НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах

НД ТЗІ 2.6-001-11

Адміністрація Державної служби спеціального зв'язку
та захисту інформації України

Київ 2011

НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

ЗАТВЕРДЖЕНО
Наказ Адміністрації Державної
служби спеціального зв'язку
та захисту інформації України
25 березня 2011 року № 65

Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах

НД ТЗІ 2.6-001-11

Адміністрація Державної служби спеціального зв'язку
та захисту інформації України

Київ

ПЕРЕДМОВА

РОЗРОБЛЕНО Товариством з обмеженою відповідальністю "Інститут комп'ютерних технологій".

ВНЕСЕНО Департаментом з питань захисту інформації в інформаційно-телекомунікаційних системах Адміністрації Державної служби спеціального зв’язку та захисту інформації України.

УВЕДЕНО ВПЕРШЕ.

Цей документ не може бути повністю чи частково відтворений, тиражований та розповсюджений без дозволу Адміністрації Державної служби спеціального зв’язку та захисту інформації України

ЗМІСТ

НД ТЗІ 2.6-001-11

Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах

Чинний від 2011-03-25

1 Галузь застосування

Цей нормативний документ (НД) містить опис загальних положень та порядку проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу (НСД) та комплексних систем захисту інформації (КСЗІ), оброблюваної в інформаційно-телекомунікаційних системах (ІТС), у сфері технічного захисту інформації (ТЗІ).

НД призначено для державних органів, органів місцевого самоврядування, органів управління Збройних Сил України, інших військових формувань, а також підприємств, установ і організацій всіх форм власності, які виконують роботи зі створення та проведення експертизи засобів технічного захисту інформації (ЗТЗІ) від НСД та КСЗІ в ІТС на відповідність вимогам НД системи ТЗІ в Україні.

2 Нормативні посилання

У цьому НД ТЗІ наведено посилання на такі нормативні документи:

Закон України "Про інформацію".

Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.99 № 1229.

Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. Затверджено постановою Кабінету Міністрів України від 16.02.98 № 180.

Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави. Затверджена постановою Кабінету Міністрів України від 28.11.98 № 1893.

Порядок організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях. Затверджений постановою Кабінету Міністрів України від 02.10.2003 № 1561-12.

Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373.

ДСТУ 2851-94 Програмні засоби ЕОМ. Документування результатів випробувань.

ДСТУ 2853-94 Програмні засоби ЕОМ. Підготовлення і проведення випробувань.

ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни і визначення.

ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технологій. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій.

Звід відомостей, що становлять державну таємницю. Затверджений наказом Служби безпеки України від 12.08.2005 № 404. Зареєстрований у Міністерстві юстиції України 17.08.2005 за № 902/11182.

Положення про державну експертизу в сфері технічного захисту інформації. Затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93. Зареєстровано в Міністерстві юстиції України 16.07.2007 за № 820/14087.

Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису. Затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141. Зареєстровано в Міністерстві юстиції України 30.07.2007 за № 862/14129.

Положення про порядок розроблення, виробництва та уведення в експлуатацію засобів криптографічного захисту конфіденційної інформації, що є власністю держави. Затверджено наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 22.04.2008 № 82/ДСК. Зареєстровано в Міністерстві юстиції України 16.05.2008 за № 418/15109.

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

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

НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

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

НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення.

НД ТЗІ 2.2-005-08 Технічний захист інформації. Захист інформації, яку обробляють засобами електронної обчислювальної техніки на об’єктах інформаційної діяльності, від витоку інформації за рахунок побічних електромагнітних випромінювань і наведень. Норми ефективності захисту.

НД ТЗІ 2.3-014-08 Захист інформації на об’єктах інформаційної діяльності. Методика оцінки ефективності зашумлення ліній електроживлення технічних засобів.

НД ТЗІ 2.3-015-08 Захист інформації на об’єктах інформаційної діяльності. Технічний захист інформації, яка обробляється засобами обчислювальної техніки, від витоку за рахунок побічних електромагнітних випромінювань та наведень. Методика оцінки захищеності об’єкта ЕОТ від витоку секретної інформації лініями електроживлення без використання на них засобів захисту.

НД ТЗІ 2.3-016-08 Захист інформації на об’єктах інформаційної діяльності. Технічний захист інформації, яка обробляється засобами обчислювальної техніки, від витоку інформації за рахунок наведень побічних електромагнітних випромінювань на лінії та комунікації. Методика інструментального контролю ефективності захисту технічних засобів ЕОТ від

витоку секретної інформації за рахунок ПЕМВН на лінії сигналізації та зв’язку, які виходять за межі контрольованої зони.

НД ТЗІ 2.4-007-08 Захист інформації на об’єктах інформаційної діяльності. Технічний захист інформації, яка обробляється засобами обчислювальної техніки, від витоку за рахунок побічних електромагнітних випромінювань та наведень. Рекомендації з використання мережевих фільтрів.

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

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

НД ТЗІ 2.5-007-2007 Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробленні в автоматизованих системах класу "1".

НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

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

НД ТЗІ 2.7-007-08 Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки щодо зашумлення ліній електроживлення технічних засобів.

НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Передпроектні роботи.

НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

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.

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

НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

Тимчасове положення про категорування об`єктів (ТПКО-95).

ГОСТ 19.301-79 Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению.

ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.

РД 50-34.698-90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Требования к содержанию документов.

3 Визначення

У цьому НД ТЗІ застосовуються терміни та визначення, встановлені ДСТУ 3396.2-97 та

НД ТЗІ 1.1-003-99.

Крім цього, використано такі терміни та визначення.

Верифікація - одинична дія у процесі проведення оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки, яка передбачає виконання детального дослідження змісту матеріалів з метою прийняття рішення про достатність наведених у них аргументів на користь коректності доказів.

Випробування – експериментальне визначення кількісних та/або якісних характеристик властивостей об'єкта експертизи за результатом впливу на нього під час його функціонування.

Внутрішньосистемний інтерфейс – визначена Розробником сукупність засобів, методів та правил взаємодії між складовими частинами (підсистемами, компонентами, модулями) об’єкта експертизи.

Дослідження – одинична дія в процесі проведення експертизи, яка передбачає виконання поглибленого аналізу змісту матеріалів на предмет відповідності висунутим вимогам з використанням спеціальних знань та досвіду Експерта.

Ефективність – властивість об'єкта експертизи, що характеризується мірою досягнення цілей, поставлених під час його створення.

Засіб випробувань – програмний, програмно-апаратний або апаратний засіб, що використовується з метою здійснення перевірок у процесі проведення випробувань.

Засіб технічного захисту інформації від несанкціонованого доступу – програмний, апаратний або програмно-апаратний засіб, який створюється як окремий продукт виробництва, має необхідну проектну та/або експлуатаційну документацію і забезпечує самостійно або в комплексі з іншими засобами захист від загроз несанкціонованого доступу для інформації, оброблюваної в інформаційно-телекомунікаційній системі.

Захищений від несанкціонованого доступу компонент обчислювальної системи – програмний, апаратний або програмно-апаратний засіб, в якому додатково до основного призначення передбачено функції захисту інформації від загроз несанкціонованого доступу.

Захищеність інформації – характеристика рівня безпеки інформації, оброблюваної в певній ІТС.

Зовнішній інтерфейс – визначена Розробником сукупність засобів, методів та правил взаємодії між об’єктом експертизи та іншими відносно нього об’єктами (користувачами, процесами, системами тощо).

Інформаційна модель процесу – модель процесу, подана у вигляді опису суттєвих для розгляду вхідних, вихідних та внутрішніх параметрів процесу та зв'язків між ними, яка дозволяє моделювати зміну вихідних параметрів процесу залежно від зміни певних його вхідних та внутрішніх параметрів.

Інформаційна система – організаційно-технічна система, в якій реалізується технологія оброблення інформації з використанням технічних і програмних засобів.

Інформаційний ресурс – будь-які дані в електронному вигляді, які обробляються або зберігаються в інформаційно-телекомунікаційній системі.

Інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які в процесі оброблення інформації діють як єдине ціле.

Комплекс технічного захисту інформації – сукупність організаційних, інженерних і технічних заходів та засобів, призначених для захисту від витоку інформації з обмеженим доступом технічними каналами на об’єктах інформаційної діяльності.

Метод випробувань – визначений (встановлений) спосіб виконання перевірок у процесі проведення випробувань.

Методика випробувань – визначені (встановлені) способи проведення випробувань.

Методика експертизи – визначені (встановлені) способи проведення експертних робіт в ході експертизи.

Методика перевірки дотримання вимог до рівня гарантій – визначені (встановлені) способи проведення перевірки дотримання вимог до рівня гарантій коректності реалізації функціональних послуг безпеки.

Об'єкт експертизи – засіб технічного захисту інформації від несанкціонованого доступу, захищений від несанкціонованого доступу компонент обчислювальної системи або комплексу засобів захисту комплексної системи захисту інформації, комплексна система захисту інформації, стосовно яких здійснюється експертиза в сфері технічного захисту інформації.

Об'єкт інформаційної діяльності – будівлі, приміщення, транспортні засоби чи інші інженерно-технічні споруди, функціональне призначення яких передбачає обіг інформації з обмеженим доступом.

Оцінювання – визначення міри відповідності характеристик об'єкта експертизи заданим критеріям та вимогам.

Перевірка – одинична контрольна дія в процесі проведення експертизи.

Працездатність – характеристика стану об'єкта експертизи (складової частини, компонента), що відображає його здатність виконувати певні функції із заданою ефективністю та протягом потрібного часу.

Програма випробувань – документована сукупність вимог, що підлягає перевірці в процесі проведення випробувань.

Програма експертизи – документована сукупність вимог, що підлягає перевірці в процесі проведення експертизи.

Програма перевірки рівня гарантій – документована сукупність вимог, що підлягають перевірці в процесі експертизи оцінюваного об'єкта експертизи на відповідність вимогам до рівня гарантій коректності реалізації функціональних послуг безпеки.

Телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Тестова процедура – документально зафіксована послідовність виконання перевірок у процесі проведення випробувань.

Тестове покриття – міра, що характеризує здатність тестових даних випробовувати вимоги до об'єкта експертизи.

Тестові дані – дані, що використовуються як вхідні в процесі проведення випробувань об'єкта експертизи.

Функціональна послуга безпеки – сукупність функцій, що визначені відповідно до вимог НД ТЗІ 2.5-004-99 та забезпечують захист інформації від певної загрози або від множини загроз.

Функціональна специфікація об'єкта експертизи – впорядкований перелік реалізованих в об'єкті експертизи функціональних послуг безпеки згідно з НД ТЗІ 2.5-004-99 разом з описом їх політики або іншим чином визначений перелік функцій захисту з описом їх політик згідно з вимогами міжнародних стандартів.

4 Позначення та скорочення

У цьому НД ТЗІ використано такі позначення та скорочення:

АС – автоматизована система;

ВІ – відкрита інформація;

ВІВД – відкрита інформація, що є власністю держави;

ЗТЗІ – засіб технічного захисту інформації;

ІДТ – інформація, що становить державну таємницю;

ІзОД – інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ – комплекс засобів захисту;

КЗІ – криптографічний захист інформації;

КІ – конфіденційна інформація;

КІВД – конфіденційна інформація, що є власністю держави;

КСЗІ – комплексна система захисту інформації;

НД – нормативний документ;

НСД – несанкціонований доступ;

ОЕ – об'єкт експертизи;

ОІД – об’єкт інформаційної діяльності;

ПРД – правила розмежування доступу;

СЗІ – служба захисту інформації;

ТЗІ – технічний захист інформації;

ФПБ – функціональна послуга безпеки.

5 Вступні положення щодо порядку проведення експертизи засобів захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації

5.1 Як зазначається в НД ТЗІ 1.1-002-99, у проблемі захисту від НСД інформації, оброблюваної в ІТС, відокремлюються два напрями:

- забезпечення захищеності інформації у функціонуючих та/або створюваних ІТС;
- створення ЗТЗІ від НСД або захищених від НСД компонентів обчислювальної системи поза конкретним середовищем експлуатації.

При цьому як у першому, так і в другому випадку доцільним (а якщо в ІТС планується оброблення інформації, порядок захисту якої регламентується законами України або іншими нормативно-правовими актами (наприклад, інформації, яка становить державну таємницю або вимоги щодо захисту якої встановлено законодавством), то обов'язковим є незалежне підтвердження (оцінювання) відповідності реалізованих засобів та заходів захисту встановленим вимогам та нормам. Результатами проведеного оцінювання має бути відповідний висновок, на підставі якого власники ІТС та оброблюваних у них інформаційних ресурсів можуть приймати рішення щодо прийнятності та достатності вжитих заходів і реалізованих засобів.

5.2 Система оцінювання відповідності реалізованих засобів та заходів захисту встановленим вимогам та нормам в Україні функціонує на підставі Положення про державну експертизу в сфері технічного захисту інформації. Згідно з вимогами цього документа оцінювання відповідності реалізованих засобів та заходів захисту встановленим вимогам та нормам здійснюється шляхом проведення експертизи. Суб'єктами експертизи є: юридичні та фізичні особи, які є Замовниками експертизи; уповноважений державний орган; підрозділи уповноваженого державного органу, підприємства, установи та організації, які проводять експертизу (Організатори експертизи); державні органи, які проводять експертизу в сфері свого управління; фізичні особи – виконавці експертних робіт з ТЗІ (Експерти). Об'єктами експертизи (ОЕ) можуть бути як КСЗІ, які є невід'ємною складовою частиною ІТС, так і окремі ЗТЗІ від НСД, у тому числі захищені від НСД компоненти обчислювальної системи.

5.3 Якщо ОЕ являє собою ЗТЗІ від НСД (у тому числі захищений від НСД компонент обчислювальної системи), мета експертизи має передбачати оцінювання відповідності

реалізованих в ОЕ функціональних послуг безпеки (ФПБ) та рівня гарантій коректності їх реалізації вимогам НД ТЗІ 2.5-004-99. Крім цього, мета експертизи може передбачати оцінювання відповідності ОЕ вимогам чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу (НД ТЗІ 2.5-007-2007, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 тощо) або будь-яким іншим вимогам.

5.4 Якщо ОЕ являє собою КСЗІ, яка є невід'ємною складовою частиною ІТС, мета експертизи має передбачати оцінювання відповідності КСЗІ технічному завданню, вимогам чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу (НД ТЗІ 2.5-007-2007, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 тощо), вимогам інших чинних нормативних документів і визначення можливості введення КСЗІ в складі ІТС в експлуатацію та забезпечення захисту інформації відповідно до встановлених вимог.

5.5 Згідно з вимогами Положення про державну експертизу в сфері технічного захисту інформації експертиза може бути первинною, додатковою та контрольною. Первинна експертиза є основним видом експертизи і передбачає виконання Організатором експертизи усіх необхідних заходів, визначених у Положенні про державну експертизу в сфері технічного захисту інформації та необхідних для підготовки та прийняття рішення щодо відповідності ОЕ висунутим вимогам. Додаткова експертиза проводиться стосовно ОЕ, щодо яких відкрилися нові наукові та науково-технічні обставини або в зв'язку із закінченням терміну дії документів, що засвідчують результати експертизи. Контрольна експертиза проводиться іншим Організатором експертизи з ініціативи Замовника за наявності у нього обґрунтованих претензій до висновку первинної чи додаткової експертизи або з ініціативи уповноваженого державного органу для перевірки висновку первинної чи додаткової експертизи.

5.6 Загальний порядок організації та проведення робіт з експертизи, права, обов’язки та відповідальність суб’єктів експертизи, а також порядок взаємодії суб’єктів експертизи визначаються Положенням про державну експертизу в сфері технічного захисту інформації. У частині, що стосується безпосередньо виконання експертних робіт, цей порядок передбачає збирання Експертами та подальше оцінювання необхідних свідоцтв (сукупності свідоцтв), які характеризують ступінь відповідності ОЕ висунутим вимогам, з подальшим формулюванням результатів оцінювання у вигляді відповідного Експертного висновку.

5.7 З метою забезпечення максимальної достовірності та повноти результатів при організації та проведенні експертизи мають бути дотримані такі основні принципи її проведення:

- незалежність Організаторів експертизи та Експертів. Організатори експертизи та Експерти мають бути незалежні у своїй діяльності та невідповідальні за створення (розроблення) ОЕ. Незалежність є підставою для неупередженості при проведенні експертизи та об'єктивності при формулюванні висновків за результатами експертизи. Дотримання принципу незалежності означає, що Організаторами експертизи (Експертами) не можуть бути організації (особи), для яких може бути документально підтверджено причетність до будь-яких етапів робіт зі створення ОЕ, у тому числі надання консультаційних послуг, які стосуються виконання окремих етапів робіт зі створення ОЕ, обґрунтування та вибору певних проектних рішень.

Примітка. Зазначений принцип не заперечує залучення як Організаторів експертизи та Експертів організацій та осіб, що причетні до створення (розроблення) окремих компонентів складеного ОЕ, стосовно яких проведено окремі експертизи та наявні Експертні висновки, зареєстровані в установленому порядку;

- повнота оцінювання. Експертні роботи повинні охоплювати всі аспекти, які стосуються виконання вимог, що висуваються до ОЕ. Крім того, повнота оцінювання визначається достатністю наданих Замовником експертизи (Розробником ОЕ) матеріалів та документів, а також рівнем їх відповідності висунутим вимогам. Повнота оцінювання є необхідною умовою для формування об'єктивних висновків за результатами експертизи;

- оцінювання на підставі одержаних свідоцтв (сукупності свідоцтв). Проведення

оцінювання на підставі свідоцтв є єдиним способом, який дозволяє одержати повторювані висновки за результатами експертизи, що підвищує довіру до таких висновків. Для цього повинна забезпечуватися можливість повторної перевірки свідоцтв оцінювання (сукупності свідоцтв).

Примітка. Основними джерелами свідоцтв оцінювання можуть бути: одержані від Замовника експертизи (Розробника ОЕ) документи та матеріали; усні висловлювання та письмові відповіді співробітників Замовника експертизи (Розробника ОЕ), одержані у процесі проведених опитувань; результати спостереження за діяльністю співробітників Замовника експертизи (Розробника ОЕ); результати самостійного виконання Експертами експертних робіт;

- достовірність свідоцтв оцінювання. В Експертів повинна бути впевненість у достовірності наявних свідоцтв оцінювання.

Примітка. Довіра до документальних свідоцтв підвищується при підтвердженні їх достовірності третьою стороною або керівництвом Замовника експертизи (Розробника ОЕ). Довіра до фактів, одержаних при опитуванні співробітників Замовника експертизи (Розробника ОЕ), підвищується при підтвердженні цих фактів з різних джерел. Довіра до фактів, отриманих при спостереженні за діяльністю співробітників Замовника експертизи (Розробника ОЕ), підвищується, якщо вони отримані безпосередньо при функціонуванні процедур або процесів, які перевіряються;

- компетентність Експертів. Компетентність базується на наявності в Експерта необхідних знань та навичок в галузі технічного захисту інформації та на здатності застосовувати їх під час виконання експертних робіт.

Примітка. Відповідно до Положення про державну експертизу в сфері технічного захисту інформації контроль компетентності Експертів здійснюється Замовником. На вимогу Замовника Експерт зобов'язаний надати йому документи, які підтверджують його досвід та рівень кваліфікації;

- етичність поведінки Експертів. Етичність поведінки передбачає відповідальність, непідкупність, неупередженість.

5.8 З метою виконання зазначених принципів Експерти повинні дотримуватися таких основних принципів виконання оцінювання:

- об'єктивність – результати оцінювання повинні ґрунтуватися на використовуваних свідоцтвах та містити мінімум суб'єктивної думки Експерта;
- неупередженість – результати оцінювання повинні бути неупередженими навіть у тих випадках, коли потрібне суб'єктивне судження;
- повторюваність – дії того самого Експерта, виконувані з використанням однієї і тієї самої сукупності свідоцтв, повинні привести до одних і тих же результатів;
- відтворюваність – дії іншого Експерта, виконувані з використанням однієї і тієї самої сукупності свідоцтв, повинні привести до одних і тих же результатів;
- коректність – повинні виконуватися лише ті дії Експерта, які потрібні, і вони повинні виконуватися належним чином, щоб забезпечити правильні результати оцінювання;
- достатність – кожний вид дій Експерта повинен здійснюватися до рівня, необхідного для задоволення всіх висунутих вимог;
- прийнятність – кожна дія Експерта повинна сприяти підвищенню довіри до результатів оцінювання, щонайменше – пропорційно витраченим зусиллям.

5.9 Якщо ОЕ являє собою ЗТЗІ від НСД (у тому числі захищений від НСД компонент обчислювальної системи), проведення первинної експертизи повинно передбачати виконання таких етапів експертних робіт:

1. З оцінювання ФПБ:
   - попередній аналіз оцінюваного ОЕ;
   - розроблення програми випробувань ФПБ;
   - розроблення методики випробувань ФПБ;
   - проведення випробувань засобів реалізації ФПБ;
   - аналіз, документування та затвердження результатів випробувань ФПБ.

2. З оцінювання рівня гарантій коректності реалізації ФПБ:

- ознайомлення з оцінюваним ОЕ, збирання та аналіз матеріалів (документів), що характеризують організацію процесу розроблення, виробництва та постачання Замовнику оцінюваного ОЕ;
- розроблення програми перевірки дотримання вимог до рівня гарантій;
- розроблення методики перевірки дотримання вимог до рівня гарантій;
- виконання оцінювання рівня гарантій згідно з розробленими програмою та методикою;
- аналіз та документування результатів оцінювання рівня гарантій;
- оцінювання (за необхідності) відповідності ОЕ вимогам чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу або іншим вимогам, які висуваються до нього;
- документування та затвердження результатів експертизи.

Проведення додаткової або контрольної експертизи ЗТЗІ від НСД може передбачати як виконання усіх робіт, передбачених для випадку первинної експертизи, так і (за погодженням з уповноваженим державним органом) лише тих робіт, які обумовлені причинами проведення відповідної експертизи.

Детальний опис порядку проведення робіт з експертизи ЗТЗІ від НСД наведено в розділі 6.

5.10 Якщо ОЕ являє собою КСЗІ, яка є невід'ємною складовою частиною певної ІТС, проведення первинної експертизи має передбачати виконання таких етапів експертних робіт:

- попереднє ознайомлення з ОЕ;
- поглиблене обстеження ОЕ;
- розроблення програми проведення експертизи КСЗІ;
- розроблення методики проведення експертизи КСЗІ;
- проведення експертних випробувань та досліджень ОЕ за розробленими програмою та методикою;
- документування та затвердження результатів експертизи.

Проведення додаткової або контрольної експертизи КСЗІ може передбачати як виконання усіх робіт, передбачених для випадку первинної експертизи, так і (за погодженням з уповноваженим державним органом) лише тих робіт, які обумовлені причинами проведення відповідної експертизи.

Детальний опис порядку проведення робіт з експертизи КСЗІ наведено в розділі 7.

6 Опис порядку проведення робіт з експертизи засобів технічного захисту інформації від несанкціонованого доступу

6.1 Порядок проведення робіт з первинної експертизи засобів технічного захисту інформації від несанкціонованого доступу

6.1.1 Роботи з первинної експертизи ЗТЗІ від НСД проводяться в такій послідовності:

- оцінювання ФПБ;
- оцінювання рівня гарантій коректності реалізації ФПБ;
- оцінювання (за необхідності) відповідності ОЕ вимогам чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу або будь-яким іншим вимогам (далі – додатковим вимогам);
- документування та затвердження результатів експертизи.

6.1.2 Оцінювання ФПБ передбачає виконання таких етапів експертних робіт:

- попередній аналіз оцінюваного ОЕ;
- розроблення програми випробувань ФПБ;
- розроблення методики випробувань ФПБ;
- проведення випробувань засобів реалізації ФПБ;
- аналіз та документування результатів випробувань ФПБ.

6.1.2.1 Метою етапу попереднього аналізу оцінюваного ОЕ є прийняття рішення щодо можливості проведення робіт з експертизи ОЕ, визначення обсягів та плану робіт.

6.1.2.1.1 Послідовність та обсяг робіт Експерта на етапі попереднього аналізу оцінюваного ОЕ залежать від варіанта подання ОЕ на експертизу, тобто:

- ОЕ подано на експертизу Розробником разом з проектною та експлуатаційною документацією, при цьому в проектній документації Розробником визначено функціональні специфікації ОЕ;
- ОЕ подано на експертизу Розробником, який володіє інформацією щодо особливостей реалізації в ОЕ функцій захисту, разом з експлуатаційною документацією, при цьому Розробником не визначено функціональних специфікацій ОЕ;
- ОЕ подано на експертизу представником Розробника (Заявником), який не володіє інформацією щодо особливостей реалізації в ОЕ функцій захисту, разом з експлуатаційною документацією, при цьому Розробником не визначено функціональних специфікацій ОЕ.

6.1.2.1.2 На етапі попереднього аналізу оцінюваного ОЕ Експертами повинні бути виконані:

- дослідження оцінюваного ОЕ з метою перевірки його готовності до виконання експертних робіт;
- визначення (ідентифікація) або уточнення множини випробовуваних ФПБ, їх рівнів та політики;
- документування отриманих результатів та прийняття рішення щодо проведення подальших етапів робіт або щодо їх припинення.

6.1.2.1.3 При виконанні робіт з попереднього аналізу оцінюваного ОЕ Експертам слід керуватися відповідними методичними рекомендаціями, наведеними в п. 5.2 НД ТЗІ 2.7-009-09.

6.1.2.1.4 На основі результатів дослідження оцінюваного ОЕ, якщо отримані результати підтверджують його готовність до проведення подальших робіт (слід розуміти, як мінімум, підтвердження працездатності ОЕ у заявлених умовах та функціонування згідно з характеристиками, наведеними в експлуатаційній документації), повинно бути здійснено визначення (ідентифікацію) або уточнення множини випробовуваних ФПБ, їх рівнів та політики. За наявності у проектній або експлуатаційній документації чітко визначених функціональних специфікацій ОЕ таку ідентифікацію (уточнення) можна здійснювати шляхом аналізу відповідності формальних вимог до ФПБ (функцій захисту) опису порядку реалізації відповідних функцій в оцінюваному ОЕ, наведеного в проектній документації, а також результатів анкетування спеціалістів Розробника з використанням переліку спеціальних запитань. За відсутності у проектній документації чітко визначених функціональних специфікацій ОЕ таку ідентифікацію можна здійснювати шляхом проведення Експертами досліджень оцінюваного ОЕ, метою яких є ідентифікація (виявлення наявності) механізмів захисту та реалізованих ними ФПБ, оцінювання можливості запобігання ними певним загрозам інформації з подальшим уточненням політики ФПБ та з використанням переліку спеціальних запитань, наведеного в Додатку А до НД ТЗІ 2.7-009-09.

6.1.2.1.5 При здійсненні ідентифікації ФПБ, уточненні їх рівнів і політики Експертам слід керуватися відповідними методичними рекомендаціями, наведеними в розділі 6 НД ТЗІ 2.7-009-09.

6.1.2.1.6 Результатом виконання робіт з попереднього аналізу має бути звіт, в якому Експерти, що здійснювали аналіз, повинні викласти свою думку з приводу повноти та змісту наданих матеріалів, обґрунтувати рішення щодо можливості та доцільності проведення подальших робіт з експертизи або щодо їх припинення, а у випадку позитивного рішення – навести пропозиції щодо плану та послідовності проведення подальших робіт. Крім цього, у випадку позитивного рішення щодо проведення подальших робіт, результатом цього етапу має також бути узгоджений з Розробником або Заявником документ, що містить уточнений опис переліку та політики ФПБ, на відповідність яким здійснюватиметься перевірка ОЕ, наприклад, у вигляді технічних вимог до оцінюваного ОЕ в частині реалізації ФПБ та опису порядку реалізації цих вимог. Цей документ (у випадку успішного завершення експертизи) повинен бути поданий як невід'ємний додаток до Експертного висновку щодо відповідності оцінюваного ОЕ вимогам НД ТЗІ.

6.1.2.2 Метою етапу розроблення програми випробувань ФПБ є розроблення та погодження в установленому порядку програми випробувань ФПБ.

6.1.2.2.1 Як вхідні дані на етапі розроблення програми випробувань ФПБ Експертом повинні використовуватися:

- проектна документація (за наявності) на оцінюваний ОЕ (наприклад, матеріали передпроектних досліджень, технічне завдання, технічні вимоги, матеріали ескізного, технічного та робочого проектів тощо), яка, зокрема містить функціональні специфікації ОЕ у вигляді переліку реалізованих у ОЕ ФПБ згідно з НД ТЗІ 2.5-004-99 та опису їх політики;

- документація (за наявності), що містить результати проведених Розробником випробувань ОЕ (програма випробувань, методика випробувань, протоколи випробувань тощо);

- підготовлений на етапі попереднього аналізу документ, який містить уточнений опис переліку та політики ФПБ, наприклад, у вигляді уточнених технічних вимог до оцінюваного ОЕ, на відповідність яким має здійснюватися перевірка ОЕ.

6.1.2.2.2 У розробленій програмі випробувань ФПБ повинен бути наведений опис того, які властивості оцінюваного ОЕ мають бути перевірені під час проведення випробувань з метою підтвердження або спростування реалізації в оцінюваному ОЕ уточненого на етапі попереднього аналізу переліку ФПБ. При визначенні цих властивостей в першу чергу слід керуватися наведеними в НД ТЗІ 2.5-004-99 вимогами щодо політики окремих ФПБ різних рівнів, а також результатами етапу попереднього аналізу. Крім цього, можуть бути враховані такі чинники:

- результати випробувань, надані Розробником ОЕ. Повинні бути враховані: аргументи Розробника про достатність тестового покриття для тестування певних ФПБ; можливість розширення прийнятого Розробником підходу; повнота і коректність проведених Розробником випробувань ФПБ;

- відомі вразливості, характерні для того типу систем, до яких належить оцінюваний ОЕ, у тому числі наведені у матеріалах передпроектних досліджень;

- важливість різних ФПБ, реалізованих в оцінюваному ОЕ, з погляду запобігання можливим загрозам інформації;

- складність (комплексність) засобів реалізації ФПБ в оцінюваному ОЕ;

- можливість неявної перевірки окремих ФПБ;

- наявність в оцінюваному ОЕ нових або нерегламентованих НД ТЗІ 2.5-004-99 функцій захисту.

6.1.2.2.3 При розробленні та документуванні програми випробувань ФПБ Експертам слід керуватися відповідними методичними вказівками, наведеними в розділі 7 НД ТЗІ 2.7-009-09.

6.1.2.2.4 Результатом етапу повинна бути розроблена та згідно з вимогами Положення

про державну експертизу в сфері технічного захисту інформації погоджена із Замовником експертизи та уповноваженим державним органом програма випробувань ФПБ.

6.1.2.3 Метою етапу розроблення методики випробувань ФПБ є розроблення та погодження в установленому порядку методики випробувань ФПБ.

6.1.2.3.1 У процесі підготовки методики випробувань повинні бути виконані дії з вибору тестових процедур, методів випробувань і відповідних перевірок, розроблення (вибору) необхідних для випробувань програмних та/або апаратних засобів (засобів випробувань). При цьому Експерт, залежно від варіанта подання ОЕ на експертизу, на цьому етапі повинен використовувати:

- ОЕ у працездатному стані, підготовлений для проведення випробувань;
- проектну документацію (за наявності) на оцінюваний ОЕ (наприклад, матеріали передпроектних досліджень, технічне завдання, технічні вимоги, матеріали ескізного, технічного та робочого проектів тощо), яка містить функціональні специфікації ОЕ у вигляді переліку реалізованих у ОЕ ФПБ згідно з НД ТЗІ 2.5-004-99 та опису їх політики;
- експлуатаційну документацію на оцінюваний ОЕ (наприклад, опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратора; настанову користувача тощо);
- документацію (за наявності), що містить результати проведених Розробником випробувань ОЕ (програму випробувань, методику випробувань, протоколи випробувань тощо);
- підготовлений на етапі попереднього аналізу документ, який містить уточнений опис переліку та політики ФПБ, наприклад, у вигляді уточнених технічних вимог до оцінюваного ОЕ, на відповідність яким повинна здійснюватися перевірка ОЕ;
- підготовлену на попередньому етапі програму випробувань ФПБ.

6.1.2.3.2 У процесі розроблення методики випробувань, яка описує порядок та засоби проведення випробувань кожної ФПБ, зазначеної у програмі випробувань, Експерт повинен, з урахуванням уточнених вимог до ФПБ, визначених на попередніх етапах, обрати найбільш прийнятний спосіб перевірки кожної ФПБ.

6.1.2.3.3 При розробленні методики випробувань повинні враховуватися такі основні вимоги щодо загального підходу (стратегії) проведення випробувань:

- забезпечення достатності тестового покриття для перевірки кожної заявленої ФПБ з урахуванням її політики та особливостей реалізації;
- зниження кількості взаємозалежних методів випробувань (перевірок) різних ФПБ;
- забезпечення максимальної незалежності від стану оцінюваного ОЕ, тобто наявності засобів генерації всієї необхідної тестової та службової інформації для кожної перевірки, незалежних від фактів та результатів виконання попередніх перевірок;
- забезпечення максимального використання засобів автоматизації при проведенні випробувань, у тому числі для генерації тестової інформації, виконання підготовчих дій і безпосереднього виконання перевірок;
- забезпечення повторюваності процесу і результатів випробувань.

6.1.2.3.4 При виборі тестових процедур, методів випробувань і відповідних перевірок, залежно від виду оцінюваного ОЕ, можуть бути обрані такі підходи:

- підхід з використанням монолітного тестування (метод "чорної скриньки"), який передбачає використання в процесі проведення випробувань лише зовнішніх документованих інтерфейсів оцінюваного ОЕ, завдяки чому випробування можуть бути здійснені без використання додаткових спеціально розроблюваних засобів;
- підхід з використанням функціонально-синтетичного тестування (метод "білої скриньки"), який передбачає використання в процесі проведення випробувань як зовнішніх

документованих інтерфейсів ОЕ, так і внутрішньосистемних інтерфейсів, але потребує спеціально розроблених засобів випробувань, що реалізують внутрішньосистемні інтерфейси доступу до функціональних компонентів оцінюваного ОЕ;

- змішаний підхід (метод "сірої скриньки"), при використанні якого намагаються максимальну кількість перевірок здійснювати з використанням зовнішніх документованих інтерфейсів, а внутрішньосистемні інтерфейси використовувати лише для тих перевірок, які не можна виконати в інший спосіб.

6.1.2.3.5 Оскільки згідно з положеннями НД ТЗІ 2.5-004-99 наявність, повнота та ступінь детальності опису внутрішньосистемних інтерфейсів залежать від заявленого рівня гарантій коректності реалізації ФПБ, вибір підходу щодо проведення випробувань повинен здійснюватися з урахуванням цього рівня гарантій.

6.1.2.3.6 При розробленні та документуванні методики випробувань ФПБ Експертам слід керуватися відповідними методичними вказівками, наведеними в розділі 8 НД ТЗІ 2.7-009-09.

6.1.2.3.7 Результатом етапу має бути розроблена та згідно з вимогами Положення про державну експертизу в сфері технічного захисту інформації погоджена з уповноваженим державним органом методика випробувань ФПБ.

6.1.2.4 Метою етапу проведення випробувань засобів реалізації ФПБ є здійснення перевірки згідно із затвердженою методикою та фіксації (у відповідному журналі проведення випробувань, форма ведення якого може бути аналогічною формі журналу випробувань, встановленій ДСТУ 2851-94) фактів реалізації в оцінюваному ОЕ заявленого та уточненого Експертом переліку ФПБ, а також підтвердження їх політики, уточненої Експертом на етапі попереднього аналізу.

6.1.2.4.1 Результатом цього етапу мають бути відомості, зафіксовані в журналі проведення випробувань, в яких, з посиланням на відповідні пункти методики випробувань ФПБ, зафіксовано висновки Експерта щодо результатів виконання перевірок.

6.1.2.5 Метою етапу аналізу та документування результатів оцінювання ФПБ є проведення аналізу отриманих у процесі проведення випробувань та зафіксованих відповідним чином результатів з подальшим документуванням результатів оцінювання.

6.1.2.5.1 На підставі результатів проведеного аналізу має бути складено (у частині, що стосується оцінювання ФПБ) протокол експертизи, в якому повинно бути наведено результати, отримані під час проведення випробувань за кожним пунктом методики випробувань ФПБ, та зроблено висновок щодо відповідності або невідповідності наданого для випробувань ОЕ висунутим вимогам.

6.1.2.5.2 При виконанні аналізу та документуванні результатів оцінювання ФПБ слід керуватися відповідними методичними вказівками, наведеними в розділі 9 НД ТЗІ 2.7-009-09, а також рекомендаціями щодо викладення змістовної частини протоколу експертизи ЗТЗІ від НСД, наведеними в Додатку Г.

6.1.3 Оцінювання рівня гарантій коректності реалізації ФПБ передбачає виконання таких етапів експертних робіт:

- ознайомлення з оцінюваним ОЕ, збирання та аналіз матеріалів (документів), що характеризують організацію процесу його розроблення, виробництва та постачання Замовнику;
- розроблення програми перевірки дотримання вимог до рівня гарантій;
- розроблення методики перевірки дотримання вимог до рівня гарантій;
- виконання оцінювання рівня гарантій згідно з розробленими програмою та методикою;
- аналіз та документування результатів оцінювання рівня гарантій.

6.1.3.1 Метою етапу ознайомлення з оцінюваним ОЕ, збирання та аналізу матеріалів

(документів) є прийняття рішення щодо можливості проведення робіт з оцінювання рівня гарантій коректності реалізації ФПБ у наданому на експертизу ОЕ, визначення обсягів та плану подальших робіт.

