Навчально-методичне видання

В.Д. Козюра, В.О. Хорошко,
М.Є. Шелест, Ю.М. Ткач, С.В. Зайцев

ПРОЕКТУВАННЯ, ВВЕДЕННЯ В ДІЮ ТА СУПРОВОДЖЕННЯ КСЗІ

Навчальний посібник

В авторській редакції

Відповідальний за випуск – *Лук'яненко В.В.*

Підписано до друку 26.04.2019 р.
Формат 60х 84/16. Папір офсетний. Друк числовий.
Гарнітура Times New Roman. Обл.-вид. арк. 14,22.
Ум. друк. арк. 13,95. Тираж 300 прим.
Зам. № 565.

Віддруковано з оригінал-макету замовника

Видавець - ФОП Лук'яненко В.В. ТПК «Орхідея»

Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
серія ДК № 3020 від 02.11.2007 р.

16600, Чернігівська обл., м. Ніжин, вул. Небесної сотні, 13 а.
Тел.: 068 815 06 60
E-mail: holdingvv@ gmail.com

В.Д. Козюра, В.О. Хорошко,
М.Є. Шелест, Ю.М. Ткач, С.В. Зайцев

ПРОЕКТУВАННЯ, ВВЕДЕННЯ В ДІЮ ТА СУПРОВОДЖЕННЯ КСЗІ

Навчальний посібник

Ніжин
2019

УДК 004.415.056.5(075)

П - 79

Рекомендовано до друку вченою радою Чернігівського національного технологічного університету (протокол № 4 від 22 квітня 2019 року)

Рецензенти:

Ю. Є. Яремчук - директор Центру інформаційних технологій і захисту інформації Вінницького національного технологічного університету, д.т.н., професор.

О. Г. Корченко – завідувач кафедри безпеки інформаційних технологій НАУ д.т.н., професор, лауреат Державної премії України в галузі науки і техніки.

В. В. Литвинов – завідувач кафедри інформаційних технологій і програмної інженерії ЧНТУ, д.т.н., професор.

П-79 **Проектування, введення в дію та супроводження КСЗІ**: навчальний посібник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, С.В. Зайцев. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 240 с.

ISBN 978-617-7609-29-1

В навчальному посібнику розкривається комплекс проблем, які виникають під час проектування комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. У виданні здійснено огляд загальних підходів до створення комплексних систем захисту інформації. Запропонований загальний методологічний підхід до проектування систем захисту інформації в інформаційно-телекомунікаційних системах.

УДК 004.415.056.5(075)

ISBN 978-617-7609-29-1

20. Малюк А.А. Информационная безопасность: Концептуальные и методологические основы защиты информации / А.А. Малюк. – М.: Высшая школа, 2004. – 280 с.

21. Малюк А.А. Теоретические основы формализации прогнозной оценки уровня безопасности информации в системах обработки данных / А.А. Малюк. – Москва.: 1998. – 40 с.

22. Павлов І.М. Проектування комплексних систем захисту інформації / І.М. Павлов, В.О. Хорошко. – К: – ВІТІ – ДУІКТ, 2011. – 245 с.

23. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Текст] / НД ТЗІ 3.7 – 003 – 05. – Київ.: 2005. – 35 с.

24. Протасов И.Д. Теория игр и исследование операцій: Учебное пособие / И.Д. Протасов. – Москва.: 2003. – 368 с.

25. Reddy Y. The DARPA Initiative in Concurent Engineering, Concurent Engineering Research in Review, Reddy Y., Wood R., Cleetus Y. vol. 1, 2007.

26. Семкин С.Н. Основы безопасности обьектов обработки информации / С.Н. Семкин, А.Н. Семкин. – Москва.: 2000. – 123 с.

27. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу./ НД ТЗІ 1.1 – 003 – 99. – К.: 1999. – 47 с.

28. Technical Report 161 Laboratory for Computer Scince, Massachusetts Institute of Technology, Cambridge, Massachusetts, June 1976, pp 194.

29. Тимченко А.А. Основы информатики системного проектирования объектов новой техник / А.А. Тимченко, А.А. Радионов. – Наукова думка. – Киев.: 2000.– 152 с.

30. Harrison M. Protection in Operating Systems / Harrison M. – Communications of the ACM, August 1976, Vol. 19, Number 8.

31. Хорошко В.А. Методы и средства защиты информации / Хорошко В.А., Чекатков А.А. – К: изд. Юниор, 2003. – 504с.

32. Широчин В.П. Вопросы проектирования средств защиты информации в компьютерных системах и сетях / Широчин В.П., Мухин В.Е., Кулик. – К.: 2000. – 111 с.

33. Щеглов А.Ю. Защита компьютерной безопасности от несанкционированного доступа / Щеглов А.Ю. – С.Пб.: 2004. – 384 с.

ЛІТЕРАТУРА:

1. Андрєев В.І. Стратегія управління інформаційною безпекою / В.І. Андрєев,
В.Д. Козюра, Л.М. Скачек, В.О. Хорошко – К: ДУІКТ, 2007. – 277с.
2. Бадулин С.С. Автоматизированное проектирование цифровых устройств / Бадулин С.С. – «Радио и связь». – М.: 1980. – С. 57 – 79.
3. Батанов Л.А. Автоматизация проектирования цифровых вычислительных устройств / Батанов Л.А. – «Энергия». – М.: 1978. – 356 с.
4. D.E. Bell Secure Computer Systems: Mathematical foundations and model / D.E. Bell, L.J. La Padula. – Report ESD – TR – 73 – 278, Mitre Corp., Bedford, Mass, Nov. 1973.
5. Вертузаев М.С. Защита информации в компьютерных системах от несанкционированного доступа / Вертузаев М.С., Юрченко О.М. – К.: 2001. – 321 с.
6. Габарчук В. Кибернетический подход к проектированию систем защиты информации / Габарчук В., Зинович З., Свиц А. – К.: 2003. – 657 с.
7. Гайкович В.Ю. Основы безопасности информационных технологий / В.Ю. Гайкович, Д.В. Ершов // – Москва.: 1995. – 145 с.
8. Гайворонський М.В. Безпека інформаційно-комунікаційних систем / Гайворонський М.В., Новиков О.М. – К.: вид. група BHV, 2009. – 608 с.
9. Домарев В.В. Безопасность информационных технологий. Системный подход / Домарев В.В. – М., СПб., К.: 2004. – 975 с.
10. Єжова Л.Ф. Управління інформаційною безпекою. В 2-х томах / Єжова Л.Ф., Мачалін І.О., Невойт Я.В., Хорошко В.О. Київ. Вид. ДУІКТ. 2011.
11. Иващенко А.В. Основы моделирования сложных систем на ЭВМ / Иващенко А.В., Сыпченко Р.П. – Л.: 1988. – 270 с.
12. Капур К. С. Надёжность и проектирование систем. / Капур К. С., Ламберсон Л.А. – М.: 1980. – 435 с.
13. Кобозева А.А. Анализ информационной безопасности / Кобозева А.А., Хорошко В.А. – К.: изд. ГУИКТ, 2009. – 251 с.
14. Кобозева А.А. Аналіз захищеності інформаційних систем / Кобозева А.А., Мачалін І.О., Хорошко В.О. – Київ. Вид. ДУІКТ. – 2010. – 316 с.
15. Коженевский С.Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4 доповн. І переробл. / Коженевський С.Р., Кузнєцов Г.В., Хорошко В.А., Чирков Д.В. – Київ. Вид ДУІКТ, 2007. – 365 с.
16. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу / НД ТЗІ 2.5 – 004 – 99. – К.: 1999. – 51 с.
17. Крушевский А.В. Теория игр / А.В. Крушевский. – Киев: Вища школа. – 2003. – 368 с.
18. Kusiak A., Concurent Engineering: Automation, Tools and Techniques, J. Wiley and Sons, N.Y., 2003.
19. Ленков С.В. Методы и средства защиты информации в 2-х томах / ленков С.В., Прегудов Д.А., Хорошко В.А. – К.: Арий, 2008.

ЗМІСТ

входження України у світовий інформаційний простір, як суб'єкта рівноправних міжнародних відносин.

На підставі цього одним з важливих завдань державної політики в сфері інформаційної безпеки має бути – формування та проектування систем захисту інформації на основі науково обґрунтованих політичних, соціальних, економічних критеріїв та світового досвіду правового регулювання і організації забезпечення їх стійкого функціонування. Система захисту інформації, яка підлягає охороні з боку держави, повинна відповідати правовому режиму, діяти безперервно в будь-яких умовах і бути адекватною загрозам, що діють в інформаційній сфері.

Насамкінець зауважимо, що глобалізація інформаційного простору несе загрозу можливих серйозних струсів глобального характеру – при зловмисному або випадковому втручанні в процеси, які протекають в інформаційному просторі. Тому завдання проектування систем захисту інформації є актуальним і суттєво важливим завданням не тільки в галузі інформаційної безпеки а і вцілому в напрямку інформаційних відносин.

ПІСЛЯМОВА

Розробка КСЗІ – складний і багатоплановий процес. Під час створення та впровадження систем захисту інформації необхідно користуватися відповідною нормативно-правовою базою. Так як КСЗІ проходитиме державну експертизу, розробник на кожному етапі має узгоджувати свої дії із рекомендаціями та вимогами вітчизняних нормативних докуметів, зокрема НД ТЗІ 3.7 – 003 – 05 та НД ТЗІ 3.7 – 001 – 99.

Комплекси захисту інформації – це багаторівневі, як правило територіально-розподілені системи з суворою ієрархічною структурою, яка забезпечує ешелонований захист інформації замовника.

В рамках комплексних систем захисту інформації функціонують різні незалежні по виконанню задач та взаємопов'язані між собою з єдиною метою забезпечення інформаційної безпеки комплекси, такі як:

– управління доступом, який реалізує функції управління доступом до ресурсів;

– регістрації та обліку, який виконує регістрацію і облік дій користувачів в різних системах;

– – забезпечення цілісності, який дозволяє попереджати шкідливузаміну програмного продукту;

– криптографічного захисту, який забезпечує захист даних під час зберігання, передачі, отримання інформації по засобам АС, а також забезпечення безпечного документообігу;

– захисту від спама, вірусів;

– забезпечення мережевої безпеки від мережевих атак;

– контролю витоку інформації по каналам НСД;

– забезпечення безперервності роботи без збоїв;

– управління інцидентами ІБ;

– контроля захищеності – для проведення інвентаризації інформаційних ресурсів та контролю за виконанням політики безпеки, та інш.

Супроводження діючих систем захисту інформації є важливою складовою забезпечення безпеки інформації. Цей процес теж регламентується вітчизняними нормативними документами та стандартами. Використання міжнародних стандартів буде сприяти підвищенню якості реалізації систем захисту інформації.

Формування і забезпечення функціонування ефективно діючої системи інформаційної безпеки на підприємстві, в організації та державі – складний і багатогранний процес, який потребує значних зусиль усіх гілок влади, вітчизняної науки, керівників усіх рівнів. Вирішення усіх цих проблем, очевидно, потребує не одного року, але їх вирішення зумовлено необхідністю формування виваженої державної політики забезпечення інформаційної безпеки. Водночас інформаційна безпека, яка забезпечує охорону з боку держави, не повинна гальмувати процеси формування національного інформаційного простору, який відповідав би інформаційно-інтелектуальному потенціалу держави та не гальмувала би

ПЕРЕЛІК СКОРОЧЕНЬ

АС – автоматизована система
ВМІП – варіативна матриця інформаційного процесу
ДІ – джерело інформації
ДЗ – джерело загроз
ЗІ – захист інформації
ІзОД – інформація з обмеженим доступом
ІТС – інформаційно-телекомунікаційна система
КЗЗ – комплекс засобів захисту
КІ – конфіденційна інформація
КС – комп'ютерна система
КСР – корнева структура
КСЗІ – комплексна система захисту інформації
ЛОС – локальна обчислювальна система
МАІ – метод аналізу ієрархії
МІЗІП – матриця інформаційної зв'язності інформаційного процесу
МЗ – механізми захисту
НДР – науково-дослідницька робота
НДКР – науково-дослідницька конструкторська робота
НД ТЗІ – нормативний документ технічного захисту інформації
НСД – несанкціонований доступ до інформації
НСЛ – нервова система людини
ОС – обчислювальна система
ОП – об'єкт проектування
ОПР – особа, яка приймає рішення
ОС – операційна система
ПЗ – програмне забезпечення
ПЕОМ – персональна електронно-обчислювальна машина
ПЕМВН – побічні електромагнітні випромінювання і наведення
СЗІ – система захисту інформації
СОД – система обробки даних
СПІ – система передачі інформації
СЗіА – система зв'язку і автоматизації
ТЗ – технічне завдання
ТЗЗІ – технічні засоби захисту інформації
ТДО – технічні демаскуючі ознаки
ЕОМ – електронно-обчислювальна машина

ВСТУП

Масове створення, впровадження і експлуатація інформаційних систем привели до виникнення спектру нових проблем в сфері безпеки інформації. І це закономірно.

Потреби в забезпеченні безпеки пов'язані з тим, що існує множина суб'єктів і структур, які зацікавлені в чужій інформацій і готових платити за це високу ціну.

В таких умовах все більше розповсюджується аксіома, що захист інформації повинен по своїм характеристикам бути відповідним масштабам загроз. Відхилення від цього правила приведе до додаткових збитків. Для кожної інформаційної системи мається оптимальний рівень захищеності, який необхідно постійно підтримувати.

Нема сумнівів, що захист критично важливих для інформаційних систем масивів повинен відповідати міжнародним, корпоративним, нормативним і методичним документам. Застосовуються високовартісні технічні засоби і впроваджуються суворо регламентовані організаційні заходи. Однак нема відповіді на саме важливе питання – наскільки рішення, яке запропоновується або реалізовується, дійсно добре, яка його плануємо і реальна ефективність. Такому положенню, яке мається в інформаційній системі, но неможливому в області забезпечення інформаційної безпеки є ряд причин:

ігнорування системного підходу до методології аналізу і синтезу СЗІ;

відсутність механізмів повного і достовірного підтвердження якості СЗІ;

недоліки нормативно-методичного забезпечення інформаційної безпеки, перш за все в області показників і критеріїв.

Усім фахівцям в області захисту інформації відомі основні постулати, які не втратили актуальність до сих пір: абсолютний захист створити неможливо; система захисту інформації повинна бути комплексною; СЗІ повинна бути адаптованою до змін обстановки; СЗІ повинна бути системою, а не простим набіром хаотичних деяких технічних засобів і організаційних заходів, як це частіше буває на практиці; системний підхід до захисту інформації повинен застосовуватися, починаючи з підготовки технічного завдання і закінчуючи оцінкою ефективності і якості СЗІ в процесі її експлуатації – життєвий цикл КСЗІ.

Перш за все, СЗІ повинна мати цільове призначення. Причому, чім більш конкретно сформульована мета захисту інформації, детально уяснені ресурси, які маються і визначений комплекс обмежень, тім в більшої ступені можливо отримання позитивного результату. Коли мета забезпечення інформаційної безпеки проста і принципово досягається, то достатньо нескладних по структурі СЗІ. Однак при розширенні кола проблем, які треба вирішувати для забезпечення інформаційної безпеки, зміст цільового призначення системи на формалізованому рівні визначає багатомірний, векторний характер. При цьому важливість свойств окремих елементів СЗІ знижується і на перший план виходять загальносистемні задачі – визначення оптимальної структури і режимів функціонування системи, організація взаємодії між її елементами, облік впливів зовні-

6. Що є показники єффективности системи? Які вимоги до них?

7. Що таке критерії ефективності КСЗІ? Які концепції використовують для прийняття рішень?

8. Приклади критеріїв придатності, оптимальності й раціональності.

9. Які підходи використовують для оцінки ефективності КСЗІ?

проблеми, яка перед нею стоїть. Ефективність системи E є мірою її доцільності, пов'язаної з її призначенням, її вигідності, показником її здатності плідно працювати, зрештою – мірою її життєвості. Поняття ефективності завжди пов'язане з отриманням деякого корисного результату, який називають виграшем G. Виграш отримується ціною енергетичних, інформаційних, грошових та інших витрат, що забезпечують функціонування системи і називаються платою за виграш C.

5. Критерій ефективності системи – це правило, яке дозволяє співвідносити системи, що характеризуються різноманітною ефективністю, і здійснити направлений вибір систем з багатьох допустимих. Критерій ефективності формулюється на основі вибраного показника ефективності і відображає суб'єктивну мету прийняття рішення. Критерій ефективності вводиться на основі певної концепції прийняття рішень людиною:

- концепція максимізації корисності – критерій оптимальності – управлінське рішення вважається оптимальним, якщо воно забезпечує максимальну ефективність використання системи;
- концепція обмеженої раціональності – критерій придатності - управлінське рішення вважається задовільним, якщо воно забезпечує необхідну ефективність використання системи;
- концепція адаптивності – критерій раціональності – управлінське рішення вважається раціональним, якщо воно забезпечує оперативне реагування системи на поточну інформацію, що поступає до змін умов її функціонування

Контрольні питання

1. Яка мета етапу науково-дослідної розробки КСЗІ?
2. Визначте послідовність і зміст науково-дослідної розробки КСЗІ.
3. Що є моделювання КСЗІ? Які типи моделей використовуються?
4. У чому полягають особливості моделювання КСЗІ?
5. Які основні етапи оцінювання КСЗІ?

шнього середовища тощо. При цілеспрямованому об’єднанні елементів в систему остання потрибує специфічних свойств, які не маються ні в одній з її елементів, частин. При системному підході мають першочергове значення тільки ті свойства елементів, які визначають взаємодію друг з другом і не впливають на систему вцілому, а також на досягнення поставленої мети.

Результативне рішення задач аналізу і синтезу СЗІ не може бути забезпечено одними лише способами простого опису їх поведінки в різних умовах – системотехніка видвігає проблеми, які потребують кількісні оцінки характеристик. Такі дані, які отримані експериментально або шляхом математичного *моделювання*, повинні розкривати властивості СЗІ. Основним з них є ефективність, під якою розуміється ступінь відповідності результатів захисту інформації поставленій меті. Остання, в залежності від ресурсів, які маються, знань розробників та інших факторів, може бути досягнута в тій або іншій мірі, при цьому можливі альтернативні шляхи її реалізації. Ефективність має безпосередній зв’язок з іншими системними властивостями, в тому числі надійністю, живучістю, завадозахіщеністю – а в цілому стійкістю. Тому кількісна оцінка ефективності дозволяє вимірювати і об’єктивно аналізувати основні властивості систем на всіх стадіях їх життєвого циклу.

Частіше замовник СЗІ пагано уявляє собою значення того або іншого засобу і його необхідність в загальному рівні безпеки і в результаті збільшуються витрати при практичній невизначеності досягнутого ефекту. В подальшому замовник СЗІ не отримує те, що йому реально потрібно, і не може об’єктивно перевірити і оцінити якість і ефективність запропонованого рішення.

Тому на перший план стає проблема – як створити таку систему захисту інформації, яка б спроможна була при мінімальних витратах виконувати максимальні задачі захисту інформації. Цю проблему необхідно вирішувати поступово, починаючи з головного етапу життєвого циклу – проектування систем захисту інформації в комплексі з особливостями об’єкту захисту.

Автори висвітлюють глибоку подяку за уважне та доброзичливе рецензування, за висловлені зауваження і поради, які сприяли значному покращенню та поглибленню навчального посібника.

1 Порядок проведення робіт зі створення КСЗІ

Створення КСЗІ в ІТС здійснюється відповідно до **НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»** на підставі технічного завдання, розробленого згідно з вимогами **НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі»**.

1.1 Загальні положення щодо створення КСЗІ в інформаційно-телекомунікаційних системах

Нормативні документи з технічного захисту інформації визначають:

1. **Комплексна система захисту інформації (КСЗІ)** – сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС.

2. **Комплекс засобів захисту інформації (КЗЗ)** – сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

3. **Інформаційно-телекомунікаційна система (ІТС)** – це:

- **інформаційна** (або **автоматизована**) **система (ІС, АС)** – організаційно-технічна система, що реалізує технологію обробки інформації за допомогою засобів обчислювальної техніки та програмного забезпечення;
- **телекомунікаційна система (ТС)** – організаційно-технічна система, що реалізує технологію інформаційного обміну за допомогою технічних і програмних засобів шляхом передавання та приймання інформації у вигляді сигналів, знаків, звуків, зображень чи іншим чином;
- **інтегрована система** – сукупність двох або кількох взаємопов'язаних інформаційних та (або) телекомунікаційних систем, в якій функціонування однієї з них залежить від результатів функціонування іншої таким чином, що цю сукупність у процесі взаємодії можна розглядати як єдину систему.

Висновки

1. Науково-дослідна і дослідно-конструкторська розробка – це сукупність робіт, спрямованих на отримання нових знань і практичне застосування при створенні нового виробу або технології, при цьому: науково-дослідна робота (НДР) – робота пошукового, теоретичного і експериментального характеру, що виконується з метою визначення технічної можливості створення нової техніки в певні терміни. НДР підрозділяються на фундаментальні дослідження (отримання нових знань) і прикладні дослідження (застосування нових знань для вирішення конкретних завдань). Дослідно-конструкторська робота і Технологічна робота – комплекс робіт з розробці конструкторської і технологічної документації на дослідний зразок системи, виготовленню і випробуванням дослідного зразка системи, виконуваних за технічним завданням.

2. Моделювання КСЗІ полягає в побудові образу (моделі) системи, з певною точністю відтворюючого процеси, що відбуваються в реальній системі. Реалізація моделі дозволяє отримувати і досліджувати характеристики реальної системи. При моделюванні можуть використовуваться аналітичні (функціонування КСЗІ представляється у вигляді математичних і/або логічних співвідношень), імітаційні (на комп'ютері реалізуються алгоритми зміни основних характеристик реальної КСЗІ відповідно до еквівалентних реальним процесам математичними і логічними залежностями), детерміновані (оперують з детермінованими величинами) і стохастичні (оперують з випадковими величинами) типи моделей

3. Для подолання складнощів моделювання КСЗІ використовуються різні підходи: спеціальні методи неформального моделювання (структуризація архітектури процесів функціонування складних систем, неформальні методи оцінювання, неформальні методи пошуку оптимальних рішень), декомпозиція загального завдання на ряд часткових завдань), макромоделювання (здійснюється для загальної оцінки системи).

4. Оцінка ефективності КСЗІ можлива, якщо визначені показники її ефективності. Показник ефективності системи – це міра якості рішення системою

ефективності систем захисту є те, що не визначається ефективність конкретного механізму захисту, а констатується лише факт його наявності або відсутності. Цей недолік в якійсь мірі компенсується завданням в нормативних документах досить детальних вимог до цих механізмів захисту і вказівкою забезпечення гарантій.

3. **Експериментальний підхід** полягає в тому, що ефективність існуючих КСЗІ оцінюється шляхом спроб подолання захисних механізмів системи фахівцями, виступаючими в ролі порушників. Порядок експериментальної перевірки наступний:

- як умовний порушник вибирається один або декілька фахівців в області інформаційної боротьби найвищої кваліфікації;
- складається план проведення експерименту, в якому визначаються черговість і матеріально-технічне забезпечення проведення експериментів за визначенням слабких ланок в системі захисту (при цьому можуть моделюватися дії порушників, відповідні різним моделям їх поведінки: від некваліфікованого порушника, що не має офіційного статусу в досліджуваній ІТС, до висококваліфікованого співробітника служби безпеки);
- служба захисту інформації до моменту подолання захисту «порушниками» вводить в КСЗИ нові механізми захисту (змінює старі), щоб уникнути «злому» системи захисту;
- «порушник» використовуючи стандартні засоби ІТС або впроваджуючи власні апаратно-програмні засоби, намагається «зламати» систему захисту.

Такий підхід до оцінки ефективності дозволяє отримувати об'єктивні дані про можливості існуючих КСЗІ, але вимагає високої кваліфікації виконавців і великих матеріальних і тимчасових витрат. Для проведення експериментів необхідно мати найсучасніше устаткування (засоби інженерно-технічної розвідки, апаратно-програмні й випробувальні комплекси (стенди) і т.п.).

Процес створення КСЗІ полягає у *здійсненні комплексу взаємоузгоджених заходів*, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими актами та НД у сфері захисту інформації.

Порядок створення КСЗІ в ІТС – це сукупність впорядкованих у часі, взаємопов’язаних, об’єднаних в окремі етапи робіт, виконання яких необхідне й достатнє для КСЗІ, що створюється. Цей порядок не залежить від того, створюється КСЗІ в ІТС, яка проектується, чи в діючій ІТС, якщо виникла необхідність забезпечення захисту інформації або модернізації вже створеної КСЗІ.

Послідовність виконання та типовий зміст робіт кожного з етапів створення КСЗІ повинні узгоджуватися з відповідними стадіями і етапами робіт зі створення ІТС, визначеними **ГОСТ 34.601-90 Автоматизированные системы. Стадии создания**.

Етапи робіт, які виконуються під час створення КСЗІ в конкретній ІТС, їх зміст та результати, терміни виконання визначаються ТЗ на створення КСЗІ.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються:

– властивостями оброблюваної інформації;
– класом ІТС (АС);
– умовами експлуатації ІТС.

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

1) *витоку технічними каналами*:
– ПЕМВН;
– акустичними;
– електричними та електромагнітними;
– візуально-оптичними та ін.
2) *несанкціонованих дій та НСД до інформації*:
– підключення до апаратури та ліній зв’язку;
– маскування під зареєстрованого користувача;

– подолання заходів захисту з метою використання інформації або нав’язування хибної інформації;

– застосування закладних пристроїв чи програм;

– використання комп’ютерних вірусів та ін.;

3) *спеціального впливу на інформацію*:

– формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту;

У випадках, визначених законодавством, роботи з проектування, розроблення, виготовлення, випробування, експлуатації ІТС мають виконуватись у комплексі із заходами, щодо забезпечення режиму секретності, протидії технічним розвідкам, а також з режимними заходами щодо охорони ІзОД, яка не є державною таємницею.

Створення комплексів ТЗІ від витоку технічними каналами здійснюється, якщо в ІТС обробляється інформація, що становить державну таємницю, або коли необхідність цього визначено власником інформації.

Створення КЗЗ здійснюється в усіх ІТС, де обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІТС, де така необхідність визначена власником інформації.

Роботи зі створення КСЗІ виконуються організацією-власником (розпорядником) ІТС з дотриманням вимог нормативно-правових актів щодо провадження діяльності у сфері захисту інформації.

Для організації робіт зі створення КСЗІ в ІТС створюється служба захисту інформації, порядок створення, завдання, функції, структура та повноваження якої визначено в **НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі**.

Якщо ІТС є інтегрованою, то КСЗІ рекомендується будувати за *модульним принципом*, тобто кожна достатньо незалежна складова частина ІТС повинна мати свій власний модуль КСЗІ, взаємодія між якими забезпечується єдиною

безлічі необхідних функцій і досягається максимум або мінімум вибраного критерію, а також виконуються обмеження на деякі показники ефективності.

Така постановка застосовна не лише для вирішення загальної задачи, але і часткових завдань оцінки ефективності комплексної системи захисту інформації.

Ефективність КСЗІ оцінюється як на етапі розробки, так і в процесі експлуатації. В оцінці ефективності КСЗІ, залежно від використовуваних показників і способів їх отримання, можна виділити три підходи:

1. **Класичний підхід** пов'язаний з визначенням оцінки ефективності КСЗІ на основі використання *критеріїв ефективності*, отриманих за допомогою *показників ефективності*. Значення показників ефективності визначають шляхом моделювання або обчислювання за характеристиками реальних ІТС і систем захисту в них.

Такий підхід використовується при розробці і модернізації КСЗІ. Проте можливості класичних методів комплексного оцінювання ефективності стосовно КСЗІ обмежені через низку обставин:

- висока міра невизначеності вихідних даних;
- складність формалізації процесів функціонування;
- відсутність загальновизначених методик розрахунку показників ефективності і вибору критеріїв оптимальності та ін.

2. **Офіційний підхід** пов'язаний із застосуванням системи нормативних актів або стандартів держави, що визначають вимоги до захищеності інформації різних категорій конфіденційності і важливості.

Вимоги до КСЗІ задаються переліком механізмів захисту інформації, які необхідно мати в ІТС, щоб вона відповідала певному профілю захищеності. Використовуючи такі документи, можна оцінити ефективність КСЗІ. В цьому випадку критерієм ефективності КСЗІ є відповідність її характеристик і можливостей заданому профілю захищеності, вказаному в ТЗ (див. підрозділ 2.3).

Безперечною гідністю такого підходу до оцінки ефективності КСЗІ є простота використання. Основним недоліком офіційного підходу до визначення

ції та інформації, що прогнозується, з метою досягнення або збереження визначеної ефективності системи при змінних умовах функціонування.

Раціональним є рішення $u^*(t)$ з множини припустимих , яке, наприклад, забезпечує виконання умови

$$E_t(u^*(t),\tau) = \underset{u(t)\in U_{доп}(t)}{\text{extr}} E_t\left(u(t),\tau\right),\ G(u^*(t),\tau) \geq G_{t0},$$

де t - час; τ - упередження прогнозу.

$E_t(u(t),\tau)$ визначає, що на різноманітних етапах процесу функціонування системи можуть використовуватися різні показники ефективності.

Після вибору показників ефективності і критерію ефективності може бути здійснена **математична постановка завдання розробки КСЗІ**:

На цьому етапі вже відомі:

- $Q = \{Q_1, Q_2, \ldots, Q_N\}$ – функції, які повинна виконувати КСЗІ;
- $M = \{M_1, M_2, \ldots, M_L\}$ – можливі механізми захисту;
- $U = \{U_1, U_2, \ldots, U_F\}$ – способи управління КСЗІ;
- $F = \{F_1, F_2, \ldots, F_R\}$ – показники ефективності КСЗІ.

Показники ефективності залежать від виконуваних функцій, механізмів захисту і способів управління КСЗІ:

$$F = \Phi(Q, M, U).$$

Критерій ефективності виходить з використанням показників ефективності:

$$K = E(F).$$

Тоді **математична постановка завдання розробки КСЗІ** в загальному випадку може бути представлена в наступному виді: знайти

$$\text{extr}\ \Phi(Q, M^*, U^*) \text{ при } M^* \in M,\ U^* \in U,$$

яким відповідають $F^* \in F_{\text{доп}}$, де $F_{\text{доп}}$ - множина допустимих значень показників ефективності КСЗІ.

Вимагається *створити або вибрати такі механізми захисту інформації і способи управління системою захисту, при яких забезпечується виконання усієї*

підсистемою управління та обміну інформацією. Вибір заходів і механізмів захисту кожного модуля здійснюється відповідно до політики безпеки інформації в ІТС і концепції побудови КСЗІ ІТС, чим забезпечується їх узгодження між собою. Такий підхід має на меті забезпечити:

– реалізацію відкритої архітектури безпеки, зміст концепції, якої надано в **ISO 7498-2-89 Information proceeding systems. Open Systems Interconnection. Basic Reference Model. Part 2: SecurityArchitecture**;

– можливість незалежної розробки, впровадження, проведення випробувань, експлуатації окремо кожної складової частини КСЗІ;

– уніфікацію і здешевлення проектування КСЗІ;

– можливість оцінювання кожної складової частини КСЗІ окремо (для будь-якого виду випробувань).

1.2 Етапи створення КСЗІ

Загальна послідовність створення КСЗІ приведена на рис. 2.1.

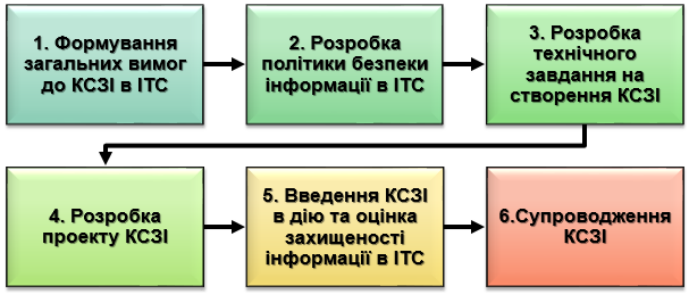

Рис. 2.1 Основні етапи створення КСЗІ

1. Формування загальних вимог до КСЗІ в ІТС

Цей етап включає наступні завдання:

- обґрунтування необхідності створення КСЗІ;
- обстеження середовищ функціонування ІТС;
- формування завдання на створення КСЗІ.

Обґрунтування необхідності створення КСЗІ. Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які

встановлюють обов'язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

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

- *аналізу нормативно-правових актів*, на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;
- *визначення наявності у складі інформації, яка підлягає автоматизованій обробці*, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно- правових актів;
- *оцінки можливих переваг* (фінансово-економічних, соціальних і т.п.) експлуатації ІТС у разі створення КСЗІ.

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ.

Обстеження середовищ функціонування ІТС. Під час обстеження ІТС розглядається як організаційно-технічна система, що поєднує обчислювальну систему (ОС), фізичне середовище її функціонування, середовище користувачів та експлуатаційників, інформацію, що наколюється та оброблюється, використовувані технології обробки інформації.

Цілями обстеження є:

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

меженнях (обмеження звичайно задаються системою рівнянь), тобто

$$E(u^*) = \operatorname*{extr}_{u \in U_{\text{пр}}} E(u),\ G(u) \geq G_0.$$

Застосування концепції оптимізації виправдано в тих випадках, коли умови функціонування системи суворо фіксовані, а показник ефективності не змінюється в часі.

Ця концепція призводить до цілеспрямованої, але не гнучкої системи дій, тобто не враховується поточна інформація щодо змін, які проходять в системі і у зовнішньому середовищі при реалізації рішень u^*.

Приклади критеріїв оптимальності:

- **критерій максимального середнього результату**, наприклад, якщо показником ефективності служить , то застосування критерію *максимуму математичного очікування числа відвернених атак порушників* на об'єкт інформаційної діяльності приведе до вибору такого рішення u^* з множини припустимих , яке забезпечує:

- **критерій максимальної гарантії** грунтується на показнику ефективності в формі *максимуму імовірності*. Наприклад, якщо використовується імовірність , то результатом використання критерію максимальної гарантії буде вибір рішення u^*, для якого:

3. **Критерії раціональності** використовуються для прийняття адаптивних рішень, тобто рішень, які передбачають можливість оперативного реагування в процесі функціонування системи на поточну інформацію, що поступає щодо змін умов її функціонування.

Концепція адаптивності полягає в зміні параметрів, структури і алгоритмів функціонування системи на основі не тільки апріорної, але і поточної інформа-

Якщо для прийняття рішення використовується скалярний показник ефективності, то задовільним буде будь-яке рішення u, якому відповідає оцінка показника ефективності не гірше, ніж деяке «порогове» значення E_0:

де – множина припустимих рішень.

Якщо використовується векторний показник ефективності, то задовільним буде рішення, яке задовольняє усім вимогам за частковими показниками одночасно або забезпечують необхідне значення узагальненого показника ефективності.

Прикладами критеріїв придатності є наступні:

- **критерій прийнятного середнього результату**, наприклад, *математичне очікування числа відвернених атак порушників* на об'єкт інформаційної діяльності, що захищається (). Наслідком застосування критерію прийнятного результату буде вибір тих рішень u^* з множини припустимих , які забезпечують виконання умови:

- **критерій припустимої гарантії.** В якості показника ефективності використовуються *імовірності досягнення цілі*, наприклад, імовірність збереження інформаційного об'єкту при атаці на нього (). Результатом застосування такого критерію буде прийняття u^* з множини припустимих , які забезпечують виконання умов:

2. **Критерії оптимальності** використовується для прийняття оптимальних рішень, тобто рішень, які забезпечують максимальну ефективність функціонування системи.

Оптимізація зводиться до визначення рішень , що екстремизують (максимізують або мінімізують) обраний показник ефективності при фіксованих об-

Обстеження виконується, коли розроблена концепція ІТС (основні принципи і підходи побудови); визначені основні завдання і характеристики ІТС, функціональних комплексів ІТС; існує варіант(и) їх реалізації.

Обстеження обчислювальної системи ІТС. ОС є центральним елементом ІТС і має бути ретельно проаналізована і описана:

а) *загальна структурна схема ОС та її склад*:

- перелік і склад обладнання, технічних і програмних засобів;
- їхні зв'язки, особливості конфігурації, архітектури та топології;
- програмні та програмно-апаратні засоби захисту інформації;
- взаємне розміщення засобів тощо.

б) *види і характеристики каналів зв'язку*;

в) *особливості взаємодії окремих компонентів*, їх взаємний вплив один на одного;

г) *можливі обмеження* щодо використання засобів та ін.

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

В процесі обстеження мають бути виявлені:

- компоненти ОС, які містять/не містять засобів і механізмів захисту інформації;
- потенційні можливості цих засобів і механізмів;
- їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням та ін.

При **обстеженні інформаційного середовища** аналізу підлягає вся інформація, що обробляється і зберігається в ІТС (дані і ПЗ). Під час аналізу інформація повинна бути:

- класифікована за режимом доступу;
- за правовим режимом;
- визначені й описані види (в термінах об’єктів ОС) її представлення в ІТС.

Для кожного виду інформації і типу об'єкта, в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність) чи ОС (спостережність), яким вони повинні задовольняти.

Обстеження технології обробки інформації повинно:

- виявити особливості обігу електронних документів;
- визначити джерела утворення інформаційних потоків та місця їх призначення;
- визначити й описати інформаційні потоки і середовища, через які вони передаються;
- визначити принципи та методи керування інформаційними потоками.

За результатами обстеження формується структурна **схема інформаційних потоків**, циркулюючих в ІТС, на якої фіксуються види носіїв інформації та порядок їх використання під час функціонування ІТС.

Для кожного структурного елемента схеми інформаційних потоків фіксуються:

- склад інформаційних об'єктів;
- режим доступу до них;
- можливий вплив на нього (елементу) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.

При **обстеженні фізичного середовища** здійснюється аналіз взаємного розміщення засобів обробки інформації ІТС на об'єктах інформаційної діяльності, комунікацій, систем життєзабезпечення і зв'язку, а також режим функціонування цих об'єктів.

Порядок проведення обстеження повинен відповідати **ДСТУ 3396.1 Захист інформації. Технічний захист інформації. Порядок проведення робіт**, а в частині, що стосується захисту інформації від витоку технічними каналами, – **НД ТЗІ 3.1-001 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи**.

пустима плата рівна C^*, то

$$E = G\big|_{C \le C^*}.$$

Оцінка ефективності КСЗІ проводиться з метою прийняття конкретних рішень при аналізі і синтезі таких систем (етап проектування), а також в процесі їх експлуатації. Такі рішення приймаються людьми за результатами використання *критеріїв ефективності*.

Критерій ефективності системи – це правило, яке дозволяє співвідносити системи, що характеризуються різноманітною ефективністю, і здійснити направлений вибір систем з багатьох допустимих.

Критерій ефективності формулюється на основі вибраного показника ефективності E і відображає суб'єктивну мету прийняття рішення. На відміну від показника, який лише оцінює кількісно або якісно ступінь досягнення мети, критерій ефективності дозволяє винести судження про прийнятність того чи іншого рішення.

Рис. 2.53 Можливі концепції прийняття рішень людиною

Критерій ефективності вводиться на основі певної концепції прийняття рішень людиною (рис. 2.53).

1. **Критерії придатності** використовується для прийняття задовільних рішень, які забезпечують необхідну ефективність функціонування системи.

ними величинами, які дозволяють кількісно оцінювати ефект застосування системи;

2) *адекватність* – відповідність меті системи (адекватний показник дозволяє оцінювати ефективність системи за ступенем досяжності її основної мети);

3) *змістовність* (*повнота*) – здатність показника дослідити ефективність системи без залучання інших її характеристик;

4) *чутливість* – здатність показника реагувати на зміни характеристик зовнішнього середовища і системи, які впливають на ефективність.

Ефективність системи *E* є мірою її доцільності, пов'язаної з її призначенням, її вигідності, показником її здатності плідно працювати, зрештою – мірою її життєвості.

Поняття ефективності завжди пов'язане з отриманням деякого корисного результату, який називають **виграшем *G***. Виграш отримується ціною енергетичних, інформаційних, грошових та інших витрат, що забезпечують функціонування системи і називаються **платою за виграш *C***.

Плату ***C*** не слід змішувати з первинними витратами на створення системи. Зрештою плата витрачається в зовнішньому середовищі, з яким взаємодіє система. Ця витрата може привести до руйнування внутрішньої структури системи, якщо його не заповнювати. Джерелом ресурсу для заповнення витрат служить виграш ***G***.

Якщо виграш ***G*** і плата ***C*** виражені в однакових одиницях виміру, то ефективність системи можна представити як різницю між виграшем і платою:

$$E = G - C.$$

Якщо виграш і плата виражені в різних одиницях виміру, то застосовуються інші форми ефективності, наприклад у вигляді відношення:

$$E = \frac{G}{C}.$$

Найбільш широке застосування знаходить форма ефективності, при якій ефективність дорівнює виграшу ***G*** при обмеженій платі ***C***. Якщо гранично до-

Аналізу підлягають такі характеристики фізичного середовища:

- територіальне розміщення компонентів ІТС (генеральний план, ситуаційний план);
- наявність охорони території та перепускний режим;
- наявність категорійованих приміщень, в яких мають розміщуватися компоненти ІТС;
- режим доступу до компонентів фізичного середовища ІТС;
- вплив чинників навколишнього середовища, захищеність від засобів технічної розвідки;
- наявність елементів комунікацій, систем життєзабезпечення і зв’язку, що мають вихід за межі контрольованої зони;
- наявність та технічні характеристики систем заземлення;
- умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;
- наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

При **обстеженні середовища користувачів** здійснюється аналіз:

- наявності служби захисту інформації в ІТС;
- функціонального та кількісного складу користувачів, їхніх функціональних обов’язків та рівня кваліфікації;
- повноважень користувачів щодо допуску до відомостей, які обробляються в ІТС, доступу до ІТС та її окремих компонентів;
- повноважень користувачів щодо управління КСЗІ;
- рівня можливостей різних категорій користувачів, що надаються їм засобами ІТС.

Результати обстеження середовищ функціонування ІТС оформлюються у вигляді **акту** і включаються, у разі необхідності, до відповідних розділів плану захисту інформації в ІТС, який розробляється згідно з **НД ТЗІ 1.4-001**.

За результатами обстеження середовищ функціонування ІТС затверджується **перелік об’єктів захисту** (з урахуванням рекомендацій **НД ТЗІ 1.4-001**,

НД ТЗІ 2.5-007, **НД ТЗІ 2.5-008**, **НД ТЗІ 2.5-010** щодо класифікації об'єктів), а також **визначаються потенційні загрози** для інформації і **розробляються модель загроз** та **модель порушника**. Побудова моделей здійснюється відповідно до положень **НД ТЗІ 1.1-002**, **НД ТЗІ 1.4-001** та **НД ТЗІ 1.6-003**.

Модель загроз для інформації та модель порушника рекомендується оформляти у вигляді окремих документів (або поєднаних в один документ) плану захисту.

Етап завершується формуванням **завдання на створення КСЗІ**, в якому визначаються:

- завдання захисту інформації в ІТС;
- мета створення КСЗІ;
- варіант вирішення задач захисту (відповідно до **ДСТУ 3396.1**);
- основні напрями забезпечення захисту.
- перелік суттєвих загроз (на основі аналізу ризиків – вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз; величини можливих збитків та ін.);
- загальна структура та склад КСЗІ;
- вимоги до можливих заходів, методів та засобів захисту інформації;
- допустимі обмеження щодо застосування певних заходів і засобів захисту;
- інші обмеження щодо середовищ функціонування ІТС, обмеження щодо використання ресурсів ІТС для реалізації задач захисту;
- припустимі витрати на створення КСЗІ;
- умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів);
- загальні вимоги до співвідношення та меж застосування в ІТС організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ.

Про виконання робіт цього етапу складається **звіт** та оформлюється **заявка на розробку КСЗІ** (тактико-технічного завдання на створення КСЗІ або інший документ аналогічного змісту, що його замінює).

10.3 Вибір показників ефективності та критеріїв оптимальності КСЗІ

Проектування і експлуатація КСЗІ виявили проблеми, рішення яких можливе тільки на основі комплексної оцінки різних за своєю природою чинників, різнорідних зв'язків, зовнішніх умов. У зв'язку з цим в системному аналізі виділяють розділ, пов'язаний з визначенням якості систем і ефективності процесів, що реалізовуються в цих системах.

Цілі оцінки складних систем:

- *оптимізація* – вибір найкращого алгоритму з декількох, що реалізовують закон функціонування системи;
- *ідентифікація* – визначення системи, якість якої найбільш відповідає реальному об'єкту в заданих умовах;
- *підготовка даних для прийняття рішень* по управлінню системою.

Основні етапи оцінювання КСЗІ показані на рис. 2.52

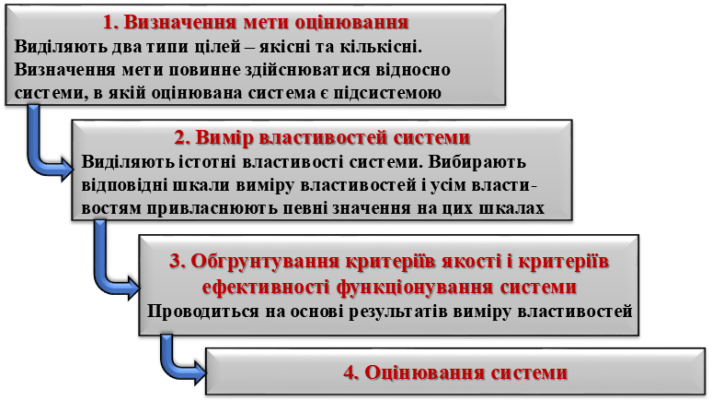

Рис. 2.52 Етапи оцінювання КСЗІ

Оцінка ефективності КСЗІ можлива, якщо визначені *показники* її ефективності. **Показник ефективності системи** – це *міра якості рішення системою проблеми, яка перед нею стоїть*.

Вимоги до показників ефективності системи:

1) *обчислювальність* – значення можуть бути розмірними або безрозмір-

умови, що атака на шифр можлива тільки шляхом перебору ключів, і відомий метод шифрування. **Середній час злому шифру** за цих умов розраховується по формулі:

$$T = \frac{A^S \cdot t}{2}.$$

де A – число символів, які можуть бути використані при виборі ключа (потужність алфавіту шифрування);

S – довжина ключа, виражена у кількості символів;

t – час перевірки одного ключа, який залежить від продуктивності використовуваного для атаки на шифр комп'ютера і складності алгоритму шифрування.

