**Восьмий семестр. Заняття 20.**

**Лекція 8.**

**Державна експертиза КСЗІ в ІТС.**

**Вступ.**

**Питання 1. Законодавча база експертизи.**

**Питання 2. Положення про організацію та проведення наукової та науково-технічної експертизи.**

**Питання 3. Експлуатаційні питання проведення експертизи.**

**Контрольні питання.**

**Вступ**

### Питання 1.

Правові, організаційні і фінансові основи експертної діяльності в науково-технічній сфері визначає

**Який нормативний акт визначає правові основи експертної діяльності в науково-технічній сфері?**

Закон України «**Про наукову і науково-технічну експертизу**» (далі - Закон).

Згідно **статті 1**Закону наукова і науково-технічна експертиза (далі - експертиза) - це діяльність, метою якої є дослідження, перевірка, аналіз та оцінка науково-технічного рівня об'єктів експертизи і підготовка обґрунтованих висновків для прийняття рішень щодо таких об'єктів.

Експертиза у сфері науково-технічних розробок та дослідно-конструкторських робіт (далі - НДР), фундаментальних і прикладних досліджень, у тому числі на стадії їх практичного застосування, проводиться науково-дослідними організаціями та установами, вищими навчальними закладами, іншими організаціями та окремими юридичними і фізичними особами які акредитовані на цей вид діяльності.

Згідно **статті 2** Закону основними завданнями експертизи є:

- об'єктивне, комплексне дослідження об'єктів експертизи;

- перевірка відповідності об'єктів експертизи вимогам і нормам чинного законодавства;

- оцінка відповідності об'єктів експертизи сучасному рівню наукових і технічних знань, тенденціям науково-технічного прогресу, принципам державної науково-технічної політики, вимогам екологічної безпеки, економічної доцільності;

- аналіз рівня використання науково-технічного потенціалу, оцінка результативності НДР;

- прогнозування науково-технічних, соціально-економічних і екологічних наслідків реалізації чи діяльності об'єкта експертизи;

- підготовка науково обґрунтованих експертних висновків.

**Хто є суб'єктами експертизи згідно закону України?**

Згідно **статті 4** Закону суб'єктами експертизи є замовники, організатори експертизи, а також експерти.

**Які органи та установи проводять державну експертизу згідно закону України?**

Замовниками експертизи можуть бути державні органи і органи місцевого самоврядування, підприємства, установи і організації, громадяни, заінтересовані у   
проведенні такої експертизи.

**Що формують замовники експертизи згідно закону України?**

Замовники експертизи формують завдання на проведення експертизи,

**Що забезпечують замовники експертизи згідно закону України?**

забезпечують оплату витрат на її проведення, оплату праці експертів або послуг організаторів експертизи.

Організаторами експертизи є фізичні та юридичні особи, які

**На підставі чого організатори експертизи проводять її згідно закону України?**

на підставі доручення або договору з замовниками

**Що роблять організатори експертизи згідно закону України?**

організовують та проводять експертизу і подають експертні висновки.

Експертизу можуть проводити:

- органи виконавчої влади у межах своєї компетенції;

- підприємства, установи та організації всіх форм власності, тимчасові творчі колективи, що здійснюють наукову і науково-технічну діяльність, спеціалізовані експертні організації;

- окремі експерти, групи експертів та експертні ради.

Експертами є фізичні особи, які мають високу кваліфікацію, спеціальні знання і безпосередньо здійснюють наукову чи науково-технічну експертизу та несуть персональну відповідальність за достовірність і повноту аналізу, обґрунтованість рекомендацій відповідно до вимог завдання на проведення експертизи.

Не дозволяється поєднання в одній особі функцій автора розробки чи іншим чином заінтересованої особи та її експерта.

Згідно **статті 5** Закону об'єктами експертизи можуть бути:

- діючі об'єкти техніки та промисловості, споруди, природні об'єкти тощо, стосовно яких виникає потреба отримати науково обґрунтовані експертні висновки;

- проекти, програми, пропозиції різного рівня, щодо яких необхідно провести науково обґрунтований аналіз і дати висновок про доцільність їх прийняття, впровадження, подальшого використання тощо.

Згідно **статті 6** Закону підставами для проведення експертизи є:

- рішення органів виконавчої влади та органів місцевого самоврядування, прийняті в межах їх повноважень;

- договори на проведення експертизи, укладені підприємствами, установами та організаціями, фізичними особами.

Згідно **статті 7** Закону фізичні особи, які на постійній або професійній основі здійснюють діяльність, пов'язану з наданням експертних послуг, крім осіб, зазначених у частині другій цієї статті, та юридичні особи, статутом яких передбачено таку діяльність, повинні пройти державну акредитацію і отримати свідоцтво, що підтверджує кваліфікацію його отримувача з питання організації та проведення експертизи.

Порядок проведення державної акредитації фізичних і юридичних осіб на право проведення експертизи, форму свідоцтва на право проведення такої експертизи та перелік документів державного зразка, що дають фізичним особам право на провадження експертної діяльності і надання експертних послуг без отримання свідоцтва, визначаються центральним органом виконавчої влади, що забезпечує формування державної політики у сфері науки.

Державну акредитацію осіб на право проведення експертизи проводить центральний орган виконавчої влади, що реалізує державну політику у сфері наукової, науково-технічної діяльності.

Згідно **статті 10** Закону державну експертизу проводять:

- органи виконавчої влади;

- державні підприємства,установи та організації.

**На які експертизи можуть передаватися об'єкти експертизи згідно закону України?**

Згідно **статті 13** Закону об'єкти експертизи можуть передаватися на попередню, первинну, повторну, додаткову, контрольну експертизи.

Згідно **статті 14** Закону попередня експертиза проводиться з метою з'ясування відповідності формальних ознак об'єкта експертизи встановленим нормам і правилам технічної та екологічної безпеки, вимогам стандартів тощо.

Згідно **статті 15** Закону первинна експертиза передбачає здійснення всіх необхідних заходів у процесі підготовки обґрунтованого висновку щодо об'єктів експертизи, які передаються заінтересованими фізичними та юридичними особами - замовниками експертизи на аналіз та оцінку експертним організаціям або експертам.

