захисту Web-ресурсів від несанкціонованого доступу «Тайфун-Web» (№ 25/3-2176 від 19.09.2011), які погоджені із Департаментом з питань захисту інформації в інформаційно-телекомунікаційних системах Адміністрації Держспецзв'язку встановленим порядком.

## 5 ПЕРЕЛІК ДОКУМЕНТІВ І СПЕЦИФІКАЦІЇ ПРОГРАМНИХ ТА ТЕХНІЧНИХ ЗАСОБІВ, ЯКІ НАДАНО ЗАМОВНИКОМ ОРГАНІЗАТОРУ ЕКСПЕРТИЗИ

Для проведення досліджень надано дистрибутивний пакет КЗЗ «Тайфун-Web» згідно специфікації UA.21541987.00019 – 01. Уміст інсталяційного CD-ROM КЗЗ «Тайфун-Web» версії 1.02, наданого для виконання робіт, наведено нижче.

*Уміст кореневого каталогу:*

**DOC** – каталог із файлами експлуатаційної документації;

**PT\_UCGS** – інсталяційний пакет програмних засобів генерації ключів та обслуговування сертифікатів користувачів комплексу програмних засобів реалізації інфраструктури відкритих ключів «Тайфун-РКІ»;

**tfnwebi.exe** – програма інсталяції;

**tfnwebi.ini** – файл налаштувань програми інсталяції.

*Уміст каталогу Doc:*

**T\_PKI** – каталог із файлами експлуатаційної документації програмних засобів генерації ключів та обслуговування сертифікатів користувачів комплексу програмних засобів реалізації інфраструктури відкритих ключів «Тайфун-РКІ»;

**Tfn\_Web\_OP\_r4.pdf** – файл з документом «Опис комплексу»;

**Tfn\_Web\_RUE\_r4.pdf** – файл з документом «Настанова з встановлення та експлуатації».

Склад інсталяційного пакету КЗЗ «Тайфун-Web» версії 1.02, наданого для виконання робіт:

Ім'я файлу	Опис	Розмір, байт	Дата, час створення
TFNWEBI.EXE	Модуль інсталяції	10883035	2014-08-13, 13:57
TFNWEB.IMM	Файл кодів контролю цілісності комплексу	722	2014-07-25, 09:31
TFN_ARM.EXE	Модуль адміністрування	487424	2014-07-24, 14:54
TFNSRV.EXE	Модуль ініціалізації параметрів захищених з'єднань	151552	2013-02-05, 16:16
TFNCRYPTSRV.EXE	Резидентна частина модуля реалізації криптографічних протоколів	61440	2014-07-23, 15:41
TFNLSPDLL.DLL	Модуль обробки мережевого трафіка (Winsock) для 32-розрядних ОС	245760	2014-07-11, 15:08
TFNLSPDLL_X64.DLL	Модуль обробки мережевого трафіка (Winsock) для 64-розрядних ОС	422912	2014-07-24, 10:03
TFN_ISAPI.DLL	Модуль обробки мережевого трафіка (ISAPI) для 32-розрядних ОС	241664	2014-07-25, 09:21
TFN_ISAPI_X64.DLL	Модуль обробки мережевого трафіка (ISAPI) для 64-розрядних ОС	393728	2014-07-23, 15:43