Головна складність методу декомпозиції при оцінці КСЗІ полягає в обліку взаємозв'язку і взаємного впливу окремих задач оцінювання і оптимізації. Цей вплив враховується як при рішенні задачі декомпозиції, так і в процесі отримання інтегральних оцінок.

3. **Макромоделювання КСЗІ** здійснюється для загальної оцінки системи. Задача спрощується за рахунок використання при побудові моделі тільки основних характеристик КСЗІ. До таких моделей прибігають, в основному, для отримання попередніх оцінок системи.

Наприклад, якщо в КСЗІ використовується k рівнів захисту, а порушник не має ніякого офіційного статусу на об'єкті ІТС, то йому необхідно здолати усі k рівнів захисту, щоб отримати доступ до інформації. Для такого порушника ймовірність діставання несанкціонованого доступу до інформації $P_{\text{нсд}}$ може бути розрахована за формулою:

де P_i – ймовірність подолання порушником i-го рівня захисту.

На макрорівні можна, наприклад, досліджувати необхідне число рівнів захисту, їх ефективність по відношенню до передбачуваної моделі порушника з урахуванням особливостей ІТС і фінансових можливостей проектування і побудови КСЗІ.

2. Розробка політики безпеки інформації в ІТС

Наступним етапом створення КСЗІ є розробка найважливішого документу – **політики інформаційної безпеки в ІТС** – комплексу взаємопов'язаних керівних принципів і розроблених на їх основі правил, процедур і практичних прийомів, прийнятих в організації для забезпечення інформаційної безпеки в ІТС. На цьому етапі вирішуються завдання:

- вивчення об'єкта, на якому створюється КСЗІ, і проведення науково-дослідних робіт;
- вибір варіанту КСЗІ;
- оформлення політики безпеки.

При **вивченні об'єкта, на якому створюється КСЗІ**, розробник КСЗІ проводить детальне вивчення об'єкта інформатизації, на якому створюється КСЗІ, уточнює моделі загроз, потенційного порушника та результати аналізу можливості керування ризиками. В разі необхідності він виконує додаткові науково-дослідні роботи (НДР), пов'язані з пошуком шляхів реалізації завдання на створення КСЗІ, розробкою альтернативних варіантів концепції створення КСЗІ і планів їх реалізації.

За результатами НДР здійснюється **вибір оптимального варіанту КСЗІ** на основі оцінки переваг і недоліків кожного з альтернативних варіантів. Обрана концепція оформлюється у вигляді звіту.

Оформлення політики безпеки. При вирішенні цього завдання здійснюється:

- *вибір основних рішень* з протидії всім суттєвим загрозам;
- *формування загальних вимог*, правил, обмежень, рекомендацій і т.п., які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій;
- *документальне оформлення* політики безпеки інформації.

Політика безпеки може розроблятись для ІТС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремих

компонентів, для окремої функціональної задачі, для окремої технології обробки інформації тощо.

Політика безпеки розробляється згідно з положеннями **НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу** та рекомендаціями **НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі** .

Політику безпеки рекомендується оформляти у вигляді окремого документу – **Плану захисту**.

3. Розробка технічного завдання на створення КСЗІ

Технічне завдання (ТЗ) на створення КСЗІ в ІТС є засадним організаційно-технічним документом, який визначає:

- вимоги із захисту оброблюваної в ІТС інформації;
- порядок створення КСЗІ;
- порядок проведення всіх видів випробувань КСЗІ;
- порядок введення КСЗІ в експлуатацію в складі ІТС.

ТЗ на створення КСЗІ розробляється на відповідній стадії робіт зі створення ІТС з урахуванням *комплексного підходу* до побудови КСЗІ, який передбачає об'єднання в єдину систему усіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу ІТС.

ТЗ на створення КСЗІ розроблюється для вперше створюваних ІТС, а також під час модернізації вже існуючих ІТС.

Для оформлення ТЗ на КСЗІ можуть бути використані такі варіанти:

1) у вигляді *окремого розділу ТЗ* на створення ІТС (рекомендується застосовувати для вперше створюваних ІТС);

2) у вигляді *окремого* (*часткового*) *ТЗ*;

3) у вигляді *доповнення до ТЗ* на створення ІТС (рекомендується застосовувати у випадку модернізації КСЗІ, модернізації діючих ІТС, а також для ІТС, які вже мають затверджене ТЗ на створення, в якому не міститься окремого розділу із захисту інформації).

Для інтегрованих ІТС, які будуються за модульним принципом, вимоги до

го відсікання безперспективних шляхів руху лабіринтом і серед шляхів, що залишилися, з великою ймовірністю знайде шлях рішення поставленої задачі.

Концептуальний метод припускає виконання дій з *концептами*, під якими розуміються узагальнені елементи і зв'язки між ними. Концепти формуються в процесі побудови структурованої моделі. Фахівець проводить уявний експеримент із структурованою моделлю і породжує обмежену ділянку лабіринту, в якої вже нескладно знайти рішення.

Еволюційним моделюванням є різновид імітаційного моделювання. Особливість його полягає в тому, що в процесі моделювання удосконалюється алгоритм моделювання.

2. **Декомпозиція загальної задачі оцінки ефективності функціонування КСЗІ**. Для вирішення проблеми складності дослідження КСЗІ застосовується метод декомпозиції (розподілу) загальної задачі оцінки ефективності на ряд часткових задач:

- оцінка ефективності захисту від збоїв і відмов апаратних і програмних засобів;
- оцінка ефективності захисту від НСД;
- оцінка ефективності захисту від ПЕМВН;
- оцінка ефективності захисту від розголошення;
- оцінка ефективності захисту комунікаційних каналів і т.д.

Наприклад, при оцінці ефективності захисту від відмов, що призводять до знищення інформації, використовується ймовірність безвідмовної роботи $\boldsymbol{P(t)}$ системи за час t, яка обчислюється за формулою:

де $\boldsymbol{P_{від}(t)}$ – ймовірність відмови системы за час t.

Величина $\boldsymbol{P_{від}(t)}$, у свою чергу, розраховується по відомій в теорії надійності формулі:

де $\boldsymbol{\lambda}$ – інтенсивність відмов системи (число відмов в одиницю часу).

Просто вирішується задача **оцінки ефективності методу шифрування** за

- *методи неформального зведення складного завдання до формального опису і рішення задачі формальними методами* (використовують методи теорії нечітких множин, теорії конфліктів, теорії графів, формально-евристичні методи, еволюційне моделювання тощо);

- *методи неформального пошуку оптимального рішення* засновані на тому, що людина бере участь не тільки в побудові моделі, але і в процесі її реалізації.

Методи теорії нечітких множин дозволяють отримувати аналітичні вирази для кількісних оцінок нечітких умов приналежності елементів до тієї або іншої множини. Ця теорія добре узгоджується з умовами моделювання систем захисту, оскільки багато вихідних даних моделей (наприклад, характеристики загроз і окремих механізмів захисту) не є строго визначеними.

Теорія конфліктів моделює конфлікт між порушником і системою захисту, що розгортається на тлі випадкових загроз. Дві протиборчі сторони переслідують строго протилежні цілі. Конфлікт розвивається в умовах неоднозначності і слабкої передбаченості процесів, здатності сторін оперативно змінювати цілі. Теорія конфліктів є розвитком *теорії ігор*, яка дозволяє структурувати завдання, представити його в осяжному вигляді, знайти області кількісних оцінок, впорядкувань, переваг, виявити домінуючі стратегії, якщо вони існують.

З **теорії графів** для дослідження систем захисту інформації найбільшою мірою застосуємо апарат *мереж Петрі*. Управління умовами у вузлах мережі Петрі дозволяє моделювати процеси подолання захисту порушником.

До **формально-евристичних методів** віднесені методи пошуку оптимальних рішень не на основі строгих математичних, логічних співвідношень, а грунтуючись на досвіді людини, наявних знаннях та інтуїції. Отримувані рішення можуть бути далекі від оптимальних, але вони завжди будуть кращі за рішення, що отримуються без евристичних методів. Найбільшого поширення з евристичних методів набули *лабіринтові* і *концептуальні методи*.

У **лабіринтовій моделі** задача представляється людині у вигляді лабіринту можливих шляхів рішення. Передбачається, що фахівець має здатність швидко-

КСЗІ кожної із складових частин ІТС рекомендується оформляти окремим документом.

Дозволяється готувати один документ (доповнення до ТЗ на створення ІТС, окреме ТЗ) на декілька однотипних складових частин КСЗІ, вказавши існуючі між ними відмінності чи особливості.

Єдиним обмеженням при розробці окремого ТЗ на створення КСЗІ або доповнення до ТЗ на створення ІТС є *дотримання в них єдиної системи понять, позначень, ідентифікації об'єктів* тощо, які застосовуються в ТЗ на створення ІТС.

Для будь-якого з наведених варіантів розроблення та оформлення ТЗ на КСЗІ його зміст, порядок погодження та затвердження повинен відповідати **НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі** та **ГОСТ 34.602-89 Комплекс стандартів на автоматизовані системи. Технічне завдання на створення автоматизованої системи**.

4. Розробка проекту КСЗІ

Проект КСЗІ розробляється на підставі та у відповідності до ТЗ на створення ІТС. Під час розробки проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації.

Проектування КСЗІ виконується на таких стадіях створення ІТС:

- ескізне проектування;
- технічне проектування;
- робоче проектування.

Стадію ескізного проектування можливо вилучити, а стадії технічного і робочого проектування об'єднати в єдину стадію «Техноробочий проект КСЗІ».

Для всіх стадій розробки проекту КСЗІ склад документації, що розроблюється, визначається ТЗ на КСЗІ, її види та зміст – **ГОСТ 34.201-89 Виды, комплектность и обозначение документов при создании автоматизированных**

систем, **НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу**. Документація на програмні засоби виконується згідно з вимогами комплексу стандартів єдиної системи програмної документації (ЄСПД), на технічні засоби – згідно з комплексом стандартів єдиної системи конструкторської документації (ЄСКД).

На стадії **ескізного проекту КСЗІ** здійснюється розробка попередніх проектних рішень КСЗІ та, у разі необхідності, її окремих складових частин, а також розроблення, оформлення, узгодження та затвердження документації на КСЗІ. Зміст та стиль документації повинні бути достатніми для повного опису проектних рішень рівня ескізного проекту.

В ескізному проекту визначаються:

- функції КСЗІ в цілому та функції її окремих складових частин;
- склад комплексів технічного захисту інформації від витоку технічними каналами та від спеціальних впливів;
- склад заходів протидії технічним розвідкам, організаційних, правових та інших заходів захисту;
- склад комплексу засобів захисту (КЗЗ);
- узагальнена структура КСЗІ та схема взаємодії складових частин.

Пропонуються попередні технічні рішення, за допомогою яких передбачається реалізація завдань і функцій КСЗІ.

На стадії **технічного проекту КСЗІ** здійснюється розробка:

1) проектних рішень КСЗІ:
2) документації на КСЗІ
3) документації на постачання засобів захисту інформації
4) завдань на проектування в суміжних частинах

При **розробці проектних рішень КСЗІ** виконується:

- розробка загальних проектних рішень, необхідних для реалізації вимог ТЗ на КСЗІ;

витком формального опису складних систем, поширеного на організаційно-технічні системи.

Умови структурованого опису систем, що вивчаються, і процесів їх функціонування:

- повнота відображення основних елементів і їх взаємозв'язків;
- адекватність;
- простота внутрішньої організації елементів опису і взаємозв'язків елементів між собою;
- стандартність і уніфікованість внутрішньої структури елементів і структури взаємозв'язків між ними;
- модульність;
- гнучкість (можливість розширення і зміни структури);
- доступність вивчення і використання моделі будь-якому фахівцеві середньої кваліфікації відповідного профілю.

2) **Методи неформального оцінювання** полягають в залученні для отримання деяких характеристик КСЗІ, які не можуть бути виміряні безпосередньо або вичислені аналітичними методами, фахівців-експертів у відповідних галузях знань.

До таких характеристик КСЗІ відноситься:

- ймовірність реалізації деяких загроз;
- цінність відомостей, що захищаються;
- окремі характеристики ефективності систем захисту та ін.

Найбільшого поширення з неформальних методів оцінювання набули методи *експертних оцінок* (асоціацій, парних порівнянь, векторів переваг, середньої точки, експертних опитувань, Дельфі, мозкового штурму, аналізу ієрархій та ін.). Будь-який з методів експертних оцінок є алгоритмом підбору фахівців-експертів, завдання правил отримання незалежних оцінок кожним експертом і подальшої статистичної обробки отриманих результатів.

3) **Неформальні методи пошуку оптимальних рішень** розділяються на дві групи:

Рис. 2.50 Особливості моделювання КСЗІ

Для подолання складнощів моделювання КСЗІ використовуються різні підходи (рис. 2.51).

Рис. 2.51 Підходи подолання складнощів моделювання КСЗІ

1. В основі **спеціальних методів неформального моделювання** лежить застосування положень теорії систем. Основними складовими частинами неформальної теорії систем є:

1) **Структуризація архітектури і процесів функціонування КСЗІ** є роз-

- розробка рішень щодо структури КСЗІ (організаційної структури, структури технічних і програмних засобів), алгоритмів функціонування та умов використання засобів захисту;
- розробка рішень щодо архітектури КЗЗ та механізмів реалізації, визначених функціональним профілем послуг безпеки інформації.

Здійснюються 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 специфікаціями **НД ТЗІ 2.5-004**, **НД ТЗІ 2.5-007**, **НД ТЗІ 2.5-008**, **НД ТЗІ2.5-010**.

Розробка документації на КСЗІ – виконується розроблення, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ на КСЗІ. Зміст та стиль документації повинні бути достатніми для повного опису проектних рішень рівня технічного проекту.

Розробка документації на постачання засобів захисту інформації та/або технічних вимог (технічних завдань) на їх розробку – готується та оформляється документація на постачання засобів захисту або продукції, що містить їх у своєму складі, для комплектації КСЗІ. Якщо необхідної продукції немає на ринку засобів захисту, то визначаються технічні вимоги (складаються ТЗ) на розроблення відповідних засобів.

Розробка завдань на проектування в суміжних частинах – здійснюється розроблення, оформлення і затвердження завдань на проектування з суміжних питань, які пов’язані зі створенням КСЗІ або впливають на умови її функціонування (будівельні, електротехнічні, санітарно-технічні та інші підготовчі роботи).

На стадії **робочого проекту КСЗІ** здійснюється розроблення, оформлення та затвердження робочої та експлуатаційної документації КСЗІ та її окремих складових частин. Робоча документація містить:

- детальні рішення щодо реалізації технічного проекту КСЗІ;
- рішення щодо забезпечення управління КСЗІ і взаємодії її компонентів;

- документацію, необхідну для тестування, проведення пусконалагоджувальних робіт, проведення випробувань КСЗІ.

Проводиться розробка засобів захисту інформації або адаптація готової продукції до умов функціонування КСЗІ. Розробка засобів захисту інформації від НСД здійснюється згідно з **НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу**.

До складу робочої документації на комплекси ТЗІ від витоку технічними каналами повинні входити схеми розміщення основних технічних засобів (ОТЗ) ІТС, кабельного обладнання, мереж живлення та систем заземлення, які виконуються у відповідності до вимог нормативних документів **ТР ЕОТ – 95**, **ТР ТЗІ – ПЕМВН-95**, **СТР-2**, **СТР-3**, **НД ТЗІ 3.3-001**, **НД ТЗІ 2.4-007**, **СВТР-78**. При цьому враховуються умови їх розміщення і мінімально допустимі відстані між цими засобами та допоміжними технічними засобами (ДТЗ) (засоби зв'язку, системи та засоби кондиціювання, сигналізації, електроосвітлення, радіомовлення, часофікації тощо), що знаходяться у приміщенні, де розташоване обладнання ІТС, та у суміжних приміщеннях. Зазначені умови розміщення та мінімально допустимі відстані беруться з експлуатаційної документації, яка супроводжує сертифіковані ОТЗ.

У разі відсутності для ОТЗ, що використовуються в складі КСЗІ, сертифікатів відповідності вимогам з ТЗІ, мінімально допустимі відстані та інші умови розміщення цих засобів мають бути визначені за результатами їх спеціальних досліджень.

До складу робочої документації на КЗЗ повинні входити описи:

- процедур інсталяції та ініціалізації комплексу;
- налагодження всіх механізмів розмежування доступу користувачів до інформації та апаратних ресурсів ІТС;
- контролю за діями користувачів;
- формування та актуалізації баз даних захисту;

- типи використовуваних апаратних і програмних засобів і режими їх роботи;
- взаємодія із зовнішніми системами.

10.2 Методи моделювання КСЗІ

Ефективність захисту інформації – це ступінь відповідності результатів захисту інформації поставленої мети.

Оцінка ефективності функціонування КСЗІ є складним науково- технічним завданням.

Комплексна система захисту інформації оцінюється в процесі:

- розробки ІТС;
- в період експлуатації ІТС;
- при створенні (модернізації) КСЗІ для вже існуючих ІТС

за допомогою *моделювання*.

При розробці КСЗІ поширеним методом проектування є *синтез з подальшим аналізом*: система синтезується шляхом узгодженого об'єднання блоків, пристроїв, підсистем і аналізується (оцінюється) ефективність отриманого рішення. З множини синтезованих систем вибирається краща за наслідками аналізу, який здійснюється за допомогою моделювання.

Моделювання КСЗІ полягає в побудові образу (моделі) системи, з певною точністю відтворюючого процеси, що відбуваються в реальній системі. Реалізація моделі дозволяє отримувати і досліджувати характеристики реальної системи.

Таблиця 2.46 Моделі КСЗІ

Тип моделі	Особливості
Аналітична	Функціонування КСЗІ записується у вигляді математичних і/або логічних співвідношень
Імітаційна	На комп'ютері реалізуються алгоритми зміни основних характеристик реальної КСЗІ відповідно до еквівалентних реальним процесам математичними і логічними залежностями
Детермінована	Оперує з детермінованими величинами
Стохастична	Оперує з випадковими величинами

Моделювання КСЗІ має ряд **особливостей**, перерахованих на рис. 2.50.

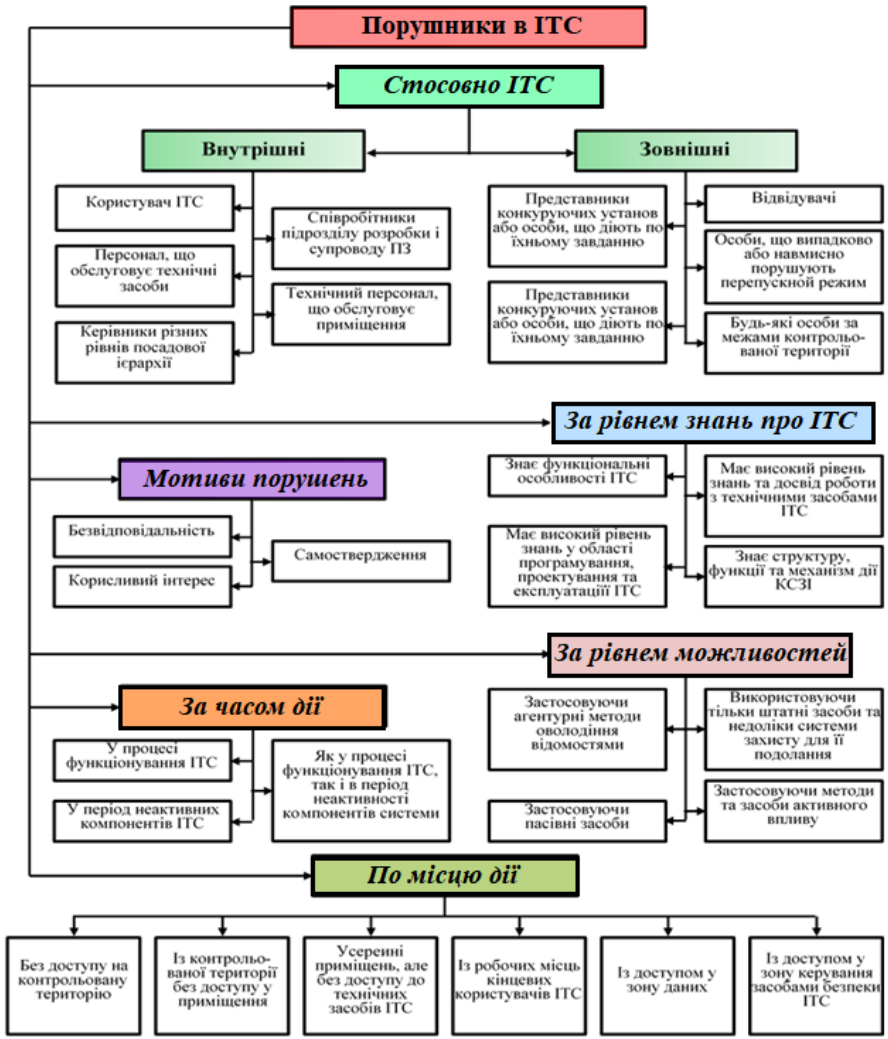

Рис. 2.49 Графічне представлення моделі порушника

7. **ІТС, що захищається**:
   - географічне положення ІТС;
   - тип ІТС (розподілена або зосереджена);
   - структура ІТС (технічна, програмна, інформаційна);
   - продуктивність і надійність елементів ІТС;

- контролю цілісності програмного забезпечення та баз даних захисту.

Документація робочого проекту повинна містити вихідні дані для внесення їх до баз даних захисту.

Експлуатаційна документація включає:

- опис порядку функціонування КСЗІ;
- настанови (інструкції) щодо забезпечення цього порядку обслуговуючим персоналом і користувачами, порядку супроводження КСЗІ впродовж життєвого циклу ІТС.

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

Цей етап створення КСЗІ пов'язаний з фізичним втіленням рішень, прийнятих на стадії технічного проектування системи захисту, і включає реалізацію ряду завдань, перерахованих на рис. 2.2.

Рис. 2.2 Завдання, що реалізовуються на етапі введення в експлуатацію

1. Підготовка КСЗІ до введення в дію. На цей стадії проводяться роботи з підготовки організаційної структури, розроблюються розпорядчі документи, що регламентують діяльність із забезпечення захисту інформації в ІТС, здійснюється створення служби захисту інформації (СЗІ) (призначаються відповідальні особи за захист інформації), якщо цього не було зроблено на попередніх етапах.

В основному має бути завершена розробка і затверджені документи, що входять до Плану захисту (за виключенням тих, для розробки яких необхідні результати наступних етапів робіт).

Створення СЗІ та розробка Плану захисту здійснюється згідно з **НД ТЗІ 1.4-001**.

2. Навчання користувачів ІТС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та користувачів, які мають повноваження щодо управління засобами КСЗІ та ін.):

- в частині, що їх стосується;
- основним положенням документів Плану захисту, які необхідні їм для дотримання правил політики безпеки інформації;
- експлуатації засобів захисту інформації тощо;
- перевірка їх уміння користуватись впровадженими технологіями захисту інформації;
- реєстрація результатів навчання.

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

4. Будівельно-монтажні роботи. Роботи цій стадії виконуються під час переобладнання існуючих або при будівництві нових спеціалізованих споруд (приміщень), призначених для розміщення технічних засобів ІТС та персоналу, сховищ матеріальних носіїв інформації.

При проведенні будівельно-монтажних робіт враховуються вимоги ТЗ на створення КСЗІ в ІТС.

Будівельні роботи здійснюються силами організації-власника ІТС або будівельно-монтажними організаціями згідно з проектною документацією на будівництво, яка розробляється проектною організацією у відповідності до вимог нормативних документів **ДБН А.2.2-2**, **ДБН2.2-3-2004**.

Після завершення будівельних робіт створюється комісія з прийняття робіт. За результатами роботи комісії складається **акт приймання робіт** з оцінкою їх відповідності вимогам ТЗІ, який затверджується керівником організації-замовника будівництва.

- розробка моделі загроз безпеці інформації в ІТС (містить систематизовані відомості про всі можливі випадкові і навмисні загрози, їх небезпеку, тимчасові рамки дії, вірогідність реалізації) (рис. 2.48);

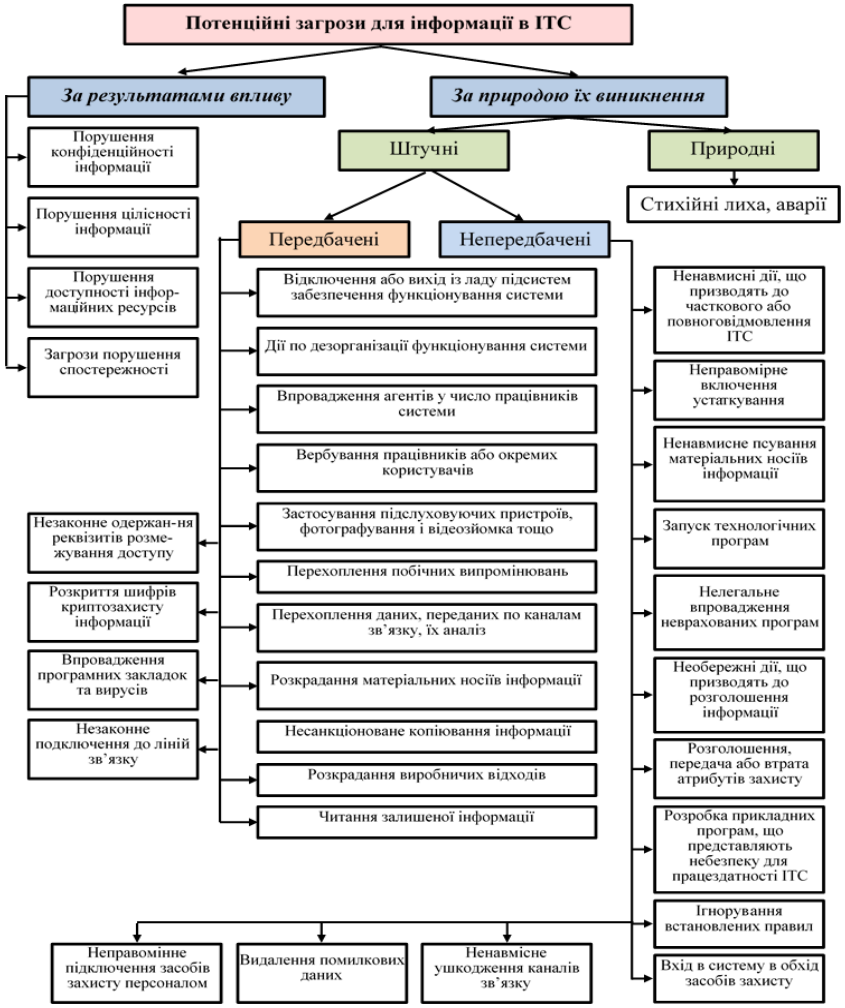

Рис. 2.48 Графічне представлення моделі загроз

- розробка моделі порушника, яка орієнтується на висококваліфікованого зловмисника-професіонала, оснащеного всім необхідним і що має легальний доступ на всіх рубежах захисту (рис. 2.49).

нову, або організовує спільну їх роботу.

Послідовність і зміст науково-дослідницької розробки КСЗІ приведена на рис. 2.47.

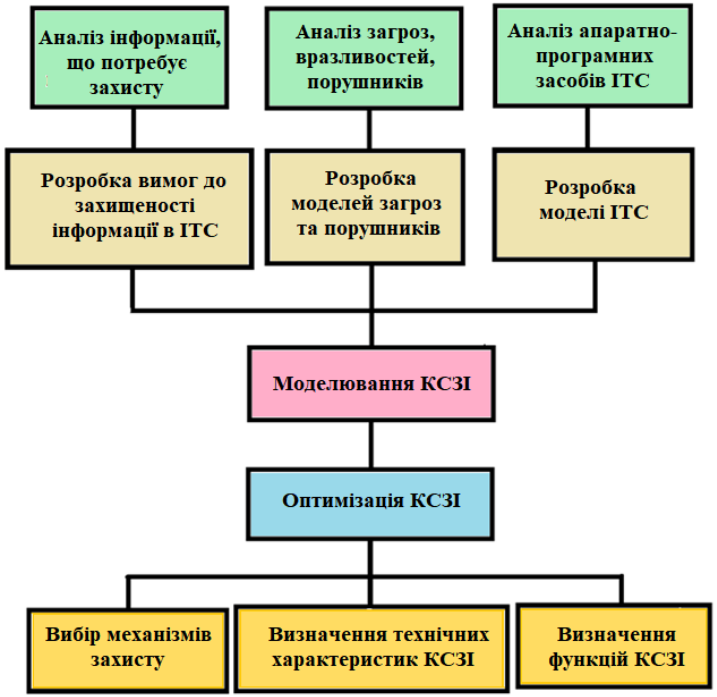

Рис. 2.47 Основні моделі, що створюються в процесі НДР КСЗІ

Науково-дослідна розробка КСЗІ починається з аналізу:

5. **Конфіденційності і важливості інформації в ІТС**:

- визначаються потоки конфіденційної інформації, елементи ІТС, в яких вона обробляється і зберігається;
- розглядаються питання розмежування доступу до інформації окремих користувачів і сегментів ІТС;
- визначаються вимоги до захищеності інформації (шляхом присвоєння грифу конфіденційності, встановлення ПРД).

6. **Загроз безпеці інформації в ІТС, вразливостей апаратно-програмних засобів і технологій обробки інформації**:

5. Пуско-налагоджувальні роботи. Метою цій стадії є:

- монтаж обладнання і атестація комплексу ТЗІ від витоку технічними каналами;
- встановлення і налагодження КЗЗ;
- перевірка працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії.

Монтаж ОТЗ ІТС, кабельного обладнання, мереж живлення та заземлення здійснюється згідно з конструкторською документацією робочого проекту.

Якщо до складу КСЗІ входять ОТЗ, які не мають сертифікатів відповідності вимогам з ТЗІ, визначаються мінімально допустимі відстані між цими засобами та ДТЗ за результатами їх спеціальних досліджень.

Ефективність вжитих заходів із захисту інформації повинна бути підтверджена результатами *інструментальної перевірки* під час випробувань створеного комплексу ТЗІ.

Спеціальні дослідження та інструментальні вимірювання рівня ПЕМВН виконуються підрозділом ТЗІ організації-власника ІТС або іншими суб'єктами господарювання за умови наявності ліцензії чи дозволу на здійснення відповідного виду робіт.

За результатами робіт складається **акт**, де зазначаються:

- категорії приміщень, де розташоване обладнання ІТС;
- межі контрольованих зон для приміщень;
- перелік ОТЗ, ДТЗ і комунікацій (із вказівкою найменування, типу, заводського номеру), що знаходяться у цих приміщеннях;
- оцінка відповідності проведення монтажних робіт вимогам експлуатаційних документів на засоби та нормативних документів;
- пропозиції щодо застосування додаткових заходів захисту, впровадження яких є необхідним у разі неможливості під час виконання монтажних робіт дотримання окремих вимог із розміщення ОТЗ.

Акт затверджується керівником організації – власника ІТС.

Здійснюється впровадження додаткових заходів захисту, необхідність

впровадження яких зафіксована в акті, відповідно до порядку проведення робіт етапу та відповідне коригування проектної, робочої, експлуатаційної документації.

Оцінка повноти та якості виконання робіт з ТЗІ в приміщеннях проводиться шляхом *атестації* впровадженого комплексу ТЗІ від витоку технічними каналами, за результатами якої надається документ встановленого зразка – **«Акт атестації комплексу технічного захисту інформації»**. Порядок здійснення атестації, зміст та форма «Акту ...» визначається **НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації**.

На стадії здійснюється інсталяція, ініціалізація та перевірка працездатності КЗЗ згідно з документацією робочого проекту.

Інсталяція та ініціалізація КЗЗ, який має експертний висновок щодо його відповідності вимогам НД ТЗІ, здійснюється у порядку, визначеному в експлуатаційній документації на цей комплекс.

Під час інсталяції мають бути задіяні всі механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, контролю за діями користувачів, а також контролю цілісності програмного забезпечення та бази даних захисту КЗЗ.

До бази даних захисту вносяться відомості про користувачів ІТС, встановлюються їх повноваження щодо доступу до захищених об'єктів КС, їх створення, модифікації, архівування, знищення, експорту/імпорту із системи та інші дані.

6. Попередні випробування. Метою цих 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 методиками випробувань, які готує розробник КСЗІ, а узгоджує замовник ІТС. Програма та методики випробувань, протоколи випробувань розробляються та оформлю-

можливості створення нової техніки в певні терміни. НДР підрозділяються на:

- *фундаментальні дослідження* (отримання нових знань);
- *прикладні дослідження* (застосування нових знань для вирішення конкретних завдань).

Дослідно-конструкторська робота (ДКР) і **Технологічна робота (ТР)** – комплекс робіт по розробці конструкторської і технологічної документації на дослідний зразок системи, виготовленню і випробуванням дослідного зразка системи, виконуваних за технічним завданням.

Метою етапу науково-дослідної розробки КСЗІ є розробка технічного завдання на проектування КСЗІ, яке містить:

3) Основні технічні вимоги до КСЗІ:
   - значення основних технічних характеристик;
   - виконувані функції;
   - режими роботи;
   - взаємодія із зовнішніми системами і т.д.
4) Узгоджені взаємні зобов'язання замовника і виконавця розробки.

Рис. 2.46 Характеристики оцінки апаратно-програмних засобів КСЗІ

Основним змістом етапу науково-дослідної розробки КСЗІ є *визначення оцінок характеристик апаратно-програмних засобів КСЗІ* (рис. 2.46), а також *складу виконуваних функцій* і *режимів роботи засобів захисту*, *порядку їх використання і взаємодії із зовнішніми системами*. Для проведення досліджень на цьому етапі замовник може привертати виконавця або науково-дослідну уста-

10 Науково-практичні дослідження КСЗІ

Система захисту інформації повинна створюватися спільно із створюваною ІТС. Одним з основних етапів розробки КСЗІ є *етап розробки технічного завдання*. Саме на цьому етапі вирішуються практично всі специфічні завдання, характерні саме для розробки КСЗІ.

Процес розробки систем, що закінчується виробленням технічного завдання, називають **науково-дослідною розробкою**, а решту частини роботи із створення складної системи називають **дослідно-конструкторською розробкою апаратно-програмних засобів**, яка ведеться із застосуванням систем автоматизації проектування.

10.1 Науково-дослідна розробка КСЗІ

При розробці і побудові КСЗІ в ІТС необхідно дотримуватися певних методологічних принципів проведення досліджень, проектування, виробництва, експлуатації і розвитку таких систем.

КСЗІ в ІТС відносяться до класу *складних систем* і для їх побудови використовуються основні **принципи побудови складних систем** з урахуванням специфіки вирішуваних завдань:

- паралельна розробка ІТС і КСЗІ;
- системний підхід до побудови захищених ІТС;
- багаторівнева структура КСЗІ;
- ієрархічна система управління КСЗІ;
- блокова архітектура захищених ІТС;
- можливість розвитку КСЗІ;
- дружній інтерфейс захищених ІТС з користувачами.

Науково-дослідна і дослідно-конструкторська розробка (НДДКР) – це сукупність робіт, спрямованих на отримання нових знань і практичне застосування при створенні нового виробу або технології, при цьому:

Науково-дослідна робота (НДР) – робота пошукового, теоретичного і експериментального характеру, що виконується з метою визначення технічної

ються згідно з вимогами **РД 50-34.698-90 Руководящий документ по стандартизации. Автоматизированные системы. Требования к содержанию документов**.

Попередні випробування організовує замовник ІТС, а проводить розробник КСЗІ спільно із замовником. Для проведення попередніх випробувань замовником ІТС створюється комісія. Головою комісії призначається представник замовника.

Результати попередніх випробувань оформлюються **«Протоколом випробувань»**, де міститься висновок щодо можливості прийняття КСЗІ у дослідну експлуатацію, а також перелік виявлених недоліків, необхідних заходів з їх усунення, і рекомендовані терміни виконання цих робіт.

Після усунення недоліків у випадку їх наявності та коригування проектної, робочої, експлуатаційної документації КСЗІ оформлюється **акт про приймання КСЗІ у дослідну експлуатацію**.

7. Дослідна експлуатація. Під час дослідної експлуатації КСЗІ:

- відпрацьовуються технології обробки інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;
- співробітники СЗІ та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;
- здійснюється доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування КЗЗ;
- здійснюється коригування робочої та експлуатаційної документації.

За результатами робіт складається **акт про завершення дослідної експлуатації**, який містить висновок щодо можливості (або неможливості) представлення КСЗІ на державну експертизу.

8. Державна експертиза КСЗІ – це окремий етап приймальних випробувань ІТС, який проводиться з метою визначення відповідності КСЗІ технічному

завданню, вимогам НД із захисту інформації та визначення можливості введення КСЗІ в складі ІТС в експлуатацію.

Державна експертиза КСЗІ в ІТС проводиться згідно з **Положенням про державну експертизу в сфері ТЗІ** (наказ від 16.05.2007 № 93 Адміністрації ДССЗЗІ України).

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

Для інтегрованих ІТС може проводитись державна експертиза кожної складової частини (модуля) КСЗІ окремо. Державна експертиза КСЗІ інтегрованої ІТС полягає у перевірці взаємодії (адміністрування, обміну даними бази даних захисту тощо) вже оцінених модулів.

Документи, що містять результати робіт кожного з етапів (протоколи, акти, атестати відповідності) для КСЗІ ІТС в цілому, оформлюються з урахуванням відповідних документів на складові частини КСЗІ.

Якщо інтегрована КСЗІ має у своєму складі типові модулі, які створювались за єдиним ТЗ, то експертиза таких модулів КСЗІ виконується в два етапи:

- на першому проводиться у повному обсязі експертиза одного обраного типового модуль;
- на другому – здійснюється перевірка відповідності умов експлуатації типовим на кожному конкретному об’єкті для всіх модулів КСЗІ цього типу.

Введення до складу діючої КСЗІ нового (оціненого) модуля здійснюється без проведення повторної експертизи всієї КСЗІ. Проводиться оцінювання взаємодії нового модуля зі складовими частинами КСЗІ, які вже знаходяться в експлуатації.

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

3. Які вимоги ТЗІ мають бути вказані в завданні на проектування об'єкту?
4. Визначите основні функції замовника об'єкту будівництва.
5. Яка мета пуско-налагоджувальних робіт?
6. Що включає організація доступу до ресурсів?
7. Поясніть основні принципи контролю доступу в ІТС.
8. Які функції системи розмежування доступу?
9. Яка структура системи розмежування доступу?
10. Якими шляхами забезпечується цілісність і доступність інформації в ІТС на етапі експлуатації?
11. Поясніть завдання, які вирішуються в процесі технічної експлуатації КСЗІ.

пристроїв згідно з вимогами експлуатаційно-технічної документації;

- *метрологічне забезпечення* – дозволяє підтримувати вимірювальні прилади в справному стані;

- *забезпечення безпеки експлуатації* – в процесі експлуатації важливо забезпечувати безпеку обслуговуючого персоналу і користувачів передусім від загрози поразки електричним струмом, а також від можливих пожеж.

В цілому від рівня технічної експлуатації багато в чому залежить ефективність використання КСЗІ.

Висновки

1. Введення КСЗІ в дію включає: підготовку КСЗІ до введення в дію, навчання користувачів, кмплектування КСЗІ, будівельно-монтажні роботи, пусконалагоджувальні роботи, попередні випробування, дослідну експлуатацію, державну експертизу КСЗІ.

2. Процес експлуатації КСЗІ можна розділити на застосування системи по прямому призначенню, що припускає виконання усього комплексу заходів, безпосередньо пов'язаних із захистом інформації в ІТС, і технічну експлуатацію.

3. Експлуатація в техніці – частина життєвого циклу технічної системи, упродовж якого вона використовується за призначенням. Задачі, що вирішуються в процесі технічної експлуатації КСЗІ: організаційні задачі (планування технічної експлуатації, організація чергування, робота з кадрами, робота з документами), підтримку працездатності КСЗІ (проведення технічного обслуговування, постійний контроль працездатності, її відновлення у разі відмови), забезпечення технічної експлуатації (матеріально-технічне забезпечення, транспортування і зберігання, метрологічне забезпечення, забезпечення безпеки експлуатації.

Контрольні питання

1. Які роботи виконуються при введенні КСЗІ в дію?
2. У чому сенс будівельно-монтажних робіт?

Приймальні випробування ІТС проводяться при функціонуючій в її складі КСЗІ.

6. Супроводження КСЗІ

На цьому етапі виконуються роботи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійному і післягарантійному технічному обслуговуванню засобів захисту інформації.

Висновки

1. Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими актами та НД у сфері захисту інформації. Порядок створення КСЗІ в ІТС – це сукупність впорядкованих у часі, взаємопов’язаних, об’єднаних в окремі етапи робіт, виконання яких необхідне й достатнє для КСЗІ, що створюється.

2. До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від витоку технічними каналами, несанкціонованих дій та несанкціонованого доступу до інформації, спеціального впливу на інформацію. Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС.

3. Етапи створення КСЗІ: 1) формування загальних вимог до КСЗІ в ІТС, 2) розробка політики безпеки інформації в ІТС, 3) розробка технічного завдання на створення КСЗІ, 4) розробка проекту КСЗІ, 5) введення КСЗІ в дію та оцінка захищеності інформації в ІТС, 6) супроводження КСЗІ.

Контрольні питання

1. У чому суть процесу і порядку створення КСЗІ?
2. У чому сенс побудови КСЗІ інтегрованою ІТС за модульним принципом?

3. З яких етапів складається процес створення КСЗІ?

4. Які рішення приймаються на етапі формування загальних вимог до КСЗІ?

5. Як обґрунтовується необхідність створення КСЗІ в ІТС?

6. У чому полягає мета обстеження середовища функціонування ІТС?

7. Що визначається в процесі формування завдання на створення КСЗІ?

8. У чому сенс розробки політики безпеки інформації в ІТС?

9. Що здійснюється в процесі оформлення політики безпеки?

10. Що визначає технічне завдання на створення КСЗІ?

11. Які існують варіанти на оформлення ТЗ на КСЗІ?

12. Що визначається на етапі ескізного проектування КСЗІ?

13. Що виконується на етапі технічного проектування КСЗІ?

14. Що робиться на етапі робочого проектування КСЗІ?

15. Які роботи включені в етап введення КСЗІ в дію?

16. У чому полягає зміст пусконалагоджувальних робіт?

17. Яка мета попередніх випробувань КСЗІ?

18. Що виконується під час дослідницької експлуатації КСЗІ?

19. Яка мета державної експертизи КСЗІ і що при цьому робиться?

20. У чому сенс супроводу КСЗІ?

ти за сумісництвом і функції загального адміністрування в комп'ютерній мережі. Робоче місце оператора КСЗІ, як правило, розташовується у безпосередній близькості від найбільш важливих компонентів ІТС (серверів, міжмережевих екранів і т.п.) і оснащується усіма необхідними засобами оперативного управління КСЗІ.

Робота з обслуговуючим персоналом і користувачами зводиться до підбору кадрів, їх навчання, виховання, до створення умов для високоефективної праці.

В процесі технічної експлуатації використовується чотири типи документів:

1) закони (загальні питання експлуатації КСЗІ);

2) відомчі керівні документи (інструкції, директиви, державні стандарти, методичні рекомендації і т.п.);

3) документація підприємств-виробників (технічні описи, інструкції з експлуатації, формуляри (паспорти) та ін.);

4) документація, що розробляється в процесі експлуатації (планююча і обліково-звітна документація).

Працездатність підтримується за рахунок проведення технічного обслуговування, постійного контролю працездатності та її відновлення у разі відмови. Працездатність засобів захисту інформації контролюється постійно за допомогою апаратно-програмних засобів вбудованого контролю і періодично посадовцями служби безпеки і комісіями. Терміни проведення контролю і об'єм робіт визначаються в керівних документах.

Успіх технічної експлуатації залежить від якості забезпечення, яке включає:

- *матеріально-технічне забезпечення* – дозволяє задовольнити потребу у витратних матеріалах, запасних виробах і приладах, інструментах та інших матеріальних засобах, необхідних для експлуатації КСЗІ;

- *транспортування і зберігання облаштувань захищеної ІТС* повинні передбачати захист від НСД до пристроїв в дорозі і в сховищах. Для забезпечення необхідних умов транспортування і зберігання виконуються заходи підготовки

- *контроль над реалізацією політики безпеки*.

9.3 Технічна експлуатація КСЗІ

Експлуатація в техніці – частина життєвого циклу технічної системи, упродовж якого вона *використовується за призначенням*.

Задачі, що вирішуються в процесі технічної експлуатації КСЗІ, показано на рис. 2.45.

Рис. 2.45 Завдання, що реалізовуються в процесі експлуатації КСЗІ

Планування технічної експлуатації здійснюється на тривалі терміни (півроку, рік і більше). Використовується також середньострокове (квартал, місяць) і короткострокове планування (тиждень, доба). На тривалі терміни плануються піврічне технічне обслуговування і робота комісій, постачання устаткування, запасних виробів і приладів, ремонти пристроїв і т.п. Середньострокове планування і короткострокове застосовуються при організації технічного обслуговування, проведенні доопрацювань, організації чергування та ін.

Для безперервного виконання організаційних заходів захисту і експлуатації усіх механізмів захисту організовується *чергування*. Режим чергування залежить від режиму використання ІТС. Черговий оператор КСЗІ може виконува-

2 Технічне завдання на створення КСЗІ в ІТС

Створення КСЗІ в ІТС здійснюється відповідно до **НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі** на підставі технічного завдання, розробленого згідно з вимогами **НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі**.

2.1 Загальні вимоги до розробки технічного завдання на створення КСЗІ в ІТС

Технічне завдання на створення КСЗІ в ІТС (ТЗ на КСЗІ) є засадничим організаційно-технічним документом для виконання робіт щодо забезпечення захисту інформації в системі і розробляється у разі необхідності розробки або модернізації КСЗІ існуючої ІТС.

В разі розробки КСЗІ в процесі проектування ІТС допускається оформлення вимог з захисту інформації в ІТС у вигляді окремого (часткового) ТЗ, доповнення до загального ТЗ на ІТС або розділу загального ТЗ на ІТС.

ТЗ на КСЗІ розроблюється з урахуванням *комплексного підходу* до побудови КСЗІ, який передбачає об'єднання в єдину систему всіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу ІТС.