Згідно **статті 16** Закону повторна експертиза може проводитися:

- у разі порушення встановлених вимог і правил під час проведення первинної експертизи;

- на вимогу замовника експертизи чи автора розробки за наявності обґрунтованих претензій до висновку первинної експертизи.

**Стосовно яких об'єктів проводиться додаткова експертиза згідно закону України?**

Згідно **статті 17** Закону додаткова експертиза проводиться стосовно об'єктів, щодо яких відкрилися нові наукові і науково-технічні обставини.

**Для чого здійснюється контрольна експертиза згідно закону України?**

Згідно **статті 18** Закону контрольна експертиза здійснюється з ініціативи замовника для перевірки висновків первинної експертизи або з ініціативи фізичних чи юридичних осіб, заінтересованих у спростуванні окремих положень, частин або в цілому висновків раніше проведених експертиз.

**Що є основним юридичним документом, що регламентує відносини між замовником і організатором у сфері експертизи згідно закону України?**

Згідно **статті 22** Закону основним юридичним документом, що регламентує відносини між замовником і організатором у сфері експертизи, є договір на її проведення.

Згідно **статті 34** Закону у сфері державної експертизи фінансову підтримку діяльності експертів забезпечує держава.

В усіх інших випадках матеріальне стимулювання експертів здійснюється за рахунок коштів замовника експертизи або інших організацій і установ за дорученням замовника.

Максимальний розмір коштів, що спрямовуються на покриття витрат на експертизу, не може перевищувати:

- для експертизи наукових і науково-технічних програм та проектів - 1,5 % кошторису витрат, передбачених на їх виконання;

- для експертизи виконаних науково-дослідних або проектно-конструкторських робіт - 3 % вартості обсягу виконаних робіт.

**Питання 2.**

**Як називається наказ, що встановлює вимоги до проведення науково-технічної експертизи?**

24 квітня 1998 року наказом Міністерства України у справах науки і технологій № 131, зареєстрованим в Міністерстві юстиції України 16 липня 1998 року за № 462/2902, було затверджено «**Положення про організацію та проведення наукової та науково-технічної експертизи**» (далі - Положення), яке встановлює такі вимоги:

1.11. Під час проведення експертизи встановлюються відповідність об'єктів експертизи вимогам національної економічної, оборонної та екологічної безпеки; науково-технічна новизна об'єктів експертизи; відповідність технологій, обладнання, устаткування кращим вітчизняним та зарубіжним аналогам; відповідність вимогам чинних стандартів, вимогам технічної безпеки; реальність термінів упровадження об'єктів експертизи та актуальність об'єктів на момент її завершення; ступінь економічної ефективності, матеріаломісткості технологій і обладнання.

**2. Види експертизи**

2.1. Експертиза може бути попередня, первинна, повторна, додаткова та контрольна.

**У якому разі науково-технічна експертиза набуває статусу державної?**

2.7. Експертиза набуває статусу державної, якщо вона провадиться державними органами або на виконання їх доручень академіями наук.

**3. Координація діяльності суб'єктів експертизи**

**Що подає замовник науково-технічної експертизи до організатора експертизи?**

3.1. Замовник експертизи подає до організатора експертизи заяву про проведення експертизи разом з супровідними документами щодо об'єкта експертизи.

Замовник експертизи формує завдання на проведення експертизи, забезпечує оплату витрат на її проведення.

3.6. Основним документом, що регламентує стосунки між замовником і організатором експертизи, є договір на її проведення. До договору додаються документи, які визначають об'єкт експертизи та забезпечують її проведення. Документи подаються на паперовому та магнітному носіях.

3.8. Організатор веде реєстр поданих проектів та надає авторам проектів довідку про реєстраційний номер та консультації з процедурних питань.

**4. Вимоги до експертного висновку**

4.1. Висновок експертизи складається із вступної, констатувальної та заключної частин. Чітка і ясна оцінка проекту у висновках експертизи (за одним із вказаних варіантів) є обов'язковою. Висновок, що не має такої оцінки, не може бути підписаний чи затверджений уповноваженими посадовими особами.

4.2. Підготовлений експертний висновок підписується експертом і керівником організації (установи) - організатором експертизи.

4.6. Висновок експертизи зберігає чинність протягом терміну, визначеного договором на її проведення. Після закінчення терміну дії висновку експертизи відповідні об'єкти експертизи підлягають повторній експертизі.

**5. Права та обов'язки експертів**

5.1. Експертами є фізичні особи, які мають сертифікат на проведення експертизи або інший документ, що його заміняє, високу кваліфікацію, знання з даної галузі науки або техніки, володіють методикою науково-експертної оцінки, безпосередньо здійснюють експертизу та персонально відповідають за достовірність, повноту, об'єктивність аналізу, обґрунтованість рекомендацій відповідно до вимог завдання на проведення експертизи та чинного законодавства.

Експерти залучаються на підставі договорів або контрактів.

5.4. Експерт письмово оформляє висновок експертизи. Не допускається повторне проведення експертизи щодо конкретного проекту одним і тим самим експертом.

**6. Порядок організації та проведення експертизи**

**У який термін, як правило, повинна проводитись науково-технічна експертиза?**

**В який термін Експертна рада приймає рішення про доцільність проведення експертизи? В який термін, як правило, проводиться державна експертиза КСЗІ?**

**Який є термін дії зареєстрованої декларації?**

6.3. Термін проведення експертизи визначається замовником і, як правило, не повинен перевищувати 30 календарних днів.

**У який максимальний термін може проводитись науково-технічна експертиза?**

У разі потреби, за погодженням із замовником, термін може бути продовжений до 45 календарних днів. У виняткових випадках, залежно   
від складності проблеми, - до 90 календарних днів.

Термін проведення експертизи в кожному окремому випадку визначається договорами між виконавцями і замовниками експертизи.

**Який є термін дії висновку науково-технічної експертизи?**

6.4. Термін дії висновку експертизи визначається договором, але не перевищує 2 років від дня його видачі.

