**Заняття 3. Прийняття рішення про створення систем захисту інформації.**

**Вступ.**

**Питання 1. Обґрунтування необхідності створення КСЗІ.**

**Питання 2. Категоріювання ІТС.**

**Питання 3. Обстеження середовищ функціонування ІТС, документування результатів.**

**Контрольні питання.**

**Вступ.**

Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов’язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;

- визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;

- оцінки можливих переваг (фінансово-економічних, соціальних тощо) експлуатації ІТС у разі створення КСЗІ.

На підставі НД ТЗІ 2.5-005-99 «Класифікація АС і стандартні функціональні профілі захищеності оброблюваної інформації від НСД» за сукупністю характеристик ІТС виділено три ієрархічні класи, вимоги до функціонального складу КЗЗ яких істотно відрізняються.

Клас «1» - одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності. Особливості такого класу:

- в кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка оброблюється;

- технічні засоби (носії інформації і засоби У/В ) з точки зору захищеності відносяться до однієї категорії і всі можуть використовуватись для збереження і У/В всієї інформації.

Приклад - автономна ПЕОМ, доступ до якої контролюється з використанням організаційних заходів.

Клас «2» - локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності. Істотна відміна від попереднього класу - наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності. Приклад - ЛОМ.

Клас «3» - розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності. Істотна відміна від попереднього класу - необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки. Приклад - глобальна мережа.

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ. Після прийняття такого рішення відповідальний за ТЗІ організації-власника (розпорядника) ІТС готує для керівника організації 3 накази:

1) про створення Служби захисту інформації в ІТС (далі - СЗІ), порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000 «Типове положення про СЗІ в АС»;

2) про призначення комісії з категоріювання ІТС, завдання та повноваження якої визначено в НД ТЗІ 1.6-005-2013 «Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці»;

3) про призначення комісії з обстеження середовищ функціонування ІТС, завдання та повноваження якої визначено в ДСТУ 3396.1-96 «Технічний захист інформації. Порядок проведення робіт».

До складу СЗІ, який визначається наказом, повинні призначатися фахівці з таких питань:

захисту інформації від витоку технічними каналами;

захисту каналів зв’язку і комутаційного обладнання,

налагодження і адміністрування засобів захисту інформації,

керування базами даних захисту інформації;

налагодження і керування активним мережевим обладнанням;

захищених технологій обробки інформації.

За функціональними обов’язками особовий склад СЗІ складається з таких спеціалістів (за рівнем ієрархії):

системний адміністратор ІТС;

мережевий адміністратор ІТС;

адміністратор безпеки інформації в ІТС;

адміністратор КСЗІ в ІТС.

Після призначення СЗІ її керівник складає «Положення про СЗІ в ІТС», що має бути оформлене у вигляді окремого документа згідно рекомендацій НД ТЗІ 1.4-001-2000 та затверджене керівником організації-власника (розпорядника) ІТС.

Положення повинно складатись з таких розділів:

загальні положення;

завдання СЗІ;

функції СЗІ;

повноваження та відповідальність СЗІ;

- взаємодія СЗІ з іншими підрозділами організації та зовнішніми підприємствами, установами, організаціями;

штатний розклад та структура СЗІ;

організація та фінансування робіт СЗІ.

В залежності від конкретних завдань і умов функціонування СЗІ дозволяється, у разі необхідності, поєднувати окремі розділи в один, вводити нові розділи або вилучати розділи, що не є актуальними.

До Положення у вигляді додатків можуть включатися нормативні документи, таблиці, схеми, графіки, необхідні для визначення заходів захисту інформації, плани об’єктів захисту з вказанням робочих місць та встановлених на них технічних засобів передачі, прийому, зберігання, обробки інформації, що підлягає захисту, та інші документи.

Положення має бути погоджене з юрисконсультом та керівниками підрозділів (служби безпеки, РСО, підрозділу ТЗІ) організації.

Зміни суттєвого характеру вносяться до Положення на підставі наказу керівника організації (підрозділу, до якого структурно входить СЗІ).

**Питання 2.**

Об’єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься ІзОД, підлягають обов’язковому категоріюванню. Об’єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься тільки відкрита інформація, категоріюванню не підлягають.

Об’єктами категоріювання є об’єкти інформаційної діяльності (далі - ОІД), в тому числі об’єкти електронно-обчислювальної техніки (далі - ЕОТ) ІТС. ОІД - це інженерно-технічна споруда (приміщення), транспортний засіб, де здійснюється озвучення та/або обробка технічними засобами ІзОД.