В ТЗ на КСЗІ викладаються:

1) *вимоги до функціонального складу і порядку розробки і впровадження технічних засобів*, що забезпечують безпеку інформації в процесі її обробки в обчислювальній системі ІТС;

2) *вимоги до організаційних, фізичних та інших заходів захисту*, що реалізуються поза обчислювальної системи ІТС у доповнення до комплексу програмно-технічних засобів захисту інформації.

Перелік вимог з захисту інформації, які включаються в ТЗ на КСЗІ, може бути для кожної конкретної ІТС як *розширений*, так і *скорочений* відносно ре-

комендованого переліку в рамках діючих законодавчих і нормативних документів.

Вимоги повинні передбачати розробку та використання сучасних ефективних засобів і методів захисту, які дають можливість забезпечити виконання цих вимог з найменшими матеріальними затратами.

ТЗ на КСЗІ є одним із обов'язкових засадничих документів під час проведення експертизи ІТС на відповідність вимогам захищеності інформації.

Вихідні дані для розробки ТЗ на КСЗІ наведені на рис. 2.3.

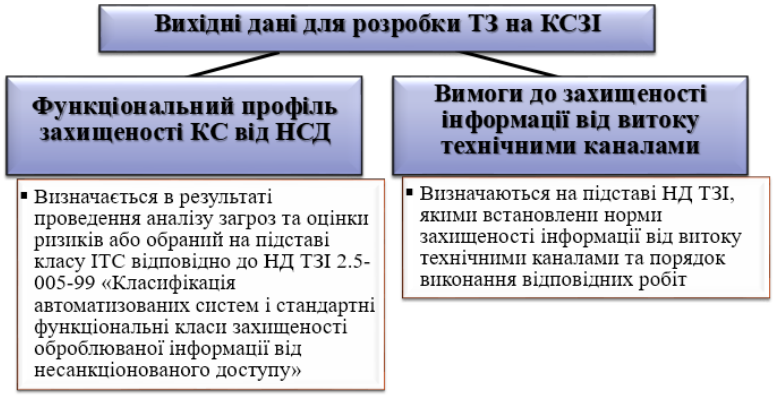

Рис. 2.3 Вихідні дані, що потрібні для створення технічного завдання

В ТЗ повинно бути наведено обгрунтування вибору функціонального профілю захищеності та вимог до показників захищеності інформації від витоку технічними каналами.

Перелік основних робіт етапу формування ТЗ:

- *класифікація та опис ресурсів ІТС* (обчислювальної системи, засобів зв'язку і комунікацій, інформації, її категорій, виду подання, місця зберігання, технології обробки тощо, обслуговуючого персоналу і користувачів, території і приміщень і т.ін.);

- *розробка інформаційної моделі для існуючої ІТС*, тобто опис (формальний або неформальний) інформаційних потоків ІТС, інтерфейсів між користувачем та ІТС і т.ін.;

В процесі виконання спеціальних робіт необхідно виключити використання не перевірених апаратних і програмних засобів, відхилення від встановленої документацією технології проведення робіт, доступ до носіїв з конфіденційною інформацією і до елементів ІТС, що функціонують в робочих режимах.

Спеціальні роботи завершуються контролем працездатності ІТС і відсутності закладок:

- перевірка на відсутність апаратних закладок здійснюється шляхом огляду пристроїв і тестування їх в усіх режимах;

- відсутність програмних закладок перевіряється по контрольних сумах, а також шляхом тестування.

Результати доопрацювань приймаються комісією і оформляються актом, в якому мають бути відбиті результати перевірки працездатності і відсутності закладок. Після перевірок здійснюється відновлення інформації і задіюються усі механізми захисту.

Успіх експлуатації КСЗІ великою мірою залежить від *рівня організації управління процесом експлуатації*. Ієрархічна система управління дозволяє організувати реалізацію політики безпеки інформації на етапі експлуатації ІТС. При організації системи управління слід дотримуватися наступних принципів:

- *рівень компетенції керівника повинен відповідати його статусу в системі управління* (кожен посадовець повинен мати знання і навички роботи з КСЗІ в об'ємі, достатньому для виконання своїх функціональних обов'язків);

- *строга регламентація дій посадовців* (посадовці повинні розташовувати мінімально можливими відомостями про конкретні механізми захисту і про інформацію, що захищається);

- *документування алгоритмів забезпечення захисту інформації* (це дозволяє, при необхідності, легко замінювати посадовців, а також здійснювати контроль над їх діяльністю);

- *безперервність управління* (досягається за рахунок організації чергування операторів КСЗІ);

- *адаптивність системи управління до умов функціонування, що змінюються*;

періодичність і способи контролю їх цілісності мають бути визначені перед початком експлуатації ІТС.

Контроль **цілісності програм і файлів** здійснюється:

- обчисленням *контрольних сум*;
- використанням криптографічних *хеш-функцій*.

Для унеможливлення внесення змін до контрольованого файлу з подальшою корекцією контрольної суми необхідно зберігати контрольну суму в зашифрованому виді або використовувати секретний алгоритм обчислення контрольної суми.

Значення хеш-функції практично неможливо підробити без знання ключа. Тому слід зберігати в зашифрованому виді або в пам'яті, недоступній порушникові, тільки ключ хешування (стартовий вектор хешування).

Особлива увага має бути зосереджена на забезпеченні *цілісності структур ІТС* і *конфіденційності інформації*, захисту від розкрадання і несанкціонованого копіювання інформаційних ресурсів під час проведення технічного обслуговування, відновлення працездатності, ліквідації аварій, а також в період модернізації ІТС.

Оскільки на час проведення таких спеціальних робіт відключаються (чи знаходяться в непрацездатному стані) багато технічних і програмних засобів захисту, то їх відсутність компенсується системою організаційних заходів:

- підготовка ІТС до виконання робіт;
- допуск фахівців до виконання робіт;
- організація робіт на об'єкті;
- завершення робіт.

Перед проведенням робіт повинні робитися наступні кроки:

- відключити фрагмент ІТС, на якому необхідно виконувати роботи, від функціонуючої ІТС;
- зняти носії інформації з пристроїв;
- здійснити стирання інформації в пам'яті ІТС;
- підготувати приміщення для роботи фахівців.

- *визначення переліку загроз* і *можливих каналів витоку інформації*;
- *експертна оцінка очікуваних втрат* у разі здійснення загроз;
- *визначення послуг безпеки*, які треба реалізувати;
- *обґрунтування необхідності проведення спецперевірок і спецдосліджень* засобів обчислювальної техніки (ЗОТ) та інших технічних засобів, а також спеціального обладнання приміщень;
- *визначення вимог до організаційних, фізичних та інших заходів захисту*, що реалізуються у доповнення до комплексу програмно-технічних засобів захисту;
- *визначення вимог до метрологічного забезпечення* робіт;
- *визначення переліку макетів*, що розробляються, і технологічних стендів;
- *оцінка вартості і ефективності обраних засобів*;
- *прийняття остаточного рішення про склад КСЗІ*.

ТЗ на КСЗІ оформлюється відповідно до ГОСТ 34.602-89 Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системи. Розділи ТЗ приведені на рис. 2.4.

Рис. 2.4 Зміст технічного завдання на створення КСЗІ

2.2 Вимоги до змісту розділів технічного завдання

1. Загальні відомості. В підрозділі зазначають:

- повне найменування КСЗІ та її умовне позначення;
- шифр теми і реквізити договору на створення КСЗІ;
- найменування підприємств-розробників і замовника (користувача) КСЗІ та їх реквізити;
- перелік документів, на підставі яких створюється КСЗІ, ким і коли затверджені ці документи;
- планові терміни початку і закінчення роботи із створення КСЗІ;
- відомості про джерела і порядок фінансування робіт;
- порядок оформлення і подання замовнику результатів робіт із створення КСЗІ, з виготовлення і налагодження окремих засобів (технічних, програмних, інформаційних) і програмно-технічних (програмно-методичних) комплексів системи.

2. Мета і призначення КСЗІ. Вказується мета розробки КСЗІ в ІТС, функціональне призначення і особливості застосування. Необхідно зазначати, на підставі яких нормативно-правових актів, інших нормативних документів регламентується порядок захисту інформації в ІТС.

3. Загальна характеристика ІТС і умов її функціонування. В підрозділі рекомендується зазначити такі моменти:

а) *загальну структурну схему і склад обчислювальної системи ІТС*:

- перелік і склад устаткування, технічних і програмних засобів;
- їх зв'язки;
- особливості конфігурації і архітектури;
- особливості підключення до локальних або глобальних мереж тощо;

б) *технічні характеристики каналів зв'язку*:

- пропускна спроможність;
- типи кабельних ліній;
- види зв'язку з віддаленими сегментами ІТС і користувачами і т.ін.;

в) *характеристики інформації, що обробляється*:

тему, забезпечує необхідну конфігурацію і режими роботи ІТС, вводить в СРД повноваження і атрибути користувачів, здійснює контроль і управляє доступом користувачів до ресурсів ІТС.

На етапі експлуатації ІТС цілісність і доступність інформації в системі забезпечується різними шляхами (рис. 2.44).

Однією з головних умов забезпечення цілісності і доступності інформації в ІТС є її **дублювання**. Стратегія дублювання вибирається з урахуванням:

- важливості інформації,
- вимог до безперервності роботи ІТС,
- трудомісткості відновлення даних.

Дублювання інформації забезпечується черговим адміністратором ІТС.

Цілісність і доступність інформації підтримується шляхом *резервування апаратних засобів*, *блокувань помилкових дій людей*, *використання надійних елементів ІТС і відмовостійких систем*. Усуваються також умисні загрози перевантаження елементів систем використовуванням механізмів виміру інтенсивності вступу заявок на виконання (передачу) і механізмів обмеження або повного блокування передачі таких заявок. Має бути передбачена також можливість визначення причин різкого збільшення потоку заявок на виконання програм або передачу інформації.

В результаті збоїв апаратних або програмних засобів, алгоритмічних помилок, допущених на етапі розробки, помилок операторів в системі відбуваються *зациклення програм*, *непередбачені остановки* та інші ситуації, вихід з яких можливий лише шляхом переривання обчислювального процесу і подальшого його відновлення. На етапі експлуатації ведеться статистика і здійснюється аналіз таких ситуацій. «Зависання» своєчасно виявляються і обчислювальний процес відновлюється. При відновленні, як правило, необхідно повторити виконання перерваної програми з початку або з контрольної точки, якщо використовується механізм контрольних точок.

У захищеній ІТС повинне використовуватися тільки *дозволене програмне забезпечення*. Перелік офіційно дозволених до використання програм, а також

зберігаються на зовнішніх пристроях пам’яті, а також за рахунок повного стирання файлів при їх знищенні і стирання тимчасових файлів.

У розподілених ІТС доступ між підсистемами регулюється за допомогою *міжмережевих екранів*. Міжмережевий екран необхідно використовувати для управління обміном між захищеною і незахищеною комп'ютерними системами.

Якщо атрибути суб'єкта доступу або алгоритм його дій не є дозволеними для цього суб'єкта, то подальша робота в ІТС такого порушника припиняється до втручання оператора КСЗІ. Засоби блокування виключають або значною мірою утрудняють автоматичний підбір атрибутів доступу.

В журналах реєстрації подій записуються дані про вхід користувачів в систему і про вихід з неї, про усі спроби виконання несанкціонованих дій, про доступ до певних ресурсів і т.п. Налаштування журналу на фіксацію певних подій і періодичний аналіз його вмісту здійснюється черговим оператором і вищестоящими посадовцями з підрозділу СЗІ. Процес налаштування і аналізу журналу доцільно автоматизувати програмним шляхом.

Рис. 2.44 Шляхи забезпечення цілісності і доступності інформації на етапі експлуатації ІТС

Безпосереднє управління СРД здійснює черговий оператор КСЗІ, який, як правило, виконує і функції чергового адміністратора ІТС. Він завантажує сис-

- категорії інформації;
- вищий гриф конфіденційності (секретності) й т.ін.;

г) *характеристики персоналу*:

- кількість користувачів і категорій користувачів;
- форми допуску тощо;

д) *характеристики фізичного середовища*:

- наявність категорованих приміщень;
- територіальне розміщення компонентів ІТС;
- їх фізичні параметри;
- вплив на них чинників навколишнього середовища;
- захищеність від засобів технічної розвідки і т.п.;

е) *загальні технічні характеристики ІТС*:

- обсяги основних інформаційних масивів і потоків;
- швидкість обміну інформацією і продуктивність системи під час розв'язання функціональних завдань;
- тривалість процедури підготовки ІТС до роботи після подачі живлення на її компоненти;
- тривалість процедури відновлення працездатності після збоїв;
- наявність засобів підвищення надійності та живучості й т.ін.;

є) *особливості функціонування ІТС*:

- надання машинного часу або устаткування в оренду стороннім організаціям;
- цілодобовий режим роботи без відключення живлення тощо;

ж) *особливості реалізованих або припустимих організаційних, фізичних та інших заходів захисту*:

- режимні заходи в приміщеннях і на території;
- охорона, сигналізація, протипожежна охорона і т.ін.;

з) *інші чинники*, що впливають на безпеку оброблюваної інформації;

и) *потенційні загрози інформації*:

- способи здійснення НСД;

- можливі технічні канали витоку інформації і умови їх формування;
- стихійні лиха і т.ін.;
- можливі наслідки їх реалізації.

і) клас ІТС згідно з **НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу**;

ї) *функціонуючі* в складі ІТС (для існуючої ІТС) *засоби захисту*;

й) *засоби захисту*, реалізовані в компонентах, *які планується використовувати* для побудови ІТС.

Треба враховувати, що функції захисту, які реалізуються засобами імпортного виробництва, не мають зв'язаного з ними рівня гарантій. Використання таких засобів у складі КСЗІ можливе тільки за наявності експертного висновку, зареєстрованого Адміністрацією ДССЗЗІ України.

В підрозділі не вказуються ті характеристики і умови функціонування ІТС, опис яких є в ТЗ на ІТС або в інших документах. Даються тільки посилання на розділи цих документів.

4. Вимоги до КСЗІ визначаються окремо для захисту від загроз НСД і витоку інформації технічними каналами.

Вимоги до КСЗІ в ІТС в частині захисту від НСД мають бути викладені відповідно до **НД ТЗІ 2.5-004-99 Критерії оцінки захищеності комп'ютерних систем від несанкціонованого доступу**. Згідно з цим документом в процесі оцінки захищеності КС розглядаються вимоги двох видів:

1) вимоги до функцій (послуг) забезпечення безпеки;
2) вимоги до рівня гарантій.

Тому в ТЗ на КСЗІ повинні бути зазначені вимоги обох видів.

Крім того, має бути вказаний *функціональний профіль захищеності*, який передбачається реалізувати. Профіль може бути або вибраний із профілів, описаних в **НД ТЗІ 2.5-005-99**, або визначений як упорядкована сукупність рівнів послуг згідно з вимогами зазначеного документа. Повинен бути вказаний рівень гарантій, що передбачається досягти.

- контроль над правильністю виконання процедур автентифікації в ІТС.

При компрометації атрибутів доступу (пароля, персонального коду і т.п.) потрібне термінове їх виключення зі списку дозволених. Ці дії виконуються черговим оператором СРД.

Розподіл секретних ключів шифрування повинен здійснюватися поза ІТС, що захищається. Значення ідентифікаторів користувача не повинні зберігатися і передаватися в системі у відкритому виді.

Засоби розмежування доступу до технічних засобів перешкоджають несанкціонованим діям порушника:

- включення технічного засобу;
- завантаження операційної системи;
- введення-виведення інформації;
- використання нештатних пристроїв і т.д.

Розмежування доступу здійснюється оператором СРД шляхом використання технічних і програмних засобів. Він контролює використання ключів від замків подачі живлення безпосередньо на технічний засіб або на усі пристрої, що знаходяться в окремому приміщенні, дистанційно управляє блокуванням подачі живлення на пристрій або блокуванням завантаження операційної системи.

На апаратному або програмному рівні оператор може змінювати технічну структуру засобів, які може використовувати конкретний користувач.

Апаратно-програмні засоби розмежування доступу до програм і даних використовуються найінтенсивніше і багато в чому визначають характеристики СРД. Вони настроюються посадовцями підрозділу СЗІ і змінюються при зміні повноважень користувача або при зміні програмної та інформаційної структури.

Доступ до файлів регулюється **диспетчером доступу**. Доступ до записів і окремих полів записів у файлах баз даних регулюється також за допомогою СКБД.

Ефективність СРД можна підвищити за рахунок шифрування файлів, що

- реакцію на спроби НСД, наприклад, сигналізацію, блокування, відновлення після НСД;
- тестування;
- очищення оперативної пам'яті і робочих областей на магнітних носіях після завершення роботи користувача з даними, що захищаються;
- облік вихідних друкарських і графічних форм і твердих копій в ІТС;
- контроль цілісності програмної і інформаційної частини як СРД, так і засобів, що забезпечують її.

Структура системи розмежування доступу приведена на рис. 2.43.

Рис. 2.43 Система розмежування доступу в ІТС

Ефективність функціонування СРД залежить від надійності механізмів автентифікації, яка здійснюється із застосуванням методів криптографії. При експлуатації механізмів автентифікації основними завданнями є:

- генерація або виготовлення ідентифікаторів;
- їх облік і зберігання;
- передача ідентифікаторів користувачеві;

Опису послуг має передувати **опис політики безпеки інформації**, яку повинен реалізувати комплекс засобів захисту ІТС (рис. 2.5).

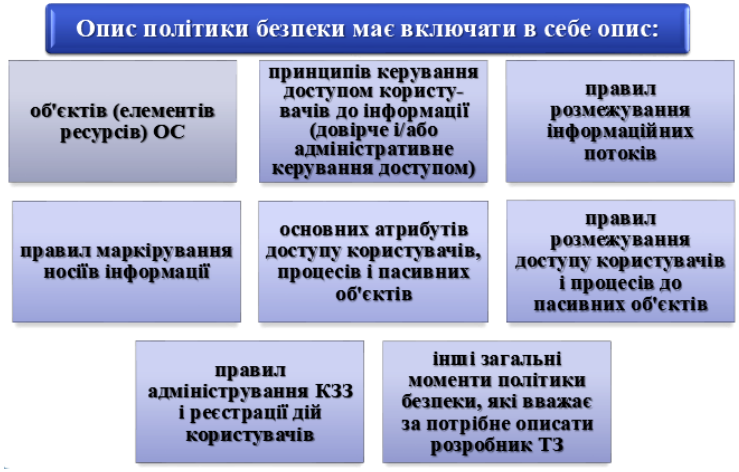

Рис. 2.5 Моменти, що відображаються в опису політики безпеки

Вимоги до послуг безпеки мають бути викладені і згруповані в тому порядку і стилі, в якому вони подані в Критеріях (**НД ТЗІ 2.5-004**).

В розділі мають бути викладені вимоги до реалізації послуг забезпечення конфіденційності, цілісності, доступності та спостереженості.

Для кожної включеної до розділу послуги відповідно до Критеріїв має бути визначений рівень послуги, який передбачається реалізувати.

Має бути описана політика даної послуги: визначення об'єктів, до яких застосовується дана послуга, і правил (в тому числі, що застосовуються за умовчанням), відповідно до яких повинні функціонувати механізми, що реалізують послугу. Відповідно до особливостей розроблюваної ІТС мають бути конкретизовані всі вимоги, що викладені в Критеріях для відповідного рівня кожної послуги.

У разі, якщо передбачається реалізувати послуги безпеки, які не зазначені в Критеріях, їх також необхідно описати.

Вимоги до гарантій мають бути викладені і згруповані в тому порядку і стилі, як вони подані в Критеріях. Це передбачає включення вимог до архітек-

тури КЗЗ, середовища розробки (організації процесу розробки і системи керування конфігурацією), гарантій проектування (етапності розробки і проектної документації), середовища функціонування, експлуатаційної документації, випробувань комплексу засобів захисту. Всі вимоги повинні відповідати належному рівню гарантій.

Вимоги до КСЗІ в ІТС в частині захисту від витоку інформації технічними каналами мають бути:

- сформульовані до усіх об'єктів (компонентів ІТС), що захищаються,
- визначені засоби захисту і засоби їх використання (наприклад, реалізація вимог до захищеності повинна досягатись без застосування екранування приміщень, активні засоби мають застосовуватись тільки для захисту інформації головного сервера ІТС і т.ін.).

Наводиться перелік нормативних і методичних документів, відповідно до яких повинні проводитись роботи щодо захисту інформації від витоку технічними каналами.

Вказуються вимоги до *розмірів зони безпеки інформації*, необхідні величини *показників захищеності*, що враховують реальну завадову обстановку на об'єкті електронної обчислювальної техніки. В якості показників виступають:

1) відношення величин електричної і магнітної складових напруженості поля побічних електромагнітних випромінювань до рівня завад на об'єкті ЕОТ;

2) відношення величини напруженості інформативного сигналу в провідних комунікаціях на межі зони безпеки інформації до рівня завад на об'єкті ЕОТ;

3) величина нерівномірності струму, який споживається по мережі електроживлення;

4) коефіцієнт екранування засобів обчислювальної техніки, в тому числі від впливу зовнішніх електромагнітних випромінювань.

Гранично допустимі значення основних показників є нормованими величинами і визначаються за відповідними методиками.

Відношення розрахованих (виміряних) значень основних показників до

пу.

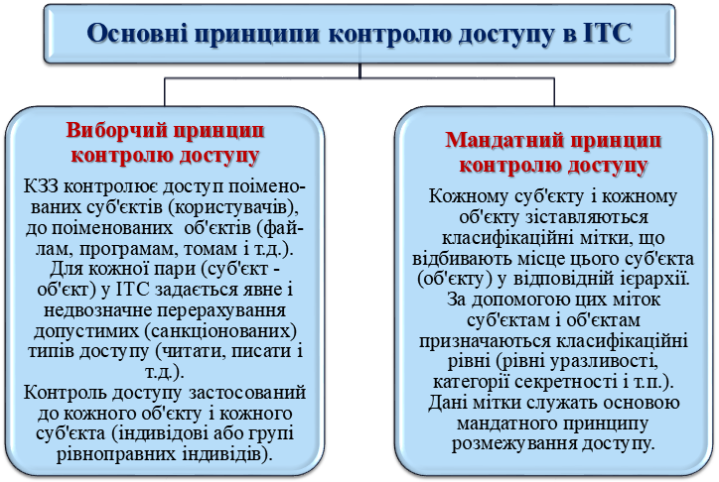

Рис. 2.42 Принципи контролю доступу в ІТС

Функції системи розмежування доступу:

- реалізація ПРД суб'єктів та їх процесів до даних;
- реалізація ПРД суб'єктів та їх процесів до облаштувань створення твердих копій;
- ізоляція програм процесу, що виконується в інтересах суб'єкта, від інших суб'єктів;
- управління потоками даних з метою запобігання запису даних на носії невідповідного грифа;
- реалізація правил обміну даними між суб'єктами для ІТС, побудованих на мережевих принципах.

Правила розмежування доступу передбачають наявність забезпечуючих засобів для СРД, які виконують наступні функції:

- ідентифікацію і автентифікацію суб'єктів і підтримку прив'язки суб'єкта до процесу, що виконується, для суб'єкта;
- реєстрацію дій суб'єкта і його процесу;
- надання можливостей виключення і включення нових суб'єктів і об'єктів доступу, а також зміна повноважень суб'єктів;

ставних пристроїв аудіо- і відеорозвідки, а також забезпечується захищеність ліній зв'язку від прослуховування.

Охорона об'єкту ІТС забезпечує розмежування безпосереднього доступу людей на контрольовану територію, у будівлі і приміщення:

- підрозділ охорони може знаходитися на об'єкті, а може охороняти декілька об'єктів. У останньому випадку на об'єкті знаходяться тільки технічні засоби охорони і сигналізації;
- відповідно до прийнятої політики безпеки керівництво спільне з СЗІ визначають структуру системи охорони;
- кількісний склад і режим роботи підрозділу охорони визначається важливістю і конфіденційністю інформації ІТС, а також використовуваними технічними засобами охорони і сигналізації.

Права доступу – сукупність правил, що регламентують порядок і умови доступу суб'єкта до об'єктів ІТС (інформації, її носіям, процесам та іншим ресурсам), встановлених правовими документами або власником інформації.

Права доступу *визначають набір дій* (наприклад, читання, запис, виконання), дозволених для виконання суб'єктам (наприклад, користувачам системи) над об'єктами даних. Для цього потрібна **система розмежування доступу** (апаратно-програмний комплекс засобів захисту інформації) суб'єктів до об'єктів, яка розглядається в якості головного засобу захисту від НСД до інформації в ІТС.

Основні **принципи контролю доступу в ІТС** (рис. 2.42):

1) *виборчий принцип контролю доступу* – КЗЗ контролює доступ поіменованих суб'єктів (користувачів), до поіменованих об'єктів (файлам, програмам, томам і т.д.);

2) *мандатний принцип контролю доступу* – кожному суб'єкту і кожному об'єкту зіставляються класифікаційні мітки, що відбивають місце цього суб'єкта (об'єкта) у відповідній ієрархії. За допомогою цих міток суб'єктам і об'єктам призначаються класифікаційні рівні (рівні уразливості, категорії секретності і т.п.). Дані мітки служать основою мандатного принципу розмежування досту-

гранично допустимих (нормованих) значень визначають необхідні умови захисту інформації.

Мають бути вказані вимоги щодо застосування способів, методів і засобів досягнення необхідних показників захищеності. Рекомендується застосування таких способів, методів і засобів:

а) *системо- і схемотехнічних методів*:

- обмеження використання інтерфейсів з передачею сигналів у вигляді послідовного коду і в режимі багатократних повторень;
- використання мультиплексних режимів обробки інформації, а також ЗОТ і системного забезпечення, що базуються на багаторозрядних платформах, інтерфейсів з передачею сигналів у вигляді багаторозрядного паралельного коду;
- використання раціональних способів монтажу, за яких забезпечується мінімальна довжина електричних зв'язків і комунікацій;
- використання ЗОТ і технічних засобів, до складу яких входять стійкі до самозбудження схеми, розв'язувальні і фільтрувальні елементи, комплектуючі з низькими рівнями електромагнітних випромінювань;
- використання мережевих фільтрів для блокування витоку ІзОД мережами електроживлення, а також лінійних (високочастотних) фільтрів для блокування витоку ІзОД лініями зв'язку;
- використання ЗОТ і технічних засобів у захисному виконанні;

б) *засобів просторового і лінійного «зашумлення»*;

в) *засобів локального або загального екранування*;

г) *засобів оптимального розміщення ЗОТ і технічних засобів* з метою мінімізації зони, в межах якої граничне відношення сигнал/шум не перевищує встановлених норм.

Мають бути вказані вимоги до проведення спецдосліджень ЗОТ і технічних засобів, мета яких – пряме вимірювання показників електромагнітних випромінювань.

Мають бути вказані вимоги до проведення спецперевірки ЗОТ, мета якої –

виявлення та вилучення (блокування) спеціальних електронних (закладних) пристроїв.

5. Вимоги до складу проектної та експлуатаційної документації. Наводиться перелік проектної та експлуатаційної документації, що розробляється в процесі створення КСЗІ в ІТС.

Склад обов'язкової проектної і експлуатаційної документації визначаються вимогами нормативних документів, відповідно до яких проводиться розробка (зокрема, вимогами Критеріїв для відповідного рівня гарантій).

Повний перелік необхідної документації визначається розробником КСЗІ і погоджується із замовником.

6. Етапи виконання робіт. Процес створення КСЗІ доцільно поділяти на етапи, зміст яких детально описаний в п. 2.1.2 цього посібника. Кожний з етапів допускається поділяти на окремі підетапи.

Всі основні роботи кожного етапу відображаються в календарному плані, де зазначаються терміни проведення робіт за окремими етапами, види звітності і форми подання результатів замовнику.

7. Порядок внесення змін і доповнень до ТЗ на створення КСЗІ в ІТС. Зміни затвердженого ТЗ на створення КСЗІ в ІТС, необхідність внесення яких виявлена в процесі виконання робіт, оформляються окремим доповненням, яке погоджується і затверджується в тому ж порядку і на тому ж рівні, що і основний документ.

Доповнення до ТЗ на створення КСЗІ в ІТС складається з вступної частини і змінюваних підрозділів. У вступній частині зазначається причина випуску доповнення. В змінюваних підрозділах наводяться номери та зміст змінюваних, нових або пунктів, що скасовуються.

8. Порядок проведення випробувань КСЗІ. Для кожного виду випробувань (попередніх, державних, сертифікаційних та ін.) комплексної системи (підсистеми, компонента) захисту виконавець розробляє **«Програму і методику випробувань комплексної системи (підсистеми, компонента) захисту інформації в ІТС»**, яка затверджується в установленому порядку. Терміни подання

Організація доступу до ресурсів припускає:

- розмежування прав користувачів і обслуговуючого персоналу по доступу до ресурсів КС відповідно до функціональних обов'язків посадовців;
- організацію роботи з конфіденційними інформаційними ресурсами на об'єкті;
- захист від технічних засобів розвідки;
- охорону об'єкту;
- експлуатацію системи розмежування доступу.

Права посадовців по доступу до ресурсів ІТС встановлюються керівництвом організації, в інтересах якої використовується ІТС:

- кожному посадовцю визначаються для використання технічні ресурси (робоча станція, сервер, апаратура передачі даних і т.д.), дозволені режими і час роботи;
- керівництвом встановлюється рівень компетенції посадовців по маніпулюванню інформацією;
- особа, відповідальна за організацію безпеки інформації в ІТС, на підставі рішення керівника про розмежування доступу посадовців забезпечує введення відповідних повноважень доступу в систему розмежування доступу.

Керівництво спільне з СЗІ визначає порядок роботи з конфіденційними інформаційними ресурсами, не використовуваними безпосередньо в ІТС, хоч би і тимчасово. До таких ресурсів відносяться конфіденційна друкарська продукція, у тому числі і отримана за допомогою ІТС, а також машинні носії інформації. Обліком, зберіганням і видачею таких ресурсів займаються посадовці з СЗІ, або інші посадовці за сумісництвом.

СЗІ виконується увесь комплекс заходів *протидії технічним засобам розвідки*:

- контролюється застосування пасивних засобів захисту від ПЕМВН;
- активні засоби захисту від загроз цього класу використовуються відповідно до графіку роботи об'єкту;
- періодично здійснюються перевірки приміщень на відсутність в них за-

можливості) представлення КСЗІ на державну експертизу.

8. **Державна експертиза КСЗІ.** Державна експертиза проводиться згідно з **Положенням про державну експертизу в сфері ТЗІ** з метою визначення відповідності КСЗІ технічному завданню, вимогам нормативних документів із захисту інформації та визначення можливості введення КСЗІ в складі ІТС в експлуатацію. Виявлені під час державної експертизи недоліки усуваються до її завершення. Приймальні випробування ІТС проводяться при функціонуючій в її складі КСЗІ.

9.2 Застосування КСЗІ за призначенням

Процес експлуатації КСЗІ можна розділити на *застосування системи по прямому призначенню*, що припускає виконання усього комплексу заходів, безпосередньо пов'язаних із захистом інформації в ІТС, і *технічну експлуатацію* (рис. 2.41).

Рис. 2.41 Види експлуатації КСЗІ

Застосування за призначенням передбачає організацію доступу до ресурсів ІТС і забезпечення їх цілісності.

Організація доступу до ресурсів – це комплекс заходів, який виконується в процесі експлуатації ІТС для запобігання несанкціонованій дії на технічні і програмні засоби, а також на інформацію.

проекту Програми, його розгляду і затвердження погоджуються з замовником.

Для проведення випробувань замовником призначається комісія, склад якої погоджується з розробником КСЗІ.

Випробування проводяться з використанням умовної інформації (що не є ІзОД).

Наводиться необхідне для проведення випробувань забезпечення (необхідна нормативна, методична та інша документація, програмні та технічні засоби, метрологічне, спеціальне та інше обладнання, створення інших умов для проведення випробувань), сторона, що його надає, порядок усунення зауважень і т.ін.

Наводиться перелік документів, якими завершуються випробування (етапи випробувань):

- акт приймання;
- сертифікат (атестат, експертний висновок) відповідності встановленим критеріям;
- наказ про введення в експлуатацію тощо.

Висновки

1. Технічне завдання на КСЗІ є засадничим організаційно-технічним документом для виконання робіт щодо забезпечення захисту інформації в системі. Воно створюється у разі необхідності розробки або модернізації КСЗІ існуючої ІТС. В разі розробки КСЗІ в процесі проектування ІТС допускається оформлення вимог з захисту інформації в ІТС у вигляді окремого (часткового) ТЗ, доповнення до загального ТЗ на ІТС або розділу загального ТЗ на ІТС.

2. ТЗ на КСЗІ повинно розроблятись з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину систему всіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу ІТС.

3. ТЗ на КСЗІ є одним із обов'язкових засадничих документів під час проведення експертизи ІТС на відповідність вимогам захищеності інформації.

4. ТЗ на КСЗІ в загальному випадку повинно містити такі основні підроз-

діли: 1) загальні відомості; 2) мета і призначення КСЗІ; 3) загальна характеристика ІТС та умов її функціонування; 4) вимоги до КСЗІ; 5) вимоги до складу проектної та експлуатаційної документації; 6) етапи виконання робіт; 7) порядок внесення змін і доповнень до ТЗ; 8) порядок проведення випробувань КСЗІ.

Контрольні питання

1. Що є ТЗ на КСЗІ? У яких випадках воно розробляється?
2. Що викладається в ТЗ на КСЗІ?
3. Що є вихідними даними для розробки ТЗ на КСЗІ?
4. Які основні роботи виконуються на етапі формування ТЗ на КСЗІ?
5. Які розділи включаються в зміст ТЗ на КСЗІ?
6. Що визначається в розділі «Загальні відомості»?
7. Які моменти визначаються в розділі «Загальна характеристика ІТС і умов її функціонування»?
8. Яка інформація включається в розділ «Вимоги до КСЗІ»?
9. Що включається в опис політики безпеки?
11. Які вимоги рекомендується включати в ТЗ відносно вживаних способів, методів і засобів?
12. Що включається в розділ «Вимоги до складу проектної та експлуатаційної документації»?
13. Що включається в розділ «Етапи виконання робіт»?
14. Що включається в розділ «Порядок проведення випробувань КСЗІ»?

ми Керівного документу стандартизації **РД 50-34.698-90 Автоматизированные системы. Требования к содержанию документов** (готує програму и методики розробник КСЗІ, а узгоджує замовник ІТС).

Попередні випробування організовує замовник ІТС, а проводить розробник КСЗІ спільно із замовником. Випробування проводить комісія. Головою комісії призначається представник замовника.

Результати попередніх випробувань оформлюються **Протоколом випробувань**, де міститься

- висновок щодо можливості прийняття КСЗІ у дослідну експлуатацію;
- перелік виявлених недоліків, необхідних заходів з їх усунення;
- рекомендовані терміни виконання цих робіт.

Після усунення недоліків та коригування проектної, робочої, експлуатаційної документації КСЗІ оформлюється **акт про приймання КСЗІ у дослідну експлуатацію**.

7. **Дослідна експлуатація.** На цій стадії

1) відпрацьовуються технології:
   - оброблення інформації;
   - обігу машинних носіїв інформації;
   - керування засобами захисту;
   - розмежування доступу користувачів до ресурсів ІТС;
   - автоматизованого контролю за діями користувачів;

2) співробітники СЗІ та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;

3) доопрацюється програмне забезпечення, додаткове налагоджується та конфігурується КЗЗ;

4) коригується робоча та експлуатаційна документація.

За результатами робіт за довільною формою складається **акт про завершення дослідної експлуатації**, який містить висновок щодо можливості (не-

- вносити у визначеному порядку пропозиції щодо покращення техніко-економічних показників робіть.

5. **Пуско-налагоджувальні роботи.** Мета пуско-налагоджувальних робіт:

- монтаж обладнання і атестація комплексу ТЗІ від витоку технічними каналами;
- встановлення і налагодження КЗЗ;
- перевірка працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії.

Монтаж ОТЗ ІТС, кабельного обладнання, мереж живлення та заземлення здійснюється згідно з конструкторською документацією робочого проекту.

Згідно з документацією робочого проекту здійснюється інсталяція ПЗ, ініціалізація та перевірка працездатності КЗЗ.

Під час інсталяції мають бути задіяні всі механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, контролю за діями користувачів, а також контролю цілісності ПЗ та бази даних захисту КЗЗ.

За результатами робіт складається **акт**, де зазначаються:

- категорії приміщень, де розташоване обладнання ІТС;
- межі контрольованих зон для приміщень;
- перелік ОТЗ, ДТЗ і комунікацій (із вказівкою найменування, типу, заводського номеру), що знаходяться у цих приміщеннях;
- оцінка відповідності проведення монтажних робіт вимогам експлуатаційних документів на засоби та нормативних документів;
- пропозиції щодо застосування додаткових заходів захисту, впровадження яких є необхідним у разі неможливості під час виконання монтажних робіт дотримання окремих вимог із розміщення ОТЗ.

Акт затверджується керівником організації-власника ІТС.

6. **Попередні випробування.** Мета:

- перевірка працездатності КСЗІ та відповідності її вимогам ТЗ;
- визначення можливості прийняття КСЗІ у дослідну експлуатацію.

Розробка програми й методики випробувань здійснюється згідно з вимога-

3 Оцінка захищеності інформації в ІТС від несанкціонованого доступу

Захищені ІТС – це системи, на які покладаються функції підтримки конфіденційності, цілісності довіреної інформації, а також її доступності при авторизованому доступі.

При побудові КСЗІ виникає питання: наскільки захищена (чи не захищена) ІТС на даний момент і наскільки вимагається підвищити рівень захисту, щоб ризик виникнення проблеми, пов'язаної з інформаційною безпекою, і витрати на її усунення були в межах допустимих значень. Для відповіді на подібні питання використовуються *офіційні критерії оцінки захищеності ІТС*, визначувані **НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу**.

3.1 Побудова і структура критеріїв захищеності інформації

Нормативний документ **НД ТЗІ 2.5-004-99** встановлює критерії оцінки захищеності інформації, оброблюваної в ІТС, від НСД.

Критерій – це ознака, підстава, правило прийняття рішення щодо оцінки чого-небудь на відповідність висунутим вимогам.

Критерії є методологічною базою для визначення вимог з захисту інформації в ІТС від НСД у процесі:

- створення захищених ІТС і засобів захисту від НСД;
- оцінки захищеності інформації в ІТС та їх придатності для обробки інформації, що вимагає захисту.

Критерії надають:

- *порівняльну шкалу* для оцінки надійності механізмів захисту інформації від НСД, реалізованих в ІТС;
- *базу* (*орієнтири*) *для розробки ІТС*, в яких мають бути реалізовані функції захисту інформації;

Спектр ІТС, в яких можуть використовуватися офіційні критерії оцінки захищеності інформації, наведений на рис. 2.6.

Рис. 2.6 ІТС, в яких використовуються критерії оцінки захищеності інформації

В процесі оцінки спроможності ІТС забезпечувати захист оброблюваної інформації від НСД розглядаються вимоги двох видів:

1) *вимоги до функцій захисту* (*послуг безпеки*);

2) *вимоги до гарантій*.

Виконання вимог першого виду забезпечується розробником в процесі проектування (розробки) і перевіряється експертною комісією в процесі оцінки. Виконання вимог другого виду забезпечується як діями розробника, проте вже на всіх стадіях життєвого циклу ІТС, так і спільними діями розробника і експертної комісії в процесі оцінки.

З точки зору захисту інформації ІТС розглядається як *набір функціональних послуг*, де кожна послуга – це 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 (1) і зростають до значення *n*, де *n* – унікальне для кожного виду послуг.

Функціональні критерії дозволяють оцінити наявність послуг безпеки в ІТС і розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів:

1. **Конфіденційність.** Загрози, що відносяться до *несанкціонованого ознайомлення з інформацією*, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то від-

- готувати і передавати у визначеному порядку проектній організації завдання на проектування заходів ТЗІ;
- видавати проектній організації, при необхідності, додаткові дані для прийняття рішень з ТЗІ;
- організовувати перевірку якості робіт з ТЗІ;
- висувати, при необхідності, додаткові вимоги ТЗІ та вносити відповідні зміни (доповнення) до завдання на проектування заходів ТЗІ;
- брати участь у розробленні заходів ТЗІ;
- контролювати хід виконання робіт з ТЗІ;
- зупиняти виконання робіт, якщо є відхилення від проектних рішень з ТЗІ.

Проектна організація повинна:

- організовувати й виконувати проектні роботи згідно із завданням та цим ДБН;
- видавати субпідрядним організаціям завдання на проведення інженерно- вишукувальних робіт з урахуванням вимог ТЗІ;
- коректувати проектно-кошторисну документацію за результатами експертизи;
- організовувати та здійснювати авторський нагляд за реалізацією проектних рішень з ТЗІ в процесі виконання будівельно-монтажних робіт;
- зупиняти проведення будівельно-монтажних робіт, якщо вони мають відхилення від проектних рішень з ТЗІ;
- подавати замовнику пропозиції про внесення до завдання змін (доповнень), якщо в ході проектування з'явилась можливість підвищити ефективність проектних рішень з ТЗІ або значно знизити кошторисну вартість;
- дотримуватись відповідних режимних вимог під час вишуку, проектування, авторського нагляду за будівництвом об'єкта.

Будівельно-монтажна організація повинна:

- своєчасно та якісно виконувати роботи щодо реалізації передбачених проектною документацією заходів ТЗІ;

- генерального плану;
- будівель і споруд;
- систем інженерного забезпечення виробництва та технічних засобів.

До складу проектної документації на здійснення заходів з ТЗІ повинні входити робочі креслення, кошторис на документація та специфікація устаткування і матеріалів.

Обгрунтування рішень з ТЗІ, що передбачені у розділах проектної документації, викладаються в окремому розділі **«Заходи ТЗІ»** загальної пояснювальної записки. У решті розділів проектної документації, при необхідності, слід робити посилання на розділ **«Заходи ТЗІ»**.

Проектна документація з ТЗІ підлягає експертизі на загальних підставах згідно з визначеним порядком проведення державної експертизи інвестиційних проектів і програм та допуску посадових осіб до матеріалів з ТЗІ.

Під час експертизи проектної документації на будівництво перевіряються:

- відповідність технічних рішень затвердженому завданню на проектування заходів ТЗІ;
- дотримання вимог нормативних документів системи ТЗІ;
- відповідність рівня виконаних розробок сучасному стану науки і техніки в галузі ТЗІ.

У висновку експертизи повинні бути зазначені результати виконання вимог ТЗІ в проектній документації на будівництво. Висновки експертизи заносяться до окремого розділу експертної документації. Експертизу проектної документації на будівництво особливо важливих об’єктів необхідно проводити у встановленному порядку за участю спеціалістів з питань ТЗІ. Висновки експертизи повинні бути подані в орган, що погодив завдання на проектування заходів ТЗІ.

Основні функції замовника, проектної і будівельно-монтажної організацій:

Замовник повинен:

- приймати рішення щодо необхідності ТЗІ;

повідні послуги треба шукати в розділі «Критерії конфіденційності»;

2. **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»;

3. **Доступність.** Загрози, що відносяться до *порушення можливості використання ІТС 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»;

4. **Спостереженість.** *Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою* становлять предмет послуг спостереженості та 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 спостереженості».

Другу групу складають **критерії гарантій** дозволяють оцінити коректність реалізації послуг і включають вимоги до:

- архітектури комплексу засобів захисту;
- середовища розробки;
- послідовності розробки;
- випробування комплексу засобів захисту;
- середовища функціонування;
- експлуатаційної документації.

Вводиться сім ієрархічних рівнів гарантій (**Г-1**, ..., **Г-7**). Ієрархія рівнів гарантій відбиває поступово наростаючу міру певності в тому, що реалізовані в ІТС послуги захисту 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 ІТС.

Критерії захищеності інформації в ІТС від НСД, прийняті в Україні, приведені на рис. 2.7.

Всі послуги є більш-менш незалежними. Якщо ж така залежність виникає, тобто реалізація якої-небудь послуги неможлива без реалізації іншої, то цей факт відбивається як необхідні умови для даної послуги (або її рівня).

За винятком послуги **Аналіз прихованих каналів** залежність між функціональними послугами і гарантіями відсутня.

Рівень послуги **Цілісність комплексу засобів захисту НЦ-1** є необхідною умовою абсолютно для всіх рівнів всіх інших послуг.

Рис. 2.7 Система офіційних критеріїв захищеності інформації в ІТС від НСД

Експертна комісія, яка проводить оцінку ІТС, визначає, які послуги і на якому рівні реалізовані в даній ІТС, і як дотримані вимоги гарантій.

Результатом оцінки є **рейтинг** – упорядкований ряд (перелічення) буквено-числових комбінацій, що позначають рівні реалізованих послуг, в поєднанні з рівнем гарантій. Комбінації упорядковуються в порядку опису послуг в критеріях.

урахуванням вимог ТЗІ повинна бути визначена після виконання наступних підготовчих робіт:

- визначення переліку приміщень, в яких циркулює інформація, що підлягає технічному захисту;
- обгрунтування необхідності розроблення заходів захисту ІзОД з урахуванням шкоди від її витоку або порушення цілісності;
- уточнення меж контролюємої території на основі аналізу загроз безпеці інформації;
- визначення головних задач технічного захисту ІзОД;
- визначення шляхів і засобів реалізації заходів ТЗІ з урахуванням технічної та економічної доцільності.

Підсумки підготовчих робіт і вихідні дані є підставою для розроблення завдання на проектування заходів ТЗІ.

Завдання на проектування заходів ТЗІ включає:

- мету, задачі, вимоги ТЗІ;
- вихідні дані для проектування комплексного ТЗІ;
- вимоги до контролю за реалізацією передбачених заходів ТЗІ.

Завдання на проектування заходів ТЗІ розробляється замовником і узгоджується з проектною організацією і, при необхідності, із організацією, якій підпорядкований замовник.

Розроблення проектної документації включає:

1) розроблення *документації передпроектних досліджень*:
   - виявлення характерних особливостей об’єкта, які впливають на вибір проектних рішень з ТЗІ;
   - оцінка умов реалізації заходів ТЗІ;
   - орієнтовний вибір основних проектних рішень з ТЗІ та їх економічне обгрунтування;
   - обгрунтування вибору майданчика для будівництва;
2) розроблення *проектної документації для будівництва*:
   - технології виробництва;

ладнання існуючих або при будівництві нових спеціалізованих споруд (приміщень), призначених для розміщення технічних засобів ІТС та персоналу, сховищ матеріальних носіїв інформації.