6.5. Проведення експертизи здійснюється за рахунок замовника експертизи. Сума коштів, спрямованих на проведення експертизи проектів, визначається договором на проведення експертизи, але не перевищує норми, встановлені Законом України «Про наукову і науково-технічну експертизу».

6.6. Розмір оплати експертів визначається згідно з «**Нормами оплати праці експертів, які залучаються для проведення державної наукової та науково-технічної експертиз, що проводяться за рахунок коштів державного бюджету**», затвердженими наказом Міністерства соціальної політики України від 8 травня 2013 року № 262, зареєстрованим у Міністерстві юстиції України 20 травня 2013 року за № 778/23310), або окремим договором.

6.7. Право на інтелектуальну власність, що може виникнути під час проведення експертизи, належить замовнику експертизи або визначається відповідно до договору на її проведення.

**Як називається наказ, що визначає проведення експертизи КСЗІ в ІТС?**

**Який орган виконавчої влади визначає проведення експертизи КСЗІ в ІТС?**

16 травня 2007 року наказом Адміністрації Держспецзв’язку № 93, зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087, було затверджене «**Положення про державну експертизу в сфері ТЗІ**», яке визначає такі вимоги:

**З якою метою проводиться державна експертиза в сфері ТЗІ?**

1.2. Державна експертиза в сфері ТЗІ (далі - експертиза) проводиться з метою дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо їх відповідності вимогам НД ТЗІ та можливості їх використання для забезпечення ТЗІ.

1.3. Дія цього Положення поширюється на всіх юридичних та фізичних осіб, які є суб'єктами експертизи.

Суб'єктами експертизи є:

- юридичні та фізичні особи - власники (розпорядники) ІТС, технічних і програмних засобів, які реалізують функції ТЗІ, - замовники експертизи (далі - Замовники);

- Адміністрація Держспецзв'язку (далі - Адміністрація);

- підрозділи Держспецзв'язку, підприємства, установи та організації, які проводять експертизу (далі - Організатори);

- державні органи, які проводять експертизу в сфері свого управління;

- фізичні особи - виконавці експертних робіт з ТЗІ (далі - Експерти).

**Що є об'єктами державної експертизи у сфері ТЗІ?**

1.4. Об'єктами експертизи є:

- КСЗІ, які є невід'ємною складовою частиною ІТС;

- технічні та програмні засоби, які реалізують функції ТЗІ (далі - засоби ТЗІ).

**Що таке державна експертиза КСЗІ в ІТС?**

1.5. Експертиза КСЗІ є процедурою підтвердження відповідності КСЗІ вимогам НД ТЗІ і

**Шляхом чого проводиться державна експертиза засобів ТЗІ?**

проводиться шляхом експертних випробувань або шляхом аналізу декларації про відповідність КСЗІ вимогам НД ТЗІ (далі - декларація).

Експертиза засобів ТЗІ проводиться шляхом експертних випробувань.

**Шляхом аналізу чого може проводитись експертиза КСЗІ в АС класу 1?**

**В яких АС класу 1 державна експертиза здійснюється шляхом аналізу декларації?**

1.6. Експертиза КСЗІ шляхом аналізу декларації проводиться у випадках, якщо:

- КСЗІ створено в ІТС, яка згідно з НД ТЗІ 2.5-005-99 «**Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу**» класифікована як АС класу 1 і в якій передбачається обробка інформації, що не становить державної та іншої передбаченої законом таємниці, і де використовуються засоби захисту інформації, які мають чинний сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ;

- закінчився строк дії атестата відповідності КСЗІ в ІТС вимогам НД ТЗІ (далі - Атестат), яка згідно з нормативними документами із ТЗІ класифікується як АС класу 1 і в якій передбачається обробка інформації, що не становить державної та іншої передбаченої законом таємниці.

**В яких АС класу 1 державна експертиза здійснюється шляхом експертних випробувань?**

У всіх інших випадках експертиза КСЗІ в ІТС проводиться шляхом експертних випробувань.

1.7. Експертиза може бути первинною, додатковою та контрольною.

Первинна експертиза є основним видом експертизи і передбачає виконання Організатором усіх потрібних заходів, визначених у розділі 3 цього Положення, для підготовки та прийняття рішення щодо об'єкта експертизи.

Додаткова експертиза проводиться стосовно об'єктів експертизи, щодо яких відкрилися нові наукові та науково-технічні обставини або в зв'язку з закінченням терміну дії документів, що засвідчують результати експертизи.

Контрольна експертиза проводиться іншим Організатором з ініціативи Замовника за наявністю у нього обґрунтованих претензій до висновку первинної чи додаткової експертизи або з ініціативи Адміністрації для перевірки висновку первинної чи додаткової експертизи.

**3. Порядок організації та проведення експертизи**

**В яких АС державна експертиза здійснюється шляхом експертних випробувань?**

3.1. Для проведення експертизи шляхом експертних випробувань Замовник надсилає заяву на ім'я Голови Держспецзв'язку (крім випадків, передбачених у розділі 5 цього Положення) про проведення експертизи КСЗІ в ІТС або засобу ТЗІ, а шляхом аналізу декларації –

**Які документи надсилаються до Держспецзв’язку разом з декларацією?**

декларацію про відповідність КСЗІ вимогам нормативних документів із ТЗІ (додаток 3), формуляр ІТС і акт про завершення робіт зі створення КСЗІ.

3.2. З метою розгляду декларацій і заяв, координації заходів і прийняття рішень щодо проведення експертиз в Адміністрації створюється експертна рада з питань державної експертизи у сфері технічного захисту інформації (далі - Експертна рада).

**В який строк Експертна рада приймає рішення про реєстрацію декларації?**

3.3. За результатами аналізу декларації і поданих разом із нею документів Експертна рада в місячний строк приймає рішення про реєстрацію декларації. Зареєстровану декларацію та інші подані документи Адміністрація повертає Замовнику.

