МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет Магістерської підготовки
Кафедра Інформаційних технологій

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Дослідження та впровадження комплексної системи захисту інформації»

Виконав студент 2 курсу групи МІС-18 спеціальності 122 Комп'ютерні науки
Салабаш Олександр Юрійович

Керівник д.т.н., проф.
Казакова Н.Ф.

Консультант

Рецензент д.т.н., проф.
Положаєнко С.А

Одеса 2020

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

АС – автоматизована система.

ВНЗ – вищий навчальний заклад.

ДСК – для службового користування.

ДСТСЗІ – державна служба спеціального зв'язку та захисту інформації.

ЗЗІ – засоби захисту інформації.

ЗІ – захист інформації.

ІБ – інформаційна безпека

ІКС –інформаційно-криптографічні системи.

ІТС – інформаційно-телекомунікаційні системи.

К – конфіденційно.

КЗСІ – комплексна система захисту інформації.

НДД – не для друку

НДДКР – науково-дослідні та дослідно-конструкторські роботи

НДР – науково-дослідні роботи

ОВ – особливої важливості.

Т – таємна.

ТЗІ – технічний захист інформації

ЦТ – цілком таємно

ВСТУП

Сучасні методи обробки, передачі та накопичення інформації сприяли появі загроз, пов'язаних з можливістю втрати, перекручування та розкриття даних, які адресовані або належать кінцевим користувачам. Тому забезпечення інформаційної безпеки комп'ютерних систем і мереж є одним з провідних напрямків розвитку IT. Комп'ютерні інформаційні технології швидко розвиваються та вносять помітні зміни в наше життя. Інформація стала товаром, який можна придбати, продати, обміняти. При цьому вартість інформації часто в сотні разів перевершує вартість комп'ютерної системи, в якій вона зберігається. Інформаційна безпека комп'ютерних систем досягається забезпеченням конфіденційності, цілісності та достовірності даних, що обробляються, а також доступності та цілісності інформаційних компонентів і ресурсів системи. При розробці комп'ютерних систем, вихід з ладу або помилки в роботі можуть призвести до тяжких наслідків, питання комп'ютерної безпеки стають першочерговими. Відомо багато заходів, спрямованих на забезпечення комп'ютерної безпеки, основними серед них є технічні, організаційні та правові. Захищеність інформаційної системи від випадкового або навмисного втручання, що завдає шкоди власникам або користувачам інформації, залежить, в основному, від доступності (можливість за розумний час отримати необхідну інформаційну послугу); цілісності (актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованого зміни); конфіденційності (захист від несанкціонованого прочитання). Сучасна інформаційна система являє собою складну систему, що складається з великого числа компонентів різного ступеня автономності, які пов'язані між собою і обмінюються даними. Практично кожен компонент може піддатися зовнішньому впливу або вийти з ладу.

1 ОГЛЯД НОРМАТИВНИХ ДОКУМЕНТІВ, ЯКІ РЕГЛАМЕНТУЮТЬ КОНЦЕПЦІЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

1.1 Державна політика в сфері інформаційної безпеки та її реалізація в законодавстві України

Державна політика у сфері охорони інформації в Україні спрямована на накопичення та захист національних інформаційних ресурсів держави, розробку та впровадження сучасних безпечних технологій, побудову захищеної національної інформаційної інфраструктури, формування і розвиток інформаційних стосунків тощо. Вона повинна реалізовуватись шляхом створення і забезпечення ефективного функціонування в Україні цілісної системи ІБ, а також вдосконалення існуючої і розробку нової нормативно-правової бази, яка регулює відносини в сфері ІБ, встановлює вимоги і правила провадження діяльності у цій сфері.

Основною метою реалізації державної інформаційної політики є створення політико-правових, економічних, організаційних та матеріально-технічних умов для формування сучасної моделі державної інформаційної політики, підвищення ефективності використання усіх видів інформаційних ресурсів і управління елементами інформаційно-комунікаційної інфраструктури, державної підтримки виробництва і розповсюдження вітчизняної інформаційної продукції, забезпечення розвитку та захисту вітчизняної інформаційної сфери виходячи з пріоритету прав і свобод людини і громадянина, її запитів та інтересів.

Відповідно до Закону України «Про Основні засади державної інформаційної політики» Державна інформаційна політика базується на принципах:

- верховенства права;
- пріоритету прав і свобод людини, зокрема права кожного на вільне одержання, використання, поширення та зберігання інформації;
- дотримання балансу інтересів особи, суспільства і держави, їх взаємної відповідальності та безумовного забезпечення прав людини;

– захисту національних інтересів, зокрема у сфері інформаційної безпеки;

– забезпечення культурної, мовної, ідеологічної та політичної багатоманітності в суспільстві;

– протекціоністської політики щодо виробництва і розповсюдження вітчизняної інформаційної продукції;

– сприяння постійному збагаченню, оновленню та захисту національних інформаційних ресурсів;

– забезпечення незалежності засобів масової інформації;

– забезпечення системності та координації дій органів державного управління і регулювання в інформаційній сфері;

– забезпечення охорони і захисту інформації, зокрема запобігання відповідно до закону розголошенню інформації з обмеженим доступом;

– впровадження демократичних стандартів щодо одержання, використання, поширення та зберігання інформації на міжнародному рівні;

– недопущення зловживання свободою діяльності засобів масової інформації на шкоду правам і свободам людини [1][1)].

На державному рівні інформаційну безпеку розуміють як складову частину національної безпеки, що характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз. Серед загроз інформації за своїми небезпечними наслідками особливе місце займають:

– здобування технічними розвідками відомостей у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку;

[1)] [1] Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9 січня 2007 року № 537-V // Відомості Верховної Ради України (ВВР). 2007. № 12. ст.102.

– несанкціонований доступ до інформації, яка обробляється та циркулює в ІТС, а також спеціальний вплив на інформацію з метою її спотворення, руйнування, знищення, порушення нормального функціонування системи обробки інформації;

– витік інформації з обмеженим доступом технічними каналами внаслідок виникнення побічних електромагнітних випромінювань і наводок, ведення акустичної та оптико-електронної розвідки в безпосередній близькості від об’єкту інформаційної діяльності.

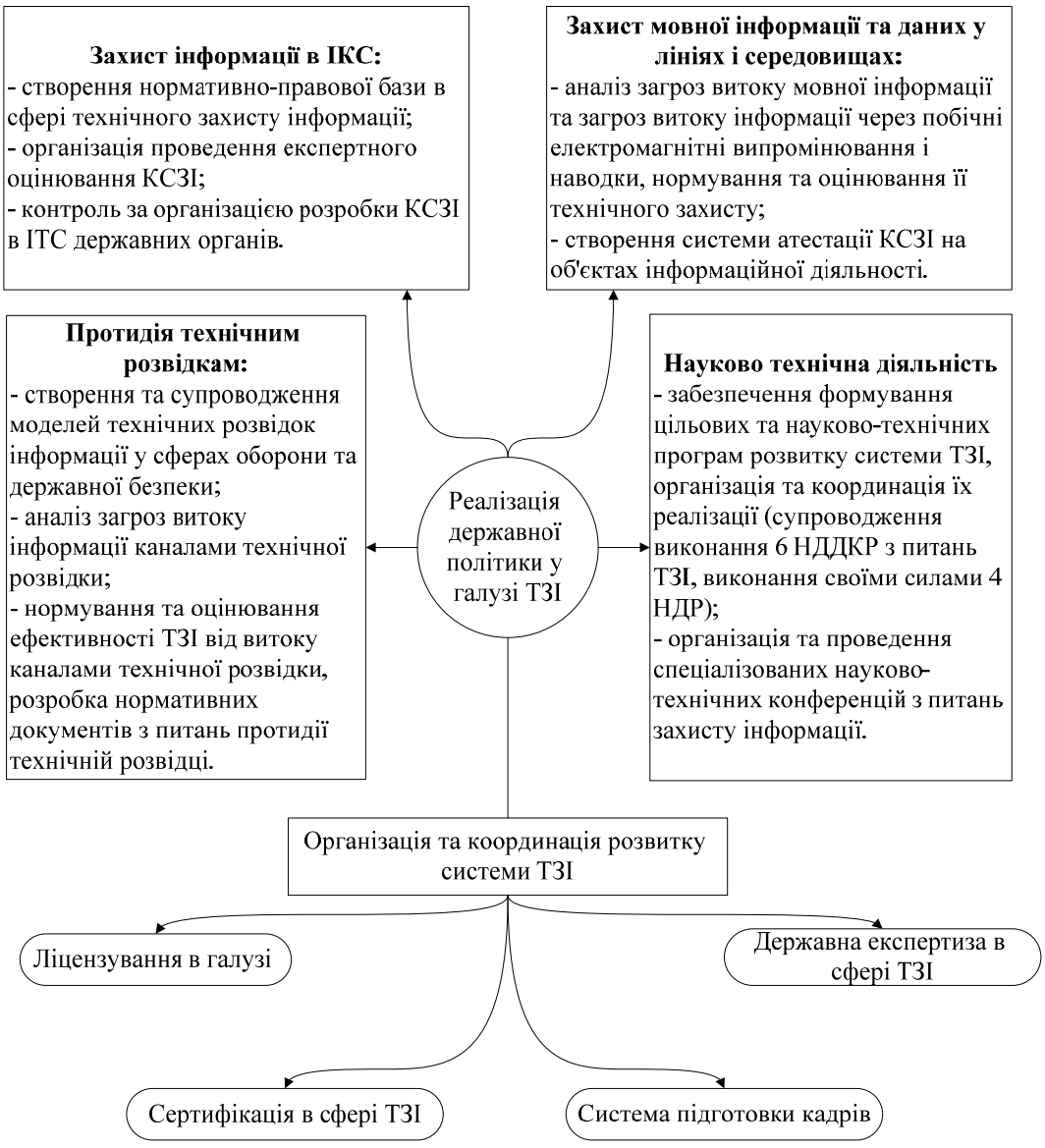

Рисунок 1.1 – Побудова і організаційна структура системи ТЗІ в Україні

З метою протидії цим загрозам державна політика ІБ передбачає створення та розвиток системи ТЗІ, що є сукупністю організаційних структур, об'єднаних завданнями та цілями стосовно ЗІ, нормативно-правової бази, та матеріально-технічної бази. Ця схема зображена на рис. 1.1 [2][1)].

Як зазначено в Проекті Концепції інформаційної безпеки України основними суб'єктами реалізації державної політики в сфері інформаційної безпеки, в межах їх повноважень та завдань, є:

- служба безпеки України;
- міністерство внутрішніх справ України;
- міністерство оборони України;
- служба зовнішньої розвідки України;
- центральний орган виконавчої влади із спеціальним статусом, який забезпечує формування та реалізує державну політику у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій і користування радіочастотним ресурсом України [3][2)].

Згідно Закону центральним органом України, який відповідає за питання функціонування і розвитку державної системи захисту державних інформаційних ресурсів, є Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язок, ДСТСЗІ). Держспецзв'язок підконтрольний Верховній Раді України, але з питань, пов'язаних із забезпеченням національної безпеки України він підпорядкований і підконтрольний Президенту України.

Як зазначено у Білій книзі ДСТСЗІ інформаційна безпека включає такі складові як гуманітарну та технологічну, але крім них існують ще технічна, економічна, функціональна складові щодо результатів ЗІ. Правильно побудована та добре захищена інформаційна система має дозволяти отримання ефектів різного характеру.

[1)] [2] Правові основи охорони інформації: підручник / [В.М. Сердюков, О.М. Стаднік, З.Б. Живко, В.О. Хорошко]; за заг. ред. В.О. Хорошко. Київ: ДУІКТ, 2009. 354 с.

[2)] [3] Проект Концепція інформаційної безпеки України [електронний ресурс]. Режим доступу: http://mip.gov.ua/done_img/d/30- project_08_06_15.pdf 3.

Законодавче і правове забезпечення ЗІ повинне являти собою високо впорядковану сукупність організаційних рішень, законів, нормативів і правил, що регламентують як загальну організацію робіт із ЗІ, так і створення, і функціонування систем ЗІ в конкретних умовах. З цього визначення випливає:

- організаційно-правове забезпечення ЗІ є багатоаспектним поняттям, що включає рішення, нормативи, закони і правила;
- припускає реалізацію перерахованих аспектів к стосовно до конкретних умов, так і до систем відомства.
- При побудові правової бази системі ІБ в Україні враховувався міжнародний досвід у цій галузі та вирішувались наступні проблеми:
- Розробити підвалини правового забезпечення системи – базовий закон, що регламентує відношення сфери повноважень всіх учасників інформаційних відносин, а також державних органів, що забезпечують інформаційну безпеку і контроль держави за розмежуванням доступу до інформації;
- Видати й отримати за структурою і складом правові норми й законодавчі документи, що всебічно охоплюють всі сфери, проблеми, які розглядаються і мають самостійне значення в сенсі розмежування у предметній і цільовій галузях.

Ефективна охорона інформації в умовах, що склались в Україні, може бути досягнута тільки під час створення системи безпеки інформації, що реалізує державну політику в цій галузі здійсненням управлінської, адміністративно-господарської і виробничої діяльності.

Сучасна постановка проблеми ЗІ й об’єктів вимагає реалізації на підприємствах і в організаціях комплексних систем захисту інформації (КСЗІ), що включають в себе засоби і системи організаційно-режимного забезпечення робіт, захисту інформації від несанкціонованого доступу, захисту від технічних розвідок, охоронної та пожежної сигналізації.

1.2 Огляд законодавчої бази та нормативних документів із захисту інформації

Законодавча база України із захисту інформації насамперед спирається на Конституцію України. Виходячи із цього закони та інші нормативно-правові акти також приймаються на основі Конституції і повинні відповідати її положенням та формують систему правового захисту інформації (рис. 1.2) [4][1)].

Станом на 2019 рік законодавча база України з питань ЗІ спирається на дії таких законів як:

- «Про національну безпеку України»;
- «Про Концепцію Національної програми інформатизації»;
- «Про інформацію»;
- «Про державну таємницю»;
- «Про захист інформації в інформаційно-телекомунікаційних системах»;
- «Про електронний цифровий підпис»;
- «Про доступ до публічної інформації»;
- «Про електронні документи та електронний документообіг»;
- «Про захист персональних даних»;
- «Про інформацію»;
- «Про Національну систему конфіденційного зв'язку»;
- «Про Державну службу спеціального зв'язку та захисту інфомації України»;
- «Про Службу безпеки України»;
- «Про контррозвідувальну діяльність»;
- «Про зв’язок»;
- «Про основні засади забезпечення кібербезпеки України»;

[1)] [4] Богуш В. М. Інформаційна безпека від А до Я / В. М. Богуш, А. М. Кусин. К. : ДУІКТ, 2006. 126 с.

- «Про електроні довірчі послуги»;
- «Про національний банк України».

Рисунок 1.2 – Система правового захисту інформації

Нормативні документи із захисту інформації визначають методологічні основи рішення задач ЗІ на об’єктах інформаційної діяльності та регламентують питання визначення вимог щодо захисту об’єктів від НСД, створення захищених систем та засобів їх захисту від НСД, оцінку захищеності систем та об’єктів та їх придатність для рішення задач користувача. Вони розробляються в ході проведення робіт із стандартизації та нормування у галузі технічного захисту інформації та забезпечують такі пункти як:

- створення єдиної технічної політики у державі;

– створення та доповнення єдиної термінологічної бази;

– функціонування багаторівневих систем захисту інформації;

– функціонування систем сертифікації, ліцензування й атестації;

– формування та розвиток сфери послуг у галузі ТЗІ;

– установлення порядку розробки, виготовлення та експлуатації засобів технічного захисту інформації;

– організація проектування будівельних робіт відповідно із потребами ТЗІ;

– підготовка кадрів, що мають відповідну кваліфікацію із питань ТЗІ.

– До цих документів відносяться:

– ДБН А.2.2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектні документації для будівництва;

– Тимчасові положення про категоріювання об’єктів;

– НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу;

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

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

– НД ТЗІ 1.1-004-2003 Протидія технічним розвідкам. Терміни та визначення;

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

– НД ТЗІ 1.6-002-03 Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації;

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

– НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці;

– НД ТЗІ 2.6-002-15 Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, затверджений наказом Адміністрації Держспецзв’язк від 27.04.2016 № 293;

– НД ТЗІ 2.6-003-2015 Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, затверджений наказом Адміністрації Держспецзв’язку від 27.04.2016 № 294;

– НД ТЗІ 2.6-013-2016 Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99, затверджений наказом Адміністрації Держспецзв’язку від 27.04.2016 № 295;

Нормативні документи системи ТЗІ поділяються на:

– нормативні документи із стандартизації у галузі ТЗІ;

– державні стандарти та прирівняні до них нормативні документи;

– нормативні акти міжвідомчого значення, що реєструються у Міністерстві юстиції України;

– нормативні документи міжвідомчого значення технічного характеру, що реєструються уповноваженим Кабінетом Міністрів органом;

– нормативні документи відомчого значення органів державної влади та органів місцевого самоврядування [5][1)].

[1)] [5] ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення: - Чинний від 1997-01-01. К.: Держстандарт України. 1996. 3 с.

Класифікаційна структура типових документів із захисту інформації в Україні зображена на рис. 1.3 [6][1)].

Нормативно-правові норми визначають порядок забезпечення конфіденційності, доступності, цілісності та спостережності інформації під час створення та функціонування інформаційної системи; регламентує порядок попередження загроз та знешкодження атак шляхом побудови відповідної КСЗІ на об'єктах інформаційної діяльності на яких циркулює та обробляється інформація з обмеженим доступом; регламентує права, обов'язки та відповідальність користувачів, робота яких пов'язана з інформаційною безпекою; упорядковую створення та функціонування інформаційно-комунікаційних систем та мереж.