6.1.3.1.1 Послідовність та обсяг робіт Експерта на етапі ознайомлення з оцінюваним ОЕ залежать від варіанта подання ОЕ на експертизу, тобто:

- ОЕ подано на експертизу разом з проектною, експлуатаційною та супровідною документацією, при цьому в проектній документації Розробником ОЕ визначено функціональні специфікації ОЕ;
- ОЕ подано на експертизу разом із супровідною та експлуатаційною документацією, в якій Розробником ОЕ не визначено функціональних специфікацій ОЕ.

6.1.3.1.2 На етапі ознайомлення з ОЕ, збирання та аналізу матеріалів Експертами повинні бути виконані такі дії:

- ознайомлення з оцінюваним ОЕ з метою перевірки його готовності до виконання робіт з експертизи (може бути виконано в процесі проведення робіт з оцінювання ФПБ);
- попередній аналіз наданих матеріалів з метою попереднього визначення рівня гарантій, який може бути призначено ОЕ за результатами експертизи, та визначення наявності необхідних для виконання оцінювання матеріалів (документів), перелік та зміст яких визначається вимогами до цього рівня гарантій;
- доопрацювання, за необхідності, одержаних матеріалів (або одержання та аналіз додатково запитаних Експертом матеріалів) з метою задоволення вимог відповідного рівня гарантій, встановленого НД ТЗІ 2.5-004-99;
- документування отриманих результатів та прийняття рішення щодо проведення подальших етапів робіт або щодо їх припинення.

6.1.3.1.3 На основі результатів ознайомлення з оцінюваним ОЕ, якщо отримані результати підтверджують його готовність до проведення подальших робіт, необхідно проводити аналіз наданих матеріалів з метою попереднього визначення рівня гарантій, який може бути призначено ОЕ за результатами експертизи, після чого визначати наявність всіх необхідних для виконання оцінювання матеріалів (документів), перелік та зміст яких визначається вимогами до відповідного рівня гарантій (з уточненням, за необхідності та з урахуванням вимог цього рівня гарантій, їх складу та змісту). У випадку наявності в проектній або експлуатаційній документації чітко визначених функціональних специфікацій ОЕ, жодних обмежень на попередньо визначений рівень гарантій не накладається, цей рівень визначається лише вмістом наданих документів. За відсутності в наданих матеріалах чітко визначених функціональних специфікацій ОЕ такі специфікації та опис порядку їх реалізації (на рівні деталізації, який задовольняє, як мінімум, вимоги рівня Г-1 критеріїв гарантій щодо послідовності розробки), за згодою Розробника (Заявника), можуть бути розроблені Експертом (може бути використаний документ відповідного змісту, розроблений у процесі проведення робіт з оцінювання ФПБ). Оскільки розроблення функціональних специфікацій ОЕ та опису порядку їх реалізації Експертом не надають можливості впевнитися в дотриманні Розробником у процесі проектування та реалізації ОЕ вимог забезпечення відповідності специфікацій комплексу засобів захисту (КЗЗ) ОЕ різного рівня деталізації (функціональні специфікації, проект архітектури, детальний проект, реалізація), максимальний рівень гарантій, який може бути призначений такому ОЕ за результатами експертизи, становить Г-1.

6.1.3.1.4 При виконанні робіт з ознайомлення з ОЕ, збирання та аналізу матеріалів Експертам слід керуватися відповідними методичними рекомендаціями, наведеними в розділі 6 НД ТЗІ 2.7-010-09.

6.1.3.1.5 Результатом виконання робіт з ознайомлення з ОЕ, збирання та аналізу матеріалів має бути звіт, в якому Експерти, які здійснювали аналіз, повинні викласти свою думку щодо повноти та змісту наданих матеріалів, обґрунтувати рішення щодо можливості

та доцільності проведення подальших робіт з експертизи або щодо їх припинення, а у випадку позитивного рішення – попередньо визначити рівень гарантій, який може бути призначено ОЕ за результатами експертизи, та надати пропозиції щодо плану та послідовності проведення подальших робіт. Крім цього, у випадку позитивного рішення щодо проведення подальших робіт для ОЕ, який надано на експертизу без чітко визначених функціональних специфікацій, результатом етапу повинен також бути узгоджений з Розробником або Заявником документ, який містить опис переліку та політики ФПБ, які реалізуються ОЕ, наприклад, у вигляді технічних вимог до оцінюваного ОЕ у частині реалізації ФПБ та опису порядку реалізації цих вимог (може бути використаний документ відповідного змісту, розроблений у процесі проведення робіт з оцінювання ФПБ).

6.1.3.2 Метою етапу розроблення програми перевірки дотримання вимог до рівня гарантій є розроблення та погодження в установленому порядку програми перевірки дотримання вимог до заявленого Розробником (Заявником) та уточненого Експертом рівня гарантій коректності реалізації ФПБ у процесі розроблення, виробництва та постачання ОЕ.

6.1.3.2.1 Як вхідні дані на цьому етапі Експертом мають використовуватися всі матеріали, які були зібрані, проаналізовані та уточнені (або розроблені Експертом) на попередньому етапі робіт.

6.1.3.2.2 У розробленій програмі перевірки дотримання вимог до рівня гарантій повинен бути наведений опис того, відповідність яким саме вимогам критеріїв гарантій, встановлених НД ТЗІ 2.5-004-99, а також яким саме вимогам інших чинних нормативних документів має бути перевірено з метою підтвердження або спростування їх дотримання у процесі розроблення, виробництва та постачання ОЕ.

6.1.3.2.3 При розробленні та документуванні програми перевірки дотримання вимог до рівня гарантій Експертам слід керуватися відповідними методичними вказівками, наведеними в розділі 7 НД ТЗІ 2.7-010-09.

6.1.3.2.4 Результатом етапу повинна бути розроблена та згідно з вимогами Положення про державну експертизу в сфері технічного захисту інформації погоджена із Замовником експертизи та уповноваженим державним органом програма перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ в оцінюваному ОЕ.

6.1.3.3 Метою етапу розроблення методики перевірки дотримання вимог до рівня гарантій є розроблення та погодження в установленому порядку методики перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ у процесі розроблення, виробництва та постачання ОЕ. У процесі розроблення методики перевірки має також бути визначена необхідність відвідування Експертом підприємства – Розробника ОЕ, календарний план проведення таких відвідувань та обсяг перевірок, виконуваних під час відвідувань.

6.1.3.3.1 Як вхідні дані на цьому етапі Експертом повинні використовуватися:

- матеріали, що характеризують організацію процесу розроблення, виробництва та постачання Замовнику оцінюваного ОЕ, які були зібрані, проаналізовані та уточнені (або розроблені Експертом) на етапі збирання та аналізу матеріалів;
- розроблена на попередньому етапі програма перевірки дотримання вимог до рівня гарантій.

6.1.3.3.2 У розробленій методиці перевірки дотримання вимог до рівня гарантій повинен бути наведений опис того, які саме перевірки, з використанням яких документів (матеріалів) та в якій послідовності мають бути виконані з метою підтвердження або спростування дотримання в процесі розроблення, виробництва та постачання ОЕ вимог критеріїв гарантій певного рівня, встановлених НД ТЗІ 2.5-004-99, а також вимог інших чинних нормативних документів.

6.1.3.3.3 При розробленні та документуванні методики перевірки дотримання вимог до рівня гарантій Експертам слід керуватися відповідними методичними вказівками, наведеними в розділі 8 НД ТЗІ 2.7-010-09.

6.1.3.3.4 Результатом етапу має бути розроблена та згідно з вимогами Положення про державну експертизу в сфері технічного захисту інформації погоджена з уповноваженим державним органом методика перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ в оцінюваному ОЕ, а також підготовлений та узгоджений з Розробником календарний план проведення відвідувань підприємства – Розробника ОЕ з метою перевірки умов розроблення, виробництва та постачання ОЕ.

6.1.3.4 Метою етапу оцінювання рівня гарантій є здійснення, згідно із затвердженою методикою, певних дій щодо оцінювання (перевірки, аналізу та/або верифікації зібраних матеріалів, у тому числі під час відвідування підприємства – Розробника ОЕ) з фіксацією (у відповідному журналі результатів проведення перевірок рівня гарантій, форма ведення якого може бути аналогічною формі журналу випробувань, встановленій ДСТУ 2851-94) висновків Експерта щодо результатів виконання певних пунктів методики.

6.1.3.4.1 При виконанні оцінювання рівня гарантій коректності реалізації ФПБ Експертам слід керуватися відповідними методичними вказівками, наведеними в розділі 9 НД ТЗІ 2.7-010-09.

6.1.3.4.2 Результатом етапу мають бути відомості, зафіксовані в журналі результатів проведення перевірок рівня гарантій, в яких з посиланням на відповідні пункти методики перевірки рівня гарантій та використані при цьому матеріали зафіксовано висновки Експерта щодо результатів виконання дій з оцінювання.

6.1.3.5 Метою етапу аналізу та документування результатів оцінювання рівня гарантій є проведення аналізу отриманих у процесі проведення оцінювання та зафіксованих у відповідному журналі результатів з подальшим документуванням результатів оцінювання.

6.1.3.5.1 На підставі результатів проведеного аналізу має бути складено (у частині, що стосується оцінювання рівня гарантій коректності реалізації ФПБ) протокол експертизи, в якому повинно бути узагальнено результати, отримані під час проведення перевірок за кожним пунктом методики перевірки рівня гарантій, та зроблено висновок щодо дотримання або недотримання в процесі розроблення, виробництва та постачання ОЕ вимог критеріїв гарантій певного рівня, встановлених НД ТЗІ 2.5-004-99.

6.1.3.5.2 При виконанні аналізу та документуванні результатів оцінювання рівня гарантій слід керуватися відповідними методичними вказівками, наведеними в розділі 10 НД ТЗІ 2.7-010-09, а також рекомендаціями щодо викладення змістовної частини протоколу експертизи ЗТЗІ від НСД, наведеними в Додатку Г.

6.1.4 Оцінювання відповідності ОЕ додатковим вимогам передбачає виконання таких етапів експертних робіт:

- розроблення програми випробувань ОЕ на відповідність додатковим вимогам;
- розроблення методики випробувань ОЕ на відповідність додатковим вимогам;
- проведення випробувань ОЕ на відповідність додатковим вимогам;
- аналіз та документування результатів оцінювання ОЕ на відповідність додатковим вимогам.

6.1.4.1 Метою етапу розроблення програми випробувань є розроблення та погодження в установленому порядку програми випробувань ОЕ на відповідність додатковим вимогам.

6.1.4.1.1 Як вхідні дані на етапі розроблення програми випробувань Експертом повинні використовуватися:

- документ (документи), в яких визначено додаткові вимоги;
- проектна документація на оцінюваний ОЕ (наприклад, матеріали передпроектних досліджень, технічне завдання, технічні вимоги, матеріали ескізного, технічного та робочого проектів тощо), яка містить опис порядку реалізації додаткових вимог;
- документація (за наявності), що містить результати проведених Розробником випробувань ОЕ (програма випробувань, методика випробувань, протоколи випробувань

тощо) у частині, що стосується перевірки відповідності додатковим вимогам.

6.1.4.1.2 У розробленій програмі випробувань має бути наведений опис того, які властивості оцінюваного ОЕ повинні бути перевірені під час проведення випробувань з метою підтвердження або спростування відповідності ОЕ додатковим вимогам.

6.1.4.1.3 При розробленні та документуванні програми випробувань Експерти можуть враховувати методичні вказівки щодо розроблення та документування програми випробувань ФПБ, наведені в розділі 7 НД ТЗІ 2.7-009-09.

6.1.4.1.4 Результатом етапу повинна бути розроблена та згідно з вимогами Положення про державну експертизу в сфері технічного захисту інформації погоджена із Замовником експертизи та уповноваженим державним органом програма випробувань ОЕ на відповідність додатковим вимогам.

6.1.4.2 Метою етапу розроблення методики випробувань є розроблення та погодження в установленому порядку методики випробувань ОЕ на відповідність додатковим вимогам.

6.1.4.2.1 У процесі підготовки методики випробувань мають також бути виконані дії з вибору тестових процедур, методів випробувань і відповідних перевірок, розроблення (вибору) необхідних для випробувань програмних та/або апаратних засобів (засобів випробувань). При цьому Експерт залежно від варіанта подання ОЕ на експертизу на цьому етапі повинен використовувати:

- ОЕ у працездатному стані, підготовлений для проведення випробувань;
- документ (документи), в яких визначено додаткові вимоги;
- проектну документацію на оцінюваний ОЕ (наприклад, матеріали передпроектних досліджень, технічне завдання, технічні вимоги, матеріали ескізного, технічного та робочого проектів тощо), яка містить опис порядку реалізації додаткових вимог;
- документацію (за наявності), що містить результати проведених Розробником випробувань ОЕ (програма випробувань, методика випробувань, протоколи випробувань тощо) у частині, що стосується перевірки відповідності додатковим вимогам;
- підготовлену на попередньому етапі програму випробувань ОЕ на відповідність додатковим вимогам.

6.1.4.2.2 При виборі тестових процедур, методів випробувань і відповідних перевірок залежно від виду оцінюваного ОЕ доцільно обирати підходи, аналогічні використовуваним при проведенні випробувань засобів реалізації ФПБ.

6.1.4.2.3 При розробленні та документуванні методики випробувань ОЕ на відповідність додатковим вимогам Експерти можуть враховувати методичні вказівки щодо розроблення та документування методики випробувань ФПБ, наведені в розділі 8 НД ТЗІ 2.7-009-09.

6.1.4.2.4 Результатом етапу повинна бути розроблена та згідно з вимогами Положення про державну експертизу в сфері технічного захисту інформації погоджена з уповноваженим державним органом методика випробувань ОЕ на відповідність додатковим вимогам.

6.1.4.3 Метою етапу випробувань є здійснення, згідно із затвердженою методикою, перевірки та фіксації (у відповідному журналі проведення випробувань, форма ведення якого може бути аналогічною формі журналу випробувань, встановленій ДСТУ 2851-94) фактів реалізації в оцінюваному ОЕ властивостей, наявність або відсутність яких повинна бути перевірена з метою підтвердження або спростування відповідності ОЕ додатковим вимогам.

6.1.4.3.1 Результатом цього етапу повинні бути відомості, зафіксовані в журналі проведення випробувань, в яких з посиланням на відповідні пункти методики випробувань ОЕ на відповідність додатковим вимогам зафіксовано висновки Експерта щодо результатів виконання певних перевірок.

6.1.4.4 Метою етапу аналізу та документування результатів оцінювання на відповідність додатковим вимогам є проведення аналізу отриманих у процесі проведення

випробувань та зафіксованих відповідним чином результатів з подальшим документуванням результатів оцінювання.

6.1.4.4.1 На підставі результатів проведеного аналізу має бути складено (у частині, що стосується оцінювання відповідності ОЕ додатковим вимогам) протокол експертизи, в якому повинно бути наведено результати, отримані під час проведення випробувань за кожним пунктом методики випробувань, та зроблено висновок щодо відповідності або невідповідності наданого для випробувань ОЕ висунутим вимогам.

6.1.4.4.2 При виконанні аналізу та документуванні результатів оцінювання ФПБ слід керуватися рекомендаціями щодо викладення змістовної частини протоколу експертизи ЗТЗІ НСД, наведеними в Додатку Г.

6.1.5 Документування та затвердження результатів експертизи передбачає виконання таких робіт:

- оформлення та затвердження протоколу виконання робіт щодо експертизи ЗТЗІ від НСД (далі – протокол експертизи ЗТЗІ від НСД);
- оформлення, затвердження та надання Замовнику експертизи Експертного висновку за результатами експертизи ЗТЗІ від НСД.

6.1.5.1 При оформленні протоколу експертизи ЗТЗІ від НСД слід керуватися вимогами Положення про державну експертизу в сфері технічного захисту інформації щодо форми протоколу, а також рекомендаціями, наведеними в Додатку Г, щодо його змістовної частини.

6.1.5.2 При складанні Експертного висновку за результатами експертизи ЗТЗІ від НСД слід керуватися вимогами Положення про державну експертизу в сфері технічного захисту інформації щодо форми Експертного висновку, а також рекомендаціями, наведеними в Додатку Е, щодо його змістовної частини. При цьому слід зазначити, що поширювати результати експертизи не лише на конфігурацію ОЕ, яку було надано на експертизу, а і на оновлені конфігурації ОЕ дозволяється за таких умов:

- за результатами експертизи підтверджено рівень гарантій коректності реалізації ФПБ, не нижчий, ніж Г-4 згідно з НД ТЗІ 2.5-004-99;
- стосовно оновлених конфігурацій ОЕ проведено в повному обсязі приймальні випробування по зазначеній у п. А.2.18 Додатка А до НД ТЗІ 2.7-010-09 програмі та методиці випробувань ФПБ;
- затверджені в установленому порядку протоколи приймальних випробувань оновлених конфігурацій ОЕ передано до уповноваженого державного органу.

У всіх інших випадках поширювати результати експертизи на оновлені конфігурації ОЕ дозволяється лише за результатами додаткової експертизи, проведеної у порядку, наведеному в п. 6.2.

6.1.5.3 Якщо мета експертизи передбачала оцінювання ФПБ та рівня гарантій коректності їх реалізації, на титульному аркуші Експертного висновку повинен бути наведений узагальнений перелік ФПБ (функціональний профіль захищеності) згідно з НД ТЗІ 2.5-004-99, який реалізується оцінюваним ОЕ, а також рівень гарантій коректності реалізації ФПБ, підтверджені за результатами експертизи. Якщо крім оцінювання ФПБ та рівня гарантій коректності їх реалізації мета експертизи передбачала оцінювання відповідності ОЕ вимогам чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу (НД ТЗІ 2.5-007-2007, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 тощо), на титульному аркуші Експертного висновку мають бути зазначені відомості щодо відповідності ОЕ вимогам зазначених нормативних документів, а також висновки щодо можливості або неможливості застосування ОЕ з метою забезпечення захисту інформації в ІТС відповідного типу.

6.1.5.4 Затверджені Організатором експертизи протокол та Експертний висновок у порядку, визначеному в Положенні про державну експертизу в сфері технічного захисту

інформації, повинні бути зареєстровані уповноваженим державним органом та надані Замовнику експертизи. Замовнику експертизи рекомендується забезпечувати вільний доступ всіх зацікавлених підприємств, установ і організацій усіх форм власності до Експертних висновків за результатами експертизи ЗТЗІ від НСД з усіма додатками до них.

6.2 Особливості проведення робіт з додаткової та контрольної експертизи засобів технічного захисту інформації від несанкціонованого доступу

6.2.1 Проведення додаткової або контрольної експертизи ЗТЗІ від НСД може передбачати як виконання всіх експертних робіт, передбачених для випадку первинної експертизи, так і за погодженням з уповноваженим державним органом лише тих робіт, які обумовлені причинами проведення відповідної експертизи.

6.2.2 Перелік та обсяг експертних робіт з додаткової експертизи повинен визначатися на підставі обставин, які зумовили її проведення.

6.2.2.1 Якщо додаткова експертиза проводиться в зв'язку із закінченням терміну дії документів, що засвідчують результати попередньої експертизи, або достроково з метою оцінювання оновленої конфігурації ОЕ, перелік та обсяг відповідних експертних робіт повинні визначатися на підставі наявності та суті змін у реалізації конфігурації ОЕ, наданої на додаткову експертизу, порівняно з тією конфігурацією ОЕ, яка була надана на первинну експертизу.

6.2.2.2 Якщо змін у реалізації ОЕ не відбулося, тобто всі структурні компоненти ОЕ збігаються з тими, стосовно яких здійснювалися експертні роботи при проведенні первинної експертизи, в процесі додаткової експертизи достатньо перевірити та підтвердити цей факт шляхом проведення відповідних випробувань (перевірок) за затвердженими в установленому порядку програмою та методикою експертизи. У цьому випадку змістовна частина відповідних розділів Експертного висновку за результатами додаткової експертизи повинна відтворювати змістовну частину відповідних розділів Експертного висновку за результатами первинної експертизи.

6.2.2.3 Якщо у реалізації ОЕ відбулися зміни, тобто певні структурні компоненти ОЕ за своїм вмістом (фізичним поданням) не збігаються з тими, стосовно яких здійснювалися експертні роботи при проведенні первинної експертизи, в процесі додаткової експертизи необхідно обов’язково перевірити та підтвердити дотримання Розробником при розробленні та виробництві оновлених структурних компонентів ОЕ вимог рівня гарантій коректності реалізації ФПБ, визначеного за результатами первинної експертизи, а також коректне функціонування оновлених структурних компонентів ОЕ при реалізації політики тих ФПБ (функцій захисту), в реалізації яких вони використані. При цьому програма та методика додаткової експертизи повинна передбачати використання (у частині проведення відповідних перевірок) програми та методики первинної експертизи. У цьому випадку змістовна частина відповідних розділів Експертного висновку за результатами додаткової експертизи повинна формулюватися з урахуванням змістовної частини відповідних розділів Експертного висновку за результатами первинної експертизи.

6.2.2.4 Якщо додаткова експертиза проводиться у зв'язку з відкриттям нових наукових та/або науково-технічних обставин стосовно ОЕ, які потенційно можуть впливати на здатність ОЕ запобігати певним загрозам та/або функціонувати у визначеному в проектної документації порядку, вона повинна передбачати виконання у повному обсязі робіт з оцінювання ФПБ, оцінювання (за необхідності) відповідності ОЕ додатковим вимогам, документування та затвердження результатів експертизи. При виконанні відповідних робіт повинні враховуватися суть відповідних обставин та їх вплив на порядок функціонування ОЕ.

6.2.3 Перелік та обсяг експертних робіт з контрольної експертизи повинні визначатися з урахуванням тих висновків первинної або додаткової експертизи, стосовно яких виникли обґрунтовані претензії та які мають бути повторно перевірені.

6.2.4 Порядок проведення певних експертних робіт при проведенні додаткової або контрольної експертизи повинен відповідати порядку проведення аналогічних робіт у випадку проведення первинної експертизи.

7 Опис порядку проведення робіт з експертизи комплексних систем захисту інформації

7.1 Порядок проведення робіт з первинної експертизи комплексних систем захисту інформації

7.1.1 Первинна експертиза КСЗІ у загальному випадку передбачає виконання таких етапів експертних робіт:

- попереднє ознайомлення з ОЕ;
- поглиблене обстеження ОЕ;
- розроблення програми експертизи;
- розроблення методики експертизи;
- проведення експертних випробувань та досліджень ОЕ за розробленими програмою та методикою;
- документування та затвердження результатів експертизи.

7.1.1.1 Метою етапу попереднього ознайомлення з ОЕ є прийняття рішення щодо можливості проведення робіт з експертизи ОЕ, визначення обсягів та плану подальших робіт.

7.1.1.1.1 На етапі попереднього ознайомлення з ОЕ Експертами повинні бути виконані такі дії:

- попередній аналіз наданих Замовником вхідних даних щодо ОЕ з метою отримання та усвідомлення первинної інформації про основні вимоги із захисту інформації, які висуваються чинними нормативними документами та задоволення яких має забезпечуватися ОЕ, а також основні характеристики ОЕ, які повинні бути підтверджені в ході проведення експертизи;
- ознайомлення з ОЕ в реальних умовах функціонування ІТС з метою визначення ступеня його готовності до виконання робіт з експертизи;
- попередній аналіз наданої Замовником проектної, експлуатаційної та нормативно-розпорядчої документації щодо відповідності її складу вимогам чинних нормативних документів;
- документування отриманих результатів та прийняття рішення щодо проведення подальших етапів робіт або щодо їх припинення.

7.1.1.1.2 При виконанні попереднього аналізу вхідних даних щодо ОЕ Експерту слід користуватися відомостями, наведеними у матеріалах, наданих Замовником експертизи (технічне завдання на створення КСЗІ в ІТС та формуляр ІТС, наявність яких на цьому етапі є необхідною відповідно до вимог Положення про державну експертизу в сфері технічного захисту інформації), а також, за необхідності, поясненнями Замовника експертизи. За результатами проведеного аналізу зазначених матеріалів Експерт повинен сформувати попередню думку про:

- архітектуру та функціональний склад ІТС;
- клас та підклас ІТС як АС згідно з вимогами НД ТЗІ 2.5-005-99;
- інформаційні ресурси, оброблювані в ІТС, які відповідно до вимог чинного законодавства підлягають захисту, а також про технологію їх оброблення;
- характеристику інформації відповідно до встановленого Законом України "Про інформацію" та іншими законодавчими актами правового режиму та режиму доступу (відкрита

інформація (ВІ); відкрита інформація, що є власністю держави (ВІВД); конфіденційна інформація (КІ); конфіденційна інформація, що є власністю держави (КІВД); інформація, що становить державну таємницю (ІДТ)), яка міститься у певних інформаційних ресурсах та відповідно до вимог чинного законодавства потребує захисту;

- вимоги чинних нормативних документів щодо захисту певних властивостей (конфіденційності, цілісності, доступності) інформації, оброблюваної в ІТС, задоволення яких має забезпечуватися КСЗІ;

- функціональний склад ОЕ та його основні характеристики, які мають бути підтверджені в ході проведення експертизи (реалізований функціональний профіль захищеності; рівень гарантій коректності реалізації ФПБ; певний перелік організаційних, фізичних та інших заходів захисту тощо);

- місце розташування, категорію та інші загальні характеристики ІТС, у складі якої створено та функціонує ОЕ.

7.1.1.1.3 При ознайомленні з ОЕ в реальних умовах функціонування ІТС зусилля Експерта мають бути спрямовані, у першу чергу, на збирання доказів, які підтверджують сам факт існування ОЕ у тому складі та з тими характеристиками, які були виявлені під час попереднього аналізу вхідних даних щодо ОЕ.

7.1.1.1.4 При проведенні попереднього аналізу наданої документації на ОЕ щодо відповідності її вимогам чинних нормативних документів Експерту слід з урахуванням результатів попереднього аналізу вхідних даних щодо ОЕ, а також рекомендацій, викладених у Додатку А, перевірити склад наданої Замовником проектної, експлуатаційної та нормативно-розпорядчої документації й визначити, чи відповідає він з урахуванням зазначених рекомендацій вимогам чинних нормативних документів, задоволення яких має забезпечуватися КСЗІ.

7.1.1.1.5 Результатом виконання робіт з попереднього ознайомлення з ОЕ повинен бути звіт, в якому Експерти, що здійснювали аналіз відповідних матеріалів та ознайомлення з ОЕ, повинні викласти свою думку щодо ступеня відповідності ОЕ наданим відомостям, повноти складу наданої проектної, експлуатаційної та нормативно-розпорядчої документації, обґрунтувати рішення щодо можливості та доцільності проведення подальших робіт з експертизи або щодо їх припинення, а у випадку позитивного рішення – пропозиції щодо плану та послідовності проведення подальших робіт. У звіті можуть бути наведені рекомендації щодо необхідності доопрацювання наданих документів, розроблення додаткових документів або надання додаткових матеріалів, які повинні бути використані на подальших етапах експертизи.

7.1.1.2 Метою етапу поглибленого обстеження ОЕ є збирання та ретельний аналіз всіх відомостей про ОЕ, які визначають або можуть визначати перелік та обсяг експертних робіт з розроблення програми та методики проведення експертизи КСЗІ, а також проведення експертних випробувань і досліджень ОЕ за розробленими програмою та методикою та одержання необхідних вхідних даних для проведення подальших етапів експертних робіт.

7.1.1.2.1 На етапі поглибленого обстеження ОЕ Експертами повинні бути виконані такі дії:

- поглиблений аналіз ОЕ та наданої проектної, експлуатаційної та нормативно-розпорядчої документації щодо її повноти та відповідності її змісту реальній ІТС та умовам її функціонування;

- перевірка складу КЗЗ, створеного у складі ОЕ, та визначення необхідності проведення експертизи складових частин КЗЗ, які не мають Експертних висновків щодо відповідності вимогам чинних нормативних документів системи ТЗІ.

7.1.1.2.2 При проведенні поглибленого аналізу ОЕ та наданої проектної, експлуатаційної та нормативно-розпорядчої документації Експерту слід крім використання матеріалів, що аналізуються, враховувати результати, одержані на етапі попереднього

ознайомлення з ОЕ, а також, за необхідності, пояснення Замовника експертизи та/або Розробника ОЕ. Крім цього, при виконанні такого аналізу Експерту слід використовувати викладені у Додатку А рекомендації щодо змісту відповідної документації, а також вимоги чинних нормативних документів щодо забезпечення захисту інформації. За результатами проведеного аналізу зазначених матеріалів Експерт повинен:

- розширити та деталізувати уявлення про ОЕ та його особливості (архітектура та функціональний склад ІТС; клас та підклас ІТС як автоматизованої системи (АС) згідно з вимогами НД ТЗІ 2.5-005-99; інформаційні ресурси, оброблювані в ІТС, які підлягають захисту, і технологія їх оброблення; характеристика інформації, що міститься у певних інформаційних ресурсах та потребує захисту, відповідно до встановленого законодавством правового режиму та режиму доступу; вимоги чинних нормативних документів щодо захисту певних властивостей інформації, оброблюваної в ІТС; функціональний склад КСЗІ та її основні характеристики, які мають бути підтверджені в ході проведення експертизи; структурний склад підсистем КСЗІ, у тому числі структурний склад КЗЗ КСЗІ тощо);
- надати (за наявності) Замовнику зауваження щодо змісту окремих документів та рекомендації щодо усунення наданих зауважень.

Примітка. Рівень деталізації зауважень щодо змісту окремих документів повинен бути не нижчим, ніж рівень деталізації викладення рекомендацій щодо змісту відповідних документів, наведених у Додатку А, або рівень деталізації викладення вимог та рекомендацій щодо змісту відповідних документів у чинній нормативно-правовій базі в сфері ТЗІ;

- провести повторний аналіз доопрацьованих документів та прийняти рішення щодо повноти наданої документації та відповідності її змісту реальній ІТС та умовам її функціонування, а також щодо можливості та доцільності проведення подальших робіт з експертизи. Якщо надані Замовнику зауваження щодо змісту окремих документів не усунуто, Експерт може прийняти рішення щодо припинення подальших робіт або щодо їх призупинення до усунення всіх наданих зауважень.

7.1.1.2.3 При виконанні перевірки складу КЗЗ, створеного у складі ОЕ, Експертом на підставі відомостей щодо структурного складу КЗЗ КСЗІ, що містяться у зазначеній у п. А.2.2 проектній документації КСЗІ, а також з урахуванням складу та вмісту матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ, зазначених у п. А.2.3, повинні бути визначені (за наявності) складові частини КЗЗ, які не мають Експертних висновків щодо відповідності вимогам чинних нормативних документів системи ТЗІ, та прийнято рішення щодо оцінювання ФПБ та рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ в ході робіт з експертизи КСЗІ. При цьому обов'язково мають бути оцінені лише ті ФПБ, реалізація яких покладається на відповідні компоненти (складові частини) КЗЗ КСЗІ згідно з положеннями зазначеної у п. А.2.2 проектної документації КСЗІ, а також ФПБ, наявність яких згідно з вимогами НД ТЗІ 2.5-004-99 є необхідною умовою для реалізації ФПБ, що оцінюються.

7.1.1.2.4 Результатом виконання робіт щодо поглибленого обстеження ОЕ має бути уточнений перелік відомостей про ОЕ та інших вхідних даних, необхідних для розроблення програми та методики проведення експертизи.

7.1.1.2.5 Допускається об'єднання етапів попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ. У цьому випадку допускається не виконувати роботи, передбачені в п. 7.1.1.1.5.

7.1.1.3 Метою етапу розроблення програми експертизи є розроблення та погодження в установленому порядку програми проведення експертизи КСЗІ.

7.1.1.3.1 Як вхідні дані на цьому етапі Експертом повинні використовуватися всі матеріали, які були зібрані, проаналізовані та, за необхідності, доопрацьовані на попередніх етапах робіт.

7.1.1.3.2 У розробленій програмі експертизи КСЗІ повинен бути наведений опис того,

відповідність ОЕ яким саме вимогам та в якій послідовності має бути перевірена з метою підтвердження або спростування його відповідності вимогам Технічного завдання на створення КСЗІ в ІТС та вимогам чинних нормативних документів системи ТЗІ.

7.1.1.3.3 При розробленні змістовної частини програми проведення експертизи КСЗІ Експертам слід керуватися вимогами щодо змісту програми проведення експертизи КСЗІ в ІТС, викладеними в Додатку Б.

7.1.1.3.4 При документуванні програми проведення експертизи КСЗІ Експертам слід керуватися вимогами Положення про державну експертизу в сфері технічного захисту інформації, ГОСТ 19.301-79, ДСТУ 2853-94, інших чинних стандартів та нормативних документів у галузі інформаційних технологій та захисту інформації, що стосуються підготовки та проведення випробувань.

7.1.1.3.5 Результатом етапу повинна бути розроблена та згідно з вимогами Положення про державну експертизу в сфері технічного захисту інформації погоджена із Замовником експертизи та уповноваженим державним органом програма проведення експертизи КСЗІ.

7.1.1.3.6 У випадку проведення експертизи однотипних ОЕ, які являють собою реалізацію типового проектного рішення, допускається за погодженням з уповноваженим державним органом використовувати єдину типову програму проведення експертизи КСЗІ, розроблену та погоджену у порядку, наведеному в пп. 7.1.1.3.1-7.1.1.3.5.

7.1.1.4 Метою етапу розроблення методики експертизи є розроблення та погодження в установленому порядку методики проведення експертизи КСЗІ.

7.1.1.4.1 Як вхідні дані на цьому етапі Експертом мають використовуватися всі матеріали, які були зібрані, проаналізовані та, за необхідності, доопрацьовані на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ, а також розроблена на попередньому етапі програма проведення експертизи КСЗІ.

7.1.1.4.2 У розробленій методиці проведення експертизи КСЗІ повинен бути наведений опис того, з використанням яких документів (матеріалів), засобів та в якій послідовності мають бути виконані експертні роботи з метою підтвердження або спростування відповідності ОЕ вимогам Технічного завдання на створення КСЗІ в ІТС та вимогам чинних нормативних документів системи ТЗІ.

7.1.1.4.3 При розробленні змістовної частини методики експертизи КСЗІ Експертам слід керуватися вимогами щодо змісту методики проведення експертизи КСЗІ в ІТС, викладеними в Додатку В.

7.1.1.4.4 При документуванні методики проведення експертизи КСЗІ Експертам слід керуватися вимогами Положення про державну експертизу в сфері технічного захисту інформації, ГОСТ 19.301-79, ДСТУ 2853-94, інших чинних стандартів та нормативних документів у галузі інформаційних технологій та захисту інформації, що стосуються підготовки та проведення випробувань.

7.1.1.4.5 Результатом етапу повинна бути розроблена та згідно з вимогами Положення про державну експертизу в сфері технічного захисту інформації погоджена з уповноваженим державним органом методика проведення експертизи КСЗІ.

7.1.1.4.6 У випадку проведення експертизи однотипних ОЕ, які являють собою реалізацію типового проектного рішення, допускається за погодженням з уповноваженим державним органом використовувати єдину типову методику проведення експертизи КСЗІ, розроблену та погоджену у порядку, наведеному в пп. 7.1.1.4.1-7.1.1.4.5.

7.1.1.5 Метою етапу проведення експертних випробувань та досліджень ОЕ є виконання повного обсягу експертних робіт, передбаченого затвердженою програмою проведення експертизи, шляхом здійснення визначених у затвердженій методиці проведення експертизи дій та перевірок з фіксацією (у відповідному журналі результатів проведення експертних робіт, форма якого може бути аналогічною формі журналу випробувань, встановленій ДСТУ 2851-94) висновків Експерта щодо результатів виконання певних

пунктів методики.

7.1.1.5.1 Проведення експертних випробувань та досліджень ОЕ за розробленими з урахуванням вимог, викладених у Додатках Б та В, програмою та методикою проведення експертизи передбачає (з урахуванням особливостей ОЕ) виконання таких експертних робіт:

- аналіз документації, розробленої на етапі виконання передпроектних робіт зі створення КСЗІ;
- аналіз Технічного завдання на створення КСЗІ в ІТС;
- оцінювання (за необхідності) ФПБ, що реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ;
- оцінювання (за необхідності) рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ;
- аналіз проектної документації КСЗІ та матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ;
- аналіз експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ;
- аналіз нормативно-розпорядчої документації КСЗІ;
- аналіз документації щодо проведених випробувань КСЗІ;
- аналіз організаційно-розпорядчої документації КСЗІ;
- перевірка фактичного використання внесених до складу КЗЗ КСЗІ засобів захисту інформації;
- перевірка порядку використання внесених до складу КЗЗ КСЗІ засобів захисту інформації;
- перевірка впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту;
- перевірка підготовленості співробітників служби захисту інформації (СЗІ), персоналу та користувачів ІТС;
- перевірка (за необхідності) результатів створення та атестації комплексу ТЗІ.

7.1.1.5.2 Роботи з оцінювання ФПБ, що реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ, а також з оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ повинні проводитися у порядку, наведеному в розділі 6.

7.1.1.5.3 Роботи з аналізу документації, що стосується створення КСЗІ (документації, розробленої на етапі виконання передпроектних робіт; Технічного завдання на створення КСЗІ в ІТС; проектної документації КСЗІ та матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ; експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ; нормативно-розпорядчої документації КСЗІ; документації щодо проведених випробувань КСЗІ; організаційно-розпорядчої документації КСЗІ) можуть виконуватися як в умовах випробувальної лабораторії, так і безпосередньо в умовах ІТС, у складі якої функціонує ОЕ.

7.1.1.5.4 Роботи з перевірки фактичного використання внесених до складу КЗЗ КСЗІ засобів захисту інформації, з перевірки порядку використання внесених до складу КЗЗ КСЗІ засобів захисту інформації, з перевірки впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту, з перевірки підготовленості співробітників СЗІ, персоналу та користувачів ІТС, з перевірки результатів створення та атестації комплексу ТЗІ повинні виконуватися безпосередньо в умовах ІТС, у складі якої функціонує ОЕ.