3.4. У разі ненадання документів, зазначених у пункті 3.1 цього розділу, неповноти наданих у них відомостей або невідповідності порядку створення КСЗІ вимогам НД ТЗІ Адміністрація в місячний строк повертає Замовнику декларацію для доопрацювання.

3.5. Адміністрація має право в установленому порядку зупинити дію декларації або скасувати її реєстрацію

3.6. Строк дії зареєстрованої декларації є необмеженим. У разі внесення змін, не передбачених у технічному завданні на створення КСЗІ, Замовник зобов'язаний надіслати на ім'я Голови Держспецзв'язку декларацію в порядку, передбаченому в пункті 3.1 цього розділу.

3.7. За результатами розгляду заяви Експертна рада у місячний термін приймає рішення про доцільність проведення експертизи та визначає її Організатора.

3.8. У разі наявності у Замовника обґрунтованих претензій щодо порядку проведення або результатів експертизи він може звернутися до Адміністрації з пропозицією щодо здійснення контролю за проведенням Організатором експертних випробувань або із заявою на ім'я Голови Держспецзв'язку про проведення контрольної експертизи.

3.10. Основним документом, що регламентує відносини між Замовником і Організатором, є укладений між ними договір на проведення експертизи.

3.12. Результати, матеріали, висновки експертизи та створене або придбане за кошти Замовника матеріально-технічне забезпечення є його власністю, якщо інше не передбачено договором між Замовником і Організатором.

3.13. Термін проведення експертизи визначається договором і не повинен перевищувати, як правило, 6 місяців. У випадку значного обсягу експертних робіт термін проведення експертизи може бути продовжений за згодою Адміністрації та Замовника.

3.14. Список Експертів, які залучаються до виконання експертних робіт, визначається Організатором.

3.16. Організатор, за результатами аналізу наданих документів і з урахуванням загальних методик оцінювання задекларованих характеристик засобів ТЗІ і КСЗІ, формує програму і окремі методики проведення експертизи об'єкта та розробляє, у разі необхідності, порядок відбору зразків засобів ТЗІ для проведення випробувань і відповідне програмно-технічне забезпечення.

3.17. Програма проведення експертизи узгоджується із Замовником та Департаментом з питань захисту інформації в ІТС (далі – ДЗІ ІТС) Адміністрації, а окремі методики - з зазначеним департаментом.

3.18. Терміни розробки окремої методики та необхідних програмно-апаратних засобів залежать від характеру та складності об'єкта експертизи і визначаються у договорі на проведення експертизи.

3.19. Під час проведення експертизи кожний Експерт виконує експертні роботи тільки за дорученням Організатора та у відповідності з визначеною окремою методикою.

**У якому вигляді оформлюються результати роботи експертів КСЗІ?**

3.20. Результати роботи оформлюються у вигляді протоколу виконання робіт (додаток 6) за підписом Експертів, які її виконували. Протокол затверджується Організатором.

3.23. У протоколі можуть бути зафіксовані особливі думки Експертів відносно результатів виконаних робіт.

3.24. У разі виявлення невідповідності об'єкта експертизи вимогам НД ТЗІ Організатор може запропонувати Замовнику виконати доробку об'єкта.

3.26. Відомості щодо всіх доробок, а також результати додаткових експертних робіт оформлюються окремими протоколами.

3.27. Результати робіт, визначених окремою методикою, узагальнюються Організатором в Експертному висновку.

3.28. Висновки щодо кожного пункту окремої методики, а також особливі думки Експертів, зафіксовані в протоколах, включаються до Експертного висновку як складові частини без унесення до них будь-яких змін.

**Який документ складає організатор експертизи за результатами проведених робіт?**

3.29. За результатами проведених робіт Організатор складає Експертний висновок відповідного змісту щодо відповідності об'єкта експертизи вимогам НД ТЗІ, підписує його і разом із протоколами виконання робіт подає до Адміністрації.

**4. Порядок надання Експертного висновку та Атестата**

**Що видається Замовнику у разі затвердження результатів експертизи засобу ТЗІ?**

4.1. Експертний висновок на засіб ТЗІ розглядається Експертною радою і, у разі затвердження результатів експертизи, реєструється та видається Замовнику.

**Що видається Замовнику на підставі позитивного рішення щодо експертизи КСЗІ?**

4.2. На підставі позитивного рішення щодо експертизи КСЗІ Замовнику видається зареєстрований Атестат відповідності за підписом Голови Держспецзв'язку.

4.3. Адміністрація має право в установленому порядку зупинити дію або скасувати Експертний висновок або Атестат.

**5. Особливості проведення експертиз КСЗІ державними органами**

5.1. Адміністрація надає державному органу повноваження з організації та проведення первинних або додаткових експертиз КСЗІ в ІТС шляхом експертних випробувань за умови погодження з Адміністрацією порядку їх здійснення.

5.2. Державні органи, які мають дозвіл Адміністрації на проведення робіт з ТЗІ для власних потреб та отримали від Адміністрації зазначені повноваження:

- здійснюють організацію та проведення експертиз КСЗІ в ІТС у сфері свого управління шляхом експертних випробувань;

- видають Атестат відповідності, який реєструється Адміністрацією.

**Питання 3.**

19 березня 2009 року наказом Адміністрації Держспецзв'язку № 64 був затверджений «**Стандарт надання адміністративної послуги з видачі атестатів відповідності КСЗІ в ІТС вимогам НД ТЗІ**»,

**З якою метою в Адміністрації Держспецзв’язку створена Експертна рада?**

метою якого є підвищення якості надання адміністративної послуги з видачі атестатів відповідності КСЗІ в ІТС вимогам НД ТЗІ.

**Які документи додаються до заяви про проведення державної експертизи КСЗІ?**

До заяви про проведення первинної або додаткової експертизи додаються:

- технічне завдання на створення КСЗІ в ІТС;

- формуляр ІТС.

Прийняте Адміністрацією Держспецзв’язку рішення про можливість проведення експертизи КСЗІ в ІТС за заявою, поданою одержувачем, та про визначення організатора експертизи повідомляється одержувачу у термін, що не повинен перевищувати 15 робочих днів.

