НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу

Департамент спеціальних телекомунікаційних систем та захисту інформації
Служби безпеки України

Київ 2003

НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Затверджено
наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України
від “ 02 “ квітня 2003 р. № 33
із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806

Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу

НД ТЗІ 2.5-010-03

ДСТСЗІ СБ України

Київ

Передмова

1 РОЗРОБЛЕНО і ВНЕСЕНО Головним управлінням технічного захисту інформації Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

2 ВВЕДЕНО ВПЕРШЕ

Зміст

НД ТЗІ 2.5-010-03
Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу

Чинний від 2003-04-15

1 Галузь використання

Цей нормативний документ системи технічного захисту інформації (НД ТЗІ) встановлює вимоги до технічних та організаційних заходів захисту інформації WEB-сторінки в мережі Інтернет.

Згідно з визначеними НД ТЗІ 2.5-004-99 специфікаціями він встановлює мінімально необхідний перелік послуг безпеки інформації та рівнів їх реалізації у комплексах засобів захисту інформації WEB-сторінки від несанкціонованого доступу.

Мета цього НД ТЗІ – надання нормативно-методологічної бази для розроблення комплексу засобів захисту від несанкціонованого доступу до інформації WEB-сторінки під час створення комплексної системи захисту інформації.

Цей НД ТЗІ призначений для суб'єктів відносин (власників або розпорядників WEB-сторінки, операторів (провайдерів), користувачів), діяльність яких пов'язана з розробкою та експлуатацією WEB-сторінки, розробників комплексної системи захисту інформації та постачальників окремих її компонентів, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності WEB-сторінки на відповідність вимогам ТЗІ.

Встановлені цим НД ТЗІ вимоги є обов'язковими для виконання державними органами, Збройними Силами України, іншими військовими формуваннями, утвореними відповідно до законів України, Радою Міністрів Автономної республіки Крим та органами місцевого самоврядування, а також підприємствами, установами та організаціями (далі - установи) усіх форм власності під час захисту інформації, що належить до державних інформаційних ресурсів на WEB-сторінках.

Для захисту інших видів інформації власники WEB-сторінок користуються цим НД ТЗІ на власний розсуд.

2 Нормативні посилання

У цьому НД ТЗІ наведено посилання на такі нормативні документи:

Положення про державну експертизу в сфері технічного захисту інформації. Затверджене наказом Адміністрації Державної служби спеціального зв'язку тп захисту інформації України від 16.05.2007 № 93, зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087;

НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі;

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

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

3 Визначення

У цьому НД ТЗІ використовуються терміни та визначення, що відповідають встановленим ДСТУ 2226 та НД ТЗІ 1.1-003.

Інші терміни, ужиті в цьому НД ТЗІ, мають такі значення:

Інтернет (мережа Інтернет) – сукупність мереж та обчислювальних засобів, які використовують стек протоколів TCP/IP (Transport Control Protocol/Internet Protocol), спільний простір імен та адрес для забезпечення доступу до інформаційних ресурсів мережі будь-якій особі;

Оператор (провайдер, provider) – юридична або фізична особа, яка надає користувачам доступ до мережі Інтернет;

Броузер (browser) – програмне забезпечення, що надає інтерфейс для доступу до інформації WEB-сторінок та їх перегляду;

Робоча станція (клієнт мережі) – окрема (персональна) ЕОМ або віддалений термінал мережі, з яких користувачі отримують доступ до ресурсів мережі Інтернет;

Сервер (server) – об'єкт комп'ютерної системи (програмний або програмно-апаратний засіб), що надає послуги іншим об'єктам за їх запитами;

WEB-сервер – сервер, який обслуговує запити користувачів (клієнтів) згідно з протоколом HTTP (Hyper Text Transfer Protocol), забезпечує актуалізацію, збереження інформації WEB-сторінки, зв'язок з іншими серверами;

WEB-сторінка (WEB-сайт) – мережевий інформаційний ресурс, що надається користувачу у вигляді HTML-документу і має у мережі свою унікальну адресу;

HTML-документ – файл текстової або нетекстової природи (звук, відео, зображення), створений за допомогою мови гіпертекстової розмітки HTML (Hyper Text Mark-up Language);

Посилання (гіпертекстове посилання) – адреса іншого мережевого інформаційного ресурсу у форматі URL (Universal Resource Location), який тематично, логічно або будь-яким іншим способом пов'язаний з документом, у якому це посилання визначене.

4 Позначення та скорочення

Позначення послуг безпеки згідно з НД ТЗІ 2.5-004, які використовуються у цьому НД ТЗІ:

ДВ-1 - ручне відновлення після збоїв;

ДР-1 - квоти;

КА-2 - базова адміністративна конфіденційність;

КВ-1 - мінімальна конфіденційність при обміні;

НВ-1 - автентифікація вузла;

НИ-2 - одиночна ідентифікація і автентифікація;

НК-1 - однонаправлений достовірний канал;
НО-1 - розподіл обов'язків;
НР-2 - захищений журнал;
НТ-1 - самотестування за запитом;
НЦ-1 - КЗЗ з контролем цілісності;
ЦА-1 - мінімальна адміністративна цілісність;
ЦВ-1 - мінімальна цілісність при обміні;
ЦО-1 - обмежений відкат.

У цьому НД ТЗІ використовуються такі скорочення:
АС - автоматизована система;
ЕОМ - електронно-обчислювальна машина;
ІзОД - інформація з обмеженим доступом;
КЗЗ - комплекс засобів захисту;
КСЗІ - комплексна система захисту інформації;
НД ТЗІ - нормативний документ системи технічного захисту інформації;
НСД - несанкціонований доступ;
ОС - обчислювальна система;
ПЕОМ - персональна електронно-обчислювальна машина;
ПЗ - програмне забезпечення;
СЗІ - служба захисту інформації;
ТЗІ - технічний захист інформації.

5 Загальні вимоги

5.1 Установа, під час створення WEB-сторінки та визначення операторів, вузли яких будуть використовуватися для підключення до мережі Інтернет, повинна керуватися законами України, іншими нормативно-правовими актами, що встановлюють вимоги з технічного захисту інформації.