7.1.1.5.5 Виконання зазначених в окремих розділах Додатка В та у методиці проведення експертизи перевірок матеріалів (документів) або перевірок певних фактів передбачає просте порівняння змісту матеріалів (документів) з висунутими вимогами без залучення

спеціальних знань та досвіду Експерта або фіксацію (за наявності або відсутності відповідних ознак, визначених у методиці експертизи як мета перевірки) підтвердження або спростування відповідних фактів. Висновки, які формулюються за результатами виконаної перевірки, повинні містити лише результати виконаної перевірки без їх обґрунтування.

7.1.1.5.6 Виконання зазначених в окремих розділах Додатка В та у методиці проведення експертизи досліджень матеріалів (документів) з метою формулювання обґрунтованого висновку про відповідність висунутим вимогам передбачає виконання поглибленого аналізу вмісту матеріалів на предмет відповідності висунутим вимогам з використанням спеціальних знань та досвіду Експерта. Висновки, які формулюються за результатами виконаних досліджень, повинні містити як результати проведеного аналізу, так і їх обґрунтування, що містить аргументацію на користь цих висновків.

7.1.1.5.7 При виконанні окремих пунктів методики експертизи, які стосуються перевірки фактичного використання внесених до складу КЗЗ КСЗІ засобів захисту інформації та порядку їх використання, перевірки впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту, а також перевірки підготовленості співробітників СЗІ, персоналу та користувачів ІТС, Експерти можуть використовувати (у частині, що стосується виконання аналогічних робіт) рекомендації щодо відвідування підприємств, викладені у Додатку Г до НД ТЗІ 2.7-010-09.

7.1.1.5.8 Сформульовані Експертом висновки за результатами виконання перевірок згідно з певними пунктами методики проведення експертизи повинні фіксуватися в журналі результатів проведення експертних робіт. У цьому журналі повинні фіксуватися як висновки Експерта, так і (безпосередньо або шляхом посилання на проаналізовані матеріали та документи) аргументи, на підставі яких були зроблені відповідні висновки.

7.1.1.6 Документування та затвердження результатів експертизи передбачають виконання таких робіт:

- оформлення та затвердження протоколу виконання робіт з експертизи КСЗІ (далі – протокол експертизи КСЗІ);
- оформлення, затвердження та надання Замовнику експертизи Експертного висновку за результатами експертизи КСЗІ.

7.1.1.6.1 При оформленні протоколу експертизи КСЗІ слід керуватися вимогами Положення про державну експертизу в сфері технічного захисту інформації щодо форми протоколу, а також рекомендаціями, наведеними в Додатку Д, щодо його змістовної частини.

7.1.1.6.2 При оформленні Експертного висновку за результатами експертизи КСЗІ слід керуватися вимогами Положення про державну експертизу в сфері технічного захисту інформації щодо форми Експертного висновку, а також рекомендаціями, наведеними в Додатку Ж, щодо його змістовної частини.

7.1.1.6.3 Затверджені Організатором експертизи протокол та Експертний висновок у порядку, визначеному Положенням про державну експертизу в сфері технічного захисту інформації, повинні бути зареєстровані уповноваженим державним органом та надані Замовнику експертизи. На підставі позитивного Експертного висновку уповноважений державний орган надає Замовнику експертизи Атестат відповідності КСЗІ в ІТС вимогам нормативних документів з технічного захисту інформації.

7.2 Особливості проведення робіт з додаткової та контрольної експертизи комплексних систем захисту інформації

7.2.1 Проведення додаткової або контрольної експертизи КСЗІ може передбачати як виконання всіх експертних робіт, передбачених для випадку первинної експертизи, так і за погодженням з уповноваженим державним органом лише тих робіт, які обумовлені причинами проведення відповідної експертизи.

7.2.2 Перелік та обсяг експертних робіт з додаткової експертизи повинні визначатися на

підставі обставин, які зумовили її проведення.

7.2.2.1 Якщо додаткова експертиза проводиться в зв'язку із закінченням терміну дії документів, що засвідчують результати попередньої експертизи, перелік та обсяг відповідних експертних робіт повинні визначатися на підставі наявності або відсутності змін у середовищах функціонування ІТС або змін у реалізації ОЕ порівняно з тими, які досліджувалися та оцінювалися при проведенні первинної експертизи. Факт наявності цих змін повинен встановлюватися за результатами виконання етапів попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ.

7.2.2.2 Якщо за результатами виконання етапів попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ встановлено, що змін у середовищах функціонування ІТС та змін у реалізації ОЕ не відбулося, тобто середовища функціонування ІТС та всі структурні компоненти ОЕ відповідають тим, стосовно яких здійснювалися експертні роботи при проведенні первинної експертизи, в процесі додаткової експертизи достатньо перевірити та підтвердити цей факт шляхом проведення відповідних випробувань (перевірок) за затвердженими в установленому порядку програмою та методикою проведення експертизи. У цьому випадку змістовна частина відповідних розділів Експертного висновку за результатами додаткової експертизи повинна відтворювати змістовну частину відповідних розділів Експертного висновку за результатами первинної експертизи.

7.2.2.3 Якщо за результатами виконання етапів попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ встановлено, що у середовищах функціонування ІТС або реалізації ОЕ відбулися зміни, тобто середовища функціонування ІТС або певні структурні компоненти ОЕ не відповідають тим, стосовно яких здійснювалися експертні роботи при проведенні попередньої експертизи, додаткова експертиза повинна передбачати виконання експертних робіт у повному обсязі. При цьому проведення додаткової експертизи може передбачати (залежно від обсягу та суті внесених змін) як використання програми та методики проведення первинної експертизи, так і розроблення нових.

7.2.2.4 Якщо додаткова експертиза проводиться в зв'язку з відкриттям нових наукових та/або науково-технічних обставин стосовно ОЕ, які потенційно можуть впливати на здатність ОЕ запобігати певним загрозам та/або функціонувати у визначеному в проектної документації порядку, вона повинна передбачати виконання експертних робіт у повному обсязі. При виконанні відповідних робіт повинні враховуватися суть та вплив відповідних обставин на порядок функціонування ОЕ.

7.2.3 Перелік та обсяг експертних робіт з контрольної експертизи повинні визначатися з урахуванням тих висновків первинної або додаткової експертизи, стосовно яких виникли обґрунтовані претензії та які повинні бути повторно перевірені.

7.2.4 Порядок проведення певних експертних робіт при проведенні додаткової або контрольної експертизи повинен відповідати порядку проведення аналогічних робіт у випадку проведення первинної експертизи.

Додаток А
(рекомендований)

Рекомендації щодо складу та змісту проектної, експлуатаційної та нормативно-розпорядчої документації, яка надається Замовником при проведенні експертизи комплексної системи захисту інформації

У Додатку А викладено рекомендації щодо складу та змісту матеріалів (документів), які надаються Замовником Організатору експертизи для використання Експертами в процесі проведення експертизи КСЗІ. Рекомендації викладено з урахуванням положень чинної нормативно-правової бази в сфері ТЗІ, яка регламентує порядок проведення робіт зі створення КСЗІ в АС різного класу, в яких обробляється інформація, для якої законодавством встановлено різні правові режими та режими доступу. У п. А.1 наведено рекомендований склад матеріалів (документів), які з урахуванням класу ІТС як АС згідно з НД ТЗІ 2.5-005-99, а також характеристик оброблюваної в ІТС інформації повинні бути розроблені на різних етапах створення КСЗІ та надані Замовником Організатору експертизи для подальшого використання Експертами в процесі проведення експертизи. У пп. А.2, А.3 наведено рекомендації щодо змісту окремих документів, які визначені з урахуванням вимог чинної нормативно-правової бази в сфері ТЗІ.

А.1 Рекомендований склад матеріалів (документів), які надаються Замовником Організатору експертизи

Рекомендований склад матеріалів (документів), які повинні бути розроблені в процесі створення КСЗІ та надані Замовником Організатору експертизи для використання Експертами в процесі проведення експертизи, наведено в таблиці А.1.

Таблиця А.1

№ з/п	Тип документа	Характеристика оброблюваної інформації відповідно до встановленого законодавством правового режиму та режиму доступу					Клас/підклас ІТС як АС згідно з НД ТЗІ 2.5-005-99
		ІДТ	КІВД	КІ	ВІВД	ВІ	
1	Документація щодо створення КСЗІ						
1.1	Документація, розроблювана на етапі виконання передпроектних робіт						
1.1.1	Перелік інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.1.2	Акт категорування ІТС	+	+	+/-	-	-	1.Кхх, 2.Кхх, 3.Кхх
1.1.3	Положення про службу захисту інформації в ІТС	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.1.4	Результати обстеження середовищ функціонування ІТС	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.1.5	Опис політики безпеки інформації в ІТС	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.1.6	Опис моделі порушника безпеки інформації в ІТС	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.1.7	Опис моделі загроз для інформації, оброблюваної в ІТС	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.1.8	Звіт за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.1.9	План захисту інформації в ІТС	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх

Продовження таблиці А.1

№ з/п	Тип документа	Характеристика оброблюваної інформації відповідно до встановленого законодавством правового режиму та режиму доступу					Клас/підклас ІТС як АС згідно з НД ТЗІ 2.5-005-99
		ІДТ	КІВД	КІ	ВІВД	ВІ	
1.1.10	Технічне завдання на створення КСЗІ в ІТС	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.2	Проектна документація КСЗІ						
1.2.1	Документація ескізного проекту КСЗІ в ІТС	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.2.2	Документація технічного проекту КСЗІ в ІТС	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.2.3	Документація робочого проекту КСЗІ в ІТС	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.3	Матеріали, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ						
1.3.1	Експертні висновки щодо відповідності вимогам чинних нормативних документів системи ТЗІ, використовуваних у складі КЗЗ КСЗІ засобів захисту інформації	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.3.2	Експертні висновки, сертифікати, інші документи, що підтверджують відповідність вимогам чинних нормативних документів системи криптографічного захисту інформації (КЗІ), використовуваних у складі КЗЗ КСЗІ засобів КЗІ	+	+	+	+	+	1.Кхх, 2.Кхх, 3.Кхх, 1.хЦх, 2.хЦх, 3.хЦх
1.4	Матеріали (документи), необхідні для оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ, створення та експертиза яких здійснюється в ході створення та експертизи КСЗІ	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.5	Експлуатаційна документація компонентів (складових частин) КЗЗ КСЗІ	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.6	Нормативно-розпорядча документація КСЗІ						
1.6.1	Інструкції щодо забезпечення правил оброблення інформації з обмеженим доступом (ІзОД) в ІТС	+	+	-	-	-	1.Кхх, 2.Кхх, 3.Кхх
1.6.2	Посадові (функціональні) інструкції співробітників СЗІ, персоналу та користувачів ІТС	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.6.3	Технологічні (операційні) інструкції (настанови) щодо виконання завдань з адміністрування та обслуговування КСЗІ	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.6.4	Інструкції про порядок використання засобів КЗІ	+	+	+	+	+	1.Кхх, 2.Кхх, 3.Кхх, 1.хЦх, 2.хЦх, 3.хЦх
1.7	Документація щодо проведених випробувань КСЗІ	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.8	Організаційно-розпорядча документація КСЗІ	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.9	Супровідна документація КСЗІ в ІТС	+	+	+	+	+	1.ххх, 2.ххх, 3.ххх
1.10	Журнали обліку та реєстрації сховищ і матеріальних носіїв ІзОД	+	+	-	-	-	1.Кхх, 2.Кхх, 3.Кхх

Продовження таблиці А.1

№ з/п	Тип документа	Характеристика оброблюваної інформації відповідно до встановленого законодавством правового режиму та режиму доступу					Клас/підклас ІТС як АС згідно з НД ТЗІ 2.5-005-99
		ІДТ	КІВД	КІ	ВІВД	ВІ	
2	Документація щодо створення комплексу ТЗІ						
2.1	Документація, що розробляється на етапі виконання передпроектних робіт	+	+/-	+/-	-	-	1.Кхх, 2.Кхх, 3.Кхх
2.2	Документація, що розробляється на етапі розроблення та впровадження заходів із захисту інформації	+	+/-	+/-	-	-	1.Кхх, 2.Кхх, 3.Кхх
2.3	Документація, що розробляється на етапі випробувань та атестації комплексу ТЗІ	+	+/-	+/-	-	-	1.Кхх, 2.Кхх, 3.Кхх

Примітка. У таблиці використовуються такі позначення: "+" – вимога щодо наявності документа висувається на підставі положень чинної нормативно-правової бази в сфері ТЗІ; "+/-" – вимога щодо наявності документа висувається за рішенням власника (розпорядника) інформації, що обробляється в ІТС; "-" – вимога щодо наявності документа не висувається.

А.2 Рекомендації до змісту документації щодо створення КСЗІ

А.2.1 Документація, що розробляється на етапі виконання передпроектних робіт

А.2.1.1 Перелік інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту

А.2.1.1.1 У переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, має бути наведено перелік інформаційних ресурсів (видів інформації), що підлягають обробленню в ІТС, класифікований за такими ознаками:

- семантичний вміст відповідного інформаційного ресурсу, який визначається цільовим призначенням відповідної інформації;
- характеристики інформації відповідно до встановленого законодавством правового режиму та режиму доступу (ІДТ, КІВД, КІ, ВІВД, ВІ);
- вищий ступінь обмеження доступу (для ІДТ) до інформації (ступінь секретності) відповідно до вимог Зводу відомостей, що становлять державну таємницю;
- критичні властивості інформації з погляду забезпечення її захищеності, визначені з урахуванням вимог Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і вимог власника (розпорядника) інформації;
- вимоги (за наявності) щодо обмеження доступу до інформації користувачів ІТС різних категорій, визначені з урахуванням, наприклад, вимог Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах (для ІДТ) або Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави (для КІВД).

Окрім зазначених вище, можуть бути використані додаткові класифікаційні ознаки, корисні з погляду подальшого формулювання політики безпеки інформації, оброблюваної в ІТС, наприклад, вид подання відповідних інформаційних ресурсів тощо.

А.2.1.1.2 Перелік інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, може бути оформлений у вигляді окремого документа, затвердженого керівником організації (установи), яка є власником (розпорядником) відповідної інформації або його заступником, відповідальним за забезпечення ТЗІ, або внесений у вигляді розділу до інших документів (Опису політики безпеки інформації в ІТС, Плану захисту інформації в ІТС, Технічного завдання на створення КСЗІ в ІТС тощо).

А.2.1.2 Акт категорування ІТС

А.2.1.2.1 В акті категорування ІТС повинні бути викладені результати відповідного категорування, проведеного у порядку, визначеному ТПКО-95. Структура та зміст акта категорування мають відповідати вимогам ТПКО-95. Зокрема, в акті категорування повинні бути обов'язково наведені такі відомості:

- підстава для категорування (первинне, планове, у зв`язку зі змінами);
- вищий ступінь обмеження доступу (ступінь секретності) інформації, що підлягає автоматизованому обробленню в ІТС;
- категорія, призначена ІТС.

А.2.1.2.2 Наведені в акті категорування відомості щодо ступеня обмеження доступу (ступеня секретності) інформації, що підлягає автоматизованому обробленню в ІТС, повинні відповідати аналогічним відомостям, наведеним у Переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, зазначеному в п. А.2.1.1.

А.2.1.2.3 Згідно з вимогами ТПКО-95, акт категорування ІТС має бути складений комісією, призначеною керівником організації (установи), яка є власником (розпорядником) ІТС, та затверджений керівником організації (установи), яка є власником (розпорядником) ІТС.

А.2.1.3 Положення про службу захисту інформації в ІТС

А.2.1.3.1 Положення про СЗІ в ІТС має визначати завдання, функції, повноваження та відповідальність, штатний розклад та структуру СЗІ, порядок організації її робіт та взаємодії з іншими підрозділами організації (установи), яка є власником (розпорядником) ІТС, а також порядок її фінансування.

Відповідно до вимог Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, якщо обсяг робіт, пов'язаних із захистом інформації в ІТС, є незначним, забезпечення захисту інформації в такій ІТС може бути покладено на одну особу, а СЗІ в такій ІТС може не створюватися. В цьому випадку завдання, функції, повноваження та відповідальність особи, на яку покладено забезпечення захисту інформації в ІТС (в обсязі, що відповідає наведеним вище вимогам), повинні бути визначені у відповідному наказі керівника організації (установи), яка є власником (розпорядником) ІТС, або його заступника, відповідального за забезпечення ТЗІ.

А.2.1.3.2 Структура та зміст Положення про СЗІ в ІТС повинні відповідати рекомендаціям НД ТЗІ 1.4-001-2000 та враховувати особливості функціонування конкретної ІТС (зокрема в частині, що стосується реалізованої інформаційної технології, переліку інформаційних ресурсів, що потребують захисту, встановленого розподілу обов'язків персоналу та користувачів ІТС тощо).

А.2.1.3.3 Завдання та функції співробітників (посадових осіб) СЗІ, визначені у Положенні про СЗІ в ІТС, мають бути сформульовані з урахуванням вимог Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-007-2007, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 та інших чинних нормативних документів, які визначають вимоги щодо порядку створення, введення в експлуатацію та експлуатації КСЗІ в ІТС певного типу, та формулюють завдання, які повинен вирішувати персонал ІТС на різних стадіях створення КСЗІ.

А.2.1.3.4 Положення про СЗІ в ІТС має бути оформлено у вигляді окремого документа відповідно до рекомендації НД ТЗІ 1.4-001-2000. Згідно з вимогами Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та НД ТЗІ 1.4-001-2000, Положення про СЗІ в ІТС має бути затверджене керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

А.2.1.4 Результати обстеження середовищ функціонування ІТС

А.2.1.4.1 Результати обстеження середовищ функціонування ІТС повинні містити результати проведеного обстеження обчислювальної системи ІТС, інформаційного середовища, фізичного середовища, середовища користувачів. Загальні вимоги щодо порядку проведення такого обстеження та змісту його результатів визначено в ДСТУ 3396.1-96 та НД ТЗІ 3.7-003-05.

А.2.1.4.2 У частині, що стосується результатів обстеження обчислювальної системи ІТС, повинні бути наведені:

- загальна структурна схема та склад обчислювальної системи ІТС;
- види і характеристики каналів мережі передачі даних;
- особливості взаємодії окремих компонентів ІТС, їх взаємний вплив один на одного;
- можливі обмеження щодо використання певних засобів тощо.

Повинні бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів щодо забезпечення захисту інформації, відповідні їхні властивості та характеристики тощо.

Наведені результати обстеження обчислювальної системи ІТС повинні надавати вичерпні відомості щодо можливостей обчислювальної системи ІТС як з погляду забезпечення функціонування загальносистемного та прикладного програмного забезпечення ІТС, так і з погляду забезпечення функціонування засобів захисту, які можуть бути реалізовані та впроваджені в процесі створення КСЗІ.

Якщо склад та особливості обчислювальної системи ІТС повністю відповідають зазначеним у НД ТЗІ 2.5-007-2007, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 або інших чинних нормативних документах, які визначають вимоги щодо порядку створення, введення в експлуатацію та експлуатації КСЗІ в ІТС певного типу, замість наведення відповідних відомостей у розгорнутому вигляді допускається навести посилання на відповідний нормативний документ та зазначити конкретні характеристики компонентів ІТС.

А.2.1.4.3 У частині, що стосується результатів обстеження інформаційного середовища, мають бути наведені:

- уточнений перелік та класифікація (на підставі та з урахуванням відомостей, наведених у Переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, зазначеному в п. А.2.1.1) інформаційних ресурсів ІТС (даних та програмного забезпечення), які потребують захисту. Як додаткові до зазначених у п. А.2.1.1 класифікаційних ознак можуть використовуватися, наприклад, вид подання відповідної інформації в різних компонентах обчислювальної системи (в термінах об'єктів КС згідно з НД ТЗІ 1.1-002-99), стан відповідних інформаційних об'єктів (зберігання, оброблення, передавання тощо), характеристики (атрибути) відповідних об'єктів у різному стані тощо;
- опис технології оброблення інформації, що потребує захисту, в усіх загальносистемних та прикладних програмних засобах ІТС з наведенням компонентів обчислювальної системи ІТС, на базі яких функціонують відповідні програмні засоби, інформаційних потоків, що створюються в процесі оброблення, середовищ, через які вони передаються, джерел утворення інформаційних потоків та місць їх призначення. Як частина опису має бути наведена структурна схема інформаційних потоків, у якій для кожного елемента схеми повинен бути визначений склад, вид подання, критичні з погляду захищеності властивості інформації та інші необхідні характеристики відповідних інформаційних об'єктів;
- припущення (за наявності) щодо можливого впливу (з погляду збереження критичних властивостей інформації) на інформаційні об'єкти, що містять інформацію, яка потребує захисту, елементів середовища користувачів та фізичного середовища.

Якщо характеристики інформаційного середовища повністю відповідають зазначеним у

НД ТЗІ 2.5-007-2007, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 або інших чинних нормативних документах, які визначають вимоги щодо порядку створення, введення в експлуатацію та експлуатації КСЗІ в ІТС певного типу, замість наведення відповідних відомостей у розгорнутому вигляді допускається навести посилання на відповідний нормативний документ.

А.2.1.4.4 У частині, що стосується результатів обстеження фізичного середовища, повинні бути наведені такі характеристики:

- територіальне розміщення компонентів ІТС;
- наявність охорони території та перепускний режим;
- наявність категорованих приміщень, в яких повинні розміщуватися компоненти ІТС (з урахуванням результатів відповідного категорування, зазначених у п. А.2.1.2);
- режим доступу до компонентів фізичного середовища ІТС;
- вплив чинників навколишнього середовища, захищеність від засобів технічної розвідки (наводиться у випадку, якщо передбачається створення комплексу ТЗІ);
- наявність елементів комунікацій, систем життєзабезпечення і зв'язку, що мають вихід за межі контрольованої зони (наводиться у випадку, якщо передбачається створення комплексу ТЗІ);
- наявність та технічні характеристики систем заземлення (наводиться у випадку, якщо передбачається створення комплексу ТЗІ);
- умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;
- наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

А.2.1.4.5 У частині, що стосується результатів обстеження середовища користувачів, повинні бути наведені такі характеристики:

- функціональний та кількісний склад персоналу та користувачів ІТС, їх класифікація за функціональними обов'язками та рівнем кваліфікації;
- повноваження користувачів ІТС різних категорій щодо доступу до інформаційних ресурсів, які обробляються в ІТС, доступу до ІТС та її окремих компонентів, визначені з урахуванням відповідних вимог, наведених у Переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, зазначеному в п. А.2.1.1;
- рівня можливостей різних категорій користувачів, що надаються (можуть бути наданими) їм засобами ІТС;
- повноваження персоналу щодо управління засобами захисту КСЗІ, визначені з урахуванням відповідних вимог щодо завдань та функцій співробітників (посадових осіб) СЗІ, наведених у Положенні про СЗІ в ІТС, зазначеному в п. А.2.1.3.

А.2.1.4.6 Згідно з вимогами Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, НД ТЗІ 3.7-003-05, НД ТЗІ 1.4-001-2000 та НД ТЗІ 3.7-001-99, результати обстеження середовищ функціонування ІТС повинні бути оформлені у вигляді відповідного акта, затвердженого керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС, та внесені, за необхідності, до відповідних розділів Плану захисту інформації в ІТС та Технічного завдання на створення КСЗІ в ІТС.

А.2.1.5 Опис політики безпеки інформації в ІТС

А.2.1.5.1 Опис політики безпеки інформації в ІТС повинен містити набір вимог, правил, обмежень, рекомендацій тощо, які регламентують порядок оброблення в ІТС інформації, зазначеної у Переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, зазначеному в п. А.2.1.1, та спрямовані на захист її критичних

властивостей від загроз, притаманних умовам функціонування конкретної ІТС.

А.2.1.5.2 Відповідно до рекомендацій НД ТЗІ 1.1-002-99 та НД ТЗІ 1.4-001-2000 в Описі політики безпеки інформації в ІТС повинні бути (з урахуванням результатів обстеження середовищ функціонування ІТС, зазначених у п. А.2.1.4) визначені інформаційні ресурси ІТС, що потребують захисту. Мають бути сформульовані основні загрози для інформації з різними характеристиками відповідно до встановленого законодавством правового режиму та режиму доступу, компонентів обчислювальної системи, персоналу та вимоги щодо захисту від цих загроз. Як складові частини загальної політики безпеки інформації в ІТС повинні бути наведені політики забезпечення конфіденційності, цілісності та доступності оброблюваної інформації, а також політика забезпечення спостережності ІТС.

А.2.1.5.3 З урахуванням визначених повноважень користувачів ІТС різних категорій щодо доступу до інформаційних ресурсів, які обробляються в ІТС, як частина політики безпеки мають бути сформульовані правила розмежування доступу (ПРД) користувачів та процесів до інформаційних ресурсів ІТС, що потребують захисту. Як атрибути користувачів, процесів та інформаційних об'єктів у сформульованих ПРД мають використовуватися атрибути, що відповідають вимогам Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, НД ТЗІ 2.5-007-2007, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 та інших чинних нормативних документів, які визначають вимоги щодо порядку створення, введення в експлуатацію та експлуатації КСЗІ в ІТС певного типу (у частині, що стосується розмежування доступу до захищених інформаційних ресурсів), а також забезпечують підтримку повноважень користувачів ІТС різних категорій щодо доступу до інформаційних ресурсів та управління засобами захисту КСЗІ, визначених за результатами обстеження середовища користувачів.

А.2.1.5.4 З урахуванням відповідних вимог щодо завдань та функцій співробітників (посадових осіб) СЗІ, наведених у Положенні про СЗІ в ІТС, зазначеному в п. А.2.1.3, в Описі політики безпеки інформації в ІТС має бути визначена відповідальність персоналу за виконання положень політики безпеки.

А.2.1.5.5 Згідно з вимогами Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, НД ТЗІ 3.7-003-05, НД ТЗІ 1.4-001-2000 та НД ТЗІ 3.7-001-99, Опис політики безпеки інформації в ІТС має бути затверджений керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС, та внесений, за необхідності, до відповідних розділів Плану захисту інформації в ІТС та Технічного завдання на створення КСЗІ в ІТС.

А.2.1.6 Опис моделі порушника безпеки інформації в ІТС

А.2.1.6.1 Опис моделі порушника безпеки інформації в ІТС має містити абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії тощо. В описі моделі порушника (з урахуванням результатів обстеження середовищ функціонування ІТС, зазначених у п. А.2.1.4) мають бути визначені:

- можливі цілі порушника та їх градація за ступенями небезпечності для ІТС та інформації, що потребує захисту;
- категорії персоналу, користувачів ІТС та сторонніх осіб, із числа яких може бути порушник;
- припущення щодо кваліфікації порушника;
- припущення щодо характеру його дій.

А.2.1.6.2 Відповідно до рекомендацій НД ТЗІ 1.1-002-99 доцільно класифікувати порушників за рівнем можливостей, які надаються їм засобами ІТС.

А.2.1.6.3 Опис моделі порушника безпеки інформації в ІТС (у частині, що стосується припущень щодо кваліфікації порушника та характеру його дій) має бути викладений

настільки детально, щоб дозволяти однозначне визначення можливості або неможливості реалізації порушником певних загроз інформації (певних атак) з використанням уразливостей певних компонентів обчислювальної системи ІТС або використовуваних програмних засобів.

А.2.1.6.4 Згідно з вимогами Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, НД ТЗІ 3.7-003-05, НД ТЗІ 1.4-001-2000 та НД ТЗІ 3.7-001-99, Опис моделі порушника безпеки інформації в ІТС повинен бути затверджений керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС, та внесений, за необхідності, до відповідних розділів Плану захисту інформації в ІТС.

А.2.1.7 Опис моделі загроз для інформації, оброблюваної в ІТС

А.2.1.7.1 Опис моделі загроз для інформації, що обробляється в ІТС, має містити абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз для інформації, яка потребує захисту. В Описі моделі загроз для інформації (з урахуванням результатів обстеження середовищ функціонування ІТС, зазначених у п. А.2.1.4, а також прийнятої моделі потенційного порушника політики безпеки інформації в ІТС, зазначеної в п. А.2.1.6) мають бути визначені:

- перелік можливих типів загроз, класифікований за результатом впливу на інформацію, тобто на порушення яких її властивостей вони спрямовані (конфіденційності, цілісності або доступності інформації);

- перелік можливих способів реалізації загроз певного типу (способів атак) відносно різних інформаційних об’єктів ІТС у різному стані класифікований, наприклад, за такими ознаками, як компонент обчислювальної системи ІТС або програмний засіб, уразливості яких експлуатуються порушником, причини виникнення відповідної уразливості тощо.

А.2.1.7.2 Опис моделі загроз для інформації, що обробляється в ІТС (у частині, що стосується переліку можливих способів реалізації загроз та їх класифікації), має бути викладений настільки детально, щоб дозволяти (на етапі аналізу ризиків, пов’язаних з реалізацією загроз для інформації в ІТС) однозначне визначення як збитків, що завдаються у випадку успішної реалізації загрози, так і ймовірності реалізації загрози (здійснення атаки) в певний спосіб.

А.2.1.7.3 Згідно з вимогами Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, НД ТЗІ 3.7-003-05, НД ТЗІ 1.4-001-2000 та НД ТЗІ 3.7-001-99, Опис моделі загроз для інформації в ІТС має бути затверджений керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС, та внесений, за необхідності, до відповідних розділів Плану захисту інформації в ІТС та Технічного завдання на створення КСЗІ в ІТС.

А.2.1.8 Звіт за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ

А.2.1.8.1 Звіт за результатами проведення аналізу ризиків та формування завдання на створення КСЗІ повинен містити:

- формалізований або неформалізований опис результатів аналізу ризиків, пов’язаних з реалізацією загроз для інформації в ІТС;

- формулювання, з урахуванням результатів виконаного аналізу ризиків, завдань на створення КСЗІ в ІТС.

А.2.1.8.2 В описі результатів аналізу ризиків, проведеного з урахуванням рекомендацій НД ТЗІ 1.1-002-99 та ДСТУ ISO/IEC TR 13335-2:2003, для кожного зі способів реалізації загроз інформації, наведених в Описі моделі загроз для інформації, оброблюваної в ІТС, зазначеному в п. А.2.1.7, мають бути надані результати оцінювання ризику, пов’язаного з реалізацією певної загрози в певний спосіб, як функції ймовірності реалізації відповідної

загрози у відповідний спосіб, виду та величини збитків, що завдаються у випадку успішної реалізації загрози. Повинні бути визначені неприйнятні ризики і загрози для інформації та способи їх реалізації, з якими ці ризики пов'язані.

А.2.1.8.3 Завдання на створення КСЗІ повинні бути сформульовані з урахуванням вимог НД ТЗІ 3.7-003-05 та необхідності забезпечення (в результаті створення КСЗІ) запобігання тим загрозам для інформації та способів їх реалізації, з якими пов'язані неприйнятні ризики. Зокрема, у завданнях на створення КСЗІ мають бути визначені завдання захисту інформації в ІТС та можливі варіанти їх вирішення, загальна структура та склад КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо застосування певних заходів і засобів захисту, інші обмеження щодо середовищ функціонування ІТС, обмеження щодо використання ресурсів ІТС для реалізації завдань захисту, припустимі витрати на створення КСЗІ, умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до співвідношення та меж застосування в ІТС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ.

А.2.1.8.4 При формулюванні завдань на створення КСЗІ мають бути враховані вимоги Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-007-2007, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 та інших чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу.

А.2.1.8.5 Згідно з вимогами Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та НД ТЗІ 3.7-003-05, Звіт за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ має бути затверджений керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

А.2.1.9 План захисту інформації в ІТС

А.2.1.9.1 План захисту інформації в ІТС має містити: класифікацію інформації, що обробляється в ІТС; опис технології оброблення інформації в ІТС; опис моделі загроз для інформації в ІТС; опис політики безпеки інформації в ІТС; визначення завдань захисту інформації в ІТС; визначення переліку документів, згідно з якими має здійснюватися захист інформації в ІТС; перелік і строки виконання робіт СЗІ в ІТС.

А.2.1.9.2 Структура та зміст Плану захисту інформації в ІТС повинні відповідати рекомендаціям НД ТЗІ 1.4-001-2000, враховувати особливості функціонування конкретної ІТС, а також завдання захисту, що мають вирішуватися створюваною КСЗІ, викладені у: Переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, зазначеному в п. А.2.1.1; Положенні про СЗІ в ІТС, зазначеному в п. А.2.1.3; результатах обстеження середовищ функціонування ІТС, зазначених у п. А.2.1.4; Описі політики безпеки інформації в ІТС, зазначеному в п. А.2.1.5; Описі моделі порушника безпеки інформації в ІТС, зазначеному в п. А.2.1.6; Описі моделі загроз для інформації, оброблюваної в ІТС, зазначеному в п. А.2.1.7; Звіті за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ, зазначеному в п. А.2.1.8.

А.2.1.9.3 При формулюванні Плану захисту інформації в ІТС мають бути враховані вимоги Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-007-2007, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 та інших чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу.

А.2.1.9.4 План захисту інформації в ІТС повинен бути оформлений у вигляді окремого документа відповідно до рекомендації НД ТЗІ 1.4-001-2000. Згідно з вимогами Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-

телекомунікаційних системах та НД ТЗІ 1.4-001-2000, План захисту інформації в ІТС має бути затверджений керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

А.2.1.10 Технічне завдання на створення КСЗІ в ІТС

А.2.1.10.1 Технічне завдання на створення КСЗІ в ІТС є засадничим організаційно-технічним документом для виконання робіт щодо забезпечення захисту інформації в ІТС. У Технічному завданні на створення КСЗІ в ІТС, відповідно до положень НД ТЗІ 3.7-003-05 та НД ТЗІ 3.7-001-99, повинні бути викладені вимоги щодо функціонального складу, порядку розроблення та впровадження технічних, організаційних, фізичних та інших заходів захисту, які у сукупності складають КСЗІ.

А.2.1.10.2 Структура та зміст Технічного завдання на створення КСЗІ в ІТС повинні відповідати вимогам НД ТЗІ 3.7-003-05, НД ТЗІ 3.7-001-99 та рекомендаціям НД ТЗІ 2.7-010-09 (у частині, що стосується визначення функціональних специфікації КЗЗ КСЗІ для відповідного рівня гарантій коректності реалізації ФПБ), враховувати особливості функціонування конкретної ІТС, а також завдання захисту, що мають вирішуватися створюваною КСЗІ, викладені у: Переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, зазначеному в п. А.2.1.1; Положенні про СЗІ в ІТС, зазначеному в п. А.2.1.3; результатах обстеження середовищ функціонування ІТС, зазначених у п. А.2.1.4; Описі політики безпеки інформації в ІТС, зазначеному в п. А.2.1.5; Описі моделі порушника безпеки інформації в ІТС, зазначеному в п. А.2.1.6; Описі моделі загроз для інформації, що обробляється в ІТС, зазначеному в п. А.2.1.7; Звіті за результатами проведення аналізу ризиків та формування завдання на створення КСЗІ, зазначеному в п. А.2.1.8; Плані захисту інформації в ІТС, зазначеному в п. А.2.1.9.

А.2.1.10.3 При розробленні Технічного завдання на створення КСЗІ в ІТС мають бути враховані вимоги Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-007-2007, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 та інших чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу.

А.2.1.10.4 Відповідно до НД ТЗІ 3.7-003-05 та НД ТЗІ 3.7-001-99, Технічне завдання на створення КСЗІ в ІТС може бути оформлено:

- у вигляді окремого розділу технічного завдання на створення ІТС;
- у вигляді окремого (часткового) технічного завдання;
- у вигляді доповнення до технічного завдання на створення ІТС.

Згідно з вимогами Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та НД ТЗІ 3.7-001-99, Технічне завдання на створення КСЗІ в ІТС має бути погоджено з Розробником ІТС, затверджено виконавцем робіт зі створення КСЗІ в ІТС та керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС. У випадках, передбачених Положенням про технічний захист інформації в Україні та НД ТЗІ 3.6-001-2000, Технічне завдання на створення КСЗІ в ІТС має бути погоджено з уповноваженим державним органом.

А.2.2 Проектна документація КСЗІ

А.2.2.1 Документація ескізного проекту КСЗІ в ІТС

А.2.2.1.1 У документації ескізного проекту КСЗІ, відповідно до положень НД ТЗІ 3.7-003-05, мають бути наведені відомості щодо попередніх проектних рішень, які визначають порядок реалізації вимог Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10, щодо КСЗІ в цілому та, за необхідності, щодо її окремих складових частин. Якщо відповідно до положень НД ТЗІ 3.7-003-05 етап ескізного проектування КСЗІ вилучається, документація ескізного проекту КСЗІ не розробляється.

А.2.2.1.2 Зміст та склад документації ескізного проекту повинні бути достатніми для повного опису проектних рішень рівня ескізного проекту. Конкретний перелік документації ескізного проекту має визначатися на підставі ГОСТ 34.201-89 та РД 50-34.698-90 з урахуванням особливостей відповідної КСЗІ. Обов'язковою є наявність пояснювальної записки до ескізного проекту КСЗІ, структура та зміст якої повинні відповідати вимогам РД 50-34.698-90.

А.2.2.1.3 Документація ескізного проекту КСЗІ в ІТС має бути погоджена з Розробником ІТС, затверджена виконавцем робіт зі створення КСЗІ в ІТС та керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

А.2.2.2 Документація технічного проекту КСЗІ в ІТС

А.2.2.2.1 У документації технічного проекту КСЗІ, відповідно до положень НД ТЗІ 3.7-003-05, мають бути наведені відомості щодо загальних проектних рішень, достатніх (з урахуванням результатів ескізного проектування, зазначених у п. А.2.2.1) для забезпечення реалізації вимог Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10; рішень щодо структури КСЗІ (організаційної структури, структури технічних і програмних засобів); рішень щодо архітектури та складу КЗЗ КСЗІ (у тому числі щодо використовуваних засобів антивірусного захисту, засобів виявлення та попередження про мережеві вторгнення тощо); рішень щодо механізмів реалізації ФПБ, визначених у наведеному в Технічному завданні функціональному профілі захищеності; рішень щодо алгоритмів, порядку та умов функціонування засобів захисту інформації, які використовуються у складі КЗЗ КСЗІ для реалізації певних ФПБ (функцій захисту).

