УДК 004.056.5

д.т.н., проф. **Оксіюк О.Г.** (КНУ)
Шестак Я.В. (КНУ)

МЕТОДОЛОГІЯ РОЗРОБКИ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Розглядається методологія створєння комплексної системи захисту інформації відповідно до вимог законодавства України. Наведено порядок та етапи створення комплексної системи захисту інформації в інформаційно-телекомунікаційних системах.

Розглядаються основні проблемні питання, пов'язані зі створенням комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Обґрунтовані та запропоновані шляхи, основні завдання та рекомендації з вирішення досліджених проблем створення комплексів технічного захисту інформації. Розглядається порядок здійснення заходів та засобів при створенні комплексних систем захисту інформації в сучасних інформаційно-телекомунікаційних системах.

Аналізуються і класифікуються можливі загрози безпеки інформації, розглядаються методи і засоби захисту від несанкціонованого доступу до інформації, розкриваються підходи до побудови і експлуатації комплексних систем захисту

Ключові слова: комплексна система захисту інформації, інформація з обмеженим доступом, автоматизована система, інформаційно-телекомунікаційна система.

Інформація, будучи продуктом діяльності, виступає як власність держави, підприємств, установ, організацій та громадян, і, як об'єкт власності, вимагає захищеності. Проте проблема захисту інформації не зводиться тільки до захисту прав її власників, але і містить в собі такий важливий аспект, як захист прав громадян на вільний доступ до відомостей, гарантований Конституцією. Основи захисту інформації розробляються органами державної

влади, виходячи з умов забезпечення інформаційної безпеки зокрема і національної безпеки України в цілому. Відповідно до ст. 20, 21 Закону України "Про інформацію", вся інформація за порядком доступу поділяється на відкриту та інформацію з обмеженим доступом (ІзОД). ІзОД є конфіденційна, таємна та службова інформація [1]. Такий розподіл по режимах доступу здійснюється виняткова на підставі ступеня конфіденційності інформації. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб' єктів владних повноважень [1].

Оскільки в умовах інформатизації країни [2], розвитку інформаційних технологій, інформаційні ресурси (сукупність документів у інформаційних системах [2]) формуються у всіх сферах діяльності, і насамперед: в політичній, військовій, економічній, науково-технічній, тому інформаційну безпеку слід розглядати як комплексний показник національної безпеки. Цим визначається її важливе місце і одна з провідних ролей в системі національної безпеки країни в сучасних умовах [3].

Згідно із Законом України "Про захист персональних даних" об'єктами захисту є персональні дані, які обробляються в базах персональних даних. Персональні дані за режимом доступу є ІзОД [4]. Відповідно до ст. 8 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" "Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством".

Відповідно до вимог законодавства України [1-4,6-8], для забезпечення конфіденційності, доступності, цілісності та спостереженості зазначеної інформації в кожній автоматизованій системі (АС) має створюватися комплексна система захисту інформації (КСЗІ).

Над вирішенням проблем у сфері захисту інформації, в автоматизованій системі працюють сучасні дослідники, такі як В.А. Хорошко, С.В. Ленков, Д.А.Перегудов та ін. Освітлені загальні питання теорії захисту інформації, а також методи і засоби її реалізації. Розкрито теоретичне обгрунтування і практичні рекомендації щодо питання створення комплексної системи захисту інформаціїї.[5].

Варіант захисту мовної інформації зі створенням комплексів технічного захисту інформації на об'єктах інформаційної діяльності розглянуто в роботі [9], дослідження порядку та особливості проведення державної експертизи комплексних систем захисту інформації в інформаційно-телекомунікаційних системах пропонується в роботі [10], принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних системах розглянуто в [11].

Метою статті є здійснити повний аналіз створення комплексної системи захисту інформацій відповідно до вимог законодавства України.

1. Створення комплексної системи захисту інформацій

Комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [12]. Порядок проведення робіт із створення КСЗІ в інформаційно-телекомунікаційній системі (ІТС) розглянуто в НД ТЗІ 3.7-003-05, а також вимоги в частині ор+ганізації робіт із захисту інформації та порядку створення КСЗІ в ІТС, розвиває основні положення ДСТУ 3396.0-96, ДСТУ 3396.1-96, НД ТЗІ 3.6-001-2000, НД ТЗІ 3.7-001-07 та інших нормативних документів технічного захисту інформації (НД ТЗІ). Для організації робіт зі створення КСЗІ в ІТС створюється служба захисту інформації, порядок створення, завдання, функції, структура та повноваження якої визначено в НД ТЗІ 1.4-001-2000.