5.2 WEB-сторінка установи може бути розміщена на власному сервері або на сервері, що є власністю оператора. Власник сервера зобов'язаний гарантувати власнику інформації рівень захисту у відповідності до вимог цього НД ТЗІ.

5.3 Функціонування WEB-сторінки забезпечується АС, за допомогою якої здійснюється актуалізація розміщених на WEB-сторінці інформаційних ресурсів та керування доступом до них.

Для забезпечення захисту інформації WEB-сторінки в цій АС створюється КСЗІ, що є сукупністю організаційних і інженерно-технічних заходів, а також програмно-апаратних засобів, які забезпечують захист інформації.

5.4 Створення КСЗІ здійснюється відповідно до технічного завдання, розробленого згідно з НД ТЗІ 3.7-001.

5.5 КСЗІ підлягає державній експертизі у порядку, передбаченому Положенням про державну експертизу в сфері технічного захисту інформації.

5.6 Захист інформації на всіх етапах створення та експлуатації WEB-сторінки здійснюється відповідно до розробленого установою плану захисту інформації, зміст якого визначено НД ТЗІ 1.4-001. План захисту затверджується

керівником установи, а у випадку використання сервера оператора – погоджується з власником сервера.

5.7 Перелік інформації, призначеної для публічного розміщення на WEB-сторінці, визначається з урахуванням вимог діючого законодавства та затверджується керівником установи, що є власником WEB-сторінки.

5.8 Організація робіт із захисту інформації та забезпечення контролю за станом її захищеності на WEB-сторінці в установі здійснюється відповідальним підрозділом або відповідальною особою (далі - службою захисту інформації, СЗІ).

5.9 У випадку користування послугами оператора щодо розміщення, експлуатації та адміністрування WEB-сторінки власник інформаціі укладає з оператором договір (угоду), яким визначаються права і обов'язки сторін, умови підключення, розміщення інформації та забезпечення доступу до неї, інші питання, що вимагають урегулювання між власником інформації WEB-сторінки та оператором, виходячи з вимог законодавства у сфері захисту інформації та цього НД ТЗІ.

Окремі питання із захисту інформації можуть оформлятися у вигляді додатків, які є невід'ємною частиною договору.

6 Характеристика типових умов функціонування та вимоги до захисту інформації WEB-сторінки

До складу АС, яка забезпечує функціонування WEB-сторінки, входять: ОС, фізичне середовище, в якому вона знаходиться і функціонує, середовище користувачів, оброблювана інформація, у тому числі й технологія її оброблення. Під час забезпечення захисту інформації мають бути враховані всі характеристики зазначених складових частин, які впливають на реалізацію політики безпеки WEB-сторінки.

У випадку, якщо WEB-сторінка містить посилання на інформаційні ресурси іншої WEB-сторінки, умови функціонування останньої не повинні порушувати встановлену для даної WEB-сторінки політику безпеки.

У цьому розділі визначаються типові умови функціонування всіх складових АС, вводяться обмеження до умов функціонування та встановлюються загальні вимоги із захисту інформації до окремих компонентів АС. Для визначеної таким чином типової схеми функціонування АС встановлюються можливі варіанти для вибору функціональних профілів захищеності інформації від НСД.

6.1 Інформація WEB-сторінки та технологія її оброблення

6.1.1 Характеристика

6.1.1.1 Інформація WEB-сторінки поділяється на дві категорії:

- загальнодоступна інформація;
- технологічна інформація.

6.1.1.2 До загальнодоступної інформації відноситься публічно оголошувана інформація, користуватися якою можуть будь-які фізичні або юридичні особи (користувачі інформаційних ресурсів), що мають доступ до мережі Інтернет.

6.1.1.3 До технологічної інформації WEB-сторінки відноситься технологічна інформація КСЗІ та технологічна інформація щодо адміністрування та управління обчислювальною системою АС і засобами обробки інформації – дані про мережеві адреси, імена, персональні ідентифікатори та паролі користувачів, їхні повноваження та права доступу до об’єктів, інформація журналів реєстрації дій користувачів, інша інформація баз даних захисту, встановлені робочі параметри окремих механізмів або засобів захисту, інформація про профілі обладнання та режими його функціонування, робочі параметри функціонального ПЗ тощо.

Технологічна інформація призначена для використання тільки уповноваженими користувачами з числа співробітників СЗІ та персоналу, що забезпечує функціонування АС.

6.1.1.4 Способи і методи обробки інформації WEB-сторінки (зберігання, супроводження, передачі, введення, актуалізації та використання інформації) визначають технології оброблення інформації.

6.1.1.5 Технологічні особливості роботи користувачів із загальнодоступною інформацією WEB-сторінки визначаються особливостями системного та функціонального ПЗ, зокрема броузерів, які ними використовуються.

Технологічні особливості роботи користувачів інших категорій визначаються, крім того, архітектурою АС, способами оброблення та передавання інформації між компонентами АС і способами здійснення доступу до неї.

6.1.1.6 Можливі наступні способи здійснення доступу до технологічної інформації та передавання даних для актуалізації загальнодоступної інформації:

- з робочої станції, розміщеної на тій самій території, що і WEB-сервер (установи-власника WEB-сторінки або оператора) або з терміналу WEB-сервера;
- з робочої станції, яка розміщена на території установи-власника WEB-сторінки, до WEB-сервера, що розміщений на території оператора, з використанням мереж передачі даних.

6.1.2 Вимоги

6.1.2.1 КСЗІ повинна забезпечувати реалізацію вимог із захисту цілісності та доступності розміщеної на WEB-сторінці загальнодоступної інформації, а також конфіденційності та цілісності технологічної інформації WEB-сторінки.

6.1.2.2 Технологія оброблення інформації повинна відповідати вимогам політики безпеки інформації, визначеної для АС, що забезпечує функціонування WEB-сторінки.

6.1.2.3 Вимоги щодо забезпечення цілісності загальнодоступної інформації WEB-сторінки та конфіденційності й цілісності технологічної інформації вимагають застосування технологій, що забезпечують реалізацію контрольованого і санкціонованого доступу до інформації та заборону неконтрольованої й несанкціонованої її модифікації.

