ІНСТИТУТ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу «Тайфун-Web»

Версія 1.02

Опис

Редакція 4

Київ 2014

ПЕРЕЛІК ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ВК – відкритий ключ

ЕІД – електронний ідентифікатор

ЕЦП – електронний цифровий підпис

ІТС – інформаційно-телекомунікаційна система

КЗІ – криптографічний захист інформації

ОК – особистий ключ

ПЗ ГКОСК – програмні засоби генерації ключів та обслуговування сертифікатів користувачів

РС – робоча станція

СКД – список керування доступом

ФПБ – функціональна послуга безпеки

HTTP – протокол передачі гіпертекстових сторінок

IIS - Internet Information Server

URL – уніфікований покажчик інформаційного ресурсу

ИНСТИТУТ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
e-mail: ict@ict.com.ua
http://www.ict.com.ua

ЗМІСТ

1 ПРИЗНАЧЕННЯ

Суттєва частина сучасних інформаційних систем (ІС) побудована на базі сучасних Web-технологій, які характеризуються такими ознаками:

- технічною основою побудови відповідних ІС є розподілені мережі, наприклад, Internet;
- інформаційні ресурси розташовуються та оброблюються на спеціальних серверах застосувань, доступ до яких здійснюється за протоколом HTTP (Web-серверах);
- для доступу до необхідних інформаційних ресурсів користувачі використовують спеціалізовані програми (Web-браузери);
- інформація з Web-серверів до Web-браузерів передається у вигляді гіпертекстових сторінок (Web-сторінок), які можуть бути як статичними, тобто, створеними заздалегідь, так і динамічними, тобто, створеними за запитом відповідного користувача.

У ІС, побудованих на базі Web-технологій, може оброблюватися як відкрита інформація, так і інформація з обмеженим доступом (конфіденційна інформація, вимоги до захисту якої встановлені законодавством, персональні дані тощо). При цьому найбільш небезпечними для інформації з обмеженим доступом є загрози порушення її конфіденційності (шляхом несанкціонованого доступу до відповідних даних, що зберігаються та оброблюються на серверах, або перехоплення відповідних повідомлень при передачі по каналам розподіленої мережі) та цілісності (шляхом несанкціонованої модифікації відповідних даних, що зберігаються та оброблюються на серверах, пошкодження, знищення або нав'язування хибних повідомлень при передачі по каналам розподіленої мережі). Забезпечення захисту від зазначених загроз вимагають також "Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах", затверджені постановою Кабінету Міністрів України від 29.03.2006 р. № 373.

Комплекс засобів захисту Web-ресурсів від несанкціонованого доступу «Тайфун-Web» призначений для криптографічного захисту та розмежування доступу до інформації, оброблюваної в ІС, побудованих на базі Web-технологій. Як приклади ІС, захист інформації в яких може забезпечуватися за допомогою комплексу «Тайфун-Web», можна навести:

- електронні платіжні системи типа "Internet Клієнт-Банк";
- загальнодержавні та/або відомчі банки даних (реєстри інформації), у яких міститься конфіденційна інформація та доступ до яких здійснюється з використанням каналів мережі Internet або інших розподілених мереж (реєстр втрачених паспортів Міністерства внутрішніх справ, реєстри кредитних історій, реєстри нерухомого майна, реєстри автотранспорту, реєстри абітурієнтів вищих навчальних закладів, реєстри облікових карток держслужбовців тощо);
- внутрішньокорпоративні Web-сайти територіально розподілених корпорацій, які не призначені для загального доступу;
- Web-сайти органів державної влади та місцевого самоврядування, адміністрування яких здійснюється за технологією Т2, визначеною НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу».

Реалізована технологія інтеграції серверної та клієнтської компонентів комплексу до стеку мережевих протоколів операційної системи (ОС), які реалізують функції Winsock, забезпечує незалежність від використовуваних Web-браузерів та Web-серверів. Для забезпечення сумісності із засобами MS Internet Information Server (IIS), в якому функції Winsock не використовуються, реалізована можливість підключення серверної компоненти комплексу безпосередньо до MS IIS через інтерфейс ISAPI.