КСЗІ складається з організаційних і інженерних заходів, комплексу технічного захисту інформації (КТЗІ), захист від витоку інформації технічними каналами) та комплексу засобів захисту (КЗЗ) від несанкціонованого доступу (НСД) до ІзОД.

Організаційні заходи є обов'язковою складовою побудовою будь-яких КСЗІ. Організаційні заходи включають в себе:

- створення концепції інформаційної безпеки;
- складання посадових інструкцій для користувачів та обслуговуючого персоналу;
- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;
- розробка планів дій у разі виявлення спроб НСД до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;
- навчання правилам інформаційної безпеки користувачів.

Інженерно-технічні заходи — сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захищеності інформації, який необхідно забезпечити. У рамках проведення інженерно-технічних заходів, можуть бути встановлені:

- система охоронної сигналізації;
- система відеоспостереження;
- система пожежної сигналізації;
- система автоматичного пожежогасіння;
- система охорони периметра;
- система контролю управління доступом;
- система збору обробки інформації.

До складу КСЗІ входять заходи та засоби, які реалізують способи, які реалізують способи, методи, механізми захисту інформації від:

- витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань та наведень (ПЕМВН), акустоелектричні та інші канали;
- несанкціонованих дій та НСД до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм, використання комп' ютерних вірусів та ін.;
- спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Створення КТЗІ від витоку технічними каналами здійснюється, якщо в ІТС обробляється інформація, що становить державну таємницю (1, 2, 3 категорій об' єктів згідно з ТПКО-95 [13]), або коли необхідність цього визначено власником інформації [14].

Впровадження КЗЗ здійснюється в усіх ІТС, де обробляється інформація, що є власністю дер-жави, яка належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІТС, де така необхідність визначена власником інформації.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС.

Виділяються наступні етапи створення КСЗІ:

- формування загальних вимог до КСЗІ в ІТС;
- розробка політики безпеки інформації в ІТС;
- розробка технічного завдання, та створення КСЗІ;
- розробка проекту КСЗІ;
- введення КСЗІ в дію та оцінка захищеності інформації в ІТС;
- супроводження КСЗІ.

2. Етапи створення КСЗІ

Формування загальних вимог до КСЗІ в ІТС. Обгрунтування необхідності створення КСЗІ. На цьому етапі проводиться аналіз 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.

Результ роботи — наказ про створення КСЗІ; положення про службу захисту інформації; проекти посадових інструкцій; наказ про встановлення контрольованої зони: план заходів на рік; наказ про створення комісії для проведення категоріювання ІТС, приміщення; акт проведення ка-тегоріювання ІТС, приміщення; наказ про створення комісії з проведення обстеження ІТС.

Обстеження середовищ функціонування ІТС. При обстеженні середовищ функціонування ІТС необхідно проаналізувати всі складові: обчислювальну систему; фізичне середовище; середовище користувачів; оброблювану інформацію і технологію її обробки.

Порядок проведення обстеження має відповідати ДСТУ 3396.1-96. Результати обстеження середовищ функціонування ІТС оформляються у вигляді акту і включаються, у разі необхідності, до відповідних розділів плану захисту інформації в ІТС, який розробляється згідно з НД ТЗІ 1.4-001-2000. За результатами обстеження середовищ функціонування ІТС затверджується перелік об' єктів захисту (з урахуванням рекомендацій НД ТЗІ 1.4-001-2000, НД ТЗІ 2.5-007-07, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 щодо класифікацій об’єктів), а також визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника. Побудова моделей здійснюється відповідно до положень НД ТЗІ 1.1-002-99, НД ТЗІ 1.4-001-2000 та НД ТЗІ 1.6-003-04.

Результат роботи — акт обстеження ІТС (містить опис, принципи побудови й архітектуру ІТС); перелік об'єктів захисту ІТС; модель порушника; модель загроз інформації.

Формування завдання на створення КСЗІ. На цьому етапі визначається завдання захисту інформації в ІТС, мета створення КСЗІ, варіант вирішення задач захисту, основні напрямки забезпечення захисту, загальна структура та склад КСЗІ, засобів захисту інформації; здійснюється аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначається перелік суттєвих загроз. Здійснюється оформлення звіту про виконання робіт цієї стадії та оформлення заявки на розробку КСЗІ-технічного завдання (ТЗ) на створення КСЗІ.

Результат роботи – затверджений акт обстеження та перелік об'єктів захисту.

Розробка політики безпеки інформації в ІТС. Політика безпеки розробляється згідно з положеннями НД Т31 1.1-002-99 та рекомендаціями НД Т3І 1.4-001-2000. Політику безпеки рекомендується оформляти у вигляді окремого документа – плану захисту інформації.