Будівельні роботи здійснюються силами організації-власника ІТС або будівельно-монтажними організаціями згідно з проектною документацією на будівництво, яка розробляється проектною організацією у відповідності до вимог нормативних документів **ДБН А.2.2-2**, **ДБН 2.2-3**.

Після завершення будівельних робіт створюється комісія з прийняття робіт. За результатами роботи комісії складається акт приймання робіт з оцінкою їх відповідності вимогам ТЗІ, який затверджується керівником організації-замовника будівництва.

Державі будівельні норми України **ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва** встановлюють вимоги до забезпечення технічного захисту інформації під час організації проектування будівництва (нового будівництва, розширення, реконструкції та капітального ремонту) підприємств, будівель та споруд;

Технічний захист ІзОД передбачає *застосування систем інженерно- технічних споруд разом із засобами забезпечення ТЗІ*.

Вимоги ТЗІ повинні бути викладені в завданні на проектування заходів ТЗІ і враховуватися в процесі проектування об’єкта, зокрема під час розробки:

- ситуаційного плану розміщення об’єкта;
- технології виробництва;
- принципових схем виробничих технологічних процесів;
- схеми генерального плану виробничого комплексу;
- архітектурно-будівельних рішень щодо об’єкта;
- принципових рішень з організації систем зв’язку, сигналізації, управління, автоматизованих та інших систем;
- основних рішень з організації будівництва.

Необхідність розробки проектної документації для будівництва об’єкта з

Для того, щоб до рейтингу ІТС міг бути включений певний рівень послуги чи гарантій, повинні бути виконані всі вимоги, перелічені в критеріях для даного рівня послуги або гарантій.

У табл. 2.1 перераховані позначення усіх послуг забезпечення захисту інформації в ІТС, передбачені **НД ТЗІ 2.5-004-99.**

Таблиця 2.1 Позначення послуг захисту

Конфіденційності:	***Цілісності:***
КД – довірча конфіденційність; КА – адміністративна конфіденційність; КО – повторне використання об’єктів; КК – аналіз прихованих каналів; КВ – конфіденційність при обміні.	ЦД – довірча цілісність; ЦА – адміністративна цілісність; ЦО – відкат; ЦВ – цілісність при обміні.
Доступності:	***Спостереженості:***
ДР – використання ресурсів; ДС – стійкість до відмов; ДЗ – гаряча заміна; ДВ – відновлення після збоїв.	НР – реєстрація; НИ – ідентифікація и автентифікація; НК – достовірний канал; НО – розподіл обов’язків; НЦ – цілісність КЗЗ; НТ – самотестування; НВ – автентифікація при обміні; НА – автентифікація відправника; НП – автентифікація одержувача.

3.2 Критерії конфіденційності, цілісності, доступності, спостереженості

Критерії конфіденційності

Для того, щоб ІТС могла бути оцінена на предмет відповідності критеріям конфіденційності, КЗЗ оцінюваної ІТС повинен надавати послуги з захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації).

Конфіденційність забезпечується реалізацією послуг, наведених на рис. 2.8.

В будь-якій ІТС інформація може переміщуватись в одному з двох напрямів: від користувача до об'єкта або від об'єкта до користувача. Шляхи переміщування 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.

Рис. 2.8 Критерії конфіденційності

Принципи, що лежать в основі реалізації послуг, визначаються *політикою конфіденційності*.

Довірча конфіденційність – ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів.

Рівні послуги ранжируються на підставі повноти захисту і вибірковості керування:

- **КД-1. Мінімальна довірча конфіденційність** – 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.
- **КД-2. Базова довірча конфіденційність** – атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача.
- **КД-3. Повна довірча конфіденційність** – користувач, домену якого належить об'єкт, може вказати права доступу для кожного конкретного користувача і групи користувачів.
- **КД-4. Абсолютна довірча конфіденційність** – забезпечує повне керу-

- документи, що регламентують доступ до ІТС і т.д.

Створення СЗІ та розробка Плану захисту здійснюється згідно з **НД ТЗІ 1.4-001- 2000 Типове положення про службу захисту інформації в автоматизованій системі**.

2. **Навчання користувачів** (рис. 2.39).

Рис. 2.39 Контингент тих, хто навчається, і чому навчають

3. **Комплектування КСЗІ** (рис. 2.40).

Рис. 2.40 Роботи при комплектуванні КСЗІ

4. **Будівельно-монтажні роботи.** Ці роботи виконуються під час переоб-

9 Введення КСЗІ в дію

Функціонування КСЗІ залежить не лише від характеристик створеної системи, але і від ефективності її використання на етапі експлуатації ІТС.

Основними завданнями етапу експлуатації є *максимальне використання можливостей КСЗІ*, закладених в систему при побудові, і вдосконалення її захисних функцій відповідно до умов, що змінюються.

9.1 Введення КСЗІ в дію

Роботи, що виконуються при введенні КСЗІ в дію приведені на рис. 2.38.

Рис. 2.38 Роботи, що виконуються при введенні КСЗІ

1. **Підготовка КСЗІ до введення в дію** включає:

- підготовку організаційної структури;
- розробку розпорядчих документів;
- створення служби захисту інформації;
- завершення розробки і затвердження документів, що входять до Плану захисту інформації в ІТС.

До організаційно-розпорядливих документів відносяться:

- організаційна структура;
- штатний розклад;
- положення про відділи і посадові інструкції співробітників, пов'язаних з експлуатацією ІТС і КСЗІ;

вання 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. Для такої системи можна побудувати повну матрицю доступу користувачів, процесів і пар користувач/процес до захищених об'єктів і процесів.

Таблиця 2.1 Критерії довірчої конфіденційності

<table>
<tr><th>КД-1. Мінімальна довірча конфіденційність</th><th>КД-2. Базова довірча конфіденційність</th><th>КД-3. Повна довірча конфіденційність</th><th>КД-4. Абсолютна довірча конфіденційність</th></tr>
<tr><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати мно-жину об'єктів ІТС, до яких вона відноситься</td><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ІТС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>процесу і захищеного об'єкта</td><td colspan="2">користувача і захищеного об'єкта</td><td>користувача, процесу і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта</td></tr>
<tr><td colspan="4">КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити</td></tr>
<tr><td>конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право ініціювати процес</td><td colspan="2">конкретних користувачів (і групи користувачів), які мають, а також тих, що не мають права ініціювати процес</td></tr>
<tr><td colspan="4">Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НИ-1</td><td colspan="2">НЕОБХІДНІ УМОВИ: КО-1, НИ-1</td></tr>
</table>

Система, яка реалізує довірче керування доступом, дозволяє звичайному користувачеві модифікувати, в т.ч. створювати нові потоки інформації.

Під **об'єктами, що належать домену користувача**, маються на увазі об'єкти, власником яких є користувач (тобто те, що створені користувачем).

Для відображення функціональності ІТС 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 ІТС, 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.

Адміністративна конфіденційність – ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів.

Рівні 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:

- **КА-1. Мінімальна адміністративна конфіденційність**;
- **КА-2. Базова адміністративна конфіденційність**;
- **КА-3. Повна адміністративна конфіденційність**;
- **КА-4. Абсолютна адміністративна конфіденційність**.

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

4. СЗІ у своїй діяльності керується Конституцією України, законами України, нормативно-правовими актами Президента України і Кабінету Міністрів України, іншими нормативно-правовими актами з питань захисту інформації, державними і галузевими стандартами, розпорядчими та іншими документами організації. СЗІ здійснює діяльність відповідно до «Плану захисту інформації в автоматизованій системі», календарних, перспективних та інших планів робіт, затверджених керівником організації.

Контрольні питання

1. Що таке управління КСЗІ? У чому його сенс і мета?
2. У чому полягають особливості систем управління КСЗІ?
3. Які завдання вирішуються в процесі управління КСЗІ?
4. У чому полягають принципи управління КСЗІ?
5. Яка структура управління КСЗІ? Що виконують її основні елементи?
6. Як класифікують завдання управління КСЗІ?
7. Поясніть модель PDCA.
8. Які розділи включає Положення про СЗІ в ІТС?
9. Що таке СЗІ в ІТС? Які правові основи її створення і діяльності?
10. Які завдання і функції СЗІ?
11. У чому полягають повноваження і відповідальність СЗІ?
12. Який штатний склад і структура СЗІ?
13. Як організовується робота СЗІ?
14. Які основні види планів робіт створюються в СЗІ?
15. Яке документаційне забезпечення СЗІ?

- інструкції користувача в ІТС, адміністратора безпеки, системного адміністратора;
- інструкцію з тестування системи;
- інструкцію з виконання регламентних та ремонтних робіт;
- інструкцію про порядок введення в експлуатацію КСЗІ;
- інструкцію про порядок модернізації КСЗІ;
- паспорт-формуляр на ІТС.

Висновки

1. Суть управління КСЗІ – цілеспрямована діяльність керівництва організації, посадовців і служби захисту інформації, спрямована на досягнення цілей захисту інформації. Сенс і мета управління в КСЗІ – такі зміни організаційної структури, сил і засобів захисту інформації, їх стану, методів і способів застосування, які забезпечують максимальну ефективність їх застосування для досягнення цілей захисту інформації.

2. Задача управління – основний елемент процесу управління - технологічний модуль перетворення інформації, що служить для досягнення за заданий час конкретного результату. Функція управління – стійка сукупність задач реалізації процесу управління (його частини) для досягнення приватних цілей управління, заснована на розподілі управлінської праці в органах управління. Основні управлінські функції: планування, оперативне управління, контроль, облік.

3. Служба захисту інформації — це підрозділ організації, який забезпечує захист інформації шляхом управління комплексною системою захисту інформації. Метою створення СЗІ є організаційне забезпечення завдань керування КСЗІ в ІТС та здійснення контролю за її функціонуванням. На СЗІ покладається виконання робіт з визначення вимог з захисту інформації в ІТС, проектування, розроблення і модернізації КСЗІ, а також з експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації в ІТС.

здійснює запит на доступ до інформації, авторизованим користувачем.

Згідно з політикою адміністративної конфіденційності об'єкту присвоюються атрибути доступу, що визначають домен, якому повинні належати ті користувачі або процеси, які намагаються одержати інформацію.

Таблиця 2.2 Критерії адміністративної конфіденційності

<table>
<tr><th>КА-1. Мінімальна адміністративна конфіденційність</th><th>КА-2. Базова адміністративна конфіденційність</th><th>КА-3. Повна адміністративна конфіденційність</th><th>КА-4. Абсолютна адміністративна конфіденційність</th></tr>
<tr><td colspan="2">Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів ІТС, до яких вона відноситься</td><td colspan="2">Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ІТС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>процесу і захищеного об'єкта</td><td colspan="2">користувача і захищеного об'єкта</td><td>користувача, процесу і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження</td></tr>
<tr><td colspan="4">КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити</td></tr>
<tr><td>конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право ініціювати процес</td><td colspan="2">конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес</td></tr>
<tr><td colspan="4">Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НО-1, НИ-1</td><td colspan="2">НЕОБХІДНІ УМОВИ: КО-1, НО-1, НИ-1</td></tr>
</table>

Повторне використання об'єктів – ця послуга дозволяє забезпечити ко-

ректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу. Реалізація даної послуги дозволяє забезпечити захист від атак типу «збирання сміття».

Повторне використання об'єкта може бути реалізовано також шляхом шифрування інформації, що міститься в об'єктах, і використання керування криптографічними ключами замість знищення інформації.

Таблиця 2.3 Критерії повторного використання об’єктів

КО-1. Повторне використання об'єктів
Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ІТС. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.
НЕОБХІДНІ УМОВИ: **НЕМАЄ**

Аналіз прихованих каналів виконується з метою виявлення і усунення потоків інформації, які існують, але не контролюються іншими послугами.

Рівні послуги ранжируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів:

- **КК-1. Виявлення прихованих каналів**;
- **КК-2. Контроль прихованих каналів**;
- **КК-3. Перекриття прихованих каналів**.

Таблиця 2.4 Критерії аналізу прихованих каналів

КК-1. Виявлення прихованих каналів	**КК-2. Контроль прихованих каналів**	**КК-3. Перекриття прихованих каналів**
Повинен бути виконаний аналіз прихованих каналів		
Всі приховані канали, які існують в апаратному і програмному забезпеченні, а також в програмах ПЗП, повинні бути документовані. Має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, одержана на підставі теоретичної оцінки або вимірів. Для прихованих каналів, які можуть використовуватися спільно, повинна бути документована сукупна пропускна здатність		Всі (затверджена підмно-жина) знайдені під час аналізу приховані канали повинні бути усунені

Документаційне забезпечення СЗІ

1. Проектна документація на КСЗІ повинна включати:

- технічний проект на КСЗІ та ІТС;
- робочу документацію на КСЗІ;
- класифікацію інформації;
- класифікацію користувачів за рівнем повноважень та місцем їх розміщення;
- загальний опис КСЗІ;
- модель загроз безпеці інформації та модель потенційних порушників;
- опис політики безпеки інформації;
- план технічного захисту;
- опис технічних засобів захисту.

2. Експлуатаційна документація на КСЗІ повинна включати:

- накази про створення комісії з обстеження (категорювання) ІТС;
- акт категорювання ІТС;
- наказ про створення СЗІ, призначення адміністратора безпеки та інших адміністраторів;
- наказ про створення комісії з проведення попередніх випробувань КСЗІ;
- програму та методики випробувань;
- протокол попередніх випробувань КСЗІ;
- акт про передачу КСЗІ в дослідну експлуатацію;
- наказ про проведення дослідної експлуатації;
- журнал навчання користувачів;
- акт завершення дослідної експлуатації;
- політику безпеки інформації;
- положення про службу захисту інформації в ІТС;
- план захисту інформації в ІТС;
- інструкцію із забезпечення режиму безпеки при роботі в ІТС;
- інструкцію щодо порядку забезпечення антивірусного захисту інформації в ІТС;

Плани робіт складаються керівником СЗІ після обговорення на виробничій нараді СЗІ організаційно-технічних питань, що належать до її компетенції, і затверджуються керівником організації або керівником підрозділу, до складу якого входить СЗІ.

Реорганізація або ліквідація СЗІ здійснюється за рішенням загальних зборів акціонерів або керівництва організації. Реорганізаційна або ліквідаційна процедура здійснюється відповідною комісією, яка створюється за наказом (розпорядженням) керівника організації.

З метою забезпечення конфіденційності робіт, які виконуються співробітниками СЗІ, при прийомі на роботу (звільненні з роботи) вони дають *письмові зобов'язання щодо нерозголошення відомостей*, що становлять службову, комерційну або іншу таємницю, і які стали їм відомими в період роботи в організації.

Матеріально-технічну базу для забезпечення діяльності СЗІ складають належні їй на правах власності (оперативного управління, повного господарського відання) засоби захисту інформації, ПЗ, технічне та інженерне обладнання, засоби вимірювань і контролю, відповідна документація, а також інші засоби і обладнання, які необхідні для виконання СЗІ покладених на неї завдань.

Засоби захисту інформації та захищені засоби, що використовуються співробітниками СЗІ при виконанні своїх службових обов'язків, повинні мати, одержаний у встановленому порядку документ, що засвідчує їхню відповідність вимогам нормативних документів.

СЗІ фінансується за рахунок:

- коштів, що виділяються в організації на утримання органів управління;
- прибутку організації (ІТС) та інших коштів за рішенням керівництва організації або рішенням загальних зборів акціонерів;
- коштів, отриманих за виконання СЗІ договірних робіт та надання послуг;
- інших джерел фінансування, не заборонених законодавством.

—	КЗЗ повинен забезпечувати реєстрацію використання затвердженої підмножини знайдених прихованих каналів	
НЕОБХІДНІ УМОВИ: **КО-1, Г-3**	НЕОБХІДНІ УМОВИ: **КО-1, НР-1, Г-3**	НЕОБХІДНІ УМОВИ: **КО-1, Г-3**

Конфіденційність при обміні – ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Рівні послуги ранжируються на підставі повноти захисту і вибірковості керування:

- **КВ-1. Мінімальна конфіденційність при обміні**;
- **КК-2. Базова конфіденційність при обміні**;
- **КК-3. Повна конфіденційність при обміні**;
- **КВ-4. Абсолютна 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.

Найчастіше послуга реалізується з використанням криптографічних перетворень.

Рівні послуги ранжируються на підставі повноти захисту і вибірковості керування.

Таблиця 2.5 Критерії конфіденційності при обміні

КВ-1. Мінімальна конфіденційність при обміні	**КВ-2. Базова конфіденційність при обміні**	**КВ-3. Повна конфіденційність при обміні**	**КВ-4. Абсолютна конфіденційність при обміні**
Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься		Політика конфіденційності при обміні, що реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих інтерфейсних процесів	
Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захи-			

щеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності			
КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається			
—	Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження		
—	Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу		
	—	і приймальника об'єкта	
—	Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу		
	—	і джерела об'єкта	
—		Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника	
			Політика конфіденційності при обміні повинна включати опис інформації , яку можливо отримати шляхом сумісного аналізу ряду одержаних об'єктів. Повинен бути виконаний аналіз прихованих каналів обміну. Всі знайдені приховані канали обміну і максимальна пропускна здатність кожного із них мають бути документовані. Повинна бути забез-печена реєстрація використання затвердженої підмножини знайдених прихованих каналів, їх часткове перекрит-тя або усунення
НЕОБХІДНІ УМОВИ: **НЕМАЄ**	**НО-1**	**НО-1, НВ-1**	**НО-1, НВ-1, НР-1, Г-3**

Критерії цілісності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям цілісності, КЗЗ оцінюваної КС повинен надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації (включаючи її знищення).

Організація робіт служби захисту інформації

Трудові відносини в СЗІ будуються на основі законодавства України з урахуванням положень статуту організації, правил внутрішнього трудового розпорядку та встановлених в організації норм техніки безпеки праці, гігієни і санітарії, інших розпорядчих документів організації.

СЗІ здійснює свою роботу з реалізації основних організаційних та організаційно-технічних заходів із створення і забезпечення функціонування КСЗІ у відповідності з планами робіт. Підставою для розроблення планів робіт є «План захисту інформації в ІТС».

До планів включаються наступні основні заходи:

- *разові* (одноразово виконувані, необхідність у повторенні яких виникає за умови повного перегляду прийнятих рішень з захисту інформації);
- *постійно виконувані* (заходи, що потребують виконання неперервно або дискретно у випадковий чи заданий час);
- *періодично виконувані* (з заданим інтервалом часу);
- *виконувані за необхідності* (заходи, що потребують виконання під час здійснення або виникнення певних змін в ІТС чи зовнішньому середовищі).

Основні **види планів робіт СЗІ**:

1) Календарний план робіт (щодо реалізації заходів з проектування, реалізації, оцінювання, впровадження, технічного обслуговування, експлуатації КСЗІ та інших питань);

2) План заходів з оперативного реагування на непередбачені ситуації (в тому числі надзвичайні та аварійні) та поновлення функціонування ІТС;

3) Поточний план робіт (на місяць, квартал, рік);

4) Перспективний план розвитку та удосконалення діяльності СЗІ з питань захисту інформації (до 5 років);

5) План заходів з забезпечення безпеки інформації під час виконання окремих важливих робіт, при проведенні нарад, укладенні договорів, угод тощо;

6) Бізнес-план створення і функціонування СЗІ.

ІТС СЗІ має **штатний розклад**, який включає перелік функціональних обов'язків усіх співробітників, необхідних вимог до рівня їхніх знань та навичок.

Безпосереднє керівництво роботою СЗІ здійснює її **керівник**. У випадку, коли СЗІ є структурною одиницею підрозділу ТЗІ (служби безпеки організації), – керівник цього підрозділу (заступник керівника). Призначення і звільнення з посади керівника СЗІ здійснюється керівництвом організації за узгодженням з особами, що відповідають за забезпечення безпеки інформації (керівник підрозділу ТЗІ, керівник служби безпеки та ін.).

Штат СЗІ комплектується спеціалістами, які мають спеціальну технічну освіту та практичний досвід роботи, володіють навичками з розробки, впровадження, експлуатації КСЗІ і засобів захисту інформації, а також реалізації організаційних, технічних та інших заходів з захисту інформації, знаннями і вмінням застосовувати нормативно-правові документи у сфері захисту інформації.

Функціональні обов'язки співробітників визначаються переліком і характером завдань, які покладаються на СЗІ керівництвом ІТС (організації).

В залежності від обсягів і особливостей завдань СЗІ до її складу можуть входити спеціалісти (групи спеціалістів, підрозділи та ін.) різного **фаху**:

- спеціалісти з питань захисту інформації від витоку технічними каналами;
- спеціалісти з питань захисту каналів зв'язку і комутаційного обладнання, налагодження і керування активним мережевим обладнанням;
- спеціалісти з питань адміністрування засобів захисту, керування базами даних захисту;
- спеціалісти з питань захищених технологій обробки інформації.

Категорії співробітників СЗІ за посадами:

- керівник СЗІ;
- адміністратори захисту АРМ (безпеки баз даних, безпеки системи тощо);
- спеціалісти служби захисту.

Цілісність забезпечується реалізацією послуг, наведених на рис. 2.9.

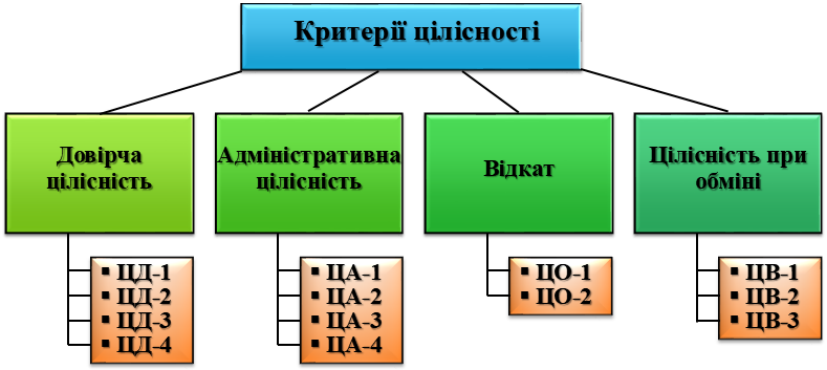

Рис. 2.9 Критерії цілісності

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.

Довірча цілісність – ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену.

Рівні послуги ранжируються на підставі повноти захисту і вибірковості керування.

- **ЦД-1. Мінімальна довірча цілісність** – 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;
- **ЦД-2. Базова довірча цілісність** – 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;

- **ЦД-3. Повна довірча цілісність** – основна відмінність між рівнями ЦД-2 і ЦД-3 – 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;

- **ЦД-4. Абсолютна довірча цілісність** – 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.

Таблиця 2.6 Критерії довірчої цілісності

<table>
<tr><th>ЦД-1. Мінімальна довірча цілісність</th><th>ЦД-2. Базова довірча цілісність</th><th>ЦД-3. Повна довірча цілісність</th><th>ЦД-4. Абсолютна довірча цілісність</th></tr>
<tr><td colspan="2">Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів ІТС, до яких вона відноситься</td><td colspan="2">Політика довірчої цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ІТС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>користувача і захищеного об'єкта</td><td colspan="2">процесу і захищеного об'єкта</td><td>процесу, користувача і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта</td></tr>
<tr><td colspan="4">КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт</td><td>конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт</td><td>конкретні процеси (і групи процесів), які мають, а також тих, що не мають права модифікувати об'єкт</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, що не мають права модифікувати об'єкт</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право ініціювати процес</td><td colspan="2">конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес</td></tr>
<tr><td colspan="4">Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НИ-1</td><td colspan="2">НЕОБХІДНІ УМОВИ: КО-1, НИ-1</td></tr>
</table>

чних та інших заходів з оцінки стану захищеності інформації в ІТС, які включені до плану робіт СЗІ;

- якість та правомірність документального оформлення результатів робіт окремих етапів створення КСЗІ, документального оформлення результатів перевірок;

- інші питання персональної відповідальності, які покладені на керівника та співробітників СЗІ у відповідності з специфікою та особливостями діяльності ІТС (організації).

СЗІ взаємодіє, узгоджує свою діяльність та встановлює зв’язки з:

- РСО організації;

- Службою безпеки організації;

- підрозділами служб безпеки іноземних фірм, їхніми представництвами;

- підрозділом ТЗІ організації;

- зовнішніми організаціями, які є партнерами, користувачами, постачальниками, виконавцями робіт;

- адміністрацією ІТС та ін. підрозділами організації, виробнича діяльність яких пов’язана з захистом інформації або її автоматизованою обробкою;

- іншими суб’єктами діяльності у сфері захисту інформації.

СЗІ координує свою діяльність з аудиторською службою під час проведення аудиторських перевірок.

Штатний розклад та структура СЗІ

СЗІ є *штатним підрозділом організації*, безпосередньо підпорядкованим керівнику організації або його заступнику, що відповідає за забезпечення безпеки інформації. Або СЗІ є *структурною* (штатною або позаштатною) *одиницею* підрозділу ТЗІ (служби безпеки) організації.

Структура СЗІ, її склад і чисельність визначається фактичними потребами ІТС для виконання вимог політики безпеки інформації та затверджується керівництвом організації. Чисельність і склад СЗІ мають бути достатніми для виконання усіх завдань з захисту інформації в ІТС.

З метою ефективного функціонування і керування захистом інформації в

- інші обов’язки, покладені на керівника та співробітників СЗІ у відповідності з специфікою та особливостями діяльності ІТС (організації).

3. **Відповідальність.** Керівництво та співробітники СЗІ за невиконання або неналежне виконання службових обов’язків, допущені ними порушення встановленого порядку захисту інформації в ІТС несуть дисциплінарну, адміністративну, цивільно-правову кримінальну відповідальність згідно з законодавством України.

Персональна відповідальність керівника та співробітників СЗІ визначається посадовими (функціональними) інструкціями.

Керівник СЗІ відповідає за:

- організацію робіт з захисту інформації в ІТС, ефективність захисту інформації відповідно до діючих нормативно-правових актів;
- своєчасне розроблення і виконання «Плану захисту інформації в ІТС»;
- якісне виконання співробітниками СЗІ завдань, функцій та обов'язків, зазначених у «Положенні про СЗІ в ІТС», посадових інструкціях, а також планових заходів із захисту інформації, затверджених керівником організації;
- координацію планів діяльності підрозділів та служб ІТС (організації) з питань захисту інформації;
- створення системи навчання співробітників, користувачів, персоналу ІТС з питань захисту інформації;
- виконання особисто та співробітниками СЗІ розпоряджень керівника організації, правил внутрішнього трудового розпорядку, встановленого режиму, правил охорони праці та протипожежної охорони.

Співробітники СЗІ відповідає за:

- додержання вимог нормативних документів, що визначають порядок організації робіт з захисту інформації, інформаційних ресурсів та технологій;
- повноту та якість розроблення і впровадження організаційно-технічних заходів із захисту інформації в ІТС, точність та достовірність отриманих результатів і висновків з питань, що належать до компетенції СЗІ;
- дотримання термінів проведення контрольних, інспекційних, перевіро-

Адміністративна цілісність – ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів.

Рівні послуги ранжируються на підставі повноти захисту і вибірковості керування:

- **ЦА-1. Мінімальна адміністративна цілісність**;
- **ЦА-2. Базова адміністративна цілісність**;
- **ЦА-3. Повна адміністративна цілісність**;
- **ЦА-4. Абсолютна адміністративна цілісність**.

Таблиця 2.7 Критерії адміністративної цілісності

<table>
<tr><th>ЦА-1. Мінімальна адміністративна цілісність</th><th>ЦА-2. Базова адміністративна цілісність</th><th>ЦА-3. Повна адміністративна цілісність</th><th>ЦА-4. Абсолютна адміністративна цілісність</th></tr>
<tr><td colspan="2">Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів ІТС, до яких вона відноситься</td><td colspan="2">Політика адміністративної цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ІТС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>користувача і захищеного об'єкта</td><td colspan="2">процесу і захищеного об'єкта</td><td>процесу, користувача і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження</td></tr>
<tr><td colspan="4">КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт</td><td>конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт</td><td>конкретні процеси (і групи процесів), які мають, а також тих, які не мають права модифікувати об'єкт</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права модифікувати об'єкт</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право ініціювати процес</td><td colspan="2">конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес</td></tr>
</table>

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту	
НЕОБХІДНІ УМОВИ: **НО-1, НИ-1**	НЕОБХІДНІ УМОВИ: **КО-1, НО-1, НИ-1**

Згідно з політикою адміністративної цілісності 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.

Відкат – ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкотити) захищений об'єкт до попереднього стану.

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 (відкотити) захищений об’єкт до попереднього стану.

Відкат – завжди доступна автоматизована послуга.

Рівні послуги ранжируються на підставі множини операцій, для яких забезпечується відкат:

- **ЦО-1. Обмежений відкат**;
- **ЦО-2. Повний відкат**.

Таблиця 2.8 Критерії відкату

ЦО-1. Обмежений відкат	**ЦО-2. Повний відкат**
Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься	
Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкотити або відмінити	
певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу	всі операції, виконані над захищеним об'єктом за певний проміжок часу
НЕОБХІДНІ УМОВИ: **НИ-1**	

хідні для здійснення виробничої діяльності організації, особливо технологій, доступ до яких обмежено, інших проектів, що потребують технічної підтримки з боку співробітників СЗІ;

- виходити до керівництва організації з пропозиціями щодо узгодження планів і регламенту відвідування ІТС сторонніми особами;
- інші права, які надані СЗІ у відповідності з специфікою та особливостями діяльності організації (ІТС).

2. Обов’язки:

- організовувати забезпечення повноти та якісного виконання організаційно- технічних заходів з захисту інформації в ІТС;
- вчасно і в повному обсязі доводити до користувачів і персоналу ІТС інформацію про зміни в галузі захисту інформації, які їх стосуються;
- перевіряти відповідність прийнятих в ІТС (організації) правил, інструкцій щодо обробки інформації, здійснювати контроль за виконанням цих вимог;
- здійснювати контрольні перевірки стану захищеності інформації в ІТС;
- забезпечувати конфіденційність робіт з монтажу, експлуатації та технічного обслуговування засобів захисту інформації, встановлених в ІТС (організації);
- сприяти і, у разі необхідності, брати безпосередню участь у проведенні вищими органами перевірок стану захищеності інформації в ІТС;
- сприяти (технічними та організаційними заходами) створенню і дотриманню умов збереження інформації, отриманої організацією на договірних, контрактних або інших підставах від організацій-партнерів, постачальників, клієнтів та приватних осіб;
- періодично, не рідше одного разу на місяць (інший термін), подавати керівництву організації звіт про стан захищеності інформації в ІТС і дотримання користувачами та персоналом ІТС встановленого порядку і правил захисту інформації;
- негайно повідомляти керівництво ІТС (організації) про виявлені атаки та викритих порушників;

теріальною базою, навчальними посібниками, нормативно-правовими актами, нормативними документами, методичною літературою та ін.

До **повноважень та відповідальності СЗІ** відносяться:

1. **Права:**

- здійснювати контроль за діяльністю будь-якого структурного підрозділу організації (ІТС) щодо виконання ним вимог нормативно-правових актів і нормативних документів із захисту інформації;
- подавати керівництву організації пропозиції щодо призупинення процесу обробки інформації, заборони обробки, зміни режимів обробки, тощо у випадку виявлення порушень політики безпеки або у випадку виникнення реальної загрози порушення безпеки;
- складати і подавати керівництву організації акти щодо виявлених порушень політики безпеки, готувати рекомендації щодо їхнього усунення;
- проводити службові розслідування у випадках виявлення порушень;
- отримувати доступ до робіт та документів структурних підрозділів організації (ІТС), необхідних для оцінки вжитих заходів з захисту інформації та підготовки пропозицій щодо їхнього подальшого удосконалення;
- готувати пропозиції щодо залучення на договірній основі до виконання робіт з захисту інформації інших організацій;
- готувати пропозиції щодо забезпечення ІТС (КСЗІ) необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою, які дозволені для використання в Україні з метою забезпечення захисту інформації;
- виходити до керівництва організації з пропозиціями щодо подання заяв до відповідних державних органів на проведення державної експертизи КСЗІ або сертифікації окремих засобів захисту інформації;
- узгоджувати умови включення до складу ІТС нових компонентів та подавати керівництву пропозиції щодо заборони їхнього включення, якщо вони порушують прийняту політику безпеки або рівень захищеності ресурсів ІТС;
- надавати висновки з питань, що належать до компетенції СЗІ, які необ-

Цілісність при обміні – ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування:

- **ЦВ-1. Мінімальна цілісність при обміні**;
- **ЦВ-2. Базова цілісність при обміні**;
- **ЦВ-3. Повна цілісність при обміні**.

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.

Таблиця 2.9 Критерії цілісності при обміні

<table>
<tr><th>ЦВ-1: Мінімальна цілісність при обміні</th><th colspan="2">ЦВ-2: Базова цілісність при обміні</th><th>ЦВ-3: Повна цілісність при обміні</th></tr>
<tr><td colspan="4">Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів ІТС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності</td></tr>
<tr><td colspan="4">КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається</td></tr>
<tr><td rowspan="3">—</td><td colspan="3">а також фактів його видалення або дублювання</td></tr>
<tr><td colspan="3">Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу</td></tr>
<tr><td>—</td><td colspan="2">і приймальника об'єкта</td></tr>
<tr><td rowspan="3">—</td><td colspan="3">Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу</td></tr>
<tr><td>—</td><td colspan="2">і джерела об'єкта</td></tr>
<tr><td colspan="3">Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження</td></tr>
<tr><td>—</td><td colspan="3"></td></tr>
</table>

	—	Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника
НЕОБХІДНІ УМОВИ: **НЕМАЄ**	**НО-1**	**НО-1, НВ-1**

Критерії доступності

Для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання ІТС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність ІТС функціонувати у випадку відмови її компонентів.

Доступність забезпечується реалізацією послуг, наведених на рис. 2.10.

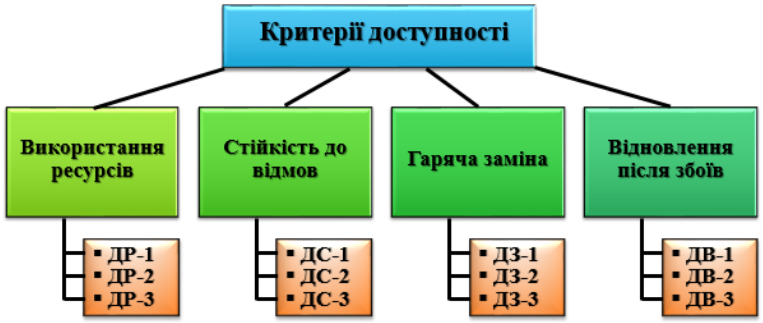

Рис. 2.10 Критерії доступності

Використання ресурсів – ця послуга дозволяє користувачам керувати використанням послуг і ресурсів.

Рівні послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг ІТС:

- **ДР-1. Квоти** – найслабкіша форма контролю за використанням ресурсів: всі захищені об'єкти ІТС (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 дано-

14) негайне втручання в процес роботи ІТС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника;

15) регулярне подання звітів керівництву організації-власника (розпорядника) ІТС про виконання користувачами ІТС вимог із захисту інформації;

16) аналіз відомостей щодо технічних засобів захисту інформації нового покоління, обґрунтування пропозицій щодо придбання засобів для організації;

17) контроль за виконанням персоналом і користувачами ІТС вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації, у тому числі контроль за забезпеченням режиму секретності у разі обробки в ІТС інформації, що становить державну таємницю;

18) контроль за забезпеченням охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що підлягають захисту;

19) розробка і реалізація спільно з РСО (підрозділом ТЗІ, службою безпеки) організації комплексних заходів з безпеки інформації під час проведення заходів з науково-технічного, економічного, інформаційного співробітництва з іноземними фірмами, а також під час проведення нарад, переговорів та ін., здійснення їхнього технічного та інформаційного забезпечення.

3. Функції СЗІ з організації навчання персоналу з питань забезпечення захисту інформації:

1) розроблення планів навчання і підвищення кваліфікації спеціалістів СЗІ та персоналу ІТС;

2) розроблення спеціальних програм навчання, які б враховували особливості технології обробки інформації в організації (ІТС), необхідний рівень її захищеності та ін.;

3) участь в організації і проведенні навчання користувачів і персоналу ІТС правилам роботи з КСЗІ, захищеними технологіями, захищеними ресурсами;

4) взаємодія з державними органами, навчальними закладами, іншими організаціями з питань навчання та підвищення кваліфікації;

5) участь в організації забезпечення навчального процесу необхідною ма-

3) вжиття заходів у разі виявлення спроб НСД до ресурсів ІТС, порушенні правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів;

4) забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід з ладу або порушення режимів функціонування;

5) організація керування доступом до ресурсів ІТС (розподілення між користувачами необхідних реквізитів захисту інформації – паролів, привілеїв, ключів та ін.);

6) супроводження і актуалізація бази даних захисту інформації (матриці доступу, класифікаційні мітки об’єктів, ідентифікатори користувачів тощо);

7) спостереження (реєстрація і аудит подій в ІТС, моніторинг подій тощо) за функціонуванням КСЗІ та її компонентів;

8) підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в ІТС, впровадження нових технологій захисту і модернізації КСЗІ;

9) організація та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ІТС або КСЗІ;

10) участь в роботах з модернізації ІТС – узгодженні пропозицій з введення до складу ІТС нових компонентів, нових функціональних завдань і режимів обробки інформації, заміни засобів обробки інформації тощо;

11) забезпечення супроводження і актуалізації еталонних, архівних і резервних копій програмних компонентів КСЗІ, забезпечення їхнього зберігання і тестування;

12) проведення аналітичної оцінки поточного стану безпеки інформації в ІТС (прогнозування виникнення нових загроз і їх врахування в моделі загроз, визначення необхідності її коригування, аналіз відповідності технології обробки інформації і реалізованої політики безпеки поточній моделі загроз та ін.);

13) інформування власників інформації про технічні можливості захисту інформації в ІТС і типові правила, встановлені для персоналу і користувачів ІТС;

му рівні послуги немає гарантій, що користувач не зможе повністю захопити решту певного ресурсу, обмежуючи тим самим доступ до нього інших користувачів;

- **ДР-2. Недопущення захоплення ресурсів** – являє собою реалізацію досконалішої форми квот, які 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;

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

Таблиця 2.10 Критерії використання ресурсів

<table>
<tr><th>ДР-1. Квоти</th><th>ДР-2. Недопущення захоплення ресурсів</th><th>ДР-3. Пріоритетність використання ресурсів</th></tr>
<tr><td>Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів ІТС, до яких вона відноситься</td><td colspan="2">Політика використання ресурсів, що реалізується КЗЗ, повинна відноситися до всіх об'єктів ІТС</td></tr>
<tr><td colspan="3">Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються</td></tr>
<tr><td colspan="2">окремому користувачу</td><td>окремому користувачу і довільним групам користувачів</td></tr>
<tr><td colspan="3">Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження</td></tr>
<tr><td rowspan="2">—</td><td colspan="2">Повинна існувати можливість встановлювати обмеження таким чином, щоб КЗЗ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ або захищених об'єктів. КЗЗ повинен контролювати такі дії, здійснювані з боку</td></tr>
<tr><td>окремого користувача</td><td>окремого користувача і довільних груп користувачів</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НО-1</td></tr>
</table>

Стійкість до відмов гарантує доступність ІТС (можливість використання інформації, окремих функцій або ІТС в цілому) після відмови її компонента.

Рівні послуги ранжируються на підставі спроможності КЗЗ забезпечити можливість функціонування ІТС в залежності від кількості відмов і послуг, доступних після відмови:

- **ДС-1. Стійкість при обмежених відмовах**;
- **ДС-2. Стійкість з погіршенням характеристик обслуговування**;
- **ДС-3. Стійкість без погіршення характеристик обслуговування**.

Таблиця 2.11 Критерії стійкості до відмов

<table>
<tr><th>ДС-1. Стійкість при обмежених відмовах</th><th>ДС-2. Стійкість з погіршенням характеристик обслуговування</th><th>ДС-3. Стійкість без погіршення характеристик обслуговування</th></tr>
<tr><td colspan="3">Розробник повинен провести аналіз відмов компонентів КС</td></tr>
<tr><td>Політика стійкості до відмов, що реалізується КЗЗ, повинна визначати множину компонентів ІТС, до яких вона відноситься, і типи їх відмов, після яких ІТС в змозі продовжувати функціонування</td><td colspan="2">Політика стійкості до відмов, що реалізується КЗЗ, повинна відноситися до всіх компонентів КС</td></tr>
<tr><td colspan="3">Повинні бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги</td></tr>
<tr><td colspan="2">Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг, а має в гіршому випадку проявлятися в зниженні характеристик обслуговування</td><td>Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг або до зниження характеристик обслуговування</td></tr>
<tr><td colspan="3">КЗЗ повинен бути спроможний повідомити адміністратора про відмову будь-якого захищеного компонента</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НО-1</td></tr>
</table>

Гаряча заміна – ця послуга дозволяє гарантувати доступність ІТС (можливість використання інформації, окремих функцій або ІТС в цілому) в процесі заміни окремих компонентів.

Рівні послуги ранжируються на підставі повноти реалізації.

- **ДЗ-1. Модернізація**;
- **ДЗ-2. Обмежена гаряча заміна**;
- **ДЗ-3. Гаряча заміна будь-якого компонента**.

2) розробка та коригування:
   - моделі загроз та порушників;
   - моделі захисту інформації в ІТС;
   - політики безпеки інформації в ІТС;
3) визначення і формування вимог до КСЗІ;
4) організація і координація робіт з проектування та розробки КСЗІ, безпосередня участь у проектних роботах із створення КСЗІ;
5) підготовка технічних пропозицій, рекомендацій щодо запобігання витоку інформації технічними каналами та попередження спроб НСД до інформації під час створення КСЗІ;
6) організація робіт і участь у випробуваннях КСЗІ, проведенні її експертизи;
7) вибір організацій-виконавців робіт з створення КСЗІ, здійснення контролю за дотриманням встановленого порядку проведення робіт з захисту інформації, у взаємодії з підрозділом ТЗІ (РСО, службою безпеки організації) погодження основних технічних і розпорядчих документів, що супроводжують процес створення КСЗІ (технічне завдання, технічний і робочий проекти, програма і методика випробувань, плани робіт та ін.);
8) участь у розробці нормативних документів, чинних у межах організації і ІТС, які встановлюють:
   - дисциплінарну відповідальність за порушення вимог з безпеки інформації та встановлених правил експлуатації КСЗІ;
   - правила доступу користувачів до ресурсів ІТС, визначають порядок, норми, правила з захисту інформації та здійснення контролю за їх дотриманням (інструкцій, положень, наказів, рекомендацій та ін.).

2. Функції СЗІ під час експлуатації КСЗІ:

1) організація процесу управління КСЗІ;
2) розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій;

давством, підтримка необхідного рівня захищеності інформації, ресурсів і технологій;

4) розроблення проектів нормативних і розпорядчих документів, чинних у межах організації, згідно з якими повинен забезпечуватися захист інформації в ІТС;

5) організація робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу ІТС;

6) участь в організації професійної підготовки і підвищенні кваліфікації персоналу та користувачів ІТС з питань захисту інформації;

7) формування у персоналу і користувачів розуміння необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації;

8) організація забезпечення виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів з захисту інформації в ІТС та проведення контрольних перевірок їх виконання.

Функції СЗІ розрізняються для різних періодів життєвого циклу КСЗІ:

- під час створення КСЗІ;
- під час експлуатації КСЗІ;
- з організації навчання персоналу з питань забезпечення захисту інформації.

1. Функції СЗІ під час створення комплексної системи захисту інформації:

1) визначення:
   - переліків відомостей, які підлягають захисту в процесі обробки, інших об’єктів захисту в ІТС;
   - класифікація інформації за вимогами до її конфіденційності або важливості для організації;
   - необхідних рівнів захищеності інформації;
   - визначення порядку введення (виведення), використання та розпорядження інформацією в ІТС;

Мета реалізації послуги – встановлення нової версії системи, відмова або заміна захищеного компонента не повинні призводити до того, що система потрапить до стану, коли політика безпеки стане скомпрометованою.

Таблиця 2.12 Критерії гарячої заміни

ДЗ-1. Модернізація	**ДЗ-2. Обмежена гаряча заміна**	**ДЗ-3. Гаряча заміна будь-якого компонента**
Політика гарячої заміни, що реалізується КЗЗ, повинна визначати політику проведення модернізації ІТС	Політика гарячої заміни, що реалізується КЗЗ, повинна визначати множину компонентів ІТС, які можуть бути замінені без переривання обслуговування	Політика гарячої заміни, що реалізується КЗЗ, повинна забезпечувати можливість заміни будь-якого компонента без переривання обслуговування
Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість провести модернізацію (upgrade) ІТС. Модернізація ІТС не повинна призводити до необхідності ще раз проводити інсталяцію ІТС або до переривання виконання КЗЗ функцій захисту	Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість замінити будь-який захищений компонент	
НЕОБХІДНІ УМОВИ: **НО-1**	НЕОБХІДНІ УМОВИ: **НО-1, ДС-1**	

Відновлення після збоїв – ця послуга забезпечує повернення ІТС у відомий захищений стан після відмови або переривання обслуговування.

Рівні послуги ранжируються на підставі ступені автоматизації процесу відновлення:

- **ДВ-1. Ручне відновлення**;
- **ДВ-2. Автоматизоване відновлення**;
- **ДВ-3. Вибіркове відновлення**.

Таблиця 2.13 Критерії відновлення після збоїв

ДВ-1. Ручне відновлення	**ДВ-2. Автоматизоване відновлення**	**ДВ-3. Вибіркове відновлення**
Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов ІТС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція ІТС		
Після відмови ІТС або переривання обслуговування КЗЗ повинен перевести ІТС до стану, із якого повернути її до	Після відмови ІТС або переривання обслуговування КЗЗ має бути здатним визначити, чи можуть бути використані	Після будь-якої відмови ІТС або переривання обслуговування, що не призводить до необхідності заново інста-

нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження	автоматизовані процедури для повернення ІТС до нормального функціонування безпечним чином. Якщо такі процедури можуть бути використані, то КЗЗ має бути здатним викона-ти їх і повернути ІТС до нормального функціонування	лювати ІТС, КЗЗ повинен бути здатним ви-конати необхідні процедури і безпечним чином повернути ІТС до нормального функціонування або, в гіршому випадку, функціонування в режимі з погіршеними характеристиками обслуговування
—	Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести ІТС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження	
Повинні існувати ручні процедури, за допомогою яких можна безпечним чином		
повернути ІТС до нормального функціонування		повернути ІТС з режиму з погіршеними характеристиками обслуговування в режим нормального функціонування
НЕОБХІДНІ УМОВИ: **НО-1**		

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.