При використанні комплексу «Тайфун-Web» забезпечується:

- взаємна сувора 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).

На відміну від вбудованих у ОС засобів забезпечення конфіденційності та цілісності інформації, що передається між клієнтом та сервером за протоколом HTTP (засобів протоколу SSL), у комплексі "Тайфун-Web" реалізовані лише дозволені для використання з метою захисту інформації з обмеженим доступом криптографічні алгоритмі та протоколи, а використовувані засоби криптографічного захисту інформації (КЗІ) мають позитивний експертний висновок за результатами державної експертизи в сфері КЗІ.

Програмні засоби комплексу функціонують на IBM-сумісних комп'ютерах (робочих станціях користувачів, Web-серверах, Proxy-серверах) в 32 та 64 розрядних ОС Windows XP/Vista/Server 2003/7/8/Server 2008/Server 2012. Програмні засоби комплексу сумісні з MS IIS версії 6.0 та вище. При використанні засобів комплексу на Proxy-серверах (рис. 1), жодних обмежень щодо ОС Web-серверів, на яких зберігаються та оброблюються захищені Web-ресурси, не висувається.

2 РЕАЛІЗОВАНІ ФУНКЦІЇ

Комплекс «Тайфун-Web» реалізує такі основні функції:

- ідентифікацію та автентифікацію користувачів комплексу на основі атрибутів, отриманих від 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;
- сувору взаємну автентифікацію клієнтської та серверної компонентів комплексу та їхніх користувачів з використанням відповідних протоколів, у яких використовується механізм вироблення/ перевірки електронного цифрового підпису (ЕЦП) за алгоритмом, установленим ДСТУ 4145, 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 (РС) 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 РС 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;
- можливість використання для збереження ОК користувачів, як незахищених (дискета, flash-drive і т.д.), так і захищених (пристрій eToken Pro виробництва Aladdin Knowledge Systems, Ізраїль; смарт-карта eToken Pro/SC; пристрій SecureToken виробництва компанії «Автор», Україна тощо) носіїв;
- можливість автоматичної та ручної перевірки наявності оновлень програмного забезпечення на ресурсах, вказаних уповноваженими адміністраторами; можливість завантаження наявних оновлень та проведення процесу оновлення комплексу;
- можливість завантаження документів користувачів (у т.ч. сертифікатів ВК користувачів, списків відкликаних сертифікатів) з вказаних уповноваженими адміністраторами ресурсів;
- можливість передачі документів користувачів (у т.ч. сертифікатів ВК користувачів, списків відкликаних сертифікатів) на вказані уповноваженими адміністраторами ресурси.

3 СКЛАД КОМПЛЕКСУ

До складу комплексу входять такі функціональні компоненти (модулі), установлювані на серверах та РС користувачів (рис. 1):

- 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 РС 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 розміщаються 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 РС користувачів.