6.1.2.4 Технологія оброблення інформації повинна бути здатною реалізовувати можливість виявлення спроб несанкціонованого доступу до

інформації WEB-сторінки та процесів, які з цією інформацією пов’язані, а також забезпечити реєстрацію в системному журналі визначених політикою відповідної послуги безпеки подій (як НСД, так і авторизованих звернень).

6.1.2.5 Для користувачів, які порушили встановлені правила розмежування доступу до WEB-сторінки, засоби КСЗІ на період сеансу роботи повинні забезпечити блокування доступу до WEB-сторінки.

6.1.2.6 Технологічними процесами повинна бути реалізована можливість створення резервних копій інформації WEB-сторінки та процедури їх відновлення з використанням резервних копій.

6.1.2.7 Технологія оброблення інформації повинна передбачати можливість аналізу використання користувачами і процесами обчислювальних ресурсів АС і забезпечувати керування ресурсами.

6.2 Обчислювальна система

6.2.1 Характеристика

6.2.1.1 Узагальнена функціонально-логічна структура обчислювальної системи АС включає:

- підсистему обробки інформації;
- підсистему взаємодії з користувачами АС;
- підсистему обміну даними.

6.2.1.2 Підсистема обробки інформації забезпечує створення, зберігання, актуалізацію інформації WEB-сторінки і складається із засобів обробки інформації, системного та функціонального ПЗ.

До засобів обробки інформації належать WEB-сервер та необхідна кількість робочих станцій (або терміналів) для забезпечення всіх функцій щодо супроводження WEB-сторінки та захисту інформації.

6.2.1.3 Підсистема взаємодії з користувачами АС забезпечує за запитами користувачів надання доступу до загальнодоступної інформації WEB-сторінки, яка має вигляд HTLM-документу, з використанням мереж передачі даних та стандартних Інтернет-протоколів.

Підсистема складається, як мінімум, з програмно-апаратного комплексу, який дозволяє здійснювати маршрутизацію запитів користувачів, забезпечувати пошук необхідних користувачу інформаційних ресурсів і доступ до них.

6.2.1.4 Підсистема обміну даними забезпечує підготовку та безпосередньо імпорт/експорт інформації в/із АС, а також внутрішньосистемний обмін інформацією між WEB-сервером та робочими станціями з реалізацією фаз встановлення, підтримання та завершення з’єднання.

6.2.1.5 Відповідно до політики безпеки інформації в АС підсистеми комплектуються засобами захисту інформації (можуть використовуватися штатні засоби захисту системного і функціонального ПЗ та/або спеціалізовані засоби), які складають компоненти КЗЗ.

6.2.2 Вимоги

6.2.2.1 Програмно-апаратні засоби захисту, що входять до складу КЗЗ, повинні мати належним чином оформлені документи (експертні висновки,

сертифікати), які засвідчують відповідність цих засобів вимогам нормативних документів системи ТЗІ.

6.2.2.2 Встановлення на ОС нових (додаткових) компонентів, ПЗ (системного та/або функціонального), сервісів та розміщення будь-яких інших мережевих ресурсів, які не належать до категорії WEB-сторінки установи, не повинно порушувати політику безпеки інформації в АС, що забезпечує функціонування WEB-сторінки.

6.2.2.3 Вимоги до робочих станцій фізичних і юридичних осіб, які є користувачами загальнодоступної інформації WEB-сторінки, та їхнього ПЗ не висуваються.

6.3 Середовище користувачів

6.3.1 Характеристика

За рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконуються в процесі функціонування АС, користувачі поділяються на такі категорії:

а) користувачі, яким надано право доступу тільки до загальнодоступної інформації WEB-сторінки;

б) користувачі, яким надано повноваження супроводжувати КСЗІ та забезпечувати керування АС (адміністратор безпеки, інші співробітники СЗІ, користувачі з функціональними обов’язками WEB-майстрів, адміністраторів сервісів, адміністраторів мережевого обладнання, адміністраторів ресурсів DNS (Domain Name System), PROXY, FTP (File Transfer Protocol) та ін., якщо передбачається їх взаємодія з WEB-сторінкою, тощо);

в) технічний обслуговуючий персонал, що забезпечує належні умови функціонування АС, повсякденну підтримку життєдіяльності фізичного середовища (електрики, технічний персонал з обслуговування приміщень будівель, ліній зв’язку тощо);

г) розробники ПЗ, які здійснюють розробку та впровадження нових функціональних процесів, а також супроводження вже діючого функціонального ПЗ сервера, розробники та проектанти фізичної структури АС;

д) постачальники обладнання і технічних засобів та фахівці, що здійснюють його монтаж, поточне гарантійне й післягарантійне обслуговування.

6.3.2 Вимоги

6.3.2.1 Користувачі, яким надано повноваження супроводжувати КСЗІ та забезпечувати управління АС, повинні володіти навиками обслуговування засобів захисту інформації та використання технічних і програмних засобів, що застосовуються ними під час виконання своїх службових і функціональних обов’язків.

6.3.2.2 Користувачі, що належать до категорії "в" за 6.3.1, повинні мати належний рівень кваліфікації для виконання своїх службових та функціональних обов’язків у відповідності до визначених в установі технологічних процесів та режимів експлуатації обладнання.

6.3.2.3 Доступ до інформації WEB-сторінки повинен надаватися

користувачам у відповідності до положень політики безпеки інформації, визначеної для АС, що забезпечує функціонування WEB-сторінки.

Порядок доступу до ПЗ та компонентів АС користувачів різних категорій розробляється СЗІ й затверджується керівником установи.

6.3.2.4 Обов'язковою є реєстрація в АС користувачів, що належать до категорії "б" за 6.3.1, чим забезпечується можливість однозначного їх ідентифікування, а також їхніх дій щодо інформації WEB-сторінки.

Для встановлення правил та регламентації доступу цих користувачів до інформації WEB-сторінки СЗІ розробляються та впроваджуються нормативні та розпорядчі документи, передбачені планом захисту інформації.