А.2.2.2.2 Зміст та склад документації технічного проекту повинні бути достатніми для повного опису проектних рішень КСЗІ в обсязі, достатньому для виконання етапу робочого (технороботочого) проектування (реалізації) КСЗІ. Конкретний перелік документації технічного проекту має визначатися на підставі ГОСТ 34.201-89 та РД 50-34.698-90 з урахуванням особливостей відповідної КСЗІ. Обов'язковою є наявність пояснювальної записки до технічного проекту КСЗІ, структура та зміст якої повинні відповідати вимогам РД 50-34.698-90 та рекомендаціям НД ТЗІ 2.7-010-09 (у частині, що стосується проекту архітектури та детального проекту компонентів КЗЗ КСЗІ, створення яких здійснюється в ході створення КСЗІ, для визначеного у Технічному завданні на створення КСЗІ в ІТС рівня гарантій коректності реалізації ФПБ).

А.2.2.2.3 Документація технічного проекту КСЗІ в ІТС має бути погоджена з Розробником ІТС, затверджена виконавцем робіт зі створення КСЗІ в ІТС та керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

А.2.2.3 Документація робочого проекту КСЗІ в ІТС

А.2.2.3.1 У документації робочого проекту КСЗІ, відповідно до положень НД ТЗІ 3.7-003-05, мають бути наведені детальні рішення щодо реалізації технічного проекту КСЗІ, щодо забезпечення управління КСЗІ та взаємодії її компонентів, а також відомості, необхідні для проведення пусконалагоджувальних робіт і тестування підсистем та засобів КСЗІ.

А.2.2.3.2 Зміст та склад документації робочого проекту повинні бути достатніми для повного виконання етапу робочого (технороботочого) проектування (реалізації) КСЗІ. Конкретний перелік документації робочого проекту має визначатися на підставі ГОСТ 34.201-89 та РД 50-34.698-90 з урахуванням особливостей відповідної КСЗІ. Якщо в ході створення КСЗІ здійснюються роботи зі створення певних компонентів КЗЗ КСЗІ, обов'язковою є наявність матеріалів робочого проекту (реалізації) відповідних компонентів КЗЗ, зміст яких відповідає рекомендаціям НД ТЗІ 2.7-010-09 для визначеного у Технічному завданні на створення КСЗІ в ІТС, зазначеному в п. А.2.1.10, рівня гарантій коректності реалізації ФПБ.

А.2.2.3.3 Документація робочого проекту КСЗІ в ІТС має бути погоджена з

Розробником ІТС, затверджена виконавцем робіт зі створення КСЗІ в ІТС та керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

А.2.3 Матеріали, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ

А.2.3.1 Експертні висновки щодо відповідності використовуваних у складі КЗЗ КСЗІ засобів захисту інформації вимогам чинних нормативних документів системи ТЗІ

А.2.3.1.1 Експертні висновки щодо відповідності використовуваних у складі КЗЗ КСЗІ засобів захисту інформації вимогам чинних нормативних документів системи ТЗІ повинні надаватися для всіх засобів захисту інформації (у тому числі засобів антивірусного захисту, засобів виявлення та попередження про мережеві вторгнення тощо), які визначені у документації технічного проекту КСЗІ, зазначеній у п. А.2.2.2, як складові частини КЗЗ КСЗІ, та проведення державної експертизи яких не передбачається в ході проведення експертизи КСЗІ.

А.2.3.1.2 Зміст наданих Експертних висновків повинен відповідати вимогам Положення про державну експертизу в сфері технічного захисту інформації та враховувати рекомендації, наведені в Додатку Е.

А.2.3.1.3 На вимогу Експертів додатково до Експертних висновків мають бути надані технічні вимоги (зміст яких відповідає рекомендаціям НД ТЗІ 2.7-009-09) або аналогічні матеріали, які деталізують політику ФПБ (функції захисту), що реалізуються певним засобом захисту інформації, а також порядок та особливості реалізації відповідних ФПБ (функцій захисту).

А.2.3.1.4 Вміст наданих Експертних висновків та додаткових матеріалів повинен бути достатнім для того, щоб підтвердити можливість застосування визначених у документації технічного проекту КСЗІ засобів захисту інформації для реалізації політики відповідних ФПБ (відповідних функцій захисту), а також підтвердити коректність та обґрунтованість визначеного в документації технічного проекту порядку їх функціонування при реалізації відповідних ФПБ (функцій захисту).

А.2.3.2 Експертні висновки, сертифікати або інші документи, що підтверджують відповідність вимогам чинних нормативних документів системи КЗІ використовуваних у складі КЗЗ КСЗІ засобів КЗІ

А.2.3.2.1 Експертні висновки, сертифікати або інші документи, що підтверджують відповідність вимогам чинних нормативних документів системи КЗІ використовуваних у складі КЗЗ КСЗІ засобів КЗІ, мають надаватися для тих складових частин (компонентів) КЗЗ, що використовуються при реалізації політики певних ФПБ за допомогою механізмів, побудованих з використанням алгоритмів криптографічних перетворень. Експертні висновки (сертифікати або інші документи) щодо відповідності вимогам чинних нормативних документів системи КЗІ повинні надаватися у таких випадках:

- якщо проведення експертизи засобів реалізації відповідних ФПБ передбачається в ході проведення експертизи КСЗІ;
- якщо вимоги щодо наявності відповідних Експертних висновків (сертифікатів або інших документів) містяться у наданих Експертних висновках щодо відповідності вимогам чинних нормативних документів системи ТЗІ використовуваних у складі КЗЗ КСЗІ засобів захисту інформації, зазначених у п. А.2.3.1.

А.2.3.2.2 Зміст наданих Експертних висновків (сертифікатів або інших документів) повинен відповідати вимогам Положення про державну експертизу в сфері криптографічного захисту інформації та іншої чинної нормативно-правової бази в сфері КЗІ.

А.2.3.2.3 Вміст наданих Експертних висновків (сертифікатів або інших документів) має бути достатнім для того, щоб підтвердити коректність реалізації відповідними засобами КЗІ алгоритмів криптографічних перетворень, а також підтвердити коректність та

обґрунтованість визначеного в документації технічного проекту КСЗІ, зазначеній у п. А.2.2.2, порядку їх функціонування при реалізації відповідних ФПБ (функцій захисту).

А.2.4 Матеріали (документи), необхідні для оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ, створення та експертиза яких здійснюється в ході створення та експертизи КСЗІ

А.2.4.1 Склад та зміст матеріалів (документів), необхідних для оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ, створення та експертиза яких здійснюється в ході створення та експертизи КСЗІ, повинні визначатися з урахуванням рекомендацій НД ТЗІ 2.7-010-009 для визначеного у Технічному завданні на створення КСЗІ в ІТС, зазначеному в п. А.2.1.10, рівня гарантій коректності реалізації ФПБ.

А.2.4.2 Функціональні специфікації окремих компонентів (складових частин) КЗЗ КСЗІ можуть бути наведені у Технічному завданні на створення КСЗІ в ІТС.

А.2.4.3 Проекти архітектури та детальні проекти окремих компонентів (складових частин) КЗЗ КСЗІ можуть бути надані у складі документації технічного проекту КСЗІ, зазначеній у п. А.2.2.2.

А.2.4.4 Вхідний код та інші матеріали щодо реалізації окремих компонентів (складових частин) КЗЗ КСЗІ можуть бути надані у складі документації робочого проекту КСЗІ, зазначеній у п. А.2.2.3.

А.2.4.5 Програма та методика випробувань ФПБ та протоколи випробувань ФПБ, які реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ, можуть бути надані у складі документації щодо проведених випробувань КСЗІ, зазначеній у п. А.2.7.

А.2.4.6 Описи послуг безпеки, які реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ, настанови адміністраторам з послуг безпеки, настанови користувачам з послуг безпеки, опис процедур безпечної інсталяції, генерації та запуску можуть бути надані у складі експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ, зазначеній у п. А.2.5.

А.2.5 Експлуатаційна документація компонентів (складових частин) КЗЗ КСЗІ

А.2.5.1 До складу експлуатаційної документації мають входити документи, що визначають порядок інсталяції, ініціалізації, налаштування та експлуатації всіх без винятку компонентів (складових частин) КЗЗ КСЗІ, визначених у документації технічного проекту КСЗІ в ІТС, зазначеній у п. А.2.2.2.

А.2.5.2 Відповідно до вимог НД ТЗІ 2.5-004-99, для кожного компонента (складової частини) КЗЗ КСЗІ у вигляді окремих документів або розділів інших документів повинні бути надані:

- опис процедур безпечної інсталяції, генерації та запуску;
- опис послуг безпеки, що реалізуються відповідним компонентом;
- настанови адміністратору з послуг безпеки;
- настанови користувачу з послуг безпеки.

А.2.5.3 Зміст відповідних документів повинен відповідати вимогам НД ТЗІ 2.5-004-99 та рекомендаціям НД ТЗІ 2.7-010-09.

А.2.6 Нормативно-розпорядча документація КСЗІ

А.2.6.1 Інструкції щодо забезпечення правил оброблення ІзОД в ІТС

А.2.6.1.1 Інструкції щодо забезпечення правил оброблення ІзОД в ІТС (Інструкція про забезпечення режиму секретності під час оброблення в ІТС інформації, що становить державну таємницю, або Інструкція про порядок оброблення в ІТС конфіденційної інформації, що є власністю держави) мають розроблюватися у випадку, якщо в ІТС передбачається оброблення ІзОД, що становить ІДТ, або КІВД. У відповідних інструкціях

має бути окреслено перелік заходів, спрямованих на дотримання визначеного вимогами чинної нормативно-правової бази режиму доступу до ІзОД, визначено порядок дій персоналу та користувачів ІТС з метою реалізації зазначених заходів, а також встановлено їх відповідальність у випадку порушення зазначених вимог. Зокрема, в інструкціях щодо забезпечення правил оброблення ІзОД в ІТС рекомендується у вигляді, наприклад, окремих розділів викласти:

- загальні відомості щодо організації захисту ІзОД в ІТС;
- опис порядку доступу до приміщень, в яких розташовані засоби обчислювальної системи ІТС;
- опис порядку захисту інформації від витоку технічними каналами;
- опис порядку захисту інформації від НСД;
- опис порядку здійснення антивірусного захисту;
- опис порядку впровадження і використання програмного забезпечення;
- опис порядку створення захищених інформаційних ресурсів, реєстрації користувачів та надання прав доступу до інформації користувачам ІТС;
- опис порядку контролю за дотриманням користувачами правил роботи із засобами ІТС;
- опис порядку обліку, зберігання, обігу, резервування, ротації та знищення матеріальних носіїв, що використовуються для зберігання ІзОД;
- опис порядку проведення ремонтних робіт та відновлення працездатності ІТС;
- опис порядку контролю за забезпеченням захисту ІзОД в ІТС;
- обов’язки користувачів та персоналу ІТС стосовно дотримання встановленого порядку оброблення ІзОД;
- відповідальність користувачів та персоналу ІТС за порушення встановленого порядку оброблення ІзОД.

А.2.6.1.2 В Інструкції про забезпечення режиму секретності під час оброблення в ІТС інформації, що становить державну таємницю, повинні бути враховані вимоги Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах та Порядку організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, а в Інструкції про порядок оброблення в ІТС конфіденційної інформації, що є власністю держави – вимоги Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, щодо організації та порядку оброблення відповідної інформації в ІТС. Зокрема, мають бути враховані вимоги щодо використання журналів обліку та реєстрації сховищ та матеріальних носіїв ІзОД, зазначених у п. А.2.10, а також визначено порядок та особливості використання відповідних журналів.

А.2.6.1.3 В Інструкціях щодо забезпечення правил оброблення ІзОД в ІТС мають бути враховані положення посадових (функціональних) інструкцій співробітників СЗІ, персоналу та користувачів ІТС, зазначених у п. А.2.6.2, а також технологічних (операційних) інструкцій (настанов) щодо виконання завдань з адміністрування та обслуговування КСЗІ, зазначених у п. А.2.6.3.

А.2.6.1.4 Інструкції щодо забезпечення правил оброблення ІзОД в ІТС мають бути погоджені з режимно-секретним органом організації (установи), яка є власником (розпорядником) ІТС, погоджені з виконавцем робіт зі створення КСЗІ в ІТС та затверджені керівником організації (установи).

А.2.6.2 Посадові (функціональні) інструкції співробітників СЗІ, персоналу та користувачів ІТС

А.2.6.2.1 Посадові (функціональні) інструкції співробітників СЗІ, персоналу та користувачів ІТС мають визначати обов'язки, відповідальність та порядок дій співробітників (посадових осіб) СЗІ, персоналу та користувачів ІТС у процесі виконання ними завдань щодо керування засобами ІТС та КСЗІ, а також оброблення в ІТС інформаційних ресурсів, що потребують захисту. Перелік та зміст цих інструкцій повинні визначатися з урахуванням:

- структури та штатного розкладу СЗІ, визначених у Положенні про СЗІ в ІТС, зазначеному в п. А.2.1.3;
- завдань, функцій та повноважень співробітників (посадових осіб) СЗІ, наведених у Положенні про СЗІ в ІТС;
- категорій персоналу та користувачів ІТС, визначених в Описі політики безпеки інформації в ІТС, зазначеному в п. А.2.1.5, та вимог Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10, щодо розподілу обов'язків користувачів та їх функціональних завдань;
- порядку дій співробітників (посадових осіб) СЗІ, персоналу та користувачів ІТС, який випливає з положень Опису політики безпеки інформації в ІТС, документації технічного проекту КСЗІ в ІТС, зазначеної у п. А.2.1.2, документації робочого проекту КСЗІ в ІТС, зазначеної у п. А.2.1.3, та експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ, зазначеної у п. А.2.5, щодо забезпечення визначеного порядку функціонування ІТС та КСЗІ.

Як приклади зазначених інструкцій можна розглядати такі:

- Інструкція системного адміністратора ІТС;
- Інструкція адміністратора безпеки ІТС;
- Інструкція користувача ІТС.

А.2.6.2.2 У посадових (функціональних) інструкціях необхідно у вигляді, наприклад, окремих розділів викласти:

- загальні положення, в яких визначено категорії співробітників СЗІ, персоналу або користувачів ІТС, на яких поширюються вимоги відповідних інструкцій;
- основні завдання та функції (функціональні завдання), що мають виконуватися співробітниками СЗІ, персоналом або користувачами ІТС, на яких поширюються вимоги відповідних інструкцій;
- опис правил та порядку дій співробітників СЗІ, персоналу або користувачів ІТС в процесі виконання функціональних завдань;
- повноваження, обов'язки та відповідальність осіб, на яких поширюються вимоги відповідних інструкцій.

А.2.6.2.3 У посадових (функціональних) інструкціях співробітників СЗІ, персоналу та користувачів ІТС повинні бути враховані положення технологічних (операційних) інструкцій (настанов) щодо виконання завдань з адміністрування та обслуговування КСЗІ, зазначених у п. А.2.6.3.

А.2.6.2.4 Посадові (функціональні) інструкції співробітників СЗІ, персоналу та користувачів ІТС можуть бути оформлені як у вигляді окремих документів, так і у вигляді структурних частин інших документів, наприклад, Інструкції щодо забезпечення правил оброблення ІзОД в ІТС, зазначеної у п. А.2.6.1.

А.2.6.2.5 Посадові (функціональні) інструкції співробітників СЗІ, персоналу та користувачів ІТС мають бути погоджені з Розробником ІТС, виконавцем робіт зі створення КСЗІ в ІТС та затверджені керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

А.2.6.3 Технологічні (операційні) інструкції (настанови) щодо виконання завдань з адміністрування та обслуговування КСЗІ

А.2.6.3.1 Технологічні (операційні) інструкції (настанови) щодо виконання завдань з адміністрування та обслуговування КСЗІ повинні детально визначати послідовність дій співробітників (посадових осіб) СЗІ та персоналу ІТС у процесі виконання відповідних завдань. Перелік та зміст відповідних інструкцій повинні визначатися з урахуванням:

- структури та штатного розкладу СЗІ, визначених у Положенні про СЗІ в ІТС, зазначеному в п. А.2.1.3;
- завдань, функцій та повноважень співробітників (посадових осіб) СЗІ, наведених у Положенні про СЗІ в ІТС;
- категорій персоналу та користувачів ІТС, визначених в Описі політики безпеки інформації в ІТС, зазначеному в п. А.2.1.5, та вимог Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10, щодо розподілу обов'язків користувачів та їх функціональних завдань;
- порядку дій співробітників (посадових осіб) СЗІ, персоналу та користувачів ІТС, який випливає з положень Опису політики безпеки інформації в ІТС, документації технічного проекту КСЗІ в ІТС, зазначеної у п. А.2.1.2, документації робочого проекту КСЗІ в ІТС, зазначеної у п. А.2.1.3, та експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ, зазначеної у п. А.2.5, щодо забезпечення визначеного порядку функціонування ІТС та КСЗІ.

Як приклади зазначених інструкцій можна розглядати такі:

- Інструкція про порядок введення в експлуатацію КСЗІ;
- Інструкція про порядок модернізації КСЗІ;
- Інструкція про порядок резервування та відновлення інформації в ІТС;
- Інструкція про порядок оперативного відновлення функціонування ІТС;
- Інструкція про порядок проведення ремонтних робіт;
- Інструкція про організацію контролю за функціонуванням КСЗІ;
- Інструкція про порядок розроблення, впровадження та модернізації програмного забезпечення ІТС;
- Інструкція про порядок реєстрації користувачів ІТС;
- Інструкція про порядок створення захищених інформаційних ресурсів в ІТС;
- Інструкція про порядок надання доступу до захищених інформаційних ресурсів в ІТС;
- Інструкція про порядок забезпечення антивірусного захисту в ІТС.

А.2.6.3.2 У технологічних (операційних) інструкціях (настановах) необхідно у вигляді, наприклад, окремих розділів викласти:

- загальні положення, в яких визначено завдання з адміністрування та обслуговування КСЗІ, порядок виконання яких встановлюється інструкцією (настановою), категорії співробітників СЗІ або персоналу ІТС, на яких поширюються вимоги відповідних інструкцій (настанов) та які є відповідальними за виконання відповідних завдань;
- опис послідовності, правил та порядку здійснення технологічних операцій в ході виконання відповідальними особами певних завдань з адміністрування та обслуговування КСЗІ;
- опис порядку реєстрації фактів та результатів виконання певних завдань у відповідних реєстраційних журналах.

Повинні бути визначені (наприклад, у додатках до інструкцій) форми використовуваних реєстраційних журналів.

А.2.6.3.3 У технологічних (операційних) інструкціях (настановах) мають бути враховані положення посадових (функціональних) інструкцій співробітників СЗІ та персоналу ІТС, зазначеному в п. А.2.6.2.

А.2.6.3.4 Технологічні (операційні) інструкції (настанови) щодо виконання завдань з адміністрування та обслуговування КСЗІ можуть бути оформлені як у вигляді окремих документів, так і у вигляді структурних частин інших документів, наприклад, Інструкції щодо забезпечення правил оброблення ІзОД в ІТС, зазначеної у п. А.2.6.1.

А.2.6.3.5 Технологічні (операційні) інструкції (настанови) щодо виконання завдань з адміністрування та обслуговування КСЗІ мають бути погоджені з Розробником ІТС, виконавцем робіт зі створення КСЗІ в ІТС та затверджені керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

А.2.6.4 Інструкції про порядок використання засобів КЗІ

А.2.6.4.1 Інструкції про порядок використання засобів КЗІ повинні визначати порядок забезпечення безпеки, порядок керування ключовими даними використовуваних у складі КЗЗ КСЗІ засобів КЗІ та, за необхідності, порядок користування засобами КЗІ. Перелік та зміст відповідних інструкцій визначаються вимогами чинної нормативно-правової бази у сфері КЗІ, зокрема Положенням про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису і Положенням про порядок розроблення, виробництва та уведення в експлуатацію засобів криптографічного захисту конфіденційної інформації, що є власністю держави.

Так, відповідно до вимог Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису повинні бути розроблені:

- Інструкція із забезпечення безпеки експлуатації засобів КЗІ;
- Інструкція щодо порядку генерації ключових даних та поводження з ключовими документами.

А.2.6.4.2 Інструкції про порядок використання засобів КЗІ повинні бути (за результатами державної експертизи) погоджені з уповноваженим державним органом (розроблені на основі типових інструкцій, погоджених відповідним чином з уповноваженим державним органом) та затверджені керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

А.2.7 Документація щодо проведених випробувань КСЗІ

А.2.7.1 До складу документації щодо проведених випробувань КСЗІ, відповідно до положень НД ТЗІ 3.7-003-05, повинні входити:

- Програма та методика випробувань КСЗІ в ІТС;
- Протокол (протоколи) попередніх випробувань КСЗІ в ІТС.

А.2.7.2 Програма та методика випробувань КСЗІ в ІТС має містити перелік перевірок та опис методів (методик) виконання окремих перевірок, успішне проведення яких дозволяє дійти однозначного висновку щодо відповідності створеної КСЗІ вимогам Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10. Зміст Програми та методики випробувань КСЗІ в ІТС має відповідати вимогам РД 50-34.698-90. При розробленні Програми та методики випробувань КСЗІ в ІТС можуть (як довідкові) використовуватися вимоги, викладені у Додатку Б та Додатку В. Якщо в ході створення КСЗІ здійснюються роботи зі створення певних компонентів КЗЗ КСЗІ, до складу Програми та методики випробувань КСЗІ в ІТС може бути введено Програму та методику випробувань ФПБ, зміст якої відповідає рекомендаціям НД ТЗІ 2.7-010-09 для визначеного у Технічному завданні на створення КСЗІ в ІТС рівня гарантій коректності реалізації ФПБ.

А.2.7.3 Програма та методика випробувань КСЗІ в ІТС має бути погоджена з

Розробником ІТС, керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС, та затверджена виконавцем робіт зі створення КСЗІ в ІТС. Якщо до складу Програми та методики випробувань КСЗІ в ІТС входить Програма та методика випробувань ФПБ, у випадках, передбачених НД ТЗІ 3.6-001-2000, Програма та методика випробувань КСЗІ в ІТС має бути погоджена з уповноваженим державним органом.

А.2.7.4 Протокол (протоколи) попередніх випробувань КСЗІ в ІТС повинен містити:

- задокументовані результати випробувань, передбачених Програмою та методикою випробувань КСЗІ в ІТС;
- перелік виявлених недоліків, необхідних заходів щодо їх усунення та рекомендовані терміни виконання цих робіт;
- висновки щодо можливості прийняття КСЗІ в дослідну експлуатацію.

А.2.7.5 Зміст Протоколу (протоколів) попередніх випробувань КСЗІ в ІТС має відповідати вимогам РД 50-34.698-90 та рекомендаціям НД ТЗІ 2.7-010-09 для визначеного у Технічному завданні на створення КСЗІ в ІТС рівня гарантій коректності реалізації ФПБ.

А.2.7.6 Протокол (протоколи) попередніх випробувань має бути підписаний членами комісії з проведення випробувань та затверджений керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

А.2.8 Організаційно-розпорядча документація КСЗІ

А.2.8.1 До складу організаційно-розпорядчої документації КСЗІ, відповідно до положень НД ТЗІ 3.7-003-05 та інших чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу, повинні входити:

- Акт про приймання КСЗІ в ІТС у дослідну експлуатацію;
- Акт завершення дослідної експлуатації КСЗІ в ІТС;
- Акт завершення робіт зі створення КСЗІ в ІТС.

А.2.8.2 Зміст Акта про приймання КСЗІ в ІТС у дослідну експлуатацію має відповідати вимогам РД 50-34.698-90. В Акті про приймання КСЗІ в ІТС у дослідну експлуатацію мають бути відображені задокументовані в Протоколі (протоколах) попередніх випробувань КСЗІ в ІТС, зазначеному в п. А.2.7.1, відомості щодо результатів випробувань, виявлених недоліків та необхідних заходів з їх усунення, а також наведені висновки щодо можливості прийняття КСЗІ в дослідну експлуатацію.

А.2.8.3 Акт про приймання КСЗІ в ІТС у дослідну експлуатацію має бути підписаний членами комісії з проведення випробувань (представниками виконавця робіт зі створення КСЗІ в ІТС, представниками організації (установи), яка є власником (розпорядником) ІТС) та затверджений керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

А.2.8.4 Акт завершення дослідної експлуатації КСЗІ в ІТС має бути складений у довільній формі. В Акті завершення дослідної експлуатації КСЗІ в ІТС мають бути відображені результати дослідної експлуатації, а також наведені висновки щодо можливості (неможливості) надання КСЗІ на державну експертизу.

А.2.8.5 Акт завершення дослідної експлуатації КСЗІ в ІТС має бути підписаний представниками виконавця робіт зі створення КСЗІ в ІТС, представниками організації (установи), яка є власником (розпорядником) ІТС, та затверджений керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

А.2.8.6 Зміст Акта завершення робіт зі створення КСЗІ в ІТС має відповідати вимогам РД 50-34.698-90 та у випадках створення КСЗІ в ІТС, яка являє собою АС класу 1 згідно з НД ТЗІ 2.5-005-99, в якій обробляється інформація, що становить державну таємницю, рекомендаціям НД ТЗІ 2.5-007-2007.

А.2.8.7 Акт завершення робіт зі створення КСЗІ в ІТС має бути підписаний представниками виконавця робіт зі створення КСЗІ в ІТС, представниками організації (установи), яка є власником (розпорядником) ІТС, та затверджений керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

А.2.9 Супровідна документація КСЗІ

А.2.9.1 До складу супровідної документації КСЗІ, відповідно до положень НД ТЗІ 3.7-003-05 та інших чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу, повинні входити:

- Формуляр ІТС;
- реєстраційні журнали, використовувані для реєстрації фактів та результатів виконання певних завдань з адміністрування та обслуговування КСЗІ.

А.2.9.2 Форма та зміст Формуляра ІТС мають відповідати вимогам РД 50-34.698-90 та у випадках створення КСЗІ в ІТС, яка являє собою АС класу 1 згідно з НД ТЗІ 2.5-005-99, в якій обробляється інформація, що становить державну таємницю, рекомендаціям НД ТЗІ 2.5-007-2007. У частині, що стосується відомостей про стан ІТС, Формуляр ІТС може містити посилання на відповідні реєстраційні журнали.

А.2.9.3 Перелік та форми реєстраційних журналів повинні відповідати визначеним у технологічних (операційних) інструкціях (настановах) щодо виконання завдань з адміністрування та обслуговування КСЗІ, зазначених у п. А.2.6.3.

Як приклади зазначених реєстраційних журналів можна розглядати такі:

- Журнал обліку користувачів ІТС;
- Журнал обліку роботи користувачів ІТС;
- Журнал обліку захищених інформаційних ресурсів ІТС;
- Журнал реєстрації проведених робіт з технічного обслуговування, ремонту, модернізації;
- Журнал реєстрації перевірок складу програмних засобів ІТС;
- Журнал реєстрації нештатних ситуацій у роботі ІТС.

А.2.10 Журнали обліку та реєстрації сховищ та матеріальних носіїв ІзОД

А.2.10.1 Журнали обліку та реєстрації сховищ та матеріальних носіїв ІзОД є окремою частиною супровідної документації КСЗІ. Журнали обліку та реєстрації сховищ та матеріальних носіїв ІзОД використовуються у випадку, якщо в ІТС передбачається оброблення ІзОД, що становить ІДТ або КІВД.

А.2.10.2 Якщо в ІТС передбачається оброблення ІзОД, що становить ІДТ, під час функціонування ІТС використовуються такі журнали, форми та правила ведення яких встановлені Порядком організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях:

- Журнал обліку сховищ матеріальних носіїв секретної інформації та ключів від них (форма 23 зазначеного вище Порядку);
- Журнал здавання (приймання) з-під охорони режимних приміщень, сховищ матеріальних носіїв секретної інформації та ключів від них (форма 24 зазначеного вище Порядку);
- Журнал обліку вхідних і підготовлених секретних документів (форма 27 зазначеного вище Порядку);
- Журнал обліку підготовлених секретних документів (форма 28 зазначеного вище Порядку);
- Журнал обліку робочих зошитів, спецблокнотів, окремих аркушів, бланків, форм (форма 37 зазначеного вище Порядку).

А.2.10.3 Якщо в ІТС передбачається оброблення ІзОД, що становить КІВД, під час функціонування ІТС використовуються такі журнали, форми та правила ведення яких встановлені Інструкцією про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави:

- Журнал обліку документів та видань з грифом "Для службового користування" (форма 2 зазначеної вище Інструкції);
- Журнал обліку магнітних носіїв інформації з грифом "Для службового користування" (форма 4 зазначеної вище Інструкції).

А.3 Рекомендації до змісту документації щодо створення комплексу ТЗІ

А.3.1 Документація, що розробляється на етапі виконання передпроектних робіт

А.3.1.1 До складу документації щодо створення комплексу ТЗІ, що розробляється на етапі виконання передпроектних робіт**,** відповідно до положень НД ТЗІ 1.1-005-07, НД ТЗІ 3.1-001-07 та інших чинних нормативних документів щодо забезпечення ТЗІ на об'єктах інформаційної діяльності (ОІД), входять:

- Протокол про визначення вищого ступеня обмеження доступу до інформації;
- Акт категорування приміщень ОІД;
- Акт обстеження ОІД стосовно створення комплексу ТЗІ;
- Модель загроз для ІзОД (стосовно забезпечення захисту від витоку ІзОД технічними каналами);
- Технічне завдання на створення комплексу ТЗІ (технічні вимоги з питань ТЗІ).

А.3.1.2 Форма, зміст та порядок затвердження Протоколу про визначення вищого ступеня обмеження доступу до інформації мають відповідати вимогам НД ТЗІ 1.1-005-07. Наведені у протоколі відомості щодо ступеня обмеження доступу (ступеня секретності) інформації, що циркулює на ОІД, мають відповідати аналогічним відомостям, наведеним у Переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, зазначеному в п. А.2.1.1.

А.3.1.3 Форма, зміст та порядок затвердження Акта категорування приміщень ОІД мають відповідати вимогам ТПКО-95. Наведені в Акті категорування приміщень ОІД відомості щодо ступеня обмеження доступу (ступеня секретності) інформації, що циркулює на ОІД, а також щодо категорії відповідних приміщень мають відповідати аналогічним відомостям, наведеним у Переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, та Акті категорування ІТС, зазначеному в п. А.2.1.2.

А.3.1.4 Форма, зміст та порядок затвердження Акта обстеження ОІД стосовно створення комплексу ТЗІ мають відповідати вимогам НД ТЗІ 3.1-001-07. Наведені в Акті обстеження ОІД відомості щодо технічних засобів, які передбачається використовувати для оброблення ІзОД (основні технічні засоби ІТС, кабельне обладнання), та щодо їх розташування повинні відповідати аналогічним відомостям, наведеним у результатах обстеження середовищ функціонування ІТС, зазначених у п. А.2.1.4.

А.3.1.5 Форма, зміст, порядок розроблення та затвердження Моделі загроз для ІзОД (стосовно забезпечення захисту від витоку ІзОД технічними каналами) мають відповідати вимогам НД ТЗІ 1.6-003-04. У загальному випадку до складу моделі загроз мають входити: ситуаційний план ОІД та його опис; генеральний план ОІД та його опис; схема розташування та опис ОТЗ та систем; схема розташування та опис додаткових технічних засобів та систем; опис можливих технічних каналів витоку інформації. Наведені в Моделі загроз для ІзОД схема розташування та опис ОТЗ і систем мають відповідати аналогічним відомостям, наведеним у результатах обстеження середовищ функціонування ІТС.

А.3.1.6 Форма, зміст, порядок розроблення та затвердження Технічного завдання на

створення комплексу ТЗІ (технічних вимог з питань ТЗІ) мають відповідати вимогам НД ТЗІ 3.1-001-07. Відомості та вимоги, наведені в Технічному завдання на створення комплексу ТЗІ, мають відповідати аналогічним відомостям, наведеним в іншій документації, розроблюваній на етапі виконання передпроектних робіт зі створення комплексу ТЗІ (Протоколу про визначення вищого ступеня обмеження доступу до інформації, Акту категорування приміщень ОІД, Акту обстеження ОІД стосовно створення комплексу ТЗІ, Моделі загроз для ІзОД).

А.3.1.7 Відповідно до положень НД ТЗІ 3.7-001-99, технічні вимоги з питань ТЗІ можуть бути викладені у вигляді окремого розділу Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10.

А.3.2 Документація, що розробляється на етапі розроблення та впровадження заходів із захисту інформації

А.3.2.1 До складу документації щодо створення комплексу ТЗІ, що розробляється на етапі розроблення та впровадження заходів із захисту інформації, відповідно до положень НД ТЗІ 1.1-005-07, НД ТЗІ 3.3-001-07 та інших чинних нормативних документів щодо забезпечення ТЗІ на ОІД, входять:

- Пояснювальна записка з ТЗІ;
- проектно-кошторисна, конструкторська та експлуатаційна документація комплексу ТЗІ.

А.3.2.2 Порядок розроблення та затвердження Пояснювальної записки з ТЗІ має відповідати вимогам НД ТЗІ 3.3-001-07. У загальному випадку у Пояснювальній записці з ТЗІ мають бути визначені перелік, зміст, терміни виконання робіт щодо створення комплексу ТЗІ, склад документів, що розробляються під час його створення тощо. Зміст заходів, наведених у Пояснювальній записці з ТЗІ, має забезпечувати виконання всіх вимог, визначених у Технічному завданні на створення комплексу ТЗІ, зазначеному в п. А.3.1.

А.3.2.3 Проектно-кошторисна, конструкторська та експлуатаційна документація комплексу ТЗІ розробляється у складі, визначеному Пояснювальною запискою з ТЗІ. Порядок розроблення та затвердження відповідної документації має відповідати вимогам НД ТЗІ 3.3-001-07. При розробленні відповідної документації мають бути враховані положення чинних НД ТЗІ, що стосуються реалізації певних заходів захисту під час створення на ОІД комплексів ТЗІ (НД ТЗІ 2.4-007-08, НД ТЗІ 2.7-007-08 тощо).

А.3.3 Документація, що розробляється на етапі випробувань та атестації комплексу ТЗІ

А.3.3.1 До складу документації щодо створення комплексу ТЗІ, що розробляється на етапі випробувань та атестації комплексу ТЗІ, відповідно до положень НД ТЗІ 1.1-005-07, НД ТЗІ 3.3-001-07, НД ТЗІ 2.1-002-07 та інших чинних нормативних документів щодо забезпечення ТЗІ на ОІД, входять:

- програми та методики випробувань комплексу ТЗІ;
- протоколи за результатами випробувань комплексу ТЗІ;
- Акт атестації комплексу ТЗІ;
- Паспорт на комплекс ТЗІ.

А.3.3.2 Зміст, порядок розроблення та затвердження програм і методик випробувань комплексу ТЗІ мають відповідати вимогам НД ТЗІ 2.1-002-07. При розробленні відповідних програм та методик повинні бути враховані положення чинних НД ТЗІ, що стосуються перевірки ефективності створених на ОІД комплексів ТЗІ (НД ТЗІ 2.2-005-08, НД ТЗІ 2.3-014-08, НД ТЗІ 2.3-015-08, НД ТЗІ 2.3-016-08 тощо).

А.3.3.3 Зміст, порядок підготовлення та затвердження протоколів за результатами випробувань комплексу ТЗІ мають відповідати вимогам НД ТЗІ 2.1-002-07. У протоколах мають бути наявні висновки про відповідність створеного комплексу ТЗІ вимогам чинних

НД з питань ТЗІ. Висновки повинні містити конкретні формулювання, що забезпечують їх однозначне трактування.

А.3.3.4 Зміст, порядок підготовлення та затвердження Акта атестації комплексу ТЗІ мають відповідати вимогам НД ТЗІ 2.1-002-07. В Акті атестації мають бути наведені відомості про:

- підстави для проведення атестації;
- виконавця атестації;
- дату проведення атестації;
- результати атестації;
- зауваження та рекомендації (додаткові умови, яких потрібно дотримуватися під час експлуатації ОІД);
- висновки щодо відповідності комплексу ТЗІ вимогам технічних завдань і НД з питань ТЗІ;
- термін проведення чергової атестації (строк дії Акта атестації).

А.3.3.5 Форма, зміст, порядок розроблення та затвердження Паспорта на комплекс ТЗІ мають відповідати вимогам НД ТЗІ 3.3-001-07.

Додаток Б
(обов'язковий)

Вимоги щодо змісту програми проведення експертизи комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

У Додатку Б викладено специфічні вимоги щодо змісту програми проведення експертизи КСЗІ в ІТС. Вимоги викладено з урахуванням положень чинної нормативно-правової бази в сфері ТЗІ, яка регламентує порядок проведення робіт зі створення та експертизи КСЗІ в ІТС, а також з урахуванням рекомендацій щодо складу та змісту проектної, експлуатаційної та нормативно-розпорядчої документації, яка надається Замовником при проведенні експертизи КСЗІ, наведених у Додатку А.У п. Б.1 наведено вимоги щодо змісту програми проведення експертизи КСЗІ у частині, що стосується визначення переліку та етапності експертних робіт, а у п. Б.2 – вимоги щодо змісту програми проведення певних етапів експертних робіт.