Рисунок 1.3 – Класифікаційна структура типових документів із захисту інформації

Для того щоб документацій не забезпечення мало системний характер, передбачається його однозначна, інформативна і наочна ідентифікація.

[1)] [6] Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О. К. Юдін. – К.:НАУ, 2011. 640с.

1.3 Загальні відомості щодо інформації оброблюваної в АС

1.3.1 Види оброблюваної інформації

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [7][1)].

Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Відповідно до статті 20 Закону України «Про інформацію», за режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом (рис. 1.4).

Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Відкрита інформація поділяється на інформацію, що належить особі, та інформацію, що належить державі.

Рисунок 1.4 – Види інформації

[1)] [7] Про інформацію: Закон України від 02 листопада 1992 року № 2657-XII // Відомості Верховної Ради України (ВВР). 1992. N 48. ст. 650.

Інформація з обмеженим доступом в свою чергу поділяється на конфіденційну, таємну (державна таємниця) та службову. Таємна та службова інформація має свій гриф секретності та термін його дії. Грифи таємності наведені у табл. 1.1 [8][1)].

Таблиця 1.1 – Грифи секретності інформації

Гриф секретності інформації	Термін дії грифа
Для службового користування (ДСК) Конфіденційна (К)	3 роки
Таємна (Т)	5 років
Цілком таємна (ЦТ)	10 років
Особливої важливості (ОВ)	30 років
Не для друку (НДД)	Не визначено
Знак інтелектуальної власності	Не визначено

Конфіденційна інформація – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Не може бути віднесена до конфіденційної інформація.

Таємна інформація – інформація, доступ до якої обмежується відповідно до Закону України «Про доступ до публічної інформації», і розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.

До службової інформації належить інформація:

– що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної

[1)] [8] Про державну таємницю: Закон України від 21.01.1994 року № 3855-12-ВР// Відомості Верховної Ради України (ВВР). 1994. № 24. ст. 296.

влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

– зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф "для службового користування" [9][1)].

Технічний захист інформації з обмеженим доступом є однією із складових частин управлінської наукової і виробничої діяльності, спрямованої на забезпечення безпеки інформації, та являє собою сукупність організаційних і технічних заходів, що базуються на принципах доцільності, безперервності і комплексності, погоджених за часом і місцем застосування [10][2)].

Відповідно до статті 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 що має сертифікат відповідності згідно з законодавством.

1.3.2 Захист інформації в автоматизованих системах та класи автоматизованих систем

Захисту підлягає будь-яка інформація в автоматизованих системах (АС) та безпосередньо її властивості. Необхідність організації процесу захисту визначається власником інформаційних ресурсів або чинним законодавством.

---

1) [9] Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI // Відомості Верховної Ради України (ВВР). 2011. № 32. ст. 314.

2) [10] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР // Відомості Верховної Ради України (ВВР). 1994. № 31. ст.286.

Доступ до інформації оброблюваної в АС здійснюється лише згідно з правилами розмежування доступу, встановлених власником інформації, уповноваженою особою чи політикою безпеки організації.

Захист інформації в АС забезпечується через:

- дотримання суб'єктами правових відносин, вимог та правил організаційного і технічного характеру щодо захисту оброблюваної інформації;
- використання засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку і АС в цілому, засобів захисту інформації, які відповідають встановленим вимогам до захисту інформації;
- перевірку відповідності засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку і АС в цілому;
- контроль захисту інформації (рис. 1.5).

Вимоги і правила щодо захисту інформації, яка є власністю держави, або інформації, захист якої гарантовано державою, встановлюються державним органом, уповноваженим Кабінетом Міністрів України. Ці вимоги і правила є обов'язковими для власників АС, де така інформація обробляється, і мають рекомендаційний характер для інших суб'єктів права власності на інформацію [11][1)].

Автоматизована система являє собою організаційно-технічну систему, що об'єднує ОС, фізичне середовище, персонал і оброблювану інформацію. Основні складові автоматизованої системи зображені на рис. 1.6. Вимоги до функціонального складу КЗЗ залежать від характеристик оброблюваної інформації, самої ОС, фізичного середовища, персоналу і організаційної підсистеми [12][2)] [13][3)].

[1)] [11] Про захист інформації в автоматизованих системах: Закон Україні від 05.07.1994 № 81/94-ВР// Відомості Верховної Ради України (ВВР). 1994. № 31. ст. 287.

[2)] [12] НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: Чинний від 1999-04-28. К.: Нормативний документ. Системи технічного захисту інформації. 1999. 16 с.

[3)] [13] НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: Чинний від 1999-04-28. К.: Нормативний документ. Системи технічного захисту інформації. 1999. 20 с.

Рисунок 1.5 – Напрями захисту інформації в АС

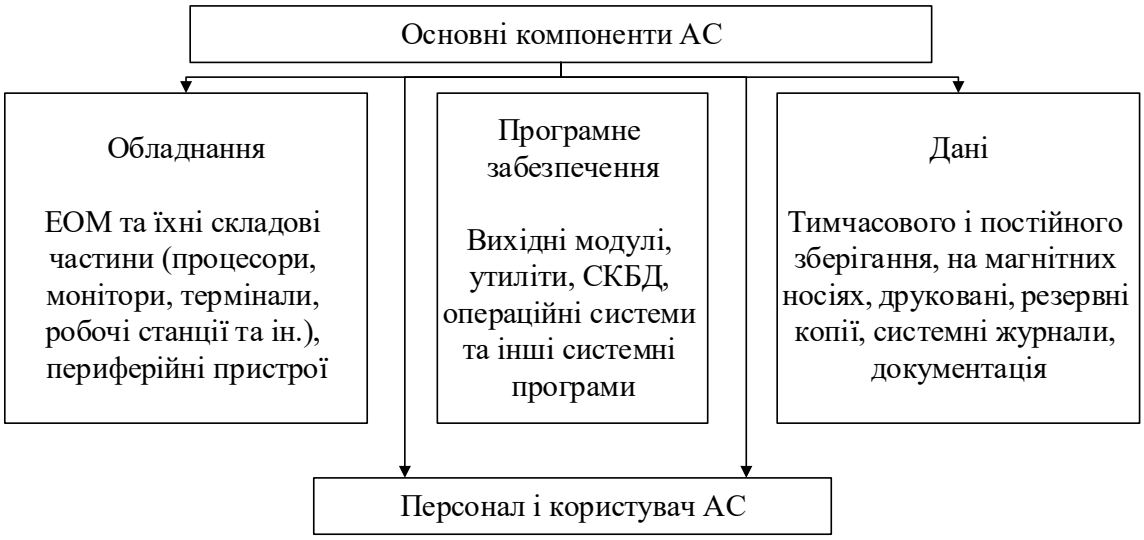

Рисунок 1.6 – Складові автоматизованої системи

Автоматизовані системи, в яких обробляється інформація, що потребує захисту, умовно поділяються на 3 класи:

Клас «1» – одномашинний однокористувачевий комплекс, що може обробляти інформацію різних категорій конфіденційності – тобто це один комп'ютер, який не підключено до локальної мережі або мережі Інтернет

Істотні особливості:

- 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/або У/В всієї інформації.

Приклад – автономна персональна ЕОМ, доступ до якої контролюється з використанням організаційних заходів.

Клас «2» – локалізований багатомашинний багатокористувачевий комплекс, який може обробляти 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 організації, що не підключена до мережі Інтернет і обробляє відкриту та конфіденційну інформацію.

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 – центральний офіс та філії, що передають інформацію через мережу Інтернет.

З погляду безпеки інформація характеризується трьома властивостями: конфіденційністю, цілісністю і доступністю. У зв’язку з цим у кожному класі АС виділяються такі підкласи:

- АС з підвищеними вимогами до забезпечення конфіденційності оброблюваної інформації (х. К);

– АС з підвищеними вимогами до забезпечення цілісності оброблюваної інформації (х. Ц);

– АС з підвищеними вимогами до забезпечення доступності оброблюваної інформації (х. Д);

– АС з підвищеними вимогами до забезпечення конфіденційності і цілісності оброблюваної інформації (х. КЦ);

– АС з підвищеними вимогами до забезпечення конфіденційності і доступності оброблюваної інформації (х. КД);

– АС з підвищеними вимогами до забезпечення доступності і цілісності оброблюваної інформації (х. ЦД);

– АС з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації (х. КЦД);

Для кожного з підкласів кожного класу вводиться деяка кількість ієрархічних стандартних функціональних профілів, яка може бути різною для кожного класу і підкласу АС. Профілі є ієрархічними в тому розумінні, що їх реалізація забезпечує підвищену захищеність від загроз відповідного типу.

Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які мають бути реалізовані в АС, щоб задовольнити певні вимоги до захищеності інформації. Вони будуються на підставі існуючих вимог до захисту певної інформації від певних загроз і відомих послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання поставлених вимог.

Для стандартних функціональних профілів захищеності не вимагаються ні зв’язані з ними політики безпеки, ні рівні гарантій, хоч їх наявність і допускається в разі потреби. Політика безпеки КС, що реалізує певний стандартний профіль, має бути «успадкована» з відповідних документів, що встановлюють вимоги до порядку оброблення певної інформації в АС. Так, один і той самий профіль захищеності може використовуватись для опису функціональних вимог із захисту оброблюваної інформації і для ОС, і для СУБД, у той час, як їх політика безпеки, зокрема визначення об’єктів, буде різною.

2 ОЦІНКА СТАНУ ЗАХИСТУ ІНФОРМАЦІЇ В ВНЗ

2.1 Аналіз інформації з обмеженим доступом, що обробляється в вищих навчальних закладах

У сучасному вищому навчальному закладі зберігається і обробляється величезна кількість різних даних, пов'язаних не тільки із забезпеченням навчального процесу, але й з науково-дослідними та проектно-конструкторськими розробками, персональні дані студентів і співробітників, службова, комерційна та інша конфіденційна інформація. Зростання кількості злочинів у сфері високих технологій диктує свої вимоги до захисту ресурсів обчислювальних мереж навчальних закладів і ставить завдання побудови власної інтегрованої системи безпеки. Саме вирішення цього завдання потребує наявності нормативно-правової бази, формування концепції безпеки, розробку заходів, планів і процедур щодо безпечної роботи, проектування, реалізації та супроводу технічних засобів захисту інформації (ЗЗІ) в рамках освітньої установи. Ці складові визначають єдину політику забезпечення інформаційної безпеки у вищому навчальному закладі.

Слід зазначити, що ВНЗ в першу чергу є соціальним інститутом, призначення якого − виховання та професійна підготовка фахівців для різних сфер життєдіяльності суспільства. Від якості та безперервності підготовки залежить рівень розвитку економіки та суспільства в цілому.

В ВНЗ як і на любому іншому державному або приватному підприємстві, циркулююча інформація поділяється на два типи: відкриту інформацію та інформацію з обмеженим доступом. Типи інформації зображено на рис.2.1.

Для більш точного визначення циркулюючої в навчальному закладі інформації подальшого її категоріювання необхідно визначитися з основними підрозділами. В кожному ВНЗ до особливо важливих підрозділів можна віднести ректорат, режимно-секретний підрозділ, відділ кадрів, директорати інститутів, приймальну комісію та інші. Перелік підрозділів та інформація що в них обробляється зображені в табл. 2.1.

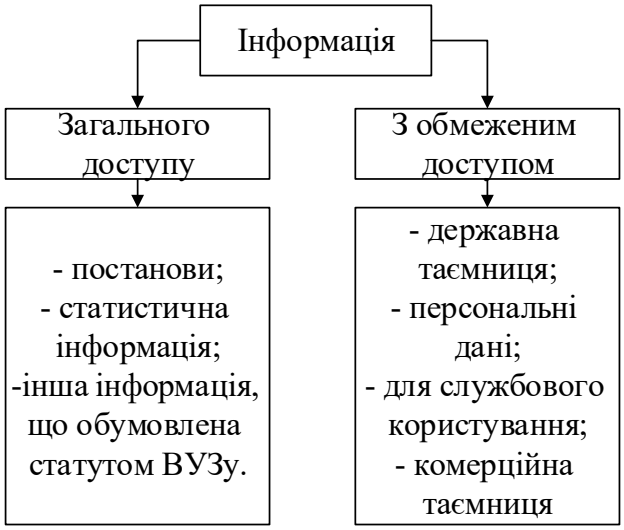

Рисунок 2.1 – Класифікація інформації по типу її регламентації розповсюдження та використання в ВНЗ

Зазвичай у ВНЗ структура інформаційної системи побудована так, щоб за наявності Державної Таємниці, вона оброблялась в автоматизованій системі першого класу, яка відповідає вимогам законодавства. Також при побудові інформаційної системи в першу чергу особливу увагу приділяють таким підрозділам як ректорат, бухгалтерія, відділ кадрів та приймальна комісія.

Таблиця 2.1 – Основні підрозділи, в яких циркулює інформація з обмеженим доступом

Назва підрозділу	Вид інформації
Ректорат	ДСК, ПД
Режимно-секретний відділ	Т, ПД
Відділ кадрів	ПД
Бухгалтерія	ДСК, ПД
Директорати інститутів	ДСК, ПД
Приймальна комісія	ПД
Здравпункт	ПД
Профілакторій	К, ПД
Столова	ДСК, К, ПД
Гуртожиток	ДСК, К, ПД

Саме через ці підрозділи проходить найбільший потік інформації що потребує захисту. Принцип побудови інформаційної системи ВНЗ зображено на рис.2.2.

Після побудови моделі функціонування підрозділів в ВНЗ ми можемо визначитись з основними об’єктами, що підлягають захисту. До таких об’єктів можна віднести:

- робочі станції користувачів;
- робочі станції адміністраторів;
- сервери (мережеві, баз даних);
- апаратура зв’язку (модеми, маршрутизатори);
- периферійні пристрої (принтери, сканери);
- приміщення (місця установки обладнання, сховища машинних носіїв інформації).

Рисунок 2.2 – Принцип побудови інформаційної мережі

Також ми можемо визначити основні типи даних, що потребують захисту в ВНЗ. До них ми можемо віднести:

- Данні, що обробляються на робочих станціях та в автоматизованих системах;
- данні на жорстких або гнучких переносних накопичувачах;
- данні на локальному жорсткому диску робочої станції;
- данні на локальному жорсткому диску сервера;
- данні, що оброблюються або зберігаються в апаратурі зв’язку;

- данні, що передаються каналами зв’язку;
- данні, що виводяться на периферійні пристрої.

Після цього ми можемо провести обстеження об’єкта інформаційної діяльності та провести категоріюваня об’єктів та інформації, що циркулює на них.

До таких об’єктів відносяться об’єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці і вони підлягають обов’язковому категоріюванню. Категоріювання здійснюється для визначення необхідного (зі встановлених нормативно-правовими актами та нормативними документами системи технічного захисту інформації рівнів) рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об’єкті. Об’єктам, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, встановлюється четверта (IV) категорія. За рішенням розпорядників (користувачів) інформації або за рішенням власників (розпорядників, користувачів) об’єктів, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, об’єктам може встановлюватися ІІІ категорія. Об’єкти, яким встановлено відповідну категорію, вносяться до Переліку категорійованих об’єктів, який ведеться власником (розпорядником, користувачем) об’єктів інформаційної діяльності.

В вищому навчальному закладі, у якому проводились роботи із захисту інформації наказом ректора було визначено перелік важливих підрозділів, інформація в яких підлягала категоріюванню та відповідно до НД ТЗІ 1.6-005-2013 «Захист інформації на об’єктах інформаційної діяльності [14][1)]. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим до-

[1)] [14] НД ТЗІ 1.6-005-2013. Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці: Чинний від 2013-04-15. К.: Нормативний документ. Системи технічного захисту інформації. 2013. 9 с.

ступом, що не становить державної таємниці» була створена комісія з категоріювання. Також відповідно до наказу Міністерства освіти і науки №273 від 28.03.2008р "Про затвердження Переліку службової інформації. Перелік службової інформації у галузі освіти і науки України» керівники структурних підрозділів повинні були розробити та надати комісії перелік документів, які створюються, обробляються або надходять до підрозділів університету, та містять конфіденційну інформацію, що є власністю держави або службовою інформацією. Приклад переліку наведено у Додатку В. На основі цього було складено акти категоріювання. Приклад акту категоріювання наведено у Додатку Г.

Після проведення категоріювання інформації можна перейти до обстеження ОІД. Метою обстеження є підготовка вихідних даних для формування вимог щодо створення комплексу ТЗІ.

Обстеження на ОІД проводить комісія, склад якої затверджується керівником установи-замовника згідно із затвердженою програмою (за необхідності).

До складу комісії включають фахівців: структурних підрозділів установи, інформаційна діяльність яких пов’язана з ІзОД, підрозділів, які заявляють створення комплексу ТЗІ, підрозділу, якому доручено супроводження робіт з ТЗІ в установі, підрозділів щодо будівництва, енергопостачання тощо.

Програма проведення обстеження на ОІД може містити:

- назву установи, що замовляє створення комплексу ТЗІ;
- назву ОІД;
- підстави для проведення обстеження (рішення керівника установи щодо створення комплексу ТЗІ);
- перелік, обсяги робіт з обстеження, терміни їх виконання;
- виконавці, спів виконавці обстеження.
- Під час обстеження проводять аналіз:

– умов функціонування ОІД, особливостей розташування його на місцевості, відносно меж контрольованої зони (КЗ), архітектурно-будівельних особливостей тощо;

– технічних засобів, що оброблятимуть ІзОД, та технічних засобів, які не використовують безпосередньо для її оброблення, визначають місця їх розташування на ОІД;

– розташування інженерних комунікацій та металоконструкцій, виявляють транзитні, незадіяні (повітряні, зовнішні, підземні) комунікації (для опрацювання пропозицій щодо їх вилучення чи доопрацювання), а також такі, що виходять за межі КЗ;

– необхідності впровадження інженерних і технічних заходів захисту від витоку ІзОД технічними каналами.