Категоріювання ІТС здійснюється комісією організації-власника (розпорядника) ІТС для визначення необхідного рівня захисту інформації, що обробляється на об’єктах ЕОТ ІТС. Категоріювання здійснюється за ознакою ступеня обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД.

Згідно ТПКО-95 «Тимчасове положення про категоріювання об'єктів» установлюються 4 категорії об'єктів, на яких обробляється технічними засобами та/або озвучується ІзОД, що:

- становить державну таємницю, для якої встановлено гриф секретності «особливої важливості» - перша (І);

- становить державну таємницю, для якої встановлено гриф секретності «цілком таємно» - друга (ІІ);

- становить державну таємницю, для якої встановлено гриф секретності «таємно», а також інформація, що містить відомості, які становлять іншу передбачену законом таємницю - третя (ІІІ);

- не становить державної таємниці - четверта (ІV).

Категоріювання ОІД четвертої категорії здійснюється згідно вимог НД ТЗІ 1.6-005-2013 «Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці».

Категоріювання може бути первинним, черговим або позачерговим. Первинне категоріювання здійснюється у разі створення ІТС, де буде оброблятися ІзОД. Чергове - не рідше ніж один раз на 5 років. Позачергове - у разі зміни ознаки, за якою була встановлена категорія ІТС.

Комісія з категоріювання визначає ступень обмеження доступу до інформації, яка оброблятиметься в ІТС, та з урахуванням цього ступеня встановлює категорію ІТС. Встановлена категорія зазначається в Акті категоріювання ІТС, який складається комісією за результатами її роботи. Акт категоріювання є чинним протягом 5 років з моменту проведення категоріювання, якщо не змінилась ознака, за якою була встановлена категорія об’єкта.

В акті зазначається:

1. Підстава для категоріювання (рішення про створення КСЗІ, закінчення терміну дії акта категоріювання, зміна ознаки, за якою була встановлена категорія, та реквізити наказу про призначення комісії з категоріювання.

2. Вид категоріювання: первинне, чергове, позачергове (у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання, та реквізити акту, яким було встановлено цю категорію).

3. В ІТС здійснюється обробка ІзОД.

4. Ступінь обмеження доступу до ІзОД, що обробляється в ІТС (передбачена законом таємниця; службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, інша конфіденційна інформація, вимога щодо захисту якої встановлена законом).

5. Встановлена комісією категорія.

ІТС, яким комісія встановила відповідну категорію, вносяться до «Переліку категорійованих об’єктів», який ведеться власником (розпорядником, користувачем) ОІД.

**Питання 3.**

Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

При обстеженні обчислювального середовища ІТС повинні бути проаналізовані й описані:

обладнання - ЕОМ та їхні складові частини (процесори, монітори, термінали, робочі станції та ін.), периферійні пристрої;

програмне забезпечення - вихідні, завантажувальні модулі, утиліти, СКБД, операційні системи та інші системні програми, діагностичні і тестові програми тощо;

- види і характеристики каналів зв'язку;

- особливості взаємодії окремих компонентів, їх взаємний вплив один на одного, можливі обмеження щодо використання засобів тощо.

Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням тощо.

Повинні бути зафіксовані всі активні і пасивні об’єкти, які беруть участь у технологічному процесі обробки і тим чи іншим чином впливають на безпеку інформації. Для кожного активного об’єкту ІТС має бути визначено перелік пасивних об’єктів, які з ним взаємодіють.

Окрім компонентів ІТС, необхідно дати опис технології обробки інформації в ІТС, що потребує захисту, тобто способів і методів застосування засобів обчислювальної техніки під час виконання функцій збору, зберігання, обробки, передачі і використання даних, або алгоритмів окремих процедур.

При цьому рекомендується розробити структурну схему інформаційних потоків в ІТС, яка б відображала інформаційну взаємодію між основними компонентами ІТС (завданнями, об’єктами) з прив’язкою до кожного елемента схеми категорій інформації та визначених політикою безпеки рівнів доступу до неї.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

При обстеженні інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІТС. Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, за типом їхнього представлення в ІТС, визначені й описані види її представлення в ІТС. Класифікація є підставою для визначення власником (розпорядником) інформації або ІТС методів і способів захисту кожного окремого виду інформації.