Результат роботи – план захисту інформації: модель загроз інформації, завдання на створення КСЗІ, політика захисту інформації в ІТС.

3. Розробка технічного завдання на створення КСЗІ

Технічне завдання на створення КСЗІ в ІТС є організаційно-технічним документом, який визначає вимоги із захисту оброблюваної в ІТС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію у складі ІТС. Розроблення та оформлення ТЗ на КСЗІ його зміст, порядок погодження та затвердження має відповідати НД ТЗІ 3.7-001-99 та ГОСТ 34.602-89.

Результат роботи – технічне завдання на створення КСЗІ, яке погоджується з Державною службою спеціального зв'язку та захисту інформації України (ДССЗЗІ України), після цього затверджується підприємством.

4. Розробка проекту КСЗІ

Проект КСЗІ розробляється на підставі та відповідно до ТЗ на створення ІТС. Проект КСЗІ виконується на таких стадіях створення ІТС: ескізний проект, технічний проект,

робочий проект. Технічний проект на створення КСЗІ є комплектом документів, у який входить частина документів розроблених на попередніх етапах і ряд нових документів, у яких описано, як саме створюватиметься, експлуатуватиметься та модернізуватиметься КСЗІ.

Результат роботи – технічний проект на створення КСЗІ; технічна, робоча та експлуатаційна документація КСЗІ в ІТС.

5. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС

Піготовка КСЗІ до введення в дію. Проводяться роботи з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС.

Навчання користувачів. Проводиться навчання користувачів ІТС усіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та користувачів, які мають повноваження щодо управління засобами КСЗІ та ін.) в частині, що їх стосується, основним положенням документів плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації тощо, перевірка їх уміння користуватися впровадженими технологіями захисту інформації і реєстрації навчання.

Результат роботи – ознайомлення користувачів з відподними інструкціями.

Комплектування КСЗІ. Забезпечується отримання продукції (засобів захисту інформації, матеріалів, обладнання та ін.) від постачальників та співвиконавців робіт. Приймається рішення щодо підготовки до проведення оцінки на відповідність вимогам НД ТЗІ засобів захисту, які на момент проектування КСЗІ не мали відповідних сертифікатів або експертного висновку, а також порядку проведення такої оцінки під час державної експертизи КСЗІ.

Будівельно-монтажні роботи. Роботи цього етапу виконуються під час переобладнання існуючих або при будівництві нових спеціалізованих споруд (приміщень), призначених для розміщення технічних засобів ІТС та персоналу, сховищ матеріальних носіїв інформації. Під час проведення будівельно-монтажних робіт враховуються вимоги технічного завдання на створення КСЗІ в ІТС.

Пусконалагоджувальні роботи. Метою пусконалагоджувальних робіт є: монтаж обладнання і атестація комплексу технічного захисту інформації від витоку технічними каналами; встановлення і налагодження КЗЗ; перевірка працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії. Монтаж основних технічних засобів (ОТЗ) ІТС, кабельного обладнання, мереж живлення та заземлення здійснюється згідно з конструкторською документацією робочого проекту.

Попередні випробування. Випробування – експериментальне визначення кількісних та/або якісних характеристик властивостей об'єкта експертизи за результатом впливу на нього під час його функціонування [15]. Метою попередніх випробувань є перевірка працездатності КСЗІ та визначення можливості прийняття її у дослідну експлуатацію. Під час випробувань перевіряються працездатність КСЗІ та відповідність її вимогам ТЗ.

Результат роботи – програма та методика попередніх випробувань; протокол проведення попередніх випробувань; акт завершення попередніх випробувань КСЗІ ІТС.

Дослідна експлуатація. Під час дослідної експлуатації КСЗІ: відпрацьовуються технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежуваня доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів; співробітники служби захисту інформації (СЗІ) та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів; здійснюється (за необхідністю) доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування КЗЗ; здійснюється (за необхідністю) коригування робочої та експлуатаційної документації.

Результат роботи – установлення необхідних технічних або криптографічних засобів захисту інформації; засобів фізичного захисту елементів ІТС (встановлюється необхідне

обладнання й програмне забезпечення, засоби контролю доступу, охоронна й пожежна сигналізації) і т.д. Пакет документів "Експлуатаційна документація на КСЗІ": інструкції експлуатації КСЗІ і її елементів; процедури регламентного обслуговування КСЗІ; правила й положення з проведення тестування й аналізу роботи КСЗІ. Акт приймання КСЗІ в ІТС у дослідну експлуатацію, акт завершення дослідної експлуатації КСЗІ в ІТС.