2.2 Оцінка стану захищеності інформації від несанкціонованого доступу

На різних етапах життєвого циклу інформації, що потребує захисту, неминуче постає задача оцінювання її рівня захищеності від несанкціонованого доступу до неї. Реалізація процедури оцінювання рівня захисту завжди пов’язана із вибором відповідного методу або методики оцінювання.

Оцінка рівня захищеності базується на основі методів аналізу ризиків, які поділяються на дві групи.

Перша група методів дозволяє оцінювати рівень захищеності шляхом визначення ступеня відповідності поточного рівня ризику певному набору вимог, що висуваються до забезпечення інформаційної безпеки. В якості джерела таких вимог як правило, виступають:

– рекомендації міжнародних стандартів (ISO 17799, ISO 15408 та інші);

– вимоги чинного законодавства (керівні документи Служби спеціального зв’язку та захисту інформації України та ін.);

– нормативно-правові документи підприємства, що стосуються питань інформаційної безпеки;

– рекомендації компаній-виробників програмного і апаратного забезпечення тощо.

Методи даної групи базуються на принципі системності, що закладено в стандарти безпеки. Даний принцип полягає в номінально-ранговому (якісному) підході до багатовимірної оцінки параметрів, властивостей і функцій, що реалізують механізми захисту інформації в ІТС.

Друга група методів базується на визначенні ймовірності реалізації атак, а також рівня збитку, який завдається ними. У даному випадку значення ризику обчислюється окремо для кожної атаки і, в загальному випадку, представляється добутком ймовірності проведення атаки на величину можливого збитку від цієї атаки. Значення збитку визначається власником інформаційного ресурсу, а ймовірність атаки обчислюється групою експертів, що здійснюють оцінювання. Таким чином, чим більший ризик – тим менший ризик збитку ІТС.

Нормативний документ НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу» [15][1)] установлює критерії оцінювання захищеності інформації, оброблюваної в комплексній системі, від несанкціонованого доступу.

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Критерії надають:

[1)] [15] НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: - Чинний від 1994-04-28. К.: Нормативний документ. Системи технічного захисту інформації. 1999. 24 с.

– порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах;

– базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та ін.

Цей документ призначено для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації, а також для органів, що здійснюють функції оцінювання захищеності такої інформації та контролю за її обробкою.

Цей документ відображає сучасний стан проблеми і підходів до її розв'язання. З розвитком нових тенденцій в галузі і за умови достатньої обгрунтованості документ є відкритим для включення до його складу Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України нових послуг.

В процесі оцінки спроможності комп'ютерної системи забезпечувати захист оброблюваної інформації від несанкціонованого доступу розглядаються вимоги двох видів:

– вимоги до функцій захисту (послуг безпеки);

– вимоги до гарантій.

В контексті Критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту,

проте не обов'язково являють собою точну підмножину один одного. Рівні починаються з першого і зростають до значення n, де n – унікальне для кожного виду послуг.

Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів.

Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги треба шукати в розділі “Критерії конфіденційності”. В цьому розділі описані такі послуги (в дужках наведені умовні позначення для кожної послуги): довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні (експорті/імпорті).

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. Якщо існують вимоги щодо обмеження можливості модифікації інформації, то відповідні послуги треба шукати в розділі “Критерії цілісності”. В цьому розділі описані такі послуги: довірча цілісність, адміністративна цілісність, відкат і цілісність при обміні.

Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то відповідні послуги треба шукати в розділі “Критерії доступності”. В цьому розділі описані такі послуги: використання ресурсів, стійкість до відмов, горяча заміна, відновлення після збоїв.

Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої

функції, то відповідні послуги треба шукати у розділі “Критерії спостережності”. В цьому розділі описані такі послуги: реєстрація, ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, автентифікація при обміні, автентифікація відправника (невідмова від авторства), автентифікація одержувача (невідмова від одержання).

Структуру Критеріїв показано на рис. 2.3.

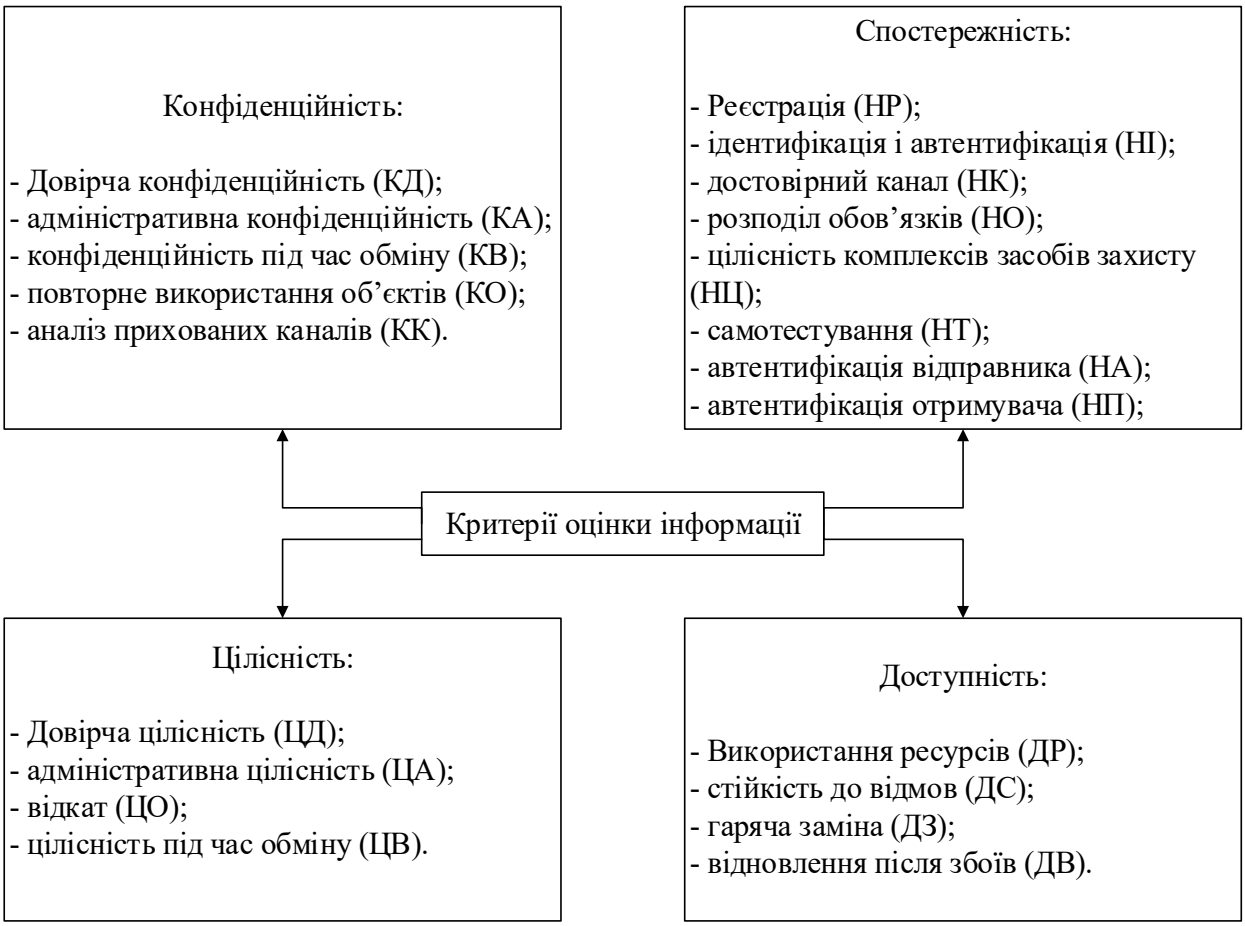

Рисунок 2.3 – Критерії оцінювання захищеності інформаційних систем

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, цей документ містить критерії гарантій, що дозволяють оцінити коректність реалізації послуг. Критерії гарантій включають вимоги до архітектури комплексу засобів захисту, середовища розро-

бки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації. В цих Критеріях вводиться сім рівнів гарантій (Г-1, ..., Г-7), які є ієрархічними. Ієрархія рівнів гарантій відбиває поступово наростаючу міру певності в тому, що реалізовані в комп'ютерній системі послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації комп'ютерної системи.

2.2.1 Критерії конфіденційності

В будь-якій КС інформація може переміщуватись в одному з двох напрямів: від користувача до об'єкта або від об'єкта до користувача. Шляхи переміщування, як і пристрої введення-виведення, можуть бути різноманітними. Конфіденційність забезпечується через додержання вимог політики безпеки щодо переміщення інформації від об'єкта до користувача або процесу. Правильне (допустиме) переміщення визначається як переміщення інформації до авторизованого користувача, можливо, через авторизований процес.

В цьому розділі Критеріїв зібрані послуги, реалізація яких дозволяє забезпечити захист інформації від несанкціонованого ознайомлення з нею (компрометації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні. Принципи, що лежать в основі реалізації послуг, визначаються політикою конфіденційності.

Довірча конфіденційність.

Послуги довірча конфіденційність і адміністративна конфіденційність, довірча цілісність і адміністративна цілісність, а також деякою мірою – використання ресурсів, є класичними послугами, що безпосередньо реалізують ту частину політики безпеки, яка складає ПРД.

Основні особливості і відмінність довірчого і адміністративного керування доступом розглянуті в НД ТЗІ 1.1-002-99 “Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу" [16][1)]. Система, яка реалізує адміністративне керування доступом, повинна гарантувати, що потоки інформації всередині системи встановлюються адміністратором і не можуть бути змінені звичайним користувачем. З іншого боку, система, яка реалізує довірче керування доступом, дозволяє звичайному користувачеві модифікувати, в т. ч. створювати нові потоки інформації всередині системи.

Послуга довірча конфіденційність дозволяє користувачеві керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Як правило, під об'єктами, що належать домену користувача, маються на увазі об'єкти, власником яких є користувач (створені користувачем).

Для відображення функціональності КС у простір, в якому не розглядаються права власності, використовується концепція матриці доступу. Матриця доступу являє собою таблицю, уздовж кожного виміру якої відкладені ідентифікатори об'єктів КС, а як елементи матриці виступають дозволені або заборонені режими доступу. Матриця доступу може бути двовимірною (наприклад, користувачі/пасивні об'єкти) або тривимірною (користувачі/процеси/пасивні об'єкти). Матриця доступу може бути повною, тобто містити вздовж кожної з осей ідентифікатори всіх існуючих в даний час об’єктів КС даного типу, або частковою. Повна тривимірна матриця доступу дозволяє точно описати хто (ідентифікатор користувача), через що (ідентифікатор процесу), до чого (ідентифікатор пасивного об'єкта) та який вид доступу може отримати.

Рівні послуги довірча конфіденційність ранжируються на підставі повноти захисту і вибірковості керування.

[1)] [16] НД ТЗІ 1.1-002-99. Загальні положення з захисту інформації в комп’ютерних системах від НСД: Чинний від 1999-04-28. К.: Нормативний документ. Системи технічного захисту інформації. 1999. 22 с.

Мінімальна довірча конфіденційність (КД-1). Найбільш слабкою мірою гарантії захисту від несанкціонованого ознайомлення є накладення обмеження на одержання інформації процесами. На цьому рівні дозволені потоки інформації від об'єкта тільки до певних процесів. Хоч і не існує обмеження на те, хто може активізувати процес, тобто, хто може одержувати інформацію, КЗЗ обмежує потоки інформації фіксованому списку процесів, ґрунтуючись на атрибутах доступу об'єктів і процесів. Користувач, домену якого належить об’єкт, може змінювати список процесів, які можуть одержувати інформацію від об'єкта. Для такої системи можна побудувати часткову або повну матрицю доступу процесів до захищених об'єктів.

Базова довірча конфіденційність (КД-2). В системі, яка реалізує послугу довірча конфіденційність на рівні КД-2, атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації. Керування правами доступу на даному рівні має невисоку вибірковість. Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів і процесів. Прикладом реалізації даного рівня послуги є реалізоване в UNIX керування доступом на підставі тріад власник / група / всі інші.

Повна довірча конфіденційність (КД-3). Основна відміна від попереднього рівня це те, що КЗЗ повинен забезпечувати більш високу вибірковість керування тим, які користувачі можуть одержати інформацію від об'єкта або ініціювати процес. Користувач, домену якого належить об'єкт, може вказати права доступу для кожного конкретного користувача і групи користувачів. Є можливим включати або вилучати користувачів із списку доступу. Для такої

системи можна побудувати повну матрицю доступу користувачів до захищених об'єктів і процесів. Така вибірковість керування може бути одержана, наприклад, за рахунок використання списків доступу.

Абсолютна довірча конфіденційність (КД-4). Даний рівень забезпечує повне керування потоками інформації в КС. Атрибути доступу користувача, процесу і об'єкта повинні містити інформацію, що використовується КЗЗ для визначення користувачів, процесів і пар процес/користувач, які можуть отримати інформацію від об'єкта. Таким чином гарантується, що інформація надсилається об’єктом потрібному користувачеві через авторизований процес. Вимоги до вибірковості керування залишаються такими ж самими, як і для попереднього рівня. Для такої системи можна побудувати повну матрицю доступу користувачів, процесів і пар користувач/процес до захищених об'єктів і процесів.

Для всіх рівнів даної послуги необхідною умовою є реалізація рівня НІ-1 послуги ідентифікація і автентифікація, що цілком очевидно. Для рівнів КД-3 і КД-4 необхідною умовою є реалізація рівня КО-1 послуги повторне використання об'єктів, оскільки, якщо при виділенні об'єкта користувачеві в цьому об'єкті міститься інформація, що залишилась від попереднього користувача, то це може призвести до витоку інформації, і всі зусилля щодо реалізації даних рівнів послуги будуть марні.

Адміністративна конфіденційність.

Послуга адміністративна конфіденційність дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів.

Згідно з політикою адміністративної конфіденційності об'єкту присвоюються атрибути доступу, що визначають домен, якому повинні належати ті користувачі або процеси, які намагаються одержати інформацію. Найбільше розповсюдження отримав механізм, коли у вигляді атрибутів доступу використовуються мітки, що визначають рівень конфіденційності інформації (об'єкта) і рівень допуску користувача. Таким чином КЗЗ на підставі порівняння міток

об'єкта і користувача може визначити, чи є користувач, що здійснює запит на доступ до інформації, авторизованим користувачем.

Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування повністю аналогічне рівням послуги довірча конфіденційність з тією відмінністю, що тільки адміністратор або авторизований адміністратором користувач має право включати і вилучати користувачів, процеси і об'єкти до/з конкретних доменів або піддоменів.

Як і для послуги довірча конфіденційність, для всіх рівнів даної послуги необхідною умовою є реалізація рівня НІ-1 послуги ідентифікація і автентифікація, а для рівнів КА-3 і КА-4 – рівня КО-1 послуги повторне використання об'єктів. Додатковою необхідною умовою для всіх рівнів даної послуги є реалізація рівня НО-1 послуги розподіл обов'язків, оскільки в системі повинні бути визначені ролі звичайного користувача і адміністратора.

Повторне використання об’єктів.

КС забезпечує послугу повторне використання об'єктів, якщо перед наданням користувачеві або процесу в розділювальному об'єкті не залишається інформації, яку він містив, і скасовуються попередні права доступу до об’єкта. Реалізація даної послуги дозволяє забезпечити захист від атак типу "збирання сміття".

Критерії не встановлюють, коли саме має виконуватися очищення об'єкта. Залежно від реалізованих механізмів можна виконувати очищення об'єкта під час його звільнення користувачем або безпосередньо перед його наданням наступному користувачу. Повторне використання об'єкта може бути реалізовано також шляхом шифрування інформації, що міститься в об'єктах, і використання керування криптографічними ключами замість знищення інформації.

Аналіз прихованих каналів.

Аналіз прихованих каналів виконується з метою виявлення і вилучення потоків інформації, що існують, але не контролюються іншими послугами. Рівні даної послуги ранжируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів.

Ніякого обмеження на смугу пропускання прихованих каналів і ніякої різниці між прихованими каналами з пам'яттю і тимчасовими прихованими каналами не робиться. Проте це не означає, що смуга пропускання прихованих каналів не повинна обмежуватись. На практиці, наприклад, може виявитись даремною реалізація послуг конфіденційності на рівнях КД-4 і КА-4, якщо в системі існують приховані канали з смугою пропускання у декілька сотень кілобайт за секунду.

Необхідною умовою для реалізації всіх рівнів даної послуги є рівень гарантій не нижче Г-3, оскільки розробник повинен виконати аналіз прихованих каналів на етапі проектування системи, а також реалізація рівня КО-1 послуги повторне використання об'єктів, оскільки можливість одержання інформації, що залишилась в об'єкті від попереднього користувача, сама собою може розглядатися як прихований канал.

Конфіденційність при обміні.

В розподіленому оточенні можуть взаємодіяти різні КЗЗ, які часто реалізують різні політики безпеки інформації. Послуги захисту інформації при обміні (конфіденційність при обміні, цілісність при обміні, ідентифікація і автентифікація при обміні, автентифікація відправника і автентифікація одержувача) дозволяють забезпечити безпеку обміну інформацією між такими КЗЗ через незахищене середовище.

КЗЗ розглядає ресурси КС в якості об'єктів і управляє взаємодією цих об'єктів відповідно до реалізованої політики безпеки інформації. Як об'єкти ресурси характеризуються двома аспектами: логічне подання (зміст, семантика, значення) і фізичне подання (форма, синтаксис). Об'єкт характеризується своїм станом (змістом), що в свою чергу характеризується атрибутами, і поводженням, яке визначає засоби зміни стану.