Атестат відповідності КСЗІ в ІТС вимогам нормативних документів з ТЗІ оформляється протягом 5 робочих днів на підставі позитивного рішення Адміністрації Держспецзв’язку щодо результатів експертизи. Зареєстрований атестат надсилається організатору експертизи для видачі одержувачу разом з експертним висновком.

Адміністративна послуга з видачі атестатів відповідності КСЗІ в ІТС вимогам НД ТЗІ надається безоплатно.

Інформація щодо порядку проведення експертизи КСЗІ в ІТС та форми заяв про проведення експертизи КСЗІ в ІТС розміщені на офіційному сайті Держспецзв’язку в мережі Інтернет (електронна адреса: *www.dsszzi.gov.ua*, розділ «Діяльність» - «Експертиза» - «Технічний захист інформації»).

1 жовтня 2010 року наказом Адміністрації Держспецзв’язку № 291 було затверджене «**Положення про Експертну раду з питань державної експертизи в сфері ТЗІ**», яка є постійно діючим колегіальним органом Адміністрації Держспецзв'язку з питань організації та проведення державної експертизи у сфері ТЗІ.

Метою діяльності Експертної ради є координація заходів з дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо їх відповідності вимогам нормативно-правових актів і НД ТЗІ та оцінювання результатів експертизи.

Формою роботи Експертної ради є засідання, які проводяться за потреби, але не рідше одного разу на місяць.

На підставі рішень Експертної ради про затвердження результатів державних експертиз оформляються, реєструються та надаються замовникам Експертні висновки на засоби ТЗІ, оформляються та видаються Атестати відповідності КСЗІ.

16 квітня 2008 року наказом Адміністрації Держспецзв'язку № 64 був затверджений «**Порядок формування Реєстру організаторів державної експертизи у сфері ТЗІ та Реєстру експертів з питань ТЗІ**»

До реєстру Організаторів вносяться всі підрозділи Держспецзв'язку, підприємства, установи та організації, визначені Експертною радою як Організатори, за результатами розгляду заяв замовників про проведення державної експертизи у сфері ТЗІ.

До реєстру Експертів вносяться всі фахівці з питань ТЗІ, які залучаються Організаторами до виконання експертних робіт під час проведення державних експертиз у сфері ТЗІ.

Картки реєстрації Організатора та Експертів зберігаються в окремій справі ДЗІ ІТС відповідно до встановлених у Держспецзв'язку вимог щодо ведення діловодства.

25 березня 2011 року наказом Адміністрації Держспецзв'язку № 65 був затверджений НД ТЗІ 2.6-001-11 «**Порядок проведення робіт з державної експертизи засобів ТЗІ від НСД та КСЗІ в ІТС**», який складається з таких основних розділів:

- вступні положення щодо порядку проведення експертизи засобів ТЗІ від несанкціонованого доступу та КСЗІ;

- опис порядку проведення робіт з експертизи засобів ТЗІ від несанкціонованого доступу;

- опис порядку проведення робіт з експертизи КСЗІ.

Він має такі додатки:

- рекомендації щодо складу та змісту проектної, експлуатаційної та нормативно-розпорядчої документації, яка надається Замовником при проведенні експертизи КСЗІ;

- вимоги щодо змісту програми проведення експертизи КСЗІ в ІТС;

- вимоги щодо змісту методики проведення експертизи КСЗІ в ІТС;

- рекомендації щодо викладення змістовної частини протоколу експертизи засобу ТЗІ від несанкціонованого доступу;

- рекомендації щодо викладення змістовної частини протоколу експертизи КСЗІ;

- рекомендації щодо викладення змістовної частини Експертного висновку за результатами експертизи засобу ТЗІ від несанкціонованого доступу

- рекомендації щодо викладення змістовної частини Експертного висновку за результатами експертизи КСЗІ.

**Етапи роботи експерта**

**З яких етапів аналізу складається робота експерта КСЗІ?**

Робота експерта КСЗІ складається з 3-х етапів аналізу:

- розроблених документів;

- проведених робіт;

- розпорядчих документів.

**1. Аналіз розроблених документів:**

- аналіз Технічного завдання на створення КСЗІ та проектної документації;

- перевірка відповідності комплекту документації на КСЗІ вимогам НД ТЗІ;

- перевірка повноти та змісту документів.

У Додатку до НД ТЗІ 2.6-001-2011 «Порядок проведення робіт з державної експертизи засобів ТЗІ від НСД та КСЗІ в ІТС» вказаний перелік документів, які повинні бути розроблені в процесі створення КСЗІ та надані Організатору експертизи для використання Експертом в процесі проведення експертизи.

При цьому в таблиці використовуються такі позначення:

- ІДТ - інформація, що становить державну таємницю; СІ - службова інформація; КІ - конфіденційна інформація, що не є власністю держави; ВІВД - відкрита інформація, що є власністю держави; ВІ - відкрита інформація, що не є власністю держави;