6.3.2.5 Користувачі, що належать до категорій "в" – "д" за 6.3.1, можуть мати доступ до програмних та апаратних засобів АС лише під час робіт із тестування й інсталяції ПЗ, встановлення і регламентного обслуговування обладнання тощо, за умови обмеження їхнього доступу до технологічної інформації КСЗІ.

Зазначені категорії осіб повинні мати дозвіл на доступ до відомостей, які містяться в програмній і технічній документації на АС або окремі її компоненти, і необхідні їм для виконання функціональних обов'язків.

6.3.2.6 Вимоги до користувачів, яким надається право доступу до загальнодоступної інформації WEB-сторінки, не висуваються.

Користувачі загальнодоступної інформації одержують доступ до WEB-сторінки у відповідності до діючих у мережі Інтернет правил та регламенту.

6.4 Фізичне середовище

6.4.1 Характеристика

Фізичне середовище, що призначене для розміщення, експлуатації, адміністрування WEB-сторінки установи, включає:

- приміщення, в яких розташовані сервер і робочі станції з усіма компонентами (ОС, сховища для носіїв інформації та документації, робочі місця обслуговуючого персоналу і т.і.);
- засоби енергопостачання, заземлення, життєзабезпечення та сигналізації приміщення;
- допоміжні технічні засоби та засоби зв'язку.

6.4.2 Вимоги

6.4.2.1 Приміщення, де розміщуються компоненти ОС, повинні знаходитися на контрольованій території і мати охорону. Доступ до цих приміщень дозволяється тільки особам, що належать:

- до категорій "б" і "в" за 6.3.1 - без обмежень;
- до категорій "г" і "д" за 6.3.1 - за необхідністю.

Доступ здійснюється у порядку, визначеному СЗІ та затвердженому власником WEB-сторінки, або у відповідності до умов, передбачених договором (угодою) між власником WEB-сторінки та оператором (провайдером).

6.4.2.2 Вимоги до засобів енергопостачання, заземлення, життєзабезпечення, сигналізації приміщення та допоміжних технічних засобів і засобів зв'язку не висуваються.

7 Політика реалізації послуг безпеки інформації WEB-сторінки

7.1 Склад та вимоги до профілів захищеності інформації

7.1.1 Політика безпеки інформації в АС повинна поширюватися на об'єкти комп'ютерної системи, які безпосередньо чи опосередковано впливають на безпеку інформації.

До таких об'єктів належать:

- адміністратор безпеки та співробітники СЗІ;
- користувачі, яким надано повноваження забезпечувати управління АС;
- користувачі, яким надано право доступу до загальнодоступної інформації;
- інформаційні об'єкти, що містять загальнодоступну інформацію;
- системне та функціональне ПЗ, яке використовується в АС для оброблення інформації або для забезпечення функцій КЗЗ;
- технологічна інформація КСЗІ (дані про мережеві адреси, імена, персональні ідентифікатори та паролі користувачів, їхні повноваження та права доступу до об'єктів, встановлені робочі параметри окремих механізмів або засобів захисту, інша інформація баз даних захисту, інформація журналів реєстрації дій користувачів тощо);
- засоби адміністрування і управління обчислювальною системою АС та технологічна інформація, яка при цьому використовується;
- обчислювальні ресурси АС (наприклад, дисковий простір, тривалість сеансу роботи користувача із засобами АС, час використання центрального процесора і т. ін.), безконтрольне використання або захоплення яких окремим користувачем може призвести до блокування роботи інших користувачів, компонентів АС або АС в цілому.

7.1.2 З урахуванням особливостей надання доступу до інформації WEB-сторінки, типових характеристик середовищ функціонування та особливостей технологічних процесів оброблення інформації, зазначених у розділі 6, визначаються наступні мінімально необхідні рівні послуг безпеки для забезпечення захисту інформації від загроз:

- за умови, коли WEB-сервер і робочі станції розміщуються на території установи-власника WEB-сторінки або на території оператора (технологія Т1), мінімально необхідний функціональний профіль визначається:

КА-2, ЦА-1, ЦО-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1;

- за умови, коли WEB-сервер розміщується у оператора, а робочі станції – на території власника WEB-сторінки, взаємодія яких з WEB-сервером здійснюється з використанням мереж передачі даних (технологія Т2), мінімально необхідний функціональний профіль визначається:

КА-2, КВ-1, ЦА-1, ЦО-1, ЦВ-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1,НЦ-1, НТ-1, НВ-1.

7.1.3 Технологія Т1 різниться від технології Т2 способом передачі інформації від робочої станції до WEB-сервера, а саме: наявністю у другому випадку незахищеного середовища, яке не контролюється, і додатковими вимогами щодо ідентифікації та автентифікації між КЗЗ робочої станції й КЗЗ

WEB-сервера під час спроби розпочати обмін інформацією та забезпечення цілісності інформації при обміні.

7.1.4 За власником WEB-сторінки залишається право реалізації, у разі необхідності, окремих послуг безпеки інформації зазначених профілів з більш високим рівнем, доповнення цих профілів іншими послугами, а також реалізація послуг безпеки з більш високим рівнем гарантій.

У випадках, коли в АС вимоги до політики реалізації якоїсь з послуг безпеки забезпечуються організаційними або іншими заходами захисту, які в повному обсязі відповідають встановленим НД ТЗІ 2.5-004 специфікаціям для певного рівня послуги безпеки, то рівень такої послуги, що входить до визначених згідно з 7.1.2 профілів захищеності, може бути знижений на відповідну величину.

7.2 Вимоги до реалізації функціональних послуг безпеки інформації

7.2.1 Базова адміністративна конфіденційність

КЗЗ повинен реалізувати рівень КА-2.

Ця послуга дозволяє адміністратору безпеки керувати потоками інформації від захищених об'єктів до користувачів.