Локалізований КЗЗ (наприклад, операційна система з функціями захисту) розглядає тільки логічне подання об'єктів. Фізичне подання об'єктів захищене тільки від внутрішніх об'єктів, а не від впливу з боку зовнішніх сутностей (агентів). Захист від зовнішніх щодо КС загроз реалізується організаційними заходами і заходами фізичного захисту. До зовнішніх впливів схильні об'єкти, що зберігаються в енергонезалежній пам'яті (зовнішніх носіях).

У розподіленому оточенні не можна гарантувати, що зовнішній агент не може отримати доступ до фізичного подання об'єктів. Особливо це відноситься до ліній зв'язку (каналів взаємодії). Таким чином, необхідно, щоб об’єкти були захищені під час їх експорту із фізично безпечного оточення.

Послуга конфіденційність при обміні дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що в них міститься, під час їх експорту/імпорту через незахищене середовище. Найчастіше дана послуга реалізується з використанням криптографічних перетворень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Під повнотою захисту в даному випадку розуміють множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, розуміють криптостійкість використовуваних алгоритмів шифрування.

Так, реалізація даної послуги на рівні КВ-1 забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації. Прикладом реалізації може служити програмне шифрування файлів перед їх передачею каналами зв'язку або прозоре шифрування файлів перед їх записуванням на диск.

Реалізація даної послуги на рівні КВ-2 дозволяє керувати засобами експорту і імпорту об'єктів і додатково забезпечує захист від помилок користувача та інших випадкових помилок, а також від витоку інформації при підключенні несанкціонованих користувачів.

Реалізація даної послуги на рівні КВ-3 дозволяє забезпечити криптографічне розділення каналів обміну і є необхідною для забезпечення взаємодії

КЗЗ, що підтримують обробку інформації рівня секретної або реалізують різні політики безпеки.

Реалізація даної послуги на рівні КВ-3 дозволяє забезпечити захист від компрометації за рахунок аналізу трафіку і від витоку інформації прихованими каналах обміну, що існують. Для реалізації даного рівня від розробника вимагається виконання аналізу прихованих каналів.

2.2.2 Критерії цілісності

Цілісність забезпечується дотриманням вимог політики безпеки щодо переміщення інформації до об’єкта з боку користувача або процесу. Правильне (допустиме) переміщення визначається як переміщення інформації до об’єкта від авторизованого користувача або процесу

В даному розділі Критеріїв зібрані послуги, реалізація яких дозволяє забезпечити захист інформації від несанкціонованої модифікації (включаючи її знищення). Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні. Принципи, що лежать в основі реалізації послуг, визначаються політикою цілісності.

Довірча цілісність.

Дана послуга дозволяє користувачеві керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна довірча цілісність (ЦД-1). На даному рівні користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку інших користувачів. Керування правами має грубу вибірковість (на рівні розподілу потоків інформації між групами користувачів). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів.

Базова довірча цілісність (ЦД-2). Більш сильним методом запобігання неавторизованій модифікації є накладення обмежень на те, який процес або група процесів може модифікувати об’єкт. Користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку процесів і груп процесів. Для такої системи можна побудувати часткову матрицю доступу процесів до захищених об'єктів.

Повна довірча цілісність (ЦД-3). Основна відмінність між рівнями ЦД-2 і ЦД-3 полягає в тому, що на даному рівні надається більш висока вибірковість керування тим, які процеси можуть або не можуть модифікувати об'єкт. Для такої системи можна побудувати повну матрицю доступу процесів до захищених об'єктів.

Абсолютна довірча цілісність (ЦД-4). Реалізація послуги довірча цілісність на даному рівні забезпечує повне керування потоками інформації всередині системи. Атрибути доступу користувача, процесу і об'єкта повинні містити інформацію, що використовується КЗЗ для визначення користувачів, процесів і пар процес/користувач, які можуть модифікувати об'єкт. Це гарантує, що модифікація об'єкта здійснюється авторизованим користувачем за допомогою авторизованого процесу. Для такої системи можна побудувати повну матрицю доступу користувачів, процесів і пар користувач/ процес до захищених об'єктів і процесів.

Для всіх рівнів даної послуги необхідною умовою є реалізація рівня НІ-1 послуги ідентифікація і автентифікація, що цілком очевидно. Для рівнів ЦД-3 і ЦД-4 необхідною умовою є реалізація рівня КО-1 послуги повторне використання об'єктів, оскільки її відсутність може привести до того, що під час подання об'єкта користувачеві в цьому об'єкті вже міститься деяка інформація, джерело якої не визначено.

Адміністративна цілісність.

Ця послуга дозволяє адміністратору чи спеціально авторизованому користувачу керувати потоками інформації від користувачів і процесів до захи-

щених об'єктів. Згідно з політикою адміністративної цілісності (в повній аналогії з адміністративною конфіденційністю) об'єкту привласнюються атрибути доступу, що визначають домен, якому повинні належати ті користувачі чи процеси, які намагаються модифікувати об’єкт. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування аналогічно рівням послуги довірча цілісність з тією відмінністю, що тільки адміністратор або авторизований адміністратором користувач має право включати і вилучати користувачів, процеси і об'єкти до/з конкретних доменів або піддоменів.

Як і для послуги довірча цілісність для всіх рівнів даної послуги необхідною умовою є реалізація рівня НІ-1 послуги ідентифікація і автентифікація, а для рівнів КА-3 і КА-4 − рівня ДО-1 послуги повторне використання об'єктів. Додатковою необхідною умовою для всіх рівнів даної послуги є реалізація рівня НО-1 послуги розподіл обов'язків, оскільки в системі повинні бути визначені ролі звичайного користувача і адміністратора.

Відкат.

Відкат є багатосторонньою послугою, що дозволяє відновлюватися після помилок користувача, збоїв програмного забезпечення або апаратури і підтримувати цілісність баз даних, додатків, побудованих на транзакціях і т. ін. Дана послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об’єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

Мається на увазі, що відкат – завжди доступна автоматизована послуга. Використання відкладеного резервування, що вимагає втручання користувача для завантаження резервного носія, не є реалізацією відкату. Якщо система реалізує дану послугу, то її використання має фіксуватись в журналі. Відміна операції не повинна приводити до видалення з журналу запису про операцію, яка пізніше була відмінена.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НИ-1 послуги ідентифікація і автентифікація

Цілісність при обміні.

Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, як цифровий підпис і коди автентифікації повідомлень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Під повнотою захисту, як і для послуги конфіденційність при обміні, треба розуміти множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, слід розуміти криптостійкість використовуваних алгоритмів шифрування.

Рівень ЦВ-1 даної послуги забезпечує мінімальний захист. На включення даного рівня в свій рейтинг може претендувати система, що дозволить на підставі цифрового підпису перевіряти цілісність функціонуючого на ЕОМ ПЗ, або система електронної пошти, що забезпечує цифровий підпис повідомлень.

Реалізація даної послуги на рівні ЦВ-2 додатково дозволяє керувати засобами експорту і імпорту об'єктів і додатково забезпечує захист від помилок користувача та інших випадкових помилок, а також від модифікації інформації у разі підключенні несанкціонованих користувачів.

Реалізація даної послуги на рівні ЦВ-2 додатково дозволяє забезпечити виявлення випадкових або навмисних порушень цілісності не тільки окремих повідомлень, але і потоків повідомлень в цілому.

2.2.3 Критерії доступності

Для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ КС, що оцінюється, повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної

інформації, на певному проміжку часу і гарантувати спроможність КС функціонувати в разі відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

Використання ресурсів.

Дана послуга дозволяє керувати використанням послуг і ресурсів користувачами. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

Найслабкішою формою контролю за використанням ресурсів є використання квот. Всі захищені об'єкти КС (наприклад, дисковий простір, тривалість сеансу, час використання центрального процесора і т. ін.) повинні ідентифікуватись і контролюватись диспетчером доступу шляхом накладення обмежень на максимальний обсяг даного ресурсу, що може бути виділений користувачу. На даному рівні послуги немає гарантій, що користувач не зможе повністю захопити решту певного ресурсу, обмежуючи тим самим доступ до нього інших користувачів.

Рівень послуги ДР-2 являє собою реалізацію досконалішої форми квот. Квоти використовуються таким чином, щоб гарантувати, що жоден користувач не зможе захопити решту певного ресурсу, дозволяючи виділяти менші обсяги ресурсів, ніж максимальна квота користувача, гарантуючи таким чином іншому користувачеві доступ до розділюваного ресурсу.

Рівень послуги ДР-3 додатково дозволяє управляти пріоритетністю використання ресурсів. Користувачі групуються адміністратором так, щоб визначити пріоритетні групи. Таким чином, у разі високого завантаження КС може знаходитись в стані, коли тільки користувачі, які мають високий приорітет, можуть мати доступ до системи за рахунок інших користувачів.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НО-1 послуги розподіл обов'язків (і як наслідок, − рівня НІ-1 послуги ідентифікація і автентифікація).

Стійкість до відмов.

Стійкість до відмов гарантує доступність КС (можливість використання інформації, окремих функцій чи КС в цілому) після відмови її компоненту. Рівні даної послуги ранжируються на підставі спроможності КЗЗ забезпечити можливість КС продовжувати функціонування залежно від кількості відмов і послуг, доступних після відмови.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НО-1 послуги розподіл обов'язків (і, як наслідок, − рівня НІ-1 послуги ідентифікація і автентифікація).

Гаряча заміна.

Ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів. Рівні даної послуги ранжируються на підставі повноти захисту. Основна мета реалізації даної послуги полягає в тому, що встановлення нової версії системи, відмова або заміна захищеного компонента не повинні призводити до того, що система потрапить до стану, коли політика безпеки, що реалізується нею, стане скомпрометованою.

Необхідною умовою для реалізації всіх рівнів даної послуги, є реалізація рівня НО-1 послуги розподіл обов'язків (і, як наслідок- рівня НІ-1 послуги ідентифікація і автентифікація), а для рівнів ДЗ-2 і ДЗ-3 − рівня ДС-1 послуги стійкість до відмов, оскільки для того, щоб забезпечити можливість гарячої заміни компонента, система повинна забезпечувати свою працездатність у разі відмови даного компонента.

Відновлення після збоїв.

Дана послуга забезпечує повернення КС до відомого захищеного стану після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення. Відновлення може вимагати втручання оператора, а для її більш високих рівнів реалізації КЗЗ може продукувати відновлення працездатності автоматично. Якщо відновлення неможливе, то КЗЗ повинен переводити систему до стану, з якого її може повернути до нормального функціонування тільки адміністратор.

Необхідною умовою для реалізації всіх рівнів даної послуги − реалізація рівня НО-1 послуги розподіл обов'язків (і, як наслідок, − рівня НІ-1 послуги ідентифікація і автентифікація).

2.2.4 Критерії спостережності

Для того, щоб КС могла бути оцінена на відповідність критеріям спостереженості, КЗЗ повинен надавати послуги щодо забезпечення відповідальності користувача за свої дії і щодо підтримки спроможності КЗЗ виконувати свої функції. Спостережність забезпечується в КС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача.

Реєстрація об’єктів.

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності виявлення потенційних порушень.

Реєстрація – це процес розпізнавання, фіксування і аналізу дій і подій, що пов'язані з дотриманням політики безпеки інформації. Використання засобів перегляду і аналізу журналів, а особливо засобів налагодження механізмів фіксування подій, має бути прерогативою спеціально авторизованих користувачів.

Вибір фізичного носія, що використовується для зберігання даних реєстрації, повинен відповідати способу використання і обсягу даних. Будь-яке переміщення таких даних має виконуватись способом, що гарантує їх безпеку. Одним із найбезпечніших, хоч і досить дорогих рішень, є використання носіїв з одноразовим записом. В будь-якому випадку рівень захищеності даних реєстрації має бути не нижче, ніж рівень захищеності даних користувачів, яку

забезпечують реалізовані послуги конфіденційності і цілісності. Повинні бути вироблені угоди щодо планування і ведення архівів даних реєстрації.

Для жодного з рівнів послуги не встановлюється ніякого фіксованого набору контрольованих подій, оскільки для кожної системи їх перелік може бути специфічним. Критична для безпеки подія визначається як подія, пов'язана з звертанням до якої-небудь послуги безпеки або результатів виконання якої-небудь функції КЗЗ, або як будь-яка інша подія, яка хоч прямо і не пов'язана з функціонуванням механізмів, які реалізують послуги безпеки, але може призвести до порушення політики безпеки. Остання група подій визначається як така, що має непряме відношення до безпеки. Для визначення ступеню небезпеки таких подій часто необхідним має бути їх аналіз у контексті інших подій, що відбулися.

Для реалізації найбільш високих рівнів даної послуги необхідна наявність засобів аналізу журналу реєстрації. Засоби аналізу – це засоби, що виконують більш складну, ніж перегляд, оцінку журналу реєстрації з метою виявлення можливих порушень політики безпеки. Ці засоби повинні надавати адміністратору можливість виконання сортування, фільтрації за певними критеріями та інших подібних операцій. КЗЗ повинен надавати адміністратору можливість вибирати події, що реєструються. Це може бути досягнено або через "передвибірки", або "поствибірки". Передвиборка подій, що реєструються, дозволяє виділити під час ініціалізації системи з всієї множини доступних для реєстрації подій підмножину тих, що необхідно реєструвати в журналі. Використовуючи передвибірку, адміністратор може зменшити кількість реально реєстрованих подій і, отже, розмір остаточного журнального файла. Недоліком предвибірки є те, що ті події, які не були вибрані, не можуть уже пізніше бути проаналізовані, навіть, якщо постає така необхідність. Перевага поствибірки полягає в гнучкості можливості аналізу "пост-фактум", проте така організація ведення журнального файла вимагає виділення значного обсягу пам'яті для даних реєстрації.

Для реалізації найбільш високого рівня даної послуги (НР-5) необхідно, щоб аналіз даних реєстрації здійснювався в реальному часі.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НИ-1 послуги ідентифікація і автентифікація, а для рівнів вище НР-1 – рівня НО-1 послуги розподіл обов'язків.

Ідентифікація і автинтифікація.

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача (фізичної особи), який намагається одержати доступ до КС. Хоч поняття ідентифікація і автентифікація відрізняються, на практиці обидва ці процеси важко буває поділити. Важливо, щоб в кінцевому підсумку були підстави стверджувати, що система має справу з конкретним відомим їй користувачем. За результатами ідентифікації і автентифікації користувача система (КЗЗ), по-перше, приймає рішення про те, чи дозволено даному користувачеві ввійти в систему, і, по-друге, використовує одержані результати надалі для здійснення розмежування доступу на підставі атрибутів доступу користувача, що увійшов.

Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації Відомі три основних типа автентифікації: щось, відоме користувачеві; щось, чим володіє користувач; щось, властиве користувачеві.

Пароль, персональний номер або інша подібна інформація є прикладом того, що називається "дещо, відоме користувачеві". Даний тип автентифікації є простим у реалізації і достатньо ефективним. Проте його ефективність обмежена простотою його повторення: достатньо просто обчислити або вгадати інформацію автентифікації, а для її дублювання не вимагається спеціального устаткування чи можливостей.

Такі фізичні об'єкти як смарт-карта, магнітна картка, генератор запитів-відповідей, електронний ключ або фізично прошитий криптографічний ключ є прикладами того, що називається "дещо, чим володіє користувач". Основною перевагою даного типу автентифікації є складність або висока вартість дублю-

вання інформації автентифікації. З іншого боку, втрата пристрою автентифікації може стати причиною потенційної компрометації. Проте, в більшості випадків достатньо просто установити факт втрати такого пристрою і попередити адміністратора безпеки про необхідність зміни інформації автентифікації.

Результати таких біометричних вимірювань, як відбитки пальців, параметри райдужної оболонки ока або геометрія руки служать прикладами того, що називають "дещо, що властиве користувачеві". Реалізація даного типу автентифікації повинна забезпечувати значно сильнішу автентифікацію, ніж два попередніх типи. Основною перешкодою для використання даного механізму є висока вартість пристроїв автентифікації. Крім того, використання цих достатньо дорогих засобів автентифікації не гарантує безпомилкової роботи. Рівень (ймовірність) помилок першого і другого роду для таких пристроїв може стати непридатним для деяких застосувань.

Для підвищення ефективності захисту від специфічних загроз несанкціонованого доступу для найбільш високого рівня даної послуги (НІ-3) вимагається використання комбінації мінімум двох різних типів автентифікації, наприклад, введеного з клавіатури пароля і носимого ідентифікатора.

Для реалізації рівнів НІ-2 і НІ-3 даної послуги необхідною умовою є реалізація рівня НК-1 послуги достовірний канал.

Достовірний канал.

Дана послуга дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається). Рівні даної послуги ранжируються в залежності від того, чи має КЗЗ можливість ініціювати захищений обмін, чи це є прерогативою користувача.

Реалізація даної послуги є необхідною умовою для реалізації рівнів НІ-2 і НИ-3 послуги ідентифікація і автентифікація.

Розподіл обов’язків.

Дана послуга дозволяє знизити ймовірність навмисних або помилкових неавторизованих дій користувача або адміністратора і величину потенційних збитків від таких дій. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Система, що претендує на включення даної послуги до рейтингу, повинна передусім забезпечувати існування ролей для адміністратора і звичайного користувача (рівень НО-1).