Ім'я файлу	Опис	Розмір, байт	Дата, час створення
TFN_BA.DLL	Засоби взаємодії з модулем ініціалізації параметрів захищених з'єднань для 32-розрядних ОС	106496	2013-01-28, 11:44
TFN_BA_X64.DLL	Засоби взаємодії з модулем ініціалізації параметрів захищених з'єднань для 64-розрядних ОС	130560	2014-07-14, 09:31
TFN_IPK.DLL	Засоби взаємодії модуля адміністрування з бібліотекою процедур КЗІ "Тайфун-РКІ PKCS#11"	86016	2013-04-23, 11:54
TFNLOG.DLL	Бібліотека ресурсів повідомлень, що заносяться у протоколи реєстрації модулем адміністрування та модулями обробки мережевого трафіка	16384	2010-12-24, 11:30
TFNCRYPT.DLL	Засоби реалізації криптографічних протоколів модуля реалізації криптографічних протоколів для 32-розрядних ОС	102400	2014-07-24, 12:27
TFNCRYPT_X64.DLL	Засоби реалізації криптографічних протоколів модуля реалізації криптографічних протоколів для 64-розрядних ОС	100864	2014-07-24, 12:27
PKD_HM.DLL	Модуль верхнього рівня керування взаємодією з НКІ різного типу	40960	2010-11-29, 18:30
PKD_LM01.DLL	Модуль нижнього рівня керування взаємодією з НКІ типу "знімні файлові носії"	65536	2012-11-15, 10:04
PKD_LM02.DLL	Модуль нижнього рівня керування взаємодією з НКІ типу "eToken PRO"	36864	2010-11-29, 18:30
PKD_LM03.DLL	Модуль нижнього рівня керування взаємодією з НКІ типу "Secure Token 318"	45056	2010-11-29, 18:30
PKD_LM04.DLL	Модуль нижнього рівня керування взаємодією з НКІ типу "Кристал-1"	61440	2011-05-31, 09:27
PKD_LM05.DLL	Модуль нижнього рівня керування взаємодією з НКІ типу "Secure Token 337"	57344	2014-02-18, 14:39
TFN_PKI_PKCS11.DLL	Головний модуль бібліотеки процедур КЗІ "Тайфун-РКІ PKCS#11" для 32-розрядних ОС	253952	2013-09-03, 16:26
TFN_PKI_PKCS11.IMM	Файл кодів контролю цілісності бібліотеки процедур КЗІ "Тайфун-РКІ PKCS#11"	245	2014-01-28, 15:16
PKISUPP3.DLL	Допоміжний модуль формування/розбирання наборів даних в кодуванні ASN.1 бібліотеки процедур КЗІ "Тайфун-РКІ PKCS#11" для 32-розрядних ОС	315392	2014-01-17, 15:22
AUTHPKI.DLL	Інтерфейсний модуль доступу до сховища бази даних сертифікатів відкритих ключів, яке зберігається у вигляді набору TPS-файлів у каталогах файлової системи, бібліотеки процедур КЗІ "Тайфун-РКІ PKCS#11"	81920	2010-11-29, 18:30
TLICENCE.DLL	Модуль контролю ліцензійної інформації бібліотеки процедур КЗІ "Тайфун-РКІ PKCS#11" для 32-розрядних ОС	69632	2010-11-29, 18:30
CSK_TOKEN_C.DLL	Допоміжний модуль керування доступом до сховищ бази даних сертифікатів відкритих ключів бібліотеки процедур КЗІ "Тайфун-РКІ PKCS#11" для 32-розрядних ОС	159744	2013-07-18, 13:43

Ім'я файлу	Опис	Розмір, байт	Дата, час створення
PTOK_TPS.DLL	Допоміжний модуль доступу до сховища БД сертифікатів ВК, яке зберігається у вигляді набору TPS-файлів, бібліотеки процедур КЗІ "Тайфун-РКІ РКCS#11" для 32-розрядних ОС	1923584	2014-07-07, 16:14
TFN_PKI_PKCS11_X64.DLL	Головний модуль бібліотеки процедур КЗІ "Тайфун-РКІ РКCS#11" для 64-розрядних ОС	361472	2013-09-03, 16:48
PKISUPP3_X64.DLL	Допоміжний модуль формування/розбирання наборів даних в кодуванні ASN.1 бібліотеки процедур КЗІ "Тайфун-РКІ РКCS#11" для 64-розрядних ОС	423936	2014-01-17, 15:59
TLICENCE_X64.DLL	Модуль контролю ліцензійної інформації бібліотеки процедур КЗІ "Тайфун-РКІ РКCS#11" для 64-розрядних ОС	102400	2013-07-10, 13:56
CSK_TOKEN_C_X64.DLL	Допоміжний модуль керування доступом до сховищ бази даних сертифікатів відкритих ключів бібліотеки процедур КЗІ "Тайфун-РКІ РКCS#11" для 64-розрядних ОС	233984	2013-07-18, 15:27
PTOK_TPS_X64.DLL	Допоміжний модуль доступу до сховища БД сертифікатів ВК, яке зберігається у вигляді набору TPS-файлів, бібліотеки процедур КЗІ "Тайфун-РКІ РКCS#11" для 64-розрядних ОС	291840	2013-11-01, 13:07