Політика адміністративної конфіденційності стосується: користувачів усіх категорій, крім визначених згідно з 6.3.1 "а"; об'єктів, що містять технологічну інформацію КСЗІ та технологічну інформацію щодо управління АС; системного та функціонального програмного забезпечення, що використовується для актуалізації, захисту загальнодоступної інформації та супроводження WEB-сторінки; доступу користувачів до окремих видів периферійних пристроїв (принтерів, накопичувачів інформації тощо), використання яких передбачено технологією обробки інформації.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта. Доступ до загальнодоступної інформації встановлюється для користувачів усіх категорій. Призначення атрибутів доступу користувачам і процесам до захищених об'єктів здійснюється адміністратором безпеки на основі аналізу функціональних та службових обов'язків окремих користувачів.

КЗЗ повинен надавати тільки адміністратору безпеки права доступу до технологічної інформації КСЗІ та процесів, що забезпечують її актуалізацію, супроводження та аналіз. Доступ до процесів, що забезпечують ведення системних процесів з адміністрування й забезпечення функціонування АС в цілому, окремих її компонентів та сервісів, а також до технологічної інформації щодо управління АС повинен надаватись тільки користувачам, які мають відповідні повноваження.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора безпеки.

Права доступу до кожного захищеного об'єкта, визначеного політикою безпеки послуги, повинні встановлюватися в момент його створення або ініціалізації.

7.2.2 Конфіденційність при обміні

КЗЗ повинен реалізувати рівень КВ-1.

Ця послуга дозволяє забезпечити захист об’єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Політика мінімальної конфіденційності при обміні стосується: користувачів, яким надано право супроводження КСЗІ та управління АС; об’єктів, які містять технологічну інформацію КСЗІ та технологічну інформацію щодо управління АС під час її передавання між віддаленими компонентами АС.

КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об’єкті, який передається.

КЗЗ повинен забезпечувати можливість реєстрації подій, які призвели або можуть призвести до порушення конфіденційності інформації, що міститься в об’єктах, які передаються.

7.2.3 Мінімальна адміністративна цілісність

КЗЗ повинен реалізувати рівень ЦА-1.

Ця послуга дозволяє керувати потоками інформації від користувачів до захищених об’єктів WEB-сторінки.

Політика мінімальної адміністративної цілісності стосується: користувачів усіх категорій; загальнодоступної інформації WEB-сторінки; файлової системи та функціонального ПЗ, що використовується для актуалізації, захисту загальнодоступної інформації та супроводження WEB-сторінки; створеної в процесі супроводження WEB-сторінки технологічної інформації КСЗІ та технологічної інформації щодо управління АС.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувачів і захищених об’єктів. Розмежування доступу здійснюється на рівні надання (встановлення заборони) користувачеві прав модифікувати об’єкт.

Право визначати множину об'єктів АС, цілісність яких забезпечується КЗЗ, надається адміністратору безпеки.

КЗЗ повинен надавати можливість адміністратору безпеки для кожного захищеного об’єкта визначити домен, якому повинні належати ті користувачі і/або групи користувачів, що мають право модифікувати об’єкт. Тільки йому надається право включати і вилучати користувачів та об'єкти до/з конкретних доменів.

Призначення атрибутів доступу користувачам і процесам до захищених об'єктів та запити на зміну цих прав повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора безпеки.

Користувачам, які мають доступ тільки до загальнодоступної інформації WEB-сторінки, забороняється модифікувати будь-які захищені об’єкти.

Адміністратору безпеки надається право модифікувати функціональне ПЗ, що використовується для захисту загальнодоступної інформації, та технологічну інформацію КСЗІ. Користувачам, що мають повноваження щодо управління АС, надається відповідно до функціональних обов’язків право модифікувати технологічну інформацію та функціональне ПЗ, що

використовується для актуалізації загальнодоступної інформації та супроводження WEB-сторінки.

Права доступу до захищених об’єктів WEB-сторінки повинні встановлюватися в момент їх створення або ініціалізації.

7.2.4 Цілісність при обміні

КЗЗ повинен реалізувати рівень ЦВ-1.

Ця послуга дозволяє забезпечити захист WEB-сторінки від несанкціонованої модифікації інформації, яка передається між WEB-сервером та робочими станціями у разі використання технології Т2, під час експорту/імпорту інформації через незахищене середовище. Політика послуги стосується всіх об’єктів, що передаються.

КЗЗ повинен забезпечувати контроль за цілісністю інформації в повідомленнях, які передаються, а також бути здатним виявляти факти їх несанкціонованого видалення або дублювання.

КЗЗ повинен забезпечувати можливість реєстрації подій, які призвели до порушення цілісності повідомлень, їх несанкціонованого видалення або дублювання.

7.2.5 Відкат

КЗЗ повинен реалізувати рівень ЦО-1.

Ця послуга забезпечує можливість відмінити окрему операцію або послідовність операцій і повернути захищений об'єкт після внесення до нього змін до попереднього наперед визначеного стану.

Політика обмеженого відкату стосується користувачів, яким надано право супроводження КСЗІ та управління АС; об’єктів, які містять публічну інформацію; функціонального програмного забезпечення, що використовується для актуалізації, захисту публічної інформації та супроводження WEB-сторінки; створеної в процесі супроводження WEB-сторінки технологічної інформації КСЗІ та технологічної інформації щодо управління АС. Якщо стосовно якогось з об’єктів зазначених категорій в процесі обробки не передбачається можливості його модифікації, політика послуги на нього не розповсюджується.

До складу АС повинні входити автоматизовані засоби, які дозволяють адміністратору безпеки, співробітнику СЗІ, користувачу, який має повноваження щодо управління АС, відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об’єктом WEB-сторінки за певний проміжок часу.

Факт використання послуги має реєструватись в системному журналі. Відміна операції не повинна призводити до видалення з журналу запису про операцію, яка пізніше була відмінена, якщо остання підлягала реєстрації відповідно до вимог послуги безпеки
НР-2.

7.2.6 Використання ресурсів

КЗЗ повинен реалізувати рівень ДР-1.

Ця послуга дозволяє керувати використанням користувачами послуг та ресурсів.