Для наступного рівня даної послуги вимагається, щоб система підтримувала дві або більше адміністративних ролей зі специфічними наборами адміністративних обов'язків. Одна з цих ролей повинна бути роллю адміністратора безпеки (ця роль може бути поділена на ролі адміністратора реєстрації (аудиту) і адміністратора каталогів або облікових карток користувачів). Роль адміністратора безпеки повинна бути визначена так, щоб обов'язки, що мають відношення до безпеки, могли бути виконані тільки в цій ролі. Ролі не обов’язково мають бути абсолютно взаємовиключаючими, оскільки деякі функції або команди можуть знадобитись і адміністратору, і користувачу, або різним адміністраторам і таін.

Основною відмінністю рівня НО-3 від рівня НО-2 є необхідність визначення ролей для звичайних користувачів.

Цілісність комплексів засобів захисту.

Дана послуга визначає міру спроможності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Жодна КС не може вважатися захищеною, якщо самі засоби захисту є об'єктом для несанкціонованого впливу. У зв'язку з цим рівень НЦ-1 даної послуги є необхідною умовою для абсолютно всіх рівнів усіх інших послуг.

Для рівня НЦ-1 даної послуги необхідно, щоб КЗЗ мав можливість перевіряти свою цілісність і в разі виявлення її порушення переводити систему в стан, з якого її може вивести тільки адміністратор.

Для рівня НЦ-2 необхідно, щоб КЗЗ підтримував власний домен виконання, відмінний від доменів виконання всіх інших процесів, захищаючи себе

від зовнішніх впливів. Дана вимога є однією з вимог до реалізації диспетчера доступу. Як правило, реалізація даної вимоги повинна забезпечуватися можливостями апаратного забезпечення ОС.

Для рівня НЦ-3 необхідно, щоб КЗЗ забезпечував керування захищеними ресурсами таким чином, щоб не існувало можливості доступу до ресурсів, минаючи КЗЗ. Дана вимога є другою функціональною вимогою до реалізації диспетчера доступу.

Необхідною умовою для реалізації рівня НЦ-1 даної послуги є реалізація рівнів НО-1 послуги розподіл обов'язків і НР-1 послуги реєстрація, оскільки КЗЗ повинен мати можливість ставити до відома адміністратора про факти порушення своєї цілісності.

Самотестування.

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів за ініціативою користувача, в процесі запуску або штатної роботи.

Необхідною умовою для всіх рівнів даної послуги є реалізація рівня НО-1 послуги розподіл обов'язків.

Ідентифікація а автентифікація при обміні.

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Реалізація рівня НВ-1 даної послуги дозволяє виключити можливість несанкціонованого зовнішнього підключення і є необхідною умовою для реалізації високих рівнів послуг конфіденційності і цілісності при обміні.

Реалізація рівня НВ-2 даної послуги дозволяє виключити можливість несанкціонованого використання встановленого авторизованого підключення.

Реалізація рівня НВ-3 даної послуги дозволяє виключити можливість деяких видів внутрішнього шахрайства.

Автентифікація відправка.

Ця послуга дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

Найширше для реалізації даної послуги, як і послуги автентифікації одержувача, використовується цифровий підпис, оскільки використання несиметричних криптоалгоритмів (на відміну від симетричних) дозволяє забезпечити захист від внутрішнього шахрайства і автентифікацію за взаємної недовіри сторін.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НИ-1 послуги ідентифікація і автентифікація.

Автентифікація одерживуча.

Ця послуга дає можливість забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НІ-1 послуги ідентифікація і автентифікація.

2.3 Постановка завдання та основні напрямки вирішення проблеми стосовно захисту інформації в вищих навчальних закладах

Наскільки актуальна проблема захисту інформації від різних загроз, можна побачити на прикладі даних, опублікованих Computer Security Institute (Сан-Франциско, штат Каліфорнія, США), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин:

- несанкціонований доступ — 2 %;
- укорінення вірусів — 3 %;

- технічні відмови апаратури мережі — 20 %;
- цілеспрямовані дії персоналу — 20 %;
- помилки персоналу (недостатній рівень кваліфікації) — 55%.

Таким чином, однією з потенційних загроз для інформації в інформаційних системах слід вважати цілеспрямовані або випадкові деструктивні дії персоналу (людський фактор), оскільки вони становлять 75 % усіх випадків.

Відповідно до вимог законів України "Про інформацію", "Про державну таємницю" та "Про захист інформації в автоматизованих системах" основним об'єктом захисту в інформаційних системах є інформація з обмеженим доступом, що становить державну або іншу, передбачену законодавством України, таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження. Засоби та заходи захисту такої інформації можно розділити на два основні типи:

- технічний захист інформації;
- організаційний захист інформації.
- структурну схему типової КСЗІ наведено на рис. 2.4.

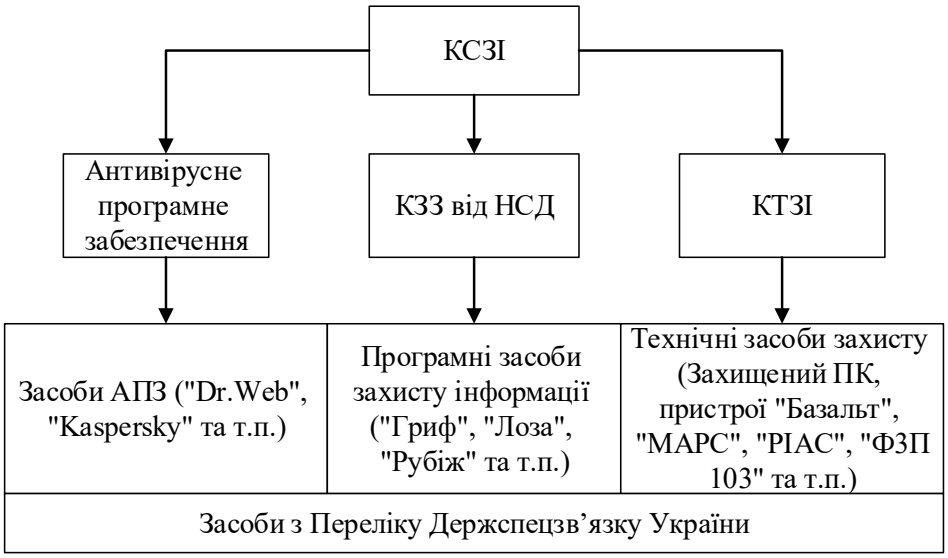

Рисунок 2.4 – Структурна схема типової КСЗІ АС

Для того щоб визначитись із основними напрямками побудови надійної системи захисту інформації необхідно розглянути кожен із цих типів більш детально.

2.3.1 Програмний метод захисту інформації

До програмного методу захисту інформації можна віднести такі системи захисту як:

- системи розмежування доступу до інформації;
- системи ідентифікації і автентифікації;
- системи аудиту та моніторингу;
- системи антивірусного захисту.

Оскільки в даній магістерській роботі проводиться розробка та аналіз комплексної системи захисту інформації в вищому навчальному закладі, то доцільно буде розглянути лише систему розмежування доступу до інформації, так як інші системи програмного захисту не є критичними для побудови КСЗІ.

Станом на 2019 рік в Україні існує три основних програмних продукта для побудови СЗІ що мають експертний висновок – ГРИФ, Лоза та Рубіж-РСО. Розглянемо ці програмні продукти більш детально та проведемо їх порівняльний аналіз.

Система «ЛОЗА» – це програмний засіб захисту інформації від несанкціонованого доступу в автоматизованих системах (зазвичай це автономний комп’ютер). Система «ЛОЗА» може працювати під керуванням операційних систем Windows XP/Vista/7/8/8.1/2003/2008/2012 (32- та 64-розрядних версіях).

Система «ЛОЗА» реалізує всі стандартні функції, необхідні для надійного захисту інформації від несанкціонованого доступу і для побудови комплексної системи захисту інформації.

Система «ЛОЗА» може використовуватись для захисту інформації, що становить державну таємницю.

Контроль друку та експорту:

– система «ЛОЗА» забезпечує можливість встановлення дозволу/заборони друку та експорту на рівні окремих документів;

– для підсилення контролю система «ЛОЗА» дозволяє забезпечити присутність адміністратора або іншої уповноваженої особи під час друку та експорту (за рахунок необхідності введення пароля).

– контроль входу користувачів до системи:

– у конфігурації «Підвищена безпека» вхід здійснюється тільки після введення пароля та встановлення ключового диска (може використовуватись звичайна дискета, «флешка» або CD/DVD-диск); діє жорстка політика паролів та політика блокування користувачів, яка протидіє підбору паролів;

– у конфігурації «Стандартна безпека» для входу достатньо ввести пароль; політика паролів менш жорстка, ніж в конфігурації «Підвищена безпека».

– реєстрація подій:

– система «ЛОЗА» веде захищений журнал, в якому реєструються всі події, важливі для захисту інформації;

– аналіз журналу та протоколів роботи не потребує спеціальної кваліфікації;

– журнал подій ніколи не перезаписується: після досягнення граничного розміру журналу всі події зберігаються у файлі на жорсткому диску;

– система «ЛОЗА» забезпечує докладну реєстрацію подій друку та експорту; поряд із стандартною інформацією у журналі фіксуються гриф та обліковий номер документа, а також серійний номер носія, на якому зберігається документ, та носія, на який здійснюється експорт;

– адміністратор має можливість формування протоколу друку документів.

Профіль системи:

Для конфігурації «Підвищена безпека»:КА-3, КО-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НІ-3, НК-1, НО-2, НЦ-2, НТ-2.

Для конфігурації «Стандартна безпека»:КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДС-1,ДЗ-1, ДВ-1, НР-2, НІ-2, НІ-3, НК-1, НО-2, НЦ-2, НТ-2.

Гриф-ХР версії 1.хх − комплекс засобів захисту інформації від несанкціонованого доступу в автоматизованій системі класу 1

Комплекс засобів захисту (КЗЗ) інформації "Гриф-ХР" призначений для забезпечення захисту інформації з обмеженим доступом (ІзОД), у тому числі інформації, що становить державну таємницю, конфіденційної інформації, яка є власністю держави, інформації, що становить комерційну таємницю, при її обробці в автоматизованих системах класу "1" на базі персональних комп'ютерів під управлінням операційної системи (ОС) MS Windows XP Professional.

Комплекс дозволяє створити на базі персонального комп'ютера спеціалізоване робоче місце з обмеженим кругом користувачів і забезпечити захист оброблюваної ІзОД від загроз цілісності, конфіденційності і доступності при реалізації політики адміністративного управління доступом до інформації, тобто захистити інформацію від несанкціонованого ознайомлення, модифікації, видалення.

Комплекс «Гриф-ХР» реалізує наступні функції:

- ідентифікацію і автентифікацію користувачів на підставі імені, пароля і носія даних автентифікації (дискети, Flash, інших змінних дисків або Touch Memory), що дозволяє розпізнати авторизованого користувача і надалі реагувати на запити цього користувача відповідно до його повноважень;
- блокування завантаження ОС із змінних носіїв (ця функція реалізується апаратною компонентою, яка поставляється опційно) що дозволяє заблокувати завантаження ОС і використання ПЕОМ сторонньою особою, а також гарантувати включення в роботу усіх компонентів КСЗ;
- розмежування обов'язків користувачів і виділення декількох ролей адміністраторів, які можуть виконувати різні функції по адмініструванню

(реєстрацію ресурсів, що захищаються, реєстрацію користувачів, призначення прав доступу, обробку протоколів аудиту і тому подібне);

– розмежування доступу користувачів до каталогів (текам) відповідно до принципів адміністративного управління доступом, що дозволяє організувати спільну роботу на ПЕОМ декількох користувачів, що мають різні службові обов'язки і права по доступу до ІзОД;

– управління потоками інформації і блокування потоків інформації, що призводять до зниження її конфіденційності (наприклад, при за рахунок копіювання файлів або перенесення інформації через системний буфер обміну); контроль за виводом інформації на друк;

– контроль за експортом інформації на змінні носії і її імпортом;

– гарантоване видалення інформації шляхом затирання вмісту файлів, ІзОД;

– розмежування доступу прикладних програм до захищених каталогів, що дозволяє забезпечити захист ІзОД від несанкціонованого або випадкового видалення, модифікації і дотримати технологію її обробки;

– контроль цілісності прикладного програмного забезпечення і ПЗ КЗЗ а також блокування завантаження програм, цілісність яких порушена, що дозволяє забезпечити захист від вірусів і дотримання технології обробки ІзОД; контроль за використанням дискового простору користувачами (квоти), що виключає можливість блокування одним із користувачів роботи інших;

– можливість блокування пристроїв інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;

– контроль цілісності і само тестування КЗЗ при старті;

– відновлення функціонування КСЗ після збоїв, що гарантує доступність інформації при дотриманні правил доступу до неї;

– реєстрацію подій (входу користувача в ОС, спроб несанкціонованого доступу, фактів запуску програм, роботи з ІзОД, виводу на друк і так

далі) в спеціальних протоколах аудиту що дозволяє адміністраторам контролювати доступ до інформації, стежити за тим, як використовується КСЗ, а також правильно його конфігурувати.

Профіль системи:

КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1,ДЗ-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2 з рівнем гарантій Г-4.

Рубіж-РСО − Комплекс засобів захисту від НСД в автоматизованій системі.

Комплекс засобів захисту від НСД забезпечує:

- захист від несанкціонованого доступу до інформації, що обробляється;
- контроль роботи комплексу технічних засобів захисту інформації від витоку фізичними каналами, при включенні до складу КЗЗ приладу контролю активності технічних засобів захисту РІАС-4КА;
- контроль цілісності комплексу технічних засобів захисту.

Функції ПЗ КЗЗ "Рубіж-РСО":

- ідентифікація приладу контролю активності технічних засобів захисту;
- можливість настроювати параметри, що надається Адміністратору безпеки;
- посилена автентифікація – при спробі користувача авторизуватись в операційній системі відбувається перевірка КЗЗ від НСД. Якщо виявлені порушення, то користувач, що не є Адміністратором безпеки не зможе здійснити вхід до системи;
- моніторинг – вмикається тоді, коли адміністратор безпеки переведе КЗЗ “Рубіж-РСО” в режим роботи Нормальний, і, вимикається, коли КЗЗ “Рубіж-РСО” переводиться в режим роботи Службовий. Тобто контроль Комплексу ТЗЗ відбувається в сеансі роботи користувача, якщо він не належить групі користувачів RSO_GROUP_4 (опціонально);

– інформування – у випадку виявлення порушень функціонування Комплексу ТЗЗ буде надано користувачеві інформативне повідомлення з певним часом аварійного завершення сеансу на виявлення та можливого вирішення ситуації зі сторони користувача, якщо це можливо, та здійснений запис в БД ПЗ КЗЗ “Рубіж-РСО”. Якщо час аварійного завершення сеансу вийшов і Комплекс ТЗЗ не відновлений, система примусово завершить сеанс користувача і переведеться в режим Службовий.

Профіль системи:

КА-2, КО-1, ЦА-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-1, НТ-2 з рівнем гарантій Г-3.

Порівняльний аналіз систем ГРИФ, Лоза версії 4 та Рубіж-РСО наведено у табл. 2.2.

Таблиця 2.2 – Порівняльний аналіз програмних комплексів захисту інформації

Характеристики	Лоза	Гриф	Рубіж РСО
Функціональний профіль	КА-3,КО-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НІ-3, НК-1, НО-2, НЦ-2, НТ-2. КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДС-1,ДЗ-1, ДВ-1, НР-2, НІ-2, НІ-3, НК-1, НО-2, НЦ-2, НТ-2.	КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1,ДЗ-1, ДВ-1, НР-2, НІ-3, НК-1, НО-2, НЦ-2, НТ-2.	КА-2, КО-1, ЦА-1, ДВ-1, НР-2, НІ-3, НК-1, НО-2, НЦ-1, НТ-2.

Продовження таблиці 2.2

Характеристики	Лоза	Гриф	Рубіж РСО
Функціональні послуги	− адміністративна конфіденц.; − довірча конфіденц.; − повторне використання об’єктів; − довірча цілісність; − адміністративна цілісність; − стійкість до відмов; − гаряча заміна; − відновлення після збоїв; − реєстрація, ідентифікація і автентифікація; − достовірний канал; − розподіл обов'язків; − цілісність КЗЗ; − самотестування;	− адміністративна конфіденц.; − повторне використання об’єктів; − відкат; адміністративна цілісність; − відновлення після збоїв; − реєстрація, ідентифікація і автентифікація; − достовірний канал; − розподіл обов'язків; − цілісність КЗЗ; −самотестування;	− адміністративна конфіденц.; − повторне використання об’єктів; − відкат; − відновлення після збоїв; − реєстрація, ідентифікація і автентифікація; − достовірний канал; − розподіл обов'язків; − цілісність КЗЗ; − самотестування;
Операційна система	MS Windows XP/Vista/7/ Server 2003/ Server 2008	MS Windows XP/Vista/7/ Server 2008	MS Windows 2000/XP
Ідентифікація та автентифікація	На підставі імені, паролю, носія TouchMemory, апаратного ідентифікатора.	На підставі імені, паролю, носія TouchMemory	На підставі імені, паролю
Рівень гарантії	Г4	Г4	Г3
Ціна	від 3 600 грн.	4 200 грн.	2 700 грн.

2.3.2 Апаратний метод захисту інформації

Для об’єктів електронно-обчислювальної техніки, на яких циркулює інформація, що становить державну таємницю, обов’язковим є створення та атестація комплексу технічного захисту інформації, який має забезпечувати захист інформації з обмеженим доступом від витоку технічними каналами, а саме каналам побічних електромагнітних випромінювань та наведень (ПЕМВН). На об’єктах, де циркулює інформація для службового користування створення комплексу технічного захисту не є обов’язковим і відбувається за бажанням.