Б.1 Вимоги щодо змісту програми проведення експертизи у частині, що стосується визначення переліку та етапності експертних робіт

Б.1.1 Перелік та етапність експертних робіт, виконання яких має передбачатися Програмою проведення експертизи КСЗІ в ІТС, повинні формуватися з урахуванням положень чинної нормативно-правової бази в сфері ТЗІ щодо проведення робіт зі створення КСЗІ в АС різного класу, в яких обробляється інформація з різними характеристиками відповідно до встановленого законодавством правового режиму та режиму доступу, а також специфічних вимог щодо створюваної КСЗІ, визначених за результатами аналізу наданих Замовником Технічного завдання на створення КСЗІ та іншої проектної, експлуатаційної та нормативно-розпорядчої документації, перелік якої наведено у таблиці А.1.

Б.1.2 У загальному випадку Програма проведення експертизи КСЗІ в ІТС має передбачати проведення (у наведеній послідовності) таких експертних робіт:

- аналіз документації, розробленої на етапі виконання передпроектних робіт;
- аналіз Технічного завдання на створення КСЗІ в ІТС;
- оцінювання (за необхідності) ФПБ, що реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ;
- оцінювання (за необхідності) рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ;
- аналіз проектної документації КСЗІ та матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ;
- аналіз експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ;
- аналіз нормативно-розпорядчої документації КСЗІ;
- аналіз документації щодо проведених випробувань КСЗІ;
- аналіз організаційно-розпорядчої документації КСЗІ;
- перевірка фактичного використання введених до складу КЗЗ КСЗІ засобів захисту інформації;
- перевірка порядку використання введених до складу КЗЗ КСЗІ засобів захисту інформації;
- перевірка впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту;
- перевірка підготовленості співробітників СЗІ, персоналу та користувачів ІТС;
- перевірка (за необхідності) результатів створення та атестації комплексу ТЗІ.

Мета та обсяги відповідних робіт повинні визначатися з урахуванням вимог пп. Б.2.1-Б.2.14.

Б.2 Вимоги щодо змісту програми проведення експертизи КСЗІ у частині, що стосується проведення певних етапів експертних робіт

Б.2.1 Вимоги щодо змісту програми проведення експертизи КСЗІ у частині, що стосується аналізу документації, розробленої на етапі виконання передпроектних робіт

Програма проведення експертизи КСЗІ у частині, що стосується аналізу документації, розробленої на етапі виконання передпроектних робіт, повинна передбачати виконання Експертом необхідних дій з метою підтвердження того, що:

Б.2.1.1 Склад документації, розробленої на етапі виконання передпроектних робіт, зазначеної в пп. А.2.1.1-А.2.1.9, відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, оброблюваної в ІТС відповідного типу.

Б.2.1.2 Зміст документації, розробленої на етапі виконання передпроектних робіт, відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, оброблюваної в ІТС відповідного типу.

Б.2.1.3 Вміст документації, розробленої на етапі виконання передпроектних робіт, відповідає особливостям конкретної ІТС та умовам її функціонування, визначеним на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ.

Б.2.1.4 Документація, розроблена на етапі виконання передпроектних робіт, узгоджена та затверджена у порядку, передбаченому положенням чинної нормативно-правової бази в сфері ТЗІ.

Б.2.2 Вимоги щодо змісту програми проведення експертизи у частині, що стосується аналізу Технічного завдання на створення КСЗІ в ІТС

Програма проведення експертизи КСЗІ у частині, що стосується аналізу Технічного завдання на створення КСЗІ в ІТС, повинна передбачати виконання Експертом необхідних дій з метою підтвердження того, що:

Б.2.2.1 У Технічному завданні на створення КСЗІ в ІТС, зазначеному в п. А.2.1.10, у повному обсязі та коректно враховані положення чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, оброблюваної в ІТС відповідного типу.

Б.2.2.2 У Технічному завданні на створення КСЗІ в ІТС у повному обсязі та коректно враховано особливості конкретної ІТС та умови її функціонування, визначені на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ, а також наведені у документації, розробленій на етапі виконання передпроектних робіт, зазначені в пп. А.2.1.1-А.2.1.9.

Б.2.2.3 Реалізація визначеного у Технічного завданні на створення КСЗІ в ІТС переліку вимог є достатньою для задоволення вимог чинних нормативних документів щодо забезпечення захисту інформації, оброблюваної у відповідній ІТС.

Б.2.2.4 Технічне завдання на створення КСЗІ в ІТС узгоджено та затверджено у порядку, передбаченому положеннями чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, оброблюваної в ІТС відповідного типу.

Б.2.3 Вимоги щодо змісту програми проведення експертизи у частині, що стосується оцінювання ФПБ, які реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ

Програма проведення експертизи КСЗІ у частині, що стосується оцінювання ФПБ, які реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ, має враховувати склад та зміст матеріалів (документів), наданих для оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ, створення та

експертиза яких здійснюється в ході створення та проведення експертизи КСЗІ, зазначених у п. А.2.4, та відповідати вимогам НД ТЗІ 2.7-009-09 для визначеного у Технічному завданні на створення КСЗІ в ІТС, зазначеному в п. А.2.1.10, рівня гарантій коректності реалізації ФПБ.

Б.2.4 Вимоги щодо змісту програми проведення експертизи у частині, що стосується оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ

Програма проведення експертизи КСЗІ у частині, що стосується рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ, має враховувати склад та зміст матеріалів (документів), наданих для оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ, створення та експертиза яких здійснюється в ході створення та проведення експертизи КСЗІ, зазначених у п. А.2.4, та відповідати вимогам НД ТЗІ 2.7-010-09 для визначеного у Технічному завданні на створення КСЗІ в ІТС, зазначеному в п. А.2.1.10, рівня гарантій коректності реалізації ФПБ.

Б.2.5 Вимоги щодо змісту програми проведення експертизи у частині, що стосується аналізу проектної документації КСЗІ та матеріалів, які містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ

Програма проведення експертизи КСЗІ у частині, що стосується аналізу проектної документації КСЗІ та матеріалів, які містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ, має передбачати виконання Експертом необхідних дій з метою підтвердження того, що:

Б.2.5.1 Склад проектної документації КСЗІ, зазначеної в п. А.2.2, відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу.

Б.2.5.2 Зміст проектної документації відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу.

Б.2.5.3 У проектній документації належним чином відображено порядок реалізації всіх вимог, висунутих у Технічному завданні на створення КСЗІ в ІТС, зазначеному в п. А.2.1.10.

Б.2.5.4 У проектній документації належним чином враховано особливості конкретної ІТС та умови її функціонування, визначені на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ, а також зазначені у документації, розробленій на етапі виконання передпроектних робіт, вказаній у пп. А.2.1.1-А.2.1.9.

Б.2.5.5 У складі матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ, зазначених у п. А.2.3, для всіх окремих компонентів (складових частин) КЗЗ КСЗІ, зазначених у проектній документації, наявні Експертні висновки (сертифікати) щодо відповідності вимогам чинних нормативних документів системи ТЗІ та/або КЗІ.

Б.2.5.6 Зміст матеріалів, що містять результати державної експертизи (сертифікації) всіх окремих компонентів (складових частин) КЗЗ КСЗІ, зазначених у проектній документації, підтверджує можливість використання відповідних засобів у складі КЗЗ КСЗІ.

Б.2.5.7 Визначений у проектній документації КСЗІ перелік заходів захисту, засобів їх реалізації, а також порядок функціонування відповідних засобів є дієвим та достатнім для задоволення вимог Технічного завдання на створення КСЗІ в ІТС.

Б.2.5.8 Проектна документація КСЗІ узгоджена та затверджена у порядку, передбаченому положенням чинної нормативно-правової бази в сфері ТЗІ.

Б.2.6 Вимоги щодо змісту програми проведення експертизи у частині, що стосується аналізу експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ

Програма проведення експертизи КСЗІ у частині, що стосується аналізу експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ, має передбачати виконання Експертом необхідних дій з метою підтвердження того, що:

Б.2.6.1 Склад експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ, зазначеної у п. А.2.5, відповідає визначеному у проектній документації КСЗІ, зазначеній в п. А.2.2, складу КЗЗ КСЗІ.

Б.2.6.2 Склад експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ відповідає положенням чинної нормативно-правової бази в сфері ТЗІ.

Б.2.6.3 Зміст експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ відповідає положенням чинної нормативно-правової бази в сфері ТЗІ.

Б.2.6.4 В експлуатаційній документації компонентів (складових частин) КЗЗ КСЗІ наявні відомості щодо порядку застосування відповідних компонентів (складових частин) КЗЗ КСЗІ при реалізації (з урахуванням положень проектної документації КСЗІ) всіх ФПБ (функцій захисту), визначених у Технічному завданні на створення КСЗІ в ІТС, зазначеному в п. А.2.1.10.

Б.2.7 Вимоги щодо змісту програми проведення експертизи у частині, що стосується аналізу нормативно-розпорядчої документації КСЗІ

Програма проведення експертизи КСЗІ у частині, що стосується аналізу нормативно-розпорядчої документації КСЗІ, має передбачати виконання Експертом необхідних дій з метою підтвердження того, що:

Б.2.7.1 Склад нормативно-розпорядчої документації КСЗІ, зазначеної у п. А.2.6, відповідає визначеному у проектній документації КСЗІ, зазначеній у п. А.2.2, складу КСЗІ.

Б.2.7.2 Склад нормативно-розпорядчої документації КСЗІ відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу.

Б.2.7.3 У нормативно-розпорядчій документації КСЗІ належним чином враховано положення чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу.

Б.2.7.4 У нормативно-розпорядчій документації належним чином враховано особливості функціонування компонентів (складових частин) КЗЗ КСЗІ, наведені в проектній документації КСЗІ та експлуатаційній документації, зазначеній у п. А.2.5, у процесі функціонування КСЗІ.

Б.2.7.5 У нормативно-розпорядчій документації належним чином враховано особливості реалізації організаційних, фізичних та інших заходів захисту, зазначені у проектній документації КСЗІ.

Б.2.7.6 Дотримання положень нормативно-розпорядчої документації забезпечує можливість задоволення вимог Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10, з урахуванням особливостей реалізації організаційних, фізичних та інших заходів захисту, наведених у проектній документації КСЗІ.

Б.2.7.7 Нормативно-розпорядча документація КСЗІ узгоджена та затверджена у порядку, передбаченому положенням чинної нормативно-правової бази в сфері ТЗІ.

Б.2.8 Вимоги щодо змісту програми проведення експертизи у частині, що стосується аналізу документації щодо проведених випробувань КСЗІ

Програма проведення експертизи КСЗІ у частині, що стосується аналізу документації щодо проведених випробувань КСЗІ, має передбачати виконання Експертом необхідних дій з

метою підтвердження того, що:

Б.2.8.1 Склад документації щодо проведених випробувань КСЗІ, зазначеної в п. А.2.7, відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється ІТС відповідного типу

Б.2.8.2 Зміст документації щодо проведених випробувань КСЗІ відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу.

Б.2.8.3 У документації щодо проведених випробувань КСЗІ належним чином враховано особливості функціонування компонентів (складових частин) КЗЗ КСЗІ, наведені у проектній документації КСЗІ, зазначеній у п. А.2.2, та експлуатаційній документації, зазначеній у п. А.2.5, у процесі функціонування КСЗІ.

Б.2.8.4 У документації щодо проведених випробувань КСЗІ належним чином враховано особливості реалізації організаційних, фізичних та інших заходів захисту, наведені у проектній документації КСЗІ та нормативно-розпорядчій документації КСЗІ, зазначеній у п. А.2.6.

Б.2.8.5 У документації щодо проведених випробувань КСЗІ наявні відомості стосовно результатів випробувань, які підтверджують задоволення засобами КСЗІ всіх вимог Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10.

Б.2.8.6 Документація щодо проведених випробувань КСЗІ узгоджена та затверджена у порядку, передбаченому положенням чинної нормативно-правової бази в сфері ТЗІ.

Б.2.9 Вимоги щодо змісту програми проведення експертизи у частині, що стосується аналізу організаційно-розпорядчої документації КСЗІ

Програма проведення експертизи КСЗІ у частині, що стосується аналізу організаційно-розпорядчої документації КСЗІ, має передбачати виконання Експертом необхідних дій з метою підтвердження того, що:

Б.2.9.1 Склад організаційно-розпорядчої документації КСЗІ, зазначеної у п. А.2.8, відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу.

Б.2.9.2 Зміст організаційно-розпорядчої документації КСЗІ відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу.

Б.2.9.3 В організаційно-розпорядчій документації КСЗІ належним чином враховані результати випробувань КСЗІ, наведені у документації щодо проведених випробувань КСЗІ, зазначеної в п. А.2.7.

Б.2.9.4 Організаційно-розпорядча документація КСЗІ узгоджена та затверджена у порядку, передбаченому положенням чинної нормативно-правової бази в сфері ТЗІ.

Б.2.10 Вимоги щодо змісту програми проведення експертизи у частині, що стосується перевірки фактичного використання введених до складу КЗЗ КСЗІ засобів захисту інформації

Програма проведення експертизи КСЗІ у частині, що стосується перевірки фактичного використання введених до складу КЗЗ КСЗІ засобів захисту інформації, має передбачати виконання Експертом необхідних дій з метою підтвердження того, що:

Б.2.10.1 Серед компонентів (складових частин) КЗЗ КСЗІ, розгорнутих на базі відповідних компонентів обчислювальної системи ІТС, наявні всі компоненти (складові частини) КЗЗ, визначені у проектній документації КСЗІ, зазначеній у п. А.2.2.

Б.2.10.2 Усі компоненти (складові частини) КЗЗ належним чином відображені у супровідній документації КСЗІ, зазначеній у п. А.2.9.

Б.2.10.3 Усі компоненти (складові частини) КЗЗ КСЗІ інстальовані та ініціалізовані

відповідно до положень експлуатаційної документації, зазначеної у п. А.2.5, та нормативно-розпорядчої документації КСЗІ, зазначеної у п. А.2.6.

Б.2.10.4 Фактичні параметри налаштування всіх наявних компонентів (складових частин) КЗЗ КСЗІ відповідають визначеному в експлуатаційній документації та нормативно-розпорядчої документації КСЗІ порядку застосування відповідних компонентів (складових частин) КЗЗ при реалізації (з урахуванням положень проектної документації КСЗІ) всіх ФПБ (функцій захисту), визначених у Технічному завданні на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10.

Б.2.10.5 Усі компоненти (складові частини) КЗЗ КСЗІ знаходяться у працездатному стані та функціонують належним чином.

Б.2.11 Вимоги щодо змісту програми проведення експертизи у частині, що стосується перевірки порядку використання введених до складу КЗЗ КСЗІ засобів захисту інформації

Програма проведення експертизи КСЗІ у частині, що стосується перевірки порядку використання введених до складу КЗЗ КСЗІ засобів захисту інформації, має передбачати виконання Експертом необхідних дій з метою підтвердження того, що:

Б.2.11.1 Фактично використовуваний порядок створення захищених інформаційних ресурсів, реєстрації користувачів, надання прав доступу до інформації користувачам ІТС та виконання інших завдань з адміністрування та обслуговування КСЗІ відповідає положенням експлуатаційної документації, зазначеної у п. А.2.5, та нормативно-розпорядчої документації КСЗІ, зазначеної у п. А.2.6.

Б.2.11.2 Фактично використовуваний порядок реєстрації фактів та результатів виконання певних завдань з адміністрування та обслуговування КСЗІ відповідає положенням нормативно-розпорядчої документації КСЗІ.

Б.2.11.3 Вміст наданих у складі супровідної документації КСЗІ в ІТС, зазначеної у п. А.2.9, реєстраційних журналів підтверджує факти належного застосування визначеного положеннями нормативно-розпорядчої документації КСЗІ порядку створення захищених інформаційних ресурсів, реєстрації користувачів, надання прав доступу до інформації користувачам ІТС та виконання інших завдань з адміністрування та обслуговування КСЗІ.

Б.2.11.4 Фактичні атрибути доступу користувачів, процесів та захищених інформаційних ресурсів, які містяться у відповідних сховищах компонентів (складових частин) КЗЗ КСЗІ, відповідають наведеним у реєстраційних журналах відомостям.

Б.2.12 Вимоги щодо змісту програми проведення експертизи у частині, що стосується перевірки впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту

Програма проведення експертизи КСЗІ у частині, що стосується перевірки впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших заходів захисту, має передбачати виконання Експертом необхідних дій з метою підтвердження того, що:

Б.2.12.1 У складі КСЗІ впроваджено всі організаційні, фізичні та інші нетехнічні заходи захисту, визначені у проектній документації КСЗІ, зазначеній у п. А.2.2, та нормативно-розпорядчій документації КСЗІ, зазначеній у п. А.2.6.

Б.2.12.2 Зміст наданої супровідної документації КСЗІ, зазначеної у п. А.2.9, а також журналів обліку та реєстрації сховищ і матеріальних носіїв ІзОД, зазначених в п. А.2.10, підтверджує факти належного застосування всіх впроваджених організаційних, фізичних та інших нетехнічних заходів захисту.

Б.2.13 Вимоги щодо змісту програми проведення експертизи у частині, що стосується перевірки підготовленості співробітників СЗІ, персоналу та користувачів ІТС

Програма проведення експертизи КСЗІ у частині, що стосується перевірки підготовленості співробітників СЗІ, персоналу та користувачів ІТС, повинна передбачати виконання Експертом необхідних дій з метою підтвердження того, що:

Б.2.13.1 Співробітники СЗІ, персонал та користувачі ІТС мають достатній для виконання своїх посадових та/або функціональних обов'язків рівень знань положень експлуатаційної та нормативно-розпорядчої документації КСЗІ.

Б.2.13.2 Співробітники СЗІ, персонал та користувачі ІТС мають достатній для виконання своїх посадових та/або функціональних обов'язків рівень практичних навичок щодо використання засобів ІТС та КСЗІ.

Б.2.14 Вимоги щодо змісту програми проведення експертизи у частині, що стосується перевірки результатів створення та атестації комплексу ТЗІ

Програма проведення експертизи КСЗІ у частині, що стосується перевірки результатів створення та атестації комплексу ТЗІ, має передбачати виконання Експертом необхідних дій з метою підтвердження того, що:

Б.2.14.1 Склад та характеристики створеного комплексу ТЗІ, наведені у документації щодо створення комплексу ТЗІ, розробленій на етапі виконання передпроектних робіт, зазначеній у п. А.3.1, та на етапі розроблення та впровадження заходів із захисту інформації, зазначеній у п. А.3.2, відповідають особливостям конкретної ІТС та умовам її функціонування, визначеним на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ, а також зазначеним у документації, розробленій на етапі виконання передпроектних робіт зі створення КСЗІ, зазначеній у пп. А.2.1.1-А.2.1.9.

Б.2.14.2 Відомості, наведені у документації, розробленій на етапі випробувань та атестації комплексу ТЗІ, зазначеної у п. А.3.3, підтверджують відповідність створеного комплексу ТЗІ вимогам технічного завдання та положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації від витоку технічними каналами.

Додаток В
(обов'язковий)

Вимоги щодо змісту методики проведення експертизи комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

У Додатку В викладено специфічні вимоги щодо змісту методики проведення експертизи КСЗІ в ІТС. Вимоги викладено з урахуванням положень чинної нормативно-правової бази в сфері ТЗІ, яка регламентує порядок проведення робіт зі створення та експертизи КСЗІ в ІТС, а також з урахуванням рекомендацій щодо складу та змісту проектної, експлуатаційної та нормативно-розпорядчої документації, яка надається Замовником при проведенні експертизи КСЗІ, наведених у Додатку А, та вимог щодо змісту програми проведення експертизи КСЗІ в ІТС, викладених у Додатку Б.

В.1 Вимоги щодо змісту методики проведення експертизи у частині, що стосується аналізу документації, розробленої на етапі виконання передпроектних робіт

Методика проведення експертизи КСЗІ у частині, що стосується аналізу документації, розробленої на етапі виконання передпроектних робіт, з метою забезпечення вимог програми проведення експертизи КСЗІ, розробленої з урахуванням вимог п. Б.2.1, має передбачати виконання Експертом:

В.1.1 Перевірки (з урахуванням результатів попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ) складу наданої документації, розробленої на етапі виконання передпроектних робіт, з метою формулювання висновку про те, чи наявні в її складі матеріали, зазначені у пп. 1.1.1-1.1.9 таблиці А.1 як рекомендовані для ІТС, яка являє собою АС відповідного класу, та характеристики оброблюваної інформації відповідно до встановленого законодавством правового режиму та режиму доступу, а саме:

- Перелік інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту;
- Акт (акти) категорування ІТС;
- Положення про СЗІ в ІТС;
- результати обстеження середовищ функціонування ІТС;
- Опис політики безпеки інформації в ІТС;
- Опис моделі порушника безпеки інформації в ІТС;
- Опис моделі загроз для інформації, що обробляється в ІТС;
- Звіт за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ;
- План захисту інформації в ІТС.

В.1.2 Дослідження зазначеного у п. А.2.1.1 Переліку інформації, що підлягає автоматизованому обробленню в ІТС, з метою формулювання обґрунтованого висновку про те, що:

- у Переліку інформації, що підлягає автоматизованому обробленню в ІТС, наведено перелік інформаційних ресурсів (видів інформації), що підлягають обробленню в ІТС, класифікований за рекомендованими у п. А.2.1.1.1 ознаками;
- наведений перелік інформаційних ресурсів (видів інформації), що підлягають обробленню в ІТС, відповідає відомостям щодо особливостей конкретної ІТС та умов її функціонування, одержаним на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ;
- результати класифікації інформаційних ресурсів (видів інформації), що підлягають

обробленню в ІТС, відповідають вимогам зазначених у п. А.2.1.1.1 та інших чинних нормативних документів, а також відомостям щодо особливостей конкретної ІТС та умов її функціонування, одержаним на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ.

В.1.3 Перевірки зазначеного у п. А.2.1.1 Переліку інформації, що підлягає автоматизованому обробленню в ІТС, з метою формулювання висновку про те, що він оформлений у вигляді та затверджений у порядку, зазначеному в п. А.2.1.1.2.

В.1.4 Перевірки зазначеного у п. А.2.1.2 Акта (актів) категорування ІТС з метою формулювання висновку про те, що:

- структура та зміст Акта (актів) категорування ІТС відповідають вимогам зазначених у п. А.2.1.2.1 та інших чинних нормативних документів;

- наведені в Акті (актах) категорування відомості щодо ступеня обмеження доступу (ступеня секретності) інформації, що підлягає автоматизованому обробленню в ІТС, відповідають аналогічним відомостям, наведеним у Переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, зазначеному в п. А.2.1.1;

- Акт (акти) категорування ІТС оформлений у вигляді та затверджений у порядку, зазначеному в п. А.2.1.2.3.

В.1.5 Дослідження зазначеного у п. А.2.1.3 Положення про СЗІ в ІТС з метою формулювання обґрунтованого висновку про те, що:

- структура та зміст Положення про СЗІ в ІТС відповідають рекомендаціям зазначених у п. А.2.1.3.2 та інших чинних нормативних документів;

- зміст Положення про СЗІ в ІТС (зокрема в частині, що стосується опису реалізованої інформаційної технології, переліку інформаційних ресурсів, що потребують захисту, встановленого розподілу обов'язків) відповідає відомостям щодо особливостей конкретної ІТС та умов її функціонування, одержаним на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ;

- завдання та функції співробітників (посадових осіб) СЗІ сформульовані у Положенні про СЗІ в ІТС з урахуванням вимог зазначених у п. А.2.1.3.3 та інших чинних нормативних документів;

- завдання та функції співробітників (посадових осіб) СЗІ, сформульовані у Положенні про СЗІ в ІТС, не суперечать відомостям щодо особливостей конкретної ІТС та умов її функціонування, одержаним на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ.

В.1.6 Перевірки зазначеного у п. А.2.1.3 Положення про СЗІ в ІТС з метою формулювання висновку про те, що воно оформлене у вигляді та затверджене у порядку, зазначеному в п. А.2.1.3.4.

В.1.7 Дослідження зазначених у п. А.2.1.4 результатів обстеження обчислювальної системи ІТС з метою формулювання обґрунтованого висновку про те, що:

- у результатах обстеження обчислювальної системи ІТС наведено достатньо відомостей щодо: загальної структурної схеми та складу обчислювальної системи ІТС; видів та характеристик каналів мережі передачі даних; особливостей взаємодії окремих компонентів ІТС, їх взаємного впливу один на одного; можливих обмежень щодо використання певних засобів;

- наведені результати обстеження обчислювальної системи ІТС містять мінімально необхідні відомості щодо можливостей обчислювальної системи ІТС як з погляду забезпечення функціонування загальносистемного та прикладного програмного забезпечення ІТС, так і з погляду забезпечення функціонування засобів захисту, які можуть бути реалізовані та впроваджені в процесі створення КСЗІ;

- результати обстеження обчислювальної системи ІТС не суперечать відомостям

щодо особливостей конкретної ІТС та умов її функціонування, одержаним на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ.

В.1.8 Дослідження зазначених у п. А.2.1.4 результатів обстеження інформаційного середовища з метою формулювання обґрунтованого висновку про те, що:

- у результатах обстеження інформаційного середовища наведено достатньо відомостей щодо: уточненого переліку та класифікації інформаційних ресурсів ІТС (даних та програмного забезпечення), які потребують захисту; опису технології оброблення інформації, що потребує захисту, в усіх загальносистемних та прикладних програмних засобах ІТС з наведенням компонентів обчислювальної системи ІТС, на базі яких функціонують відповідні програмні засоби, інформаційних потоків, що створюються в процесі оброблення, середовищ, через які вони передаються, джерел утворення інформаційних потоків та місць їх призначення;

- наведені у результатах обстеження інформаційного середовища уточнений перелік та класифікація інформаційних ресурсів ІТС, які потребують захисту, відповідають аналогічним відомостям, наведеним у Переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, зазначеному в п. А.2.1.1;

- результати обстеження інформаційного середовища не суперечать відомостям щодо особливостей конкретної ІТС та умов її функціонування, одержаним на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ.

В.1.9 Дослідження зазначених у п. А.2.1.4 результатів обстеження фізичного середовища з метою формулювання обґрунтованого висновку про те, що:

- у результатах обстеження фізичного середовища наведено достатньо відомостей щодо: територіального розміщення компонентів ІТС; наявності охорони території та перепускного режиму; наявності категорованих приміщень, в яких мають розміщуватися компоненти ІТС; режиму доступу до компонентів фізичного середовища ІТС; впливу чинників навколишнього середовища, захищеності від засобів технічної розвідки; наявності елементів комунікацій, систем життєзабезпечення і зв'язку, що мають вихід за межі контрольованої зони; наявності та технічних характеристик систем заземлення; умов зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації; наявності проектної та експлуатаційної документації на компоненти фізичного середовища;

- наведені у результатах обстеження фізичного середовища відомості щодо категорованих приміщень, в яких мають розміщуватися компоненти ІТС, відповідають аналогічним відомостям, наведеним в Акті (актах) за результатами відповідного категорування, зазначеному в п. А.2.1.2;

- результати обстеження фізичного середовища не суперечать відомостям щодо особливостей конкретної ІТС та умов її функціонування, одержаним на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ.

В.1.10 Дослідження зазначених у п. А.2.1.4 результатів обстеження середовища користувачів з метою формулювання обґрунтованого висновку про те, що:

- у результатах обстеження середовища користувачів наведено достатньо відомостей щодо: функціонального та кількісного складу персоналу та користувачів ІТС, їх класифікації за функціональними обов'язками та рівнем кваліфікації; повноважень користувачів ІТС різних категорій щодо доступу до інформаційних ресурсів, які обробляються в ІТС, доступу до ІТС та її окремих компонентів; рівнів можливостей різних категорій користувачів, що надаються (можуть бути наданими) їм засобами ІТС; повноважень персоналу щодо управління засобами захисту КСЗІ;

- наведені у результатах обстеження середовища користувачів відомості щодо повноважень користувачів ІТС різних категорій визначені з урахуванням відповідних вимог, наведених у Переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, зазначеному в п. А.2.1.1;

- наведені у результатах обстеження середовища користувачів відомості щодо повноважень персоналу визначені з урахуванням відповідних вимог щодо завдань та функцій співробітників (посадових осіб) СЗІ, наведених у Положенні про СЗІ в ІТС, зазначеному в п. А.2.1.3;

- результати обстеження фізичного середовища не суперечать відомостям щодо особливостей конкретної ІТС та умов її функціонування, одержаним на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ.

В.1.11 Перевірки зазначених у п. А.2.1.4 результатів обстеження середовища користувачів з метою формулювання висновку про те, що вони оформлені у вигляді та затверджені у порядку, зазначеному в п. А.2.1.4.6.

В.1.12 Дослідження зазначеного в п. А.2.1.5 Опису політики безпеки інформації в ІТС з метою формулювання обґрунтованого висновку про те, що:

- структура та зміст Опису політики безпеки інформації в ІТС відповідають рекомендаціям зазначених у п. А.2.1.5.2 та інших чинних нормативних документів;

- в Описі політики безпеки інформації в ІТС (з урахуванням рекомендацій зазначених у п. А.2.1.5.2 та інших чинних нормативних документів) з достатнім рівнем деталізації: визначено інформаційні ресурси ІТС, що потребують захисту; сформульовано основні загрози для інформації, що має різні характеристики відповідно до встановленого законодавством правового режиму та режиму доступу, компонентів обчислювальної системи, персоналу, а також вимоги щодо захисту від цих загроз; наведено політики забезпечення конфіденційності, цілісності та доступності оброблюваної інформації, а також політику забезпечення спостережності ІТС;

- в Описі політики безпеки інформації в ІТС (з урахуванням рекомендацій зазначених у п. А.2.1.5.3 та інших чинних нормативних документів) з достатнім рівнем деталізації сформульовано ПРД користувачів та процесів до інформаційних ресурсів ІТС, що потребують захисту;

- в Описі політики безпеки інформації в ІТС визначено відповідальність персоналу за виконання положень політики безпеки;

- наведені в Описі політики безпеки інформації в ІТС відомості щодо інформаційних ресурсів ІТС, які потребують захисту, основних загроз для інформації, що має різні характеристики відповідно до встановленого законодавством правового режиму та режиму доступу, компонентів обчислювальної системи, персоналу, а також вимог щодо захисту від цих загроз, політик забезпечення конфіденційності, цілісності, доступності оброблюваної інформації та спостережності ІТС, ПРД користувачів та процесів до інформаційних ресурсів ІТС, що потребують захисту, не суперечать результатам обстеження середовищ функціонування ІТС, зазначеним у п. А.2.1.4, та відомостям щодо особливостей конкретної ІТС та умов її функціонування, одержаним на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ;

- відповідальність персоналу за виконання положень політики безпеки визначено в Описі політики безпеки інформації в ІТС з урахуванням відповідних вимог щодо завдань та функцій співробітників (посадових осіб) СЗІ, наведених у Положенні про СЗІ в ІТС, зазначеному в п. А.2.1.3.

В.1.13 Перевірки зазначеного в п. А.2.1.5 Опису політики безпеки інформації в ІТС з метою формулювання висновку про те, що він оформлений у вигляді та затверджений у порядку, зазначеному в п. А.2.1.5.5.

В.1.14 Дослідження зазначеного в п. А.2.1.6 Опису моделі порушника безпеки інформації в ІТС з метою формулювання обґрунтованого висновку про те, що:

- в Описі моделі порушника безпеки інформації в ІТС наведено абстрактний формалізований або неформалізований опис дій порушника, що відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії тощо, в якому з достатнім рівнем

деталізації визначено: можливі цілі порушника та їх градація за ступенями небезпечності для ІТС та інформації, що потребує захисту; категорії персоналу, користувачів ІТС та сторонніх осіб, із числа яких може бути порушник; припущення щодо кваліфікації порушника; припущення щодо характеру його дій;

- в Описі моделі порушника безпеки інформації в ІТС (з урахуванням рекомендацій зазначених у п. А.2.1.6.2 та інших чинних нормативних документів) наведено класифікацію порушників за рівнем можливостей, які надаються їм засобами ІТС;

- Опис моделі порушника безпеки інформації в ІТС (у частині, що стосується припущень щодо кваліфікації порушника та щодо характеру його дій) викладено настільки детально, що дозволяє однозначне визначення можливості або неможливості реалізації порушником певних загроз інформації (певних атак) з використанням уразливостей певних компонентів обчислювальної системи ІТС або використовуваних програмних засобів;

- Опис моделі порушника безпеки інформації в ІТС не суперечить результатам обстеження середовищ функціонування ІТС, зазначеним у п. А.2.1.4.

В.1.15 Перевірки зазначеного в п. А.2.1.6 Опису моделі порушника безпеки інформації в ІТС з метою формулювання висновку про те, що він оформлений у вигляді та затверджений у порядку, зазначеному в п. А.2.1.6.4.

В.1.16 Перевірки зазначеного в п. А.2.1.7 Опису моделі загроз для інформації, що обробляється в ІТС, з метою формулювання висновку про те, що:

- в Описі моделі загроз для інформації, що обробляється в ІТС, наведено перелік можливих типів загроз, класифікований за результатом впливу на інформацію, тобто на порушення яких її властивостей вони спрямовані (конфіденційності, цілісності або доступності інформації);

- в Описі моделі загроз для інформації, що обробляється в ІТС, наведено класифікований за визначеними з урахуванням рекомендацій п. А.2.1.7.1 ознаками перелік можливих способів реалізації загроз певного типу (способів атак) відносно різних інформаційних об’єктів ІТС у різному стані.

В.1.17 Дослідження зазначеного в п. А.2.1.7 Опису моделі загроз для інформації, що обробляється в ІТС, з метою формулювання обґрунтованого висновку про те, що:

- в Описі моделі загроз для інформації, що обробляється в ІТС, наведено перелік можливих типів загроз, класифікований за результатом впливу на інформацію, тобто на порушення яких її властивостей вони спрямовані (конфіденційності, цілісності або доступності інформації);

- в Описі моделі загроз для інформації, що обробляється в ІТС, наведено класифікований за визначеними з урахуванням рекомендацій п. А.2.1.7.1 ознаками перелік можливих способів реалізації загроз певного типу (способів атак) відносно різних інформаційних об’єктів ІТС у різному стані;

- Опис моделі загроз для інформації, що обробляється в ІТС (у частині, що стосується переліку можливих способів реалізації загроз та їх класифікації) викладено настільки детально, що дозволяє однозначне визначення як збитків, що завдаються у випадку успішної реалізації загрози, так і ймовірності реалізації загрози (здійснення атаки) в певний спосіб;

- Опис моделі загроз для інформації, що обробляється в ІТС, не суперечить результатам обстеження середовищ функціонування ІТС, зазначеним у п. А.2.1.4;

- Опис моделі загроз для інформації, що обробляється в ІТС, не суперечить прийнятій моделі потенційного порушника політики безпеки інформації в ІТС, зазначеній у п. А.2.1.6.

В.1.18 Перевірки зазначеного в п. А.2.1.7 Опису моделі загроз для інформації, що обробляється в ІТС, з метою формулювання висновку про те, що він оформлений у вигляді та затверджений у порядку, зазначеному в п. А.2.1.7.3.

В.1.19 Перевірки зазначеного в п. А.2.1.8 Звіту за результатами проведення аналізу

ризиків та формування завдання на створення КСЗІ з метою формулювання висновку про те, що:

- Звіт за результатами проведення аналізу ризиків та формування завдання на створення КСЗІ містить формалізований або неформалізований опис результатів аналізу ризиків, пов'язаних з реалізацією загроз для інформації в ІТС;

- Звіт за результатами проведення аналізу ризиків та формування завдання на створення КСЗІ містить формулювання з урахуванням результатів виконаного аналізу ризиків, завдань на створення КСЗІ в ІТС.

В.1.20 Дослідження зазначеного в п. А.2.1.8.1 опису результатів аналізу ризиків, пов'язаних з реалізацією загроз для інформації в ІТС, з метою формулювання обґрунтованого висновку про те, що:

- в описі результатів аналізу ризиків, пов'язаних з реалізацією загроз для інформації в ІТС, з урахуванням рекомендацій зазначених у п. А.2.1.8.2 та інших чинних нормативних документів, для кожного зі способів реалізації загроз інформації, наведених в Описі моделі загроз для інформації, що обробляється в ІТС, зазначеному в п. А.2.1.7, наведено результати оцінювання ризику, пов'язаного з реалізацією певної загрози в певний спосіб, як функції ймовірності реалізації відповідної загрози у відповідний спосіб, виду та величини збитків, що завдаються у випадку успішної реалізації загрози;

- в описі результатів аналізу ризиків, пов'язаних з реалізацією загроз для інформації в ІТС, визначено неприйнятні ризики та загрози для інформації та способи їх реалізації, з якими ці ризики пов'язані.

В.1.21 Дослідження зазначених у п. А.2.1.8.2 завдань на створення КСЗІ в ІТС з метою формулювання обґрунтованого висновку про те, що:

- завдання на створення КСЗІ в ІТС сформульовано з урахуванням вимог зазначених у п. А.2.1.8.3 та інших чинних нормативних документів щодо необхідності забезпечення (в результаті створення КСЗІ) запобігання тим загрозам для інформації та способам їх реалізації, з якими пов'язані неприйнятні ризики;

- у завданнях на створення КСЗІ з достатнім рівнем деталізації визначено: завдання захисту інформації в ІТС та можливі варіанти їх вирішення; загальну структуру та склад КСЗІ; вимоги до можливих заходів, методів та засобів захисту інформації; допустимі обмеження щодо застосування певних заходів і засобів захисту; інші обмеження щодо середовищ функціонування ІТС; обмеження щодо використання ресурсів ІТС для реалізації завдань захисту; припустимі витрати на створення КСЗІ; умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів); загальні вимоги до співвідношення та меж застосування в ІТС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ;

- завдання на створення КСЗІ в ІТС сформульовано з урахуванням вимог зазначених у п. А.2.1.8.4 та інших чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу.

В.1.22 Перевірки зазначеного в п. А.2.1.8 Звіту за результатами проведення аналізу ризиків та формування завдання на створення КСЗІ з метою формулювання висновку про те, що він оформлений у вигляді та затверджений у порядку, зазначеному в п. А.2.1.8.5.