За режимом доступу інформація в АС має бути поділена на відкриту та з обмеженим доступом. Відкриту інформацію слід поділити на відкриту, яка не потребує захисту, або захист якої забезпечувати недоцільно, та відкриту, яка такого захисту потребує. До другої слід відносити інформацію, важливу для особи, суспільства і держави (відповідно до Концепції технічного захисту інформації в Україні), важливі для організації відомості, порушення цілісності або доступності яких може призвести до моральних чи матеріальних збитків.

За правовим режимом інформація з обмеженим доступом повинна бути поділена на таємну, службову та конфіденційну. До таємної інформації має бути віднесена інформація, що містить відомості, які становлять державну, а також іншу, передбачену законом таємницю. Правила доступу до службової та конфіденційної інформації, во­ло­діти, ко­ри­стувати­ся чи ро­з­по­ря­джати­ся якою можуть ок­ре­мі фі­зи­ч­ні, юри­ди­ч­ні осо­би або де­р­жа­ва, встановлює законодавство та її власник.

Конфіденційна інформація може мати велику цінність для її власника, втрата або передача якої іншим особам може завдати організації (власнику) значних збитків. З метою встановлення правил розмежування доступу до конфіденційної інформації необхідно класифікувати її, поділивши на декілька категорій за ступенем цінності (критерії розподілу можуть бути визначені під час оцінки ризиків).

Для встановлення правил взаємодії активних і пасивних об’єктів ІТС інформація повинна бути класифікована за типом її представлення в ІТС (для кожної з визначених категорій встановлюються типи пасивних об’єктів комп’ютерної системи, якими вона може бути представлена). Для кожного виду інформації і типу об’єкта, в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність) чи ІТС (спостереженість), яким вони повинні задовольняти.

Аналіз технології обробки інформації повинен виявити особливості обігу електронних документів, мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та місця їх призначення, принципи та методи керування інформаційними потоками, складені структурні схеми потоків. Фіксуються види носіїв інформації та порядок їх використання під час функціонування ІТС.

Для кожного структурного елемента схеми інформаційних потоків фіксуються склад інформаційних об’єктів, режим доступу до них, можливий вплив на нього (елементу) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.

За результатами обстеження інформаційного середовища складається «Перелік інформації, що підлягає автоматизованому обробленню в ІТС і потребує захисту», який оформлюється як окремий документ, затверджений керівником організації-власника (розпорядника) відповідної інформації, або як розділ у інших документах (Політика безпеки, План захисту, Технічне завдання на створення КСЗІ тощо).

У переліку має бути наведено перелік інформаційних ресурсів (видів інформації), що підлягають обробленню в ІТС, класифікований за такими ознаками:

назва 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 373 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 АС» або «Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію».

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.

При обстеженні користувацького середовища здійснюється аналіз:

- функціонального та кількісного складу користувачів, їхніх функціональних обов’язків та рівня кваліфікації;

- повноважень користувачів щодо допуску до відомостей, які обробляються в ІТС, доступу до ІТС та її окремих компонентів;

- повноважень користувачів щодо управління КСЗІ;

- рівня можливостей різних категорій користувачів, що надаються (можуть бути доступними) їм засобами ІТС.

За результатами обстеження вище зазначених середовищ складається «Формуляр ІТС», який оформлюється як окремий документ і складається з таких розділів:

- загальні відомості про ІТС;

- склад технічних засобів ІТС;

- склад програмного забезпечення;

- відомості про програмно-апаратний КЗЗ від НСД;

- відомості про впровадження, випробування та приймання в експлуатацію;

- посадові особи, відповідальні за технічне обслуговування;

- посадові особи, відповідальні за забезпечення захисту інформації;

- реєстрація проведених робіт (технічне обслуговування, ремонт, модернізація тощо);

- відмітки про проведення перевірок КСЗІ;

- перелік технічних та експлуатаційних документів КСЗІ.

Формуляр ІТС готується згідно з вимогами до його змісту, встановленими керівним документом із стандартизації РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов». 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 ІТС, акт (протокол, звіт тощо) про проведення власником ІТС випробувань КСЗІ, технічне завдання на створення КСЗІ, технічний чи техно-робочий проект КСЗІ, опис КСЗІ, модель загроз для інформації тощо. Зазначаються випадки інтегрування декількох документів, що мають самостійне значення, в один документ.

