НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ

Завідувач кафедри

Комп'ютерних систем, мереж та кібербезпеки

Касаткін Д.Ю., к. пед.н., доц.

Підпис ПІБ, вчене звання і ступінь

«___»_____2025 р.

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

На тему: Розробка комп’ютерної системи моніторингу втручання у мережу

Спеціальність 123 «Комп’ютерна інженерія»

Гарант освітньої програми

к.фіз.-мат.н., доцент _____ Євгеній НІКІТЕНКО

(науковий ступінь та вчене звання) (підпис) (ПІБ)

Керівник випускної бакалаврської роботи

д.пед.н., професор _____ Сергій МАМЧЕНКО

(науковий ступінь та вчене звання) (підпис) (ПІБ)

Виконав

(підпис) (ПІБ студента)

Київ – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАНН УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки

Касаткін Д.Ю., к.пед.н., доц. /
підпис ПІБ, вчене звання і ступінь
р.

З А В Д А Н Н Я
ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ БАКАЛАВРСЬКОЇ СТУДЕНТА

Ковальчук Дмитро Олексійович
(прізвище, ім'я, по батькові)

Спеціальність (напрям підготовки) Комп'ютерна інженерія
Тема випускної бакалаврської роботи Розробка комп'ютерної системи моніторингу втручання у мережу
керівник проекту (роботи) Мамченко С.М., д.пед.н., проф.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджено наказом ректора НУБіП України від «16» грудня 2024 р. № 2250 «С»
Термін подання завершеної роботи на кафедру 28.05.2025
(рік, місяць, число)

Вихідні дані до випускної бакалаврської роботи _____

Перелік питань, які потрібно розробити: Аналіз вимог до комп'ютерної системи моніторингу, аналіз предметної області, проєктування, реалізація, тестування системи

Перелік графічних документів (за потреби)_____

Дата видачі завдання "17" грудня 2024 р
Керівник випускної бакалаврської роботи _____ / Мамченко С.М.
(підпис) (прізвище та ініціали)
Завдання прийняв до виконання _____ / Ковальчук Д.О.
(підпис) (прізвище та ініціали студента)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Аналіз вимог до системи	07.03.2025 р.	Виконано
2	Проєктування системи	21.03.2025 р.	Виконано
3	Реалізація системи	12.04.2025 р.	Виконано
4	Тестування розробленої системи	27.04.2025 р.	Виконано
5	Оформлення пояснювальної записки	07.05.2025 р.	Виконано
6	Оформлення графічного матеріалу	15.05.2025 р.	Виконано

Студент_____ / Ковальчук Д.О. /

(підпис) (ініціали та прізвище)

Керівник проекту (роботи)_____ / Мамченко С.М../

(підпис) (ініціали та прізвище)

РЕФЕРАТ

Дипломна робота містить: 90 сторінок, 21 джерело інформації.

Робота присвячена дослідженню шляхів створення комплексної системи захисту на об‘єкті, рекомендаціям щодо розробки технічного завдання, створення служби захисту інформації, розробці політик безпеки та методів управління інформацією на основі даних поданих у нормативних документах технічного захисту інформації.

Метою цієї роботи є визначення ефективних методів створення комплексних систем захисту інформації, їх технічного проекту, служби захисту інформації на об’єкті інформаційної діяльності, який оперує конфіденціальною або секретною інформацією.

Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу та теорії інформаційної безпеки, нормативні документи, закони, державні стандарти.

Ця робота стане у нагоді для планування та побудови комплексних систем захисту інформації, технічного завдання на її побудову, політик безпеки. Були досліджені та надані основні рекомендації щодо створення комплексної системи захисту інформації.

Галузь використання – інформаційна безпека.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ТЕХНІЧНІ СИСТЕМИ ЗАХИСТУ, ЗАСОБИ ЗАХИСТУ, ТЕХНІЧНЕ ЗАВДАННЯ, ПОЛІТИКА БЕЗПЕКИ, СЛУЖБА ЗАХИСТУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНА
БЕЗПЕКА

ANNOTATION

The thesis contains 90 pages, and 21 source of literature.

The work is devoted to research of ways to create a comprehensive security system on site, recommendations for the development of technical specifications, the establishment of information security services, security policies and information management methods based on data provided in regulations on technical protection of information.

The purpose of this work is to determine effective methods of creating comprehensive information security systems, their technical design and information security service on the object of information activities, which operates confidential or classified information.

To solve the above scientific problem in the work used methods of system analysis and theory of information security, regulations, laws, state standards.

This work will be useful for planning and building comprehensive information security systems, terms of reference for its construction, security policies. Researched and provided main recommendations for the creation of a comprehensive information protection system.

The area of use is information security.

COMPREHENSIVE INFORMATION PROTECTION SYSTEM, TECHNICAL PROTECTION SYSTEMS, PROTECTIVE MEANS, TERMS OF REFERENCE, SECURITY POLICY, INFORMATION PROTECTION SERVICE, INFORMATION SECURITY

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ОІД – об’єкт інформаційної діяльності

АС – автоматизована система

ЕМВ – електромагнітне випромінювання

КЗЗ – комплекс засобів захисту

КС – комп'ютерна система

КСЗІ – комплексна система захисту інформації

НД – нормативний документ

НСД – несанкціонований доступ

ОС – обчислювальна система

ПЗ – програмне забезпечення

ТЗ – технічне завдання

ПЕМВН – побічні електромагнітні випромінювання і наводки

ТЗІ – технічний захист інформації

СЗІ – служба захисту інформації

ІТС – інформаційно-телекомунікаційна система

ОТЗ – основні технічні засоби

ПРД – правила розмежування доступу

СРД – система розмежування доступу

СКБД – система керування базами даних

НД – нормативний документ

ІзОД – інформація з обмеженим доступом

ЕОТ – електронна обчислювальна техніка

ЗОТ – засіб обчислювальної техніки

ВСТУП

Комплексний захист інформації є необхідним у будь яких сучасних компаніях чи структурах де циркулює інформація з обмеженим доступом. Тому дослідження на цю тему будуть надзвичай корисними у подальшому розвитку інформаційного суспільства.