- «+» - 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.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№**  **з/п** | **Тип документа** | **Характеристика інформації згідно режиму доступу** | | | | | **Клас / підклас ІТС** |
| **ІДТ** | **СІ** | **КІ** | **ВІВД** | **ВІ** |
| **1.** | **Перелік інформації, що підлягає обробленню в ІТС та потребує захисту** | **+** | **+** | **+** | **+** | **+** | **1-3.xxx** |
| **2.** | **Акт категоріювання ІТС** | **+** | **+** | **+/–** | **–** | **–** | **1-3.Кxx** |
| **3.** | **Положення про службу захисту інформації** | **+** | **+** | **+** | **+** | **+** | **1-3.xxx** |
| **4.** | **Результати обстеження середовищ ІТС** | **+** | **+** | **+** | **+** | **+** | **1-3.xxx** |
| **5.** | **Опис політики безпеки інформації в ІТС** | **+** | **+** | **+** | **+** | **+** | **1-3.xxx** |
| **6.** | **Опис моделі порушника безпеки в ІТС** | **+** | **+** | **+** | **+** | **+** | **1-3.xxx** |
| **7.** | **Опис моделі загроз для інформації в ІТС** | **+** | **+** | **+** | **+** | **+** | **1-3.xxx** |
| **8.** | **Звіт за результатами аналізу ризиків та формування завдань на створення КСЗІ** | **+** | **+** | **+** | **+** | **+** | **1-3.xxx** |
| **9.** | **План захисту інформації в ІТС** | **+** | **+** | **+** | **+** | **+** | **1-3.xxx** |
| **10.** | **Технічне завдання на створення КСЗІ в ІТС** | **+** | **+** | **+** | **+** | **+** | **1-3.xxx** |
| **11.** | **Інструкції щодо забезпечення правил оброблення ІзОД в ІТС** | **+** | **+** | **–** | **–** | **–** | **1-3.Кxx** |
| **12.** | **Інструкції співробітників СЗІ, персоналу та користувачів ІТС** | **+** | **+** | **+** | **+** | **+** | **1-3.xxx** |
| **13.** | **Технологічні інструкції щодо адміністрування та обслуговування КСЗІ** | **+** | **+** | **+** | **+** | **+** | **1-3.xxx** |
| **14.** | **Інструкції про порядок використання засобів КЗІ** | **+** | **+** | **+** | **+** | **+** | **1-3.Кxx**  **1-3.xЦx** |
| **15.** | **Журнали обліку сховищ і матеріальних носіїв ІзОД** | **+** | **+** | **–** | **–** | **–** | **1-3.Кxx** |

**2. Аналіз проведених робіт:**

- перевірка реальних умов експлуатації;

- перевірка відповідності реально встановлених засобів ІТС та інших технічних засобів та систем вказаним в Акті обстеження;

- перевірка впроваджених заходів захисту інформації;

- перевірка виконання вимог щодо функціонування системи антивірусного захисту.

На цьому етапі Експерт вимагає від Замовника та перевіряє:

- специфікації апаратних та апаратно-програмних засобів ІТС;

- опис програмного забезпечення з номерами ліцензій та підтвердженням, що ПЗ придбане без порушення авторських прав, (підтвердити рахунками-фактурами, ліцензіями (паспортами), серійними номерами). На встановлене антивірусне програмне забезпечення робочих станцій, серверів Замовник повинен надати експертні висновки Адміністрації Держспецзв’язку та підтвердити, що оновлення баз даних проводиться у відповідності до вимог НД ТЗІ;

- відповідність КЗЗ від НСД з визначеним рівнем гарантії вимогам НД ТЗІ у обсязі функцій, сукупність яких визначається ФПЗ та наявність експертного висновку Адміністрації Держспецзв’язку.

**3. Аналіз розпорядчих документів:**

- перевірка наявності відповідних наказів керівника Замовника на різних етапах створення та впровадження КСЗІ;

- перевірка наявності інструкцій, які регламентують функціонування КСЗІ в АС.

На цьому етапі Експерт перевіряє:

- наказ про проведення робіт зі створення КСЗІ на ОІД з висновками щодо обмеження грифу обмеження доступу до інформації, що обробляється в АС та призначення відповідальних осіб;

- наказ щодо створення служби захисту інформації;

- наказ про створення комісії з проведення випробувань КСЗІ в АС;

- наказ про забезпечення захисту інформації в АС;

- наказ про введення АС в дослідну експлуатацію тощо;

- інструкцію про порядок введення в експлуатацію КСЗІ в АС;

- інструкцію про порядок модернізації КСЗІ в АС;

- інструкцію системному адміністратору;

- інструкцію адміністратору безпеки при роботі в АС;

- інструкцію користувачу.

Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. Якщо в силу якихось причин усунути недоліки в ході експертизи неможливо, Організатор може запропонувати Замовнику виконати доробку об’єкта. Термін доробки об’єкта експертизи визначається спільним протоколом або додатковою угодою до договору між Замовником та Організатором. Відомості щодо всіх доробок, а також результати додаткових експертних робіт оформлюються окремими протоколами. Після завершення передбачених актом робіт проводиться повторна експертиза.

Для інтегрованих ІТС може проводитись державна експертиза кожної складової частини (модуля) КСЗІ окремо. Державна експертиза КСЗІ інтегрованої ІТС полягає у перевірці взаємодії (адміністрування, обміну даними бази даних захисту тощо) вже оцінених модулів. Документи, що містять результати робіт кожного з етапів (протоколи, акти, атестати відповідності) для КСЗІ ІТС в цілому, оформлюються з урахуванням відповідних документів на складові частини КСЗІ.

Результати робіт, визначених методикою, узагальнюються Організатором в Експертному висновку. Висновки щодо кожного пункту методики, а також особлива думка Експерта, зафіксовані в протоколах, включаються до Експертного висновку як складові частини без унесення до них будь-яких змін.

Ким затверджується протокол виконання робіт експертів КСЗІ?

За результатами проведених робіт Організатор складає Експертний висновок щодо відповідності об’єкта експертизи вимогам нормативних документів з ТЗІ, підписує його і разом із протоколами виконання робіт подає до Адміністрації.

На підставі позитивного рішення щодо експертизи КСЗІ Замовнику безоплатно видається зареєстрований Атестат відповідності за підписом Голови Держспецзв’язку згідно вимог «Переліку адміністративних послуг, які безоплатно надаються Адміністрацією Держспецзв'язку», затвердженого наказом Адміністрації Держспецзв'язку від 29.11.2011 № 350, зареєстрованого в Міністерстві юстиції України 15.12.2011 за № 1455/20193.

**Після чого в ІТС можна обробляти ІзОД?**

Згідно вимог п.1.6 Стандарту термін дії Атестату відповідності

Який є термін дії Атестату відповідності КСЗІ в ІТС?

становить 5 років. Отримання Атестату фіксується відповідним записом у формулярі ІТС. Атестат відповідності

**Що є підставою для Замовника видати наказ про введення КСЗІ в постійну експлуатацію?**

є підставою для Замовника видати наказ про введення КСЗІ в ІТС в постійну експлуатацію, після чого в ІТС можна обробляти ІзОД.