В.1.23 Дослідження зазначеного у п. А.2.1.9 Плану захисту інформації в ІТС з метою формулювання обґрунтованого висновку про те, що:

- структура та зміст Плану захисту інформації в ІТС відповідають рекомендаціям зазначених у п. А.2.1.9.2 та інших чинних нормативних документів;

- зміст Плану захисту інформації в ІТС не суперечить особливостям функціонування конкретної ІТС, а також завданням захисту, що мають вирішуватися створюваною КСЗІ,

наведеним у Переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, зазначеному в п. А.2.1.1, Положенні про СЗІ в ІТС, зазначеному в п. А.2.1.3, результатах обстеження середовищ функціонування ІТС, зазначених у п. А.2.1.4, Описі політики безпеки інформації в ІТС, зазначеному в п. А.2.1.5, Описі моделі порушника безпеки інформації в ІТС, зазначеному в п. А.2.1.6, Описі моделі загроз для інформації, що обробляється в ІТС, зазначеному в п. А.2.1.7, Звіті за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ, зазначеному в п. А.2.1.8;

- План захисту інформації в ІТС сформульовано з урахуванням вимог зазначених у п. А.2.1.9.3 та інших чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу.

В.1.24 Перевірки зазначеного в п. А.2.1.9 Плану захисту інформації в ІТС з метою формулювання висновку про те, що він оформлений у вигляді та затверджений у порядку, зазначеному в п. А.2.1.9.4.

В.2 Вимоги щодо змісту методики проведення експертизи у частині, що стосується аналізу Технічного завдання на створення КСЗІ в ІТС

Методика проведення експертизи КСЗІ у частині, що стосується аналізу Технічного завдання на створення КСЗІ в ІТС, з метою забезпечення вимог програми проведення експертизи КСЗІ, розробленої з урахуванням вимог п. Б.2.2, повинна передбачати виконання Експертом:

В.2.1 Дослідження зазначеного у п. А.2.1.10 технічного завдання на створення КСЗІ в ІТС з метою формулювання обґрунтованого висновку про те, що:

- структура та зміст Технічного завдання на створення КСЗІ в ІТС відповідають вимогам та рекомендаціям зазначених у п. А.2.1.10.2 та інших чинних нормативних документів;

- зміст Технічного завдання на створення КСЗІ в ІТС не суперечить особливостям функціонування конкретної ІТС, а також завданням захисту, що мають вирішуватися створюваною КСЗІ, наведеним у Переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, зазначеному в п. А.2.1.1, Положенні про СЗІ в ІТС, зазначеному в п. А.2.1.3, результатах обстеження середовищ функціонування ІТС, зазначених у п. А.2.1.4, Описі політики безпеки інформації в ІТС, зазначеному в п. А.2.1.5, Описі моделі порушника безпеки інформації в ІТС, зазначеному в п. А.2.1.6, Описі моделі загроз для інформації, що обробляється в ІТС, зазначеному в п. А.2.1.7, Звіті за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ, зазначеному в п. А.2.1.8, Плані захисту інформації в ІТС, зазначеному в п. А.2.1.9;

- Технічне завдання на створення КСЗІ в ІТС сформульовано з урахуванням вимог зазначених у п. А.2.1.10.3 та інших чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу;

- у Технічному завданні на створення КСЗІ в ІТС наявні вимоги, реалізація яких забезпечує вирішення всіх зазначених у п. А.2.1.8.2 завдань на створення КСЗІ в ІТС та всіх завдань захисту, визначених у Плані захисту інформації в ІТС, зазначеному в п. А.2.1.9;

- реалізація ФПБ, введених до складу наведеного у Технічному завданні на створення КСЗІ в ІТС функціонального профілю захищеності, згідно з визначеними вимогами щодо їх політик забезпечує запобігання всім загрозам для інформації та способам їх реалізації, з якими пов’язані неприйнятні ризики.

В.2.2 Перевірки зазначеного в п. А.2.1.10 Технічного завдання на створення КСЗІ в ІТС з метою формулювання висновку про те, що воно оформлене у вигляді та затверджене у порядку, зазначеному в п. А.2.1.10.4.

В.3 Вимоги щодо змісту методики проведення експертизи у частині, що стосується оцінювання ФПБ, які реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ

Методика проведення експертизи КСЗІ у частині, що стосується оцінювання ФПБ, які реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ, повинна враховувати склад та зміст зазначених у п. А.2.4 матеріалів (документів), наданих для оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ, створення та експертиза яких здійснюється в ході створення та експертизи КСЗІ, та відповідати вимогам НД ТЗІ 2.7-009-09 для визначеного у Технічному завданні на створення КСЗІ в ІТС, зазначеному в п. А.2.1.10, рівня гарантій коректності реалізації ФПБ.

В.4 Вимоги щодо змісту методики проведення експертизи у частині, що стосується оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ

Методика проведення експертизи КСЗІ у частині, що стосується рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ, повинна враховувати склад та зміст зазначених у п. А.2.4 матеріалів (документів), наданих для оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ, створення та експертиза яких здійснюється в ході створення та експертизи КСЗІ, та відповідати вимогам НД ТЗІ 2.7-010-09 для визначеного у Технічному завданні на створення КСЗІ в ІТС, зазначеному в п. А.2.1.10, рівня гарантій коректності реалізації ФПБ.

В.5 Вимоги щодо змісту методики проведення експертизи у частині, що стосується аналізу проектної документації КСЗІ та матеріалів, які містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ

Методика проведення експертизи КСЗІ у частині, що стосується аналізу проектної документації КСЗІ та матеріалів, які містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ, з метою забезпечення вимог програми проведення експертизи КСЗІ, розробленої з урахуванням вимог п. Б.2.5, повинна передбачати виконання Експертом:

В.5.1 Перевірки складу наданої проектної документації та матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ, з метою формулювання висновку про те, чи наявні в їх складі матеріали, зазначені у пп. 1.2.1-1.2.3, 1.3.1, 1.3.2 таблиці А.1 як рекомендовані для ІТС, що являє собою АС відповідного класу, та характеристик оброблюваної інформації відповідно до встановленого законодавством правового режиму та режиму доступу, а саме:

- документація ескізного проекту КСЗІ в ІТС (у випадку виконання відповідного етапу робіт);
- документація технічного проекту КСЗІ в ІТС;
- документація робочого проекту КСЗІ в ІТС;
- Експертні висновки щодо відповідності використовуваних у складі КЗЗ КСЗІ засобів захисту інформації вимогам чинних нормативних документів системи ТЗІ (за наявності відповідних засобів у складі КЗЗ КСЗІ);
- Експертні висновки або сертифікати щодо відповідності використовуваних у складі КЗЗ КСЗІ засобів КЗІ вимогам чинних нормативних документів системи КЗІ (за наявності відповідних засобів у складі КЗЗ КСЗІ).

В.5.2 Дослідження зазначеної у п. А.2.2.1 документації ескізного проекту КСЗІ в ІТС з метою формулювання обґрунтованого висновку про те, що:

- склад та зміст документації ескізного проекту КСЗІ в ІТС відповідають вимогам та рекомендаціям зазначених у пп. А.2.2.1.1, А.2.2.1.2 та інших чинних нормативних документів;

- у документації ескізного проекту КСЗІ в ІТС з достатнім рівнем деталізації наведені відомості щодо попередніх проектних рішень, які визначають порядок реалізації всіх вимог Технічного завдання на створення КСЗІ в ІТС, зазначеного у п. А.2.1.10, як щодо КСЗІ в цілому, так і за необхідності - щодо її окремих складових частин;

- зміст документації ескізного проекту КСЗІ в ІТС не суперечить особливостям функціонування конкретної ІТС, а також завданням захисту, що мають вирішуватися створюваною КСЗІ, наведеним у Переліку інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту, зазначеному в п. А.2.1.1, Положенні про СЗІ в ІТС, зазначеному в п. А.2.1.3, результатах обстеження середовищ функціонування ІТС, зазначених у п. А.2.1.4, Описі політики безпеки інформації в ІТС, зазначеному в п. А.2.1.5, Описі моделі порушника безпеки інформації в ІТС, зазначеному в п. А.2.1.6, Описі моделі загроз для інформації, що обробляється в ІТС, зазначеному в п. А.2.1.7, Звіті за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ, зазначеному в п. А.2.1.8, Плані захисту інформації в ІТС, зазначеному в п. А.2.1.9.

В.5.3 Перевірки зазначеної у п. А.2.2.1 документації ескізного проекту КСЗІ в ІТС з метою формулювання висновку про те, що вона оформлена у вигляді та затверджена у порядку, зазначеному в п. А.2.2.1.3.

В.5.4 Дослідження зазначеної у п. А.2.2.2 документації технічного проекту КСЗІ в ІТС з метою формулювання обґрунтованого висновку про те, що:

- склад та зміст документації ескізного проекту КСЗІ в ІТС відповідають вимогам та рекомендаціям зазначених у пп. А.2.2.2.1, А.2.2.2.2 та інших чинних нормативних документів;

- у документації технічного проекту КСЗІ в ІТС в достатньому для виконання етапу робочого (технорobочого) проектування (реалізації) КСЗІ обсязі наведено відомості щодо: загальних проектних рішень, достатніх (з урахуванням результатів ескізного проектування, зазначених у п. А.2.2.1) для забезпечення реалізації вимог Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10; рішень стосовно структури КСЗІ (організаційної структури, структури технічних і програмних засобів); рішень стосовно архітектури та складу КЗЗ КСЗІ; рішень стосовно механізмів реалізації ФПБ, визначених у наведеному в Технічному завданні на створення КСЗІ в ІТС функціональному профілі захищеності; рішень стосовно алгоритмів, порядку та умов функціонування засобів захисту інформації, які використовуються у складі КЗЗ КСЗІ для реалізації певних ФПБ.

В.5.5 Перевірки зазначеної у п. А.2.2.2 документації технічного проекту КСЗІ в ІТС з метою формулювання висновку про те, що вона оформлена у вигляді та затверджена у порядку, зазначеному в п. А.2.2.2.3.

В.5.6 Перевірки зазначених у п. А.2.3.1, а також одержаних за результатами виконання зазначених у пп. В.3, В.4 методик, матеріалів (Експертних висновків) щодо відповідності використовуваних у складі КЗЗ КСЗІ засобів захисту інформації вимогам чинних нормативних документів системи ТЗІ з метою формулювання висновку про те, що відповідні матеріали (Експертні висновки) наявні для всіх засобів захисту інформації (у тому числі засобів антивірусного захисту, засобів попередження та виявлення мережевих вторгнень тощо), які визначені у документації технічного проекту КСЗІ, зазначеній у п. А.2.2.2, як складові частини КЗЗ КСЗІ.

В.5.7 Перевірки зазначених у п. А.2.3.2 матеріалів (Експертних висновків або сертифікатів) щодо відповідності використовуваних у складі КЗЗ КСЗІ засобів КЗІ вимогам чинних нормативних документів системи КЗІ з метою формулювання висновку про те, що відповідні матеріали (Експертні висновки або сертифікати) наявні для всіх засобів КЗІ, які

визначені у документації технічного проекту КСЗІ, зазначеній у п. А.2.2.2, як складові частини КЗЗ КСЗІ.

В.5.8 Дослідження зазначених у пп. А.2.3.1, А.2.3.2, а також одержаних за результатами виконання зазначених у пп. В.3, В.4 методик, матеріалів (Експертних висновків або сертифікатів) щодо відповідності використовуваних у складі КЗЗ КСЗІ засобів захисту інформації та засобів КЗІ вимогам чинних нормативних документів системи ТЗІ або системи КЗІ разом із зазначеними в п. А.2.3.1.3 матеріалами, які деталізують політику ФПБ (функції захисту), що реалізуються певним засобом захисту інформації, а також порядку та особливостей реалізації відповідних ФПБ (функцій захисту) з метою формулювання обґрунтованого висновку про те, що:

- всі засоби захисту інформації та засоби КЗІ, визначені у документації технічного проекту КСЗІ, зазначеній у п. А.2.2.2, як складові КЗЗ КСЗІ, придатні для реалізації у повному обсязі вимог Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10, у частині, що стосується реалізації політики відповідних ФПБ (відповідних функцій захисту);

- визначений у документації технічного проекту КСЗІ, зазначеній у п. А.2.2.2, порядок функціонування засобів захисту та засобів КЗІ, що введені до складу КЗЗ КСЗІ, при реалізації відповідних ФПБ (функцій захисту) забезпечує реалізацію у повному обсязі вимог Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10, у частині, що стосується реалізації політики всіх ФПБ, визначених у наведеному в Технічному завданні на створення КСЗІ в ІТС функціональному профілі захищеності.

В.5.9 Дослідження зазначеної у п. А.2.2.3 документації робочого проекту КСЗІ в ІТС з метою формулювання обґрунтованого висновку про те, що:

- склад та зміст документації робочого проекту КСЗІ в ІТС відповідають вимогам та рекомендаціям зазначених у пп. А.2.2.3.1, А.2.2.3.2 та інших чинних нормативних документів;

- у документації робочого проекту КСЗІ в ІТС в достатньому для виконання етапу робочого (технороботочого) проектування (реалізації) КСЗІ обсязі наведено відомості щодо: детальних рішень з реалізації технічного проекту КСЗІ; забезпечення управління КСЗІ і взаємодії її компонентів; проведення пусконалагоджувальних робіт та тестування підсистем та засобів КСЗІ.

В.5.10 Перевірки зазначеної у п. А.2.2.3 документації робочого проекту КСЗІ в ІТС з метою формулювання висновку про те, що вона оформлена у вигляді та затверджена у порядку, зазначеному в п. А.2.2.3.3.

В.6 Вимоги щодо змісту методики проведення експертизи у частині, що стосується аналізу експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ

Методика проведення експертизи КСЗІ у частині, що стосується аналізу експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ, з метою забезпечення вимог програми проведення експертизи КСЗІ, розробленої з урахуванням вимог п. Б.2.6, повинна передбачати виконання Експертом:

В.6.1 Перевірки (з урахуванням результатів виконання зазначених у п. В.5 методик) складу наданої експлуатаційної документації, зазначеної у п. А.2.5, з метою формулювання висновку про те, чи наявні в її складі документи, що визначають порядок інсталяції, ініціалізації, налаштування та експлуатації всіх без винятку компонентів (складових частин) КЗЗ КСЗІ, визначених у зазначеній у п. А.2.2.2 документації технічного проекту КСЗІ в ІТС.

В.6.2 Дослідження вмісту наданої експлуатаційної документації, зазначеної у п. А.2.5, з метою формулювання обґрунтованого висновку про те, що:

- для кожного компонента (складової частини) КЗЗ КСЗІ у вигляді окремих документів або розділів інших документів надано: опис процедур безпечної інсталяції,

генерації та запуску; опис послуг безпеки, що реалізуються відповідним компонентом; настанову адміністратору з послуг безпеки; настанову користувачу з послуг безпеки;

- для кожного компонента (складової частини) КЗЗ КСЗІ зміст наданих документів відповідає вимогам та рекомендаціям зазначених у пп. А.2.5.2, А.2.5.3 та інших чинних нормативних документів;

- у наданій експлуатаційній документації компонентів (складових частин) КЗЗ КСЗІ наявні відомості щодо порядку застосування відповідних компонентів (складових частин) КЗЗ КСЗІ при реалізації (з урахуванням положень проектної документації КСЗІ, зазначеної у п. А.2.2) всіх ФПБ (функцій захисту), визначених у Технічному завданні на створення КСЗІ в ІТС, зазначеному в п. А.2.1.10.

В.7 Вимоги щодо змісту методики проведення експертизи у частині, що стосується аналізу нормативно-розпорядчої документації КСЗІ

Методика проведення експертизи КСЗІ у частині, що стосується аналізу нормативно-розпорядчої документації КСЗІ, з метою забезпечення вимог програми проведення експертизи КСЗІ, розробленої з урахуванням вимог п. Б.2.7, повинна передбачати виконання Експертом:

В.7.1 Перевірки складу наданої нормативно-розпорядчої документації з метою формулювання висновку про те, чи наявні в її складі документи, зазначені у пп. 1.6.1 - 1.6.5 таблиці А.1 як рекомендовані для ІТС, яка являє собою АС відповідного класу, та характеристик оброблюваної інформації відповідно до встановленого законодавством правового режиму та режиму доступу, а саме:

- інструкції щодо забезпечення правил оброблення ІзОД в ІТС;

- посадові (функціональні) інструкції співробітників СЗІ, персоналу та користувачів ІТС;

- технологічні (операційні) інструкції (настанови) щодо виконання завдань з адміністрування та обслуговування КСЗІ;

- інструкції про порядок використання засобів КЗІ.

В.7.2 Перевірки складу наданої нормативно-розпорядчої документації з метою формулювання висновку про те, чи відповідає її склад визначеному у зазначеній у п. А.2.2 проектній документації КСЗІ складу.

В.7.3 Дослідження змісту наданих інструкцій щодо забезпечення правил оброблення ІзОД в ІТС, зазначених у п. А.2.6.1, з метою формулювання обґрунтованого висновку про те, що:

- склад та зміст інструкцій щодо забезпечення правил оброблення ІзОД в ІТС відповідають вимогам зазначених у п. А.2.6.1.2 та інших чинних нормативних документів;

- в інструкціях щодо забезпечення правил оброблення ІзОД в ІТС з достатнім рівнем деталізації окреслено перелік заходів, спрямованих на дотримання визначеного вимогами чинної нормативно-правової бази режиму доступу до ІзОД, визначено порядок дій персоналу та користувачів ІТС з метою реалізації зазначених заходів, а також встановлено їх відповідальність у випадку порушення зазначених вимог;

- в інструкціях щодо забезпечення правил оброблення ІзОД в ІТС наведено: загальні відомості щодо організації захисту ІзОД в ІТС; опис порядку доступу до приміщень, в яких розташовано засоби обчислювальної системи ІТС; опис порядку захисту інформації від витоку технічними каналами; опис порядку захисту інформації від НСД; опис порядку здійснення антивірусного захисту; опис порядку впровадження і використання програмного забезпечення; опис порядку створення захищених інформаційних ресурсів, реєстрації користувачів та надання прав доступу до інформації користувачам ІТС; опис порядку контролю за дотриманням користувачами правил роботи із засобами ІТС; опис порядку обліку, зберігання, обігу, резервування, ротації та знищення матеріальних носіїв, що

використовуються для зберігання ІзОД; опис порядку проведення ремонтних робіт та відновлення працездатності ІТС; опис порядку контролю за забезпеченням захисту ІзОД в ІТС; обов'язки користувачів та персоналу ІТС стосовно дотримання встановленого порядку оброблення ІзОД; відповідальність користувачів та персоналу ІТС за порушення встановленого порядку оброблення ІзОД;

- в інструкціях щодо забезпечення правил оброблення ІзОД в ІТС враховано: вимоги щодо використання зазначених у п. А.2.10 журналів обліку та реєстрації сховищ та матеріальних носіїв ІзОД, а також визначено порядок та особливості використання відповідних журналів; положення зазначених у п. А.2.6.2 посадових (функціональних) інструкцій співробітників СЗІ, персоналу та користувачів ІТС; положення зазначених у п. А.2.6.3 технологічних (операційних) інструкцій (настанов) щодо виконання завдань з адміністрування та обслуговування КСЗІ.

В.7.4 Перевірки зазначених у п. А.2.6.1 інструкцій щодо забезпечення правил оброблення ІзОД в ІТС з метою формулювання висновку про те, що вони затверджені у порядку, зазначеному в п. А.2.6.1.4.

В.7.5 Дослідження вмісту наданих посадових (функціональних) інструкцій співробітників СЗІ, персоналу та користувачів ІТС, зазначених у п. А.2.6.2, з метою формулювання обґрунтованого висновку про те, що:

- склад та зміст посадових (функціональних) інструкцій співробітників СЗІ, персоналу та користувачів ІТС враховують: структуру та штатний розклад СЗІ, завдання, функції та повноваження співробітників (посадових осіб) СЗІ, визначені у зазначеному в п. А.2.1.3 Положенні про СЗІ в ІТС; категорії персоналу та користувачів ІТС, визначені у зазначеному в п. А.2.1.5 Описі політики безпеки інформації в ІТС; вимоги зазначеного в п.А.2.1.10 Технічного завдання на створення КСЗІ в ІТС щодо розподілу обов'язків користувачів та їх функціональних завдань; порядок дій співробітників (посадових осіб) СЗІ, персоналу та користувачів ІТС, який випливає з положень зазначеного в п. А.2.1.5 Опису політики безпеки інформації в ІТС, зазначеної у п. А.2.1.2 документації технічного проекту КСЗІ в ІТС, зазначеної у п. А.2.1.3 документації робочого проекту КСЗІ в ІТС та зазначеної у п. А.2.5 експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ щодо забезпечення визначеного порядку функціонування ІТС та КСЗІ;

- у посадових (функціональних) інструкціях співробітників СЗІ, персоналу та користувачів ІТС наведено: загальні положення, в яких визначено категорії співробітників СЗІ, персоналу або користувачів ІТС, на яких поширюються вимоги відповідних інструкцій; основні завдання та функції (функціональні завдання), що мають виконуватися співробітниками СЗІ, персоналом або користувачами ІТС, на яких поширюються вимоги відповідних інструкцій; опис правил та порядку дій співробітників СЗІ, персоналу або користувачів ІТС в процесі виконання функціональних завдань; повноваження, обов'язки та відповідальність осіб, на яких поширюються вимоги відповідних інструкцій;

- у посадових (функціональних) інструкціях співробітників СЗІ, персоналу та користувачів ІТС враховано положення зазначених у п. А.2.6.3 технологічних (операційних) інструкцій (настанов) щодо виконання завдань з адміністрування та обслуговування КСЗІ.

В.7.6 Перевірки зазначених у п. А.2.6.2 посадових (функціональних) інструкцій співробітників СЗІ, персоналу та користувачів ІТС з метою формулювання висновку про те, що вони затверджені у порядку, зазначеному в п. А.2.6.2.5.

В.7.7 Дослідження вмісту наданих технологічних (операційних) інструкцій (настанов) щодо виконання завдань з адміністрування та обслуговування КСЗІ, зазначених у п. А.2.6.3, з метою формулювання обґрунтованого висновку про те, що:

- склад та зміст технологічних (операційних) інструкцій (настанов) щодо виконання завдань з адміністрування та обслуговування КСЗІ враховують: структуру та штатний розклад СЗІ, завдання, функції та повноваження співробітників (посадових осіб) СЗІ,

визначені у зазначеному в п. А.2.1.3 Положенні про СЗІ в ІТС; категорії персоналу та користувачів ІТС, визначені у зазначеному в п. А.2.1.5 Описі політики безпеки інформації в ІТС; вимоги зазначеного в п. А.2.1.10 Технічного завдання на створення КСЗІ в ІТС щодо розподілу обов'язків користувачів та їх функціональних завдань; порядок дій співробітників (посадових осіб) СЗІ, персоналу та користувачів ІТС, який випливає з положень зазначеного в п. А.2.1.5 Опису політики безпеки інформації в ІТС, зазначеної у п. А.2.1.2 документації технічного проекту КСЗІ в ІТС, зазначеної у п. А.2.1.3 документації робочого проекту КСЗІ в ІТС та зазначеної у п. А.2.5 експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ щодо забезпечення визначеного порядку функціонування ІТС та КСЗІ;

- у технологічних (операційних) інструкціях (настановах) щодо виконання завдань з адміністрування та обслуговування КСЗІ наведено: загальні положення, в яких визначено завдання з адміністрування та обслуговування КСЗІ, порядок виконання яких встановлюється інструкцією, категорії співробітників СЗІ або персоналу ІТС, на яких поширюються вимоги відповідних інструкцій та які є відповідальними за виконання відповідних завдань; опис послідовності, правил та порядку здійснення технологічних операцій в ході виконання відповідальними особами певних завдань з адміністрування та обслуговування КСЗІ; опис порядку реєстрації фактів та результатів виконання певних завдань у відповідних реєстраційних журналах; форми використовуваних реєстраційних журналів;

- у технологічних (операційних) інструкціях (настановах) враховано положення зазначених у п. А.2.6.2 посадових (функціональних) інструкцій співробітників СЗІ та персоналу ІТС.

В.7.8 Перевірки зазначених у п. А.2.6.3 технологічних (операційних) інструкцій (настанов) щодо виконання завдань з адміністрування та обслуговування КСЗІ з метою формулювання висновку про те, що вони затверджені у порядку, зазначеному в п. А.2.6.3.5.

В.7.9 Дослідження змісту наданих інструкцій про порядок використання засобів КЗІ, зазначених у п. А.2.6.4, з метою формулювання обґрунтованого висновку про те, що їх склад та зміст відповідають вимогам зазначених у п. А.2.6.4.1 та інших чинних нормативних документів.

В.7.10 Перевірки зазначених у п. А.2.6.4 інструкцій про порядок використання засобів КЗІ з метою формулювання висновку про те, що вони затверджені у порядку, зазначеному в п. А.2.6.4.2.

В.8 Вимоги щодо змісту методики проведення експертизи у частині, що стосується аналізу документації щодо проведених випробувань КСЗІ

Методика проведення експертизи КСЗІ у частині, що стосується аналізу документації щодо проведених випробувань КСЗІ, з метою забезпечення вимог програми експертизи КСЗІ, розробленої з урахуванням вимог п. Б.2.8, повинна передбачати виконання Експертом:

В.8.1 Перевірки складу наданої документації щодо проведених випробувань КСЗІ з метою формулювання висновку про те, чи наявні в її складі матеріали, зазначені у п. А.2.7.1, а саме:

- Програма та методика випробувань КСЗІ в ІТС;
- Протокол (протоколи) попередніх випробувань КСЗІ в ІТС.

В.8.2 Дослідження зазначеної у п. А.2.7.1 Програми та методики випробувань КСЗІ в ІТС з метою формулювання обґрунтованого висновку про те, що:

- зміст Програми та методики випробувань КСЗІ в ІТС відповідає вимогам та рекомендаціям зазначених у п. А.2.7.2 та інших чинних нормативних документів;

- у Програмі та методиці випробувань КСЗІ в ІТС наведено перелік перевірок та опис методів (методик) виконання окремих перевірок, успішне проведення яких дозволяє дійти однозначного висновку щодо відповідності створеної КСЗІ вимогам зазначеного в п. А.2.1.10

Технічного завдання на створення КСЗІ в ІТС.

В.8.3 Перевірки зазначеної у п. А.2.7.1 Програми та методики випробувань КСЗІ в ІТС з метою формулювання висновку про те, що вона узгоджена та затверджена у порядку, зазначеному в п. А.2.7.3.

В.8.4 Перевірки зазначеного у п. А.2.7.1 Протоколу (протоколів) попередніх випробувань КСЗІ в ІТС з метою формулювання висновку про те, що:

- зміст Протоколу (протоколів) попередніх випробувань КСЗІ в ІТС відповідає вимогам та рекомендаціям зазначених у п. А.2.7.5 та інших чинних нормативних документів;

- у Протоколі (протоколах) попередніх випробувань КСЗІ в ІТС наведено: задокументовані результати випробувань, передбачених зазначеною в п. А.2.7.1 програмою та методикою випробувань КСЗІ в ІТС; перелік виявлених недоліків, необхідних заходів щодо їх усунення, рекомендовані терміни виконання цих робіт; висновки щодо можливості прийняття КСЗІ в дослідну експлуатацію.

В.8.5 Перевірки зазначеного у п. А.2.7.1 Протоколу (протоколів) попередніх випробувань КСЗІ в ІТС з метою формулювання висновку про те, що він затверджений у порядку, зазначеному в п. А.2.7.5.

В.9 Вимоги щодо змісту методики проведення експертизи у частині, що стосується аналізу організаційно-розпорядчої документації КСЗІ

Методика проведення експертизи КСЗІ у частині, що стосується аналізу організаційно-розпорядчої документації КСЗІ, з метою забезпечення вимог програми проведення експертизи КСЗІ, розробленої з урахуванням вимог п. Б.2.9, повинна передбачати виконання Експертом:

В.9.1 Перевірки складу наданої організаційно-розпорядчої документації КСЗІ з метою формулювання висновку про те, чи наявні в її складі матеріали, зазначені у п. А.2.8.1, а саме:

- Акт про приймання КСЗІ в ІТС у дослідну експлуатацію;
- Акт завершення дослідної експлуатації КСЗІ в ІТС;
- Акт завершення робіт зі створення КСЗІ в ІТС.

В.9.2 Перевірки зазначеного у п. А.2.8.1 Акта про приймання КСЗІ в ІТС у дослідну експлуатацію з метою формулювання висновку про те, що:

- зміст Акта про приймання КСЗІ в ІТС у дослідну експлуатацію відповідає вимогам та рекомендаціям зазначених у п. А.2.8.2 та інших чинних нормативних документів;

- в Акті про приймання КСЗІ в ІТС у дослідну експлуатацію наведено: задокументовані у зазначеному у п. А.2.7.1 Протоколі (протоколах) попередніх випробувань КСЗІ в ІТС відомості щодо результатів випробувань, виявлених недоліків та необхідних заходів стосовно їх усунення; висновки щодо можливості прийняття КСЗІ в дослідну експлуатацію.

В.9.3 Перевірки зазначеного у п. А.2.8.1 Акта про приймання КСЗІ в ІТС у дослідну експлуатацію з метою формулювання висновку про те, що він затверджений у порядку, зазначеному в п. А.2.8.3.

В.9.4 Перевірки зазначеного у п. А.2.8.1 Акта завершення дослідної експлуатації КСЗІ в ІТС з метою формулювання висновку про те, що в ньому відображено результати дослідної експлуатації та наведено висновки щодо можливості (неможливості) подання КСЗІ на державну експертизу.

В.9.5 Перевірки зазначеного у п. А.2.8.1 Акта завершення дослідної експлуатації КСЗІ в ІТС з метою формулювання висновку про те, що він затверджений у порядку, зазначеному в п. А.2.8.5.

В.9.6 Перевірки зазначеного у п. А.2.8.1 Акта завершення робіт зі створення КСЗІ в ІТС з метою формулювання висновку про те, що його зміст відповідає вимогам та рекомендаціям

зазначених у п. А.2.8.6 та інших чинних нормативних документів.

В.9.7 Перевірки зазначеного у п. А.2.8.1 Акта завершення робіт зі створення КСЗІ в ІТС з метою формулювання висновку про те, що він затверджений у порядку, зазначеному в п. А.2.8.7.

В.10 Вимоги щодо змісту методики проведення експертизи у частині, що стосується перевірки фактичного використання введених до складу КЗЗ КСЗІ засобів захисту інформації

Методика проведення експертизи КСЗІ у частині, що стосується перевірки фактичного використання введених до складу КЗЗ КСЗІ засобів захисту інформації, з метою забезпечення вимог програми проведення експертизи КСЗІ, розробленої з урахуванням вимог п. Б.2.10, повинна передбачати виконання Експертом:

В.10.1 Перевірки складу наданої супровідної документації КСЗІ з метою формулювання висновку про те, чи наявний у її складі зазначений у п. А.2.9.1 Формуляр ІТС.

В.10.2 Перевірки зазначеного в п. А.2.9.1 Формуляра ІТС з метою формулювання висновку про те, що:

- форма та зміст Формуляра ІТС відповідають вимогам та рекомендаціям зазначених у п. А.2.9.2 та інших чинних нормативних документів;
- усі визначені у зазначеній у п. А.2.2 проектній документації КСЗІ, зокрема у зазначеній у п. А.2.2.2 документації технічного проекту КСЗІ в ІТС, компоненти (складові частини) КЗЗ КСЗІ належним чином відображені в формулярі ІТС.

В.10.3 Перевірки наявності серед розгорнутих на базі відповідних компонентів обчислювальної системи ІТС компонентів (складових частин) КЗЗ КСЗІ всіх складових частин КЗЗ, визначених у зазначеній у п. А.2.2 проектній документації КСЗІ, зокрема у зазначеній у п. А.2.2.2 документації технічного проекту КСЗІ в ІТС.

В.10.4 Перевірки значень параметрів налаштування всіх розгорнутих на базі відповідних компонентів обчислювальної системи ІТС компонентів (складових частин) КЗЗ КСЗІ з метою формулювання висновку про те, що вони інстальовані та ініціалізовані відповідно до положень зазначеної у п. А.2.5 експлуатаційної документації та зазначеної у п. А.2.6 нормативно-розпорядчої документації КСЗІ.

В.10.5 Дослідження (з урахуванням положень зазначеної у п. А.2.2 проектної документації КСЗІ, зокрема положень зазначеної у п. А.2.2.2 документації технічного проекту КСЗІ в ІТС) положень зазначеної у п. А.2.5 експлуатаційної документації та положень зазначеної у п. А.2.6 нормативно-розпорядчої документації КСЗІ, значень параметрів налаштування всіх розгорнутих на базі відповідних компонентів обчислювальної системи ІТС компонентів (складових частин) КЗЗ КСЗІ з метою формулювання обґрунтованого висновку про те, що вони відповідають визначеному порядку застосування відповідних компонентів (складових частин) КЗЗ при реалізації всіх ФПБ (функцій захисту), визначених у зазначеному в п. А.2.1.10 Технічному завданні на створення КСЗІ в ІТС.

В.10.6 Перевірки (з урахуванням положень зазначеної у п. А.2.5 експлуатаційної документації) працездатності всіх розгорнутих на базі відповідних компонентів обчислювальної системи ІТС компонентів (складових частин) КЗЗ КСЗІ з метою формулювання висновку про те, що вони знаходяться у працездатному стані та функціонують належним чином.

В.11 Вимоги щодо змісту методики проведення експертизи у частині, що стосується перевірки порядку використання введених до складу КЗЗ КСЗІ засобів захисту інформації

Методика проведення експертизи КСЗІ у частині, що стосується перевірки порядку використання введених до складу КЗЗ КСЗІ засобів захисту інформації, з метою

забезпечення вимог програми проведення експертизи КСЗІ, розробленої з урахуванням вимог п. Б.2.11, повинна передбачати виконання Експертом:

В.11.1 Перевірки складу наданої супровідної документації КСЗІ з метою формулювання висновку про те, чи наявні в її складі зазначені у п. А.2.9.1 реєстраційні журнали, що використовуються для реєстрації фактів та результатів виконання певних завдань з адміністрування та обслуговування КСЗІ.

В.11.2 Перевірки зазначених у п. А.2.9.1 реєстраційних журналів з метою формулювання висновку про те, що їх перелік та форми відповідають визначеним у зазначених у п. А.2.6.3 технологічних (операційних) інструкціях (настановах) щодо виконання завдань з адміністрування та обслуговування КСЗІ переліку та формам.

В.11.3 Вибіркової перевірки фактично використовуваного порядку створення захищених інформаційних ресурсів, реєстрації користувачів, надання прав доступу до інформації користувачам ІТС та виконання інших завдань з адміністрування та обслуговування КСЗІ з метою формулювання висновку про те, що він відповідає положенням зазначеної у п. А.2.5 експлуатаційної документації та зазначеної у п. А.2.6 нормативно-розпорядчої документації КСЗІ.

В.11.4 Вибіркової перевірки фактично використовуваного порядку реєстрації фактів та результатів виконання певних завдань з адміністрування та обслуговування КСЗІ з метою формулювання висновку про те, що він відповідає положенням зазначеної у п. А.2.6 нормативно-розпорядчої документації КСЗІ.

В.11.5 Перевірки зазначених у п. А.2.9.1 реєстраційних журналів з метою формулювання висновку про те, що їх уміст підтверджує факти належного застосування визначеного положеннями зазначеної у п. А.2.6 нормативно-розпорядчої документації КСЗІ порядку створення захищених інформаційних ресурсів, реєстрації користувачів, надання прав доступу до інформації користувачам ІТС та виконання інших завдань з адміністрування та обслуговування КСЗІ.

В.11.6 Вибіркової перевірки фактично призначених атрибутів доступу користувачів, процесів та захищених інформаційних ресурсів, які містяться у відповідних сховищах компонентів (складових частин) КЗЗ КСЗІ, з метою формулювання висновку про те, що їх значення відповідають наведеним у відповідних реєстраційних журналах відомостям.

В.12 Вимоги щодо змісту методики проведення експертизи у частині, що стосується перевірки впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту

Методика проведення експертизи КСЗІ у частині, що стосується перевірки впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших заходів захисту, з метою забезпечення вимог програми проведення експертизи КСЗІ, розробленої з урахуванням вимог п. Б.2.12, повинна передбачати виконання Експертом:

В.12.1 Перевірки факту впровадження всіх організаційних, фізичних та інших нетехнічних заходів захисту, визначених у зазначеній у п. А.2.2 проектній документації КСЗІ та зазначеній у п. А.2.6 нормативно-розпорядчій документації КСЗІ, з метою формулювання висновку про те, що всі зазначені заходи захисту впроваджено.

В.12.2 Дослідження обсягу впровадження всіх організаційних, фізичних та інших нетехнічних заходів захисту, визначених у зазначеній у п. А.2.2 проектній документації КСЗІ та зазначеній у п. А.2.6 нормативно-розпорядчій документації КСЗІ, з метою формулювання обґрунтованого висновку про те, що всі зазначені заходи захисту впроваджено в повному обсязі.

В.12.3 Перевірки (у відповідних випадках) складу наданих журналів обліку та реєстрації сховищ та матеріальних носіїв ІзОД з метою формулювання висновку про те, що перелік і форми відповідних журналів відповідають вимогам зазначених у пп. А.2.10.2,

А.2.10.3 та інших чинних нормативних документів.

В.12.4 Перевірки зазначених у п. А.2.9.1 реєстраційних журналів та (у відповідних випадках) зазначених у пп. А.2.10.1, А.2.10.2 журналів обліку та реєстрації сховищ і матеріальних носіїв ІзОД з метою формулювання висновку про те, що їх уміст підтверджує факти належного застосування всіх організаційних, фізичних та інших нетехнічних заходів захисту, визначених у зазначеній у п. А.2.6 нормативно-розпорядчій документації КСЗІ.