Інформація один з найцінніших ресурсів людства, проте її цінність часто залежить від того хто має до неї доступ, саме тому з давніх часів люди намагалися забезпечити конфіденційність важливої інформації, щоб вона не потрапила в руки ворога або конкурента і не знецінилась або не принесла шкоди. Переслідуючи мету захисту інформації в наш час були створені спеціальні служби, системи захисту, нормативні документи що регулюють потік інформації. Однією з таких систем і є КСЗІ.

Комплексна система захисту інформації — це сукупність організаційних та інженерних заходів, програмно-апаратних засобів, криптографічних та інших засобів, які забезпечують захист інформації обмеженого доступу в ІТС від витоку, розголошення та НСД. КСЗІ включає інструменти та заходи, що реалізують методи, механізми захисту інформації від несанкціонованих дій та НСД до інформації, яка може бути здійснена шляхом підключення до обладнання та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту від використання інформації або посилання на неправдиву інформацію, використання вбудованих пристроїв або програм, використання комп’ютерних вірусів тощо.

Наразі в Україні одночасно існують дві парадигми систем захисту: КСЗІ та СУІБ у банківській сфері. Етапи створення першої визначено у НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». Замовник самотужки або із залученням підрядників розробляє технічне завдання на КСЗІ, погоджує його з державною службою спеціального зв'язку та захисту інформації України

(держспецзв'язок), а потім, на підставі нього проектує, впроваджує КСЗІ за допомогою сукупності організаційних заходів, програмно-апаратних та інженерних засобів. та вводить у дослідну експлуатацію. На підставі отриманої заявки держспецзв'язок визначає компанію-ліцензіата, яка виступає організатором державної експертизи КСЗІ. Організатор експертизи, який володіє штатом кваліфікованих експертів, розробляє програму та методику експертних випробувань, проводить їх та подає результати своєї роботи у вигляді проекту експертного висновку на розгляд експертної ради з питань технічного захисту інформації держспецзв'язку. У разі позитивного рішення КСЗД отримує атестат відповідності вимогам системи технічного захисту інформації.

Для організації робіт зі створення КСЗІ в ІТС створюється СЗІ, порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4001-2000. Система захисту інформації – це організована сукупність спеціальних органів, засобів, методів та заходів, що забезпечують захист інформації від внутрішніх та зовнішніх загроз.

Отже метою цієї роботи є визначення ефективних методів створення комплексних систем захисту інформації, їх технічного проекту, служби захисту інформації на об’єкті інформаційної діяльності, який оперує конфіденціальною або секретною інформацією на основі нормативних документів які і будуть наведені далі.

РОЗДІЛ 1. ОСНОВНІ ПОНЯТТЯ ТА ВИЗНАЧЕННЯ: НЕСАНКЦІОНОВАНИЙ ДОСТУП, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

На даний момент зростає кількість інформації, яка обробляється,передається та зберігається в сучасних інформаційно-комунікаційних системах та мережах (ІКСМ). Звідси стає зрозуміла актуальність задачі захисту інформації в ІКСМ з метою недопущення її несанкціонованому доступу, порушення конфіденційності та цілісності. Для ефективного вирішення даної задачі необхідний аналіз усіх можливих способів та методів несанкціонованого доступу до інформації в комп'ютерних системах, що дозволяє вчасно вжити заходів для протидії можливим загрозам. Несанкціонований доступ є реалізацією навмисної загрози інформаційно-комп'ютерної безпеки, яка призводить до матеріальних втрат комп’ютерної мережі та порушує її ефективне і надійне функціонування.

Сучасні ІКСМ є територіально розподіленими комп'ютерними мережами, що поєднують за допомогою каналів зв'язку різні комп'ютери і локальні мережі. Уразливість розподілених обчислювальних систем істотно перевищує уразливість автономних комп'ютерів. Це зв'язано, насамперед, з відкритістю, масштабністю і неоднорідністю самих комп'ютерних мереж. Відповідно існує чимало способів атак та несанкціонованих доступів в сучасні комп'ютерні мережі. Основними причинами реалізації несанкціонованого доступу є недоліки сучасних інформаційних технологій та структури інформаційних систем та мереж, а також неухильний ріст складності програмно-апаратних засобів обробки і захисту інформації. Система захисту даних від несанкціонованого доступу повинна забезпечувати виконання наступних функцій:

- ідентифікація ресурсів, тобто присвоєння ресурсам ідентифікаторів — унікальних ознак, по яких надалі система робить аутентифікацію;

· автентификация ресурсів, що захищаються, тобто встановлення їхньої дійсності на основі порівняння з еталонними ідентифікаторами;

· розмежування доступу користувачів по операціях над ресурсами (програми, дані), що захищаються за допомогою програмних засобів;

· адміністрування:

· визначення прав доступу до ресурсів, що захищаються,

· контроль цілісності і працездатності систем захисту.

Нами поставлене завдання провести аналіз актуальних способів та методів несанкціонованого доступу в сучасних інформаційно-комунікаційних системах та мережах, на основі проведеного аналізу розробка узагальненого алгоритму реалізації атак.

Класифікація актуальних способів та методів несанкціонованого доступу ІКСМ.

В даний час інформація, як результат автоматизованої обробки, з кожним роком визначає дії не тільки усе більшого числа людей, але й усе більшого числа технічних систем, створених людиною.

Під несанкціонованим доступом будемо розуміти такий доступ до інформації та інформаційних ресурсів ІКСМ, що здійснюється з порушенням встановлених в ній правил розмежування доступу, тобто порушує надійне та ефективне функціонування.

Об'єктами захисту, а також атаки є інформація, що обробляється, зберігається та передається в ІКСМ, права власників цієї інформації та власників комп’ютерної системи, права користувача.