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

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

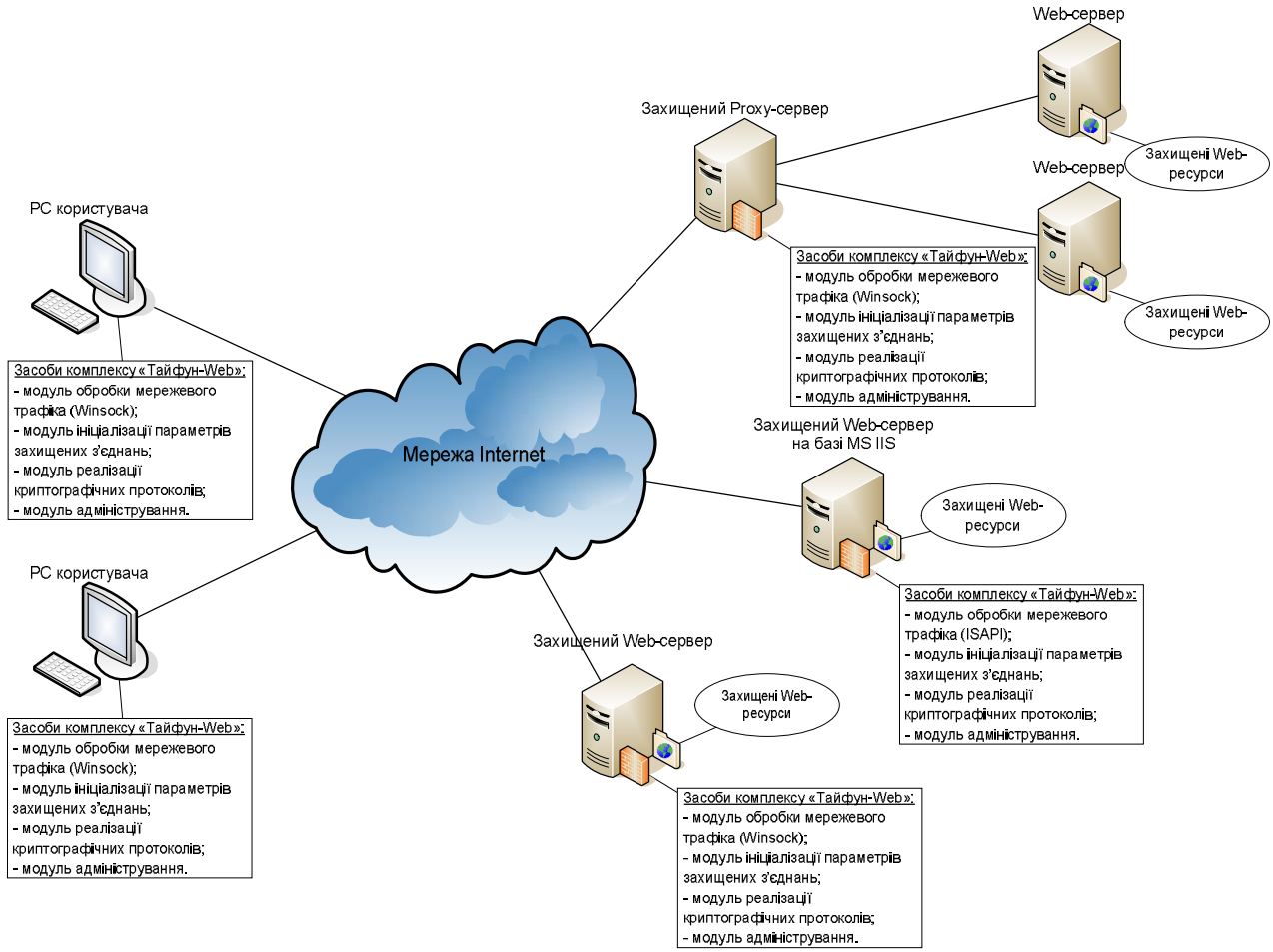

Рис. 1 Склад і архітектура комплексу «Тайфун-Web»

Для виконання криптографічних перетворень у комплексі «Тайфун-Web» (у модулі реалізації криптографічних протоколів) використовується бібліотека процедур КЗІ «Тайфун-PKI PKCS#11», Експертний висновок про відповідність вимогам діючих нормативних документів у сфері КЗІ № 05/02/02-550 від 18.02.2014 р.

Для керування ключовою інформацією (для вироблення ОК та ВК користувачів) у комплексі «Тайфун-Web» (у модулі адміністрування) використовуються програмні засоби генерації ключів та обслуговування сертифікатів користувачів (ПЗ ГКОСК) комплексу «Тайфун-PKI», Експертний висновок про відповідність вимогам діючих нормативних документів у сфері КЗІ № 5/ 1-4854 від 31.07.2009 р.

Як зовнішні засоби керування ключовою інформацією комплексу «Тайфун-Web», у яких здійснюється вироблення сертифікатів ВК користувачів, можуть використовуватися програмні засоби автоматизованих робочих місць центра реєстрації та центра сертифікації комплексу «Тайфун-PKI» або будь-які інші засоби керування сертифікатами, які реалізують вимоги до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису, затверджені наказом Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 1236/5/453 від 20.08.2012 р.

4 ФУНКЦІОНАЛЬНИЙ ПРОФІЛЬ І РІВЕНЬ ГАРАНТІЙ

У термінах НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» комплексу «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}.