Критерії спостереженості

Для того, щоб ІТС могла бути оцінена на предмет відповідності критеріям спостереженості, КЗЗ оцінюваної ІТС повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції.

Спостереженість в ІТС забезпечується реалізацією послуг, наведених на рис. 2.11.

Реєстрація дозволяє контролювати небезпечні для ІТС дії.

Рівні послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень:

- **НР-1. Зовнішній аналіз**;

Правові основи створення і діяльності СЗІ:

- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (ВВР України, 1994, № 31, ст.286);
- Положення про технічний захист інформації в Україні (Указ Президента України №1229/99);
- Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах (Постанова КМ України №180/98);
- Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (Постанова КМ України №373/2006.

СЗІ здійснює діяльність відповідно до «Плану захисту інформації в інформаційно-телекомунікаційній системі», календарних, перспективних та інших планів робіт, затверджених керівником (заступником керівника) організації.

У своїй роботі СЗІ взаємодіє з підрозділами організації – РСО, Службою безпеки організації, підрозділами ТЗІ, а також з державними органами, установами та організаціями, що займаються питаннями захисту інформації.

У разі потреби, до виконання робіт можуть залучатися зовнішні організації, що мають ліцензії на відповідний вид діяльності у сфері захисту інформації.

Завдання СЗІ:

1) захист законних прав щодо безпеки інформації організації, окремих її структурних підрозділів, персоналу в процесі інформаційної діяльності та взаємодії між собою, а також у взаємовідносинах з зовнішніми вітчизняними і закордонними організаціями;

2) дослідження технології обробки інформації в ІТС з метою виявлення можливих каналів витоку та інших загроз для безпеки інформації, формування моделі загроз, розроблення політики безпеки інформації, визначення заходів, спрямованих на її реалізацію;

3) організація та координація робіт, пов’язаних з захистом інформації в ІТС, необхідність захисту якої визначається її власником або чинним законо-

Положення має бути погоджене з юрисконсультом та керівниками підрозділів (служби безпеки, РСО, підрозділу ТЗІ) організації. Затверджується наказом керівника організації або підрозділу, до якого структурно входить СЗІ.

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

Структура Положення про службу захисту інформації в ІТС приведена на рис. 2.37.

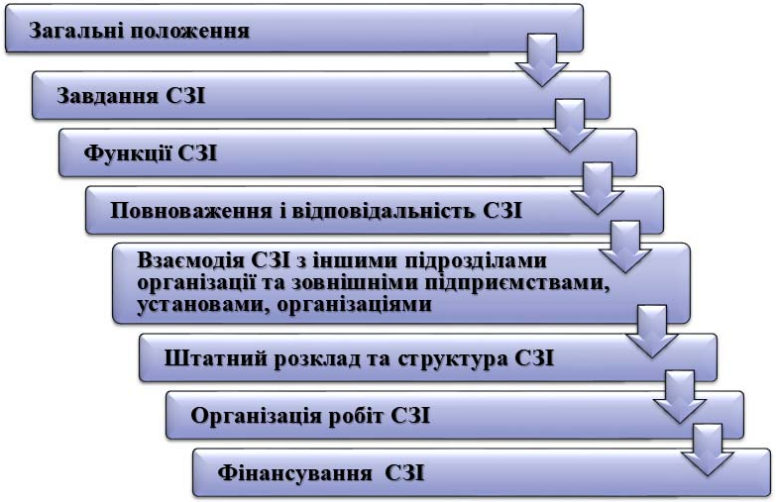

Рис. 2.37 Структура Положення про службу захисту інформації в ІТС

Метою створення СЗІ є:

1) організаційне забезпечення завдань керування КСЗІ в ІТС;
2) здійснення контролю за функціонуванням КСЗІ в ІТС.

На СЗІ покладається виконання **робіт**:

- з визначення вимог з захисту інформації в ІТС;
- проектування, розроблення і модернізації КСЗІ;
- з експлуатації, обслуговування, підтримки працездатності КСЗІ;
- контролю за станом захищеності інформації в ІТС.

- **НР-2. Захищений журнал**;
- **НР-3. Сигналізація про небезпеку**;
- **НР-4. Детальна реєстрація**;
- **НР-5. Аналіз в реальному часі**.

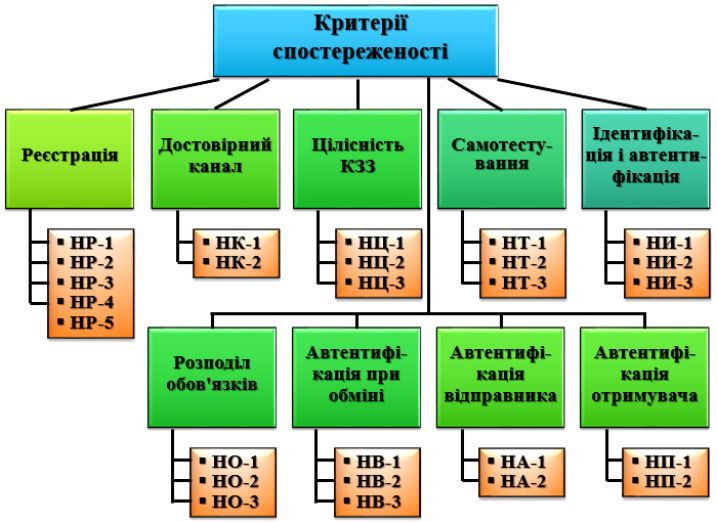

Рис. 2.11 Критерії спостереженості

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.

Таблиця 2.14 Критерії реєстрації

НР-1. Зовнішній аналіз	НР-2. Захищений журнал	НР-3. Сигналізація про небезпеку	НР-4. Детальна реєстрація	НР-5. Аналіз в реальному часі
Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються				
КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки			КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє або непряме відношення до безпеки	
Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події				

<table>
<tr><td>КЗЗ має бути здатним передавати журнал реєстрації в інші системи з використанням певних механізмів захисту</td><td colspan="2">КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.
Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації</td></tr>
<tr><td colspan="2" rowspan="2">—</td><td>КЗЗ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки ІТС.
КЗЗ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій</td></tr>
<tr><td>—</td><td>КЗЗ має бути здатним виявляти і аналізувати несанкціоновані дії в реальному часі</td></tr>
<tr><td>НЕОБХІДНІ УМОВИ: НИ-1</td><td colspan="2">НЕОБХІДНІ УМОВИ: НИ-1, НО-1</td></tr>
</table>

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.

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.

Для реалізації найбільш високих рівнів даної послуги необхідна наявність

Вдосконалення	**1. Невідповідності й корегувальні дії** – реагувати на невідповідності і за можливості виконувати дії для контролю та їх корекції; вживати заходів щодо наслідків; - оцінювати потреби в діях для усунення причин невідповідностей для запобігання їх повторення чи виникнення будь-де за допомогою перегляду невідповідностей; визначення причин невідповідностей і визначення, чи існують подібні невідповідності або потенційно можуть з'являтися; - впровадити певні дії; - переглянути ефективність виконаних коригувальних дій і внести зміни до СУІБ. Коригувальні дії мають бути адекватними до наслідків виявлених невідповідностей **2. Постійне вдосконалення**– постійно вдосконалювати придатність, адекватність та ефективність СУІБ, гарантування її постійної придатності, адекватності та ефективності.

8.2 Служба захисту інформації в ІТС: призначення, завдання, функції, повноваження та відповідальність

Служба захисту інформації (СЗІ) – це підрозділ організації, який забезпечує захист інформації шляхом управління комплексною системою захисту інформації. Це може бути:

- штатним підрозділом організації (ІТС);
- позаштатним підрозділом організації (ІТС);
- самостійним структурним підрозділом організації (ІТС);
- структурною одиницею (підрозділу ТЗІ, служби безпеки …) організації.

В організаціях, де штатним розкладом не передбачено створення СЗІ, заходи щодо забезпечення захисту інформації в ІТС здійснюють призначені наказом керівника організації працівники. У цьому випадку посадові (функціональні) обов'язки цих працівників повинні включати положення, які б передбачали виконання ними вимог щодо діяльності СЗІ.

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації (СЗІ) в ІТС – **«Положення про службу захисту інформації в інформаційно-телекомунікаційній системі»**.

	- впроваджувати плани для досягнення цілей ІБ; - зберігати документовану інформацію в обсязі, необхідному для впевненості, що процес виконується як було заплановано; - контролювати заплановані зміни та переглядати наслідки непередбачених змін, застосовуючи дії для усунення будь-яких шкідливих дій, за потреби; - гарантувати, що процеси, віддані на аутсорсинг, визначені й контрольовані. **2. Оцінювання ризиків інформаційної безпеки** – виконувати оцінювання ризиків через заплановані інтервали або коли запропоновані чи відбуваються суттєві зміни з урахуванням визначених критеріїв та зберігати задокументовану інформацію стосовно результатів оцінювання ризиків ІБ. **3. Оброблення ризиків ІБ** – впровадити план оброблення ризиків ІБ и зберігати задокументовану інформацію стосовно результатів оброблення ризиків ІБ.
Оцінювання результативності	**1. Моніторинг, вимірювання, аналіз та оцінювання** – оцінювати результативність ІБ та ефективність СУІБ и визначити: - що саме потрібно моніторити й вимірювати, включаючи процеси інформаційної безпеки та заходи безпеки; - методи моніторингу, вимірювань, аналізу та оцінювання, які може бути застосовано для гарантії обґрунтованих результатів; - коли моніторинг та вимірювання потрібно виконувати; - хто повинен виконувати моніторинг та вимірювання; - коли результати моніторингу та вимірювань потрібно аналізувати й оцінювати; - хто повинен аналізувати й оцінювати ці результати. **2. Внутрішній аудит** – проводити внутрішні аудити через заплановані інтервали часу для забезпечення того, що інформація чи СУІБ відповідають власним вимогам організації для її СУІБ та вимогам стандарту; ефективно впроваджена та підтримується; - планувати, розробляти, впроваджувати та підтримувати програму аудиту, зокрема й частоту, методи, відповідальності, заплановані вимоги та звітність. Програма аудиту повинна враховувати аналіз важливості процесів, що їх розглядають, і результати попередніх аудитів; визначити критерії аудиту та сферу застосування для кожного аудиту; призначити аудиторів і виконати аудити, які гарантують об'єктивність і неупередженість процесу аудиту; гарантувати, що результати аудиту буде доведено до відповідного керівництва; зберігати документовану інформацію як доказ програми аудиту та результатів аудиту. **3. Перегляд з боку керівництва.** Вище керівництво повинно переглядати СУІБ організації через заплановані проміжки часу для гарантування її постійної придатності, адекватності й ефективності. Перегляд з боку керівництва повинен стосуватися розгляду статусу дії, що є наслідком попереднього перегляду керівництва; зміни в зовнішніх та внутрішніх обставинах, які мають відношення до СУІБ; зворотного впливу на результативність ІБ, охоплюючи тенденції в невідповідностях та коригувальних діях, результатах моніторингу та вимірювань, результатах аудиту та досягненнях цілей ІБ; зворотного зв'язку від зацікавлених сторін; результатів оцінювання ризиків і статусу плану оброблення ризиків; можливостей для постійного вдосконалення. Вихідні дані перегляду з боку керівництва повинні включати рішення стосовно можливостей постійного вдосконалення та будь-яких потреб внесення змін до СУІБ.

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.

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до ІТС.

Рівні послуги ранжируються залежно від числа задіяних механізмів автентифікації:

- **НИ-1. Зовнішній аналіз**;
- **НИ-2. Захищений журнал**;
- **НИ-3. Сигналізація про небезпеку**.

За результатами ідентифікації і автентифікації користувача КЗЗ:

- приймає рішення про те, чи дозволено даному користувачеві ввійти в систему;
- використовує одержані результати надалі для здійснення розмежування доступу на підставі атрибутів доступу користувача, що увійшов.

Відомі три основних типи автентифікації:

- *щось відоме користувачеві*, наприклад, пароль, персональний номер або інша подібна інформація;
- *щось, чим володіє користувач*, наприклад, смарт-карта, магнітна картка, генератор запитів-відповідей, електронний ключ або фізично прошитий криптографічний ключ (основною перевагою даного типу автентифікації є складність або висока вартість дублювання інформації автентифікації);
- щось, властиве користувачеві, наприклад, відбитки пальців, параметри райдужної оболонки ока або геометрія руки. 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.

Таблиця 2.15 Критерії ідентифікації і автентифікації

НИ-1. Зовнішня ідентифікація і автентифікація	НИ-2. Одиночна ідентифікація і автентифікація	НИ-3. Множинна ідентифікація і автентифікація
Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ		
Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен		
з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифі-катор цього користувача	автентифікувати цього користувача з використанням захищеного механізму	автентифікувати цього користувача з використанням захищених механізмів двох або більше типів
—	КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування	
НЕОБХІДНІ УМОВИ: **НЕМАЄ**	НЕОБХІДНІ УМОВИ: **НК-1**	

Достовірний канал – ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається).

Рівні послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін:

- **НК-1. Однонаправлений достовірний канал**;
- **НК-2. Двонаправлений достовірний канал**.

Таблиця 2.16 Критерії достовірного каналу

НК-1. Однонаправлений достовірний канал	НК-2. Двонаправлений достовірний канал
Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ	
Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем	Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації та у випадках, коли необхідний прямий зв'язок користувач/КЗЗ або КЗЗ/користувач. Зв'язок з використанням даного каналу повинен ініціюватися користувачем або КЗЗ
—	Обмін з використанням достовірного каналу, що ініціює КЗЗ, повинен бути однозначно ідентифікований як такий і має відбутися тільки після позитивного підтвердження готовності до обміну з боку користувача
НЕОБХІДНІ УМОВИ: **НЕМАЄ**	

	- гарантує, що повторні оцінки ризиків ІБ призводять до послідовних, дійових та порівняльних результатів; - ідентифікує ризики ІБ; - виконує аналіз ризиків інформаційної безпеки; - оцінює ризики інформаційної безпеки. ***b) Оброблення ризиків інформаційної безпеки –*** визначити та застосовувати процес оброблення ризиків інформаційної безпеки для: - вибору доречних опцій оброблення ризиків ІБ з урахуванням результатів оцінки ризиків; - визначити всі заходи безпеки, які необхідно впровадити для вибраної опції оброблення ризиків; - порівняти ці заходи безпеки з наведеними в стандарті і підтвердити, що не було опущено потрібних заходів безпеки; - підготувати Положення щодо застосовності, яке містить необхідні заходи безпеки, обґрунтування для їх застосування, впроваджені необхідні заходи безпеки чи ні, обґрунтування для виключень заходів безпеки, наданих у стандарті; - розробити план оброблення ризиків ІБ; - отримати від власників ризиків підтвердження плану оброблення ризиків ІБ та згоду на залишкові ризики ІБ. **2. Цілі інформаційної безпеки та планування їх досягнення** – встановити цілі ІБ для відповідних функцій та рівнів. Цілі ІБ мають відповідати політиці ІБ; бути вимірюваними (якщо доцільно); враховувати вимоги до ІБ, які застосовують, а також результати оцінювання ризиків та оброблення ризиків; бути розповсюдженими та оновлюватися. Під час планування дій для досягнення цілей ІБ визначити: що треба зробити; які ресурси будуть потрібні; хто буде відповідальним; коли процес буде завершено; як результати будуть оцінювати.
Підтримка	**1. Ресурси** – визначити й забезпечувати наявність ресурсів, потрібних для розроблення, впровадження, підтримання й постійного вдосконалення СУІБ. **2. Компетенція** – визначити рівень необхідної компетентності персоналу, який виконує роботи, що впливають на результативність ІБ; - гарантувати, що цей персонал має компетенцію на основі відповідного навчання, тренінгів або досвіду; - забезпечувати виконання певних дій для досягнення необхідної компетенції та оцінювати ефективність таких дій; - зберігати відповідну документовану інформацію як доказ компетентності. **3. Обізнаність**. Персонал, який виконує функції під наглядом організації, повинен бути обізнаним в політиці ІБ; його вкладі в ефективність СУІБ, враховуючи переваги від вдосконалення результативності ІБ; розумінні невідповідності вимогам СУІБ. **4. Комунікація** – визначити потребу у внутрішніх та зовнішніх комунікаціях з питань СУІБ, включаючи з яких питань спілкуватися; коли спілкуватися; з ким спілкуватися; хто повинен спілкуватися; процеси, за допомогою яких комунікація повинна відбуватися. **5. Документована інформація**. СУІБ повинна включати документовану інформацію, визначену стандартом; документовану інформацію, визначену організацією як необхідну для ефективності СУІБ.
Функціонування	**1. Робоче планування й контроль**: - планувати, впроваджувати й контролювати процеси, необхідні для виконання вимог ІБ, а також впроваджувати заплановані дії;

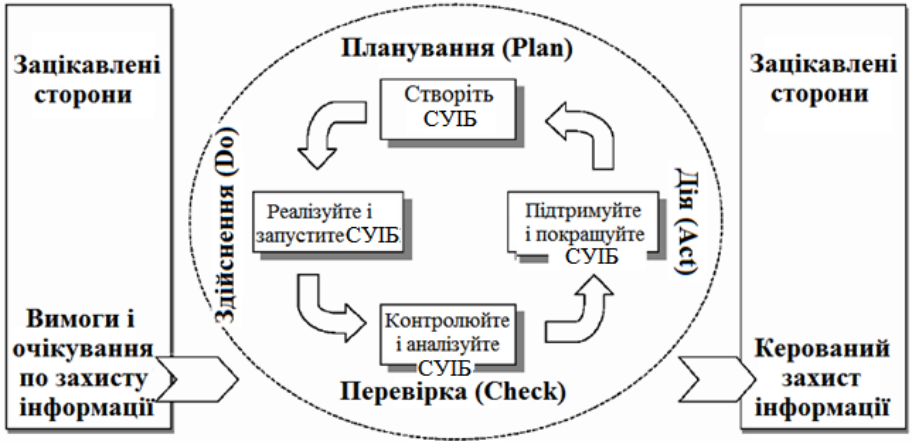

Рис. 2.36 Модель PDCA, застосована до процесів СУІБ

Таблиця 2.44 Компоненти моделі PDCA

Планування (розробка СУІБ)	Розробка політики, встановлення цілей, процесів і процедур СУІБ, що відносяться до менеджменту ризику і поліпшення інформаційної безпеки, для досягнення результатів, що відповідають загальній політиці і цілям організації
Здійснення (впровадження і забезпечення функціонування СУІБ)	Впровадження і застосування політики інформаційної безпеки, заходів управління, процесів і процедур СУІБ
Перевірка (проведення моніторингу і аналізу СУІБ)	Оцінка, у тому числі, за можливістю, кількісна, результативності процесів відносно вимог політики, цілей безпеки і практичного досвіду функціонування СУІБ і інформування вищого керівництва про результати для подальшого аналізу
Дія (підтримка і покращення СУІБ)	Проведення коригуючих і превентивних дій, що грунтуються на результатах внутрішнього аудиту або іншої відповідної інформації, і аналізу з боку керівництва в цілях досягнення безперервного поліпшення СУІБ

Стандарт визначає основні вимоги, які мають бути реалізовані організацією при створенні СУІБ (табл. 2.45).

Таблиця 2.45 Вимоги до організації із реалізації функцій управління

Функція	Що повинна виконати організація
Планування	**1. Дії щодо ризиків та можливостей** – планувати дії, які стосуються ризиків та можливостей, і, як саме, інтегрувати й упровадити ці дії до процесів її СУІБ та оцінювати ефективність цих дій. ***а) Оцінка ризиків інформаційної безпеки*** **–** визначити та застосовувати процес оцінювання ризиків ІБ, який: - встановлює та підтримує критерії ризиків ІБ, які містять критерії прийняття ризиків і критерії для виконання оцінки ризиків ІБ;

Розподіл обов'язків – ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування.

Рівні послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів:

- **НО-1. Виділення адміністратора**;
- **НО-2. Розподіл обов'язків адміністраторів**;
- **НО-3. Розподіл обов'язків на підставі привілеїв**.

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

Дана послуга дозволяє знизити ймовірність навмисних або помилкових неавторизованих дій користувача або адміністратора і величину потенційних збитків від таких дій.

Таблиця 2.17 Критерії розподілу обов'язків

<table>
<tr><th>НО-1. Виділення адміністратора</th><th>НО-2. Розподіл обов'язків адміністраторів</th><th>НО-3. Розподіл обов'язків на підставі привілеїв</th></tr>
<tr><td colspan="3">Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції</td></tr>
<tr><td rowspan="2">—</td><td colspan="2">Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі</td></tr>
<tr><td>—</td><td>Політика розподілу обов'язків повинна визначати множину ролей користувачів</td></tr>
<tr><td colspan="3">Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НИ-1</td></tr>
</table>

Цілісність комплексу засобів захисту – ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами:

- **НЦ-1. КЗЗ з контролем цілісності**:
- **НЦ-2. КЗЗ з гарантованою цілісністю**;
- **НЦ-3. КЗЗ з функціями диспетчера доступу**.

Жодна ІТС не може вважатися захищеною, якщо самі засоби захисту є об'єктом для несанкціонованого впливу. Рівень **НЦ-1** даної послуги є необхідною умовою для абсолютно всіх рівнів усіх інших послуг.

Для рівня **НЦ-1** КЗЗ має 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 КЗЗ підтримує 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** КЗЗ забезпечує керування захищеними ресурсами таким чином, щоб не існувало можливості доступу до ресурсів, минаючи КЗЗ.

Таблиця 2.18 Критерії цілісності комплексу засобів захисту

<table>
<tr><th>НЦ-1. КЗЗ з контролем цілісності</th><th>НЦ-2. КЗЗ з гарантованою цілісністю</th><th>НЦ-3. КЗЗ з функціями диспетчера доступу</th></tr>
<tr><td>Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ</td><td colspan="2">Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів</td></tr>
<tr><td>В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора і або автоматично відновити відповідність компонента еталону або перевести ІТС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження</td><td colspan="2">КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування</td></tr>
<tr><td colspan="2">Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ</td><td>КЗЗ повинен гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ</td></tr>
<tr><td>НЕОБХІДНІ УМОВИ: НР-1, НО-1</td><td colspan="2">НЕОБХІДНІ УМОВИ: НЕМАЄ</td></tr>
</table>

- мінімізацію витрат на реалізацію управляючих дій;
- відповідність заходів, що приймаються, сучасному рівню розвитку інформаційних технологій.

Для реалізації технології управління КСЗІ організації необхідно:

- наявність системи взаємозв'язаних нормативно-методичних і організаційно-розпорядливих документів;
- чіткий розподіл функцій і визначення порядку взаємодії підрозділів організації при вирішенні питань захисту інформації, зафіксовані в організаційно-розпорядливих документах;
- наявність Служби захисту інформації, наділеної необхідними повноваженнями і такий, що безпосередньо відповідає за формування і реалізацію єдиної політики інформаційної безпеки організації, що здійснює контроль і координацію дій інших структурних підрозділів організації з питань захисту інформації на усіх етапах її життєвого циклу.

Сучасні погляди на управління КСЗІ відбиває стандарт **ДСТУ ISO/IEC 27001:2015 Information technology – Security techniques – Information security management systems – Requirements** (*Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги*), який створений для визначення вимог для розроблення, впровадження, використанню, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення Системи управління інформаційною безпекою (СУІБ). Прийняття СУІБ є стратегічним рішенням для організації.

СУІБ забезпечує збереження конфіденційності, цілісності та доступності інформації за допомогою запровадження процесу управління ризиками та надає впевненості зацікавленим сторонам , що ризиками належним чином управляють.

Модель СУІБ реалізує замкнутий контур (рис. 2.36):

Плануй (**Plan**) – *Здійснюй* (**Do**) – *Перевіряй* (**Check**) – *Дій* (**Act**) (**PDCA**), яка покликана структурувати усі процеси СУІБ.

Таблиця 2.43 Задачі управління КСЗІ

Ознаки класифікації	Задачі управління КСЗІ
Приналежність до ланки управління	Кожна задача нижчого рівня ієрархії має бути погоджена (за метою, часом, ресурсам і т.п.) з відповідними завданнями вищого рівня.
Приналежність до функціональних підсистем управління	**Задачі:** - контролю режиму секретності; - пропускного режиму; - охорони; - розмежування доступу; - кадрового забезпечення; - нормативно-правові; - криптографічного захисту; - антивірусного захисту; - матеріального, фінансового і технічного забезпечення; - обліку і збереження носіїв інформації та ін.
Періодичність рішення	**Задачі:** - довгострокові; - поточні (квартальні, щомісячні, щодобові); - з випадковою періодичністю.
Ступінь визначеності вихідної інформації	**Задачі:** - детерміновані; - імовірнісні; - невизначені.
Форми розумового процесу	**Задачі аналізу** – полягають у визначенні значень показників ефективності функціонування КСЗІ при заданих структурі, характеристиках елементів і умовах функціонування. **Задачі синтезу** – зводяться до визначення структури і (чи) її характеристик при заданих обмеженнях на ресурси і вимогах (цілях) до її функціонування.
Характер перетворення інформації	**Задачі, що класифікуються:** - за формою представлення даних, - за змістом (*розрахункові* – задачі узгодження дій, змагальні, маршрутизації, заміни устаткування, розподілу ресурсів, пошуку, управління запасами, впорядкування та ін., *інформаційні* – задачі обліку, узагальнення, систематизації, передачі інформації, документування, зберігання і т.п.), - по розташуванню в просторі або в часі.

Технологія управління КСЗІ – організація діяльності керівництва і посадовців організації із забезпечення комплексного захисту інформації.

Технологія управління КСЗИ повинна забезпечувати:

- точну і своєчасну реалізацію політики інформаційної безпеки організації;

- гнучкість застосування положень політики інформаційної безпеки (облік особливостей функціонування різних підсистем організації);

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій ІТС.

Рівні послуги ранжируються на підставі можливості виконання тестів за ініціативою користувача, у процесі запуску або штатної роботи:

- **НТ-1. Самотестування за запитом**;
- **НТ-2. Самотестування при старті**.

Таблиця 2.19 Критерії самотестування

<table>
<tr><th>НТ-1. Самотестування за запитом</th><th>НТ-2. Самотестування при старті</th><th>НТ-3. Самотестування в реальному часі</th></tr>
<tr><td colspan="3">Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ</td></tr>
<tr><td colspan="3">КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження,</td></tr>
<tr><td rowspan="2">—</td><td colspan="2">при ініціалізації КЗЗ</td></tr>
<tr><td>—</td><td>і в процесі штатного функціонування</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НО-1</td></tr>
</table>

Ідентифікація і 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 послуги ранжируються на підставі повноти реалізації:

- **НВ-1. Автентифікація вузла** – дозволяє виключити можливість несанкціонованого зовнішнього підключення і є необхідною умовою для реалізації високих рівнів послуг конфіденційності і цілісності при обміні;

- **НВ-2. Автентифікація джерела даних** – дозволяє виключити можливість несанкціонованого використання встановленого авторизованого підключення;

- **НВ-3. Автентифікація з підтвердженням** – дозволяє виключити можливість деяких видів внутрішнього шахрайства.

Таблиця 2.20 Критерії ідентифікації і автентифікації при обміні

НВ-1: Автентифікація вузла	НВ-2: Автентифікація джерела даних	НВ-3: Автентифікація з підтвердженням
Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації		
—	КЗЗ повинен використовувати захищені механізми для встановлення джерела кожного об'єкта, що експортується та імпортується	
	—	Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження джерела об'єкта незалежною третьою стороною
НЕОБХІДНІ УМОВИ: **НЕМАЄ**		

Автентифікація відправника – 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 послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

- **НА-1. Базова автентифікація відправника**;
- **НА-2. Автентифікація відправника з підтвердженням**.

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

Таблиця 2.21 Критерії автентифікації відправника

НА-1: Базова автентифікація відправника	НА-2: Автентифікація відправника з підтвердженням
Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем	

процедури, операції, дії.

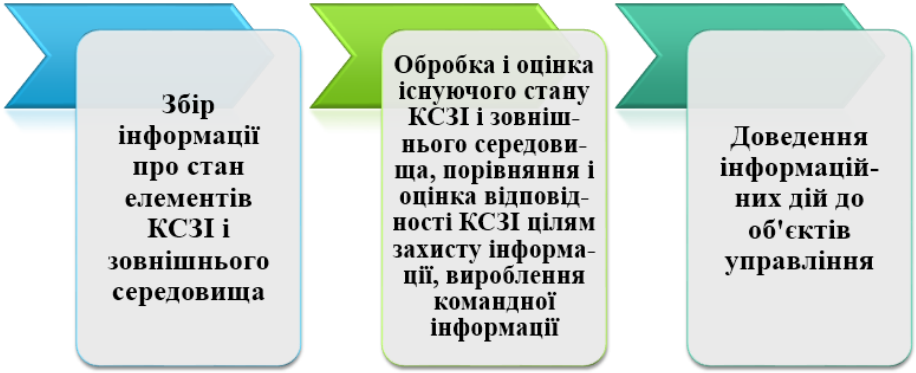

Рис. 2.35 Основні процеси управління КСЗІ

Задача управління – основний елемент процесу управління – технологічний модуль перетворення інформації, що служить для досягнення за заданий час конкретного результату.

Функція управління – стійка сукупність задач реалізації процесу управління (його частини) для досягнення часткових цілей управління, заснована на розподілі управлінської праці в органах управління.

Основні управлінські функції:

- *планування* – процес уточнення цілей системи і детальної програми їх досягнення. Змістом планування є розподіл ресурсів системи і визначення порядку їх використання для досягнення поставленої мети;
- *оперативне управління* – процес корекції поведінки системи при реалізації програми досягнення поставленої мети;
- *контроль* – процес перевірки інформації про елементи системи і зовнішнього середовища і оцінки відповідності стану системи її задачам;
- *облік* – процес виміру і реєстрації характеристик системи і зовнішнього середовища.

Класифікація задач управління КСЗІ приведена в табл. 2.43.

2) На основі цілей управління та інформації стану в ***S*** виробляється управляюча дія (*командна інформація*); вона визначає новий стан ***O***, в яке він повинен перейти при наближенні системи до мети.

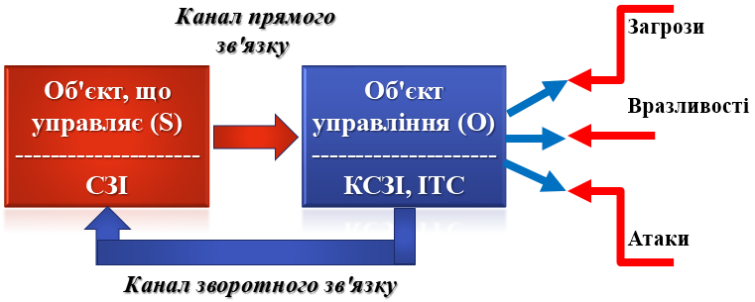

Рис. 2.34 Загальна структура системи управління

3) Сукупність правил, за якими інформація стану перетвориться в командну інформацію, називається **алгоритмом управління**.

4) Командна інформація передається по каналу прямого зв'язку. Сприйнявши інформацію, ***O*** виконує наказані йому дії.

5) Оскільки система функціонує в деякому середовищі, що є джерелом активних і пасивних перешкод, а в роботі елементів системи можливі помилки, то й новий стан ***O*** не завжди співпадатиме з бажаним. Тому разом з виконанням наказаних дій ***O*** постійно передає *S* інформацію про свій стан.

6) Сукупність заходів з управління, що виконуються при зміні середовища, прийнято називати **циклом управління**. Цикли розрізняються за тривалістю і змістом. Цикл може бути перерваний. Виконуючи цикл за циклом, система поступово наближається до мети функціонування.

7) Шлях, яким циркулює інформація між ***S*** і ***O***, називається **контуром управління**. Розрізняють одноконтурні (з одним ***O***) і багатоконтурні системи управління, а також системи управління із *замкнутим* (за наявності каналів зворотного зв'язку) і *розімкненим* контуром управління.

Основні процеси управління КСЗІ показані на рис. 2.35. Процеси при реалізації управління КСЗІ можуть бути розділені на дрібніші підпроцеси, задачі,

—	Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися для однозначного підтвердження належності об'єкта незалежною третьою стороною
Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації	
—	Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження належності об'єкта незалежною третьою стороною
НЕОБХІДНІ УМОВИ: **НИ-1**	

Автентифікація отримувача – послуга дозволяє забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною:

- **НП-1. Базова автентифікація отримувача**;
- **НП-2. Автентифікація отримувача з підтвердженням**.

Таблиця 2.22 Критерії автентифікації отримувача

НП-1: Базова автентифікація отримувача	**НП-2: Автентифікація отримувача з підтвердженням**
Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-одержувача і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був одержаний певним користувачем	
—	Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися незалежною третьою стороною для однозначного підтвердження факту одержання об'єкта
Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації	
—	Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження незалежною третьою стороною факту одержання об'єкта
НЕОБХІДНІ УМОВИ: **НИ-1**	

3.3 Оцінка коректності реалізації послуг безпеки (критерії гарантій)

Критерії гарантій включають вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, середовища функціонування, документації і випробувань КЗЗ. В цих критеріях вводиться сім рівнів гарантій, які є ієрархічними (рис. 2.12).

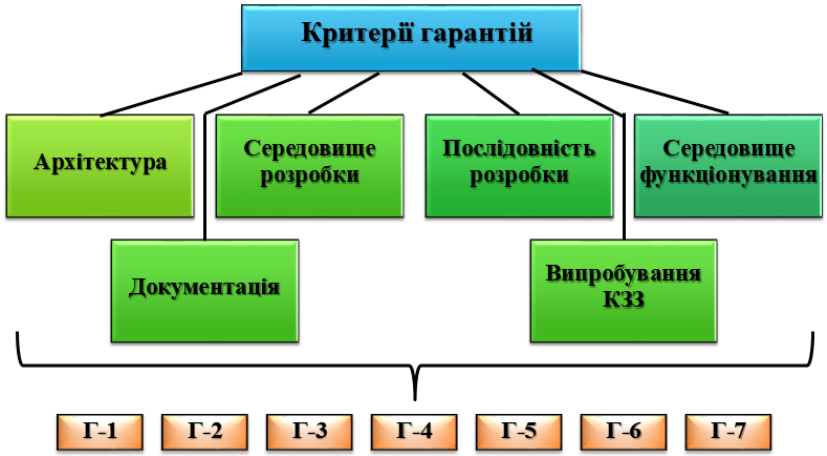

Рис. 2.12 Критерії гарантій

Виконання вимог гарантій забезпечується як діями розробника, проте вже на всіх стадіях життєвого циклу ІТС, так і спільними діями розробника і експертної комісії в процесі оцінки.

Більшість з вимог критеріїв гарантій є конкретизацію вимог щодо створення КЗЗ ІТС стандартів серії **ДСТУ ISO 9000** і для їх викладення використовується термінологія з області керування якістю продукції (**ДСТУ ISO 9000:2001 Системи управління якістю. Основні положення та словник**).

Архітектура. Вимоги до архітектури забезпечують гарантії того, що КЗЗ у змозі повністю реалізувати політику безпеки.

(*критерій «ефективність – вартість»*) – в усіх випадках вартість КСЗІ має бути менше розміру можливого збитку;

- *спеціалізації* – передбачається залучення до розробки і впровадження заходів і засобів захисту спеціалізованих організацій, що мають досвід практичної роботи і державну ліцензію на право надання послуг в цій області. Експлуатація технічних засобів і реалізація заходів захисту інформації повинні здійснюватися професійно підготовленими фахівцями;
- *взаємодії і координації* – означає здійснення заходів забезпечення безпеки на основі чіткого взаємозв'язку підрозділів і служб, сторонніх спеціалізованих організацій в цій області, координації їх зусиль для досягнення поставлених цілей, а також співпраці із зацікавленими об'єднаннями і взаємодії з органами державного управління і правоохоронними органами;
- *вдосконалення заходів і засобів захисту* – здійснюється на основі власного досвіду, появи нових технічних засобів з урахуванням змін в методах і засобах розвідки і промислового шпигунства, нормативно-технічних вимог, досягнутого вітчизняного і зарубіжного досвіду;
- *централізації управління* – припускає функціонування системи захисту інформації на основі єдиних правових, організаційних, функціональних і методологічних принципів.

Структура системи управління у загальному вигляді приведена на рис. 2.34. Вона включає дві основні підсистеми:

1. **Об'єкт, що управляє** (***S***), призначений для вироблення інформаційних дій на основі обробки і відображення зібраної інформації. В ролі такого виступає *Служба захисту інформації*.
2. **Об'єкт управління** (***O***) забезпечує видачу інформації про свій стан і стан зовнішнього середовища, *сприйняття* інформаційних дій від об'єктів, що управляють, і їх реалізацію. Це *КСЗІ* та *ІТС*.

Процес управління в такій системі полягає в наступному:

1) ***S*** по каналу зворотного зв'язку отримує інформацію про стан ***O*** і зовнішнього середовища (*інформація стану*).

	хідно розглядати КСЗІ на всіх стадіях її життєвого циклу, починаючи з моменту створення і закінчуючи повною деградацією
Схожості	Рекомендує здійснювати пошук аналогів управлінських ситуацій на предмет використання управлінських дій, що застосовувалися по них, мали позитивні результати.

Керуючи системою КСЗІ, слід враховувати і інші принципи, загальні для різних видів діяльності:

- *комплексності* – забезпечення захисту інформації від можливих загроз усіма доступними законними засобами, методами і заходами; забезпечення безпеки інформаційних ресурсів впродовж усього їх життєвого циклу, на усіх технологічних етапах їх обробки (перетворення) і використання, в усіх режимах функціонування; здатність системи до розвитку і вдосконалення відповідно до змін умов функціонування;
- *своєчасності* – заходи захисту інформації мають попереджуючий характер, вони припускають постановку завдань з комплексного захисту на ранніх стадіях розробки системи на основі аналізу і прогнозування обстановки, загроз, а також розробку ефективних заходів попередження;
- *безперервності* – вважається, що порушники постійно шукають можливість, як би обійти захисні заходи, прибігаючи для цього до легальних і нелегальних методів;
- *активності* – заходи з захисту інформації проводяться з достатньою мірою наполегливості, з широким використанням маневру силами і засобами захисту;
- *законності* – припускає розробку КСЗІ на основі законодавства в області інформатизації і захисту інформації та інших нормативних актів в цій області, із застосуванням усіх дозволених методів виявлення і припинення правопорушень;
- *обґрунтованості* – використовувані можливості і засоби захисту мають бути реалізованими на сучасному рівні розвитку науки і техніки, обґрунтованими з точки зору заданого рівня захисту і такими, що відповідають встановленим вимогам і нормам;
- *економічній доцільності та порівнянності можливого збитку і витрат*

Таблиця 2.23 Критерії гарантій архітектури

Вимоги	Г-1	Г-2	Г-3	Г-4	Г-5	Г-6	Г-7
КЗЗ повинен реалізовувати політику безпеки. Всі його компоненти повинні бути чітко визначені	+	=	=	=	=	=	=
КЗЗ повинен складатися з добре визначених і максимально незалежних компонентів. Кожний з компонентів повинен бути спроектований відповідно до принципу мінімуму повноважень	-	-	+	=	=	=	=
Критичні для безпеки компоненти КЗЗ повинні бути захищені від не критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно-апаратними засобами більш низького рівня	-	-	-	+	=	=	=
З боку Розробника мають бути вжиті зусилля, спрямовані на виключення з КЗЗ компонентів, що не є критичними для безпеки. Мають бути наведені підстави для включення до КЗЗ будь-якого елемента, який не має відношення до захисту	-	-	-	-	+	=	=
Розробка ПЗ переважно має бути спрямована на мінімізацію складності КЗЗ. КЗЗ має бути спроектований і структурований так, щоб використовувати повний і концептуально простий механізм захисту з точно визначеною семантикою. Цей механізм повинен відігравати центральну роль в реалізації внутрішньої структури КЗЗ. Під час розробки КЗЗ значною мірою повинні бути задіяні такі підходи як модульність побудови і приховання (локалізація) даних	-	-	-	-	+	=	=

* В таблицях використовуються такі позначення: «–» — вимога відсутня; «+» — вимога з'являється; «=» — вимога зберігається.

Для самих низьких рівнів критеріїв гарантій від розробника вимагається просто описати складові компоненти КЗЗ та їх призначення. Для більш високих (проміжних) рівнів вимагається логічне поділення вихідного коду на окремі незалежні компоненти (модулі), що ідентифікуються, та ізоляція компонентів КЗЗ, критичних для безпеки. Внутрішні деталі і дані, використовувані всередині кожного модуля, повинні бути приховані від усіх зовнішніх об'єктів. Послуги КЗЗ повинні бути доступні тільки через зовнішній документований інтерфейс.

Для самих верхніх рівнів розробник під час проектування ПЗ повинен зосередити зусилля на зменшенні обсягу КЗЗ до мінімального набору компонентів. Мінімізація обсягу є однією з вимог концепції диспетчера доступу і дозво-

ляє виділити у складі КЗЗ *ядро захисту*.

Середовище розробки. Вимоги до середовища розробки забезпечують гарантії того, що процеси розробки і супроводження оцінюваної ІТС є повністю керованими з боку розробника.

Таблиця 2.24 Критерії гарантій середовища розробки

Вимоги	Г-1	Г-2	Г-3	Г-4	Г-5	Г-6	Г-7
Процес розробки							
Розробник повинен визначити всі стадії життєвого циклу КС, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути документовані всі етапи кожної стадії життєвого циклу і їх граничні вимоги	+	=	=	=	=	=	=
Розробник повинен описати стандарти кодування, яким необхідно додержуватися в процесі реалізації, і повинен гарантувати, що всі вихідні коди компілюються відповідно до цих стандартів. Будь-яка з використовуваних під час реалізації мов програмування має бути добре визначена. Всі залежні від реалізації параметри мов програмування або компіляторів повинні бути документовані	-	-	+	=	=	=	=
Розробник повинен розробити, запровадити і підтримувати в робочому стані документально оформлені методики забезпечення фізичної, технічної, організаційної і кадрової безпеки	-	-	-	+	=	=	=
Керування конфігурацією							
Розробник повинен розробити, запровадити і підтримувати в робочому стані документовані методики щодо керування конфігурацією КС на всіх стадіях її життєвого циклу. Система керування конфігурацією повинна забезпечувати керування внесенням змін в апаратне забезпечення, програми ПЗП, вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією повинна гарантувати постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ	+	=	=	+*	=	=	=
Система керування конфігурацією також повинна використовуватися для генерації КЗЗ з вихідного коду і обліку всіх змін з появою нових версій	-	-	-	+	=	=	=

Рис. 2.33 Принципи управління КСЗІ

До управління КСЗІ застосовні и принципи системного підходу, перераховані в табл. 2.42.

Таблиця 2.42 Принципи системного підходу

Принципи	Пояснення
Мети (*цілеобумовленості*)	Орієнтує керівника на першочерговість формулювання цілей об'єкту, які повинні досягатися при його функціонуванні. Мета обумовлює структуру і поведінку системи. В процесі функціонування мета системи може мінятися. Відповідно до цього повинні мінятися структура і\або спосіб функціонування системи
Двоїстості (*відносності*)	КСЗІ повинна розглядатися і як система, і як підсистема системи вищого рівня ієрархії – системи безпеки організації
Цілісності	Система управління КСЗІ повинна розглядатися не як простий набір елементів, а як щось ціле, єдине
Складності	Управління є складною сукупністю різних елементів, що знаходяться в різноманітних зв'язках між собою і елементами довкілля. Кожному об'єкту властива нескінченна складність, невичерпність
Всебічності	Вимагає враховувати при управлінні КСЗІ усі зв'язки в ній і чинники, що впливають на її функціонування
Множинності	Орієнтує керівника на те, що для повного опису результатів управляючої дії на КСЗІ потрібна множина моделей, кожна з яких описує її в якому-небудь аспекті (функціональному, структурному, інформаційному і т.д.)
Динамізму	Вказує на те, що управління необхідно розглядати з урахуванням динаміки функціонування КСЗІ (тобто усі характеристики є функціями часу)
Історизму	Зобов'язує проводити дослідження минулого системи захисту, оскільки її функціонування у минулому і сьогоденні дозволяє розкрити закономірності і виявити тенденції розвитку в майбутньому. Необ-

вника) і є центральним моментом, ядром управління. Суть прийняття рішення полягає в тому, що керівник (начальник) повинен творчо і відповідально визначити:

- задум захисту інформації;
- задачі підрозділам і підлеглим;
- основні питання взаємодії і забезпечення;
- організацію управління.

Особливості прийняття рішення в сучасних умовах:

- жорсткий дефіцит часу;
- нестача вихідної інформації;
- ведення інформаційної війни.

Приймаючи рішення, необхідно враховувати об'єктивні закони управління:

1) залежність організаційних форм і методів управління КСЗІ від структури організації, матеріально-технічної бази і умов управління;

2) єдність організаційно-методологічних основ на усіх рівнях управління КСЗІ;

3) збереження пропорційності і оптимального співвідношення усіх елементів системи управління;

4) сумісність систем і засобів управління підлеглих підприємству організацій, а також взаємодіючих організацій;

5) єдність і впідпорядкованість критеріїв ефективності, використовуваних при управлінні КСЗІ;

6) відповідність потрібного часу, що розташовується, при рішенні завдань управління;

7) залежність ефективності рішення задач управління від об'єму використовуваної інформації і т.д.

Принципи управління КСЗІ, які виступають основними початковими положеннями управлінської діяльності, виробленими наукою і практикою, є засобом організації і регулювання цілеспрямованої дії на КСЗІ (рис. 2.33).

Система керування конфігурацією повинна бути здатна видавати звіти про стан елементів конфігурації	-	-	-	+	=	=	=
Повинна використовуватися система заходів технічної, фізичної, організаційної і кадрової безпеки, спрямованих на захист усіх засобів і матеріалів, використовуваних для генерації КЗЗ, від несанкціонованої модифікації або руйнування	-	-	-	-	-	+	=

* Починаючи з рівня **Г-4** система керування конфігурацією повинна базуватися на автоматизованих засобах.

Послідовність розробки. Вимоги до процесу проектування (послідовності розробки) забезпечують гарантії того, що на кожній стадії розробки (проектування) існує точний опис ІТС і реалізація ІТС точно відповідає вихідним вимогам (політиці безпеки).