Бланк «Формуляру АС» можна побачити на сайті Держспецзв’язку:

<http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=105603>

У разі обробки в ІТС інформації, що становить державну таємницю, обов’язково здійснюється також обстеження фізичного середовища, під час якого аналізується взаємне розміщення засобів обробки інформації ІТС на ОІД, комунікацій, систем життєзабезпечення і зв’язку, а також режим функціонування цих об’єктів.

Порядок проведення обстеження повинен відповідати ДСТУ 3396.1-96 «Технічний захист інформації. Порядок проведення робіт», а в частині, що стосується захисту інформації від витоку технічними каналами, - НД ТЗІ 3.1-001-07 «Створення комплексу технічного захисту інформації. Передпроектні роботи».

Аналізу підлягають такі характеристики фізичного середовища:

- характеристика об’єктів, де розташовані компоненти ІТС (дані про інженерно-технічну споруду, її частину або декілька споруд, приміщення тощо);

- архітектурно-будівельні особливості приміщень: огороджувальні будівельні конструкції: стеля, підлога, стіни, перегородки (матеріал, товщина); підвісна стеля (конструкція, матеріал); вікна, двері, інші отвори (кількість, матеріал, розміри).

- дані про складові об’єктів, що можуть впливати на показники ефективності захищеності ІзОД і які можуть бути середовищем поширення за межі КЗ її носіїв (інженерні комунікації, обладнання, оргтехніка, телебачення, електроживлення, заземлення, газо-, водопостачання, опалення, вентиляції, кондиціонування повітря, водостоку, каналізації, технологічне обладнання, огороджувальні будівельні конструкції, світлопроникні отвори приміщень, будинків, споруд тощо).

- наявність систем безпеки в установі, до яких може бути інтегрована КСЗІ (відеоспостереження, пожежна та охоронна сигналізації, системи зв’язку);

- схеми розміщення комунікацій, обладнання систем електроживлення, у тому числі трансформаторної підстанції;

- дані про складові об’єктів, які виходять за межу КЗ або її перетинають, застосування яких не обґрунтовано виробничою необхідністю і які підлягають демонтуванню, у подальшому застосуванні яких відсутня необхідність);

- опис систем заземлення (дані про перелік технічних засобів ІТС, що підлягають заземленню);

- результати аналізу фізичного середовища та пропозиції щодо необхідності отримання додаткових даних про можливі місця розміщення засобів технічної розвідки; проведення випробувань (у т.ч. спеціальних досліджень технічних засобів, які оброблятимуть ІзОД); застосування організаційних, інженерно-технічних заходів захисту (у т.ч. застосування засобів оброблення ІзОД, інших технічних засобів у захищеному виконанні).

За результатами комісія складає «Акт обстеження середовищ функціонування ІТС», який затверджується керівником організації-власника (розпорядника) ІТС і складається з таких розділів:

- клас і склад обчислювальної системи,

- перелік і характеристики інформаційних ресурсів,

- перелік і повноваження користувачів,

- опис фізичного середовища (до акту додаються генеральний і ситуаційний плани, схеми систем життєзабезпечення та заземлення).

**Контрольні питання**

Скільки ієрархічних класів має автоматизована система згідно НД ТЗІ?

Що таке автоматизована система класу «1»?

Що таке автоматизована система класу «2»?

Що таке автоматизована система класу «3»?

Який документ складає СЗІ після свого призначення?

Що таке об’єкт інформаційної діяльності?

Яку назву має нормативний документ, який визначає категорії ОІД?

За якою ознакою здійснюється категоріювання ОІД?

Які об’єкти підлягають обов’язковому категоріюванню?

Скільки є категорій об’єктів інформаційної діяльності?

Яка ІзОД відноситься до першої категорії?

Яка ІзОД відноситься до другої категорії?

Яка ІзОД відноситься до третьої категорії?

Яка ІзОД відноситься до четвертої категорії?

Яким може бути категоріювання?

Через скільки років здійснюється чергове категоріювання?

У якому разі здійснюється позачергове категоріювання?

Які середовища ІТС підлягають обстеженню?

З чого складається обчислювальне середовище?

Який документ складається за результатами обстеження інформаційного середовища?

Який експлуатаційний документ складається за результатами обстеження обчислювального, інформаційного та користувацького середовищ?

Який підсумковий документ складається за результатами обстеження всіх середовищ?

У якому разі здійснюється обов’язкове обстеження фізичного середовища ІТС?