Для проведення досліджень використано наступну документацію, надану замовником експертизи:

1. Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу "Тайфун-Web". Версія 1. Паспорт.
2. Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу "Тайфун-Web". Версія 1. Опис.
3. Комплекс средств защиты Web-ресурсов от несанкционированного доступа "Тайфун-Web". Версия 1. Руководство по установке и эксплуатации.
4. Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу "Тайфун-Web". Версія 1. Інструкція із забезпечення безпеки експлуатації засобів криптографічного захисту інформації.
5. Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу "Тайфун-Web". Версія 1. Інструкція щодо порядку генерації ключових даних та поводження з ключовими документами.
6. Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу "Тайфун-Web". Версія 1. Технічне завдання UA.21541987. 00019 - 01 90 01.
7. Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу "Тайфун-Web". Версія 1. Технічний проект UA.21541987. 00019 - 01 81 01.
8. Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу "Тайфун-Web". Версія 1. Опис відповідності специфікацій. Фрагменти вхідного коду UA.21541987. 00019 - 01 81 02.
9. Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу "Тайфун-Web". Версія 1. Опис методик діяльності розробників на протязі життєвого циклу UA.21541987. 00019 - 01 81 03.
10. Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу "Тайфун-Web". Версія 1. Специфікація UA.21541987. 00019.

11. Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу "Тайфун-Web". Версія 1. Програма та методика випробувань UA.21541987. 00019 - 01 51 01.

12. Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу "Тайфун-Web". Версія 1. Звіт про випробування UA.21541987. 00019 - 01 81 04.

13. Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу "Тайфун-Web". Версія 1. Протокол приймальних випробувань UA.21541987. 00019 - 01 81 05.

14. ТОВ «Інститут комп'ютерних технологій». Положення про порядок розроблення, впровадження та супроводження програмного забезпечення. Редакція від 14.07.2005.

15. Настанова з якості Товариства з обмеженою відповідальністю «Інститут комп'ютерних технологій».

## **6 РЕЗУЛЬТАТИ РОБІТ ЩОДО КОЖНОГО ПУНКТУ ОКРЕМОЇ МЕТОДИКИ ЕКСПЕРТИЗИ ОБ'ЄКТА**

6.1 Комплектність програмного КЗЗ «Тайфун-Web» відповідає специфікації.

6.2 КЗЗ «Тайфун-Web» забезпечує вирішення функціональних завдань згідно експлуатаційної документації.

6.3 Сукупність реалізованих у КЗЗ «Тайфун-Web» функцій та механізмів захисту інформації визначається згідно з НД ТЗІ 2.5-004-99 таким функціональним профілем: {КА-2, КВ-2, ЦА-1, ЦВ-2, ДС-1, ДЗ-1, ДВ-1, НР-1, НИ-1, НО-1, НЦ-1, НТ-2, НВ-2}.

6.4 За результатами експертизи встановлено, що:

- рівні реалізованих у КЗЗ «Тайфун-Web» функціональних послуг безпеки відповідають з рівнем гарантій Г-4 коректності їх реалізації вимогам НД ТЗІ 2.5-004;

- впроваджені виробником архітектура, середовище, процедура та послідовність розробки, процедури випробування та постачання відповідають специфікаціям рівня Г-4 гарантій коректності реалізації функціональних послуг безпеки згідно НД ТЗІ 2.5-004-99 та НД ТЗІ 3.6-001-2000;

- виробник розробив, запровадив і підтримує в робочому стані документально оформлені методики забезпечення фізичної, технічної, організаційної і кадрової безпеки;

- розроблена та впроваджена виробником система керування конфігурацією використовується для генерації КЗЗ «Тайфун-Web» з вихідного коду і обліку всіх змін з появою нових версій, а також здатна видавати звіти про стан елементів конфігурації;

- експлуатаційна документація на КЗЗ «Тайфун-Web» відповідає специфікаціям рівня Г-4 гарантій коректності реалізації функціональних послуг безпеки згідно НД ТЗІ 2.5-004-99.