На етапі розробки та впровадження комплексної системи захисту інформації, яка становить державну таємницю, в ІТС необхідно створити та провести первинну атестацію КТЗІ, яка включає такі види робіт:

- проведення спеціальних досліджень персональної електронно-обчислювальної машини (ПЕОМ) по каналах ПЕМВН, при якому визначаються можливі канали витоку інформації;
- визначення необхідності встановлення активних та/або пасивних засобів захисту;
- встановлення обладнання з Переліку засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність захисту якої визначено законодавством України;
- розробка програми та методики випробовувань;
- проведення оцінки захищеності інформації з обмеженим доступом від витоку технічними каналами на об’єкті ЕОТ (атестація комплексу ТЗІ).
- акустичним та віброакустичним;
- акустоелектричними;
- за рахунок застосування закладних пристроїв.

Необхідність проведення періодичного контролю захищеності інформації від витоку каналами побічних електромагнітних випромінювань і наводів (ПЕМВН) визначається нормативно-законодавчими актами з питань ТЗІ.

З метою запобігання витоку (технічними каналами) мовної інформації з обмеженим доступом за межі приміщення (кабінету) в якому проводяться конфіденційні переговори та наради, на яких обговорюються відомості, що відносяться до комерційної або державної таємниці пропонуємо створення та атестацію захищених приміщень (кабінетів) для ведення конфіденційних переговорів та нарад.

Захист приміщення від витоку інформації з обмеженим доступом акустичним та віброакустичним каналами здійснюється шляхом проведення дослідження приміщення на можливий витік мовної інформації зазначеними каналами.

За отриманими результатами приймається рішення про встановлення активних засобів захисту або додаткову звукоізоляцію приміщення:

- дослідження приміщення на можливий витік мовної інформації акустичним та віброакустичним каналами;
- монтаж генератора шуму типу “Базальт-4ГА” або “Марс-ТЗО;
- монтаж та підключення вібровипромінювача, акустичного випромінювача;
- монтаж пульта дистанційного керування системою активного захисту по радіоканалу;
- оцінка захищеності мовної інформації від витоку її акустичним та віброакустичним каналами з застосуванням генератора шуму типу“Базальт-4ГА” або “Марс-ТЗО-4-2”.

Захист приміщення від витоку інформації з обмеженим доступом акустоелектричними каналами здійснюється шляхом проведення спеціальних досліджень технічних засобів (комп’ютера, телевізора, DVD – програвача, музичного центру, холодильника, кондиціонера та іншої побутової техніки), розміщених в приміщенні, на наявність акустоелектричних перетворювань по радіоефіру, в мережі електроживлення, лініях передачі та прийому сигналів. Спеціальним дослідженням підлягає також пожежна та/або охоронна сигналізації на наявність акустоелектричних перетворювань по радіоефіру, лініях передачі та прийому сигналів.

Захист приміщення від витоку інформації з обмеженим доступом за рахунок застосування закладних пристроїв здійснюється шляхом проведення спецобстеження.

Система віброакустичного зашумлення (маскування) призначена для запобігання прослуховування приміщення шляхом створення шумового сигналу в діапазоні звукових частот. Така система складається, як правило, з генератора шуму та комплекту акустичних і вібраційних випромінювачів. Відкривши інтернет можна знайти декілька таких систем українського виробництва,

наприклад: „МАРС-ТЗО-4-2”, „ОЦЗІ-ВА”, „РІАС-2ГС”, „РІАС-2ГМ”, „БАЗАЛЬТ-4ГА”.

Генератори акустического шуму стаціонарний „РІАС-2ГС” і мобільний „РІАС-2ГМ” представляють собою один і той же пристрій з однією різницею – замість пазів під викрутку на регулювальних потенціометрах встановлені ручки. Оскільки вищезазначені пристрої мають однакові характеристиками, то доцільно розглядати їх разом. Будемо називати обидва пристрої „РІАС”.

До речі, незрозуміло, як використовувати мобільний генератор РІАС якщо він майже нічим не відрізняється від стаціонарного?

Таким чином, на сьогоднішній день є сенс розглядати три генератори віброакустичного зашумлення:

- генератор шумових сігналів „МАРС-ТЗО-4-2”;
- генератор акустичного шуму „РІАС”;
- пристрій захисту „БАЗАЛЬТ-4ГА”.

Всі перелічені пристрої, незважаючи на різні назви, представляють собою генератор коливань у звуковому діапазоні. Діапазон частот генераторів і ряд інших обов’язкових вимог до цих виробів визначається документом «Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації», затвердженого наказом ДСТСЗІ СБ України від 04.09.2000 № 41 (НД ТЗІ Р-001-2000). Враховуючи те, що кожний вказаний пристрій пройшов сертифікацію або має експертний висновок, немає сенсу порівнювати зазначені технічні параметри, а такі параметри, як напруга живлення генератора, ефективне значення вихідної напруги кожного каналу, споживана потужність, габаритні розміри та ряд інших параметрів не є визначальними при захисті інформації.

Порівняння генераторів віброакустичного зашумлення наведено у табл. 2.3.

Таблиця 2.3 – Порівняння генераторів віброакустичного зашумлення „МАРС-ТЗО-4-2”, „РІАС” та „БАЗАЛЬТ-4ГА”

Характеристика	МАРС-ТЗО-4-2	БАЗАЛЬТ-4ГА	РІАС
Діапазон частот шумового сигналу	від 180 Гц до 5600 Гц	від 170 Гц до 5700 Гц	від 180 Гц до 5600 Гц
Кількість каналів виходів всього, у т.ч на вібро і акустичні випромінювачі	2-2-2	2-1-1	2-1-1
Індикація рівня вихідного сигналу	по десятисегментному індикатору	відсутня	відсутня
Максимальна вихідна потужність на кожний канал у т.ч.	не менше 10 Вт	-	-
віброакустичний (п’єзоелектричний) канал	-	-	не менше 10 Вт
Вихідна середньоквадратична напруга акустичного(електромагнітного) каналу при навантаженні 4 Ом	-	-	не менше 10 дб
Максимальні ефективні напруги вихідних шумових сигналів в смузі частот (170 … 5700) Гц по:			
низьковольтному виходу на мінімальному опорі навантаження 1 Ом, В	-	не менше 2	-
високовольтному виходу на мінімальному опорі навантаження 50 Ом, В	-	не менше 15	-
Глибина регулювання рівнів шумових сигналів на виходах	не менше 20 дБ	не менше 20 дБ	не менше 20 дБ
Регулювання рівня сигналу по верхнім и нижнім частотам (по октавах) на глибину	-	не менше 25 дБ	не менше 20 дБ

Регулювання рівнів шумових сигналів на виходах – мабуть найбільш важлива властивість, що характеризує спроможність отримати якісний шумовий

сигнал. Справа у тому, що у залежності від форми і матеріалів оздоблення об'єкта, звукопоглинаючої спроможності і резонансних частот предметів інтер'єру, розподіл акустичного (віброакустичного) шуму у кожному приміщенні унікальний. Тобто при подачі широкосмугового акустичного (віброакустичного) сигналу з фіксованими характеристиками у двох різних приміщеннях, амплітуди сигналів на кожній октаві від приміщення к приміщенню будуть значно відрізняться. Тому, для найбільш оптимального розподілу частотного спектру акустичної (віброакустичної) завади бажано мати можливість регулювати амплітуду окремих частот.

Найбільш функціональний в цьому плані генератор „БАЗАЛЬТ-4ГА". Органи керування якого, дозволяють плавно регулювати рівень шуму на кожному каналі у кожній октаві. Друге місце займає „МАРС-ТЗО-4-2", у якого регулюється, як загальна амплітуда шумового сигналу, так окремо верхні та нижні складові спектру. Стосовно генератора „PIAC" повна інформація про можливість регулювання спектру сигналу відсутня (потенціометри – «ВЧ», «НЧ» є, але їх функціональне призначення потребує уточнення).

Індикація рівня шумового сигналу. Найбільш зручний в цьому відношенні виявляється генератор „МАРС-ТЗО-4-2". У цьому приладі рівень вихідного сигналу кожного каналу можна контролювати по десятисегментному індикатору. У генераторах „PIAC" і „БАЗАЛЬТ-4ГА" таки можливості відсутні (є тільки світлодіоди, сигналізують роботу кожного каналу генератора).

Тип блока живлення. Генератори „МАРС-ТЗО-4-2" і „БАЗАЛЬТ-4ГА" мають вбудовані блоки живлення, що досить зручно під час їх експлуатації у стаціонарних умовах. Що стосується приладу „PIAC", то він має зовнішній блок живлення, що менш зручно. Такий підхід більш доцільний для мобільних генераторів.

Тип кріплення генератора. Кожен з розглянутих генераторів може розташовуватися горизонтально на плоскій поверхні. Тобто стояти на підлозі, столі, тумбі, полиці тощо. Проте, вертикально кріпитися на огороджувальні конструкції та предмети інтер'єру зручніше всього генератор „МАРС-ТЗО-4-

2”, який має спеціальну кріпильну пластину для бистрої фіксації його майже у будь якому положенні. Генератори „БАЗАЛЬТ-4ГА” і „РІАС” можна кріпити тільки за отвори на корпусі або виготовити спеціальні кріплення.

Наявність додаткових виходів. Генератори „МАРС-ТЗО-4-2” і „БАЗАЛЬТ-4ГА” оснащені додатковими виходами для включення провідних систем керування (контролю) напругою 5В і 12В відповідно. Цей вихід можна використовувати, наприклад, для включення/виключення реле (лінійки реле), які комутують (включають/виключають) телефонні лінії, лінії пожежної і охоронної сигналізацій, антенні коаксіальні кабелі тощо. У приладі „РІАС” така можливість відсутня.

Побудова типового комплексу технічного захисту інформації, що циркулює в приміщенні зображено на рис. 2.5.

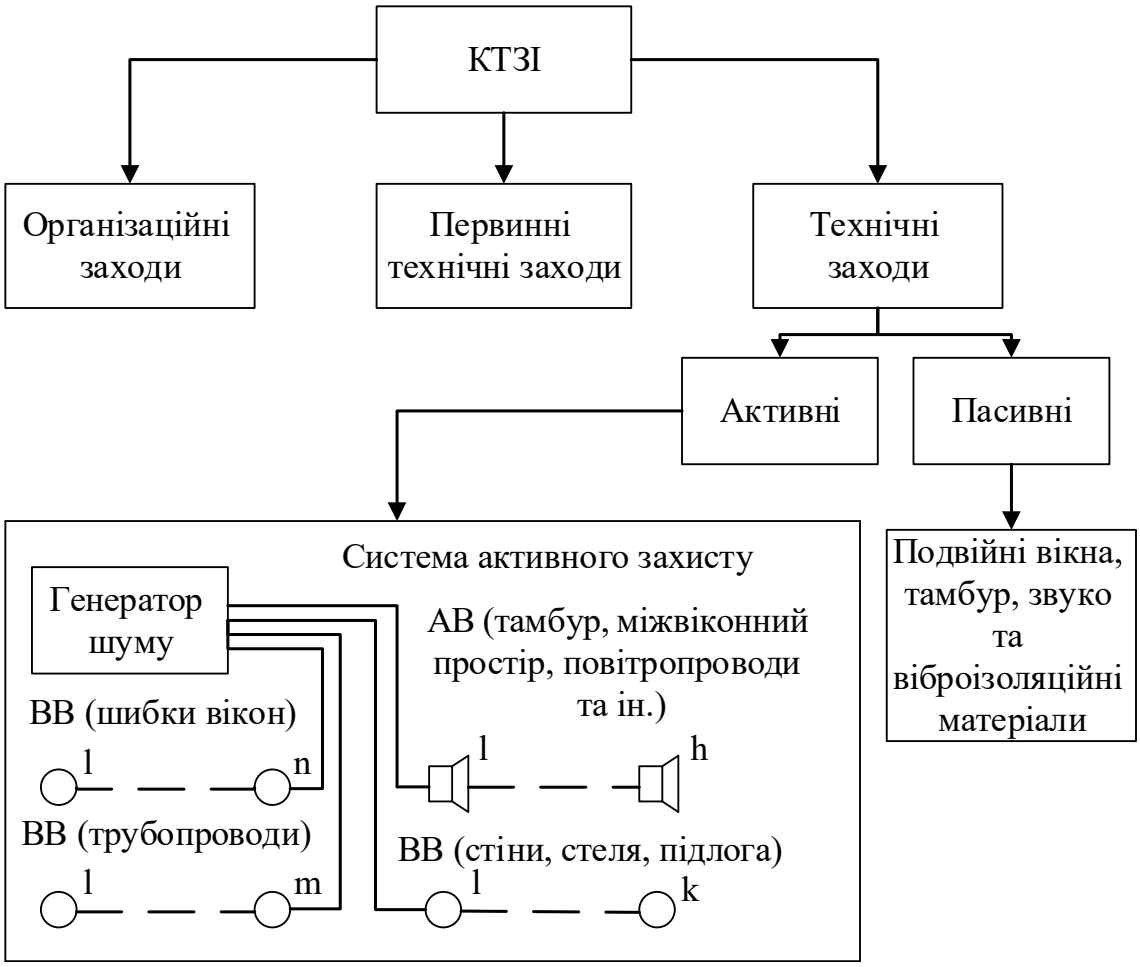

Рисунок 2.5 – Побудова типового КТЗІ приміщення

2.3.3 Організаційний метод захисту інформації

Організаційні методи захисту інформації включають заходи та дії, які повинні здійснювати посадові особи в процесі створення й експлуатації системи для забезпечення заданого рівня безпеки інформації.

Відповідно до законів і нормативних актів у міністерствах, відомствах, на підприємствах (незалежно від форм власності) для захисту інформації створюються спеціальні служби безпеки (на практиці вони можуть називатися й інакше). Ці служби підпорядковуються, як правило, керівництву установи. Керівники служб організують створення й функціонування систем захисту інформації. Повну відповідальність за стан інформаційної безпеки несуть керівники організації. На організаційному рівні вирішуються наступні завдання забезпечення безпеки інформації в системи:

- організація робіт з розробки системи захисту інформації;
- обмеження доступу на об'єкт і до ресурсів системи;
- розмежування доступу до ресурсів системи;
- планування заходів;
- розробка документації;
- виховання й навчання обслуговуючого персоналу й користувачів;
- сертифікація засобів захисту інформації;
- ліцензування діяльності по захисту інформації;
- атестація об'єктів захисту;
- удосконалювання системи захисту інформації;
- оцінка ефективності функціонування системи захисту інформації;
- контроль виконання встановлених правил роботи в системи.

Організаційні методи є базисом комплексної системи захисту інформації в системи. Тільки за допомогою цих методів можливе об'єднання на правовій основі технічних, програмних і криптографічних засобів захисту інформації в

єдину комплексну систему. Конкретні організаційні методи захисту інформації будуть приводитися при розгляді протидії загрозам безпеки інформації. Найбільша увага організаційним заходам приділяється при викладі питань побудови й організації функціонування комплексної системи захисту інформації.

До методів і засобів організаційного захисту інформації відносяться організаційно-технічні й організаційно-правові заходи, проведені в процесі створення й експлуатації системи для забезпечення захисту інформації. Ці заходи повинні проводитися при будівництві або ремонті приміщень, у яких буде розміщатися системи; проектуванні системи, монтажі й налагодженню її технічних і програмних засобів; випробуваннях і перевірці працездатності системи.

Основні властивості методів і засобів організаційного захисту:

- обмеження фізичного доступу до об'єктів захисту та реалізація режимних заходів;
- обмеження можливості перехоплення ПЕМВН;
- розмежування доступу до інформаційних ресурсів і процесам (встановлення правил розмежування доступу, шифрування інформації при її зберіганні і передачі , виявлення та знищення апаратних і програмних закладок);
- резервне копіювання найбільш важливих з точки зору втрати масивів документів;
- перед проведенням наради необхідно проводити візуальний огляд приміщення на предмет виявлення закладних пристроїв;
- кількість осіб, що у конфіденційних переговорах має бути обмежена до мінімуму;
- вхід сторонніх осіб під час проведення наради має бути заборонений;
- повинна бути чітко розроблена охорона виділеного приміщення під час наради, а також спостереження за обстановкою на поверсі;
- будь-які роботи в кімнаті, що проводяться поза часом проведення конфіденційних нарад, наприклад: прибирання, ремонт побутової техніки,

невеликий косметичний ремонт, повинен проводитися в обов'язковій присутності працівника служби безпеки;

- після проведення наради кімната повинна ретельно оглядатися, закриватися і опечатуватися;
- між нарадами кімната повинна бути закрита і опечатана відповідальною особою;
- профілактику зараження комп'ютерними вірусами.

Основою проведення організаційних заходів є використання й підготовка законодавчих і нормативних документів в області інформаційної безпеки, які на правовому рівні повинні регулювати доступ до інформації з боку користувачів.

3 РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ВНЗ

3.1 Мета створення КСЗІ

Мета розробки та створення КСЗІ полягає у виключені або мінімізації збитку власникові АС та користувачам до припустимого рівня шляхом комплексного використання організаційних (адміністративних) заходів, правових та законодавчих норм, фізичних та технічних (апаратних та програмних) засобів захисту інформації.

КСЗІ призначена для забезпечення безпеки критичної інформації та інформаційних ресурсів у процесі функціонування АС.

Мета функціонування КСЗІ полягає в підтримці необхідного рівня інформаційної безпеки АС відповідно політиці безпеки, яка визначається ії власником.

Для інформації, що є власністю держави, вимоги щодо її захисту встановлені на законодавчому рівні.

Відповідно до статті 4 Постанови Кабінету Міністрів України №373 від 29.03.2006 р. «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» захисту підлягає:

- відкрита інформація, яка є власністю держави і у визначенні Закону України «Про інформацію» належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами;

– конфіденційна інформація, яка є власністю держави або вимога до захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу;

– інформація, що становить державну або іншу передбачену законом таємницю.