Таблиця 2.25 Критерії гарантій послідовності розробки

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
***Функціональні специфікації* (*політика безпеки*)**							
На стадії розробки ТЗ Розробник повинен розробити функціональні специфікації ІТС. Представлені функціональні специфікації повинні включати неформалізований опис політики безпеки, що реалізується КЗЗ. Політика безпеки повинна містити перелік і опис послуг безпеки, що надаються КЗЗ	+	=	=	=	=	=	=
***Функціональні специфікації* (*модель політики безпеки*)**							
Відповідність політиці безпеки	-	**Показ**		**Демонстрація**			
Функціональні специфікації повинні включати модель політики безпеки	-	+	=	=	=	=	=
Стиль специфікації: неформалізована	-						
частково формалізована	-						
формалізована	-						
Проект архітектури							
Відповідність моделі політики безпеки	-	**Показ**			**Демонстрація**	**Доказ**	
На стадії розробки ескізного проекту Розробник повинен розробити проект архітектури КЗЗ. Представлений проект повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними. Повинні бути описані будь-які використовувані зовнішні послуги безпеки. Зовнішні інтерфейси КЗЗ повинні	+	=	=	=	=	=	=

бути описані в термінах винятків, повідомлень про помилки і кодів повернення							
Стиль специфікації: неформалізована							
частково формалізована							
формалізована							
Детальний проект							
Відповідність проекту архітектури	-	**Показ**				**Демонстрація**	**Доказ**
На стадіях розробки технічного проекту або робочого проекту Розробник повинен розробити детальний проект КЗЗ. Представлений детальний проект повинен містити перелік всіх компонентів КЗЗ і точний опис функціонування кожного механізму. Повинні бути описані призначення і параметри інтерфейсів компонентів КЗЗ	+	=	=	=	=	=	=
Стиль специфікації: неформалізована	**Весь КЗЗ ***						
частково формалізована							
формалізована							
Реалізація							
Відповідність детальному проекту	-	-	**Показ**				**Демонстрація**
Розробник повинен подати вихідний код: частини КЗЗ	-	-	+	=	=	=	=
всього КЗЗ	-	-	-	-	+	=	=
всіх бібліотек часу виконання	-	-	-	-	-	-	+

* Для рівня **Г-1** вимагається детальний проект компонентів КЗЗ, що мають безпосереднє відношення до безпеки.

Середовище функціонування. Вимоги до середовища функціонування забезпечують гарантії того, що ІТС поставляється замовнику без несанкціонованих модифікацій, а також інсталюється і ініціюється замовником так, як це передбачається розробником.

Таблиця 2.26 Критерії гарантій середовища функціонування

Вимоги	Г-1	Г-2	Г-3	Г-4	Г-5	Г-6	Г-7
Розробник повинен представити засоби інсталяції, генерації і запуску ІТС, які гарантують, що експлуатація ІТС починається з безпечного стану. Розробник повинен пред-	+	=	=	=	=	=	=

- запобігання НСД до інформації і передачі її особам, що не мають права на доступ до інформації;
- перекриття витоку информаци, що захищається, технічними каналами і каналів спеціального впливу;
- своєчасне виявлення фактів НСД до інформації;
- попередження можливості несприятливих наслідків порушення порядку доступу до інформації;
- недопущення впливу на технічні засоби обробки інформації, в результаті якого порушується їх функціонування;
- негайне відновлення інформації, модифікованої або знищеної внаслідок НСД до неї;
- постійний контроль за забезпеченням рівня захищеності інформації і гарантій захищеності.

Досягнення основних цілей захисту інформації пов'язане з рішенням круга задач, що становлять **зміст управління КСЗІ**. Основними з них є:

1) безперервне добування, збір, вивчення і аналіз даних обстановки;
2) підтримка системи в постійній готовності до виконання завдань захисту інформації;
3) ухвалення рішень із захисту інформації;
4) доведення завдань до підлеглих;
5) планування заходів захисту інформації;
6) організація і підтримка взаємодії структурних підрозділів організації;
7) усебічне забезпечення заходів захисту інформації;
8) організація управління, під якою розуміється створення системи управління, забезпечення її ефективного функціонування (у тому числі і зашита системи управління від усіх видів дії порушників), а також вдосконалення цієї системи із застосуванням нових інформаційних технологій;
9) управління підготовкою підрозділів захисту інформації;
10) організація і здійснення контролю і допомоги підлеглим.

Прийняття рішення в системах управління є прерогативою людини (кері-

захисту інформації.

Управління можливо тільки в тих системах, які *мають властивості*:

- у збереженні системи як цілого *вирішальна роль належить інформаційним зв'язкам*;
- система здатна *переходити в різні стани відповідно до управляючих дій*;
- існує *декілька допустимих ліній поведінки системи*, з яких орган, що управляє, вибирає найбільш прийнятну за тими або іншими критеріями;
- процес функціонування системи відрізняється *цілеспрямованістю*;
- система *відкрита для зовнішньої дії*, тобто вплив зовнішніх дій може мати найрізноманітніші природу і наслідки.

Особливості системи управління КСЗІ:

1) призначені для функціонування в конфліктних ситуаціях, оскільки захист інформації є складним двостороннім процесом (КСЗІ порушник);

2) інформація, на основі якої виробляються управляючі дії (робиться вибір засобів, методів і способів захисту інформації) відрізняється значною неповнотою, недостовірністю і суперечністю;

3) порушники постійно змінюють засоби і методи дії на систему, тактику своїх дій.

Суть управління КСЗІ – *цілеспрямована діяльність керівництва організації, посадовців і служби захисту інформації, спрямована на досягнення цілей захисту інформації*. Що ж це за цілі?

1. Забезпечення захисту інформації від неправомірного доступу, знищення, модифікування, блокування, копіювання, надання, поширення, а також від інших неправомірних дій відносно такої інформації.
2. Дотримання конфіденційності ІзОД.
3. Реалізація права на доступ до інформації.
4. Забезпечення спостереженості та керованості ІТС.

Управління КСЗІ призначене для забезпечення ефективного рішення наступних **задач**:

ставити перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску							
Повинна існувати система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ, яке поставляється Замовнику, точно відповідає еталонній копії	-	-	+	=	=	=	=
Для підтримки відповідності між КЗЗ, що поставляється Замовнику, і еталонною копією повинна існувати система керування розповсюдженням захищеної ІТС	-	-	-	-	-	+	=

Документація. Для того, щоб замовник зміг повною мірою використати послуги безпеки, що надаються ІТС для реалізації політики безпеки, встановленої в організації, йому необхідна відповідна документація, в якій були б описані ці послуги і дані вказівки щодо їх використання.

Вимоги до документації є *загальними для всіх рівнів гарантій*. У вигляді окремих документів або розділів (підрозділів) інших документів розробник повинен подати:

- *опис послуг безпеки, що реалізуються КЗЗ* – містить основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізується КЗЗ оцінюваної ІТС, а також опис самих послуг;
- *настанови адміністратору щодо послуг безпеки* – містять опис засобів інсталяції, генерації і запуску ІТС; опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску ІТС; опис властивостей ІТС, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ; інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує ІТС;
- *настанови користувача щодо послуг безпеки* – містять інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Випробування комплексу засобів захисту. Для демонстрації того, що КЗЗ оцінюваної КС піддавався випробуванням, і доказу повноти цих випробу-

вань Розробник повинен надати Експертній комісії документально оформлені результати випробувань. При організації випробувань послуг безпеки і механізмів захисту і документуванні їх результатів треба керуватися вимогами **ДСТУ 2853-94 Програмні засоби ЕОМ. Підготовлення і проведення випробувань**, **ДСТУ 2851-94 Програмні засоби ЕОМ. Документування результатів випробувань** та ін.

Таблиця 2.27 Критерії гарантій випробування комплексу засобів захисту

Вимоги	Г-1	Г-2	Г-3	Г-4	Г-5	Г-6	Г-7
Розробник повинен подати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки. Мають бути представлені аргументи для підтвердження достатності тестового покриття	+	=	=	=	=	=	=
Розробник повинен подати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування	+	=	=	=	=	=	=
Розробник повинен усунути або нейтралізувати всі знайдені «слабкі місця» і виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові «слабкі місця»	-	+	=	=	=	=	=
Розробник повинен виконати тести з подолання механізмів захисту і довести, що КЗЗ відносно або абсолютно стійкий до такого роду атак з боку Розробника	-	-	-	+	=	+	=

Вимоги до випробувань визначають такі основні елементи планування і проведення випробувань розробником:

- план випробувань;
- програма і методика випробувань;
- результати випробувань (журнал випробувань, звіт, протокол випробувань).

В *плані випробувань* повинна бути викладена стратегія випробувань розробника. План повинен надавати детальний опис всіх тестованих частин КЗЗ. Сюди входять: зовнішні інтерфейси КЗЗ; всі політики, привілеї, механізми послуг захисту і специфічних викликів системних функцій, бібліотечного ПЗ і т.ін.

8 Управління комплексною системою захисту інформації в ІТС

Для нейтралізації існуючих загроз і забезпечення інформаційної безпеки в ІТС організовують **систему управління КСЗІ**, у рамках якої проводять роботу за декількома напрямами:

- формування і практична реалізація комплексної багаторівневої політики інформаційної безпеки ІТС і системи внутрішніх вимог, норм і правил;
- організація служби інформаційної безпеки;
- розробка системи заходів і дій на випадок виникнення непередбачених ситуацій («управління інцидентами»);
- проведення аудитів (комплексних перевірок) стану інформаційної безпеки в організації.

Кожен з цих напрямів організаційної роботи має свої особливості і повинен реалізовуватися з використанням специфічних методів управління і відповідно до своїх правил.

8.1 Призначення, структура і зміст управління КСЗІ

Управління – це:

- елемент, функція організованих систем різної природи, що забезпечує збереження їх певної структури, підтримку режиму діяльності, реалізацію програми, цілей діяльності;
- процес здійснення інформаційних впливів на об'єкти управління для формування їх целенаправленного поведінка;
- процес планування, організації, мотивації і контролю, необхідний для того, щоб сформулювати і досягти мети організації;
- функція системи управління, що забезпечує організацію целенаправленої діяльності керованої системи.

Сенс і мета управління в КСЗІ – такі зміни організаційної структури, сил і засобів захисту інформації, їх стану, методів і способів застосування, які забезпечують максимальну ефективність їх застосування для досягнення цілей

ється технічними засобами. Паспорти призначено для ознайомлення з відомостями про інформацію, що підлягає захисту від витоку технічними каналами; ознайомлення з проектними і технічними рішеннями, що реалізовані у комплексі ТЗІ; встановлення правил експлуатації; відображення відомостей про технічне обслуговування комплексу, його основні характеристики, планові перевірки, атестації, а також про ремонт та утилізацію.

Контрольні питання

1. Що є етапом випробувань і атестації комплексу ТЗІ?
2. У чому полягає зміст висновків за результатами випробувань комплексу ТЗІ?
3. Визначите склад Програми і методики випробувань комплексу ТЗІ.
4. Що є атестація комплексу ТЗІ? Які існують види атестації?
5. Визначите етапи атестації комплексу ТЗІ.
6. Що містить Акт атестації комплексу ТЗІ?
7. Визначите порядок організації і проведення атестації комплексу ТЗІ.
8. Яку роль грає паспорт на комплекс ТЗІ і для чого він призначений?
9. З яких розділів складається Паспорт на комплекс ТЗІ?
10. Що в себе включає Паспорт на ОІД?

План має також відображати середовище випробувань, будь-які особливі умови, що створюються для проведення випробувань, і засоби випробувань. Повинні бути наведені аргументи на користь повноти тестового покриття.

Програма і методика випробувань повинна визначати процедури тестування кожного елемента, визначеного у плані випробувань (наприклад, системних викликів).

Для кожного окремого тесту має бути докладно описано використання засобів випробувань, необхідне оточення і особливі умови. Рівень деталізації процедур випробувань має бути достатнім для наступного повторення випробувань експертною комісією. Розробник повинен також описати очікувані результати кожного тесту.

Висновки

1. Нормативний документ НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу установлює критерії оцінки захищеності інформації, оброблюваної в ІТС, від НСД. Критерії є методологічною базою для визначення вимог з захисту інформації в ІТС від НСД у процесі створення захищених ІТС і засобів захисту від НСД та оцінки захищеності інформації в ІТС і їх придатності для обробки інформації, що вимагає захисту.
2. Критерії надають порівняльну шкалу для оцінки надійності механізмів захисту інформації від НСД, реалізованих в ІТС; базу (орієнтири) для розробки ІТС, в яких мають бути реалізовані функції захисту інформації.
3. В процесі оцінки спроможності ІТС забезпечувати захист оброблюваної інформації від НСД розглядаються вимоги двох видів: вимоги до функцій захисту (послуг безпеки); вимоги до гарантій. ІТС розглядається як набір функціональних послуг. Кожна послуга – це 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.

4. Функціональні критерії дозволяють оцінити наявність послуг безпеки в ІТС і розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів: конфіденційність, цілісність, доступність, спостереженість.

5. Критерії гарантій дозволяють оцінити коректність реалізації послуг і включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування, експлуатаційної документації.

Контрольні питання

1. Які види критеріїв визначаються в НД ТЗІ2.5-004-99?
2. Що визначають рівні кожної послуги?
3. Що є рейтингом послуг захисту інформації, що надаються, в ІТС від НСД?
4. Поясніть структуру критеріїв конфіденційності.
5. Що означають критерії довірчої та адміністративної конфіденційності?
6. Що означає критерій аналізу прихованих каналів?
7. Поясніть структуру критеріїв цілісності.
8. Що означає критерій відкату?
9. Поясніть структуру критеріїв доступності.
10. Що означає критерій гарячої заміни?
11. Поясніть структуру критеріїв спостереженості.
12. Що означає критерій реєстрації?
13. Що означає критерій достовірного каналу?
14. Що означає критерій ідентифікації та автентифікації?
15. Поясніть структуру критеріїв гарантій.
16. Який сенс критеріїв гарантій середовища розробки?
17. Який сенс критеріїв гарантій послідовності розробки?
18. Який сенс критеріїв гарантій випробувань КЗЗ?

тися для тривалого перехоплення оброблюваної ІзОД, а також найменших відстаней від технічних засобів, що оброблятимуть інформацію, до межі контрольованої зони тощо;

- дані про технічні характеристики складових комплексу ТЗІ (у разі необхідності розгортання, доповнення або окремого наведення, ці дані оформляють у вигляді табл. 2.34).

3. Відомості про проведені роботи з ТЗІ під час експлуатації приміщення – тут наводять:

- облік робіт, що виконано під час експлуатації комплексу ТЗІ у приміщенні (записи про зазначені роботи наводять у вигляді табл. 2.36, 2.37);

- періодичні, інші перевірки стану комплексу ТЗІ та правильності ведення паспорта (реєструються за формою табл. 2.38, 2.39);

- проведену перевірку засобів вимірювальної техніки (реєструється за формою табл. 2.40).

Висновки

1. Етап «Випробування та атестація комплексу ТЗІ» передбачає затвердження програм і методик випробувань; проведення випробувань, оформлення протоколів випробувань; підготовку висновків за результатами випробувань комплексу ТЗІ; підготовку пропозицій і вимог до вибору рішень щодо впровадження необхідних заходів із захисту ІзОД на ОІД; проведення атестації комплексу ТЗІ, оформлення протоколів, актів атестації; заповнення паспорта на комплекс ТЗІ.

2. Атестація комплексу ТЗІ проводиться з метою визначення відповідності вимогам НД з питань ТЗІ виконаних робіт зі створення комплексу ТЗІ на ОІД та повноти проведених випробувань. Вимоги щодо проведення атестації мають бути передбачені у технічному завданні на створення комплексу ТЗІ.

3. Основним експлуатаційним документом на комплекс ТЗІ є паспорт і його складові – паспорти на приміщення, де ІзОД озвучується та/або обробля-

відноситься, відомості про його дислокацію;

Ступінь обмеження доступу
Прим. №

ЗАТВЕРДЖЕНО
Керівник установи-замовника
_____
____. ____. 20____

Паспорт
на приміщення, де інформація з обмеженим доступом озвучується та/або обробляється технічними засобами (складова частина паспорта на комплекс ТЗІ)

(*назва, призначення приміщення*)

(*назва підрозділу установи, що заявляв створення комплексу ТЗІ*)

Документ підписують:
– керівник підрозділу установи, що заявляв створення комплексу ТЗІ;
– посадова особа, призначена для організації експлуатації комплексу ТЗІ.

Рис. 2.32 Форма титульного аркуша паспорта на приміщення, де інформація з обмеженим доступом озвучується та/або обробляється технічними засобами

- план приміщення, план розміщення пристроїв зв'язку, кабельних і телекомунікаційних мереж, інженерних комунікацій та координати точок із властивостями нелінійності, план-схеми або опис затвердженої контрольованої зони, зон безпеки інформації стосовно кожного технічного каналу її витоку;

- загальний опис приміщення, інженерних комунікацій та інші відомості; характеристику приміщення: його розташування в будинку, споруді (поверх, архітектурні осі, ряди); інформацію про суміжні приміщення (у т.ч. поверхом вище і нижче); особливості розташування вікон, дверей, інших будівельних отворів;

- витяг із затвердженої моделі загроз для ІзОД (або посилання на модель загроз), у т.ч. щодо даних про можливі місця розміщення засобів технічної розвідки (стаціонарних або автономних автоматичних), що можуть використовува-

4 Особливості проектування КСЗІ для ІТС різних класів

НД ТЗІ 2.5-005 – 99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу установлює принципи класифікації ІТС і утворення стандартних функціональних профілів захищеності оброблюваної у них інформації від НСД.

4.1 Класифікація інформаційно-телекомунікаційних (автоматизованих) систем

Мета введення класифікації ІТС і стандартних функціональних профілів захищеності – це полегшення задачі співставлення вимог до КЗЗ обчислювальної системи ІТС з характеристиками ІТС, яка є організаційно-технічною системою, що об'єднує обчислювальну систему, телекомунікаційну систему, фізичне середовище, персонал та інформацію (що зберігається, оброблюється і передається).

Вимоги до функціонального складу КЗЗ залежать від характеристик оброблюваної інформації, самої ІТС, фізичного середовища, персоналу та організаційної підсистеми.

Вимоги до гарантій визначаються насамперед характером (важливістю) оброблюваної інформації і призначенням ІТС.

За сукупністю характеристик ІТС (конфігурація апаратних засобів ІТС та їх фізичне розміщення, кількість різноманітних ступенів обмеження доступу оброблюваної інформації, кількість користувачів і повноважень користувачів) виділяють три ієрархічні класи ІТС, вимоги до функціонального складу КЗЗ яких істотно відрізняються (табл. 2.28).

Таблиця 2.28 Характеристика класів ІТС

Клас ІТС	Визначення та істотні особливості	Приклад
«1»	**Одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох ступенів обмеження доступу.**	**Автономна персональна ЕОМ**, доступ до якої контролюється з

	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; - користувачі можуть мати різні повноваження (права) щодо доступу до інформації, яка обробляється.	використанням організаційних заходів
«2»	**Локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.** **Істотна відміна від попереднього класу:** - наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних ступенів обмеження доступу.	**Локальна обчислювальна мережа (ЛОМ)**
«3»	**Розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.** **Істотна відміна від попереднього класу:** - необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.	**Глобальна комп'ютерна мережа (ГКМ)**

В межах кожного класу ІТС класифікуються на підставі вимог до забезпечення безпеки певних властивостей інформації. З точки зору безпеки інформація характеризується трьома властивостями: конфіденційністю, цілісністю, доступністю. В зв'язку з цим, в кожному класі ІТС виділяються підкласи (рис. 2.13).

Рис. 2.13 Підкласи ІТС залежно від властивостей інформації, що захищаються

Тут **х** означає клас ІТС (відповідно до табл. 2.28), а після крапки перераховуються властивості, що захищаються.

Для кожного з підкласів кожного класу вводиться деяка кількість ієрархічних стандартних функціональних профілів, яка може бути різною для кожного

Таблиця 2.39

Дата, тема періодичного контролю стану технічних характеристик, підстави для контролю (посилання на пункти табл. 2.34)	Результати контролю	Посади, прізвища, підписи виконавців контролю	Відмітка про усунення недоліків
1	2	3	4

Таблиця 2.40

Дата	Вид перевірки	Результати перевірки	Прізвища і підписи осіб, що перевіряють	Відмітка про усунення недоліків
1	2	3	4	5

- дані щодо повірки засобів вимірювань (містить перелік засобів вимірювань, які підлягають періодичній повірці, із зазначенням їх заводських номерів, періодичності повірки та дати проведення повірок). Підрозділ вводиться у разі наявності засобів вимірювань у складі комплексу ТЗІ. Відомості щодо повірки засобів вимірювань наводять у вигляді табл. 2.41;

Таблиця 2.41

Найменування та позначення засобів вимірювання	Заводський номер	Дата виготовлення	Періодичність повірки	Дата повірки (термін чергової повірки)	Примітка
1	2	3	4	5	6

- дані про інспекційні перевірки.

8. Розділ **«Особливі відмітки»** містить декілька чистих аркушів для записів, що можуть бути здійснені під час експлуатації комплексу ТЗІ.

9. До **додатків** (за необхідності) додають паспорти на кожне приміщення, де циркулює інформація з обмеженим доступом.

Паспорт на приміщення, де ІзОД озвучується та/або обробляється технічними засобами (як складова частина технічного паспорта на комплекс ТЗІ), має титульний аркуш (рис. 2.32) і містить такі розділи:

1. Загальні вказівки – містить вказівки щодо експлуатації комплексу ТЗІ в конкретному приміщенні, заповнення і ведення паспорта.

2. Технічні характеристики приміщення – містить:

- назву приміщення і структурного підрозділу в установі, до якого воно

Таблиця 2.35

Перелік висновків про результати випробувань	Дата	Виконавець проведення випробувань	Примітка
1	2	3	4

6. Розділ **«Облік технічного обслуговування»** складають у разі, якщо такі види робіт передбачені. У розділі наводять:

- відомості про технічне обслуговування комплексу ТЗІ, його види;
- дату проведення технічного обслуговування;
- відомості про виконавців технічного обслуговування.

Зазначені відомості наводять у вигляді табл. 2.36.

Таблиця 2.36

Дата	Вид технічного обслуговування	Напрацювання		Підстава (найменування, номер і дата документа)	Установа, посада, прізвище і підпис		Примітка
		з початку експлуатації	після останнього ремонту		хто виконав роботу	хто перевірив виконання роботи	
1	2	3	4	5	6	7	8

7. У розділі **«Відомості про проведені роботи під час експлуатації комплексу ТЗІ»** наводять:

- облік робіт, що виконано під час експлуатації комплексу ТЗІ на ОІД (містить записи про незаплановані роботи з усунення відмов під час експлуатації, перевірку відсутності закладних пристроїв тощо) (записи про ці роботи наводять у вигляді табл. 2.37, 2.38);

Таблиця 2.37

Дата	Найменування роботи і причина її виконання	Посада, прізвище і підпис		Примітка
		роботу виконав	перевірив виконання роботи	
1	2	3	4	5

Таблиця 2.38

Періодичний контроль відсутності закладних пристроїв, підстава для контролю	Дата	Посада, прізвище, підпис виконавців контролю	Відмітка про усунення недоліків
1	2	3	4

- періодичні та інші перевірки стану комплексу ТЗІ та правильності ведення паспорта (реєструються за формою табл. 2.39, 2.40);

класу і підкласу ІТС.

Профілі є ієрархічними в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (конфіденційності, цілісності і доступності).

Наростання ступеня захищеності може досягатись:

- підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги;
- включенням до профілю нових послуг.

Така класифікація корисна для полегшення вибору переліку функцій, які повинен реалізовувати КЗЗ проектованої або існуючої ІТС.

Цей підхід дозволяє мінімізувати витрати на початкових етапах створення КСЗІ ІТС. Проте слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної ІТС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

4.2 Функціональні профілі захищеності ІТС

Стандартний функціональний профіль захищеності – це перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи ІТС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній ІТС.

Стандартні функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються.

Єдина вимога, якої слід дотримуватися при утворенні нових профілів, – це додержання описаних в **НД ТЗІ 2.5-004-99** необхідних умов для кожної із послуг, що включаються до профілю.

Опис профілю складається з трьох частин:

- буквено-числового ідентифікатора;
- знака рівності;

- переліку рівнів послуг, взятого в фігурні дужки.

Ідентифікатор = {Перелік рівнів послуг}

Ідентифікатор, у свою чергу, включає:

- позначення класу ІТС (**1**, **2** або **3**);
- буквену частину, що характеризує види загроз, від яких забезпечується захист (**К**, і/або **Ц**, і/або **Д**);
- номер профілю;
- необов'язкове буквене позначення версії.

Всі частини ідентифікатора відділяються один від одного крапкою.

Наприклад, **2.К.4** – функціональний профіль номер чотири, що визначає вимоги до ІТС класу 2, призначених для обробки інформації, основною вимогою щодо захисту якої є забезпечення конфіденційності;

3.КЦД.1 – функціональний профіль номер один, що визначає вимоги до ІТС класу 3, призначених для обробки інформації, вимогами щодо захисту якої є забезпечення конфіденційності, цілісності та доступності.

Версія може служити, зокрема, для вказівки на підсилення певної послуги всередині профілю. Наприклад, нарощування можливостей реєстрації приведе до появи нової версії. Тим не менше, при внесенні деяких істотних змін, особливо додання нових послуг, може або привести до появи нового профілю, або до того, що профіль буде відноситись до іншого класу чи підкласу ІТС.

4.3 Особливості стандартних функціональних профілів захищеності ІТС

Стандартні функціональні профілі захищеності для ІТС класу 1

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 1, головною вимогою до яких є *забезпечення конфіденційності* оброблюваної інформації:

1.К.1 = {НР-1, НИ-1, НК-1, НО-1, НЦ-1, НТ-1}

1.К.2 = {КА-1, КО-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1}

обладнання, систем зв'язку, радіофікації, телебачення, сигналізації, автоматизації, керування, заземлення, електро, газо, водопостачання, опалення, вентиляції, кондиціонування повітря, водостоку, каналізації, огороджувальних будівельних конструкцій тощо.

3. У розділі **«Технічні характеристики комплексу ТЗІ»** наводять перелік технічних засобів як складових комплексу ТЗІ, що можуть впливати на ефективність захищеності інформації і бути середовищем поширення носіїв інформації, та їх технічні характеристики (табл. 2.34)

Таблиця 2.34

Технічна характеристика (параметр)	Номінальне значення параметра відповідно до норм, вимог	Значення параметра під час випробування комплексу	Значення параметра під час експлуатації комплексу ТЗІ			
			За результатами контролю	Вид контролю	Дата	Посада, прізвище, підпис, висновки
1	2	3	4	5	6	7

4. Розділ **«Гарантії»** складають у разі наявності відповідних зобов'язань розробника технічних засобів або виконавця впровадження заходів із захисту інформації щодо гарантійних термінів. Наводять пропозиції щодо терміну проведення чергової атестації.

5. У розділі **«Відомості про випробування і атестацію комплексу ТЗІ»** наводять:

- види інформації, стосовно яких проводили випробування і атестацію комплексу ТЗІ;
- терміни проведення випробування та атестації комплексу ТЗІ, їх виконавці;
- дані про протоколи випробування та акти атестації комплексу ТЗІ (назви документів, їх склад, реквізити, реєстраційні номери, місце зберігання, короткі витяги з них);
- терміни проведення чергової атестації і відповідних випробувань.

Висновки про результати випробувань наводять у вигляді табл. 2.35.

до нього зміни, при цьому у записах не допускається проводити підчищення, попередній запис має бути закреслений і поруч зроблено новий, що завіряється встановленим порядком.

2. У розділі **«Загальні відомості»** наводять:

- назву та дислокацію підрозділу, що замовляв створення комплексуТЗІ;
- відомості про інформацію з обмеженим доступом (табл. 2.33);

Таблиця 2.33

Характеристика ІзОД (умови озвучення, засоби оброблення тощо)	Найменування приміщень, де ІзОД озвучується та/або обробляється технічними засобами тощо	Ступінь обмеження доступу до інформації
1	2	3

- витяг із затвердженого керівником установи рішення (наказу, розпорядження) щодо створення комплексу ТЗІ на ОІД, у т.ч. інформацію про посаду та прізвище відповідальної особи, що призначена керівником установи для організації, супроводження та координації робіт на всіх етапах створення комплексу ТЗІ;
- дані про акт обстеження на ОІД, модель загроз для ІзОД, приписи на експлуатацію засобів оброблення інформації, технічні вимоги, завдання щодо створення комплексу ТЗІ, розроблену проектно-кошторисну документацію тощо, дані про їх склад, реквізити, реєстраційні номери, місце зберігання, короткі витяги (у разі необхідності) з них;
- опис конструкцій ОІД, де створено комплекс ТЗІ, а саме: будинків, споруд, салонів транспортних засобів тощо (конструкція та матеріали стін, перекриттів, вікон, дверей, інженерних комунікацій тощо), їх особливості;
- перелік технічних засобів, що обробляють ІзОД, а також засобів забезпечення ТЗІ (вказують інвентарні номери і дані про наявність сертифікатів або експертних висновків з ТЗІ);
- відомості про виконані випробування (у т.ч. спеціальні дослідження технічних засобів, які обробляють ІзОД). Назви документів, їх склад, реквізити, реєстраційні номери, місце зберігання, короткі витяги з них;
- місця виходу за межі контрольованої зони елементів технологічного

Наприклад, реалізація профілю захищеності номер два вимагає, щоб КЗЗ задовольняв наступним критеріям:

- **КА-1** – мінімальна адміністративна конфіденційність;
- **КО-1** – повторне використання об'єктів;
- **НР-2** – захищений журнал;
- **НИ-2** – одиночна ідентифікація і автентифікація;
- **НК-1** – однонаправлений достовірній канал;
- **НО-1** – виділення адміністратора;
- **НЦ-1** – КЗЗ з контролем цілісності;
- **НТ-1** – самотестування за запитом.

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 1, головною вимогою до яких є *забезпечення цілісності* оброблюваної інформації:

1.Ц.1 = {НР-1, НИ-1, НК-1, НО-1, НЦ-1, НТ-1}

1.Ц.2 = {ЦА-2, ЦО-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1}

Стандарті функціональні профілі захищеності в КС, що входять до складу ІТС класу 1, головною вимогою до яких є *забезпечення доступності* оброблюваної інформації:

1.Д.1 = {ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1}

1.Д.2 = {ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2}

1.Д.3 = {ДР-2, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-1, НЦ-2, НТ-2}

1.Д.4 = {ДР-2, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-1, НЦ-2, НТ-2}

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 1, з підвищеними вимогами до *забезпечення конфіденційності та цілісності* оброблюваної інформації:

1.КЦ.1 = {НР-1, НИ-1, НК-1, НО-1, НЦ-1, НТ-1}

1.КЦ.2 = {КА-1, КО-1, ЦА-2, ЦО-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1}

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 1, з підвищеними вимогами до *забезпечення конфіденційності та доступності* оброблюваної інформації:

1.КД.1 = {КА-1, КО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1}

1.КД.2 = {КА-1, КО-1, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2}

1.КД.3 = {КА-1, КО-1, ДР-2, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-1, НЦ-2, НТ-2}

1.КД.4 = {КА-1, КО-1, ДР-2, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-1, НЦ-2, НТ-2}

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 1, з підвищеними вимогами до *забезпечення цілісності та доступності* інформації:

1.ЦД.1 = {ЦА-1, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1}

1.ЦД.2 = {ЦА-1, ЦО-1, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2}

1.ЦД.3 = {ЦА-1, ЦО-1, ДР-2, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-1, НЦ-2, НТ-2}

1.ЦД.4 = {ЦА-1, ЦО-1, ДР-2, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-1, НЦ-2, НТ-2}

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 1, з підвищеними вимогами до *забезпечення конфіденційності, цілісності та доступності* інформації:

1.КЦД.1 = {КА-1, КО-1, ЦА-1, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1}

1.КЦД.2 = {КА-1, КО-1, ЦА-1, ЦО-1, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2}

1.КЦД.3 = {КА-1, КО-1, ЦА-1, ЦО-1, ДР-2, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-1, НЦ-2, НТ-2}

1.КЦД.4 = {КА-1, КО-1, ЦА-1, ЦО-1, ДР-2, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-1, НЦ-2, НТ-2}

Стандартні функціональні профілі захищеності для ІТС класу 2

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 2, головною вимогою до яких є *забезпечення конфіденційності* оброблюваної інформації:

2.К.1 = {КД-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1}

2.К.2 = {КД-2, КО-1, НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1}

2.К.3 = {КД-2, КА-2, КО-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2}

2.К.4 = {КД-2, КА-2, КО-1, КК-1, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2}

2.К.5 = {КД-3, КА-3, КО-1, КК-1, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2}

2.К.6 = {КД-4, КА-4, КО-1, КК-2, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2}

Паспорти затверджує керівник установи-замовника. Кожен паспорт повинен мати окремий обліковий (інвентарний, архівний) номер.

Паспорт на комплекс ТЗІ включає розділи, наведені на рис. 2..30 і має титульний аркуш (рис. 2.31).

Ступінь обмеження доступу
Прим. №

ЗАТВЕРДЖЕНО
Керівник установи-замовника

____. ____. 20____

Паспорт
на комплекс технічного захисту інформації

(*назва, належність ОІД, на якому розташований комплекс ТЗІ*)

(*назва підрозділів установи, що заявляли створення комплексу ТЗІ*)

Документ підписують:
– керівник підрозділу установи, що заявляв створення комплексу ТЗІ;
– посадова особа, призначена для організації експлуатації комплексу ТЗІ;
– представник від підрозділу, якому доручено організацію і супроводження робіт з ТЗІ в установі;
– інші особи ознайомлені з паспортом, у частині, що їх стосується.

Рис. 2.31 Форма титульного аркуша паспорта на комплекс ТЗІ

1. Розділ **«Загальні вказівки»** містить вказівки щодо експлуатації комплексу ТЗІ на ОІД та заповнення і ведення паспорта. Зокрема у цьому розділі має бути зазначено:

- фаховий рівень посадової особи, яка організовує експлуатацію комплексу ТЗІ на ОІД;
- порядок заміни обладнання, проведення ремонтних робіт на ОІД, внесення змін до паспорта на комплекс ТЗІ;
- порядок використання радіотелефонів, кінцевих пристроїв рухомого (мобільного, сотового, пейджингового, транкінгового тощо) зв'язку.

Затверджений паспорт на комплекс ТЗІ допускається коригувати, вносити

7.3 Порядок розроблення та оформлення паспорта на комплекс ТЗІ

Основним експлуатаційним документом на комплекс ТЗІ є **паспорт** і його складові – паспорти на приміщення, де ІзОД озвучується та/або обробляється технічними засобами. Паспорти призначено для:

- ознайомлення з відомостями про інформацію, що підлягає захисту від витоку технічними каналами;
- ознайомлення з проектними і технічними рішеннями, що реалізовані у комплексі ТЗІ;
- встановлення правил експлуатації (використання за призначенням, технічне обслуговування, перевірки основних характеристик, ремонт, перевірки за умови виявлення порушень правил експлуатації приміщення та технічних засобів, а також у разі порушення пломб на технічних засобах та засобах захисту тощо);
- відображення відомостей про технічне обслуговування комплексу, його основні характеристики (визначені під час приймання комплексу), планові перевірки, атестації, а також про ремонт та утилізацію.

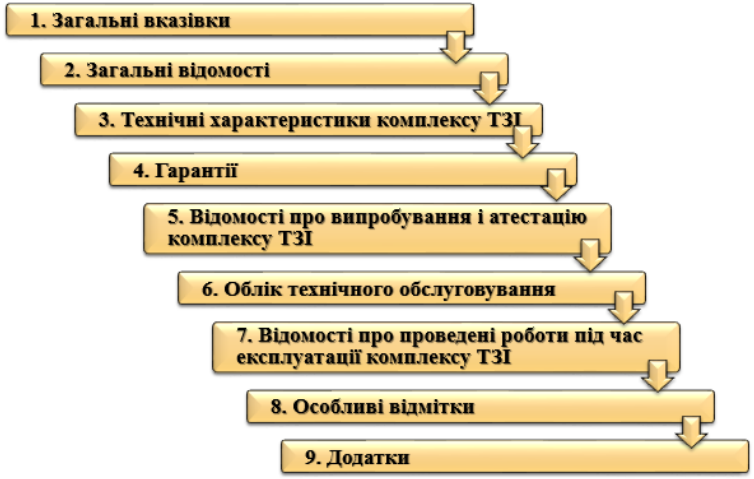

Рис. 2.30 Структура паспорта на комплекс ТЗІ

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 2, головною вимогою до яких є *забезпечення цілісності* оброблюваної інформації:

2.Ц.1 = {ЦД-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1}

2.Ц.2 = {ЦД-1, ЦО-1, НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1}

2.Ц.3 = {ЦД-1, ЦА-2, ЦО-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2}

2.Ц.4 = {КО-1, ЦД-1, ЦА-3, ЦО-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2}

2.Ц.5 = {КО-1, ЦД-4, ЦА-4, ЦО-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2}

Стандарті функціональні профілі захищеності в КС, що входять до складу ІТС класу 2, головною вимогою до яких є *забезпечення доступності* оброблюваної інформації:

2.Д.1 = {ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1}

2.Д.2 = {ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2}

2.Д.3 = {ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-1, НЦ-2, НТ-2}

2.Д.4 = {ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-1, НЦ-2, НТ-2}

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 2, з підвищеними вимогами до *забезпечення конфіденційності та цілісності* оброблюваної інформації:

2.КЦ.1 = {КД-2, ЦД-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1}

2.КЦ.2 = {КД-2, КО-1, ЦД-1, ЦО-1, НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1}

2.КЦ.3 = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2}

2.КЦ.4 = {КД-2, КА-2, КО-1, КК-1, ЦД-1, ЦА-2, ЦО-1, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2}

2.КЦ.5 = {КД-3, КА-3, КО-1, КК-1, ЦД-1, ЦА-3, ЦО-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2}

2.КЦ.6 = {КД-4, КА-4, КО-1, КК-2, ЦД-4, ЦА-4, ЦО-2, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2}

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 2, з підвищеними вимогами до забезпечення *конфіденційності та доступності* оброблюваної інформації:

2.КД.1 = {КД-2, КА-2, КО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2}

2.КД.2 = {КД-2, КА-2, КО-1, КК-1, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2}

2.КД.3 = {КД-3, КА-3, КО-1, КК-1, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2}

2.КД.4 = {КД-4, КА-4, КО-1, КК-2, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2}

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 2, з підвищеними вимогами до забезпечення *цілісності та доступності* інформації:

2.ЦД.1 = {ЦД-1, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1}

2.ЦД.2 = {ЦД-1, ЦА-2, ЦО-1, ДР-2, ДС-1, ДЗ-1, ДВ-2,НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2}

2.ЦД.3 = {КО-1, ЦД-1, ЦА-3, ЦО-2, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2}

2.ЦД.4 = {КО-1, ЦД-4, ЦА-4, ЦО-2, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2}

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 2, з підвищеними вимогами до забезпечення *конфіденційності, цілісності та доступності* інформації:

2.КЦД.1 = {КД-2, КО-1, ЦД-1, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2}

2.КЦД.2 = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2}

2.КЦД.3 = {КД-2, КА-2, КО-1, КК-1, ЦД-1, ЦА-3, ЦО-2, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2}

2.КЦД.4 = {КД-3, КА-3, КО-1, КК-1, ЦД-1, ЦА-3, ЦО-2, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2}

2.КЦД.5 = {КД-4, КА-4, КО-1, КК-2, ЦД-4, ЦА-4, ЦО-2, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2}

Стандартні функціональні профілі захищеності для ІТС класу 3

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 3, головною вимогою до яких є *забезпечення конфіденційності* оброблюваної інформації:

3.К.1 = {КД-2, КВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НВ-1}

3.К.2 = {КД-2, КО-1, КВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1, НВ-1}

3.К.3 = {КД-2, КА-2, КО-1, КВ-2, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}

До акту атестації додаються протоколи випробувань, передбачених ПМА. За результатами атестації заповнюється технічний паспорт на комплекс ТЗІ (**НД ТЗІ 3.3-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації**).

У разі незгоди з результатами атестації організація-замовник має право направити до Державної служби спеціального зв'язку та захисту інформації України апеляцію. Держслужба у місячний термін за апеляцією приймає відповідні рішення.

Гриф обмеження доступу
(за необхідності)

_____

повна назва організації-виконавця

АКТ АТЕСТАЦІЇ
комплексу технічного захисту інформації
(позначення об'єкта інформаційної діяльності, на якому розташований комплекс, повна назва організації-замовника)

№_____ «____» _____ 20__ р.

Дійсний до «____» _____ 20__ р.

Період проведення атестації.

Підстави для проведення атестації (документ щодо залучення організації-виконавця, повна назва Програми і методик атестації з реквізитами, ким погоджено, затверджено).

Короткі відомості про об'єкт інформаційної діяльності та комплекс технічного захисту інформації.

Виклад результатів випробувань (за окремими пунктами Програми і методик атестації).

Зауваження і рекомендації.

Додаткові умови, яких необхідно дотримуватись під час експлуатації (відмінні відносно передбачених експлуатаційною документацією, за необхідності).

Висновки щодо відповідності комплексу технічного захисту інформації вимогам нормативних документів.

Строк проведення чергової атестації.

Перелік додатків (протоколи випробувань та інші матеріали, що були оформлені під час проведення атестації).

Керівник організації-виконавця

_____

підпис, ініціали, прізвище

«____»_____20__ р.

Рис. 2.29 Форма та зміст Акту атестацій комплексу ТЗІ

Узгоджений організацією-замовником проект ПМА затверджує організація-виконавець.

3. Організація-замовник створює умови проведення атестації, передбачені договором та ПМА.

Перелік відомостей
про об'єкти інформаційної діяльності та комплекси технічного захисту інформації

Гриф обмеження доступу
(за необхідності)

1 Відомості про ОІД (по кожному ОІД окремо): найменування, позначення, розташування, приналежність відповідному підрозділу тощо.
2 Технологічні процеси під час функціонування ОІД із визначенням інформації, що підлягає захисту від витоку технічними каналами. Ступінь обмеження доступу до інформації.
3 Схеми затверджених контрольованих зон, їх опис.
4 Перелік технічних засобів (основних і допоміжних), розташованих в межах контрольованих зон, та відомості про їх елементи, що перетинають цю межу.
5 Зовнішні фактори, які можуть спричинити виникнення загроз для інформації.
6 Організаційна структура забезпечення захисту інформації на об'єкті.
7 Короткі відомості про комплекс ТЗІ на ОІД:
- про категоріювання вимог із захищеності інформації;
- можливі технічні канали витоку інформації;
- склад комплексу ТЗІ та схема розміщення його елементів;
- перелік експлуатаційних документів на комплекс ТЗІ.
8 Розробник комплексу ТЗІ.
9 Проектувальник та виконавець будівельно-монтажних робіт, які проводилися на забезпечення впровадження комплексу ТЗІ.
10 Виконавець робіт з ТЗІ.
11.Відомості про приймання робіт із створення комплексу ТЗІ.
12 Строк проведення та висновки попередньої атестації.
13 Підстави для проведення атестації.

Керівник організації-замовника _____
підпис, ініціали, прізвище

Рис. 2.28 Форма переліку відомостей про ОІД та комплекси ТЗІ

4. Організація-виконавець проводить випробування відповідно до ПМА та оформляє акт атестації комплексу ТЗІ (форма акту – на рис. 2.29) у 2-х примірниках (1-й надається організації-замовнику, 2-й – зберігається у організації-виконавця), який затверджує керівник установи-виконавця атестації.

3.К.4 = {КД-2, КА-2, КО-1, КК-1, КВ-3, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2}

3.К.5 = {КД-3, КА-3, КО-1, КК-1, КВ-4, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-2}

3.К.6 = {КД-4, КА-4, КО-1, КК-2, КВ-4, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2, НВ-2, НА-1}

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 3, головною вимогою до яких є *забезпечення цілісності* оброблюваної інформації:

3.Ц.1 = {ЦД-1, ЦВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НВ-1}

3.Ц.2 = {ЦД-1, ЦО-1, ЦВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1, НВ-1}

3.Ц.3 = {ЦД-1, ЦА-2, ЦО-1, ЦВ-2, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-2, НА-1}

3.Ц.4 = {КО-1, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2, НА-1, НП-1}

3.Ц.5 = {КО-1, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-3, НА-2, НП-2}

Стандарті функціональні профілі захищеності в КС, що входять до складу ІТС класу 3, головною вимогою до яких є *забезпечення доступності* оброблюваної інформації:

3.Д.1 = {ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1, НВ-1}

3.Д.2 = {ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2, НВ-1}

3.Д.3 = {ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-1, НЦ-2, НТ-2, НВ-1}

3.Д.4 = {ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-1, НЦ-2, НТ-2, НВ-1}

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 3, з підвищеними вимогами до *забезпечення конфіденційності та цілісності* оброблюваної інформації:

3.КЦ.1 = {КД-2, КВ-1, ЦД-1, ЦВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НВ-1}

3.КЦ.2 = {КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1, НВ-1}

3.КЦ.3 = {КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}

3.КЦ.4 = {КД-2, КА-2, КО-1, КК-1, КВ-3, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2}

3.КЦ.5 = {КД-3, КА-3, КО-1, КК-1, КВ-3, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1}

3.КЦ.6 = {КД-4, КА-4, КО-1, КК-2, КВ-4, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, НР-5, НИ-2, НК-2,

НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1}

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 3, з підвищеними вимогами до *забезпечення конфіденційності та доступності* оброблюваної інформації:

3.КД.1 = {КД-2, КА-2, КО-1, КВ-2, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}

3.КД.2 = {КД-2, КА-2, КО-1, КК-1, КВ-3, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2}

3.КД.3 = {КД-3, КА-3, КО-1, КК-1, КВ-4, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-2}

3.КД.4 = {КД-4, КА-4, КО-1, КК-2, КВ-4, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2, НВ-2, НА-1}

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 3, з підвищеними вимогами до *забезпечення цілісності та доступності* інформації:

3.ЦД.1 = {ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1, НВ-1}

3.ЦД.2 = {ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-2, НА-1}

3.ЦД.3={КО-1, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2, НА-1, НП-1}

3.ЦД.4={КО-1, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-3, НА-2, НП-2}

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС класу 3, з підвищеними вимогами до *забезпечення конфіденційності, цілісності та доступності* інформації:

3.КЦД.1 = {КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}

3.КЦД.2 = {КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}

3.КЦД.3 = {КД-2, КА-2, КО-1, КК-1, КВ-3, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2}

3.КЦД.4 = {КД-3, КА-3, КО-1, КК-1, КВ-3, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1}

2) аналіз умов функціонування ОІД, технічної документації на комплекс ТЗІ, результатів випробувань;

3) аналіз та оцінка відповідності проектної, конструкторської, експлуатаційної та іншої технічної документації на комплекс ТЗІ вимогам НД з питань ТЗІ;

4) перевірка відповідності вихідних даних щодо створення комплексу ТЗІ реальним умовам розміщення ОІД;

5) перевірка складу комплексу ТЗІ на відповідність даним, зазначеним у проектній, конструкторській, експлуатаційній та іншій технічній документації;

6) перевірка наявності сертифікатів або експертних висновків на засоби забезпечення ТЗІ загального призначення;

7) перевірка відповідності монтажу та умов експлуатації засобів забезпечення ТЗІ вимогам експлуатаційної документації;

8) перевірка оформлення проекту паспорта на комплекс ТЗІ і паспорта на кожне приміщення;

9) розгляд висновків за результати випробувань;

10) оформлення підсумкового документа – **акта атестації комплексу ТЗІ**;

11) оформлення актів пломбування.