**Особливості проведення експертизи шляхом декларації**

Шляхом аналізу декларації може проводитися державна експертиза КСЗІ в ІТС, яка складається з декількох компонентів, які організаційно поєднані в одну систему (окремих АРМ, які призначені для вирішення одного й того самого завдання, але функціонують автономно) і вимоги до захисту інформації від НСД кожної компоненти висуваються як для АС.

Процедурою державної експертизи шляхом аналізу декларації можуть скористатися будь-які суб’єкти: органи державної влади, місцевого самоврядування, установи, підприємства та організації незалежно від форми власності та підпорядкування, фізичні та юридичні особи (далі – установа).

Запровадження декларативного механізму проведення державної експертизи КСЗІ не зачіпає правових норм, що стосуються визначення вимог, організації робіт та порядку створення КСЗІ, не вносить жодних змін до порядку виконання робіт зі створення КСЗІ.

Декларація подається після завершення всіх робіт зі створення КСЗІ у повному обсязі і відображення їх результатів у Формулярі АС і Акті про завершення робіт зі створення КСЗІ, які повинні підтверджувати факт виконання всіх основних етапів та дотримання встановленого порядку виконання робіт.

Під словами «*всіх основних етапів робіт*» згідно вимог НД ТЗІ 3.7-003-05 розуміється, що мають бути виконані роботи з визначення й оцінки загроз для інформації, формування вимог, розроблення й реалізації проекту КСЗІ, проведення випробувань КСЗІ та введення КСЗІ в експлуатацію у складі АС.

Типові форми «Формуляру АС» і «Акту про завершення робіт зі створення КСЗІ в АС класу 1» розміщені на сайті Держспецзв'язку за адресою: *http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art\_id=105603*

Розділи формуляра мають бути заповнені відповідними відомостями з посиланням на технічні або розпорядчі документи (протоколи, акти тощо) установи з їх реєстраційними номерами, згідно з якими виконувалися або в яких зафіксовано результати виконання тих чи інших робіт. Наприклад, це може бути наказ установи про створення служби захисту інформації чи призначення відповідальних осіб за забезпечення захисту інформації в АС, акт (протокол, звіт тощо) про проведення власником АС випробувань КСЗІ, ТЗ на створення КСЗІ, техноробочий проект КСЗІ, опис КСЗІ, модель загроз для інформації тощо. Зазначаються випадки інтегрування декількох документів, що мають самостійне значення, в один документ.

До формуляра вносяться також відомості про проведення робіт із технічного обслуговування, модернізації КСЗІ, внесення інших змін до АС-1, які не впливають на технічні характеристики функціонування КСЗІ (наприклад, заміна окремих технічних засобів чи засобів обробки інформації іншими, нові призначення відповідальних осіб, зміна назви АС, місця розташування, адреси тощо).

Усі графи декларації мають бути заповнені.

До декларації вносяться відомості про повну назву установи-власника (розпорядника) ІТС, посаду, прізвище, ім’я та по батькові особи, що підписує декларацію (керівника установи), повну назву ІТС, в якій декларується створення і впровадження КСЗІ.

До декларації вноситься перелік назв з реєстраційними атрибутами розпорядчих, проектних і експлуатаційних документів (накази про призначення і виконання певних робіт, технічне завдання на створення КСЗІ, техно-робочий проект КСЗІ, опис КСЗІ, модель загроз для інформації, інструкції з експлуатації для адміністратора та користувача ІТС, інструкції з налаштування засобів захисту інформації тощо).

У графі «вид інформації за порядком доступу» вказується один або декілька видів інформації, які обробляються в ІТС (відкрита, конфіденційна, службова, персональні дані, інший вид інформації, вимога щодо захисту якої встановлена законом).

У графах з даними технічного завдання, проектних та експлуатаційних документів вказуються їх повні назви, реєстраційні атрибути, а також умовні позначення згідно з державним стандартом **ГОСТ 34.201-89** «**Виды, комплектность и обозначение документов при создании автоматизированных систем**» (у разі наявності).

Якщо документ потребує погодження з уповноваженим органом, зазначається назва органу, дата погодження, прізвище посадової особи, що його погодила.

Має бути документально підтверджено виконання обов’язкових вимог, установлених «Правилами забезпечення захисту інформації в ІТС», а також дотримання критерію щодо використання засобів захисту інформації, які мають чинний сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ.

Використання засобу захисту інформації з функціями розмежування доступу (наприклад, сервіси безпеки «Windows», КЗЗ «Лоза», «Гриф» тощо), який має чинний на момент подання декларації позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ, документально підтверджується відповідним записом у формулярі АС (вказати номер і дату експертного висновку, заводський номер і дату виготовлення впровадженого зразка засобу). Якщо у складі КСЗІ використовується засіб, термін дії експертного висновку якого закінчився, то необхідно додатково до запису у формулярі надати документ, який підтверджує легітимність засобу на момент його купівлі.

**У якому документі треба зробити запис про отримання Атестату відповідності?**

Формуляр повинен містити запис про впровадження антивірусних програм, які мають підтвердження відповідності. Застосування антивірусних засобів аналогічне тому, що і для засобів розмежування доступу.

Необхідно вказати реквізити розпорядчого документа установи, згідно з яким утворено службу захисту інформації або призначено відповідальних осіб.

Незаповнені графи у декларації та формулярі АС, відсутність висновків про позитивні результати впровадження заходів в акті завершення робіт зі створення КСЗІ, невідповідність наданих відомостей у різних документах, недостовірність відомостей є підставою для відмови у реєстрації декларації.

Адміністрація Держспецзв’язку не втручається у процес підготовки декларації, тому процес підготовки контролюється виключно власником (розпорядником) АС і тільки він є відповідальним за правильність оформлення та комплексність документів, достовірність поданих у декларації відомостей. Адміністрація Держспецзв’язку на прохання суб’єкта може тільки (і повинна) надавати необхідну консультативну та методичну допомогу з питань створення КСЗІ, оформлення результатів виконаних робіт, заповнення тексту декларації тощо.