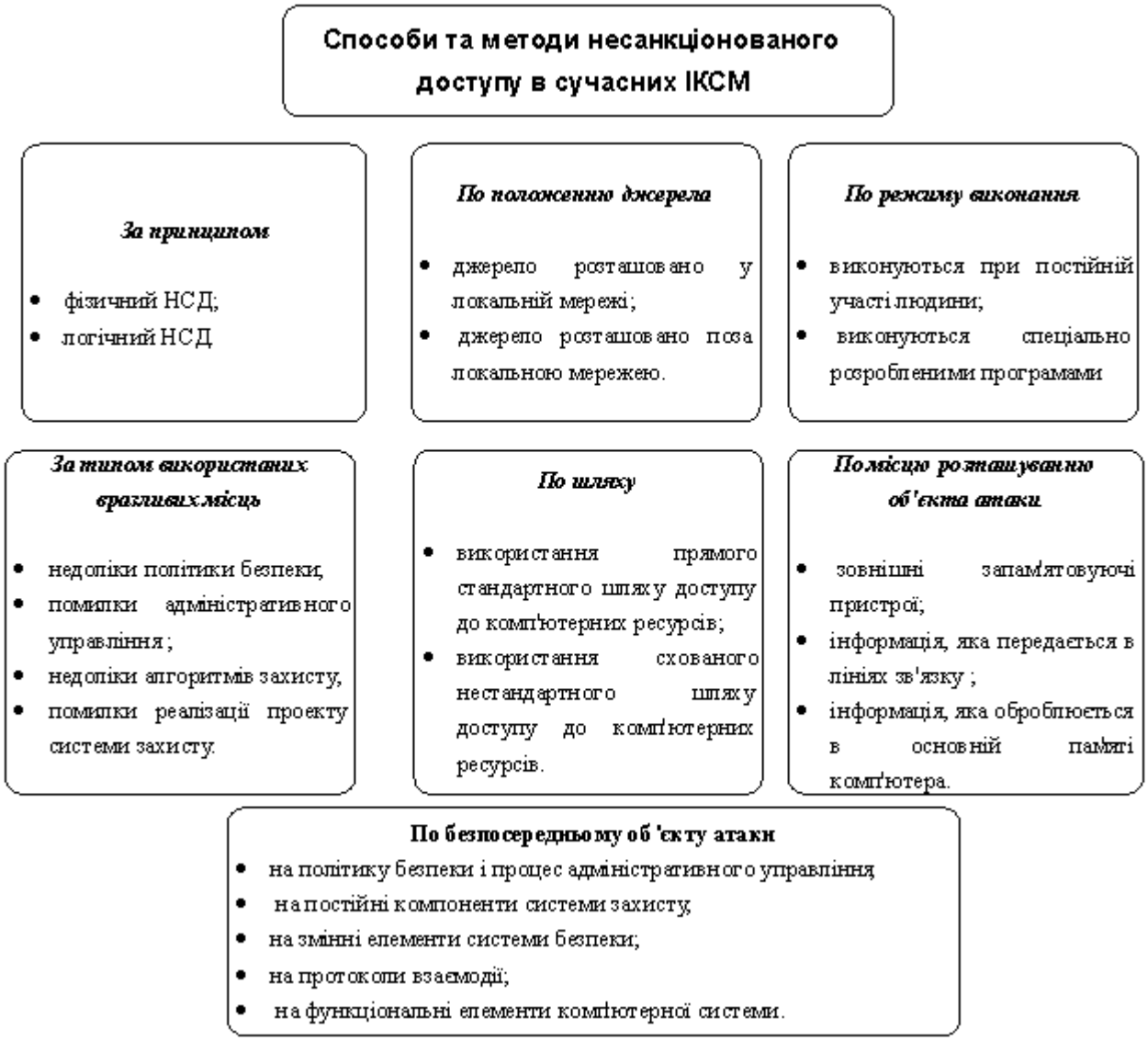

Рис. 1 Класифікація актуальних способів та методів несанкціонованого доступу в сучасних інформаційно-комунікаційних системах та мережах

Усі можливі способи несанкціонованого доступу до інформації в комп'ютерних системах, можна класифікувати по наступним ознаках [1-3].

1. За принципом несанкціонованого доступу:

а) фізичний несанкціонований доступ;

б) логічний несанкціонований доступ.

Фізичний несанкціонований доступ може бути реалізований одним з наступних способів:

· подолання рубежів територіального захисту і доступ до незахищених інформаційних ресурсів;

· розкрадання документів і носіїв інформації;

· візуальне перехоплення інформації, виведеної на екрани моніторів і принтери, а також підслуховування;

· перехоплення електромагнітних випромінювань.

Логічний несанкціонований доступ припускає логічне подолання системи захисту ресурсів активної комп'ютерної мережі. Враховуючи, що переважна більшість загроз інформації можуть бути реалізовані тільки в процесі функціонування обчислювальної системи, а також те, що логічний несанкціонований доступ є найбільш результативним для зловмисника, він і буде основним предметом аналізу.

2. По положенню джерела несанкціонованого доступу:

а) несанкціонований доступ, джерело якого розташований у локальній мережі;

б) несанкціонований доступ, джерело якого розташований поза локальною мережею.

У першому випадку атака проводиться безпосередньо з будьякої точки локальної мережі. Ініціатором такої атаки найчастіше виступає санкціонований користувач.

При підключенні будь-якої закритої комп'ютерної мережі до відкритих мереж, наприклад, до мережі Internet, високу актуальністю користуються можливості несанкціоновані дії в закриту мережу (захищену) з відкритої. Подібний вид атак характерний також для випадку, коли поєднуються окремі мережі, орієнтовані на обробку конфіденційної інформації зовсім різного рівня чи секретності різних категорій.

3. По режиму виконання несанкціонованого доступу:

- атаки, що виконуються при постійній участі людини;
- атаки, що виконуються спеціально розробленими програмами без особистої участі людини.

У першому випадку для впливу на комп'ютерну систему може використовуватися і стандартне програмне забезпечення. В другому випадку завжди застосовуються спеціально розроблені програми, в основу функціонування яких покладена вірусна технологія.

4. За типом використаних уразливих місць ІКСМ:

а) атаки, основані на недоліках встановленої політики безпеки;

б) атаки, основані на помилках адміністративного управління комп'ютерною мережею;

в) атаки, основані на недоліках алгоритмів захисту, реалізованих у засобах інформаційно-комп'ютерної безпеки;

г) атаки, основані на помилках реалізації проекту системи захисту.