За результатом випробування КСЗІ робиться висновок щодо можливості подання КСЗІ на державну експертизу.

Державна експертиза КСЗІ. Відповідно до п.1.4 Положення про Державну експертизу в сфері технічного захисту інформації КСЗІ підлягає обов'язковій перевірці на відповідність вимогам чинних нормативних документів з технічного захисту інформації в ІТС [14]. Державна експертиза КСЗІ є окремим етапом приймальних випробувань ІТС. Державна експертиза проводиться з метою визначення відповідності КСЗІ технічному завданню, вимогам нормативної документацй із захисту інформації та визначення можливості введення КСЗІ в складі ІТС в експлуатацію.

Державна експертиза КСЗІ в ІТС проводиться згідно з Положення про державну експертизу в сфері технічного захисту інформації та НД ТЗІ 2.6-001-11. Об'єктами експертизи (ОЕ) можуть бути як КСЗІ, які є невід'ємною складовою частиною ІТС, так і окремі засоби технічного захисту інформації від НСД, у тому числі захищені від НСД компоненти обчислювальної системи [15].

Державна експертиза КСЗІ, передбачає 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.

Результат роботи – программа та методика проведення експертизи КСЗІ; особлива думка експерта; протокол випробувань; атестат відповідності та експертний висновок.

Супроводження КСЗІ

Виконуються роботи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до плану захисту та експлуатації документації на компоненти КСЗІ, гарантійного і післягарантійного технічного обслуговування засобів захисту інформації.

Порядок створення КТЗІ

Для об'єктів електронно-обчислювальної техніки (ЕОТ), на яких циркулює інформація, що становить державну таємницю є обов'язковим створення та атестація КТЗІ, який має забезпечувати захист інформації з обмеженим доступом від витоку технічними каналами, а саме каналам побічних електромагнітних випромінювань та наведень.

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 [16]. Створення та випробування КТЗІ здійснюється відповідно до положень НД ТЗ1 1.1-005-07, НД ТЗІ 1.6-003-04, НД ТЗІ 3.1-001-07, НД ТЗІ 3.3-001-07, НД ТЗІ 2.1-002-07 [16-20].

Для визначення необхідних заходів захисту інформації від витоку технічними каналами проводиться спеціальне дослідження персональної електронно-обчислювальної машини по каналах ПЕМВН, при якому визначаються можливі канали витоку інформації. За результатами спеціального дослідження приймається рішення про необхідність встановлення активних та/або пасивних засобів захисту. Після цього проводиться оцінка захищеності ІзОД від витоку технічними каналами на об'єкті ЕОТ (атестація комплексу ТЗІ).

Висновки. На закінчення слід зазначити, що під час створення КСЗІ в ІТС необхідно дотримуватися певних методологічних принципів проведення досліджень, проектування,

експлуатації і розвитку таких систем відповідно до вимог законодавства України. Порядок створення КСЗІ є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких обробляється інформація, яка є власністю держави.

Таким чином, у даній статті наведено порядок та етапи створення КСЗІ в ІТС посилання на діючі нормативні документи, визначений обсяг і зміст робіт, етапності робіт, основні завдання та порядок виконання робіт кожного етапу та якими результатами вони повинні закінчуватися.

ЛІТЕРАТУРА:

1. Про внесення змін до Закону України "Про інформацію" №2938-VI від 13.01.2011. – Відомості Верховної Ради України 2011, №32, ст. 313. – (Серія видань "Законодавство України").

2. Іро внесення змін до Закону України "Про Національну програму інформатизації" №2684-III від 13.09.2001. – Відомості Верховної Ради України 2002, №1, ст. 3. – (Серія видань "Законодавство України").

3. Концепції технічного захисту інформації в Україні №1126 від 8.10.1997 р. – Із змінами, внесеними згідно з Постановою Кабінету Міністрів України №938 від 07.09.2011. – (Серія видань "Законодавство України").

4. Закон України "Про захист персональних даних" №2297-VI від 01.06.2010. – Відомості Верховної Ради України 2010, № 34, ст. 481. – (Серія видань "Законодавство України").

5. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. В 2-х томах. – К.: Арий, 2008. – Том II.

6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.99. – (Серія видань "Нормативний документ").

7. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України №22 від 28.04.1999. – (Серія видань "Нормативний документ").

8. Про внесення змін до Закону України "Про захист інформації в автоматизованих системах" №2594-IV від 31.05.2005. – Відомості Верховної Ради України 2005, №26, ст. 347. – (Серія видань "Законодавство України").