В.13 Вимоги щодо змісту методики проведення експертизи у частині, що стосується перевірки підготовленості співробітників СЗІ, персоналу та користувачів ІТС

Методика проведення експертизи КСЗІ у частині, що стосується перевірки підготовленості співробітників СЗІ, персоналу та користувачів ІТС, з метою забезпечення вимог програми проведення експертизи КСЗІ, розробленої з урахуванням вимог п. Б.2.13, повинна передбачати виконання Експертом:

В.13.1 Вибіркової перевірки рівня знань співробітниками СЗІ, персоналом та користувачами ІТС положень зазначеної у п. А.2.5 експлуатаційної документації та зазначеної у п. А.2.6 нормативно-розпорядчої документації КСЗІ (у частині, що їх безпосередньо стосується) з метою формулювання висновку про те, що співробітники СЗІ, персонал та користувачі ІТС мають достатній для виконання своїх посадових та/або функціональних обов’язків рівень знань положень відповідної документації.

В.13.2 Вибіркової перевірки практичних навичок співробітників СЗІ, персоналу та користувачів ІТС щодо виконання положень зазначеної у п. А.2.5 експлуатаційної документації та зазначеної у п. А.2.6 нормативно-розпорядчої документації КСЗІ (у частині, що їх безпосередньо стосується) з метою формулювання висновку про те, що співробітники СЗІ, персонал та користувачі ІТС мають достатній для виконання своїх посадових та/або функціональних обов’язків рівень практичних навичок щодо використання засобів ІТС та КСЗІ.

В.14 Вимоги щодо змісту методики проведення експертизи у частині, що стосується перевірки результатів створення та атестації комплексу ТЗІ

Методика проведення експертизи КСЗІ у частині, що стосується перевірки результатів створення та атестації комплексу ТЗІ, з метою забезпечення вимог програми проведення експертизи КСЗІ, розробленої з урахуванням вимог п. Б.2.14, повинна передбачати виконання Експертом:

В.14.1 Дослідження змісту зазначеної у пп. А.3.1, А.3.2 документації щодо створення комплексу ТЗІ, розробленої на етапі виконання передпроектних робіт та на етапі розроблення та впровадження заходів із захисту інформації, з метою формулювання обґрунтованого висновку про те, що склад та характеристики створеного комплексу ТЗІ відповідають особливостям конкретної ІТС та умовам її функціонування, визначеним на етапах попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ, а також наведеним у документації, розробленій на етапі виконання передпроектних робіт зі створення КСЗІ, зазначеної у пп. А.2.1.1 - А.2.1.9.

В.14.2 Перевірки змісту зазначеної у п. А.3.3 документації щодо створення комплексу ТЗІ, розробленої на етапі випробувань та атестації комплексу ТЗІ, з метою формулювання обґрунтованого висновку про те, що наведені в ній відомості підтверджують відповідність створеного комплексу ТЗІ вимогам технічного завдання та положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації від витоку технічними каналами.

Додаток Г
(рекомендований)

Рекомендації щодо викладення змістовної частини протоколу експертизи засобу технічного захисту інформації від несанкціонованого доступу

У Додатку Г викладено рекомендації щодо змістовної частини протоколу експертизи ЗТЗІ від НСД. Рекомендації викладено з урахуванням вимог Положення про державну експертизу в сфері технічного захисту інформації та методичних вказівок щодо документування результатів оцінювання ФПБ та рівнів гарантій коректності реалізації ФПБ у ЗТЗІ від НСД, наведених у НД ТЗІ 2.7-009-09 та НД ТЗІ 2.7-010-09. У п. Г.1 наведено рекомендації щодо змісту протоколу експертизи, а у п. Г.2 – рекомендації щодо змістовної частини окремих розділів протоколу експертизи.

Г.1 Рекомендації щодо змісту протоколу експертизи засобу технічного захисту інформації від НСД

Г.1.1 Відповідно до вимог Положення про державну експертизу в сфері технічного захисту інформації, у протоколі експертизи ЗТЗІ від НСД повинні бути викладені:

- зміст окремої методики (пункту) експертизи ОЕ;
- перелік документів та специфікації програмних і технічних засобів, наданих Замовником експертизи для виконання робіт;
- результати робіт щодо окремої методики (пункту) експертизи ОЕ;
- висновок щодо відповідності ОЕ вимогам нормативних документів системи ТЗІ в обсязі функцій, зазначених у паспорті засобу технічного захисту інформації;
- особливі думки Експертів.

Г.1.2 З урахуванням вимог Положення про державну експертизу в сфері технічного захисту інформації, положень ДСТУ 2851-94, РД 50-34.698-90 та інших чинних стандартів та нормативних документів у сфері інформаційних технологій та захисту інформації, що стосуються документування результатів випробувань, рекомендується вводити до складу протоколу експертизи такі розділи:

- об’єкт експертизи;
- характеристика експертизи;
- методи виконання експертних робіт;
- засоби виконання експертних робіт;
- організація експертних робіт;
- результати експертних робіт;
- висновки за результатами експертних робіт;
- додатки до протоколу.

Г.1.3 Залежно від особливостей ОЕ можливе об’єднання, додавання, вилучення певних розділів або зміна їх назв.

Г.1.4 Відповідно до вимог Положення про державну експертизу в сфері технічного захисту інформації, протокол експертизи має бути підписаний усіма Експертами, що брали участь у виконанні відповідних експертних робіт, та затверджений керівником Організатора експертизи.

Г.2 Рекомендації щодо змістовної частини окремих розділів протоколу експертизи засобу технічного захисту інформації від НСД

Г.2.1 Рекомендації щодо змістовної частини розділу "Об'єкт експертизи"

Г.2.1.1 У розділі "Об'єкт експертизи" повинні бути наведені такі відомості:

- повна та скорочена назви ОЕ;
- виробник (Розробник) ОЕ;
- призначення та стисла характеристика ОЕ;
- опис комплекту поставки (опис конфігурації) ОЕ, наданого на експертизу.

Г.2.1.2 Повна та скорочена назви ОЕ мають бути наведені відповідно до положень паспорта на ОЕ, інших відомостей, зазначених у заявці на проведення експертизи, та не суперечити положенням технічного завдання та іншої зазначеної у п. А.1 Додатка А до НД ТЗІ 2.7-010-09 документації, що надається для оцінювання рівня гарантій коректності реалізації ФПБ.

Г.2.1.3 Відомості щодо виробника (Розробника) ОЕ (назва організації (підприємства, установи), її місцезнаходження) мають бути наведені відповідно до відомостей, зазначених у заявці на проведення експертизи, рішенні уповноваженого державного органу та договорі між Замовником та Організатором експертизи на виконання відповідних робіт.

Г.2.1.4 Призначення та стисла характеристика ОЕ мають бути наведені в обсязі, достатньому для чіткого розуміння можливостей та особливостей ОЕ щодо вирішення певних завдань захисту інформації, що обробляється в ІТС. Зокрема, мають бути наведені:

- визначення проблем (цілей) забезпечення безпеки інформації, вирішення яких покладається на ОЕ;
- визначення завдань захисту, вирішення яких забезпечується ОЕ;
- високорівневе визначення переліку та політики ФПБ, заявлених Розробником як таких, що призначені для вирішення певних завдань захисту;
- стислий опис вимог до апаратного середовища функціонування ОЕ та існуючих обмежень на використовувані в ньому апаратні засоби;
- стислий опис вимог до програмного середовища функціонування ОЕ та існуючих обмежень на використовувані в ньому програмні засоби.

При формулюванні відповідних відомостей рекомендується скористатися змістом опису послуг безпеки, що реалізуються КЗЗ оцінюваного ОЕ, зазначеного у п. А.2.15 Додатка А до НД ТЗІ 2.7-010-09, або іншого аналогічного документа, в якому містяться відповідні відомості, наданого для оцінювання рівня гарантій коректності реалізації ФПБ.

Г.2.1.5 Опис комплекту поставки (опис конфігурації) ОЕ, наданого для експертизи, повинен містити:

- перелік програмних компонентів, що входять до складу інсталяційного пакета ОЕ (для ОЕ, що являє собою програмний або програмно-апаратний засіб) та надаються для проведення експертизи;
- перелік апаратних компонентів, що входять до складу ОЕ (для ОЕ, що являє собою програмно-апаратний або апаратний засіб) та надаються для проведення експертизи;
- повний перелік матеріалів (документів), визначений з урахуванням рекомендацій п. А.1 Додатка А до НД ТЗІ 2.7-010-09 та наданий Замовником експертизи (Розробником ОЕ) Експертам для проведення відповідних експертних робіт.

Для всіх компонентів ОЕ та матеріалів (документів), зазначених в описі комплекту поставки (описі конфігурації) ОЕ, мають бути наведені їх ідентифікатори, які відповідають положенням зазначеної у п. А.2.12 Додатка А до НД ТЗІ 2.7-010-09 документації системи керування конфігурацією ОЕ, що використовується Розробником ОЕ.

Г.2.2 Рекомендації щодо змістовної частини розділу "Характеристика експертизи"

Г.2.2.1 У розділі "Характеристика експертизи" мають бути наведені такі відомості щодо проведення запротокольованих експертних робіт:

- вид, мета експертизи та підстави проведення;
- Замовник та Організатор експертизи;
- перелік використаної нормативно-технічної документації;
- обсяг експертних робіт;
- перелік оцінюваних характеристик ОЕ та вимоги до них.

Г.2.2.2 Вид (первинна, додаткова або контрольна), мета та підстави проведення експертизи мають бути наведені відповідно до відомостей, зазначених у заявці на проведення експертизи, рішенні уповноваженого державного органу та договорі між Замовником та Організатором експертизи на виконання відповідних робіт.

Г.2.2.3 Відомості щодо Замовника та Організатора експертизи (назва організації (підприємства, установи), її місцезнаходження) мають бути наведені відповідно до відомостей, зазначених у заявці на проведення експертизи, рішенні уповноваженого державного органу та договорі між Замовником та Організатором експертизи на виконання відповідних робіт.

Г.2.2.4 У переліку використаної нормативно-технічної документації повинні бути наведені всі чинні нормативно-технічні документи, вимоги та положення яких використовувалися в ході проведення експертизи.

Г.2.2.5 Обсяг експертних робіт повинен бути визначений, відомості щодо нього повинні наводитися з урахуванням виду та мети експертизи, а також тієї частини загального обсягу експертних робіт, відомості стосовно яких відображаються в протоколі. У випадку проведення первинної експертизи загальний обсяг експертних робіт повинен передбачати, як мінімум оцінювання, відповідно до вимог НД ТЗІ 2.5-007-99 та положень НД ТЗІ 2.7-009-09 та НД ТЗІ 2.7-010-09, переліку та рівнів ФПБ, які реалізуються ОЕ, а також рівня гарантій коректності реалізації відповідних ФПБ. Якщо в ході експертизи передбачається оцінювання відповідності ОЕ вимогам інших чинних нормативних документів, які визначають вимоги щодо забезпечення захисту інформації в ІТС певного типу (НД ТЗІ 2.5-007-2007, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 тощо), або будь-яким іншим вимогам, відповідні відомості також мають бути наведені. Допустимим є наведення відомостей щодо обсягу експертних робіт шляхом посилання на узгоджену та затверджену в установленому порядку Програму проведення експертизи або її окремі пункти.

Г.2.2.6 У переліку оцінюваних характеристик ОЕ та вимогах до них мають бути зазначені всі характеристики ОЕ, перевірки відповідності яких певним вимогам були здійснені в ході проведення запротокольованих експертних робіт. Допустимим є наведення відомостей щодо оцінюваних характеристик ОЕ та вимог до них шляхом посилання на документи, в яких визначаються відповідні вимоги, наприклад, на розроблені відповідно до положень НД ТЗІ 2.7-009-09 технічні вимоги, що містять вимоги до ФПБ та опис порядку їх реалізації.

Г.2.3 Рекомендації щодо змістовної частини розділу "Методи виконання експертних робіт"

У розділі "Методи виконання експертних робіт" повинні бути наведені відомості щодо використовуваних у ході проведення запротокольованих експертних робіт методів виконання певних випробувань та перевірок. Зазначені відомості можуть бути наведені або шляхом цитування відповідних фрагментів узгодженої та затвердженої в установленому порядку Методики проведення експертизи (її окремих пунктів), або шляхом посилання на них.

Г.2.4 Рекомендації щодо змістовної частини розділу "Засоби виконання експертних робіт"

У розділі "Засоби виконання експертних робіт" повинні бути наведені відомості щодо використовуваних у ході проведення запротокольованих експертних робіт конкретних видів матеріально-технічного забезпечення відповідних робіт – технічних, програмних та допоміжних засобів випробувань. Має бути детально охарактеризовано середовище проведення відповідних випробувань, зокрема наведено характеристики використовуваних ПЕОМ та іншого обладнання, конфігурацію обчислювальної системи випробувального полігона, типи та версії використовуваних операційних систем, загальносистемного, спеціалізованого та прикладного програмного забезпечення тощо.

Г.2.5 Рекомендації щодо змістовної частини розділу "Організація експертних робіт"

У розділі "Організація експертних робіт" мають бути наведені такі відомості щодо проведення запротокольованих експертних робіт:

- період проведення експертних робіт;
- місце проведення експертних робіт;
- послідовність проведення експертних робіт;
- розподіл функцій між виконавцями експертних робіт.

Г.2.6 Рекомендації щодо змістовної частини розділу "Результати експертних робіт"

Г.2.6.1 У розділі "Результати експертних робіт" має бути наведено відомості щодо результатів виконання відповідних експертних робіт, наприклад:

- результати випробувань ФПБ;
- результати виконання перевірок на відповідність вимогам щодо рівня гарантій;
- результати виконання додаткових перевірок.

Г.2.6.2 У результатах випробувань засобів реалізації ФПБ мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) результати виконаних перевірок засобів реалізації певних ФПБ. Відповідно до положень НД ТЗІ 2.7-009-09 мають бути наведені підстави, які дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних перевірок та (з урахуванням цих висновків) щодо підтвердження або не підтвердження фактів реалізації в оцінюваному ОЕ певних ФПБ та їх рівнів.

Г.2.6.3 У результатах виконання перевірок на відповідність вимогам щодо рівня гарантій мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) результати проведених перевірок на відповідність вимогам щодо певних аспектів рівня гарантій (архітектури, середовища розробки, послідовності розробки, середовища функціонування, документації та випробувань ОЕ). Відповідно до положень НД ТЗІ 2.7-010-09 мають бути наведені:

- результати виконання відповідних дій щодо оцінювання згідно з пунктами розділу "Методи виконання експертних робіт" або пунктами Методики проведення експертизи;
- підстави, що дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних дій з оцінювання гарантій;
- висновки щодо підтвердження або не підтвердження фактів дотримання при розробленні, виробництві та постачанні Замовнику вимог заявленого (уточненого) рівня гарантій коректності реалізації ФПБ в оцінюваному ОЕ (у частині, що стосується відповідного аспекту рівня гарантій).

Г.2.6.4 У результатах виконання додаткових перевірок мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) результати виконаних додаткових перевірок.

Г.2.7 Рекомендації щодо змістовної частини розділу "Висновки за результатами експертних робіт"

Г.2.7.1 У розділі "Висновки за результатами експертних робіт" мають бути наведені висновки щодо результатів виконання відповідних експертних робіт:

- висновки за результатами випробувань ФПБ;
- висновки за результатами виконання перевірок на відповідність вимогам щодо рівня гарантій;
- висновки за результатам виконання перевірок додаткових вимог.

Крім цього, у розділі "Висновки за результатами експертних робіт" мають бути наведені (за наявності) особливі думки Експертів.

Г.2.7.2 У відповідних висновках (з посиланням на пункти розділу "Результати експертних робіт") мають бути наведені однозначні та обґрунтовані твердження щодо відповідності або невідповідності ОЕ висунутим вимогам у частині реалізації певних ФПБ, рівня гарантій коректності реалізації ФПБ та додаткових вимог.

Г.2.8 Рекомендації щодо змістовної частини додатків до протоколу експертизи засобу технічного захисту інформації від НСД

У додатках до протоколу експертизи ЗТЗІ від НСД рекомендується наводити відомості (свідоцтва), які одержані в ході виконання експертних робіт та слугують об’єктивному підтвердженню їх результатів (вміст каталогів файлової системи після інсталяції програмних засобів ОЕ; зразки екранних форм, одержані в ході виконання перевірок; вміст журналів реєстрації подій; одержані звіти про призначені атрибути доступу тощо).

Додаток Д
(рекомендований)

Рекомендації щодо викладення змістовної частини протоколу експертизи комплексної системи захисту інформації

У Додатку Д викладено рекомендації щодо змістовної частини протоколу експертизи КСЗІ. Рекомендації викладено з урахуванням вимог Положення про державну експертизу в сфері технічного захисту інформації, методичних вказівок з документування результатів оцінювання ФПБ та рівнів гарантій коректності реалізації ФПБ у ЗТЗІ від НСД, наведених у НД ТЗІ 2.7-009-09 та НД ТЗІ 2.7-010-09, а також вимог щодо змісту методики проведення експертизи КСЗІ в ІТС, наведених у Додатку В. У п. Д.1 наведено рекомендації щодо змісту протоколу експертизи, а у п. Д.2 – рекомендації щодо змістовної частини окремих розділів протоколу експертизи.

Д.1 Рекомендації щодо змісту протоколу експертизи КСЗІ

Д.1.1 Відповідно до вимог Положення про державну експертизу в сфері технічного захисту інформації у протоколі експертизи КСЗІ в ІТС мають бути викладені:

- зміст (пункту) окремої методики експертизи ОЕ;
- перелік документів та специфікації програмних і технічних засобів, наданих Замовником експертизи для виконання робіт;
- результати робіт щодо (пункту) окремої методики експертизи ОЕ;
- висновок щодо відповідності об'єкта експертизи вимогам нормативних документів системи ТЗІ в обсязі функцій, зазначених у Технічному завданні на створення КСЗІ в ІТС;
- особливі думки Експертів.

Д.1.2 З урахуванням вимог Положення про державну експертизу в сфері технічного захисту інформації, положень ДСТУ 2851-94, РД 50-34.698-90 та інших чинних стандартів та нормативних документів у сфері інформаційних технологій та захисту інформації, що стосуються документування результатів випробувань, рекомендується до складу протоколу експертизи вводити такі розділи:

- об’єкт експертизи;
- характеристика експертизи;
- методи виконання експертних робіт;
- засоби виконання експертних робіт;
- організація експертних робіт;
- результати експертних робіт;
- висновки за результатами експертних робіт;
- додатки до протоколу.

Д.1.3 Залежно від особливостей ОЕ можливо об’єднання, додавання, вилучення певних розділів або зміна їх назв.

Д.1.4 Відповідно до вимог Положення про державну експертизу в сфері технічного захисту інформації протокол експертизи має бути підписаний усіма Експертами, що брали участь у виконанні відповідних експертних робіт, та затверджений керівником Організатора експертизи.

Д.2 Рекомендації щодо змістовної частини окремих розділів протоколу експертизи КСЗІ

Д.2.1 Рекомендації щодо змістовної частини розділу "Об'єкт експертизи"

Д.2.1.1 У розділі "Об'єкт експертизи" мають бути наведені такі відомості:

- повна та скорочена назви ОЕ;
- призначення та стисла характеристика ОЕ;
- опис конфігурації ОЕ та опис комплекту документації, наданих для експертизи.

Д.2.1.2 Повна та скорочена назви ОЕ мають бути наведені відповідно до відомостей, зазначених у заявці на проведення експертизи, та не суперечити положенням Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10.

Д.2.1.3 Призначення і стисла характеристика ОЕ мають бути наведені в обсязі, достатньому для чіткого розуміння можливостей та особливостей ОЕ щодо вирішення певних завдань захисту інформації, що обробляється в ІТС. Зокрема, мають бути наведені:

- стисла характеристика обчислювальної системи ІТС;
- стисла характеристика інформаційного середовища ІТС;
- стисла характеристика фізичного середовища ІТС;
- стисла характеристика середовища користувачів ІТС;
- перелік завдань захисту, вирішення яких забезпечується КСЗІ;
- відомості щодо структури та складу КСЗІ, а також щодо переліку технічних, організаційних, фізичних та інших заходів захисту, які у сукупності складають КСЗІ;
- функціональні специфікації КЗЗ КСЗІ та рівень гарантій коректності реалізації ФПБ.

При формулюванні відповідних відомостей рекомендується скористатися змістом результатів обстеження середовищ функціонування ІТС, зазначених у п. А.2.1.4, Звіту за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ, зазначеного в п. А.2.1.8, Плану захисту інформації в ІТС, зазначеного в п. А.2.1.9, Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10.

Д.2.1.4 Опис конфігурації ОЕ та опис комплекту документації, що надані для експертизу, повинні містити:

- перелік апаратних компонентів, що входять до складу обчислювальної системи ІТС;
- перелік програмних компонентів ІТС;
- перелік апаратних, програмно-апаратних та програмних компонентів (складових частин), що входять до складу КЗЗ КСЗІ;
- перелік засобів захисту, що входять до складу комплексу ТЗІ;
- повний перелік матеріалів (документів), визначений з урахуванням рекомендацій Додатка А та наданий Замовником експертизи Експертам для проведення відповідних експертних робіт.

При формулюванні відповідних відомостей щодо опису конфігурації ОЕ рекомендується скористатися вмістом Формуляра ІТС, зазначеного у п. А.2.9.1, а також вмістом Паспорта на комплекс ТЗІ, зазначеного у п. А.3.3.1.

Якщо в ході експертизи КСЗІ здійснювалося оцінювання ФПБ та рівнів гарантій їх реалізації в окремих компонентах (складових частинах) КЗЗ КСЗІ, для відповідних компонентів та матеріалів (документів), зазначених в описі комплекту поставки (описі конфігурації), повинні бути наведені їх ідентифікатори, які відповідають положенням зазначеної у п. А.12 Додатка А до НД ТЗІ 2.7-010-09 документації використовуваної Розробником компонента (складової частини) КЗЗ КСЗІ системи керування конфігурацією.

Д.2.2 Рекомендації щодо змістовної частини розділу "Характеристика експертизи"

Д.2.2.1 У розділі "Характеристика експертизи" повинні бути наведені такі відомості щодо проведення запротокольованих експертних робіт:

- вид, мета експертизи та підстави проведення;
- Замовник та Організатор експертизи;
- перелік використаної нормативно-технічної документації;
- обсяг експертних робіт;
- перелік оцінюваних характеристик ОЕ та вимоги до них.

Д.2.2.2 Вид (первинна, додаткова або контрольна), мета та підстави проведення експертизи мають бути наведені відповідно до відомостей, зазначених у заявці на проведення експертизи, рішенні уповноваженого державного органу та договорі між Замовником та Організатором експертизи на виконання відповідних робіт.

Д.2.2.3 Відомості щодо Замовника та Організатора експертизи (назва організації (підприємства, установи) її місцезнаходження) мають бути наведені відповідно до відомостей, зазначених у заявці на проведення експертизи, рішенні уповноваженого державного органу та договорі між Замовником та Організатором експертизи на виконання відповідних робіт.

Д.2.2.4 У переліку використаної нормативно-технічної документації мають бути наведені всі чинні нормативно-технічні документи, вимоги та положення яких використовувалися в ході проведення експертизи.

Д.2.2.5 Обсяг експертних робіт повинен бути визначений та відомості щодо нього повинні наводитися з урахуванням виду та мети експертизи, а також тієї частини загального обсягу експертних робіт, відомості стосовно яких вказуються в протоколі. У випадку проведення первинної експертизи загальний обсяг експертних робіт має передбачати, як мінімум, виконання всіх робіт, передбачених розробленою відповідно до вимог Додатка Б програмою проведення експертизи КСЗІ в ІТС. Допустимим є наведення відомостей щодо обсягу експертних робіт шляхом посилання на узгоджену та затверджену в установленому порядку Програму проведення експертизи або її окремі пункти.

Д.2.2.6 У переліку оцінюваних характеристик ОЕ та вимогах до них мають бути зазначені всі характеристики ОЕ, перевірки відповідності яких певним вимогам були здійснені в ході проведення запротокольованих експертних робіт. Допустимим є наведення відомостей щодо оцінюваних характеристик ОЕ та вимог до них шляхом посилання на документи, в яких визначаються відповідні вимоги, зокрема на зазначене в п. А.2.1.10 Технічне завдання на створення КСЗІ в ІТС.

Д.2.3 Рекомендації щодо змістовної частини розділу "Методи виконання експертних робіт"

У розділі "Методи виконання експертних робіт" мають бути наведені відомості щодо використовуваних у ході проведення запротокольованих експертних робіт методів виконання певних випробувань та перевірок. Зазначені відомості можуть бути наведені або шляхом цитування відповідних фрагментів узгодженої та затвердженої в установленому порядку Методики проведення експертизи (її окремих пунктів), або шляхом посилання на них.

Д.2.4 Рекомендації щодо змістовної частини розділу "Засоби виконання експертних робіт"

У розділі "Засоби виконання експертних робіт" мають бути наведені відомості щодо використовуваних у ході проведення запротокольованих експертних робіт конкретних видів матеріально-технічного забезпечення відповідних робіт – технічних, програмних та допоміжних засобів випробувань.

Д.2.5 Рекомендації щодо змістовної частини розділу "Організація експертних робіт"

У розділі "Організація експертних робіт" мають бути наведені такі відомості щодо проведення запротокольованих експертних робіт:

- період проведення експертних робіт;
- місце проведення експертних робіт;
- послідовність проведення експертних робіт;
- розподіл функцій між виконавцями експертних робіт.

Д.2.6 Рекомендації щодо змістовної частини розділу "Результати експертних робіт"

Д.2.6.1 У розділі "Результати експертних робіт" мають бути наведені відомості щодо результатів виконання певних експертних робіт, наприклад, щодо:

- аналізу документації, розробленої на етапі виконання передпроектних робіт;
- аналізу Технічного завдання на створення КСЗІ в ІТС;
- оцінювання (за необхідності) ФПБ, що реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ;
- оцінювання (за необхідності) рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ;
- аналізу проектної документації КСЗІ та матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ;
- аналізу експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ;
- аналізу нормативно-розпорядчої документації КСЗІ;
- аналізу документації щодо проведених випробувань КСЗІ;
- аналізу організаційно-розпорядчої документації КСЗІ;
- перевірки фактичного використання введених до складу КЗЗ КСЗІ засобів захисту інформації;
- перевірки порядку використання введених до складу КЗЗ КСЗІ засобів захисту інформації;
- перевірки впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту;
- перевірки підготовленості співробітників СЗІ, персоналу та користувачів ІТС;
- перевірки (за необхідності) результатів створення та атестації комплексу ТЗІ.

Д.2.6.2 У результатах аналізу документації, розробленої на етапі виконання передпроектних робіт, повинні бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) сформульовані з урахуванням вимог п. В.1 результати виконання відповідних перевірок. Мають бути наведені підстави, які дозволяють або не дозволять дійти висновку щодо успішності або неуспішності здійснення певних перевірок та (з урахуванням цих висновків) щодо підтвердження або не підтвердження того, що:

- склад документації, розробленої на етапі виконання передпроектних робіт, відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу;
- зміст документації, розробленої на етапі виконання передпроектних робіт, відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу;
- зміст документації, розробленої на етапі виконання передпроектних робіт, відповідає особливостям конкретної ІТС та умовам її функціонування, визначеним на етапі попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ;

- документація, розроблена на етапі виконання передпроектних робіт, узгоджена та затверджена у порядку, передбаченому положенням чинної нормативно-правової бази в сфері ТЗІ.

Д.2.6.3 У результатах аналізу Технічного завдання на створення КСЗІ в ІТС мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) сформульовані з урахуванням вимог п. В.2 результати виконання відповідних перевірок. Мають бути наведені підстави, які дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних перевірок та (з урахуванням цих висновків) щодо підтвердження або не підтвердження того, що:

- у Технічному завданні на створення КСЗІ в ІТС у повному обсязі та коректно враховані положення чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу;

- у Технічному завданні на створення КСЗІ в ІТС у повному обсязі та коректно враховані особливості конкретної ІТС та умови її функціонування, визначені на етапі попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ, а також зазначені у документації, розробленій на етапі виконання передпроектних робіт;

- реалізація визначеного у Технічному завданні на створення КСЗІ в ІТС переліку вимог є достатньою для забезпечення надійного захисту інформації, що обробляється у відповідній ІТС;

- Технічне завдання на створення КСЗІ в ІТС узгоджено та затверджено у порядку, передбаченому положеннями чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу.

Д.2.6.4 У результатах оцінювання ФПБ, що реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ, мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) результати виконаних перевірок засобів реалізації певних ФПБ. Відповідно до положень НД ТЗІ 2.7-009-09 мають бути наведені підстави, які дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних перевірок та (з урахуванням цих висновків) щодо підтвердження або не підтвердження фактів реалізації в оцінюваному ОЕ певних ФПБ та їх рівнів.

Д.2.6.5 У результатах оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) результати проведених перевірок на відповідність вимогам щодо певних аспектів рівня гарантій (архітектури, середовища розробки, послідовності розробки, середовища функціонування, документації та випробувань ОЕ). Відповідно до положень НД ТЗІ 2.7-010-09 мають бути наведені:

- результати виконання відповідних дій щодо оцінювання згідно з пунктами розділу "Методи виконання експертних робіт" або пунктами методики;

- підстави, які дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних дій з оцінювання гарантій;

- висновки щодо підтвердження або не підтвердження фактів дотримання при розробленні, виробництві та постачанні Замовнику вимог заявленого (уточненого) рівня гарантій коректності реалізації ФПБ в оцінюваному ОЕ (у частині, що стосується відповідного аспекту рівня гарантій).

Д.2.6.6 У результатах аналізу проектної документації КСЗІ та матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ, мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) сформульовані з

урахуванням вимог п. В.5 результати виконання відповідних перевірок. Мають бути наведені підстави, які дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних перевірок та (з урахуванням цих висновків) щодо підтвердження або не підтвердження того, що:

- склад проектної документації КСЗІ відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу;
- вміст проектної документації відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу;
- у проектній документації належним чином відображено порядок реалізації всіх вимог, висунутих у Технічному завданні на створення КСЗІ в ІТС;
- у проектній документації належним чином враховано особливості конкретної ІТС та умови її функціонування, визначені на етапі попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ, а також зазначені у документації, розробленій на етапі виконання передпроектних робіт;
- у складі матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ, для всіх окремих компонентів (складових частин) КЗЗ КСЗІ, зазначених у проектній документації, наявні експертні висновки (сертифікати) щодо відповідності вимогам чинних нормативних документів у сфері ТЗІ та КЗІ;
- зміст матеріалів, що містять результати державної експертизи (сертифікації) всіх окремих компонентів (складових частин) КЗЗ КСЗІ, зазначених у проектній документації, підтверджує можливість використання відповідних засобів у складі КЗЗ КСЗІ;
- визначений у проектній документації КСЗІ перелік заходів захисту, засобів їх реалізації, а також порядок функціонування відповідних засобів є дієвим та достатнім для задоволення вимог Технічного завдання на створення КСЗІ в ІТС;
- проектна документація КСЗІ узгоджена та затверджена у порядку, передбаченому положенням чинної нормативно-правової бази в сфері ТЗІ.

Д.2.6.7 У результатах аналізу експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) сформульовані з урахуванням вимог п. В.6 результати виконання відповідних перевірок. Мають бути наведені підстави, які дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних перевірок та (з урахуванням цих висновків) щодо підтвердження або не підтвердження того, що:

- склад експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ відповідає визначеному у проектній документації КСЗІ складу КЗЗ КСЗІ;
- склад експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ відповідає положенням чинної нормативно-правової бази в сфері ТЗІ;
- зміст експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ відповідає положенням чинної нормативно-правової бази в сфері ТЗІ;
- в експлуатаційній документації компонентів (складових частин) КЗЗ КСЗІ наявні відомості щодо порядку застосування відповідних компонентів (складових частин) КЗЗ КСЗІ при реалізації (з урахуванням положень проектної документації КСЗІ) всіх ФПБ (функцій захисту), визначених у Технічному завданні на створення КСЗІ в ІТС.

Д.2.6.8 У результатах аналізу нормативно-розпорядчої документації КСЗІ мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) сформульовані з урахуванням вимог п. В.7

результати виконання відповідних перевірок. Мають бути наведені підстави, які дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних перевірок та (з урахуванням цих висновків) щодо підтвердження або не підтвердження того, що:

- склад нормативно-розпорядчої документації КСЗІ відповідає визначеному у проектній документації КСЗІ;

- склад нормативно-розпорядчої документації КСЗІ відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу;

- у нормативно-розпорядчій документації КСЗІ належним чином враховано положення чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу;

- у нормативно-розпорядчій документації належним чином враховано особливості функціонування компонентів (складових частин) КЗЗ КСЗІ, зазначені у проектній документації КСЗІ та експлуатаційній документації, в процесі функціонування КСЗІ;

- у нормативно-розпорядчій документації належним чином враховано особливості реалізації організаційних, фізичних та інших заходів захисту, зазначені у проектній документації КСЗІ;

- дотримання положень нормативно-розпорядчої документації забезпечує можливість задоволення вимог Технічного завдання на створення КСЗІ в ІТС з урахуванням особливостей реалізації організаційних, фізичних та інших заходів захисту, зазначених у проектній документації КСЗІ;

- нормативно-розпорядча документація КСЗІ узгоджена та затверджена у порядку, передбаченому положенням чинної нормативно-правової бази в сфері ТЗІ.

Д.2.6.9 У результатах аналізу документації щодо проведених випробувань КСЗІ мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) сформульовані з урахуванням вимог п. В.8 результати виконання відповідних перевірок. Мають бути наведені підстави, які дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних перевірок та (з урахуванням цих висновків) щодо підтвердження або не підтвердження того, що:

- склад документації щодо проведених випробувань КСЗІ відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу;

- зміст документації щодо проведених випробувань КСЗІ відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу;

- у документації щодо проведених випробувань КСЗІ належним чином враховано особливості функціонування компонентів (складових частин) КЗЗ КСЗІ, зазначені у проектній документації КСЗІ та експлуатаційній документації, в процесі функціонування КСЗІ;

- у документації щодо проведених випробувань КСЗІ належним чином враховано особливості реалізації організаційних, фізичних та інших заходів захисту, зазначені у проектній документації КСЗІ та нормативно-розпорядчій документації КСЗІ;

- у документації щодо проведених випробувань КСЗІ наявні відомості щодо результатів випробувань, які підтверджують задоволення засобами КСЗІ всіх вимог Технічного завдання на створення КСЗІ в ІТС;

- документація щодо проведених випробувань КСЗІ узгоджена та затверджена у порядку, передбаченому положенням чинної нормативно-правової бази в сфері ТЗІ.

Д.2.6.10 У результатах аналізу організаційно-розпорядчої документації КСЗІ мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) сформульовані з урахуванням вимог п. В.9 результати виконання відповідних перевірок. Мають бути наведені підстави, які дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних перевірок та (з урахуванням цих висновків) щодо підтвердження або не підтвердження того, що:

- склад організаційно-розпорядчої документації КСЗІ відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу;
- зміст організаційно-розпорядчої документації КСЗІ відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу;
- в організаційно-розпорядчій документації КСЗІ належним чином враховано результати випробувань КСЗІ, наведені у документації щодо проведених випробувань КСЗІ;
- організаційно-розпорядча документація КСЗІ узгоджена та затверджена у порядку, передбаченому положенням чинної нормативно-правової бази в сфері ТЗІ.

Д.2.6.11 У результатах перевірки фактичного використання введених до складу КЗЗ КСЗІ засобів захисту інформації мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) сформульовані з урахуванням вимог п. В.10 результати виконання відповідних перевірок. Мають бути наведені підстави, які дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних перевірок та (з урахуванням цих висновків) щодо підтвердження або не підтвердження того, що:

- серед компонентів (складових частин) КЗЗ КСЗІ, розгорнутих на базі відповідних компонентів обчислювальної системи ІТС, наявні всі компоненти (складові частини) КЗЗ, визначені у проектній документації КСЗІ;
- усі компоненти (складові частини) КЗЗ належним чином зазначені у супровідній документації КСЗІ;
- усі компоненти (складові частини) КЗЗ КСЗІ інстальовані та ініціалізовані відповідно до положень експлуатаційної документації та нормативно-розпорядчої документації КСЗІ;
- фактичні параметри налаштування всіх наявних компонентів (складові частини) КЗЗ КСЗІ відповідають визначеному в експлуатаційній документації та нормативно-розпорядчої документації КСЗІ порядку застосування відповідних компонентів (складових частин) КЗЗ при реалізації (з урахуванням положень проектної документації КСЗІ) всіх ФПБ (функцій захисту), визначених у Технічному завданні на створення КСЗІ в ІТС;
- усі компоненти (складові частини) КЗЗ КСЗІ знаходяться у працездатному стані та функціонують належним чином.

Д.2.6.12 У результатах перевірки порядку використання введених до складу КЗЗ КСЗІ засобів захисту інформації мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) сформульовані з урахуванням вимог п. В.11 результати виконання відповідних перевірок. Мають бути наведені підстави, які дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних перевірок та (з урахуванням цих висновків) щодо підтвердження або не підтвердження того, що:

- фактично використовуваний порядок створення захищених інформаційних ресурсів, реєстрації користувачів, надання прав доступу до інформації користувачам ІТС та виконання інших завдань з адміністрування та обслуговування КСЗІ відповідає положенням експлуатаційної документації та нормативно-розпорядчої документації КСЗІ;

- фактично використовуваний порядок реєстрації фактів та результатів виконання певних завдань з адміністрування та обслуговування КСЗІ відповідає положенням нормативно-розпорядчої документації КСЗІ;

- зміст наданих у складі супровідної документації КСЗІ в ІТС реєстраційних журналів підтверджує факти належного застосування визначеного положеннями нормативно-розпорядчої документації КСЗІ порядку створення захищених інформаційних ресурсів, реєстрації користувачів, надання прав доступу до інформації користувачам ІТС та виконання інших завдань з адміністрування та обслуговування КСЗІ;

- фактичні атрибути доступу користувачів, процесів та захищених інформаційних ресурсів, які містяться у відповідних сховищах компонентів (складових частин) КЗЗ КСЗІ, відповідають наведеним у реєстраційних журналах відомостям.