Недоліки політики безпеки означають, що розроблена для конкретної комп'ютерної мережі політика безпеки настільки не відображує реальні аспекти обробки інформації, що стає можливим використання цієї невідповідності для виконання несанкціонованих дій. Під помилками адміністративного управління розуміється некоректна організаційна реалізація чи недостатня адміністративна підтримка прийнятої в комп'ютерній мережі політики безпеки. Наприклад, відповідно до політики безпеки повинний бути заборонений доступ користувачів до визначеного каталогу, а насправді через неуважність адміністратора цей каталог доступний усім користувачам. Ефективні способи атак можуть бути також основані на недоліках алгоритмів захисту і помилках реалізації проекту системи інформаційно-комп'ютерної безпеки.

5. По шляху несанкціонованого доступу:

а) атаки, орієнтовані на використання прямого стандартного шляху доступу до комп'ютерних ресурсів;

б) атаки, орієнтовані на використання схованого нестандартного шляху доступу до комп'ютерних ресурсів.

Реалізація атак першого типу найчастіше основана на використанні уразливостей установленої політики безпеки, а також недоліків процесу адміністративного управління комп'ютерною мережею. Наприклад, при відсутності контролю на стійкі паролі можливе маскування під санкціонованого користувача комп'ютерної системи. Атаки другого типу частіше всього здійснюються шляхом використання недокументованих особливостей системи інформаційно-комп'ютерної безпеки.

6. *По поточному місцю розташуванню кінцевого об'єкта атаки:*

а) атаки на інформацію, що зберігається на зовнішніх запам'ятовуючих пристроях;

б) атаки на інформацію, передану по лініях зв'язку;

в) атаки на інформацію, оброблювану в основній пам'яті комп'ютера.

7. *По безпосередньому об'єкту атаки:*

а) атаки на політику безпеки і процес адміністративного управління;

б) атаки на постійні компоненти системи захисту;

в) атаки на змінні елементи системи безпеки;

Г) напади на протоколи взаємодії;

д) напади на функціональні елементи комп'ютерної системи.

Кінцевим об'єктом реалізації несанкціонованого доступу завжди є інформація, що захищається, а саме інформаційні ресурси, бази та банки знань Під безпосереднім же об'єктом атаки розуміється об'єкт, аналіз чи використання якого дозволяє успішно реалізувати несанкціонований доступ до інформації, що захищається. Наприклад, безпосереднім об'єктом нападу може бути криптосистема, що дозволяє зловмиснику спрогнозувати значення генеруємого секретного ключа.

Ознака класифікації способів несанкціонованого доступу по безпосередньому об'єкту атаки є найбільш важливим, тому що точніше всього дозволяє розмежувати застосовувані способи реалізації несанкціонованих доступів.

Приведена система класифікації способів несанкціонованого доступу дозволяє зробити висновок, що ефективний несанкціонований доступ до інформації здійснюється тільки на основі уразливостей системи захисту комп'ютерної мережі, що атакується.

Узагальнений алгоритм підготовки і реалізації несанкціонованого доступу, як правило, включає наступні етапи

(рис.2).

1. Ретельний аналіз структури і принципів функціонування комп'ютерної мережі, що атакується, з метою пошуку уразливостей системи захисту її ресурсів.

2. Аналіз знайдених слабостей і розробка найбільш діючих способів подолання системи інформаційно-комп'ютерної безпеки.

3. Виконання підготовлених атак і оцінка отриманих результатів.

4. При невідповідності отриманих результатів необхідний ретельний аналіз процесу виконання атак і перехід до першого кроку для уточнення способів їхньої реалізації.

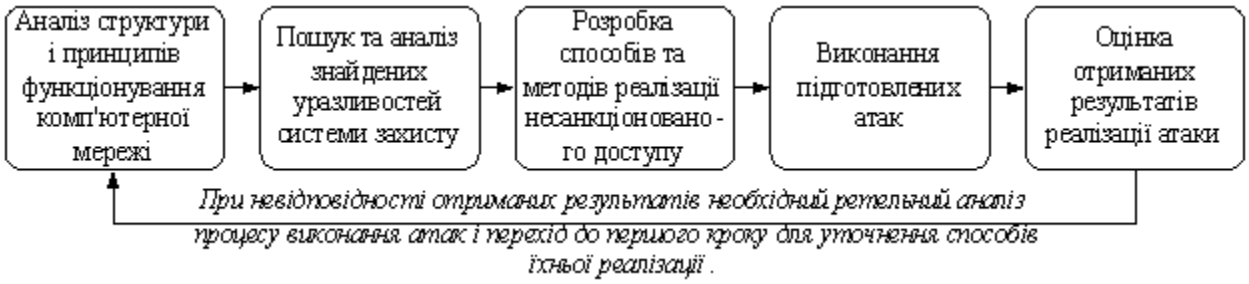

Рис.2. Алгоритм підготовки і реалізації несанкціонованого доступу в сучасних ІКСМ

Представлений алгоритм припускає поетапну процедуру реалізації впливів на комп'ютерну систему, що атакується. Для атаки важливо визначити лише її слабку ланку. Така ланка може бути виявлена в усьому, що зв'язано з інформаційнокомп'ютерною безпекою: у політику безпеки, засобах захисту,

реалізаціях програмного й апаратного забезпечення, керуванні системою. Можуть використовуватися також дефекти, що на перший погляд не мають безпосереднього відношення до забезпечення безпеки, наприклад, дефекти прикладного програмного забезпечення [4-6]..

Таким чином, на основі проведеного аналізу актуальних методів та способів несанкціонованого доступу в сучасних інформаційних системах та мережах проведено їх класифікацію за базовими критеріями. На основі проведених досліджень виділено основні недоліки при проектуванні системи захисту інформації, а саме від несанкціонованих дій користувачів і програм; втрати інформації і порушення працездатності комп'ютерної системи та адміністративного управління мережею.

1.2 Принципи створення комплексної системи захисту інформації

1. Законність. Забезпечення захисту інформації та створення КСЗІ в ІТС здійснюється відповідно до вимог чинного законодавства у сфері захисту інформації. Користувачі та працівники ІТС повинні усвідомлювати відповідальність за незаконне розголошення інформації з обмеженим доступом та порушення у сфері інформаційних відносин, визначену нормативно-правовими актами України.