Декларація складається власником (розпорядником) АС у 2-х примірниках і надсилається разом із «Формуляром АС» та «Актом про завершення робіт зі створення КСЗІ в АС» до Адміністрації Держспецзв’язку. Розгляд декларацій здійснюється Департаментом ТЗІ Адміністрації, яким перевіряється правильність заповнення декларації та дотримання відповідності порядку створення КСЗІ нормативним документам. Якщо декларація відповідає встановленим вимогам оригінал декларації реєструється Адміністрацією, кожен аркуш на звороті візується відповідальним співробітником зазначеного департаменту. Оригінал декларації, формуляр АС та акт завершення робіт зі створення КСЗІ повертається замовнику. Копія декларації залишається в Адміністрації Держспецзв’язку.

Процедура аналізу декларації Адміністрацією Держспецзв’язку є прозорою, ґрунтується на аналізі документів, визначених у Положенні, і не потребує додаткових перевірок упроваджених на об’єкті експертизи заходів і засобів захисту.

Зареєстрована декларація має таку ж саму правову силу, що і атестат відповідності, є законним документом, що підтверджує відповідність створеної КСЗІ в АС.

Відповідальність за достовірність внесених до декларації відомостей відповідно до статті 16 Закону України «**Про підтвердження відповідності**» несе подавець декларації.

Строк дії декларації не обмежений. Декларація зберігає свою чинність до того часу, доки внесені до неї відомості є достовірними. Зокрема, до втрати достовірності відомостей декларації може призводити модернізація КСЗІ, якщо вносяться зміни, які впливають на політику безпеку інформації. Наприклад, це може бути зміна видів об’єктів захисту, моделі загроз, ролей користувачів, правил розмежування доступу чи обраного для їх реалізації комплексу засобів захисту тощо.

У цьому разі власник (розпорядник) АС повинен задокументувати виконані роботи, внести відповідні відомості до декларації. Складена декларація надсилається до Адміністрації Держспецзв’язку для реєстрації. Розгляд та реєстрація складеної нової декларації здійснюється у тому ж порядку, що і під час первинної реєстрації. Власник (розпорядник) АС надсилає до Адміністрації Держспецзв’язку разом із складеною новою декларацією акт про завершення робіт зі створення КСЗІ, формуляр АС, оригінал чинної декларації. У супровідному листі вказуються причини подання нової декларації та заявляється необхідність скасування реєстрації чинної декларації.

Оригінал скасованої декларації повертається подавцю з відміткою «Скасовано», номером та датою рішення про скасування.

**Які реєстри формує та веде Адміністрація Держспецзв’язку?**

Адміністрація Держспецзв’язку має право перевіряти дотримання вимог НД ТЗІ під час експлуатації АС, КСЗІ яких мають зареєстровані декларації, та у разі виявлення порушень скасовувати їх реєстрацію або зупиняти дію до усунення цих порушень.

**Контрольні питання**

Який нормативний акт визначає правові основи експертної діяльності в науково-технічній сфері?

Хто є суб'єктами експертизи згідно закону України?

Що формують замовники експертизи згідно закону України?

Що забезпечують замовники експертизи згідно закону України?

Що роблять організатори експертизи згідно закону України?

На підставі чого організатори експертизи проводять її згідно закону України?

Які органи та установи проводять державну експертизу згідно закону України?

На які експертизи можуть передаватися об'єкти експертизи згідно закону України?

Стосовно яких об'єктів проводиться додаткова експертиза згідно закону України?

Для чого здійснюється контрольна експертиза згідно закону України?

Що є основним юридичним документом, що регламентує відносини між замовником і організатором у сфері експертизи згідно закону України?

Як називається наказ, що встановлює вимоги до проведення науково-технічної експертизи?

У якому разі науково-технічна експертиза набуває статусу державної?

Що подає замовник науково-технічної експертизи до організатора експертизи?

У який термін, як правило, повинна проводитись науково-технічна експертиза?

У який максимальний термін може проводитись науково-технічна експертиза?

Який є термін дії висновку науково-технічної експертизи?

Як називається наказ, що визначає проведення експертизи КСЗІ в ІТС?

Який орган виконавчої влади визначає проведення експертизи КСЗІ в ІТС?

З якою метою проводиться державна експертиза в сфері ТЗІ?

Що є об'єктами державної експертизи у сфері ТЗІ?

Що таке державна експертиза КСЗІ в ІТС?

Шляхом чого проводиться державна експертиза засобів ТЗІ?

Шляхом аналізу чого може проводитись експертиза КСЗІ в АС класу 1?

В яких АС класу 1державна експертиза здійснюється шляхом аналізу декларації?

В яких АС класу 1державна експертиза здійснюється шляхом експертних випробувань?

В яких АС державна експертиза здійснюється шляхом експертних випробувань?

Які документи надсилаються до Держспецзв’язку разом з декларацією?

З якою метою в Адміністрації Держспецзв’язку створена Експертна рада?

В який строк Експертна рада приймає рішення про реєстрацію декларації?

Який є термін дії зареєстрованої декларації?

В який термін Експертна рада приймає рішення про доцільність проведення експертизи?

В який термін, як правило, проводиться державна експертиза КСЗІ?

У якому вигляді оформлюються результати роботи експертів КСЗІ?

Ким затверджується протокол виконання робіт експертів КСЗІ?

Який документ складає організатор експертизи за результатами проведених робіт?

Що видається Замовнику у разі затвердження результатів експертизи засобу ТЗІ?

Що видається Замовнику на підставі позитивного рішення щодо експертизи КСЗІ?

Які документи додаються до заяви про проведення державної експертизи КСЗІ?

З яких етапів аналізу складається робота експерта КСЗІ?

Який є термін дії Атестату відповідності КСЗІ в ІТС?

Скільки коштує Замовнику Атестат відповідності КСЗІ в ІТС?

У якому документі треба зробити запис про отримання Атестату відповідності?

Що є підставою для Замовника видати наказ про введення КСЗІ в постійну експлуатацію?

Після чого в ІТС можна обробляти ІзОД?

Які реєстри формує та веде Адміністрація Держспецзв’язку?