Д.2.6.13 У результатах перевірки впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту повинні бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) сформульовані з урахуванням вимог п. В.12 результати виконання відповідних перевірок. Мають бути наведені підстави, які дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних перевірок та (з урахуванням цих висновків) щодо підтвердження або не підтвердження того, що:

- у складі КСЗІ впроваджено всі організаційні, фізичні та інші нетехнічні заходи захисту, визначені у проектній документації КСЗІ та нормативно-розпорядчій документації КСЗІ;

- зміст наданої супровідної документації КСЗІ, а також журналів обліку та реєстрації сховищ і матеріальних носіїв ІзОД підтверджує факти належного застосування всіх впроваджених організаційних, фізичних та інших нетехнічних заходів захисту.

Д.2.6.14 У результатах перевірки підготовленості співробітників СЗІ, персоналу та користувачів ІТС мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) сформульовані з урахуванням вимог п. В.13 результати виконання відповідних перевірок. Мають бути наведені підстави, які дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних перевірок та (з урахуванням цих висновків) щодо підтвердження або не підтвердження того, що:

- співробітники СЗІ, персонал та користувачі ІТС мають достатній для виконання своїх посадових та/або функціональних обов’язків рівень знань положень експлуатаційної та нормативно-розпорядчої документації КСЗІ;

- співробітники СЗІ, персонал та користувачі ІТС мають достатній для виконання своїх посадових та/або функціональних обов’язків рівень практичних навичок щодо використання засобів ІТС та КСЗІ.

Д.2.6.15 У результатах перевірки результатів створення та атестації комплексу ТЗІ мають бути викладені (з посиланням на відповідні пункти розділу "Методи виконання експертних робіт" або пункти Методики проведення експертизи) сформульовані з урахуванням вимог п. В.14 результати виконання відповідних перевірок. Мають бути наведені підстави, які дозволяють або не дозволяють дійти висновку щодо успішності або неуспішності здійснення певних перевірок та (з урахуванням цих висновків) щодо підтвердження або не підтвердження того, що:

- склад та характеристики створеного комплексу ТЗІ, наведені у документації щодо створення комплексу ТЗІ, розроблюваній на етапі виконання передпроектних робіт і на етапі розроблення та впровадження заходів із захисту інформації, відповідають особливостям конкретної ІТС та умовам її функціонування, визначеним на етапі попереднього ознайомлення з ОЕ та поглибленого обстеження ОЕ, а також зазначеним у документації, розробленій на етапі виконання передпроектних робіт зі створення КСЗІ;

- відомості, наведені у документації, розробленій на етапі випробувань та атестації комплексу ТЗІ, підтверджують відповідність створеного комплексу ТЗІ вимогам технічного завдання та положенням чинної нормативно-правової бази в сфері ТЗІ, які стосуються забезпечення захисту інформації від витоку технічними каналами.

Д.2.7 Рекомендації щодо змістовної частини розділу "Висновки за результатами експертних робіт"

Д.2.7.1 У розділі "Висновки за результатами експертних робіт" мають бути наведені висновки щодо результатів виконання відповідних експертних робіт, зокрема:

- висновки за результатами аналізу документації, розробленої на етапі виконання передпроектних робіт;
- висновки за результатами аналізу Технічного завдання на створення КСЗІ в ІТС;
- висновки за результатами оцінювання (за необхідності) ФПБ, що реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ;
- висновки за результатами оцінювання (за необхідності) рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ;
- висновки за результатами аналізу проектної документації КСЗІ та матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ;
- висновки за результатами аналізу експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ;
- висновки за результатами аналізу нормативно-розпорядчої документації КСЗІ;
- висновки за результатами аналізу документації щодо проведених випробувань КСЗІ;
- висновки за результатами аналізу організаційно-розпорядчої документації КСЗІ;
- висновки за результатами перевірки фактичного використання введених до складу КЗЗ КСЗІ засобів захисту інформації;
- висновки за результатами перевірки порядку використання введених до складу КЗЗ КСЗІ засобів захисту інформації;
- висновки за результатами перевірки впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту;
- висновки за результатами перевірки підготовленості співробітників СЗІ, персоналу та користувачів ІТС;
- висновки за результатами перевірки (за необхідності) результатів створення та атестації комплексу ТЗІ.

Крім цього, у розділі "Висновки за результатами експертних робіт" мають бути наведені (за наявності) особливі думки Експертів.

Д.2.7.2 У відповідних висновках (з посиланням на пункти розділу "Результати експертних робіт") мають бути наведені однозначні та обґрунтовані твердження щодо відповідності або невідповідності ОЕ висунутим вимогам.

Д.2.8 Рекомендації щодо змістовної частини додатків до протоколу експертизи КСЗІ

У додатках до протоколу експертизи КСЗІ рекомендується наводити відомості (свідоцтва), що одержані в ході виконання експертних робіт, слугують об’єктивному підтвердженню їх результатів та не містяться в іншій проектній, організаційно-розпорядчій, нормативно-розпорядчій документації, аналіз якої був здійснений в ході виконання запротокольованих робіт (вміст каталогів файлової системи; зразки екранних форм, одержані в ході виконання перевірок; вміст журналів реєстрації подій; одержані звіти про призначені атрибути доступу тощо).

Додаток Е

(рекомендований)

Рекомендації щодо викладення змістовної частини Експертного висновку за результатами експертизи засобу технічного захисту інформації від несанкціонованого доступу

У Додатку Е викладено рекомендації щодо змістовної частини Експертного висновку за результатами експертизи ЗТЗІ від НСД. Рекомендації викладено з урахуванням вимог Положення про державну експертизу в сфері технічного захисту інформації та методичних вказівок з документування результатів оцінювання ФПБ та рівнів гарантій коректності реалізації ФПБ у ЗТЗІ від НСД, наведених у НД ТЗІ 2.7-009-09 та НД ТЗІ 2.7-010-09. У п. Е.1 наведено рекомендації щодо змісту Експертного висновку, а у п. Е.2 – рекомендації щодо змістовної частини окремих розділів Експертного висновку.

Е.1 Рекомендації щодо змісту Експертного висновку за результатами експертизи засобу технічного захисту інформації від НСД

Е.1.1 Відповідно до вимог Положення про державну експертизу в сфері технічного захисту інформації в Експертному висновку за результатами експертизи ЗТЗІ від НСД повинні бути викладені:

- загальні відомості щодо ОЕ;
- загальна характеристика ОЕ (призначення, функції, можливості);
- вимоги нормативних документів з технічного захисту інформації, на відповідність яким здійснюється оцінка ОЕ;
- назва окремої методики, згідно з якою здійснювалася оцінка ОЕ, ким розроблена та затверджена, реєстраційний номер та дата затвердження;
- перелік документів і специфікацій програмних та технічних засобів, які надано Замовником Організатору експертизи;
- результати робіт щодо кожного пункту окремої методики експертизи ОЕ;
- розгорнутий висновок щодо відповідності ОЕ вимогам нормативних документів системи ТЗІ;
- сфера використання (вимоги до умов експлуатації) ОЕ;
- термін дії Експертного висновку;
- особливі думки Експертів, зафіксовані в протоколах.

Е.1.2 З урахуванням вимог Положення про державну експертизу в сфері технічного захисту інформації, а також з урахуванням рекомендацій щодо викладення змістовної частини протоколу експертизи ЗТЗІ від НСД, наведених у Додатку Г, рекомендується вводити до складу Експертного висновку такі розділи:

- загальні відомості щодо об’єкта експертизи;
- загальна характеристика об’єкта експертизи;
- нормативні документи, на відповідність вимогам яких здійснювалася оцінка об’єкта експертизи;
- методика проведення експертних робіт;
- перелік документів, склад програмних і технічних засобів, які надано на експертизу;
- результати експертних робіт;
- висновки за результатами експертизи;

- вимоги до умов використання об’єкта експертизи;
- термін дії Експертного висновку;
- особливі думки Експертів;
- додатки до Експертного висновку.

Е.1.3 Залежно від особливостей ОЕ можливо додавання, об’єднання або зміна назв певних розділів.

Е.1.4 Відповідно до вимог Положення про державну експертизу в сфері технічного захисту інформації Експертний висновок за результатами експертизи ЗТЗІ від НСД має бути затверджений керівником Організатора експертизи та зареєстрований уповноваженим державним органом.

Е.2 Рекомендації щодо змістовної частини окремих розділів Експертного висновку за результатами експертизи засобу технічного захисту інформації від НСД

Е.2.1 Рекомендації щодо змістовної частини розділу "Загальні відомості щодо об’єкта експертизи"

Е.2.1.1 У розділі "Загальні відомості щодо об’єкта експертизи" мають бути наведені такі відомості:

- повна та скорочена назви ОЕ;
- виробник (Розробник) ОЕ;
- вид, мета експертизи та підстави її проведення;
- Замовник та Організатор експертизи.

Е.2.1.2 Повна та скорочена назви ОЕ мають бути наведені відповідно до паспорта на ОЕ, інших відомостей, зазначених у заявці на проведення експертизи, та не суперечити положенням технічного завдання та іншої зазначеної у п. А.1 Додатка А до НД ТЗІ 2.7-010-09 документації, що надається для оцінювання рівня гарантій коректності реалізації ФПБ.

Е.2.1.3 Відомості щодо виробника (Розробника) ОЕ (назва організації (підприємства, установи), її місцезнаходження) мають бути наведені відповідно до відомостей, зазначених у заявці на проведення експертизи, рішенні уповноваженого державного органу та договорі між Замовником та Організатором експертизи на виконання відповідних робіт.

Е.2.1.4 Вид (первинна, додаткова або контрольна), мета та підстави проведення експертизи мають бути наведені відповідно до відомостей, зазначених у заявці на проведення експертизи, рішенні уповноваженого державного органу та договорі між Замовником та Організатором експертизи на виконання відповідних робіт.

Е.2.1.5 Відомості щодо Замовника та Організатора експертизи (назва організації (підприємства, установи), її місцезнаходження) мають бути наведені відповідно до відомостей, зазначених у заявці на проведення експертизи, рішенні уповноваженого державного органу та договорі між Замовником та Організатором експертизи на виконання відповідних робіт.

Е.2.2 Рекомендації щодо змістовної частини розділу "Загальна характеристика об’єкта експертизи"

Е.2.2.1 У розділі "Загальна характеристика об’єкта експертизи" мають бути наведені призначення ОЕ та стисла характеристика ОЕ.

Е.2.2.2 Призначення та стисла характеристика ОЕ мають бути наведені в обсязі, достатньому для чіткого розуміння можливостей та особливостей ОЕ щодо вирішення певних завдань захисту інформації, що обробляється в ІТС. Зокрема, мають бути наведені:

- визначення проблем (цілей) забезпечення безпеки інформації, вирішення яких покладається на ОЕ;

- визначення завдань захисту, вирішення яких забезпечується ОЕ;

- високорівневе визначення переліку та політики ФПБ, заявлених Розробником як таких, що призначені для вирішення певних завдань захисту;

- стислий опис вимог до апаратного середовища функціонування ОЕ та існуючих обмежень на використовувані в ньому апаратні засоби;

- стислий опис вимог до програмного середовища функціонування ОЕ та існуючих обмежень на використовувані в ньому програмні засоби.

Е.2.2.3 При формулюванні відповідних відомостей рекомендується скористатися відомостями, що містяться у відповідному протоколі (протоколах) експертизи, а також вмістом опису послуг безпеки, що реалізуються КЗЗ оцінюваного ОЕ, зазначеного у п. А.2.15 Додатка А до НД ТЗІ 2.7-010-09, або іншого аналогічного документа, в якому містяться відповідні відомості, наданого для оцінювання рівня гарантій коректності реалізації ФПБ.

Е.2.3 Рекомендації щодо змістовної частини розділу "Нормативні документи, на відповідність вимогам яких здійснювалася оцінка об'єкта експертизи"

Е.2.3.1 У розділі "Нормативні документи, на відповідність вимогам яких здійснювалася оцінка об'єкта експертизи" мають бути наведені:

- перелік чинних нормативних документів, відповідність вимогам яких перевірялася в ході проведення експертизи;

- розроблені та узгоджені відповідно до положень НД ТЗІ 2.7-009-09 технічні вимоги до оцінюваного ОЕ у частині реалізації ФПБ та опис порядку реалізації цих вимог.

Е.2.3.2 Якщо мета експертизи передбачала оцінювання ФПБ та рівня гарантій коректності їх реалізації, у переліку нормативних документів мають бути зазначені НД ТЗІ 2.5-004-99, НД ТЗІ 2.7-009-09 та НД ТЗІ 2.7-010-09.

Е.2.3.3 Якщо крім оцінювання ФПБ та рівня гарантій коректності їх реалізації мета експертизи передбачала оцінювання відповідності ОЕ вимогам чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу (НД ТЗІ 2.5-007-2007, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 тощо) або будь-яким іншим вимогам, у переліку мають бути зазначені відповідні документи.

Е.2.4 Рекомендації щодо змістовної частини розділу "Методика проведення експертних робіт"

У розділі "Методика проведення експертних робіт" мають бути наведені реквізити узгодженої та затвердженої в установленому порядку Методики проведення експертизи.

Е.2.5 Рекомендації щодо змістовної частини розділу "Перелік документів, склад програмних та технічних засобів, які надано на експертизу"

Е.2.5.1 У розділі "Перелік документів, склад програмних та технічних засобів, які надано на експертизу" має бути наведено:

- повний перелік матеріалів (документів), визначений з урахуванням рекомендацій п. А.1 Додатка А до НД ТЗІ 2.7-010-09 та наданий Замовником експертизи (Розробником ОЕ) Експертам для проведення експертних робіт;

- специфікація програмних компонентів, що входять до складу інсталяційного пакета ОЕ (для ОЕ, що являє собою програмний або програмно-апаратний засіб) та надані для проведення експертизи;

- специфікація апаратних компонентів, що входять до складу ОЕ (для ОЕ, що являє собою програмно-апаратний або апаратний засіб) та надані для проведення експертизи.

Е.2.5.2 Для всіх компонентів ОЕ та матеріалів (документів), зазначених у переліку, мають бути наведені їх ідентифікатори, які відповідають положенням зазначеної у п. А.2.12 Додатка А до НД ТЗІ 2.7-010-09 документації системи керування конфігурацією ОЕ, що використовується Розробником ОЕ.

Е.2.6 Рекомендації щодо змістовної частини розділу "Результати експертних робіт"

Е.2.6.1 У розділі "Результати експертних робіт" мають бути наведені відомості щодо результатів всіх експертних робіт, виконаних у ході проведення експертизи, зокрема:

- результати оцінювання ФПБ;
- результати оцінювання рівня гарантій коректності реалізації ФПБ;
- результати оцінювання відповідності ОЕ вимогам чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу або будь-яким іншим вимогам.

Е.2.6.2 Результати експертних робіт можуть викладатися або шляхом повторення всіх відомостей, які стосуються проведення робіт за кожним пунктом Методики проведення експертизи, наведених у розділі "Результати експертних робіт" протоколу (протоколів) експертизи, або шляхом стислого викладення відповідних відомостей з посиланням, за необхідності, на відповідні пункти протоколу (протоколів).

Е.2.6.3 Спосіб викладення результатів експертних робіт повинен бути однаковим для всіх робіт, вказаних у протоколі (протоколах) експертизи.

Е.2.6.4 Незалежно від того, в який спосіб викладено результати робіт за певним пунктом Методики проведення експертизи, безпосередньо у розділі "Результати експертних робіт" мають бути наведені висновки щодо визнання результатів виконання відповідних перевірок успішними або неуспішними та висновки щодо підтвердження або не підтвердження задоволення певних вимог.

Е.2.7 Рекомендації щодо змістовної частини розділу "Висновки за результатами експертизи"

Е.2.7.1 У розділі "Висновки за результатами експертизи" мають бути наведені висновки за результатами виконання відповідних експертних робіт, зокрема:

- висновки за результатами оцінювання ФПБ;
- висновки за результатами оцінювання рівня гарантій коректності реалізації ФПБ;
- висновки за результатами оцінювання відповідності ОЕ вимогам чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу або будь-яким іншим вимогам.

Е.2.7.2 У відповідних висновках з посиланням на певні вимоги нормативних документів, зазначених у розділі "Нормативні документи, на відповідність вимогам яких здійснювалася оцінка об’єкта експертизи", а також на відповідні пункти розділу "Результати експертних робіт" мають бути наведені однозначні та обґрунтовані твердження щодо відповідності або невідповідності ОЕ висунутим вимогам.

Е.2.7.3 У висновках за результатами оцінювання ФПБ та рівня гарантій коректності їх реалізації має бути наведений узагальнений перелік ФПБ (функціональний профіль захищеності), який реалізується оцінюваним ОЕ, а також рівень гарантій коректності реалізації ФПБ, підтверджені за результатами експертизи.

Е.2.7.4 Якщо в процесі експертизи було здійснено оцінювання відповідності ОЕ вимогам чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу, окремим пунктом (пунктами) висновків мають бути викладені висновки щодо можливості або неможливості застосування ОЕ з метою забезпечення захисту інформації в ІТС відповідного типу.

Е.2.7.5 Окремим пунктом (пунктами) мають бути викладені узагальнюючі висновки щодо відповідності або невідповідності ОЕ в обсязі функцій, визначених у паспорті, вимогам нормативних документів системи ТЗІ в Україні.

Е.2.7.6 Окремим пунктом (пунктами) мають бути викладені висновки щодо сфери застосування результатів експертизи, в яких має бути зазначено, чи поширюються результати експертизи лише на ту конфігурацію ОЕ, що наведена у розділі "Перелік

документів, склад програмних та технічних засобів, які надано на експертизу" та стосовно якої здійснювалася експертиза, або вони є дійсними також для оновлених конфігурацій ОЕ.

Е.2.8 Рекомендації щодо змістовної частини розділу "Вимоги до умов використання об’єкта експертизи"

Е.2.8.1 У розділі "Вимоги до умов використання об’єкта експертизи" мають бути наведені всі вимоги та обмеження щодо умов використання ОЕ, які мають бути дотримані в процесі його використання за призначенням. Зокрема, мають бути наведені:

- усі викладені у зазначеному в п. А.2.13 Додатка А до НД ТЗІ 2.7-010-09 описі процедур безпечної інсталяції, генерації та запуску ОЕ вимоги та обмеження, дотримання яких має забезпечувати безпечний перехід ОЕ від перебування під контролем системи керування конфігурацією Розробника до початкових операцій у середовищі експлуатації;
- усі викладені у зазначеній у пп. А.2.15 - А.2.17 Додатка А до НД ТЗІ 2.7-010-09 експлуатаційній документації вимоги щодо забезпечення безпечного функціонування ОЕ;
- усі викладені в описі політики ФПБ "Цілісність КЗЗ" відповідного рівня, який міститься у розробленому та узгодженому відповідно до положень НД ТЗІ 2.7-009-09 описі переліку та політики ФПБ, на відповідність яким здійснюватиметься перевірка ОЕ, обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Е.2.8.2 За наявності мають бути наведені також вимоги та обмеження щодо умов використання ОЕ, які визначаються положеннями чинної нормативно-правової бази в сфері ТЗІ, що регламентує порядок проведення робіт зі створення КСЗІ в АС різного класу, в яких обробляється інформація, що має різні характеристики відповідно до встановленого законодавством правового режиму та режиму доступу, а також вимогами зазначених у розділі "Нормативні документи, на відповідність вимогам яких здійснювалася оцінка об’єкта експертизи" нормативних документів.

Е.2.9 Рекомендації щодо змістовної частини розділу "Термін дії Експертного висновку"

У розділі "Термін дії Експертного висновку" мають бути наведені дати початку та закінчення терміну дії Експертного висновку, визначені відповідно до вимог Положення про державну експертизу у сфері технічного захисту інформації.

Е.2.10 Рекомендації щодо змістовної частини розділу "Особливі думки Експертів"

У розділі "Особливі думки Експертів" мають бути в повному обсязі наведені всі особливі думки Експертів, які містяться у відповідних пунктах протоколу (протоколів) експертизи.

Е.2.11 Рекомендації щодо змістовної частини додатків до Експертного висновку

Е.2.11.1 Відповідно до положень НД ТЗІ 2.7-009-09 невід’ємним додатком до Експертного висновку мають бути зазначені у розділі "Нормативні документи, на відповідність вимогам яких здійснювалася оцінка об’єкта експертизи" технічні вимоги до оцінюваного ОЕ в частині реалізації ФПБ, а також опис порядку реалізації цих вимог.

Е.2.11.2 В інших додатках до Експертного висновку можуть бути наведені відомості, які є необхідними та значущими з погляду повноти змістовної частини Експертного висновку, але обсяг яких не дозволяє навести їх безпосередньо у відповідних розділах Експертного висновку.

Додаток Ж
(рекомендований)

Рекомендації щодо викладення змістовної частини Експертного висновку за результатами експертизи комплексної системи захисту інформації

У Додатку Ж викладено рекомендації щодо змістовної частини Експертного висновку за результатами експертизи КСЗІ. Рекомендації викладено з урахуванням вимог Положення про державну експертизу в сфері технічного захисту інформації, методичних вказівок з документування результатів оцінювання ФПБ та рівнів гарантій коректності реалізації ФПБ у ЗТЗІ від НСД, наведених у НД ТЗІ 2.7-009-09 та НД ТЗІ 2.7-010-09, а також рекомендацій, викладених у міжнародних стандартах, загальнодержавних та відомчих нормативних документах, присвячених питанням оцінювання ІТС (систем інформаційних технологій) на відповідність вимогам щодо інформаційної безпеки. У п. Ж.1 наведено рекомендації щодо змісту Експертного висновку, а у п. Ж.2 – рекомендації щодо змістовної частини окремих розділів Експертного висновку.

Ж.1 Рекомендації щодо змісту Експертного висновку за результатами експертизи КСЗІ

Ж.1.1 Відповідно до вимог Положення про державну експертизу в сфері технічного захисту інформації в Експертному висновку за результатами експертизи КСЗІ повинні бути викладені:

- загальні відомості щодо ОЕ;
- загальна характеристика ОЕ (призначення, функції, можливості);
- вимоги нормативних документів з технічного захисту інформації, на відповідність яким здійснюється оцінка ОЕ;
- назва окремої методики, згідно з якою здійснювалася оцінка ОЕ, ким розроблена та затверджена, реєстраційний номер та дата затвердження;
- перелік документів і специфікацій програмних та технічних засобів, які надано Замовником Організатору експертизи;
- результати робіт щодо кожного пункту окремої методики експертизи ОЕ;
- розгорнутий висновок щодо відповідності ОЕ вимогам нормативних документів системи ТЗІ;
- сфера використання (вимоги до умов експлуатації) ОЕ;
- термін дії Експертного висновку;
- особливі думки Експертів, зафіксовані в протоколах.

Ж.1.2 З урахуванням вимог Положення про державну експертизу в сфері технічного захисту інформації, а також з урахуванням рекомендацій щодо викладення змістовної частини протоколу експертизи КСЗІ, наведених у Додатку Д, рекомендується вводити до складу Експертного висновку такі розділи:

- загальні відомості щодо об’єкта експертизи;
- загальна характеристика об’єкта експертизи;
- нормативні документи, на відповідність вимогам яких здійснювалася оцінка об’єкта експертизи;
- методика проведення експертних робіт;
- перелік документів, склад програмних і технічних засобів об’єкта експертизи;
- результати експертних робіт;

- висновки за результатами експертизи;
- вимоги до умов експлуатації об’єкта експертизи;
- термін дії Експертного висновку;
- особливі думки Експертів;
- додатки до Експертного висновку.

Ж.1.3 Залежно від особливостей ОЕ можливе додавання, об’єднання або зміна назв певних розділів.

Ж.1.4 Відповідно до вимог Положення про державну експертизу в сфері технічного захисту інформації Експертний висновок за результатами експертизи КСЗІ повинен бути затверджений керівником Організатора експертизи та зареєстрований уповноваженим державним органом.

Ж.2 Рекомендації щодо змістовної частини окремих розділів Експертного висновку за результатами експертизи КСЗІ

Ж.2.1 Рекомендації щодо змістовної частини розділу "Загальні відомості щодо об’єкта експертизи"

Ж.2.1.1 У розділі "Загальні відомості щодо об’єкта експертизи" мають бути наведені такі відомості:

- повна та скорочена назви ОЕ;
- вид, мета експертизи та підстави її проведення;
- Замовник та Організатор експертизи;

Ж.2.1.2 Повна та скорочена назви ОЕ мають бути наведені відповідно до відомостей, зазначених у заявці на проведення експертизи, та не суперечити положенням Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10.

Ж.2.1.3 Вид (первинна, додаткова або контрольна), мета та підстави проведення експертизи мають бути наведені відповідно до відомостей, зазначених у заявці на проведення експертизи, рішенні уповноваженого державного органу та договорі між Замовником та Організатором експертизи на виконання відповідних робіт.

Ж.2.1.4 Відомості щодо Замовника та Організатора експертизи (назва організації (підприємства, установи), її місцезнаходження) мають бути наведені відповідно до відомостей, зазначених у заявці на проведення експертизи, рішенні уповноваженого державного органу та договорі між Замовником та Організатором експертизи на виконання відповідних робіт.

Ж.2.2 Рекомендації щодо змістовної частини розділу "Загальна характеристика об’єкта експертизи"

Ж.2.2.1 У розділі "Загальна характеристика об’єкта експертизи" мають бути наведені призначення ОЕ та стисла характеристика ОЕ.

Ж.2.2.2 Призначення та стисла характеристика ОЕ мають бути наведені в обсязі, достатньому для чіткого розуміння можливостей та особливостей ОЕ щодо вирішення певних завдань захисту інформації, що обробляється в ІТС. Зокрема, мають бути наведені:

- стисла характеристика обчислювальної системи ІТС;
- стисла характеристика інформаційного середовища ІТС;
- стисла характеристика фізичного середовища ІТС;
- стисла характеристика середовища користувачів ІТС;
- перелік завдань захисту, вирішення яких забезпечується КСЗІ;
- відомості щодо структури та складу КСЗІ, а також щодо переліку технічних, організаційних, фізичних та інших заходів захисту, які у сукупності складають КСЗІ;

- функціональні специфікації КЗЗ КСЗІ та рівень гарантій коректності реалізації ФПБ.

Ж.2.2.3 При формулюванні відповідних відомостей рекомендується скористатися змістом протоколу (протоколів) експертизи, а також змістом результатів обстеження середовищ функціонування ІТС, зазначених у п. А.2.1.4, звіту за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ, зазначеного в п. А.2.1.8, Плану захисту інформації в ІТС, зазначеного в п. А.2.1.9, Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10.

Ж.2.3 Рекомендації щодо змістовної частини розділу "Нормативні документи, на відповідність вимогам яких здійснювалася оцінка об'єкта експертизи"

Ж.2.3.1 У розділі "Нормативні документи, на відповідність вимогам яких здійснювалася оцінка об'єкта експертизи" повинні бути наведені:

- перелік чинних нормативних документів, відповідність вимогам яких перевірялася в ході проведення експертизи;
- Технічне завдання на створення КСЗІ в ІТС, зазначене в п. А.2.1.10;
- якщо в ході експертизи КСЗІ здійснювалося оцінювання ФПБ та рівнів гарантій їх реалізації в окремих компонентах (складових частинах) КЗЗ КСЗІ – розроблені та узгоджені відповідно до положень НД ТЗІ 2.7-009-09 технічні вимоги до відповідних компонентів (складових частин) КЗЗ КСЗІ в частині реалізації ФПБ та опис порядку реалізації цих вимог.

Ж.2.3.2 У переліку нормативних документів мають бути наведені всі чинні нормативні документи, вимоги яких мали бути враховані в процесі робіт зі створення КСЗІ, зокрема зазначені у відповідних пунктах Додатка А, а також нормативні документи щодо забезпечення захисту інформації в ІТС відповідного типу (НД ТЗІ 2.5-007-2007, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 тощо).

Ж.2.3.3 Якщо в ході експертизи КСЗІ здійснювалося оцінювання ФПБ та рівнів гарантій їх реалізації в окремих компонентах (складових частинах) КЗЗ КСЗІ, у переліку нормативних документів мають бути зазначені НД ТЗІ 2.5-004-99, НД ТЗІ 2.7-009-09 та НД ТЗІ 2.7-010-09.

Ж.2.4 Рекомендації щодо змістовної частини розділу "Методика проведення експертних робіт"

У розділі "Методика проведення експертних робіт" мають бути наведені реквізити узгодженої та затвердженої в установленому порядку Методики проведення експертизи.

Ж.2.5 Рекомендації щодо змістовної частини розділу "Перелік документів, склад програмних та технічних засобів об'єкта експертизи"

Ж.2.5.1 У розділі "Перелік документів, склад програмних та технічних засобів об'єкта експертизи" мають бути наведені:

- перелік апаратних компонентів, що входять до складу обчислювальної системи ІТС;
- перелік програмних компонентів ІТС;
- перелік апаратних, програмно-апаратних та програмних компонентів (складових частин), що входять до складу КЗЗ КСЗІ;
- перелік засобів захисту, що входять до складу комплексу ТЗІ;
- повний перелік матеріалів (документів), визначений з урахуванням рекомендацій Додатка А та наданий Замовником експертизи Експертам для проведення відповідних експертних робіт.

Ж.2.5.2 При формулюванні відповідних відомостей рекомендується скористатися змістом протоколу (протоколів) експертизи, змістом Формуляра ІТС, зазначеного у п. А.2.9.1, а також змістом Паспорта на комплекс ТЗІ, зазначеного у п. А.3.3.1.

Ж.2.5.3 Якщо в ході експертизи КСЗІ здійснювалося оцінювання ФПБ та рівнів гарантій їх реалізації в окремих компонентах (складових частинах) КЗЗ КСЗІ, для

відповідних компонентів та матеріалів (документів) мають бути наведені їх ідентифікатори, які відповідають положенням зазначеної у п. А.12 Додатка А до НД ТЗІ 2.7-010-09 документації використовуваної Розробником компонента (складової частини) КЗЗ КСЗІ системи керування конфігурацією.

Ж.2.6 Рекомендації щодо змістовної частини розділу "Результати експертних робіт"

Ж.2.6.1 У розділі "Результати експертних робіт" мають бути наведені такі відомості щодо результатів всіх експертних робіт, виконаних у ході проведення експертизи:

- аналіз документації, розробленої на етапі виконання передпроектних робіт;
- аналіз Технічного завдання на створення КСЗІ в ІТС;
- оцінювання (за необхідності) ФПБ, що реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ;
- оцінювання (за необхідності) рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ;
- аналіз проектної документації КСЗІ та матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ;
- аналіз експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ;
- аналіз нормативно-розпорядчої документації КСЗІ;
- аналіз документації щодо проведених випробувань КСЗІ;
- аналіз організаційно-розпорядчої документації КСЗІ;
- перевірка фактичного використання введених до складу КЗЗ КСЗІ засобів захисту інформації;
- перевірка порядку використання введених до складу КЗЗ КСЗІ засобів захисту інформації;
- перевірка впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту;
- перевірка підготовленості співробітників СЗІ, персоналу та користувачів ІТС;
- перевірка (за необхідності) результатів створення та атестації комплексу ТЗІ.

Ж.2.6.2 Результати експертних робіт можуть викладатися або шляхом повторення всіх відомостей, що стосуються проведення робіт за кожним пунктом Методики проведення експертизи, наведених у розділі "Результати експертних робіт" протоколу (протоколів) експертизи, або шляхом стислого викладення відповідних відомостей з посиланням, за необхідності, на відповідні пункти протоколу (протоколів).

Ж.2.6.3 Спосіб викладення результатів експертних робіт має бути однаковим для всіх робіт, зазначених у протоколі (протоколах) експертизи.

Ж.2.6.4 Незалежно від того, в який спосіб викладено результати робіт за певним пунктом Методики проведення експертизи, безпосередньо у розділі "Результати експертних робіт" мають бути наведені висновки щодо визнання результатів виконання відповідних перевірок успішними або неуспішними та висновки щодо підтвердження або не підтвердження задоволення певних вимог.

Ж.2.7 Рекомендації щодо змістовної частини розділу "Висновки за результатами експертизи"

Ж.2.7.1 У розділі "Висновки за результатами експертизи" повинні бути наведені висновки за результатами виконання відповідних експертних робіт, зокрема висновки за результатами:

- аналізу документації, розробленої на етапі виконання передпроектних робіт;
- аналізу Технічного завдання на створення КСЗІ в ІТС;

- оцінювання ФПБ, що реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ;

- оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ;

- аналізу проектної документації КСЗІ та матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ;

- аналізу експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ;

- аналізу нормативно-розпорядчої документації КСЗІ;

- аналізу документації щодо проведених випробувань КСЗІ;

- аналізу організаційно-розпорядчої документації КСЗІ;

- перевірки фактичного використання введених до складу КЗЗ КСЗІ засобів захисту інформації;

- перевірки порядку використання введених до складу КЗЗ КСЗІ засобів захисту інформації;

- перевірки впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту;

- перевірки підготовленості співробітників СЗІ, персоналу та користувачів ІТС;

- перевірки (за необхідності) результатів створення та атестації комплексу ТЗІ.

Ж.2.7.2 У відповідних висновках (з посиланням на певні вимоги нормативних документів, зазначених у розділі "Нормативні документи, на відповідність вимогам яких здійснювалася оцінка об’єкта експертизи", а також на відповідні пункти розділу "Результати експертних робіт") мають бути наведені однозначні та обґрунтовані твердження щодо відповідності або невідповідності ОЕ висунутим вимогам.

Ж.2.7.3 Якщо в ході експертизи КСЗІ здійснювалося оцінювання ФПБ та рівнів гарантій їх реалізації в окремих компонентах (складових частинах) КЗЗ КСЗІ, при викладенні відповідних висновків слід враховувати рекомендації п. Е.2.7.

Ж.2.7.4 Окремим пунктом (пунктами) мають бути викладені узагальнюючі висновки щодо відповідності або невідповідності КСЗІ в обсязі функцій, наведених у Технічному завданні на створення КСЗІ в ІТС, зазначеному в п. А.2.1.10, вимогам нормативних документів системи ТЗІ в Україні та можливості введення ІТС в промислову експлуатацію.

Ж.2.8 Рекомендації щодо змістовної частини розділу "Вимоги до умов експлуатації об’єкта експертизи"

Ж.2.8.1 У розділі "Вимоги до умов експлуатації об’єкта експертизи" повинні бути наведені всі вимоги та обмеження щодо умов експлуатації ОЕ, які мають бути дотримані в процесі його використання за призначенням. Зокрема, слід навести:

- усі викладені у зазначених у п. А.2.3.1 Експертних висновках щодо відповідності використовуваних у складі КЗЗ КСЗІ засобів захисту інформації вимогам чинних нормативних документів системи ТЗІ вимоги щодо умов експлуатації відповідних складових частин КЗЗ КСЗІ, сформульовані з урахуванням порядку їх використання, наведеного у проектній документації КСЗІ, зазначеній у п. А.2.2;

- усі викладені у зазначеному в п. А.3.3.4 акті атестації комплексу ТЗІ умови, яких потрібно дотримуватися під час експлуатації.

Ж.2.8.2 Якщо в ході експертизи КСЗІ здійснювалося оцінювання ФПБ та рівнів гарантій їх реалізації в окремих компонентах (складових частинах) КЗЗ КСЗІ, окремими пунктами мають бути наведені вимоги до умов використання відповідних компонентів (складових частин) КЗЗ КСЗІ, сформульовані з урахуванням рекомендацій п. Е.2.8.

Ж.2.8.3 За наявності, повинні бути наведені також вимоги та обмеження щодо умов експлуатації ОЕ, які визначаються положеннями чинної нормативно-правової бази в сфері ТЗІ,

що регламентує порядок проведення робіт зі створення КСЗІ в АС різного класу, в яких обробляється інформація, що має різні характеристики відповідно до встановленого законодавством правового режиму та режиму доступу, а також вимогами зазначених у розділі "Нормативні документи, на відповідність вимогам яких здійснювалася оцінка об’єкта експертизи" нормативних документів.

Ж.2.9 Рекомендації щодо змістовної частини розділу "Термін дії Експертного висновку"

У розділі "Термін дії Експертного висновку" мають бути наведені дати початку та закінчення терміну дії Експертного висновку, визначені відповідно до вимог Положення про державну експертизу у сфері технічного захисту інформації.

Ж.2.10 Рекомендації щодо змістовної частини розділу "Особливі думки Експертів"

У розділі "Особливі думки Експертів" мають бути в повному обсязі наведені всі особливі думки Експертів, які містяться у відповідних пунктах протоколу (протоколів) експертизи.

Ж.2.11 Рекомендації щодо змістовної частини додатків до Експертного висновку

Ж.2.11.1 Якщо в ході експертизи КСЗІ здійснювалося оцінювання ФПБ та рівнів гарантій їх реалізації в окремих компонентах (складових частинах) КЗЗ КСЗІ, відповідно до положень НД ТЗІ 2.7-009-09, невід’ємним додатком до Експертного висновку повинні бути зазначені у розділі "Нормативні документи, на відповідність вимогам яких здійснювалася оцінка об’єкта експертизи" технічні вимоги до оцінюваного ОЕ в частині реалізації ФПБ та опис порядку реалізації цих вимог.

Ж.2.11.2 В інших додатках до протоколу можуть бути наведені відомості, які є необхідними та значущими з погляду повноти змістовної частини Експертного висновку, але обсяг яких не дозволяє навести їх безпосередньо у відповідних розділах Експертного висновку.