2. Системність. Системний підхід до створення КСЗІ в ІТС передбачає врахування всіх суміжних і взаємодіючих елементів, умов і факторів, які є істотними для вирішення питання інформаційної безпеки в ІТС. При створенні КСЗІ слід враховувати всі критичні та найбільш уразливі сегменти системи обробки інформації, а також характер, можливі об’єкти та напрямки атак на систему з боку порушників, шляхи проникнення в розподілені системи та НСД до інформації. КСЗІ має створюватися не лише з урахуванням усіх відомих каналів

проникнення та НСД до інформації, а й з урахуванням можливості нових шляхів реалізації загроз.

3. Комплексність. Комплексне використання заходів і механізмів захисту ІТС передбачає скоординоване використання розрізнених засобів у створенні цілісної системи захисту, яка охоплює всі суттєві канали загрози і не містить вразливостей на стиках окремих компонентів. Охорона повинна будуватися на кількох рівнях. Зовнішній захист має забезпечуватися фізичними засобами, організаційноправовими заходами. Одними з найбільш стійких до атак мають бути механізми безпеки, реалізовані на рівні операційної системи, оскільки саме ОС контролює використання ресурсів комп'ютерної системи. Застосований рівень захисту, що враховує специфіку предметної області, передбачає внутрішню межу захисту.

4. Неперервність. Захист інформації — це безперервний цілеспрямований процес, що передбачає реалізацію відповідних заходів на всіх етапах життєвого циклу ІТС, починаючи з ранніх етапів проектування системи. Більшість технічних засобів захисту для ефективного виконання своїх функцій вимагають постійної адміністративної підтримки – своєчасної зміни та забезпечення правильного зберігання та використання ідентифікаторів, паролів, ключів шифрування, присвоєння повноважень тощо. Перерви в захисті можуть бути використані зловмисниками для аналізу методів та інструментів, що використовуються для захисту інформаційних ресурсів ІТС, для встановлення спеціальних програмноапаратних вбудованих пристроїв та інших засобів подолання системи захисту після її відновлення.

5. Своєчасність. Процеси визначення завдань комплексного захисту ІТС та реалізації заходів із захисту інформації починають здійснюватися на ранніх етапах розвитку ІТС. Створення КСЗІ повинно здійснюватися паралельно з розробкою та розвитком автоматизованої системи, ресурси якої підлягають

охороні. Це дозволить врахувати вимоги до інформаційної безпеки вже на етапах проектування архітектури ІТС та створити більш ефективну захищену систему як з точки зору витрат ресурсів, так і стійкості.

6. Неперервність вдосконалення. Заходи та засоби захисту інформації, організаційно-технічні рішення, кадри повинні постійно вдосконалюватися з урахуванням змін методів і засобів перехоплення інформації, нормативних вимог щодо захисту інформації, вітчизняного та зарубіжного досвіду.

7. Достатність. Рівень витрат на захист інформації в ІТС має відповідати вартості інформаційних ресурсів та величині можливих втрат від їх розкриття, втрати, витоку, знищення та спотворення.

8. Персональна відповідальність. Покладає відповідальність за забезпечення захисту інформації та системи її обробки на кожного працівника організації в межах своїх повноважень. Розподіл прав та обов’язків працівників має здійснюватися таким чином, щоб у разі будь-якого порушення кількість винних осіб була чітко відома та зведена до мінімуму.

9. Мінімізація повноважень. Означає надання користувачам мінімальних прав доступу. Доступ до інформаційних ресурсів ІТС повинен надаватися лише за умови і в обсязі, необхідному для виконання працівником організації своїх функціональних обов'язків.

10. Гнучкість системи захисту. Вжиті заходи та встановлені засоби захисту, особливо в початковий період їхньої експлуатації, можуть забезпечити як надмірний, так і недостатній рівень захисту. Щоб забезпечити різний рівень захисту, засоби захисту повинні мати необхідну гнучкість. Ця властивість особливо важлива в тих випадках, коли установка захисних засобів повинна здійснюватися на систему, яка вже працює, не порушуючи процесу її нормального функціонування. Крім того, з часом змінюються зовнішні умови та вимоги. У таких

ситуаціях гнучкість КСЗІ звільняє власників ІТС від необхідності вживати кардинальних заходів для повної заміни засобів захисту на нові.

11. Простота захисту. Механізми інформаційної безпеки в ІТС мають бути інтуїтивно зрозумілими та простими у використанні. Використання запобіжних заходів не повинно передбачати спеціальних знань або виконання дій, які потребують додаткових навичок у нормальній роботі належним чином зареєстрованих користувачів.

12. Обґрунтованість та технічна реалізованість. Інформаційні технології, технічні та програмні засоби, засоби та заходи захисту інформації в ІТС повинні бути впроваджені на сучасному рівні науки і техніки, обґрунтовані з точки зору досягнення заданого рівня захисту інформаційних ресурсів та повинні відповідати встановленим нормам і вимогам до інформації. захист.

13. Спеціалізація та професіоналізм. Передбачає залучення до розробки засобів та впровадження заходів захисту інформації в ІТС спеціалізованих організацій, які найкраще підготовлені до певної діяльності із захисту інформаційних ресурсів, мають практичний досвід та ліцензію на провадження діяльності у сфері послуг із захисту інформації. Здійснення організаційних заходів і налагодження засобів захисту повинні здійснюватися професійно підготовленими фахівцями організації.

14. Обов’язковість контролю. Спроби порушення встановлених правил забезпечення захисту інформації в ІТС мають бути своєчасно виявлені та припинені. Контроль за діяльністю будь-якого користувача, будь-яких засобів захисту та щодо будь-якого об’єкта захисту має здійснюватися на основі використання оперативного контролю та реєстрації та охоплювати як несанкціоновані, так і санкціоновані дії користувачів.

В Україні на державному рівні правовий захист регулюється такими правовими (актами, нормами):

- Конституція;
- закони України;
- адміністративне, кримінальне право, викладені у відповідних кодексах.