Політика використання ресурсів, що реалізується КЗЗ, стосується: користувачів загальнодоступної інформації; адміністратора безпеки та користувачів, яким надано повноваження щодо управління АС; файлової системи; системного та функціонального програмного забезпечення; технологічної інформації щодо управління АС; окремих периферійних пристроїв (принтерів, накопичувачів інформації і т.ін.); обчислювальних ресурсів АС і передбачає можливість встановлення обмежень на їх використання.

Обмеження щодо використання окремим користувачем та/або процесом обсягів обчислювальних ресурсів АС або кількості об'єктів встановлюються адміністратором безпеки або користувачами, яким надано повноваження щодо управління АС. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від зазначених користувачів.

Спроби користувачів перевищити встановлені обмеження на використання ресурсів повинні реєструватися в системному журналі.

7.2.7 Відновлення після збоїв

КЗЗ повинен реалізувати рівень ДВ-1.

Політика відновлення після збоїв, що реалізується КЗЗ, стосується: системного та функціонального програмного забезпечення; засобів захисту інформації та засобів управління КСЗІ; засобів адміністрування та управління обчислювальною системою АС – і гарантує повернення АС у відомий захищений стан після відмов або переривання обслуговування, спричинених помилковими діями користувачів, неврахованою функціональною недостатністю програмного та апаратного забезпечення (наприклад, можливою наявністю не виявлених під час проектування незадекларованих функцій), іншими непередбачуваними ситуаціями.

Політика відновлення, яка реалізується КЗЗ, повинна визначати множину типів відмов WEB-сторінки і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Для кожної з відмов повинні бути чітко визначені і задокументовані рівні відмов, у разі перевищення яких необхідна повторна інсталяція WEB-сторінки.

Після відмови WEB-сторінки або переривання обслуговування, КЗЗ повинен перевести WEB-сторінку до стану, з якого повернути її в режим нормального функціонування може тільки адміністратор безпеки і користувачі, які мають повноваження щодо управління АС. Для кожного з них повинна бути визначена множина допустимих виконуваних ними операцій з метою повернення АС у відомий захищений стан.

Повернення АС з режиму, що визначається погіршеними характеристиками обслуговування, в режим нормального функціонування повинно здійснюватися за допомогою ручних (не автоматизованих) процедур.

7.2.8 Реєстрація

КЗЗ повинен реалізувати рівень НР-2.

Послуга дозволяє контролювати небезпечні відповідно до політики безпеки WEB-сторінки дії користувачів всіх категорій із захищеними об'єктами.

Політика реєстрації стосується: користувачів усіх категорій; публічної інформації WEB-сторінки; системного та функціонального програмного забезпечення, що використовується для актуалізації, захисту публічної інформації та супроводження WEB-сторінки; створеної в процесі супроводження WEB-сторінки технологічної інформації КСЗІ та технологічної інформації щодо управління АС.

КЗЗ повинен забезпечувати реєстрацію всіх подій, які мають безпосереднє відношення до безпеки. До них відносяться наступні класи подій:

- вхід/вихід або намагання входу/виходу в/із системи користувачами будь-яких категорій;
- реєстрація та видалення або намагання реєстрації та видалення користувачів будь-якої категорії в системі;
- зміна атрибутів доступу користувачем будь-якої категорії та дії, що призвели до цього;
- отримання або намагання отримання доступу користувачем будь-якої категорії до будь-яких захищених процесів і об'єктів АС;
- створення користувачем будь-якої категорії твердих копій та виведення їх на друкуючі пристрої;
- модифікація або спроби модифікації захищених процесів і об'єктів АС, у тому числі факти та спроби порушення цілісності КЗЗ;
- спроби використання обчислювальних ресурсів АС з перевищенням встановлених квот;
- інші події, обов’язковість реєстрації яких передбачена політикою реалізації окремих послуг безпеки інформації.

КЗЗ повинен надавати можливість визначення переліку реєстраційних подій виключно адміністратору безпеки.

Реєстрація всіх подій, що мають безпосереднє відношення до безпеки, здійснюється в журналі реєстрації, який повинен містити інформацію стосовно дати, часу, місця, типу і наслідків зареєстрованої події (успішність/неуспішність), ім’я (IP-адресу) та/або ідентифікатор причетного до цієї події користувача. Реєстраційна інформація повинна бути достатньою для однозначної ідентифікації користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

КЗЗ повинен мати механізми захисту для гарантування безпечної передачі інформації журналу реєстрації на віддалену робочу станцію адміністратора безпеки WEB-сторінки (для технології Т2).

Адміністратор безпеки і користувачі, яким надано повноваження щодо управління АС, повинні мати засоби перегляду та аналізу журналу реєстрації, а КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.

7.2.9 Ідентифікація і автентифікація

КЗЗ повинен реалізувати рівень НИ-2.

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особу суб’єкта, що намагається одержати доступ до захищених об’єктів WEB-сторінки.

Політика ідентифікації і автентифікації стосується: всіх користувачів WEB-сторінки, які намагаються одержати доступ до системного та функціонального програмного забезпечення, що використовується для актуалізації, захисту публічної інформації та супроводження WEB-сторінки; створеної в процесі супроводження WEB-сторінки технологічної інформації КСЗІ та технологічної інформації щодо управління АС; задіяного для цього периферійного обладнання.

КЗЗ повинен однозначно ідентифікувати категорії користувачів WEB-сторінки і за атрибутами кожної з цих категорій визначати послуги, що їм доступні. Ідентифікація здійснюється на підставі особистого імені та/або IP-адреси користувача.

КЗЗ повинен автентифікувати адміністратора WEB-сторінки, співробітників СЗІ та користувачів, які мають повноваження щодо управління АС, з використанням захищеного механізму на підставі особистого пароля. Автентифікація користувачів, що мають виключне право доступу тільки до публічної інформації, не здійснюється.

Дозвіл на виконання будь-яких дій з інформацією та обладнанням WEB-сторінки, що контролюються КЗЗ, надається користувачу тільки після успішного завершення процедур ідентифікації та/або автентифікації його КЗЗ відповідно до категорії користувача.

КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

7.2.10 Ідентифікація і автентифікація при обміні

КЗЗ повинен реалізувати рівень НВ-1.