Розробка комплексу виконана відповідно до вимог до рівня Г-4 гарантій коректності реалізації функціональних послуг безпеки, установлених НД ТЗІ 2.5-004-99.

5 РЕАЛІЗОВАНА ПОЛІТИКА БЕЗПЕКИ

5.1 Концепція

Розмежування доступу користувачів комплексу до захищених Web-ресурсів здійснюється відповідно до концепції диспетчера доступу. Відповідно до цієї концепції, засобами комплексу «Тайфун-Web» виділяються та підтримуються:

Об'єкти-користувачі – користувачі, які намагається одержати доступ до захищених Web-ресурсам.

Об'єкти-процеси – породжувані користувачами процеси, які використовуються для доступу до інформації, що міститься у захищених Web-ресурсах, та її представлення в придатному для сприйняття користувачем вигляді.

Пасивні об'єкти – пасивні джерела/приймачі інформації, що міститься у захищених Web-ресурсах.

База даних авторизації – службова інформація, що визначає права доступу (атрибути доступу) об'єктів-користувачів до об'єктів-процесів та пасивних об'єктів.

База даних реєстрації – службова інформація про результати обробки запитів об'єктів-користувачів на надання доступу до об'єктів-процесів і пасивних об'єктів.

Диспетчер доступу – сукупність засобів комплексу, які реалізують функції керування доступом і забезпечують захист інформації шляхом керування створенням об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів, надання об'єктам-користувачам доступу до об'єктів-процесів і пасивних об'єктів на підставі перевірки відповідності атрибутів доступу користувачів, що ініціюють запит на доступ, та даних авторизації, що зберігаються в базі даних (БД) авторизації, з виконанням при цьому реєстрації подій у БД реєстрації.

У комплексі «Тайфун-Web» реалізоване адміністративне керування доступом. Це означає, що керування потоками інформації між користувачами, процесами та об'єктами здійснюють тільки спеціально авторизовані користувачі (адміністратори). Звичайні користувачі змінювати права доступу користувачів до процесів і пасивних об'єктів, а також виконувати будь-які інші функції керування засобами комплексу не можуть.

5.2 Об'єкти-користувачі

Відповідно із реалізованою засобами комплексом політикою безпеки, об'єкти-користувачі діляться на уповноважених керувати засобами захисту (адміністраторів) та звичайних користувачів. Користувачі комплексу характеризуються такими атрибутами:

- ідентифікатор облікового запису користувача в ОС і відповідний до нього псевдонім користувача в ОС;
- ОК користувача;

- ВК користувача у вигляді відповідного сертифіката, однозначно зв'язаний із ОК користувача;
- електронний ідентифікатор (ЕІД) користувача, що міститься в сертифікаті ВК користувача та однозначно зв'язаний із псевдонімом користувача в ОС;
- роль користувача, обумовлена фактом включення облікового запису користувача в групу ОС із адміністративними повноваженнями.

5.3 Об'єкти-процеси й пасивні об'єкти

Відповідно до реалізованою засобами комплексу політикою безпеки, об'єктами-процесами є функціональні режими Web-застосувань, а пасивними об'єктами - Web-сторінки, що містять захищену інформації. Оскільки при використанні Web-технологій доступ як до функціональних режимів Web-застосувань, так і до захищених Web-сторінок здійснюється ідентично, обидва ці типи об'єктів характеризуються такими атрибутами:

- ідентифікатор об'єкта або групи об'єктів (URL-адреса відповідної Web-сторінки або старша частина URL-адреси групи Web-сторінок);
- список керування доступом (СКД) до об'єкта або групи об'єктів у вигляді набору елементів, що містять:
  - ЕІД користувачів, які мають права доступу до об'єкта або групи об'єктів;
  - ознаки надання даному користувачеві прав доступу з метою читання об'єкта (дозвіл на доступ до Web-сторінки з використанням методів GET, HEAD, OPTIONS протоколу HTTP) або читання й модифікації об'єкта (дозвіл на доступ до Web-сторінки з використанням довільних методів протоколу HTTP).