Відомчі нормативні акти визначаються:

- наказами;
- розпорядженнями;
- положеннями;
- інструкціями, що видаються відомствами, організаціями і підприємствами, діючими у рамках певних структур.

Висновки до розділу.

Було наведено основні поняття та визначення комплексної системи захисту інформації та принципи її створення. Сформовано завдання та цілі системи захисту, а також об’єкти захисту. Є очевидним, що комплексний захист інформації є необхідним у будь яких сучасних компаніях чи структурах де циркулює інформація з обмеженим доступом. Тому дослідження на цю тему будуть надзвичай корисними у подальшому розвитку інформаційного суспільства.

РОЗДІЛ 2. ТЕХНІЧНЕ ЗАВДАННЯ НА СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ, СТВОРЕННЯ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Розробка технічного завдання на створення КСЗІ Розробка та створення КСЗІ в ІТС здійснюється відповідно до НД ТЗІ 3.7-003-05 на підставі технічного завдання, розробленого згідно з вимогами НД ТЗІ 3.7-001-99.

Технічне завдання на створення КСЗІ в АС є засадничим організаційнотехнічним документом для виконання робіт щодо забезпечення захисту інформації в системі. Розробляється у разі необхідності розробки або модернізації КСЗІ. В разі розробки КСЗІ в процесі проектування АС допускається оформлення вимог з захисту інформації в АС у вигляді окремого (часткового) ТЗ, доповнення до загального ТЗ на АС або розділу загального ТЗ на АС. Має бути розроблено з урахуванням комплексного підходу до побудови КСЗІ, що передбачає інтеграцію в єдину систему всіх необхідних заходів і засобів захисту від різноманітних загроз інформаційній безпеці на всіх етапах інформаційної безпеки. Встановлює вимоги до функціонального складу та порядку розробки та впровадження технічних засобів забезпечення безпеки інформації в процесі її обробки в комп'ютерній системі. Крім того, необхідно викласти вимоги до організаційних, фізичних та інших заходів безпеки, які реалізуються поза комп'ютерною системою крім комплексу програмно-технічних засобів захисту інформації. Перелік вимог щодо захисту інформації, включених до ТЗ в КСЗІ, може бути як розширений, так і скорочений для кожної конкретної АС.

Вимоги мають передбачати розробку та використання сучасних ефективних засобів і методів захисту, які дають змогу забезпечити виконання цих вимог при найменших матеріальних витратах.

Технічне завдання на КСЗІ є одним із обов'язкових базових документів під час проведення експертизи АС на відповідність вимогам інформаційної безпеки.

Вихідними даними для розроблення ТЗ на КСЗІ є функціональний профіль захищеності КС від НСД і вимоги до захищеності інформації від витоку технічними каналами.

Функціональний профіль захищеності інформації в конкретній АС може бути визначений в результаті проведення аналізу загроз та оцінки ризиків або обраний на підставі класу АС відповідно до НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу".

Вимоги до захищеності інформації від витоку технічними каналами визначаються на підставі НД ТЗІ ТР ЕОТ-95 "Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок" і ТР ПЕМВН-95 "Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок ".

Перелік основних робіт етапу формування ТЗ такий:

- класифікація та опис ресурсів АС (ОС, засобів зв'язку і комунікацій, інформації, її категорій, виду подання, місця зберігання, технології обробки тощо, обслуговуючого персоналу і користувачів, території і приміщень та. ін.);
- розробка інформаційної моделі для існуючої АС, тобто опис (формальний або неформальний) інформаційних потоків АС, інтерфейсів між користувачем і АС та. ін.;
- 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 спец-перевірок і спец-досліджень 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.

Вимоги з захисту інформації визначаються замовником, погоджуються з розробником АС і виконавцем робіт по створенню КСЗІ в АС. Виконавець повинен мати відповідну ліцензію Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (Департамент). У випадках, передбачених Положенням про технічний захист інформації в Україні, ТЗ на КСЗІ погоджується з Департаментом.

Технічне завдання на КСЗІ оформлюється відповідно до того ж самого ДСТУ, що і основне ТЗ на АС, і в загальному випадку повинно містити такі основні підрозділи:

- загальні відомості;
- мета і призначення комплексної системи захисту інформації;
- загальна характеристика автоматизованої системи та умов її функціонування;
- вимоги до комплексної системи захисту інформації;
- вимоги до складу проектної та експлуатаційної документації;
- етапи виконання робіт;
- порядок внесення змін і доповнень до ТЗ;
- порядок проведення випробувань комплексної системи захисту інформації.

У розділах зазначаються: повна назва КСЗІ та її умовне позначення; код теми та деталі договору; назви підприємств-розробників та замовника (користувача) КСЗІ та їх реквізити; перелік документів, на підставі яких створюється КСЗІ, ким і коли були затверджені ці документи; планові терміни початку та закінчення роботи зі створення; відомості про джерела та порядок фінансування робіт; порядок

оформлення та представлення замовнику результатів робіт зі створення КСЗІ, з виготовлення та налагодження окремих засобів (технічних, програмних, інформаційних) та програмно-технічних (програмно-методичних) комплексів системи.

Вказують мету розробки КСЗІ в АС, функціональне призначення та особливості застосування. Необхідно вказати, на підставі яких нормативноправових актів, інших нормативних документів регулюється порядок захисту інформації.