Ця послуга дозволяє у разі використання технології Т2 компонентам КЗЗ WEB-сервера і віддаленої робочої станції здійснити взаємну ідентифікацію, перш ніж розпочати взаємодію.

Послуга ідентифікації і автентифікації при обміні стосується адміністратора безпеки та користувачів, яким надані повноваження щодо супроводження WEB-сторінки, технологічної інформації КСЗІ.

КЗЗ повинен надавати доступ до процесів, що забезпечують ініціалізацію обміну даними, тільки адміністратору безпеки і користувачам, яким надано повноваження щодо супроводження WEB-сторінки.

Обмін інформацією між компонентами КЗЗ повинен здійснюватися тільки після ідентифікації і автентифікації КЗЗ-відправником КЗЗ-отримувача інформації. Результати процедури ідентифікації і автентифікації є дійсними протягом всього сеансу обміну (незалежно від кількості об’єктів, що експортуються) і втрачають свою силу після його закінчення.

Процедура ідентифікації і автентифікація компонентів КЗЗ повинна здійснюватися на підставі їхніх імен, IP-адрес і паролів.

Підтвердження ідентичності має виконуватися на підставі затвердженого в АС протоколу автентифікації.

7.2.11 Достовірний канал

КЗЗ повинен реалізувати рівень НК-1.

Ця послуга повинна гарантувати користувачу будь-якої категорії можливість безпосередньої взаємодії з КЗЗ, а також те, що ніяка взаємодія користувача з АС не може бути модифікованою іншим користувачем або процесом. Послуга визначає вимоги до механізму встановлення достовірного зв'язку між користувачем і КЗЗ.

Політика достовірного каналу стосується користувачів усіх категорій та компонентів системного та функціонального програмного забезпечення, які задіяні для реалізації механізмів КЗЗ.

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

7.2.12 Розподіл обов’язків

КЗЗ повинен реалізувати рівень НО-1.

Ця послуга дозволяє розмежувати повноваження користувачів, визначивши категорії користувачів з певними і притаманними для кожної з категорій функціями (ролі). Послуга призначена для зменшення потенційних збитків від навмисних або помилкових дій користувачів і обмеження авторитарності керування АС.

Політика розподілу обов’язків, що реалізується КЗЗ, стосується користувачів усіх категорій і повинна визначати щонайменше такі ролі:

- адміністратора безпеки;

- користувачів, яким надано право доступу до певних видів інформації (публічної, технологічної, системного та функціонального ПЗ).

Кількість користувачів, які мають доступ до технологічної інформації та системного і функціонального ПЗ повинна бути мінімізована, щоб обмежити їх коло тільки тими, кому необхідний такий доступ для виконання функціональних обов'язків, що передбачаються експлуатаційною та розпорядчою документацією на WEB-сторінку.

Адміністратору безпеки дозволяється доступ до всієї інформації WEB-сторінки. У разі необхідності його роль може дублюватися уповноваженим співробітником СЗІ. Повноваження всіх інших користувачів щодо доступу до інформації надаються їм адміністратором безпеки.

КЗЗ повинен присвоїти користувачу атрибути, якими однозначно характеризується надана йому роль. Користувач може виступати в певній ролі тільки після того, як він виконає дії, що підтверджують прийняття ним цієї ролі.

7.2.13 Цілісність комплексу засобів захисту

КЗЗ повинен реалізувати рівень НЦ-1.

Ця послуга визначає міру здатності КЗЗ WEB-сторінки захищати себе і гарантувати свою спроможність керувати захищеними об’єктами.

Політика цілісності КЗЗ повинна визначати склад КЗЗ, механізми контролю цілісності його компонентів та порядок їх використання.

Політика цілісності КЗЗ стосується: адміністратора безпеки; окремих компонентів системного та функціонального програмного забезпечення, які задіяні для реалізації механізмів КЗЗ; засобів захисту інформації, а також технологічної інформації КСЗІ - і забезпечує взаємодію зазначених об’єктів.

Політика реалізації послуги повинна гарантувати, що всі послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ. Якщо існують обмеження, недотримання яких може призвести до надання послуг в обхід інтерфейсу КЗЗ і порушення цілісності КЗЗ, то такі обмеження повинні бути описані і задокументовані. До користувачів має бути доведено порядок їх роботи з дотриманням цих обмежень, а КЗЗ повинен надавати адміністратору можливість здійснення контролю за цим порядком.

КЗЗ повинен повідомляти адміністратора безпеки про порушення цілісності будь-якого компонента КЗЗ. WEB-сторінка під час цього має бути переведена до стану, в якому доступ до неї користувачів, крім адміністратора безпеки, заборонено. Повернення до нормального режиму функціонування може бути здійснено тільки адміністратором після відновлення відповідності цього компонента еталону.

7.2.14 Самотестування

КЗЗ повинен реалізувати рівень НТ-1.

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій захисту WEB-сторінки.

Політика самотестування поширюється на адміністратора безпеки, компоненти системного та функціонального програмного забезпечення, які задіяні для реалізації механізмів КЗЗ, засоби захисту інформації.

До складу КЗЗ повинна входити множина тестових процедур, яка враховує особливості функціонування компонентів конкретної WEB-сторінки і достатня для оцінки правильності виконання всіх критичних для безпеки публічної та технологічної інформації КСЗІ функцій, а сам КЗЗ повинен бути здатним контролювати їх виконання.

КЗЗ повинен забезпечувати виконання тестів за запитом адміністратора безпеки.

У разі некоректного виконання якогось із тестів КЗЗ повинен перевести АС до стану, коли забороняється надання користувачам доступу до WEB-сторінки, або до стану, коли забороняється надання доступу до інформації з використанням функцій, для яких тест не було виконано. Повернути АС до нормального функціонування може тільки адміністратор безпеки після відновлення працездатності КЗЗ і повторного виконання повного набору тестів.

КЗЗ повинен забезпечувати відповідність набору тестів (неможливість будь-якої модифікації) версії КЗЗ. Зміна тестів можлива лише у процесі інсталяції нової версії КЗЗ.