5.4 Правила розмежування доступу, функціональні послуги безпеки та механізми захисту

Перед початком роботи користувач входить в ОС РС користувача або захищеного сервера під призначеним йому псевдонімом, після чого засобами ОС виконується його автентифікація (наприклад, шляхом уведення відповідного пароля). Після успішної автентифікації засобами ОС у випадку, якщо користувач входить у групу користувачів ОС із адміністративними повноваженнями, він одержує можливість за допомогою модуля адміністрування вносити зміни в БД авторизації, а саме:

- налаштовувати параметри конфігурації засобів комплексу на РС користувача або захищеному сервері;
- на РС користувача - визначати, доступ до яких серверів повинен здійснюватися в захищеному режимі, указувати, який сертифікат ВК сервера з яким ЕІД користувача повинен використовуватися в процедурі взаємної автентифікації клієнтського та серверного компонентів комплексу та їхніх користувачів;
- на захищеному сервері - визначати, доступ до яких Web-ресурсів повинен здійснюватися у захищеному режимі, задавати СКД для відповідних об'єктів (Web-сторінок або груп Web-сторінок), указуючи, власники сертифікатів ВК з якими ЕІД користувачів повинні мати доступ до відповідних об'єктів з метою читання або читання та модифікації.

У такий спосіб засобами комплексу реалізується функціональна послуга безпеки (ФПБ) «Розмежування обов'язків» рівня НО-1.

Після успішної автентифікації засобами ОС у випадку, якщо необхідно одержати доступ до захищених Web-ресурсів, користувач, з використанням модуля адміністрування, завантажує свій ОК із наявного в нього носія. ОК та відповідний до нього сертифікат ВК

повинні однозначно (за заданими адміністратором правилами відповідності ЕІД користувача, що міститься в сертифікаті ВК користувача, його псевдоніму в ОС) відповідати псевдоніму користувача в ОС, інакше виконати завантаження ОК буде неможливо. У такий спосіб засобами комплексу реалізується ФПБ «Ідентифікація та автентифікація» рівня НИ-1.

Для одержання доступу до захищеного Web-ресурсу користувач за допомогою Web-браузера або спеціалізованого Web-застосування ініціює запит доступу до відповідного сервера із зазначенням відповідного URL. Сформований запит обробляється засобами комплексу (модулем обробки мережевого трафіка). У випадку, якщо доступ до запитуваного сервера повинен здійснюватися в захищеному режимі (перевірка виконується на підставі даних, що містяться в БД авторизації), з використанням ОК користувача - ініціатора запиту та ВК сервера, що міститься в його сертифікаті ВК, за допомогою модуля реалізації криптографічних протоколів формується та за допомогою модуля обробки мережевого трафіка передається на сервер початковий запит протоколу взаємної автентифікації. У складі переданого запиту, у тому числі, міститься ключова інформація. необхідна для вироблення на стороні сервера симетричного ключа зашифрування/розшифрування даних. Прийнятий на сервері модулем обробки мережевого трафіка початковий запит протоколу взаємної автентифікації обробляється модулем реалізації криптографічних протоколів. У випадку, якщо цілісність та автентичність початкового запиту автентифікації підтверджена (перевірка цілісності здійснюється з використанням механізму перевірки ЕЦП запиту), а відповідному користувачеві дозволений доступ до захищеного сервера (перевірка виконується з використанням атрибутів, що містяться в БД авторизації), з використанням ОК сервера та ВК користувача – ініціатора запиту, що міститься у його сертифікаті ВК, за допомогою модуля реалізації криптографічних протоколів формується та за допомогою модуля обробки мережевого трафіка передається на РС користувача запит-відповідь протоколу взаємної автентифікації. У складі переданого запиту-відповіді, у тому числі, міститься ключова інформація, необхідна для вироблення на стороні клієнта симетричного ключа зашифрування/розшифрування даних. Прийнятий на РС користувача модулем обробки мережевого трафіка запит-відповідь протоколу взаємної автентифікації обробляється модулем реалізації криптографічних протоколів. У випадку, якщо цілісність і автентичність запиту-відповіді протоколу взаємної автентифікації підтверджена (перевірка цілісності здійснюється з використанням механізму перевірки ЕЦП запиту), виконання протоколу взаємної автентифікації вважається успішним, а на основі прийнятих ключових даних на обох сторонах взаємодії формуються симетричні ключі зашифрування/розшифрування даних, які зберігаються в модулі ініціалізації параметрів захищених з'єднань протягом усього сеансу взаємодії. У такий спосіб засобами комплексу реалізується ФПБ «Ідентифікація та автентифікація при обміні» рівня НВ-2.