Рекомендується відзначити такі моменти, які впливають на безпеку інформації під час її обробки в АС та загальні вимоги до впровадження СЗІ:

- загальна структурна схема та склад АС (перелік і склад обладнання, апаратних і програмних засобів, їх з'єднання, особливості конфігурації та архітектури, особливості підключення до локальних або глобальних мереж тощо);
- технічні характеристики каналів зв'язку (пропускна спроможність, типи кабельних ліній, види зв'язку з віддаленими сегментами АС і користувачами і т. ін.);
- характеристики інформації, що обробляється (категорії інформації, вищий гриф секретності і т. ін.);
- характеристики персоналу (кількість користувачів і категорій користувачів, форми допуску тощо);
- характеристики фізичного середовища (наявність службових приміщень, територіальне розміщення компонентів АС, їх фізичні параметри, вплив на них чинників навколишнього середовища, захищеність від засобів технічної розвідки і т.п.);
- загальні технічні характеристики АС (обсяги основних інформаційних масивів і потоків, швидкість обміну інформацією та продуктивність системи

при вирішенні функціональних завдань, тривалість процедури підготовки АС після живлення її компонентів, тривалість процедури відновлення після відмови, надійність та живучість тощо);

- особливості функціонування АС (надання машинного часу або обладнання в оренду стороннім особам, цілодобова робота без відключень електроенергії тощо); - особливості впроваджуваних або допустимих заходів організаційних, фізичних та інших заходів захисту (режимні заходи в приміщеннях і на території, охорона, сигналізація, протипожежний захист тощо);

- інші чинники, що впливають на безпеку оброблюваної інформації;

- потенційні загрози інформації (способи впровадження НСД, можливі технічні канали витоку інформації та умови їх формування, стихійні лиха тощо), а також можливі наслідки їх реалізації;

- клас АС згідно з НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу".

Також потрібно описати засоби захисту, що діють в АС, а також засоби, реалізовані в компонентах, які планується використовувати для побудови АС. Слід мати на увазі, що функції захисту, реалізовані за допомогою імпортної продукції, не мають належного рівня гарантій. Використання таких засобів у складі КСЗІ можливе лише за наявності експертного висновку, зареєстрованого департаментом спеціальних телекомунікаційних систем та захисту інформації служби безпеки України.

Процес створення КСЗІ слід розділити на три основні етапи: попередній, проектування та розробка, випробування та введення в експлуатацію. Кожен із етапів можна розділити на окремі підетапи.

До переліку робіт етапу проектування і розробки КСЗІ включаються роботи з вибору і модернізації штатних засобів захисту ПЗ і апаратури, що використовуються, архітектури ЗОТ, стандартних інтерфейсів і протоколів обміну, а також з розробки додаткового ПЗ і апаратної частини засобів захисту.

Етап випробування та введення в експлуатацію КСЗІ включає роботи, пов'язані з організацією та проведенням випробувань, у тому числі, у разі необхідності, розробкою спеціального обладнання, програмного забезпечення та відповідної документації.

Усі основні роботи кожного етапу відображаються в календарному плані, де вказуються терміни виконання робіт на окремих етапах, види звітності та форми подання результатів замовнику.

Зміни до затверджених ТЗ щодо створення КСЗІ в АС, потреба в яких виявлена в процесі роботи, вносяться окремим доповненням, яке погоджується і затверджується в тому ж порядку і на тому ж рівні, що і основний документ. Доповнення складається зі вступної частини та змінних вузлів. У вступній частині вказується причина видачі додатка. У розділах, що змінюються, наводяться номери та зміст змінених, нових або скасованих елементів.

Для кожного виду випробувань (попереднього, державного, сертифікаційного тощо) комплексної системи (підсистеми, компонента) захисту виконавцем розробляється «Програма та методика випробування комплексної системи (підсистеми, компонента) інформаційної безпеки в АС», яка затверджена в установленому порядку. Строки подання проекту програми, її розгляду та затвердження узгоджуються із замовником.

Для проведення випробувань замовником призначається комісія, склад якої узгоджується з розробником КСЗІ. Тести виконуються з використанням умовної інформації (крім ІзОД). Надається обладнання (необхідна нормативна, методична та інша документація, програмно-технічні засоби, метрологічне, спеціальне та інше

обладнання, створення інших умов для проведення випробувань), сторона, що її надає, порядок усунення зауважень тощо.

Наводиться перелік документів, якими завершуються випробування (етапи випробувань): акт приймання, сертифікат (атестат, експертний висновок) відповідності встановленим критеріям, наказ про введення в експлуатацію тощо.

2.2 Захист від витоку інформації технічними каналами та НСД Вимоги до комплексної системи захисту інформації в АС 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 " (далі - Критерії). Згідно з цим документом в процесі оцінки захищеності КС розглядаються вимоги двох видів: вимоги до функцій (послуг) забезпечення безпеки і вимоги до рівня гарантій. Відповідно, в ТЗ на КСЗІ повинні бути зазначені вимоги обох видів.

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.

Опису послуг має передувати опис політики безпеки інформації, яку повинен реалізувати комплекс засобів захисту АС. Опис політики безпеки має включати в себе опис:

- об'єктів (елементів ресурсів);
- принципів керування доступом користувачів до інформації (довірче і/або адміністративне керування доступом);
- правил розмежування інформаційних потоків;
- правил маркірування носіїв інформації;
- основних атрибутів доступу користувачів, процесів і пасивних об'єктів;

- правил розмежування доступу користувачів і процесів до пасивних об'єктів;
- правил адміністрування КЗЗ і реєстрації дій користувачів;
- інші загальні моменти політики безпеки, які вважає за потрібне описати розробник ТЗ.

В розділі мають бути викладені вимоги до реалізації послуг забезпечення:

- конфіденційності;
- цілісності;
- доступності;
- спостережності.

Для кожної послуги, включеної до розділу, рівень послуги, що буде запроваджено, має бути визначений відповідно до критеріїв. Необхідно описати політику цього сервісу: визначення об'єктів, до яких застосовується цей сервіс, та правил (у тому числі застосованих за замовчуванням), за якими мають функціонувати механізми, що реалізують сервіс. Відповідно до особливостей розробленого АС необхідно конкретизувати всі вимоги, викладені в критеріях до відповідного рівня кожної послуги.

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

Вимоги до гарантій також мають бути викладені і згруповані в тому порядку і стилі, як вони подані в критеріях. Це передбачає включення вимог:

- до архітектури КЗЗ (додатково до загальних вимог до архітектури на даному етапі бажано визначити основні модулі (підсистеми), з яких повинен складатися КЗЗ);
- до середовища розробки (організації процесу розробки і системи керування конфігурацією);

- до гарантій проектування (поетапність розробки і проектної документації);
- до середовища функціонування;
- до експлуатаційної документації;
- до випробувань комплексу засобів захисту.
- Всі вимоги повинні відповідати належному рівню гарантій.