Порядок організації та проведення атестації

1. Організація-замовник визначає організацію-виконавця атестації. Організацією-виконавцем атестації може бути підприємство, установа чи організація, які мають відповідну ліцензію або дозвіл на провадження діяльності в галузі ТЗІ, одержані у встановленому законодавством порядку.

Відносини між організацією-замовником та організацією-виконавцем, яка є ліцензіатом, регламентуються укладеним між ними *договором*.

2. Організація-виконавець за результатами аналізу відомостей (рис. 2.28), наданих організацією-замовником, та, за необхідності, за результатами аналізу умов функціонування ОІД і загроз для інформації безпосередньо на ОІД, розробляє проект програми і методики атестації (ПМА) та подає його на узгодження організації-замовнику.

пройшов випробування.

За результатами випробувань складаються *протоколи*, де надаються висновки про відповідність вимогам нормативних документів з питань ТЗІ. Висновки повинні містити конкретні формулювання, що забезпечують їх однозначне трактування.

7. **Вимоги щодо забезпечення охорони державної таємниці та іншої інформації з обмеженим доступом**: вказують організаційні заходи, які мають бути проведені при виконанні робіт з випробувань.

7.2 Атестація комплексів захисту інформації

Атестація комплексу ТЗІ – це процес оцінювання ефективності комплексу технічного захисту інформації, який проводиться з *метою визначення відповідності вимогам НД з питань ТЗІ виконаних робіт зі створення комплексу ТЗІ на ОІД та повноти проведених випробувань*.

Атестація може проводитися окремо щодо кожного виду ІзОД, що підлягає технічному захисту (ІзОД, що озвучуватиметься та/або оброблятиметься технічними засобами, тощо). Вимоги щодо проведення атестації мають бути передбачені у ТЗ на створення комплексу ТЗІ.

До основних видів атестації відносяться:

- *первинна атестація* – здійснюється після (або під час) приймання робіт із створення комплексу ТЗІ;
- *чергова атестації* – термін її проведення визначається технічним паспортом на комплекс ТЗІ або актом попередньої атестації (строк дії акта атестації не повинен перевищувати два роки);
- *позачергова атестація* – проводиться у разі змін умов функціонування ОІД, що приводять до змін загроз для інформації, та за висновками органів, які контролюють стан ТЗІ.

Основні етапи атестації комплексу ТЗІ:

1) визначення організації-виконавця атестації та оформлення відповідних організаційних документів;

3.КЦД.5 = {КД-4, КА-4, КО-1, КК-2, КВ-4, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1}

Стандартні функціональні профілі захищеності в КС, що входять до складу ІТС, призначених для автоматизації діяльності органів державної влади

В ІТС, призначених для автоматизації діяльності органів державної влади, часто обробляється інформація з обмеженим доступом. Основними загрозами для інформації в таких системах є загрози, що призводять до несанкціонованого ознайомлення з інформацією, тобто *загрози* (*порушення*) *конфіденційності*.

У зв'язку з цим до КЗЗ ОС, що входять до складу ІТС, у першу чергу пред'являються вимоги щодо забезпечення конфіденційності оброблюваної інформації, персональної відповідальності користувачів за дотримання режиму секретності.

Політика безпеки, що реалізується, повинна відбивати встановлені в Україні правила роботи з секретними документами. Зокрема, механізми, що реалізують послугу **адміністративної конфіденційності**, повинні здійснювати *розмежування доступу на підставі грифів документів* (пасивних об'єктів) *і рівнів допуску користувачів*.

У зазначених ІТС рекомендується використовувати ОС, КЗЗ яких реалізують профілі **х.К.х**. Якщо, крім вимоги забезпечення конфіденційності, існують додаткові вимоги щодо забезпечення цілісності і/або доступності інформації, то рекомендується використовувати профілі **х.КЦ.х**, **х.КД.х**, **х.КЦД.х**.

Стандартні функціональні профілі захищеності КС, що входять до складу ІТС, які призначені для автоматизації банківської діяльності

Основні загрози для банківської інформації – це в першу чергу *загрози шахрайства* (підробка, відмова від авторства, відмова від одержання) і *порушення технології роботи*, а в другу – *порушення доступності* і *конфіденційності*.

У зв'язку з цим до КЗЗ ОС, що входять до складу банківських ІТС, пред'являються вимоги щодо забезпечення захисту від зазначених загроз. Крім того, вимоги істотно залежать від того, чи здійснюється обробка в реальному часі або відкладена обробка. Необхідно врахувати, що банківські ІТС, як правило, відносяться до класу 3, тобто є *розподіленими*.

В зазначених ІТС рекомендується використовувати ОС, КЗЗ яких реалізують профілі **3.КЦД.х**.

Стандартні функціональні профілі захищеності в КС, що входять до складу довідково-пошукових систем

Основними загрозами для довідково-пошукових систем масового обслуговування є *порушення їх доступності*. В зв'язку з цим до КЗЗ ОС, що входять до складу таких систем, в першу чергу пред'являються вимоги щодо забезпечення доступності. В зазначених ІТС рекомендується використовувати ОС, КЗЗ яких реалізують профілі **х.Д.х**, **х.ЦД.х**.

Висновки

1. За сукупністю характеристик ІТС (конфігурація апаратних засобів ІТС і їх фізичне розміщення, кількість різноманітних ступенів обмеження доступу оброблюваної інформації, кількість користувачів і повноважень користувачів) виділяють три ієрархічні класи ІТС, вимоги до функціонального складу КЗЗ яких істотно відрізняються:

- клас ІТС «1» – одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох ступенів обмеження доступу;
- клас ІТС «2» – локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу;
- клас ІТС «3» – розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

2. В межах кожного класу ІТС класифікуються на підставі вимог до забезпечення безпеки певних властивостей інформації: конфіденційності, цілісності, доступності. В зв'язку з цим, в кожному класі ІТС виділяються такі підкласи, як х.К, х.Ц, х.Д, х.КЦ, х.КД, х.ЦД, х.КЦД.

3. Стандартний функціональний профіль захищеності – це перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи ІТС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній ІТС.

4. Опис функціонального профілю захищеності складається з трьох час-

Таблиця 2.31

№ з/п	Найменування робіт	Вимоги, норми (відповідний документ)	Методики за п. 6.3.3 НД	Примітки
1	2	3	4	5

3. **Методики випробувань.** В розділі наводять відомості про методи проведення випробувань.

4. **Умови та порядок проведення випробувань**:

- умови щодо початку і завершення робіт з випробувань;
- послідовність проведення перевірок комплексу ТЗІ на відповідність вимогам нормативних документів з питань ТЗІ;
- особливості функціонування складових частин комплексу ТЗІ, що підлягають випробуванню;
- заходи, що забезпечують безпеку проведення випробувань.

5. **Матеріально-технічне і метрологічне забезпечення**:

- перелік заходів з метрологічного забезпечення випробувань із розподілом завдань і відповідальності підрозділів, що беруть участь у випробуваннях;
- склад засобів вимірювальної техніки із зазначенням ознак їх придатності до застосування, вимоги до них;
- перелік необхідної конструкторської та іншої документації;
- порядок підготовки і використання матеріально-технічних засобів у процесі випробувань.

Дані про вимірювальне обладнання викладаються у вигляді табл. 2.32.

Таблиця 2.32

№ з/п	Найменування вимірювального обладнання	Тип	Заводський номер	Виробник	Дані про повірку
1	2	3	4	5	6

6. **Аналіз і оцінка результатів випробувань**:

- обсяг вихідних даних, які необхідні для оцінки результатів випробувань;
- показники та критерії, за якими комплекс ТЗІ вважається таким, що

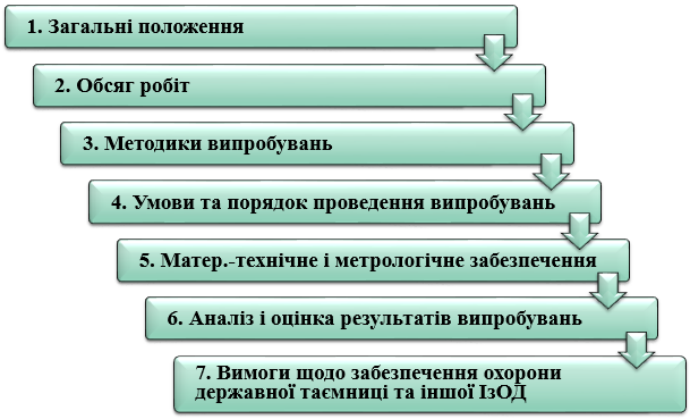

Рис. 2.27 Склад Програми і методики випробувань

Програми і методики випробувань узгоджує керівник установи-замовника створення комплексу ТЗІ та затверджує керівник установи, яка виконувала випробування.

Розглянемо зміст розділів Програми і методики випробувань.

1. **Загальні положення** містять:

- повну назву установи, підрозділу, ОІД, де створюється комплекс ТЗІ;
- підстави для проведення випробувань;
- відомості про виконавців випробувань;
- мету і основні завдання випробувань;
- види інформації (ІзОД, що озвучується та/або обробляється технічними засобами тощо), для яких впроваджуються відповідні заходи із захисту від витоку інформації технічними каналами;
- терміни проведення випробувань.

2. **Обсяг робіт.** Під час проведення випробувань здійснюють перевірку повноти та достатності реалізованих заходів із захисту інформації на ОІД (перевірку виконання вимог щодо захисту від витоку ІзОД можливими технічними каналами).

Обсяг випробувань та посилання на відповідні методики викладаються у вигляді табл. 2.31.

тин: буквено-числового ідентифікатора, знака рівності, переліку рівнів послуг, взятого в фігурні дужки.

5. В ІТС, призначених для автоматизації діяльності органів державної влади, часто обробляється інформація з обмеженим доступом. У зв'язку з цим до КЗЗ ОС, що входять до складу ІТС, у першу чергу пред'являються вимоги щодо забезпечення конфіденційності оброблюваної інформації, персональної відповідальності користувачів за дотримання режиму секретності. У зазначених ІТС рекомендується використовувати ОС, КЗЗ яких реалізують профілі х.К.х. Якщо, крім вимоги забезпечення конфіденційності, існують додаткові вимоги щодо забезпечення цілісності і/або доступності інформації, то рекомендується використовувати профілі х.КЦ.х, х.КД.х, х.КЦД.х.

Контрольні питання

1. Які класи ІТС виділяє НД ТЗІ 2.5-005 - 99? У чому полягає їх відмінність?
2. Як класифікуються ІТС на основі вимог із забезпечення захищеності певних властивостей інформації?
3. Що таке стандартний функціональний профіль захищеності ІТС?
4. Як описується профіль захищеності?
5. Визначте стандартний функціональний профіль захищеності ІТС класу «1» (забезпечення конфіденційності оброблюваної інформації).
6. Визначте стандартний функціональний профіль захищеності ІТС класу «2» (забезпечення конфіденційності та цілісності оброблюваної інформації).
7. Визначте стандартний функціональний профіль захищеності ІТС класу «3» (забезпечення конфіденційності та доступності оброблюваної інформації).
8. Визначте стандартні функціональні профілі захищеності в КС, що входять до складу ІТС, призначених для автоматизації діяльності органів державної влади.

5 Особливості захисту службової інформації від НСД в ІТС класу 2

Переважна більшість сучасних організацій (державного і приватного секторів) експлуатують ІТС класу 2 (тобто що будуються на базі локальних обчислювальних мереж), в яких обробляється службова інформація, що вимагає захисту.

НД ТЗІ 2.5-008 – 2002 Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення автоматизованих системах класу 2 встановлює згідно з визначеними **НД ТЗІ 2.5-004-99** специфікаціями мінімально необхідний перелік функціональних послуг безпеки та рівнів їх реалізації у КЗЗ інформації (стандартний функціональний профіль захищеності).

Установлені документом вимоги застосовуються також для захисту:

- таємної інформації, що не становить державної таємниці;
- конфіденційної інформації, яка перебуває у володінні розпорядників інформації, визначених частиною першою ст. 13 Закону України «Про доступ до публічної інформації»;
- іншої інформації з обмеженим доступом, необхідність захисту якої встановлено законом;
- конфіденційної інформації фізичних та юридичних осіб.

5.1 Загальні вимоги із захисту службової інформації

Засади щодо захисту службової інформації визначаються:

- Законами України **«Про інформацію»** і **«Про захист інформації в інформаційно-телекомунікаційних системах»**;
- іншими нормативно-правовими актами, виданими у відповідності з цими законами;
- **«Інструкцією про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави»** (затверджена постановою КМ України від 27 листопада 1998 р. № 1893).

- підготовка пропозицій і вимог до вибору (уточнення) рішень щодо впровадження необхідних заходів із захисту ІзОД на об'єкти інформаційної діяльності (ОІД);
- проведення атестації комплексу ТЗІ, оформлення протоколів, актів атестації;
- заповнення паспорта на комплекс ТЗІ (в т.ч. паспортів на приміщення, де ІзОД озвучується та/або обробляється технічними засобами).

Зміст документа **«Висновків за результатами випробувань комплексу ТЗІ»**:

1. Мета, призначення, вид, обсяг випробувань, місце і термін їх проведення.
2. Дані про затверджені програми і методики випробувань.
3. Склад технічних засобів, обладнання, необхідних для випробувань.
4. Результати випробувань щодо їх відповідності вимогам НД з питань ТЗІ.

Цей документ підписують виконавці випробувань, а затверджує керівник установи, яка виконувала випробування.

При проведенні випробувань необхідне матеріально-технічне і метрологічне забезпечення здійснюють їх виконавці.

Засоби вимірювальної техніки мають відповідати вимогам методик випробувань (не допускається застосовувати засоби, які не пройшли метрологічну атестацію або термін повірки прострочено).

Установа-замовник створення комплексу ТЗІ забезпечує умови проведення його атестації.

Виконавець атестації комплексу ТЗІ аналізує дані про його створення на ОІД, висновки за результатами випробувань, інші відомості.

У процесі проведення випробувань і атестації комплексів ТЗІ їх виконавці заповнюють відповідні паспорти, порядок розроблення та оформлення яких наведено в **НД ТЗІ 3.3-001-2007**.

Склад **«Програми і методики випробувань»** наведений на рис. 2.27.

7 Випробування комплексу технічного захисту інформації та його атестація

Випробування – досвідчене визначення кількісних і якісних властивостей системи захисту інформації як результату дій на неї, при її функціонуванні, при моделюванні. Випробування зазвичай проводять з метою отримання відомостей, необхідних для прийняття рішення про відповідність КСЗІ заданим вимогам.

Атестація об'єктів інформатизації (лат. *attestātio* – свідоцтво, підтвердження) – це комплекс організаційно-технічних заходів, в результаті яких спеціальним документом, – **Атестатом відповідності** підтверджується, що об'єкт відповідає вимогам стандартів або інших нормативно-технічних документів з безпеці інформації.

Обов'язковій атестації підлягають об'єкти інформатизації, призначені для обробки інформації, що становить державну таємницю.

Питання випробувань і атестації комплексів ТЗІ визначаються:

- **НД ТЗІ 2.1-002-2007. Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.**
- **НД ТЗІ 3.3-001-2007. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.**

7.1 Випробування комплексу технічного захисту інформації

Етап створення КСЗІ **«Випробування та атестація комплексу ТЗІ»** передбачає:

- затвердження програм і методик випробувань;
- проведення випробувань відповідно до затверджених програм і методик, оформлення протоколів випробувань;
- підготовка документа **«Висновки за результатами випробувань комплексу ТЗІ»**;

Впровадження заходів із захисту інформації в конкретній ІТС не повинно суттєво погіршувати основних її характеристик стосовно продуктивності, надійності, сумісності, керованості, розширюваності, масштабованості тощо.

Обробка в ІТС службової інформації здійснюється з використанням захищеної технології.

Технологія обробки інформації є захищеною, якщо вона містить програмно- технічні засоби захисту та організаційні заходи, що забезпечують виконання загальних вимог із захисту інформації.

Загальні вимоги із захисту інформації передбачають:

- наявність *переліку службової інформації*, яка підлягає автоматизованій обробці (у разі необхідності можлива її класифікація в межах категорії за цільовим призначенням, ступенем обмеження доступу окремих категорій користувачів та іншими класифікаційними ознаками);
- наявність визначеного (створеного) *відповідального підрозділу* (служби захисту інформації – СЗІ), якому надаються повноваження щодо організації і впровадження технології захисту інформації, контролю за станом захищеності інформації;
- створення *КСЗІ*, яка є сукупністю організаційних та інженерно- технічних заходів, програмно-апаратних засобів, спрямованих на забезпечення захисту інформації під час функціонування ІТС;
- розроблення *плану захисту* інформації в ІТС;
- наявність *атестата відповідності КСЗІ* в ІТС нормативним документам із захисту інформації;
- можливість визначення засобами КСЗІ декількох *ієрархічних рівнів повноважень користувачів* та декількох класифікаційних рівнів інформації;
- обов’язковість *реєстрації в ІТС* усіх користувачів та їхніх дій щодо службової інформації;
- можливість надання користувачам тільки за умови службової необхідності *санкціонованого та контрольованого доступу* до службової інформації, що обробляється в ІТС;

- заборону *несанкціонованої та неконтрольованої модифікації* службової інформації в ІТС;
- здійснення СЗІ *обліку вихідних даних*, отриманих під час вирішення функціональних задач у формі віддрукованих документів, що містять службову інформацію;
- заборону *несанкціонованого копіювання, розмноження, розповсюдження* службової інформації в електронному вигляді;
- забезпечення СЗІ контролю за санкціонованим копіюванням, розмноженням, розповсюдженням службову інформації в електронному вигляді;
- можливість здійснення *однозначної ідентифікації та автентифікації* кожного зареєстрованого користувача;
- забезпечення КСЗІ можливості *своєчасного доступу* зареєстрованих користувачів ІТС до службової інформації.

5.2 Характеристика типових умов функціонування та вимог із захисту інформації в ІТС класу 2

До ІТС класу 2 відносяться автоматизовані системи, створені на базі локалізованого багатомашинного багатокористувачевого комплексу (рис.2.14).

Рис. 2.14 Склад ІТС класу 2

Характеристика обчислювальної системи

Метою створення ІТС класу 2 є надання будь-якому користувачеві, у відповідності із захищеною технологією обробки інформації, потенційної можли-

Контрольні питання

1. Що є Планом захисту інформації в ІТС? На яких засадах він розробляється? Що він закріплює?
2. У яких випадках розробляється План захисту інформації в ІТС?
3. Які розділи включаються в План захисту інформації в ІТС?
4. У чому полягають завдання захисту інформації в ІТС?
5. На які об'єкти ІТС поширюється політика безпеки?
6. Як класифікується інформація, що обробляється в ІТС?
7. Які об'єкти ІТС підлягають інвентаризації?
8. Якими способами можуть здійснюватися загрози в ІТС?
9. Що необхідно визначити для кожної із загроз безпеки в ІТС?
10. Що є моделлю порушника інформаційної безпеки?
11. Як класифікуються порушники безпеки?
12. Що є політикою безпеки інформації в ІТС?
13. Які моменти повинні враховуватися при розробці політики безпеки?
14. На яких принципах базується політика безпеки?
15. Які моменти повинна доказово гарантувати політика безпеки?
16. Які роботи включає методологія розробки політики безпеки?
17. Що є концепція безпеки інформації в ІТС?
18. Що є аналізом ризиків?
19. Як здійснюється вибір основних рішень в забезпеченні інформаційної безпеки?
20. Що в себе включає план проведення відновних робіт і забезпечення безперервності функціонування ІТС?
21. У чому полягають правила розмежування доступу?
22. Що є система документів із забезпечення захисту інформації в ІТС?
23. З яких розділів складається календарний план робіт з організації заходів захисту інформації в ІТС?

ній, функціональними завданнями спеціалістів, що входять до складу навчальних груп та іншими чинниками.

Висновки

1. План захисту інформації в ІТС – це документ або сукупність документів, згідно з якими здійснюється організація захисту інформації на всіх етапах життєвого циклу ІТС. План захисту є обов'язковим документом для ІТС, в яких обробляється інформація, що становить державну або іншу встановлену законом таємницю; службова інформація; інформація, яка належить до державних інформаційних ресурсів; інформація, необхідність захисту якої встановлено законом.

2. План захисту повинен складатись з наступних розділів: завдання захисту інформації в ІТС; класифікація інформації, що обробляється в ІТС; опис компонентів ІТС та технології обробки інформації; загрози для інформації в ІТС; політика безпеки інформації в ІТС; система документів з забезпечення захисту інформації в ІТС.

3. Політика безпеки інформації – це набір вимог, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз.

4. Найважливішу частину політики безпеки, яка регламентує доступ користувачів і процесів до ресурсів ІТС, складають правила розмежування доступу (ПРД). ПРД – це певний абстрактний механізм, який виступає посередником при будь-яких взаємодіях об'єктів ІТС і є найбільш суттєвим елементом політики безпеки.

5. На підставі Плану захисту інформації в ІТС складається календарний план робіт з реалізації заходів захисту інформації в ІТС, який може мати такі розділи: організаційні заходи; контрольно-правові заходи; профілактичні заходи; інженерно-технічні заходи; робота з кадрами.

вості доступу до інформаційних ресурсів усіх комп'ютерів, що об'єднані в обчислювальну мережу.

Обчислювальна система ІТС включає:

- підсистему обробки інформації;
- підсистему взаємодії користувачів з ІТС;
- підсистему обміну даними.

Підсистема обробки інформації реалізує головну цільову функцію ІТС і складається із засобів обробки інформації, які утворюють основу інформаційно-обчислювальних ресурсів ІТС, що надаються користувачам (обчислення, пошук, зберігання та оброблення інформації).

Принциповими її особливостями є багатофункціональність і можливість доступу до неї для будь-яких робочих станцій ІТС.

Можливі обмеження визначаються тільки специфікою технологій, технічними й організаційними особливостями функціонування ІТС.

Як компоненти підсистеми можуть використовуватися:

- універсальні високопродуктивні ЕОМ (у тому числі й ПЕОМ);
- спеціалізовані сервери обробки даних або надання послуг (сервери баз даних, друку тощо).

Підсистема взаємодії користувачів з ІТС забезпечує користувачам доступ до засобів підсистеми обробки інформації і подання отриманого від них ресурсу у вигляді результату обчислення, інформаційного масиву або графічного зображення у зручній та зрозумілій для користувача формі.

Компоненти підсистеми у функціональному відношенні є автономно замкненими та, як правило, не передбачається доступ до їх внутрішніх обчислювальних ресурсів зі сторони інших компонентів ІТС.

Як компоненти підсистеми можуть використовуватися ПЕОМ, що укомплектовані засобами введення та відображення інформації (робочі станції), дисплейні станції.

Підсистема обміну даними забезпечує взаємодію робочих станцій із засобами підсистеми обробки інформації, а також робочих станцій між собою на

основі визначених правил, процедур обміну даними з реалізацією фаз встановлення, підтримання та завершення з'єднання; інформаційну взаємодію різних компонентів ІТС і об'єднує їх в єдине ціле як у структурному, так і у функціональному відношенні.

Підсистема обміну даними складається з:

- *пасивної мережі* для обміну даними (кабельна мережа),
- *активного мережевого обладнання* (комутаторів, концентраторів, маршрутизаторів, шлюзів тощо), що об'єднує в єдине ціле пасивну мережу з обладнанням інших підсистем для забезпечення інформаційної взаємодії (рис. 2.15).

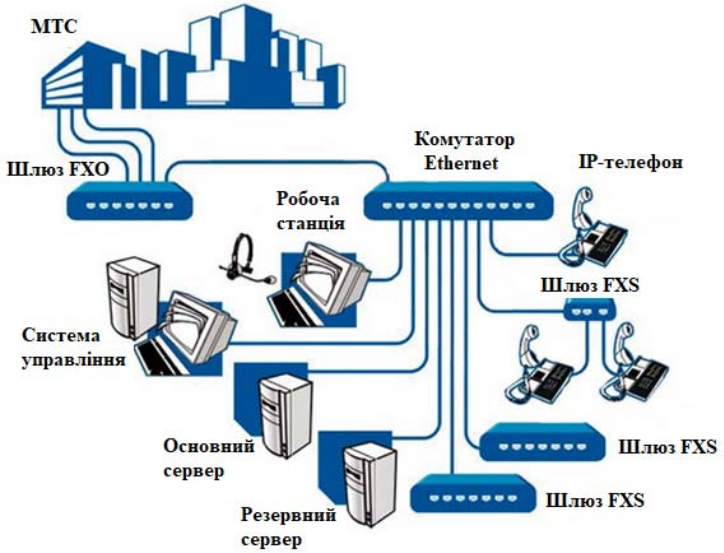

Рис. 2.15 Приклад підсистеми обміну даними

Обчислювальні системи ІТС укомплектовані:

- засобами обчислювальної техніки;
- комплексом програмно-апаратних засобів захисту інформації;
- периферійним обладнанням (пристроями друку, зберігання інформації тощо);
- комплексом програмного забезпечення (загальносистемного і прикладного).

- контроль за виконанням персоналом (користувачами) вимог відповідних інструкцій, розпоряджень, наказів;
- контроль за виконанням заходів, розроблених за результатами попередніх перевірок;
- контроль за станом зберігання та використання носіїв інформації на робочих місцях та інші.

3. До **профілактичних** слід відносити **заходи**, спрямовані на формування:

- у персоналу (користувачів) мотивів поведінки, які спонукають їх до безумовного виконання у повному обсязі вимог режиму, правил проведення робіт та ін.;
- відповідного морально-етичного стану в колективі.

4. До **інженерно-технічних** слід відносити **заходи**, спрямовані на:

- налагодження, випробування і введення в експлуатацію, супроводження і технічне обслуговування апаратних і програмних засобів захисту інформації від НСД, засобів захисту інформації від загроз її витоку технічними каналами;
- інженерне обладнання споруд і приміщень, в яких розміщуються засоби обробки інформації, у тому числі в процесі капітального будівництва тощо.

5. **Планування роботи з кадрами** включає:

- заходи з підбору та навчання персоналу (користувачів) встановленим правилам безпеки інформації, новим методам захисту інформації, підвищення їхньої кваліфікації.

Навчання персоналу (користувачів) може здійснюватись власними силами, з залученням спеціалістів зовнішніх організацій або в інших організаціях.

Навчання повинно здійснюватися згідно з програмою, затвердженою керівництвом організації (ІТС).

Навчальні програми повинні мати теоретичний і практичний курси. Доцільність і необхідність включення до програм окремих розділів визначається особливостями ІТС і технологіями захисту інформації, що використовуються в

зділи, наведені на рис. 2.26.

Рис. 2.26 Структура календарного плану робіт

1. **Організаційні заходи** з захисту інформації – це комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту інформації шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення захисту інформації.

До плану можуть включатись заходи щодо:

- розробки документів (інструкцій, методик, правил, розпоряджень тощо) з різних напрямів захисту інформації в ІТС;
- внесення змін та доповнень до чинних в ІТС документів з урахуванням зміни умов (обставин);
- розробки та впровадження нових організаційних заходів з захисту інформації;
- обгрунтування необхідності застосування та впровадження нових засобів захисту інформації;
- координації робіт та взаємодії з іншими підрозділами організації або зовнішніми організаціями на всіх етапах життєвого циклу ІТС;
- розгляду результатів виконання затверджених заходів та робіт з захисту інформації та інші.

2. До **контрольно-правових заходів** можуть бути віднесені:

У разі необхідності засоби обчислювальної техніки додатково можуть комплектуватися сумісними периферійними пристроями і відповідними модулями системного програмного забезпечення.

Склад комплекса програмного забезпечення ОС наведений на рис. 2.16.

Рис. 2.16 Склад комплекса програмного забезпечення ОС

Типові адміністративні та організаційні вимоги до ОС ІТС:

1) Для ІТС повинен бути сформований перелік необхідних функціональних послуг захисту і визначено рівень гарантій їх реалізації.

2) Сервери, робочі станції, периферійні пристрої, інші технічні засоби обробки конфіденційної інформації повинні бути категорійовані згідно з вимогами НД ТЗІ.

3) Засоби захисту інформації, інші технічні засоби та програмне забезпечення ІТС, що задіяні в КСЗІ, повинні мати підтвердження їхньої відповідності НД ТЗІ (атестат, сертифікат відповідності, експертний висновок) і використовуватись згідно з вимогами, визначеними цими документами.

4) Технічна та експлуатаційна документація на засоби захисту та обробки інформації, системне та функціональне ПЗ належним чином класифіковані і для кожної категорії користувачів визначено перелік документації, до якої вони можуть отримати доступ. Доступ до документації фіксується у відповідних реєстрах. Порядок ведення реєстрів визначає СЗІ.

5) Сервери і робочі станції, що здійснюють зберігання та обробку конфіденційної інформації, повинні розташовуватися в приміщеннях, доступ до яких обслуговуючого персоналу та користувачів різних категорій здійснюється в порядку, що визначений СЗІ та затверджений керівником організації.

6) Повинен здійснюватися контроль за доступом користувачів та обслуговуючого персоналу до робочих станцій, серверів ІТС і компонентів підсистеми обміну даними на всіх етапах життєвого циклу ІТС, а також періодичний контроль за цілісністю компонентів підсистеми обміну даними (з метою виявлення несанкціонованих відводів від компонентів підсистеми).

7) З метою забезпечення безперервного функціонування під час оброблення, зберігання та передачі службової інформації ІТС повинна мати можливість оперативного, без припинення її функціонування, проведення регламентного обслуговування, модернізації ОС в цілому або окремих її компонентів. Порядок введення в експлуатацію нових компонентів, якщо це впливає на захист інформації в ІТС, визначається СЗІ.

8) Програмно-апаратні засоби захисту, що входять до складу КЗЗ, разом з організаційними заходами повинні забезпечувати СЗІ інформацією про користувачів, які працюють в системі, з локалізацією точки їхнього входу в систему і переліком технічних засобів і процесів, до яких вони отримали доступ.

9) Має бути визначено порядок організації та проведення СЗІ процедур періодичного та/або динамічного тестування КЗЗ інформації під час функціонування ІТС.

Характеристика фізичного середовища

ІТС є територіально розосередженою системою, фізичне розташування компонентів якої можна представити як ієрархію, що включає територію, на якій вона знаходиться, будівлю, яка знаходиться на території, а також окреме приміщення в межах будівлі.

ІТС комплектується необхідними засобами енергозабезпечення, сигналізації, зв'язку, допоміжними технічними засобами, іншими системами життєзабезпечення.

технічного захисту інформації в Україні;

- нормативними документами, що містять вимоги з захисту інформації в ІТС міністерств та інших центральних органів виконавчої влади, чинність яких поширюється на сферу управління цього органу;
- нормативними, організаційно-розпорядчими та іншими документами, чинними у межах ІТС або організації.

Нормативні, організаційно-розпорядчі та інші документи, що використовуються у межах окремої організації або ІТС, враховують особливості та умови технології обробки інформації в цій організації або ІТС. Ці документи розробляються організацією, що є власником або розпорядником ІТС.

Такими документами можуть бути:

1) положення про захист інформації в ІТС, положення про службу захисту інформації в ІТС, інші документи, що входять до Плану захисту інформації.;

2) інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту, інструкції про порядок введення в експлуатацію КСЗІ, про порядок її модернізації, про порядок обробки ІзОД в ІТС, про порядок використання криптографічних засобів та ін.;

3) правила управління паролями в ІТС, правила видачі, вилучення та обміну персональних ідентифікаторів, інших атрибутів розмежування доступу;

4) інструкції, що встановлюють повноваження та відповідальність персоналу і користувачів;

5) плани виконання робіт або здійснення окремих заходів з захисту інформації в ІТС.

Розробленню підлягають документи, визначені політикою безпеки інформації. При розробленні цих документів дозволяється поєднувати декілька з них у вигляді окремих розділів в одному документі.

6.3 Календарний план робіт з захисту інформації в ІТС

На підставі Плану захисту інформації в ІТС складається **календарний план робіт з реалізації заходів захисту інформації в ІТС**, який може мати ро-

або розділів одного документа, в якому викладена політика безпеки інформації в ІТС. Структурно до політики безпеки (документів, що її складають) повинні входити наступні **розділи**:

1) загальний (визначається відношення керівництва ІТС (організації) до проблеми безпеки інформації);

2) організаційний (наводиться перелік підрозділів, робочих груп, посадових осіб, які відповідають за роботи у сфері захисту інформації, їх функції, викладаються підходи, що застосовуються до персоналу (опис посад з точки зору безпеки інформації, організація навчання та перепідготовки персоналу, порядок реагування на порушення режиму безпеки та ін.));

3) класифікаційний (визначаються матеріальні та інформаційні ресурси, які є у наявності в ІТС, та необхідний рівень їхнього захисту);

4) розділ, у якому визначаються ПРД до інформації;

5) розділ, у якому визначається підхід щодо керування робочими станціями, серверами, мережевим обладнанням тощо;

6) розділ, у якому висвітлюються питання фізичного захисту;

7) розділ, у якому висвітлюються питання захисту інформації від витоку технічними каналами;

8) розділ, де викладено порядок розробки та супроводження системи, модернізації апаратного та програмного забезпечення;

9) розділ, який регламентує порядок проведення відновлювальних робіт і забезпечення неперервного функціонування ІТС;

10) юридичний розділ, у якому приводиться підтвердження відповідності політики безпеки законодавству України.

Розділ VI Система документів з забезпечення захисту інформації в ІТС

Захист інформації в ІТС регламентується:

- законами України, іншими нормативно-правовими актами України;
- державними стандартами та іншими нормативними документами з стандартизації;
- нормативно-правовими актами і нормативними документами системи

Типові адміністративні та організаційні вимоги щодо умов розміщення компонентів ІТС:

1) Усі будівлі повинні бути розміщені в межах контрольованої території, що має пропускний та внутрішній режими, які відповідають режимним вимогам, що визначено чинними в організації нормативними та розпорядчими документами.

2) Контроль за доступом до приміщень, де знаходяться критичні з точки зору безпеки інформації компоненти ІТС, повинен забезпечуватись на всіх етапах її життєвого циклу. Порядок доступу до приміщень із визначенням категорій користувачів, які мають право це здійснювати, визначається СЗІ і затверджується керівником організації.

3) Для приміщень, в яких розташовані категорійовані компоненти ІТС, повинні бути вжиті відповідні заходи із захисту інформації від витоку технічними каналами, достатність і ефективність яких засвідчується актами атестації комплексів ТЗІ для кожного такого приміщення.

Характеристика користувачів

За рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконуються в процесі функціонування ІТС, особи, що мають доступ до ІТС, поділяються на наступні категорії:

1) **користувачі**, яким надано:

- повноваження розробляти й супроводжувати КСЗІ (адміністратори безпеки, співробітники СЗІ);
- повноваження забезпечувати управління ІТС (адміністратори операційних систем, адміністратори СКБД, адміністратори мережевого обладнання, адміністратори сервісів та ін.);
- право доступу до конфіденційної інформації одного або декількох класифікаційних рівнів;
- право доступу тільки до відкритої інформації;

2) **технічний обслуговуючий персонал**, що забезпечує належні умови функціонування ІТС;

3) **розробники та проектувальники апаратних засобів ІТС**, що забезпечують її модернізацію та розвиток;

4) **розробники ПЗ**, які здійснюють розробку та впровадження нових функціональних процесів, а також супроводження вже діючих;

5) **постачальники обладнання і технічних засобів ІТС** та фахівці, що здійснюють його монтаж, поточне гарантійне й післягарантійне обслуговування;

6) **технічний персонал**, що здійснює повсякденне підтримання життєдіяльності фізичного середовища ІТС:

- електрики;
- технічний персонал з обслуговування будівель;
- технічний персонал з обслуговування ліній зв'язку тощо.

Усі користувачі та персонал ІТС повинні пройти підготовку щодо умов та правил використання технічних та програмних засобів, які застосовуються ними під час виконання своїх службових та функціональних обов'язків.

Доступ осіб всіх категорій до службової інформації та її носіїв здійснюється на підставі дозволу, що надається наказом (розпорядженням) керівника організації. Дозвіл надається лише для виконання ними службових та функціональних обов'язків і на термін не більший, ніж той, що цими обов'язками передбачений.

Якщо в ІТС встановлено декілька класифікаційних рівнів службової інформації, кожній особі з допущених до роботи в ІТС мають бути визначені її повноваження щодо доступу до інформації певного класифікаційного рівня.

Дозвіл на доступ до службової інформації, що обробляється в ІТС, може надаватися лише користувачам. Як виключення, в окремих випадках (наприклад, аварії або інші непередбачені ситуації) дозвіл може надаватися іншим категоріям осіб на час ліквідації негативних наслідків і поновлення працездатності ІТС.

Персонал ІТС, розробники ПЗ, розробники та проектувальники апаратних засобів, постачальники обладнання та фахівці, що здійснюють монтаж і обслу-

- для попередження поширення комп'ютерних вірусів *відповідальність за дотримання правил використання ПЗ несуть*: на АРМ – *користувачі*, *адміністратор*, в ІТС – *адміністратор безпеки ІТС*. *Використовуватись повинно тільки ПЗ, яке дозволено політикою безпеки* (ліцензійне, яке має відповідні сертифікати, експертні висновки тощо);

- *за всі зміни ПЗ, створення резервних і архівних копій несе відповідальність адміністратор безпеки ІТС* (такі роботи виконуються за його дозволом);

- *кожний користувач має свій унікальний ідентифікатор і пароль*. Право видачі цих атрибутів надається адміністратору. Атрибути для адміністраторів надає адміністратор безпеки ІТС. Видача атрибутів дозволяється тільки після документальної реєстрації особи як користувача. Користувачам забороняється спільне використання персональних атрибутів;

- *користувачі проходять процедуру автентифікації* для отримання доступу до ресурсів ІТС;

- *атрибути користувачів періодично змінюються*, а невикористовувані і скомпрометовані – видаляються;

- *процедури використання активного мережевого обладнання, а також окремих видів ПЗ*, яке може суттєво впливати на безпеку (аналізатори трафіку, аналізатори безпеки мереж, засоби адміністрування та ін.), *авторизовані* і *здійснюються під контролем адміністратора безпеки ІТС*;

- *усі користувачі повинні знати* «*Інструкцію користувача*» (пройти відповідний курс навчання, скласти іспит);

- *адміністратор безпеки ІТС і адміністратори повсякденно здійснюють перевірку працездатності засобів захисту інформації*, ведуть облік критичних з точки зору безпеки подій і готують звіти щодо цього.

Загальні ПРД мають бути конкретизовані на рівні вибору необхідних функціональних послуг захисту (профілю захищеності) та впровадження організаційних заходів захисту інформації.

7. **Документальне оформлення політики безпеки.** Результати робіт з розроблення політики безпеки оформлюються у вигляді окремих документів

- порядок *тестування плану*, тобто *проведення тренувань персоналу* в умовах імітації надзвичайних ситуацій.

План проведення відновлювальних робіт і забезпечення неперервного функціонування ІТС підлягає перегляду у разі виникнення істотних змін в ІТС.

Такими змінами можуть бути:

- встановлення нового обладнання або модернізація існуючого, включення до складу ІТС нових компонентів;
- встановлення нових систем життєзабезпечення ІТС (сигналізації, вентиляції, пожежогасіння, кондиціонування та ін.);
- проведення будівельно-ремонтних робіт;
- організаційні зміни у структурі ІТС, виробничих процесах, процедурах обслуговування ІТС;
- зміни у технології обробки інформації;
- зміни у програмному забезпеченні;
- будь-які зміни у складі і функціях КСЗІ.

6. **Розробка правил розмежування доступу** (**ПРД**). Найважливішу частину політики безпеки, яка регламентує доступ користувачів і процесів до ресурсів ІТС, складають **ПРД** – це певний абстрактний механізм, який виступає посередником при будь-яких взаємодіях об'єктів ІТС і є найбільш суттєвим елементом політики безпеки.

Загальні ПРД можуть бути наступними (за припущення, що в ІТС визначено такі ієрархічні ролі – адміністратор безпеки ІТС, адміністратор, користувач):

- *кожне робоче місце повинно мати свого адміністратора*, який несе відповідальність за його працездатність та за дотримання всіх вимог і процедур, пов'язаних з обробкою інформації та її захистом. Таку роль може виконувати *уповноважений користувач*, який повинен бути забезпечений відповідними інструкціями і навчений всім вимогам і процедурам;
- для попередження неавторизованого доступу до даних, ПЗ, інших ресурсів ІТС, *керування механізмами захисту здійснюється адміністратором безпеки ІТС*;

говування технічних засобів ІТС, і не мають дозволу на доступ до службової інформації, можуть мати доступ до програмних та апаратних засобів ІТС лише під час робіт із тестування й інсталяції ПЗ, встановлення і регламентного обслуговування обладнання тощо, за умови обмеження їх доступу до даних конфіденційного характеру.

Зазначені категорії осіб повинні мати дозвіл на доступ тільки до конфіденційних відомостей, які містяться в програмній і технічній документації на ІТС або на окремі її компоненти, і необхідні їм для виконання функціональних обов'язків.

Для **організації управління доступом** до службової інформації та компонентів ІТС необхідно:

- розробити та впровадити *посадові інструкції користувачів та персоналу ІТС*, інструкції, якими регламентується порядок виконання робіт іншими особами з числа тих, що мають доступ до ІТС;
- розробити та впровадити *розпорядчі документи щодо правил перепускового режиму* на територію, в будівлі та приміщення, де розташована ІТС або її компоненти;
- визначити *правила адміністрування окремих компонентів ІТС та процесів*, використання ресурсів ІТС, забезпечити їх розмежування між різними категоріями адміністраторів;
- визначити *правила обліку, зберігання, розмноження, знищення носіїв конфіденційної інформації*;
- розробити та впровадити *правила ідентифікації користувачів* та осіб інших категорій, що мають доступ до ІТС.

Характеристика оброблюваної інформації

В ІТС обробляється службова інформація, володіти, користуватися чи розпоряджатися якою можуть окремі фізичні та/або юридичні особи, що мають доступ до неї у відповідності до правил, встановлених власником цієї інформації.

В ІТС може зберігатися і циркулювати відкрита інформація, яка не потребує захисту, або захист якої забезпечувати недоцільно, а також відкрита інфор-

мація, яка у відповідності до рішень її власника може потребувати захисту.

Службова й відкрита інформація можуть циркулювати та оброблятися в ІТС як різними процесами для кожної з категорій інформації, так і в межах одного процесу.

У загальному випадку в ІТС, безвідносно до ступеню обмеження доступу, інформація за рівнем інтеграції характеризується як:

- сукупність *сильнозв'язаних об'єктів*[1], що вимагають забезпечення своєї цілісності як сукупність;
- окремі *слабозв'язані об'єкти*[2], що мають широкий спектр способів свого подання, зберігання й передачі і вимагають забезпечення своєї цілісності кожний окремо.

Незалежно від способу подання об'єкти можуть бути *структурованими* або *неструктурованими*.

КСЗІ повинна реалізувати механізми, що забезпечують фізичну цілісність слабозв'язаних об'єктів, окремих складових сильнозв'язаних об'єктів, та підтримку логічної цілісності сильнозв'язаних об'єктів, що розосереджені в різних компонентах ІТС.

В ІТС присутня інформація, яка за часом існування та функціонування:

- є *швидкозмінюваною* з відносно коротким терміном її актуальності;
- має *відносно тривалий час існування* при високому ступені інтеграції і гарантуванні стану її незруйнованості за умови приналежності різним користувачам, в рамках сильно або слабозв'язаних об'єктів.

[1] **Сильнозв'язані об'єкти** – сукупність наборів даних, що характеризується наявністю мінімальної надлишковості і допускають їх оптимальне використання одним чи декількома процесами як одночасно, так і в різні проміжки часу і вимагають безумовного забезпечення цілісності цих наборів даних як сукупності. Прикладом таких об'єктів є *бази даних*, що підтримуються стандартними для галузі системами управління, сукупності наборів даних, які генеруються й модифікуються будь-якими функціональними або системними процесами і кожний з наборів даних, які складають цю множину, не може самостійно оброблятися, зберігатися і передаватися.

[2] **Слабозв'язані об'єкти** – відносно незалежні набори даних, що генеруються, модифікуються, зберігаються й обробляються в ІТС. Наприклад, це інформаційні структури, представлені у вигляді окремих файлів, що підтримуються штатними операційними системами робочих станцій та серверів, і кожний з них може оброблятися, зберігатися й передаватися як самостійний об'єкт.

	▪ захист ПЗ, окремих компонентів і ІТС в цілому від внесення несанкціонованих доповнень і змін; ▪ забезпечення функціонування засобів контролю, у тому числі засобів виявлення технічних каналів витоку інформації.

5. **Організація проведення відновлювальних робіт і забезпечення неперервного функціонування ІТС** – виробляються підходи щодо планування і порядку виконання відновлювальних робіт після збоїв, аварій, інших непередбачених ситуацій (надзвичайних ситуацій) з метою забезпечення неперервного функціонування ІТС в захищеному режимі.

Під час планування цих робіт рекомендується враховувати наступні питання:

- виявлення критичних з точки зору безпеки процесів у роботі ІТС;
- визначення можливого негативного впливу надзвичайних ситуацій на роботу ІТС;
- визначення та узгодження обов'язків персоналу і користувачів, а також порядку їхніх дій у надзвичайних ситуаціях;
- підготовка персоналу і користувачів до роботи в надзвичайних ситуаціях.