6.5 Докладні висновки щодо відповідності об'єкта експертизи вимогам нормативних документів системи ТЗІ за результати експертних випробувань по кожному пункту методики державної експертизи у сфері технічного захисту інформації КЗЗ «Тайфун-Web» викладені в документі «Протокол виконання робіт відповідно до розділів 4, 5 методики державної експертизи у сфері технічного захисту інформації комплексу засобів захисту Web-ресурсів від несанкціонованого доступу «Тайфун-Web» (№ 25/03-27 від 12.01.2015). Відомості



протоколу свідчать, що зміст реалізованих функціональних послуг безпеки та їх рівні відповідають вимогам ТЗ та НД ТЗІ 2.5-004-99.

## **7 РОЗГОРНУТИЙ ВИСНОВОК ЩОДО ВІДПОВІДНОСТІ ОБ'ЄКТА ЕКСПЕРТИЗИ ВИМОГАМ НОРМАТИВНИХ ДОКУМЕНТІВ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ**

7.1 За результатами виконаних перевірок, що передбачені методикою державної експертизи у сфері технічного захисту інформації КЗЗ «Тайфун-Web», зроблено наступні висновки:

– впроваджені виробником архітектура, середовище, процедура та послідовність розробки, процедури випробування та постачання відповідають специфікаціям рівня Г-4 гарантій коректності реалізації функціональних послуг безпеки згідно НД ТЗІ 2.5-004-99 та НД ТЗІ 3.6-001-2000;

– КЗЗ «Тайфун-Web» відповідає вимогам ТЗ в обсязі реалізації функціонального профілю захищеності {КА-2, КВ-2, ЦА-1, ЦВ-2, ДС-1, ДЗ-1, ДВ-1, НР-1, НИ-1, НО-1, НЦ-1, НТ-2, НВ-2} згідно НД ТЗІ 2.5-004-99. Рівні реалізованих функціональних послуг безпеки відповідають з рівнем гарантій Г-4 коректності їх реалізації вимогам НД ТЗІ 2.5-004-99.

Особливості реалізації окремих із наведених функціональних послуг безпеки полягають в наступному:

– КЗЗ «Тайфун-Web» забезпечує (в рамках реалізації політики послуг КА-2, ЦА-1) керування доступом користувачів до захищених Web-ресурсів (окремих Web-сторінок та їх сукупностей), представлених відповідними URL-адресами, на основі атрибутів доступу, призначених спеціально вповноваженими адміністраторами;

– оскільки в процесі функціонування інформаційно-телекомунікаційної системи, в якій застосовується КЗЗ «Тайфун-Web», не передбачається можливість експорту або імпорту захищених Web-ресурсів (окремих Web-сторінок та їх сукупностей) за межі системи, у КЗЗ «Тайфун-Web» (в рамках реалізації політики послуг КА-2, ЦА-1) відсутні функціональні можливості із збереження атрибутів доступу відповідних об'єктів при їх імпорті або експорті;

– КЗЗ «Тайфун-Web» забезпечує (в рамках реалізації політики послуг КВ-2, ЦВ-2) шифрування та контроль цілісності інформації, що передається між Web-браузером (або Web-застосуванням), який функціонує на РС користувача, та захищеним Web-сервером (Proху-сервером), що забезпечує захист конфіденційності інформації та захист її від несанкціонованої модифікації на всьому шляху її передачі по каналах мережі Internet;

– КЗЗ «Тайфун-Web» забезпечує (в рамках реалізації політики послуги НВ-2) взаємну автентифікацію клієнтської та серверної компонентів комплексу та їхніх користувачів;

– для реалізації послуг КВ-2, ЦВ-2, НВ-2 використовується програмний виріб «Бібліотека процедур криптографічного захисту інформації «Тайфун-РКІ РКCS#11» версії 1.02, який має позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації щодо можливості використання з метою генерації ключів та шифрування інформації з обмеженим доступом (крім інформації, що становить державну таємницю, та службової інформації), а також інформації, вимогу щодо захисту якої встановлено законом;

– в рамках реалізації послуги НІ-1 в якості ідентифікатора користувача в КЗЗ «Тайфун-Web» використовується ідентифікатор користувача в операційній системі ЕОМ, на якій він встановлений, та однозначно зв'язаний із ним псевдонім користувача в каталозі користувачів цієї операційної системи;