3.2 Об’єкти та суб’єкти КСЗІ

У процес створення КСЗІ залучаються наступні сторони:

– організація, для якої здійснюється побудова КСЗІ (Замовник);

– організація, що здійснює заходи з побудови КСЗІ (Виконавець);

– державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІУ) (Контролюючий орган);

– організація, що здійснює державну експертизу КСЗІ (Організатор експертизи);

– організація, в разі необхідності залучена Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядник).

Об'єктами захисту КСЗІ є інформація, в будь-якому її вигляді і формі подання. Матеріальними носіями інформації є сигнали.

По своїй фізичній природі інформаційні сигнали можна розділити на електричні, електромагнітні, акустичні, а також їх комбінації.

Сигнали можуть бути представлені у формі електромагнітних, механічних та інших видів коливань, причому інформація, яка підлягає захисту, міститься в їх змінних параметрах.

Залежно від природи, інформаційні сигнали поширюються в певних фізичних середовищах. Середовища можуть бути газовими, рідинними і твердими. Наприклад, повітряний простір, конструкції будівель, з'єднувальні лінії і струмопровідні елементи, грунт та інше.

Залежно від виду та форми подання інформаційних сигналів, які циркулюють в ІТС, в тому числі і в АС, при побудові КСЗІ можуть використовуватися різні засоби захисту.

3.3 Порядок проведення робіт із створення КСЗІ

Порядок проведення робіт з побудови КСЗІ в інформаційно-телекомунікаційних системах регламентується нормативним документом НД ТЗІ 3.7-003-05 «Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній Системі» [17][1)]. Вимоги до захисту інформації веб-сторінки від несанкціонованого доступу регламентуються нормативним документом НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу» [18][2)].

Згідно НД ТЗІ 3.7-003-05 «Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній Системі», побудова КСЗІ включає наступні етапи:

- формування загальних вимог до КСЗІ в АС;
- розробка політики безпеки інформації в АС;
- розробка технічного завдання на створення КСЗІ в АС;
- розробка технічного проекту КСЗІ в АС;
- впровадження КСЗІ;
- попередні випробування КСЗІ в АС;
- дослідна експлуатація КСЗІ в АС;
- державна експертиза КСЗІ в АС.

---

1) [17] НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформаційв інформаційно-телекомунікаційній системі: Чинний від 2005-11-08. К.: Нормативний документ.Системи технічного захисту інформації. 2005. 68 с.

2) [18] НД ТЗІ 2.5-010-03. Вимоги до захисту WEB-сторінки від несанкціонованого доступу: Чинний від 2003-05-02. К.: Нормативний документ. Системи технічного захисту інформації. 2003. 20 с.

Таблиця 3.1 – Порядок проведення робіт із побудови КСЗІ

№ з/п	Найменування робіт	Результат робіт	Відповідальний
Етап 1 – Формування загальних вимог до КСЗІ			
1.1	Обґрунтування необхідності створення КСЗІ	Наказ про створення КСЗІ; Наказ про створення комісії для проведення категоріювання АС, приміщення; Акт проведення категоріювання АС, приміщення; Наказ про створення комісії з проведення обстеження АС.	Виконавець Замовник
1.2	Обстеження середовища функціонування АС	Акт обстеження; Перелік об’єктів захисту.	Виконавець
1.3	Розробка моделі загроз	Модель загроз.	Виконавець
1.4	Формування завдання на створення КСЗІ	Затверджений Акт обстеження та перелік об’єктів захисту.	Виконавець
Етап 2 – Розробка політики безпеки інформації			
2.1	Розробка політики безпеки	Політика безпеки;	Виконавець
Етап 3 – Розробка технічного завдання			
3.1	Розробка технічного завдання	Технічне завдання на створення КСЗІ;	Виконавець
Етап 4 – Розробка технічного проекту			
4.1	Розробка технічного проекту	Технічна документація на КСЗІ;	Виконавець

Продовження таблиці 3.1

№ з/п	Найменування робіт	Результат робіт	Відповідальний
4.2	Розробка робочого проекту	Робоча документація КСЗІ в АС;	Виконавець
Етап 5 – Впровадження КСЗІ			
5.1	Навчання користувачів АС	Акт завершення навчання користувачів АС;	Виконавець Замовник
5.2	Створення служби захисту інформації	Наказ про створення служби захисту інформації; Положення про службу захисту інформації;	Виконавець Замовник
5.3	Пусконалагоджувальні роботи	Встановлення і налагодження КЗЗ, перевірка працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії;	Виконавець Замовник
Етап 6 – Попередні випробування КСЗІ			
6.1	Розробка програми та методики попередніх випробувань	Програма та методика попередніх випробувань;	Виконавець
6.2	Проведення попередніх випробувань	Протокол проведення попередніх випробувань; Акт завершення попередніх випробувань КСЗІ;	Виконавець Замовник
Етап 7 – Дослідна експлуатація КСЗІ			
7.1	Дослідна експлуатація	Акт приймання КСЗІ у дослідну експлуатацію; Акт завершення дослідної експлуатації;	Замовник
Етап 8 – Державна експертиза КСЗІ			
8.1	Державна експертиза КСЗІ	Атестат відповідності та експертний висновок;	Виконавець замовник

3.4 Формування загальних вимог до КСЗІ

Формування загальних вимог до КСЗІ є першим етапом в проведенні робіт із створення КСЗІ.

Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому права діяти на власний розсуд.

Вихідні данні для обґрунтування необхідності створення КСЗІ одержуються за результатами аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах підприємства замовника), 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 експлуатації АС у разі створення КСЗІ.

На підставі проведеного аналізу приймається рішення про створення КСЗІ.

На цьому етапі оцінюється стан інформаційної безпеки в АС і виявляються існуючі проблеми у цій сфері.

Замовник повинен надати необхідні відомості щодо об’єкту інформаційної діяльності для проведення обстеження, а саме:

- загальна характеристика Замовника (нормативно-правова основа діяльності Замовника, положення про структурні підрозділи, посадові інструкції тощо);
- загальна характеристика АС Замовника (назва, призначення, нормативно-правова основа для створення та експлуатації АС Замовника, відносно якої буде створюватись КСЗІ, склад, структура АС, розміщення, основні функції та режими роботи підсистем АС тощо);
- характеристика існуючої системи інформаційного захисту в АС;
- інша інформація.

Вище зазначена інформація може бути надана у вигляді копій діючих документів, в електронному вигляді та може бути зібрана в процесі обстеження об’єкту (робочі матеріали, відомості, які надає Замовник за відповідними напрямами):

- опис середовищ функціонування АС;
- опис персоналу;
- опис інформації, що обробляться в АС;
- опис технології обробки інформації;
- опис фізичного середовища;
- опис режимно-секретних заходів.

За результатами обстеження складається акт обстеження, до якого додаються схеми розміщення технічних засобів і проходження комунікацій на об’єкті, класифікується і погоджується із Замовником перелік об’єктів захисту АС, що потребують захисту.

За результатами обстеження визначаються потенційні загрози для інформації і розробляється модель загроз та модель порушника. Побудова моделей здійснюється відповідно до вимог НД ТЗІ 1.1-002 «Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу».

Визначається завдання захисту інформації в АС, мета створення КСЗІ, варіант вирішення задач захисту та основні напрямки забезпечення захисту.

3.5 Розробка політики безпеки інформації в АС

Під політикою безпеки інформації слід розуміти набір вимог, правил, обмежень, рекомендацій та ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз.

Політика стосуються всіх осіб, що мають відношення до вирішення питань щодо забезпечення надійного та безпечного функціонування АС, службовців сторонніх організацій, постачальників та розробників апаратних та програмних компонентів КСЗІ.

Політика безпеки визначає ресурси, що потребують захисту, враховує основні загрози для інформації і моделі порушників, впроваджені технології обробки інформації і вимоги до захисту інформації від загроз.

На етапі розробки політики безпеки здійснюється вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій, які регламентують використання захищених технологій обробки інформації в АС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій.

Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1-002 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» та рекомендаціями НД ТЗІ 1.4-001 «Типове положення про службу захисту інформації в автоматизованій системі» [19][1)].

3.6 Розробка технічного завдання на створення КСЗІ

Технічне завдання (ТЗ) на створення КСЗІ є засадним організаційно-технічним документом для виконання робіт щодо забезпечення захисту інформації в системі, який визначає вимоги із захисту оброблюваної інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію.

В ТЗ на КСЗІ викладаються вимоги до функціонального складу і порядку розробки і впровадження технічних засобів, що забезпечують безпеки інформації в процесі її обробки в обчислювальній системі АС. Додатково викладаються вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються поза обчислювальною системою АС у доповнення до комплексу програмно-технічних засобів захисту інформації.

[1)] [19] НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі: Чинний від 2000-12-04. К.: Нормативний документ. Системи технічного захисту інформації. 2000. 9 с.

Роботу з погодження проекту ТЗ на КСЗІ здійснюють спільно Розробник ТЗ на КСЗІ і Замовник, кожен в своїй організації.

Розробник ТЗ на КСЗІ, за домовленістю з Замовником, відправляє ТЗ на КСЗІ на затвердження в Адміністрацію Держспецзв'язку України.

3.7 Розробка технічного проекту на створення КСЗІ в АС

На етапі розробки технічного проекту виконується розробка загальних проектних рішень, необхідних для реалізації вимог ТЗ на КСЗІ, рішень щодо структури КСЗІ, алгоритмів функціонування та умов використання засобів захисту, рішень щодо архітектури КЗЗ та механізмів реалізації, визначених функціональним профілем послуг безпеки інформації.

Здійснюється організаційно-технічні заходи щодо забезпечення послідовності розробки КЗЗ, архітектури, середовища розробки, випробувань, середовища функціонування та експлуатаційної документації КЗЗ у відповідності до заданих рівнем гарантій реалізації послуг безпеки згідно із НД ТЗІ 2.5-004 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 2.5-007,НД ТЗІ 2.5-008 «Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2»,НД ТЗІ 2.5-010 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу» [20][1)].

3.8 Впровадження КСЗІ

На цьому етапі проводяться наступні роботи:

- навчання користувачів. Проводиться навчання користувачів АС в частині, що їх стосується, основним положенням документів, які необхідно їм для дотримання правил політики безпеки інформації;

[1)] [20] НД ТЗІ 2.5-008-2002. Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2: Чинний від 2002-12-28. К.: Нормативний документ. Системи технічного захисту інформації. 2002. 25 с.

- створення служби захисту інформації;
- пусконалагоджувальні роботи. Здійснюється встановлення і налагодження комплексу засобів захисту згідно з документацією робочого проекту (інсталяція, ініціалізація та перевірка працездатності комплексу засобів захисту).

3.9 Попередні випробування КСЗІ

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.

Попередні випробування проводяться згідно з програмою та методикою випробувань.

Програму і методику випробувань готує розробник КСЗІ, а узгоджує Замовник. Програма та методики випробувань, протоколи випробувань розробляються та оформляються згідно з вимогами РД 50-34.698 [21][1)].

Попередні випробування організовує Замовник, а проводить Розробник КСЗІ спільно із Замовником. Для проведення попередніх випробувань Замовником створюється комісія. Головою комісії призначається представник Замовника.

Результати попередніх випробувань оформлюється представник Замовника.

Результати попередніх випробувань оформлюється Протоколом та Актом, в якому міститься висновок щодо можливості прийняття КСЗІ у дослідну експлуатацію.

3.10 Дослідна експлуатація КСЗІ в АС

Дослідну експлуатацію організовує та проводить Замовник.

[1)] [21] РД 50-34.698-90. Комплекс стандартов и руководящих документов на автоматизированные системы. Требования к содержанию документов. М.: Б. и., 1990. 57 с.

Під час дослідної експлуатації КСЗІ в АС:

- відпрацьовується технологія оброблення інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів АС та автоматизованого контролю за діями користувачів;
- співробітники служби захисту інформації та користувачі АС 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.

За результатами робіт за довільною формою складається акт про завершення дослідної експлуатації, який містить висновок щодо можливості представлення КСЗІ в АС на державну експертизу.

3.11 Державна експертиза КСЗІ

Державна експертиза КСЗІ є окремим етапом приймальних випробувань автоматизованої системи.

Державна експертиза проводиться з метою визначення відповідності КСЗІ технічному завданню, вимогам нормативних документів із захисту інформації та визначення можливості введення КСЗІ в складі АС в експлуатацію.

Державна експертиза КСЗІ в АС проводиться згідно з вимогами документу «Положення про державну експертизу в сфері технічного захисту інформації» (Наказ Адміністрації Держспецзв'язку України №93 від 16.05.07) і містить наступні етапи:

- аналіз документації на КСЗІ;
- розробка програми та методики проведення Експертизи КСЗІ;
- узгодження програми і методики з Державною службою спеціального зв'зку та захисту інформації України та з Замовником;
- обстеження об'єкта та проведення випробувань;
- оформлення протоколів проведення випробувань;

– оформлення експертного висновку.

Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення таких самий, як і для попередніх випробувань. Якщо в силу будь-яких причин усунути недоліки в ході експертизи неможливо – це оформлюється актом, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення передбачених актом робіт проводиться повторна експертиза.

Допускається розпочинати і проводити державну експертизу КСЗІ паралельно з роботами етапів проектування КСЗІ в АС.

Державну експертизу КСЗІ не може проводити організація, яка розробляє КСЗІ. Організація, що буде проводити Державну експертизу визначається ДССЗЗІ України.

За результатами проведених робіт Організатор складає Експертний висновок відповідного змісту щодо відповідності або невідповідності об’єкта експертизи вимогам НД ТЗІ та ТЗ на КСЗІ, підписує його і подає до Адміністрації Держспецзв’язку. Результати робіт, визначених окремою методикою, узагальнюються Організатором в Експертному висновку. На підставі позитивного рішення щодо експертизи КСЗІ Замовнику видається зареєстрований Атестат відповідності за підписом Голови Держспецзв’язку. Атестати друкуються на бланках суворого обліку, які виготовляються в установленому законодавством порядку. Адміністрація Держспецзв’язку має право призупинити вбо анулювати дію Експертного висновку або Атестата.

ВИСНОВКИ

Аналіз поточної нормативно-правової бази в галузі забезпечення інформаційної безпеки сучасних інформаційно-комунікаційних систем та мереж та побудови комплексної системи захисту інформації показав що на даний час комплексний захист інформації являє собою сукупність організаційних структур, поєднаних цілями і завданнями захисту інформації, нормативно-правової та матеріально технічної бази і спрямований на забезпечення інженерно технічними, апаратними та програмно-апаратними засобами властивостей сучасних інформаційно-комунікаційних систем та мереж.

Тобто нормативно-правове забезпечення регламентує та визначає:

- порядок захисту визначених політикою безпеки властивостей інформації під час створення та експлуатації інформаційної мережі;
- порядок ефективного знешкодження і попередження загроз для ресурсів ляхом побудови КСЗІ;
- статус інформаційної системи з точки зору інформаційної безпеки; права, обов'язки й відповідальність персоналу роботи яких пов'язані з інформаційною безпекою;
- правові положення окремих видів процесу керування та управління доступом в захищених ІКСМ;
- порядок створення й використання захищених ІКСМ;
- етапи побудови КСЗІ.

Але основною проблемою при побудові коректної системи захисту інформації є відсутність штатних спеціалістів із достатнім рівнем знань та навичок. Єдиним шляхом рішення цієї проблеми є залучання сторонніх спеціалістів, але станом на сьогоднішній день не кожне підприємство може дозволити собі істотні затрати на побудову належної системи захисту інформації від несанкціонованого доступу.

Саме тому у даній роботі була поставлена мета розробки методики побудови оптимальної КСЗІ в ВНЗ, яка позволяла би, при мінімальних грошових

затратах та при наявності мінімальних знань в сфері інформаційної безпеки, перекрити основні шляхи втручання в інформацію, що потребує захисту, та забезпечити інженерно технічними, апаратними, програмними та організаційними засобами властивостей сучасних інформаційно-комунікаційних систем та мереж.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 − 2015 роки: Закон України від 9 січня 2007 року № 537-V // Відомості Верховної Ради України (ВВР). 2007. № 12. ст.102.

2. Правові основи охорони інформації: підручник / [В.М. Сердюков, О.М. Стаднік, З.Б. Живко, В.О. Хорошко]; за заг. ред. В.О. Хорошко. Київ: ДУІКТ, 2009. 354 с.

3. Проект Концепція інформаційної безпеки України [електронний ресурс]. Режим доступу: http://mip.gov.ua/done_img/d/30- project_08_06_15.pdf 3.

4. Богуш В. М. Інформаційна безпека від А до Я / В. М. Богуш, А. М. Кусин. К. : ДУІКТ, 2006. 126 с.

5. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення: Чинний від 1997-01-01. К.: Держстандарт України. 1996. 3 с.

6. Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О. К. Юдін. К. : НАУ, 2011. 640 с.

7. Про інформацію: Закон України від 02 листопада 1992 року № 2657-XII // Відомості Верховної Ради України (ВВР). 1992. N 48. ст. 650.

8. Про державну таємницю: Закон України від 21.01.1994 року № 3855-12-ВР// Відомості Верховної Ради України (ВВР). 1994. № 24. ст. 296.

9. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI // Відомості Верховної Ради України (ВВР). 2011. № 32. ст. 314.

10. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР // Відомості Верховної Ради України (ВВР). 1994. № 31. ст.286.

11. Про захист інформації в автоматизованих системах: Закон Україні від 05.07.1994 № 81/94-ВР// Відомості Верховної Ради України (ВВР). 1994. № 31. ст. 287.

12. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: Чинний від 1999-04-28. К.: Нормативний документ. Системи технічного захисту інформації. 1999. 16 с.

13. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: Чинний від 1999-04-

28. К.: Нормативний документ. Системи технічного захисту інформації. 1999. 20 с.

14. НД ТЗІ 1.6-005-2013. Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці: Чинний від 2013-04-15. К.: Нормативний документ. Системи технічного захисту інформації. 2013. 9 с.

15. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: Чинний від 1994-04-28. К.: Нормативний документ. Системи технічного захисту інформації. 1999. – 24 с.

16. НД ТЗІ 1.1-002-99. Загальні положення з захисту інформації в комп’ютерних системах від НСД: Чинний від 1999-04-28. К.: Нормативний документ. Системи технічного захисту інформації. 1999. 22 с.

17. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: Чинний від 2005-11-08. К.: Нормативний документ. Системи технічного захисту інформації. 2005. 68 с.

18. НД ТЗІ 2.5-010-03. Вимоги до захисту WEB-сторінки від несанкціонованого доступу: Чинний від 2003-05-02. К.: Нормативний документ. Системи технічного захисту інформації. 2003. 20 с.

19. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі: Чинний від 2000-12-04. К.: Нормативний документ. Системи технічного захисту інформації. 2000. 9 с.

20. НД ТЗІ 2.5-008-2002. Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2: Чинний від 2002-12-28. К.: Нормативний документ. Системи технічного захисту інформації. 2002. 25 с.

21. РД 50-34.698-90. Комплекс стандартов и руководящих документов на автоматизированные системы. Требования к содержанию документов. М.: Б. и., 1990. 57 с.

ДОДАТОК А

Класифікація автоматизованих систем

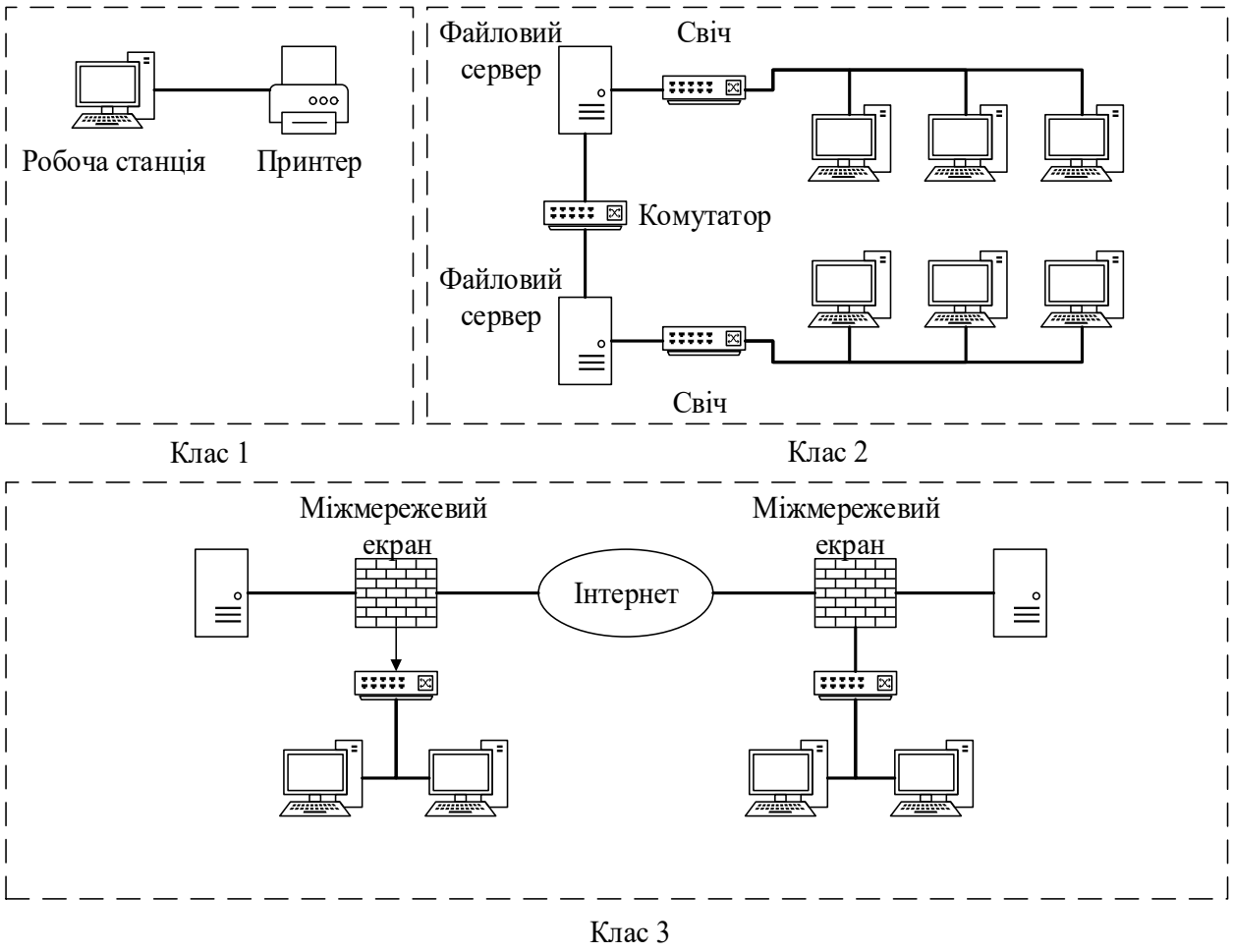

Рисунок А.1 – Автоматизовані системи класів АС1, АС2 та АС3

ДОДАТОК Б

Стандартні профілі захищеності для автоматизованих систем

Таблиця Б.1 – Функціональні профілі захищеності для АС класу 1

Стандартні функціональні профілі захищеності для АС класу 1
1.К.1 = { НР-1, НІ-1, НК-1, НО-1, НЦ-1, НТ-1 };
1.Ц.2 = { ЦА-2, ЦО-1, НР-2, НІ-2, НК-1, НО-1, НЦ-1, НТ-1 };
1.Д.1 = { ДР-1, ДВ-1, НР-2, НІ-2, НК-1, НО-1, НЦ-1, НТ-1 };
1.КЦ.1 = { НР-1, НІ-1, НК-1, НО-1, НЦ-1, НТ-1 };
1.КД.1 = { КА-1, КО-1, ДР-1, ДВ-1, НР-2, НІ-2, НК-1, НО-1, НЦ-1, НТ-1 };
1.ЦД.1 = { ЦА-1, ЦО-1, ДР-1, ДВ-1, НР-2, НІ-2, НК-1, НО-1, НЦ-1, НТ-1 };
1.КЦД.1 = { КА-1, КО-1, ЦА-1, ЦО-1, ДР-1, ДВ-1, НР-2, НІ-2, НК-1, НО-1, НЦ-1, НТ-1 }

Таблиця Б.2 – Функціональні профілі захищеності для АС класу 2

Стандартні функціональні профілі захищеності для АС класу 2
2.К.1 = { КД-2, НР-2, НІ-2, НК-1, НО-1, НЦ-1 };
2.Ц.1 = { ЦД-1, НР-2, НІ-2, НК-1, НО-1, НЦ-1 };
2.Д.1 = { ДР-1, ДВ-1, НР-2, НІ-2, НК-1, НО-1, НЦ-1, НТ-1 };
2.КЦ.1 = { КД-2, ЦД-1, НР-2, НІ-2, НК-1, НО-1, НЦ-1 };
2.КД.1 = { КД-2, КА-2, КО-1, ДР-1, ДВ-1, НР-2, НІ-2, НК-1, НО-2, НЦ-2, НТ-2 };
2.ЦД.1 = { ЦД-1, ЦО-1, ДР-1, ДВ-1, НР-2, НІ-2, НК-1, НО-1, НЦ-2, НТ-1 };
2.КЦД.1 = { КД-2, КО-1, ЦД-1, ЦО-1, ДР-1, ДВ-1, НР-2, НІ-2, НК-1, НО-2, НЦ-2. НТ-2 };

Таблиця Б.3 – Функціональні профілі захищеності для АС класу 3

Стандартні функціональні профілі захищеності для АС класу 3
3.К.1 = { КД-2, КВ-1, НР-2, НІ-2, НК-1, НО-1, НЦ-1, НВ-1 };
3.Ц.1 = { ЦД-1, ЦВ-1, НР-2, НІ-2, НК-1, НО-1, НЦ-1, НВ-1 };
3.Д.1 = { ДР-1, ДВ-1, НР-2, НІ-2, НК-1, НО-1, НЦ-1, НТ-1, НВ-1 };
3.КЦ.1 = { КД-2, КВ-1, ЦД-1, ЦВ-1, НР-2, НІ-2, НК-1, НО-1, НЦ-1, НВ-1 };
3.КД.1 = { КД-2, КА-2, КО-1, КВ-2, ДР-1, ДВ-1, НР-2, НІ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 };
3.ЦД.1 = { ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НІ-2, НК-1, НО-1, НЦ-2, НТ-1, НВ-1 };
3.КЦД.1 = { КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НІ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 };

ДОДАТОК В

Приклад переліку відомостей, що містять конфіденційну інформацію, що є власністю держави або службову інформацію

Таблиця В.1 – Перелік відомостей, що містять конфіденційну інформацію, що є власністю держави або службову інформацію

№	Назва підрозділу, в якому обробляються, надходять або створюються документи	Назва документів, що містять конфіденційну інформацію, що є власністю держави, або службову інформацію
1	Кафедра Інформаційних технологій	Дисертаційні роботи з грифами обмеження доступу та автореферати до них, що виконані співробітниками кафедри
2		протоколи засідань кафедри та витяги з них, на яких розглядалися дисертаційні роботи та автореферати до них з грифами обмеження доступу, що виконані співробітниками кафедри та співробітниками сторонніх установ
3		копії актів впровадження у НДР результатів, що ввійшли до дисертаційних робіт з грифами обмеженого доступу, які виконані співробітниками кафедри та співробітниками сторонніх установ
4		дисертаційні роботи з грифами обмеження доступу та автореферати до них, які опонувалися чи рецензувалися співробітниками кафедри
5		Копії відгуків опонентів, рецензентів, наукових керівників та консультантів – співробітників кафедри, на дисертаційні роботи та автореферати з грифом обмеження доступу
6		Копії документів та копії документів внутрішньої службової переписки, що містять конфіденційну інформацію та інформацію з грифом обмеження

Продовження таблиці В.1

№	Назва підрозділу, в якому обробляються, надходять або створюються документи	Назва документів, що містять конфіденційну інформацію, що є власністю держави, або службову інформацію
7		Списки співробітників університету та співробітників сторонніх установ та організацій, які одноразово запрошувались на засідання кафедри на яких розглядалися дисертаційні роботи та автореферати до них з грифами обмеження доступу, що виконані співробітниками кафедри та співробітниками сторонніх установ
8		За рішенням кафедри: за сукупністю даних – розділи звітів з НДР та їх електронні копії, у яких містяться відомості, що ввійшли до дисертаційних робіт з грифами обмеження доступу та авторефератів до них

ДОДАТОК Г

Приклад акту категоріювання ОІД

Для службового користування
Прим № ___

ЗАТВЕРДЖУЮ

__ _____ 20 __ р.

АКТ
категоріювання відділу кадрів

1. Підстава для категоріювання - рішення про створення КСЗІ

2. Вид категоріювання - первинне

3. На ОІД здійснюється обробка інформації технічними засобами та/або озвучування інформації

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об’єкті: службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України “Про доступ до публічної інформації”; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом

5. Встановлена категорія – IV (об'єкти, в яких циркулює службова та конфіденційна інформація, вимога щодо захисту якої встановлена законом)

Голова комісії _____
(підпис)

Члени комісії: _____
(підпис)

_____
(підпис)

____.____. 20___

ДОДАТОК Д

Алгоритм виконання робіт із захисту інформації в ас класу 2

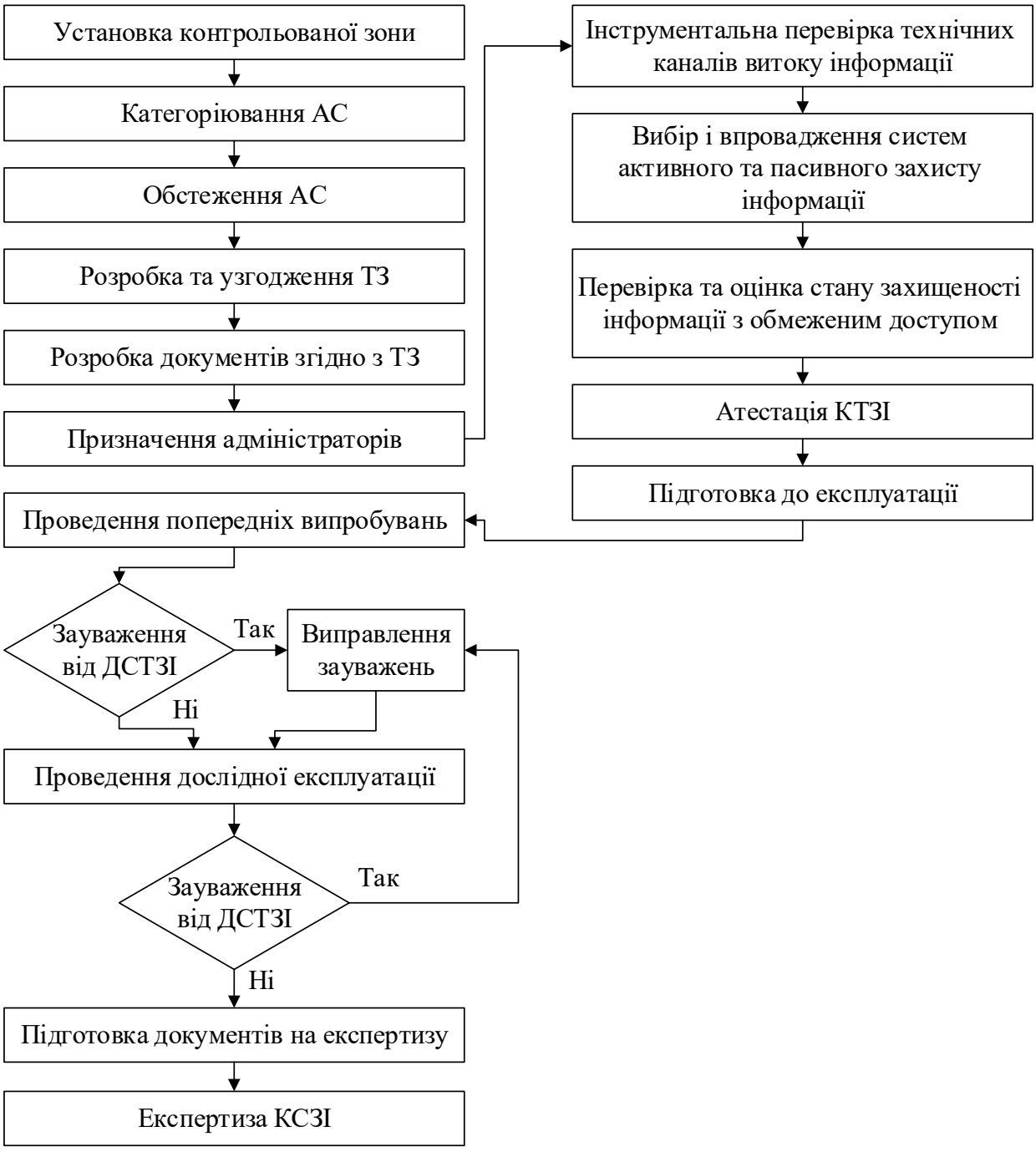

Рисунок Д.1 – Алгоритм виконання робіт із побудови комплексної системи захисту інформації в автоматизованій системі класу 2

ДОДАТОК Е

Перелік документів на КСЗІ

- Наказ на створення комплексної системи захисту інформації в АС;
- наказ про призначення комісії з категоріювання;
- акт категоріювання об’єкту інформаційної діяльності;
- акт категоріювання об’єкту ЕОТ;
- протокол про визначення вищого ступеня обмеження доступу до інформації;
- акт обстеження ОІД стосовно створення комплексу ТЗІ;
- акт обстеження середовища функціонування об’єкту;
- модель загроз для ІзОД (Стосовно забезпечення захисту від витоку ІзОД технічними каналами);
- положення про службу захисту інформації в АС;
- план захисту інформації в АС;
- технічне завдання на створення КСЗІ в АС;
- інструкція з інсталяції та конфігурування параметрів безпеки в АС;
- наказ про призначення комісії з інсталяції та конфігурування параметрів безпеки;
- протокол з інсталяції та конфігурування параметрів безпеки;
- інструкція про порядок оброблення інформації з обмеженим доступом;
- інструкція про порядок забезпечення антивірусного захисту в АС;
- інструкція адміністратора системи АС;
- інструкція адміністратора безпеки АС;
- інструкція адміністратора КЗЗ АС;
- інструкція користувача АС;
- програма та методика випробувань КСЗІ в АС;

- наказ проведення попередніх випробувань;
- протокол попередніх випробувань КСЗІ в АС;
- акт про приймання КСЗІ в АС у дослідну експлуатацію;
- акт завершення дослідної експлуатації;
- акт завершення робіт зі створення КСЗІ в АС;
- паспорт формуляр АС;
- журнал обліку користувачів АС;
- журнал обліку роботи користувачів АС;
- журнал обліку захищених інформаційних ресурсів АС;
- журнал реєстрації проведених робіт з технічного обслуговування, ремонту, модернізації;
- журнал реєстрації перевірок складу програмних засобів АС;
- журнал реєстрації нештатних ситуацій в роботі АС;
- журнал обліку документів та видань з грифом «Для службового користування»;
- журнал обліку магнітних носіїв інформації з грифом «Для службового користування».