План проведення відновлювальних робіт і забезпечення неперервного функціонування ІТС повинен описувати дії щодо улагодження інцидента, резервування, відновлення. Він включає в себе:

- опис *типових надзвичайних ситуацій*, які потенційно найбільш можливі в ІТС внаслідок наявності вразливих місць, або які реально мали місце під час роботи;
- опис *процедур реагування на надзвичайні ситуації*, які слід вжити відразу після виникнення інциденту, що може призвести до порушення політики безпеки;
- опис *процедур тимчасового переводу ІТС або окремих її компонентів на аварійний режим роботи*;
- опис *процедур поновлення нормальної виробничої діяльності* ІТС або окремих її компонентів;

	ки інформації в ІТС (організації), виконання правових та (або) договірних вимог з захисту інформації, визначення відповідальності посадових осіб, організаційної структури, комплектування і розподілу обов'язків співробітників СЗІ; - процедур доведення до персоналу і користувачів ІТС основних положень політики безпеки інформації, їхнього навчання і підвищення кваліфікації з питань безпеки інформації; - системи контролю за своєчасністю, ефективністю і повнотою реалізації в ІТС рішень з захисту інформації, дотриманням персоналом і користувачами положень політики безпеки.
2. Організаційний	- застосування режимних заходів на об'єктах ІТС; - забезпечення фізичного захисту обладнання ІТС, носіїв інформації, інших ресурсів; - організації проведення обстеження середовищ функціонування ІТС; - порядку виконання робіт з захисту інформації, взаємодії з цих питань з іншими суб'єктами системи ТЗІ в Україні; - виконання робіт з модернізації ІТС (окремих компонентів); - регламентації доступу сторонніх користувачів до ресурсів ІТС; - регламентації доступу власних користувачів і персоналу до ресурсів ІТС; - здійснення профілактичних заходів (наприклад, попередження ненавмисних дій, що призводять до порушення політики безпеки, попередження появи вірусів та ін.); - реалізації окремих положень політики безпеки, найбільш критичних з точки зору забезпечення захисту аспектів (наприклад, організація віддаленого доступу до ІТС, використання мереж передачі даних загального користування, зокрема Інтернет, використання несертифікованого ПЗ та ін.).
3. Технічний	- застосування технічних і програмно-технічних засобів, які реалізують задані вимоги з захисту інформації. Під час розгляду різних варіантів реалізації рекомендується враховувати наступні аспекти: ▪ інженерно-технічне обладнання виділених приміщень, в яких розміщуються компоненти ІТС, експлуатація і супроводження засобів блокування технічних каналів витоку інформації; ▪ реєстрація санкціонованих користувачів ІТС, авторизація користувачів в системі; ▪ керування доступом до інформації і механізмів, що реалізують послуги безпеки, включаючи вимоги до розподілу ролей користувачів і адміністраторів; ▪ виявлення і реєстрація небезпечних подій з метою здійснення повсякденного контролю або проведення розслідувань; ▪ перевірка і забезпечення цілісності критичних даних на всіх стадіях їхньої обробки в ІТС; ▪ забезпечення конфіденційності інформації, у тому числі використання криптографічних засобів; ▪ резервне копіювання критичних даних, супроводження архівів даних і ПЗ; ▪ відновлення роботи ІТС після збоїв, відмов, особливо для систем із підвищеними вимогами до доступності інформації;

КСЗІ повинна забезпечити доступність зазначених видів інформації у відповідності до особливостей процесів, що реалізують інформаційну модель конкретного фізичного об'єкта.

ІТС повинна забезпечувати підтримку окремих класів сукупностей сильнозв'язаних об'єктів стандартними СКБД, іншими функціональними чи системними процесами, які надають можливість здійснення паралельної обробки запитів і мають засоби, що в тій чи іншій мірі гарантують конфіденційність і цілісність інформації на рівні таблиць, стовпців таблиці, записів таблиці.

ІТС повинна забезпечувати підтримку окремих класів сукупностей слабозв'язаних об'єктів стандартними операційними системами, які мають засоби, що в тій чи іншій мірі гарантують конфіденційність і цілісність інформації на рівні сукупності файлів, окремих файлів.

КСЗІ повинна гарантувати забезпечення цілісності, конфіденційності й доступності інформації, яка міститься в сильно- або слабозв'язаних об'єктах і є службовою інформацією, згідно з визначеними вимогами до відповідного функціонального профілю захищеності.

Характеристика технологій оброблення інформації

Технологічні особливості функціонування ІТС класу 2 визначаються:

- особливістю архітектури ІТС;
- способами застосування засобів обчислювальної техніки для виконання функцій збору, зберігання, оброблення, передавання та використання даних;
- вимогами до забезпечення властивостей інформації.

ІТС за структурою використовуваних технічних та програмних засобів може бути *однорідною* або *гетерогенною* структурою, мати різну *топологію*, що визначає різні підходи до забезпечення режимів циркулювання інформації в ІТС та способів доступу до неї.

КСЗІ повинна гарантувати користувачам *стійкість* ІТС до відмов та можливість проведення заміни окремих її компонентів з одночасним збереженням доступності до окремих компонентів ІТС або до ІТС в цілому.

В ІТС під час зберігання, оброблення та передавання службової інформації

має забезпечуватися реєстрація дій користувачів способом, що дозволяє однозначно ідентифікувати користувача, адресу робочого місця, з якого здійснено доступ до об'єктів та час, протягом якого здійснювався доступ.

Засоби КЗЗ повинні забезпечити необхідний рівень *цілісності* та *конфіденційності* інформації в журналах реєстрації ІТС із можливим виділенням одного чи декількох серверів аудиту. Статистика роботи користувачів повинна бути спостереженою й доступною для адміністратора безпеки та/або співробітників СЗІ.

Журнали реєстрації системи повинні мати захист від НСД, модифікації або руйнування.

У загальному випадку кожен користувач ІТС, що має дозвіл на роботу зі службовою інформацією, повинен мати можливість доступу до неї з будь-якої робочої станції ІТС. У разі необхідності можуть вводитися обмеження щодо цього. За певних адміністративно-організаційних заходів та відповідних програмно-технічних рішень в ІТС, де одночасно циркулює інформація різних ступенів доступу, для роботи зі службовою інформацією, можуть бути виділені окремі робочі станції. Робота інших робочих станцій, що не віднесені до переліку зазначених вище, повинна блокуватися за умови намагання користувачем будь-якої з категорій отримати доступ до службової інформації.

КСЗІ повинна забезпечити ідентифікацію користувача з визначенням точки його входу в ІТС, однозначно автентифікувати його і зареєструвати результат (успішний чи невдалий) цих подій у системному журналі. У випадку виявлення неавторизованого користувача повинна блокуватися можливість його роботи в ІТС.

КСЗІ повинна забезпечувати можливість двох режимів роботи користувача:

1) *із службовою інформацією*, гарантуючи доступ до відповідних об'єктів і процесів як з обмеженим доступом, так і до загальнодоступних;

2) *з відкритою інформацією*, гарантуючи доступ тільки до відкритої інформації й блокування будь-якого доступу до об'єктів і процесів з обмеженим доступом.

	- досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технологію її обробки в ІТС. Якщо інформація становить державну таємницю, то необхідно застосовувати, як правило, третій варіант.
6. Оцінювання витрат на КСЗІ	Здійснюється первинне оцінювання допустимих витрат на блокування загроз, виходячи з вибраного варіанту побудови КСЗІ і виділених на це коштів. На етапі проектування КСЗІ, після формування пропозицій щодо складу заходів і засобів захисту, здійснюється оцінка залишкового ризику для кожної пропозиції (наприклад, за критерієм «ефективність/вартість»), вибирається найбільш оптимальна серед них і первинна оцінка уточнюється. Якщо залишковий ризик перевищує гранично допустимий, вносяться відповідні зміни до складу заходів і засобів захисту, після чого всі процедури виконуються повторно до одержання прийнятного результату.

3. **Визначення вимог до заходів, методів та засобів захисту.** На підставі вихідних даних (завдання і функції ІТС, результати аналізу середовищ функціонування ІТС, модель загроз, модель порушників, результати аналізу ризиків) *визначаються компоненти ІТС* (наприклад, окрема ЛОМ, спеціалізований АРМ, Інтернет-вузол тощо), для яких необхідно або доцільно розробляти свої власні політики безпеки, відмінні від загальної політики безпеки в ІТС.

Для кожного компонента та (або) ІТС в цілому *формується перелік необхідних функціональних послуг захисту від НСД* та вимог до рівнів реалізації кожної з них, *визначається рівень гарантій реалізації послуг* (згідно з **НД ТЗІ 2.5-004-99**, **НД ТЗІ 2.5-005-99**). Визначені вимоги складають *профіль захищеності інформації* в ІТС (компоненті).

Для кожного компонента та (або) ІТС в цілому визначаються загальні підходи та вимоги з захисту інформації від витоку технічними каналами.

4. **Вибір основних рішень з забезпечення безпеки інформації.** Комплекс заходів з забезпечення безпеки інформації розглядається на трьох рівнях: правовому, організаційному і технічному (табл. 2.30).

Таблиця 2.30 Комплекс заходів з забезпечення безпеки інформації в ІТС

Рівень забезпечення	Повинні бути вироблені підходи щодо:
1. Правовий	- системи нормативно-правового забезпечення робіт з захисту інформації в ІТС (організації); - підтримки керівництвом організації заходів з забезпечення безпе-

2. Ідентифікація загроз з об'єктами захисту	Встановлюється відповідність моделі загроз і об'єктів захисту, тобто складається матриця загрози/компоненти (ресурси) ІТС. Кожному елементу матриці повинен бути зіставлений опис можливого впливу загрози на відповідний компонент або ресурс ІТС
3. Оцінка ризиків	Отримаються оцінки гранично припустимого й існуючого (реального) ризику здійснення кожної загрози впродовж певного проміжку часу, тобто ймовірності її здійснення впродовж цього інтервалу. Для оцінки ймовірності реалізації загрози рекомендується вводити декілька дискретних ступенів (градацій). Оцінку слід робити за припущення, що кожна подія має найгірший, з точки зору власника інформації, що потребує захисту, закон розподілу, а також за умови відсутності заходів захисту інформації. На практиці для більшості загроз неможливо одержати достатньо об'єктивні дані про ймовірність їхньої реалізації і доводиться обмежуватися якісними оцінками. У цьому випадку значення ймовірності реалізації загрози визначається в кожному конкретному випадку експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо. Оцінка може мати числове або смислове значення (наприклад, ймовірність реалізації загрози – незначна, низька, висока, неприпустимо висока). У будь-якому випадку існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози. Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.
4. Оцінювання величини можливих збитків, пов'язаних з реалізацією загроз	Виконується кількісна або якісна оцінка збитків, що можуть бути нанесені ІТС (організації) внаслідок реалізації загроз. Доцільно, щоб ця оцінка складалась з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості ІТС внаслідок реалізації загрози. Величина можливих збитків визначається розміром фінансових втрат або, у разі неможливості визначення цього, за якісною шкалою (наприклад, величина збитків – відсутня, низька, середня, висока, неприпустимо висока).
5. Вибір варіанту побудови КСЗІ	В залежності від конфіденційності інформації, яка обробляється в ІТС, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні власника ІТС, а також інших чинників обґрунтовується пропозиція щодо доцільності застосування варіантів побудови КСЗІ. Можливі наступні варіанти: - досягнення необхідного рівня захищеності інформації за мінімальних затрат і допустимого рівня обмежень на технологію її обробки в ІТС; - досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технологію її обробки в ІТС;

В обох режимах повинна забезпечуватися можливість визначення власниками об'єктів конкретних користувачів або їх групи, яким надається право мати доступ до цих об'єктів.

Службова інформація може зберігатися на різних пристроях (рис. 2.17)

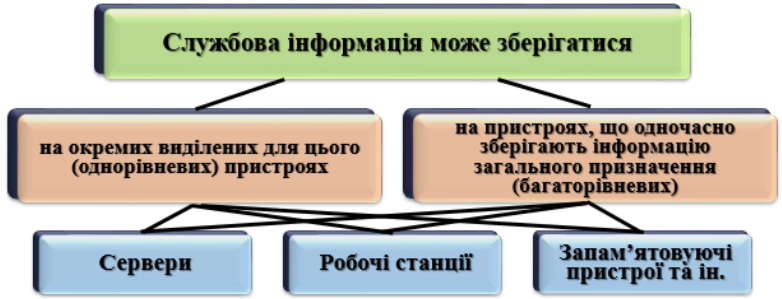

Рис. 2.17 Засоби зберігання службової інформації

КСЗІ повинна забезпечити розмежування доступу користувачів різних категорій до інформації незалежно від способу її групування на однорівневих чи багаторівневих пристроях.

В ІТС повинна надаватись можливість формування робочих груп з використанням засобів адміністрування:

- за ознакою належності до того чи іншого компонента ІТС;
- відповідно до функцій, що необхідно виконувати конкретному користувачеві або групі користувачів;
- крайній випадок – вся ІТС призначена для забезпечення виконання усіх функцій усіма користувачами або групами користувачів.

Під час цього засоби адміністрування ІТС повинні забезпечувати контроль за можливостями встановлення, перегляду, модифікації стратегій управління (наприклад, реалізація управління віртуальними мережами), а засоби КЗЗ – гарантувати забезпечення контролю за цілісністю засобів адміністрування ІТС.

Копіювання об'єктів, що містять службову інформацію, із сервера на робочу станцію користувача дозволяється тільки у випадках, коли це передбачено технологічними процесами обробки інформації. КЗЗ повинен гарантувати, що зазначені процеси перед завершенням своєї роботи забезпечують копіювання

цих об’єктів на сервер (якщо в цьому є потреба) і знищують їх на робочій станції способом, що унеможливлює відновлення або відтворення.

Під час обробки службової інформації повинна забезпечуватися можливість відміни окремої операції або певної їх послідовності до стану, що визначено користувачем або передбачено технологією реалізації певних процедур функціональним або системним програмним забезпеченням.

Виведення інформації у текстовому вигляді повинно здійснюватися на зареєстровані в установленому порядку паперові носії на спеціально виділених для цього пристроях друку.

КСЗІ повинна забезпечити контроль за процесом виконання роздруку інформації з фіксацією в системному журналі:

- імені користувача;
- імені об’єкта;
- імені робочої станції;
- часу, коли здійснюється роздрук.

У разі необхідності можлива фіксація додаткової інформації, що характеризує процес роздруку і дозволяє його однозначно ідентифікувати.

Реалізація функцій копіювання інформації в електронному вигляді на зйомні носії інформації та створення резервних копій може здійснюватися тільки уповноваженими користувачами або за дозволом адміністратора безпеки.

КСЗІ повинна контролювати зазначені процеси шляхом реєстрації в журналі системи:

- імені користувача;
- об’єкта копіювання;
- робочої станції;
- часу, коли здійснюється процес копіювання/створення резервної копії.

Допускається фіксація додаткової інформації, що характеризує ці процеси і дозволяє їх однозначно ідентифікувати.

Повинна бути реалізована можливість виявлення фактів НСД до об’єктів та (або) процесів, що потенційно можуть призвести до виникнення загроз для

1. **Концепція безпеки інформації в ІТС** викладає *систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації*.

Розроблення концепції здійснюється після вибору варіанту концепції створюваної ІТС і виконується на підставі аналізу наступних чинників:

- правових і (або) договірних засад;
- вимог до забезпечення безпеки інформації згідно з завданнями і функціями ІТС;
- загроз, яким зазнають впливу ресурси ІТС, що підлягають захисту.

За результатами аналізу мають бути сформульовані *загальні положення безпеки*, які стосуються або впливають на технологію обробки інформації в ІТС:

- *мета* і *пріоритети*, яких необхідно дотримуватись в ІТС під час забезпечення безпеки інформації;
- *загальні напрями діяльності*, необхідні для досягнення цієї мети;
- *аспекти діяльності у галузі безпеки інформації*, які повинні вирішуватися на рівні організації в цілому;
- *відповідальність посадових осіб* та інших суб’єктів взаємовідносин в ІТС, їхні *права* і *обов'язки* щодо реалізації завдань забезпечення безпеки інформації.

2. **Аналіз ризиків** передбачає вивчення моделі загроз для інформації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі *моделі захисту інформації в ІТС*. Під час проведення аналізу ризиків виконуються роботи, перечислені в табл. 2.29.

Таблиця 2.29 Роботи, що виконуються в процесі аналізу ризиків

Назва роботи	Пояснення
1. Визначення компонентів і ресурсів ІТС, які необхідно враховувати при аналізі	Визначаються критичні з точки зору безпеки компоненти і ресурси ІТС, які можуть бути об'єктами атаки або самі є потенційним джерелом порушення безпеки інформації (об’єкти захисту). Для цього використовуються відомості, одержані в результаті обстеження середовищ функціонування ІТС.

1) в ІТС *забезпечується адекватність рівня захисту інформації рівню її критичності*;

2) *реалізація заходів захисту інформації є рентабельною*;

3) в будь-якому середовищі функціонування ІТС *забезпечується оцінюваність і перевіряємість захищеності інформації*;

4) *забезпечується персоніфікація положень політики безпеки* (стосовно суб'єктів ІТС), *звітність* (реєстрація, аудит) *для всіх критичних з точки зору безпеки ресурсів*, до яких здійснюється доступ в процесі функціонування ІТС;

5) *персонал і користувачі забезпечені повним комплектом документації* стосовно порядку забезпечення захисту інформації;

6) *всі критичні з точки зору безпеки інформації технології* (*функції*) *ІТС мають відповідні плани забезпечення неперервної роботи та її поновлення* у разі виникнення непередбачених ситуацій;

7) враховані вимоги всіх документів, які регламентують порядок захисту інформації в ІТС, та забезпечується їхнє суворе дотримання.

Розроблення політики безпеки включає в роботи, що наведені на рис. 2.25.

Рис. 2.25 Роботи, які виконуються при розробленні політики безпеки

інформації, і забезпечена фіксація в журналі системи:

- імені користувача;
- об'єкта та (або) процесу, до якого була спроба доступу;
- місця та часу, коли виникла загроза.

Допускається фіксація додаткової інформації, яка дозволяє однозначно ідентифікувати процеси, що створили загрозу.

КСЗІ повинна забезпечити блокування роботи робочих станцій, з яких була здійснена загроза інформації.

В ІТС класу 2 можуть бути реалізовані різні технології обробки інформації (рис. 2.18). Одночасно в ІТС можуть застосовуватись декілька технологій.

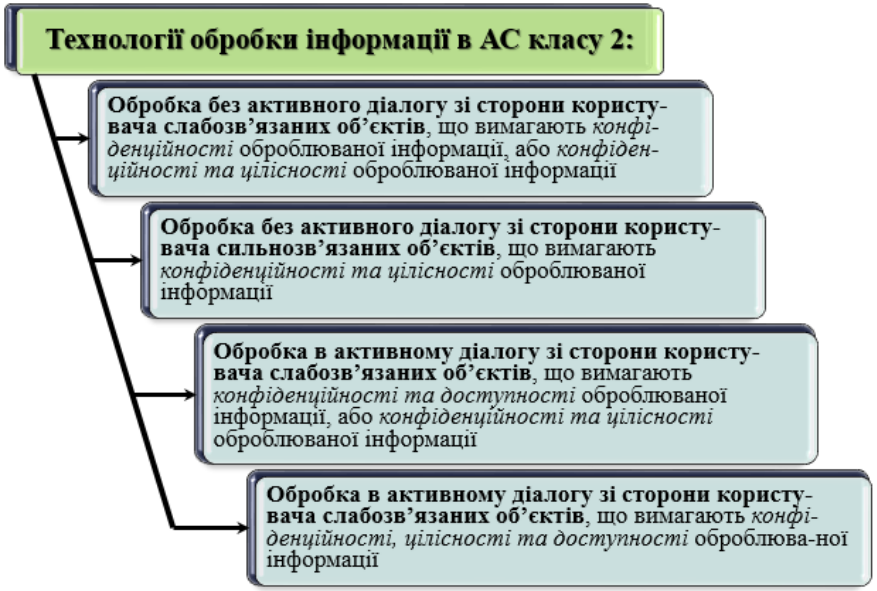

Рис. 2.18 Технології обробки інформації в ІТС

Обробка без активного діалогу зі сторони користувача слабозв'язаних об'єктів – це обробка окремого набору даних (або певної їх множини, але послідовно одне за одним) у фоновому режимі, який забезпечується операційними системами (за виключенням однокористувацьких, однозадачних), що використовуються на робочих станціях та серверах ІТС.

Обробка без активного діалогу зі сторони користувача сильнозв'язаних об'єктів – це вирішення в фоновому режимі комплексів функціональних задач, які взаємодіють із базами даних, що підтримуються стандартними СКБД, а також реалізацію будь-яких інших процесів, які здійснюють одночасну обробку певної множини наборів даних, що мають між собою логічні зв'язки.

Обробка в активному діалоговому режимі зі сторони користувача слабозв'язаних об'єктів – це обробка окремого набору даних у режимі реального часу в діалозі між користувачем та прикладним процесом, що цю обробку здійснює (наприклад, створення та редагування текстів, і т.п.).

Обробка в активному діалоговому режимі зі сторони користувача сильнозв'язаних об'єктів – це процеси реалізації в режимі реального часу взаємодії між користувачем та базою даних або сильнозв'язаними об'єктами (наприклад, будь-які інформаційні системи, що побудовані з використанням баз даних та СКБД і працюють у реальному часі; будь-які системи автоматизованого проектування тощо).

Рекомендується використовувати наступні **стандартні функціональні профілі захищеності** оброблюваної інформаці в ІТС класу 2:

1) під час застосування технології, що вимагає підвищених вимог до *забезпечення конфіденційності* оброблюваної інформації:

2.К.3 = {КД-2, КА-2, КО-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2};

2) під час застосування технології, що вимагає підвищених вимог до *забезпечення конфіденційності та цілісності* оброблюваної інформації:

2.КЦ.3 = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2};

3) під час застосування технології, що вимагає підвищених вимог до *забезпечення конфіденційності та доступності* оброблюваної інформації:

2.КД.1а = {КД-2, КА-2, КО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2};

4) під час застосування технології, що вимагає підвищених вимог до *за-*

- особливості побудови та використання обчислювальної системи;
- особливості фізичного середовища;
- інші чинники.

Як складові частини загальної політики безпеки в ІТС мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Політика безпеки повинна стосуватись:

- інформації (рівня критичності ресурсів ІТС);
- взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту),
- області застосування (яких складових компонентів ІТС політика безпеки стосується, а яких – ні).

Політика безпеки має бути розроблена таким чином, що б вона не потребувала частої модифікації (потреба частої зміни вказує на надмірну конкретизацію, наприклад, не завжди доцільно вказувати конкретну назву чи версію програмного продукту).

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації: *правові та морально-етичні норми*, *організаційні* (*адміністративні*), *фізичні*, *технічні* (*апаратні і програмні*) заходи, і визначати правила та порядок застосування в ІТС кожного з цих видів.

Політика безпеки повинна базуватися на **принципах**:

- неперервності захисту;
- комплексності;
- системності;
- відкритості алгоритмів і механізмів захисту;
- гнучкості керування системою захисту;
- простоти і зручності її використання;
- достатності механізмів і заходів захисту;
- адекватності механізмів і заходів захисту загрозам.

Політика безпеки повинна доказово давати гарантії того, що:

кувати як таких, що використовують:

- виключно агентурні методи одержання відомостей;
- пасивні технічні засоби перехоплення інформаційних сигналів;
- виключно штатні засоби ІТС або недоліки проектування КСЗІ для реалізації спроб НСД;
- способи і засоби активного впливу на ІТС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

За *місцем здійснення дії* порушники можуть класифікуватись:

- без одержання доступу на контрольовану територію організації (ІТС);
- з одержанням доступу на контрольовану територію, але без доступу до технічних засобів ІТС;
- з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів ІТС;
- з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, АРМ відповідних адміністраторів тощо);
- з одержанням доступу до засобів адміністрування ІТС і засобів керування КСЗІ.

Розділ V Політика безпеки інформації в ІТС

Політика безпеки інформації в ІТС – це набір вимог, правил, обмежень, рекомендацій і т.ін., які регламентують порядок обробки інформації в ІТС і спрямовані на захист інформації від певних загроз.

Термін «політика безпеки» може бути застосовано щодо ІТС, окремого її компонента, послуги захисту, що реалізується системою, і т.ін.

Політика безпеки інформації в ІТС є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи.

Під час розробки політики безпеки **повинні бути враховані**:

- технологія обробки інформації;
- моделі порушників і загроз;

безпечення конфіденційності, цілісності та доступності оброблюваної інформації:

2.КЦД.2а = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2}.

У разі необхідності для конкретної ІТС до визначених функціональних профілів захищеності можуть вводитися додаткові послуги безпеки, а також підвищуватись рівень будь-якої з наведених послуг.

Як виняток, послуга безпеки, що входить до визначених профілів захищеності, може не реалізовуватись, якщо її політика у повному обсязі відповідно до моделі захисту інформації спрямована на нейтралізацію лише несуттєвих загроз, визначених моделлю загроз для інформації в ІТС.

У випадках, коли в ІТС для окремих компонентів існують відмінності у характеристиках фізичного та інформаційного середовищ, середовища користувачів, технологій оброблення інформації, рекомендується визначати перелік мінімально необхідних рівнів послуг для кожного компонента окремо.

5.3 Політика реалізації послуг безпеки інформації в ІТС класу 2

Політика безпеки інформації в ІТС повинна поширюватися на об’єкти комп’ютерної системи, які безпосередньо чи опосередковано впливають на безпеку службової інформації. До таких об’єктів належать:

1) адміністратор безпеки та співробітники СЗІ;
2) користувачі, яким надано повноваження інших адміністраторів;
3) користувачі, яким надано право доступу до службової інформації або до інших видів інформації;
4) слабо- та сильнозв’язані об’єкти, які містять службову інформацію або інші види інформації, що підлягають захисту;
5) системне та функціональне ПЗ, яке використовується в ІТС для оброблення інформації або для забезпечення КЗЗ;
6) технологічна інформація КСЗІ (дані щодо персональних ідентифікаторів та паролів користувачів, їхніх повноважень та прав доступу до об’єктів,

встановлених робочих параметрів окремих механізмів або засобів захисту, інша інформація баз даних захисту, інформація журналів реєстрації дій користувачів тощо);

7) засоби адміністрування та управління обчислювальною системою ІТС та технологічна інформація, яка при цьому використовується;

8) окремі периферійні пристрої, які задіяні у технологічному процесі обробки службової інформації;

9) обчислювальні ресурси ІТС (наприклад, дисковий простір, тривалість сеансу користувача із засобами ІТС, час використання центрального процесора і т.ін.), безконтрольне використання яких або захоплення окремим користувачем може призвести до блокування роботи інших користувачів, компонентів ІТС або ІТС в цілому.

Висновки

1. Обробка в ІТС службової інформації здійснюється з використанням захищеної технології. Технологія обробки інформації є захищеною, якщо вона містить програмно-технічні засоби захисту та організаційні заходи, що забезпечують виконання загальних вимог із захисту інформації.

2. До ІТС класу 2 відносяться автоматизовані системи, створені на базі локалізованого багатомашинного багатокористувачевого комплексу. Мета створення ІТС класу 2: надання будь-якому користувачеві, у відповідності із захищеною технологією обробки інформації, потенційної можливості доступу до інформаційних ресурсів усіх комп'ютерів, що об'єднані в обчислювальну мережу.

3. Політика безпеки інформації в ІТС повинна поширюватися на об'єкти комп'ютерної системи, які безпосередньо чи опосередковано впливають на безпеку службової інформації.

Контрольні питання

1. Які загальні вимоги до процесів обробки в ІТС службової інформації?
2. Що входить до складу ІТС класу 2?

- використовувані порушником методи і способи;
- місце здійснення порушення;

За *рівнем можливостей*, що надаються порушникам засобами ІТС, вони класифікуються ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього (рис. 2.24).

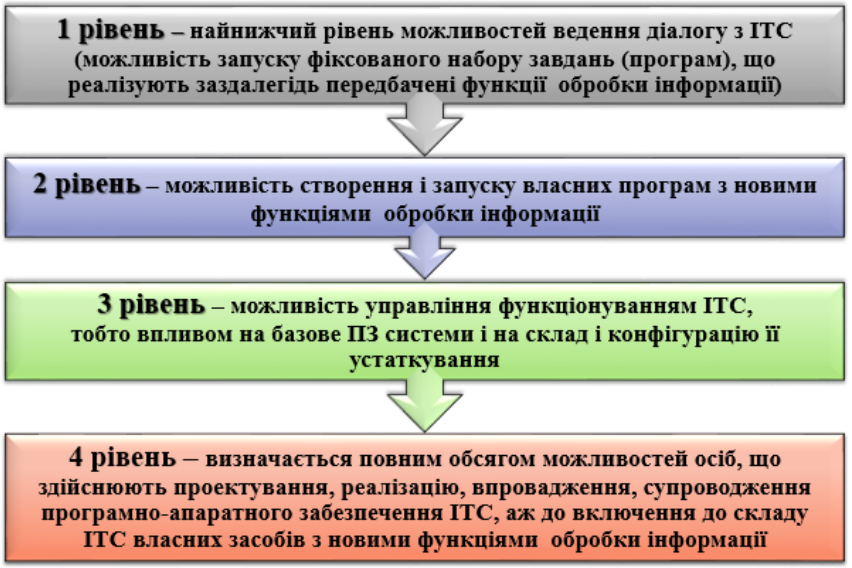

Рис. 2.24 Класифікація порушників за рівнем можливостей, що надаються їм засобами ІТС

За *рівнем знань* про ІТС порушників можна класифікувати як таких, що:

- володіють інформацією про функціональні особливості ІТС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;
- володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;
- володіють високим рівнем знань у галузі обчислювальної техніки, програмування, проектування та експлуатації ІТС;
- володіють інформацією про функції та механізм дії засобів захисту.

За *використовуваними методами і способами* порушників можна класифі-

гроза (рекомендується користуватись градаціями – порушення конфіденційності, цілісності, доступності інформації, спостережності та керованості ІТС);

- *джерела виникнення загроз* (які суб'єкти ІТС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);
- можливі *способи здійснення загроз*.

У кожному конкретному випадку, виходячи з технології обробки інформації в ІТС, необхідно розробити *модель порушника*, яка повинна бути адекватна реальному порушнику для ІТС.

Модель порушника – це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т.ін. По відношенню до ІТС порушники можуть бути *внутрішніми* (з числа співробітників, користувачів системи) або *зовнішніми* (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Модель порушника повинна визначати:

- можливу мету порушника та її градацію за ступенями небезпечності для ІТС;
- категорії осіб, з числа яких може бути порушник;
- припущення про кваліфікацію порушника;
- припущення про характер його дій.

Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами;
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

При побудові моделі порушника використовуються наступні підстави класифікації:

- рівень можливостей порушника;
- рівень знань порушника про ІТС;

3. Чим укомплектовані обчислювальні системи ІТС?
4. Що є комплексом ПЗ обчислювальної системи?
5. У чому полягають типові вимоги до обчислювальної системи ІТС в питаннях захисту інформації?
6. У чому полягають типові вимоги до умов розміщення компонентів ІТС?
7. Що необхідно виконати для організації управління доступом до службової інформації і компонент ІТС?
8. Визначите основні характеристики оброблюваною в ІТС службової інформації.
9. Визначите характеристики технології обробки службової інформації в ІТС.
10. Які технології обробки службової інформації реалізуються в ІТС класу 2?
11. Визначите функціональні профілі захищеності оброблюваної інформації в ІТС класу 2.

6 Планування захисту інформації в ІТС

Одно з найбільш важливих напрямів діяльності організації, що здійснює роботу з відомостями обмеженого характеру, – *планування заходів з їх захисту*.

Планування цих заходів займає особливе місце в системі управління діяльністю як організації в цілому, так і її структурних підрозділів (окремих посадовців).

Основними цілями планування заходів з захисту інформації є:

- організація проведення комплексу заходів з захисту інформації, спрямованих на виключення можливих каналів витоку інформації та НСД;
- встановлення персональної відповідальності посадовців за вирішення питань захисту інформації в ході виробничої та іншій діяльності організації;
- систематизація (об'єднання) усіх заходів, що проводяться на плановій основі, по різних напрямах захисту інформації;
- встановлення системи контролю за забезпеченням захисту інформації в організації, а також системи звітності про виконання конкретних заходів;
- уточнення (конкретизація) функцій і завдань, що вирішуються окремими посадовцями і структурними підрозділами організації.

Планування здійснюється відповідно до вимог, викладених ввідповідно до вимог, викладених **в НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі**.

6.1 Призначення та структура Плану захисту інформації в ІТС

План захисту інформації в ІТС – це документ або сукупність документів, згідно з якими здійснюється організація захисту інформації на всіх етапах життєвого циклу ІТС (рис. 2.19).

План захисту має фіксувати на певний момент часу:

- перелік оброблюваних відомостей;
- технологію обробки інформації;
- склад комплексу засобів захисту інформації;
- склад необхідної документації та ін.

роботи ІТС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості НСД до її ресурсів:

- порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації);
- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, уземлення, охоронної сигналізації, вентиляції та ін.);
- порушення режимів функціонування ІТС (обладнання і ПЗ);
- впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;
- використання засобів перехоплення ПЕМВН, акусто-електричних перетворень інформаційних сигналів;
- використання (шантаж, підкуп тощо) з корисливою метою персоналу ІТС;
- крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);
- несанкціоноване копіювання носіїв інформації;
- читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;
- одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача («маскарад»);
- неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;
- впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);
- інші.

Перелік суттєвих загроз має бути максимально повним і деталізованим.

Для кожної з загроз необхідно визначити:

- *на порушення яких властивостей інформації або ІТС спрямована за-*

захисту, структур даних тощо);

- помилки персоналу (користувачів) ІТС під час експлуатації;
- навмисні дії (спроби) потенційних порушників.

Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей вони спрямовані: конфіденційності, цілісності, доступності, спостережності та керованості ІТС.

Випадкові загрози суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру):

- дії, що призводять до відмови ІТС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм);
- ненавмисне пошкодження носіїв інформації;
- неправомірна зміна режимів роботи ІТС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);
- неумисне зараження ПЗ комп'ютерними вірусами;
- невиконання вимог до організаційних заходів захисту чинних в ІТС розпорядчих документів;
- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;
- будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;
- неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);
- наслідки некомпетентного застосування засобів захисту та інші.

Навмисні загрози суб'єктивної природи, спрямовані на дезорганізацію

План захисту повинен регулярно переглядатися та при необхідності змінюватись.

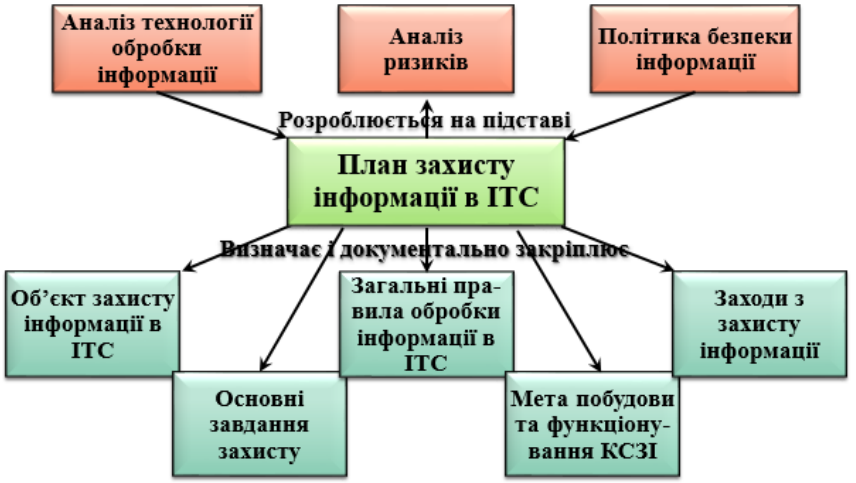

Рис. 2.19 План захисту інформації в ІТС

План захисту є обов'язковим документом для ІТС, в яких обробляється:

- інформація, що становить державну або іншу встановлену законом таємницю;
- службова інформація;
- інформація, яка належить до державних інформаційних ресурсів;
- інформація, необхідність захисту якої встановлено законом.

План захисту повинен складатись з наступних **розділів**:

I. Завдання захисту інформації в ІТС.

II. Класифікація інформації, що обробляється в ІТС.

III. Опис компонентів ІТС та технології обробки інформації.

IV. Загрози для інформації в ІТС.

V. Політика безпеки інформації в ІТС.

VI. Система документів з забезпечення захисту інформації в ІТС.

На підставі Плану захисту складається календарний план робіт з захисту інформації в ІТС.

6.2 Зміст Плану захисту інформації в ІТС

Розділ І Завдання захисту інформації в ІТС

У цьому розділі визначаються:

- мета та основні завдання захисту інформації в ІТС;
- об'єкти захисту.

Метою захисту інформації, яка зберігається, обробляється і передається в ІТС, є створенні і підтримка в дієздатному стані системи заходів (правових, організаційних, інженерних, програмно-апаратних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки.

Система зазначених заходів, що забезпечує захист інформації в ІТС, і є **комплексною системою захисту інформації**.

Досягнення цієї мети забезпечується рішенням **основних завдань**, до яких відносяться:

- забезпечення визначених політикою безпеки властивостей інформації (конфіденційності, цілісності, доступності) під час створення та експлуатації ІТС;
- своєчасне виявлення та знешкодження загроз для ресурсів ІТС, причин та умов, які спричиняють порушення її функціонування та розвитку;
- створення механізму та умов оперативного реагування на загрози для безпеки інформації, інші прояви негативних тенденцій у функціонуванні ІТС;
- ефективне знешкодження (попередження) загроз для ресурсів ІТС шляхом комплексного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки;
- керування засобами захисту інформації, керування доступом користувачів до ресурсів ІТС, контроль за їхньою роботою з боку персоналу СЗІ, оперативне сповіщення про спроби НСД до ресурсів ІТС;
- реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації;
- створення умов для максимально можливого відшкодування та локалізації збитків, що завдаються неправомірними (несанкціонованими) діями фізи-

Рис. 2.22 Можливі способи здійснювання загроз в ІТС

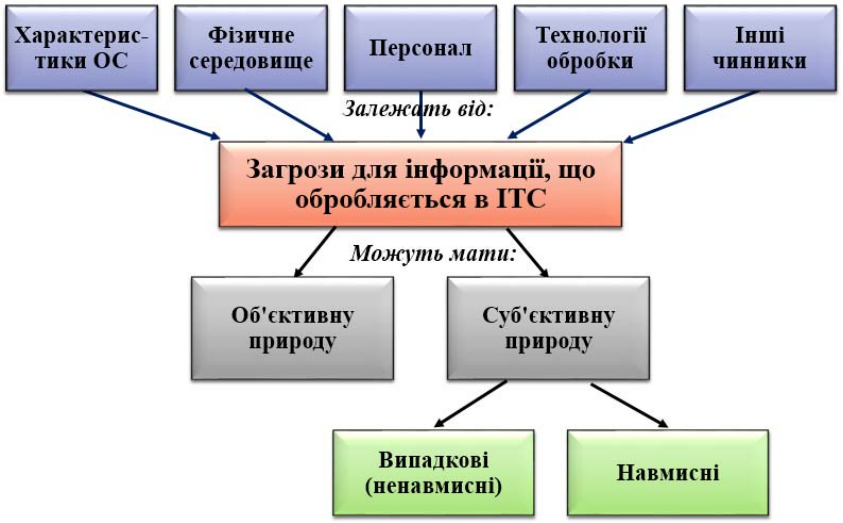

Рис. 2.23 Залежність загроз для інформації, що обробляється в ІТС

Мають бути визначені основні **види загроз об'єктивної природи** для безпеки інформації, які можуть бути реалізовані стосовно ІТС і повинні враховуватись у моделі загроз, наприклад:

- зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);
- збої і відмови у роботі обладнання та технічних засобів ІТС;
- наслідки помилок під час проектування та розробки компонентів ІТС (технічних засобів, технології обробки інформації, програмних засобів, засобів

Рис. 2.21 Об'єкти ІТС, що підлягають інвентаризації

Крім того, необхідно дати *опис технології обробки інформації в ІТС*, що потребує захисту, тобто способів і методів застосування засобів обчислювальної техніки під час виконання функцій збору, зберігання, обробки, передачі і використання даних, або алгоритмів окремих процедур. Опис (як в цілому, так і для окремих компонентів) може бути неформальним або формальним.

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

Розділ IV Загрози для інформації в ІТС

Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка *моделі загроз* для інформації та *моделі порушника*.

Для створення моделі загроз необхідно:

- скласти перелік суттєвих загроз;
- описати методи і способи їхнього здійснення.

Необхідно визначити, якими з можливих способів можуть здійснюватися загрози в ІТС (рис. 2.22).

Загрози залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об’єктивну або суб’єктивну природу (рис. 2.23).

чних та юридичних осіб, впливом зовнішнього середовища та іншими чинниками, зменшення негативного впливу наслідків порушення безпеки на функціонування ІТС.

Об’єктами захисту, на які поширюється політика безпеки, що реалізується КСЗІ, є:

1) *відомості, віднесені до ІзОД, або інших видів інформації*, що підлягають захисту, обробка яких здійснюється в ІТС і які можуть знаходитись на паперових, магнітних, оптичних та інших носіях;

2) *інформаційні масиви та бази даних, програмне забезпечення*, інші інформаційні ресурси;

3) *обладнання ІТС* (робочі станції, комунікаційні канали та обладнання, сервери, засоби друку та буферизації для утворення твердих копій, накопичувачі інформації) та інші матеріальні ресурси, включаючи технічні засоби та системи, не задіяні в обробці ІзОД, але знаходяться у контрольованій зоні, *носії інформації*, *процеси і технології її обробки*;

4) *засоби та системи фізичної охорони* матеріальних та інформаційних ресурсів, *організаційні заходи* захисту;

5) *користувачі (персонал) ІТС, власники інформації та ІТС*, а також їхні *права*;

Забезпечення безпеки інформації в ІТС досягається:

- *організацією та впровадженням системи допуску* співробітників (користувачів) до роботи з інформацією, яка потребує захисту;
- *організацією обліку, зберігання, обігу інформації, яка потребує захисту, та її носіїв*;
- *організацією і координацією робіт з захисту інформації*, яка обробляється та передається засобами ІТС;
- *здійсненням контролю за забезпеченням захисту інформації*, яка обробляється засобами ІТС, *та за збереженням конфіденційних документів* (носіїв).

Розділ II Класифікація інформації, що обробляється в ІТС

Класифікація є підставою для визначення власником (розпорядником) ін-

формації або ІТС методів і способів захисту кожного окремого виду інформації. Усі відомості, що обробляються в ІТС, класифікуються за режимом доступу, правовим режимом і типом представлення інформації (рис. 2.20).

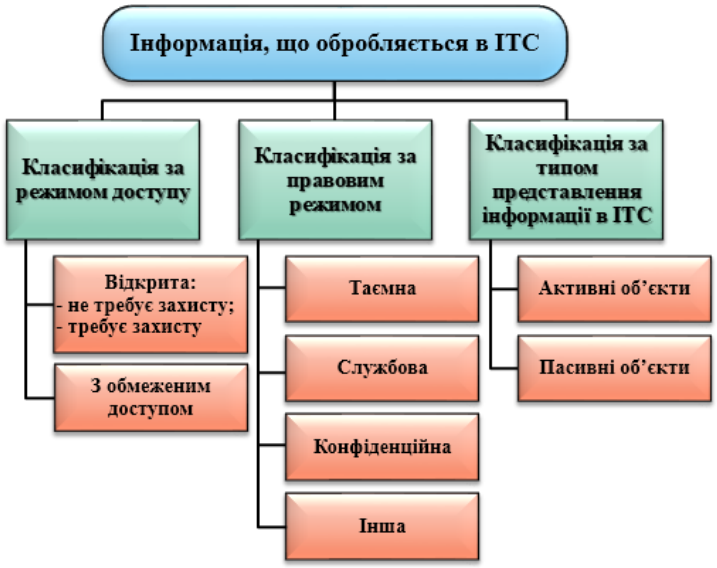

Рис. 2.20 Класифікація інформації, що обробляється в ІТС

За **режимом доступу** інформація в ІТС має бути поділена на:

- *відкриту*:

  а) яка *не потребує захисту*, або захист якої забезпечувати недоцільно;

  б) яка *потребує захисту*:

  - інформація, важлива для особи, суспільства і держави (відповідно до Концепції ТЗІ в Україні);
  - відкрита інформацію, вимога щодо захисту якої встановлена законом;
  - важливі для організації відомості, порушення цілісності або доступності яких може призвести до моральних чи матеріальних збитків;

- *з обмеженим доступом*.

За **правовим режимом** доступу ІзОД поділяється на:

- *таємну* (містить відомості, які становлять державну, а також іншу, передбачену законом таємницю);
- *службову* (правила доступу до інформації встановлюються її власником згідно з вимогами нормативно-правових актів);
- *конфіденційну* (правила доступу встановлюють фізичні та юридичні особи, у володінні яких вона перебуває);
- *іншу інформацію*, необхідність захисту якої встановлено законом.

Інформація, що становить державну таємницю, в свою чергу, поділяється на *категорії* (особливої важливості, цілком таємно та таємно) відповідно до Закону України «Про державну таємницю».

З метою встановлення правил розмежування доступу (ПРД) до конфіденційної інформації необхідно класифікувати її, поділивши на декілька категорій за *ступенем цінності* (критерії розподілу можуть бути визначені під час оцінки ризиків).

За **типом представлення інформація** в ІТС поділяється на:

- *активні об'єкти* (виконувана в даний момент програма, яка повністю характеризується своїм контекстом (поточним станом регістрів обчислювальної системи, адресним простором, повноваженнями і т.ін.));
- *пасивні об'єкти* (об'єкт КС, який в конкретному акті доступу виступає як пасивний компонент системи, над яким виконується дія і/або який служить джерелом чи приймальником інформації).

Для кожної з визначених категорій встановлюються типи пасивних об'єктів КС, якими вона може бути представлена.

Розділ ІІІ Опис компонентів ІТС та технології обробки інформації

В цьому розділі описується інвентаризація усіх компонентів ІТС і фіксуються всі активні і пасивні об'єкти, які беруть участь у технологічному процесі обробки і тим чи іншим чином впливають на безпеку інформації. На рис. 2.21 указаніы об'єкти ІТС, що підлягають інвентаризації.