– КЗЗ «Тайфун-Web» забезпечує (в рамках реалізації політики послуг НЦ-1, НТ-2) контроль цілісності та самотестування програмних засобів комплексу при старті та в процесі функціонування, що дозволяє забезпечити стійке функціонування засобів захисту та не допустити обробки повідомлень у випадку порушення працездатності; організаційно-технічні обмеження на використання КЗЗ «Тайфун-Web», які дозволяють гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ, наведені в розділі 8 цього документу;

– КЗЗ «Тайфун-Web» (в рамках реалізації політики послуги НР-1) забезпечує протоколювання критичних з погляду захищеності оброблюваної інформації подій у захищеному журналі ОС із забезпеченням можливості аналізу зареєстрованих даних аудита вповноваженими адміністраторами.

Деталізовані відомості щодо порядку та особливостей реалізації ФПБ в КЗЗ «Тайфун-Web» наведені в документі «Технічні вимоги, на відповідність яким здійснюватиметься експертиза комплексу засобів захисту Web-ресурсів від несанкціонованого доступу «Тайфун-Web» версії 1» (№ 25/3-2580 від 09.11.2011).

7.2 Вимоги до умов функціонування КЗЗ «Тайфун-Web» при його використанні для захисту службової інформації наведено у розділі 8 цього Експертного висновку.

7.3 Результати експертизи КЗЗ «Тайфун-Web» дійсні як для програмних засобів (ПЗ) КЗЗ «Тайфун-Web» версії 1.02, склад яких наведено в розділі 5 цього документа, так і для пакетів оновлення КЗЗ «Тайфун-Web» версій 1.xx, встановлення яких здійснюється з використанням засобів реалізації ФПБ «Модернізація» рівня ДЗ-1 (за умов проведення випробувань оновлених ПЗ за погодженою з Адміністрацією Держспецзв'язку України програмою та методикою приймальних випробувань «Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу «Тайфун-Web». Версія 1. Програма та методика випробувань UA.21541987.00019-01 51 01» та передачі до Адміністрації Держспецзв'язку України відповідного Протоколу випробувань).

## **8 СФЕРА ВИКОРИСТАННЯ (ВИМОГИ ДО УМОВ ЕКСПЛУАТАЦІЇ) ОБ'ЄКТА ЕКСПЕРТИЗИ**

8.1 Використання КЗЗ «Тайфун-Web» можливе лише за умови дотримання вимог та положень експлуатаційної документації, зокрема:

– забезпечується відповідність умов експлуатації КЗЗ «Тайфун-Web» вимогам експлуатаційної документації;

– забезпечується відповідність апаратного та програмного забезпечення, спільно з яким відбувається функціонування КЗЗ «Тайфун-Web», вимогам експлуатаційної документації;

– забезпечується відповідність конфігурування та керування компонентами КЗЗ «Тайфун-Web» вимогам, визначеним в експлуатаційній документації;

– забезпечується надійне збереження носіїв ключової інформації користувачів КЗЗ «Тайфун-Web» та паролів доступу до них.

**8.2** У випадку використання КЗЗ «Тайфун-Web» для захисту службової інформації повинні виконуватись наступні вимоги:

– до приміщень, у яких функціонують компоненти обчислювальної системи ІТС, на яких розгорнуто КЗЗ «Тайфун-Web», має бути організовано спеціальний режим доступу відповідно до вимог діючого законодавства з питань захисту службової інформації;

– для передачі даних між компонентами розподіленої ІТС мають використовуватись канали мережі передачі даних, які є захищеними відповідно до вимог діючого законодавства з питань технічного та криптографічного захисту інформації;

– доступ користувачів та технічного обслуговуючого персоналу до компонентів обчислювальної системи ІТС має контролюватися та обмежуватися відповідними організаційними та, за необхідності, технічними засобами.

## **9 ТЕРМІН ДІЇ ЕКСПЕРТНОГО ВИСНОВКУ**

Термін дії цього експертного висновку становить **3** роки за умови виконання вимог розділу **8** цього висновку.

Заступник начальника науково-дослідного центру

А.Л. Волошин