9. Місюра С.М. Варіант захисту мовної інформації на об'єктах інформаційної діяльності / С.М. Місюра, В.В. Овсянніков, І.Р. Мальцева // Збірник наукових праць ВІТІ НТУУ «КПІ». – 2011. – № 2. – С. 84-93.

10. Хлапонін Ю.І. Порядок та особливості проведення державної експертизи комплексних систем захисту інформації в інформаційно-телекомунікаційних системах / Ю.І. Хлапонін // Збірник наукових праць ВІТІ НТУУ «КПІ». – 2011. – № 2. – С. 123-127.

11. Принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних системах / Ю.В. Землянко // Прикладная радиоэлектроника: н.-т.-ж.: ХНУРЭ, 2010. – Том 9. – №3. –С.460-469.

12. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – Затверджено наказом ДСТСЗІ СБ України №125 від 8.11.2005. – (Серія видань «Нормативний документ»).

13. ТПКО-95. Тимчасове положення про категоріювання об'єктів №35 від 10.07.95. – Затверджено наказом Державного комітету країни з питань державних секретів та технічного захисту інформації №35 від 10.07.95. – (Серія видань «Тимчасове положення»).

14. Положення про Державну експертизу в сфері технічного захисту інформації. – Затверджено наказом Адміністрації ДССЗЗІ України №93 від 16.05.07. – Офіційний вісник України. – 2007. – №52, ст. 2153. – (Серія видань «Нормативний документ»).

15. 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. – Затверджено наказом Адміністрації ДССЗЗІ України №65 від 12 березня 2011. – (Серія видань «Нормативний документ»).

16. НД ТЗІ 1.1-005-07. Захист інформації на об'єктах інформаційної діяльності. Створення

комплексу технічного захисту інформації. Основні положення. – Затверджено наказом Адміністрації ДССЗЗІ України №232 від 12.12.2007.- (Серія видань «Нормативний документ»).

17. НД ТЗІ 3.1-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. – Затверджено наказом Адміністрації ДССЗЗІ України №232 від 12.12.2007. – (Серія видань «Нормативний документ»).

18. 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. – Затверджено наказом Адміністрації ДССЗЗІ України №232 від 12.12.2007. – (Серія видань «Нормативний документ»).

19. НД ТЗІ 2.1-002-07. Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення. – Затверджено наказом Адміністрації ДССЗЗІ України №232 від 12.12.2007. – (Серія видань «Нормативний документ»).

20. НД ТЗІ 1.6-003-04. Створення комплексів технічного захисту інформації на о'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації. – Затверджено наказом ДСТСЗІ СБ України №04 від 10.03.2004. – (Серія видань «Нормативний документ»).

Рецензент: д.т.н., проф. Юдін О.К., завідувач кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету

д.т.н., проф. Оксиюк А.Г., Шестак Я.В.

МЕТОДОЛОГИЯ РАЗРАБОТКИ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В СОВРЕМЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Рассматривается методология создания комплексной системы защиты информации согласно требованиям законодательства Украины. Приведен порядок и этапы создания комплексной системы защиты информации в информационно-телекомуникационных ситемах.

Рассматриваются основные проблемные вопросы, связанные с созданием комплексов технической защиты информации на объектах информационной деятельности. Обоснованы и предложены пути, основные задания и рекомендации по решению исследованных проблем создания комплексов технической защиты информации. Рассматривается порядок осуществления мер и применения средств защиты при создании комплексных систем защиты информации в современных ифармационно-телекоммуникационных системах.

Анализируются и классифицируются возможные угрозы безопасности информации, рассматриваются методы и средства защиты от несанкционированного доступа к информации, раскрываются подходы к построению и эксплуатации комплексных систем защиты.

Ключевые слова: комплексная система защиты информации, информация с ограниченным доступом, автоматизированная система, информационно- телекоммуникационная система.

Prof. Oksiuk A.G., Shestak Y.V.

METHODOLOGY OF DEVELOPMENT COMPLEX INFORMATION SECURITY SYSTEMS IN INFORMATION AND TELECOMMUNICATION SYSTEMS

The methodology of creating the complex system of information protection according to the requirements of the legislation of Ukraine is considered. The order and stages of creating the complex system of information protection in information and telecommunication systems are given.

We consider the major issues associated with the creation of systems of technical protection of information on objects of information activity. Substantiated and the ways, basic tasks and recommendations to address the problems of creating systems of technical protection of information investigated. A procedure for implementing measures and using means to create complex systems of information protection in modern information and telecommunication systems is considered.

Analyzes and classifies potential threats to the security of information, methods and means of protection from unauthorized access to the information disclosed approaches to the construction and operation of complex systems of protection.

Keywords: complex systems of information protection, information with limited access, automated system, information telecommunication systems.