Після завершення процедури взаємної автентифікації для одержання доступу до захищеного Web-ресурсу користувач за допомогою Web-браузера або спеціалізованого Web-застосування ініціює запит доступу до відповідного сервера із зазначенням відповідного URL. Сформований запит (запит HTTP-протоколу) обробляється засобами комплексу (модулем обробки мережевого трафіка), для всіх даних, що містяться у запиті, у модулі реалізації криптографічних протоколів виробляється код автентифікації повідомлення (імітовставка за ГОСТ 28147), усі дані, що містяться в запиті, зашифровуються в режимі гамування за ГОСТ 28147, після чого формується захищений запит HTTP-протоколу. При цьому використовуються атрибути захищеного сеансу (ключ зашифрування/розшифрування), вироблені при виконанні процедури взаємної автентифікації. За допомогою модуля обробки мережевого трафіка захищений запит HTTP-протоколу передається на сервер. Прийнятий на сервері модулем обробки мережевого трафіка захищений запит HTTP-протоколу розшифровується модулем реалізації криптографічних протоколів, з використанням обчисленого коду автентифікації повідомлення виконується перевірка його цілісності. У випадку, якщо цілісність захищеного

запита HTTP-протоколу підтверджена, а відповідному користувачеві дозволений доступ до захищеного Web-ресурсу з використанням відповідного методу протоколу HTTP (перевірка виконується з використанням атрибутів, що містяться в БД авторизації), розшифрований запит HTTP-протоколу передається для подальшої обробки в Web-сервер. Аналогічним образом здійснюється обробка повідомлень-відповідей HTTP-протоколу. У такий спосіб засобами комплексу реалізуються ФПБ «Конфіденційність при обміні» рівня КВ-2, «Цілісність при обміні» рівня ЦВ-2, «Адміністративна конфіденційність» рівня КА-2 і «Адміністративна цілісність» рівня ЦА-1.

У процесі функціонування комплексу інформація про всі події, критичні з погляду захищеності оброблюваної інформації (дані аудита), реєструються в захищеному журналі ОС (журналі застосувань). Користувачі ОС із адміністративними повноваженнями (адміністратори) мають можливість аналізу зареєстрованих даних аудита з використанням штатних засобів ОС. У такий спосіб засобами комплексу реалізується ФПБ «Реєстрація» рівня НР-1.

Крім зазначених вище, комплекс реалізує обов'язкову з погляду НД ТЗІ 2.5-004-99 ФБП «Цілісність комплексу засобів захисту» рівня НЦ-1, а також ряд ФПБ, спрямованих на забезпечення сталої роботи: «Стійкість до відмов» рівня ДС-1, «Гаряча заміна» рівня ДЗ-1, «Відновлення після збоїв» рівня ДВ-1 та «Самотестування» рівня НТ-2.

6 КОМПЛЕКТ ПОСТАВКИ

У стандартний комплект поставки входить виконуваний модуль програми інсталяції TFNWEBI.EXE з програмним забезпеченням комплексу, файл із ліцензійною інформацію бібліотеки процедур КЗІ TLICENCE.DAT, файл індивідуальних настроювань параметрів комплексу на певній РС користувача TFNWEBI.INI, експлуатаційна документація в електронному вигляді (опис комплексу, настанова із встановлення та експлуатації). Також у комплект поставки входить інсталяційний пакет ПЗ ГКОСК комплексу програмних засобів реалізації інфраструктури відкритих ключів «Тайфун-PKI» та експлуатаційна документація ПЗ ГКОСК в електронному вигляді (Настанова з встановлення та експлуатації).