7.3 Вимоги до реалізації критеріїв гарантій

Критерії гарантій включають вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, середовища функціонування, документації, випробувань КЗЗ.

Гарантії реалізації послуг безпеки повинні відповідати рівню Г2 у відповідності до НД ТЗІ 2.5-004.

7.3.1 Архітектура

Програмне забезпечення, призначене для реалізації КЗЗ, повинне, як правило, будуватися за модульним принципом.

Склад послуг безпеки, а також механізмів захисту, що реалізують кожну з послуг, визначається політикою безпеки інформації в АС і повинен відповідати її вимогам. Якщо не всі вимоги політики безпеки реалізуються КЗЗ, то вони повинні підтримуватися організаційними та іншими заходами захисту КСЗІ. У складі КЗЗ не повинні міститися послуги та використовуватися засоби, які мають не передбачені політикою безпеки функції. Використання таких засобів можливе за умови вилучення цих функцій або гарантування неможливості їх активізації.

Мають бути описані особливості архітектури компонентів КСЗІ та їх призначення. Стиль опису – неформалізований, вимоги щодо детального опису не висуваються.

7.3.2 Середовище розробки

Мають бути визначені всі стадії та етапи життєвого циклу АС, а для кожної стадії та етапу – перелік і обсяги необхідних робіт та порядок їх виконання. Всі стадії та етапи робіт повинні бути задокументовані. Види та зміст документів встановлено державними стандартами.

На всіх стадіях життєвого циклу повинні існувати процедури керування конфігурацією АС. Ці процедури повинні визначати технологію відслідковування та внесення змін в апаратне та програмне забезпечення КСЗІ, тестове покриття і документацію та гарантувати, що без дотримання цієї технології ніякі зміни не можуть бути внесені. Технологія відслідковування та внесення змін повинна гарантувати постійну відповідність між документацією і реалізацією поточної версії КЗЗ.

7.3.3 Послідовність розробки

Для всіх стадій життєвого циклу АС повинні бути розроблені функціональні специфікації КСЗІ.

На підготовчому етапі створення КСЗІ має бути виконане обстеження середовищ функціонування АС, в результаті якого визначаються об’єкти захисту, здійснюється класифікація інформації та розробляється модель загроз для інформації і концепція політики безпеки інформації в АС. На підставі цих даних мають бути сформульовані функціональні специфікації вимог із захисту інформації в АС. Ці специфікації мають бути викладені в окремому розділі в технічному завданні на створення АС або окремому технічному завданні на створення КСЗІ.

Функціональні специфікації політики безпеки і моделі політики безпеки повинні містити перелік і опис послуг безпеки, що надаються КЗЗ, а також правила розмежування доступу до захищених об’єктів АС.

Функціональні специфікації проекту архітектури КСЗІ повинні містити модель захисту (ескізний проект), де враховані всі суттєві загрози і для кожної з них визначено можливі варіанти їх блокування (попередження) за допомогою КЗЗ або організаційними чи іншими заходами захисту. Якщо існує

неоднозначність, повинні надаватися додаткові аргументи на користь вибору того чи іншого варіанту.

Функціональні специфікації детального проекту КСЗІ повинні містити принципи побудови, функціональні можливості, опис функціонування кожного механізму захисту та взаємодії механізмів між собою у складі КЗЗ. Повинні бути розроблені документи, що регламентують використання засобів КЗЗ, а також організаційних та інших заходів захисту, які входять до КСЗІ. Як реалізація детального проекту може розглядатися технічний, робочий або технорабочий проекти.

Функціональні специфікації всіх рівнів надаються в описовому (неформалізованому) вигляді.

Має бути підтверджена (показана) відповідність специфікацій КСЗІ всіх рівнів. Формальних доказів відповідності не вимагається. Таким підтвердженням може бути дотримання власником АС і суб'єктами господарювання, які беруть участь у створенні АС і КСЗІ, встановленого нормативними документами із захисту інформації порядку. Наприклад, підтвердженням відповідності між специфікаціями КСЗІ різних рівнів деталізації може бути узгодження в установленому порядку відповідних документів (моделі загроз, технічного завдання, технічного проекту тощо), висновок приймальної комісії щодо цього під час випробувань КСЗІ або окремих її компонентів, результати контролю за виконаними роботами на етапах створення АС з боку системи якості виробництвом, якщо у власника та розробників АС така система впроваджена та ін.

Окремі етапи робіт повинні бути задокументовані відповідно до вимог НД ТЗІ 1.4-001 у вигляді окремих розділів плану захисту інформації в АС або вимог інших нормативно-правових актів і нормативних документів з ТЗІ.

7.3.4 Середовище функціонування

Повинні існувати засоби інсталяції, генерації і запуску КЗЗ, які гарантують, що експлуатація АС починається з безпечного стану, а також існувати документи (інструкції), які регламентують порядок керування цими процедурами. Якщо можливі різні варіанти конфігурації КЗЗ, то всі вони повинні бути описані в інструкціях.

7.3.5 Документація

Документація на КЗЗ у вигляді окремих документів або розділів інших документів повинна містити опис послуг безпеки, що реалізуються КЗЗ, а також настанови для різних категорій користувачів (адміністратора безпеки, адміністратора баз даних, адміністратора сервісів, звичайного користувача тощо) стосовно використання послуг безпеки.

Вимоги до складу і змісту документації на інші компоненти КСЗІ, організаційні або інші заходи захисту визначаються технічним завданням на створення КСЗІ.

7.3.6 Випробування

Випробування КЗЗ можуть проводитись як самостійно, так і у складі КСЗІ.

Для проведення випробувань розробник КЗЗ повинен підготувати програму і методику випробувань, розробити процедури (тести) випробувань усіх механізмів, що реалізують послуги безпеки.

Розробник КЗЗ повинен надати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування.

Розробник КЗЗ повинен усунути або нейтралізувати всі знайдені “слабкі місця” і виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові “слабкі місця ”.

Програма і методика випробувань КЗЗ, тестове покриття, результати випробувань КЗЗ входять до складу обов’язкового комплекту документації, яка надається організатору експертизи під час проведення державної експертизи КСЗІ в АС.