Оскільки деякі вимоги щодо гарантії застосовуються до системи в цілому, а не лише до КЗЗ, цей розділ дозволяє посилання на інші розділи ТЗ. Зокрема, вимоги до поетапної розробки та складу документації мають бути визначені в розділах «Вимоги до складу проектно-експлуатаційної документації» та «Етапи роботи». Крім того, допускаються посилання на інші документи, розроблені на пізніх етапах. [17]

Необхідно сформулювати загальні вимоги до захищених об'єктів (компонентів АС), визначити засоби захисту та засоби їх використання, наприклад, виконання вимог безпеки має бути досягнуто без екранування, активні засоби повинні використовуватися лише для захисту інформації головного серверу АС тощо).

Наводиться перелік нормативних і методичних документів, відповідно до яких повинні проводитись роботи щодо захисту інформації від витоку технічними каналами. Мають бути вказані вимоги до розмірів зони безпеки інформації.

Мають бути вказані необхідні величини показників захищеності, що враховують реальну завадову обстановку на об'єкті електронної обчислювальної техніки. Основними показниками є:

- відношення величин електричної і магнітної складових напруженості поля побічних електромагнітних випромінювань до рівня завад на об'єкті ЕОТ;
- відношення величини напруженості інформативного сигналу в провідних комунікаціях на межі зони безпеки інформації до рівня завад на об'єкті ЕОТ;

- величина нерівномірності струму, який споживається по мережі електроживлення;
- коефіцієнт екранування засобів обчислювальної техніки, в тому числі від впливу зовнішніх ЕМВ.

Гранично допустимі значення основних показників є нормованими значеннями і визначаються відповідними методами. Відношення розрахункових (виміряних) значень ключових показників до гранично допустимих (нормованих) значень визначають необхідні умови захисту інформації. Необхідно вказати вимоги щодо використання методів, прийомів і засобів досягнення необхідних показників безпеки. Рекомендується використання таких методів, прийомів та засобів:

1. системотехнічних і схемотехнічних:

- 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 ЕМВ;
- 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;

2. засобів просторового і лінійного "зашумлення";

3. засобів локального або загального екранування;

4. 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 ЕМВ та спецперевірки ЗОТ, мета якої — виявлення та вилучення (блокування) спеціальних електронних (закладних) пристроїв.

Також має бути перерахована проектно-експлуатаційна документація, яка розробляється в процесі створення КСЗІ в АС.

Склад обов'язкової проектно-експлуатаційної документації визначається вимогами нормативних документів, відповідно до яких здійснюється розробка (зокрема, вимогами критеріїв належного рівня гарантій). Повний перелік необхідної документації визначається розробником КСЗІ та узгоджується із замовником.

2.3 Служба захисту інформації в ІТС

Служба захисту інформації (СЗІ) — це підрозділ організації, що забезпечує інформаційну безпеку шляхом управління комплексною системою інформаційної безпеки. Це може бути:

- штатний підрозділ організації;
- позаштатний підрозділ організації;
- самостійний структурний підрозділ організації;
- структурний підрозділ (підрозділ ТЗІ, служба безпеки…) організації.

В організаціях, де штатним розкладом не передбачено створення СЗІ, заходи щодо забезпечення захисту інформації в ІТС здійснюються працівниками, призначеними наказом керівника організації. У цьому випадку посадові обов'язки цих працівників мають включати положення, які вимагатимуть від них

відповідності вимогам СЗІ.[13]

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.

Правові основи створення і діяльності СЗІ:

- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Положення про технічний захист інформації в Україні;
- Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах;
- Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

СЗІ діє відповідно до «Плану захисту інформації в інформаційнотелекомунікаційній системі», календарних, перспективних та інших планів роботи, затверджених керівником організації. [13]

У своїй роботі СЗІ взаємодіє з підрозділами організації - РСО, службою безпеки організації, підрозділами ТЗІ, а також з державними органами, установами та організаціями, які займаються інформаційною безпекою.

У разі потреби до виконання робіт можуть залучатися сторонні організації, які мають ліцензію на відповідний вид діяльності із захисту інформації.

1) захист прав щодо інформаційної безпеки організації, її окремих структурних підрозділів, персоналу в процесі інформаційної діяльності та взаємодії один з

одним, а також у відносинах із зовнішніми вітчизняними та іноземними організаціями;

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

3) організація та координація робіт, пов'язаних із захистом інформації в ІТС, необхідність захисту якої визначається її власником або чинним законодавством, підтримання необхідного рівня безпеки інформації, ресурсів і технологій;

4) розробка проектів нормативно-правових та розпорядчих документів, що діють в організації, згідно з якими має бути забезпечений захист інформації в ІТС;

5) організація роботи зі створення та використання КСЗІ на всіх етапах життєвого циклу ІТС;

6) участь в організації професійного навчання та підвищення кваліфікації персоналу та користувачів ІТС із захисту інформації;

7) формування у персоналу та користувачів розуміння необхідності дотримання вимог нормативно-правових, нормативно-правових та розпорядчих документів, що стосуються сфери захисту інформації;

8) забезпечення дотримання працівниками та користувачами вимог нормативно-правових актів, нормативно-правових актів та розпорядчих документів щодо захисту інформації в ІТС та проведення перевірок їх виконання.

Функції СЗІ відрізняються для різних періодів життєвого циклу СЗІ:

- під час створення КСЗІ;

- під час роботи КСЗІ;

- про організацію навчання персоналу з питань інформаційної безпеки.

1. Функції СЗІ під час створення комплексної системи інформаційної безпеки:
1) визначення:

- переліки інформації, що підлягає захисту під час обробки, інших об'єктів захисту в ІТС;

- класифікація інформації за вимогами її конфіденційності або важливості для організації;

- необхідні рівні інформаційної безпеки;

- визначення порядку введення (виведення), використання та розпорядження інформації в ІТС;

2) розробка та налаштування:

- моделі погроз і порушників;

- моделі захисту інформації в ІТС;

- політики безпеки інформації в ІТС;

3) визначення та формування вимог до КСЗІ;

4) організація та координація робіт з проектування та розробки КСЗІ, безпосередня участь у проектних роботах зі створення;

5) підготовка технічних пропозицій, рекомендацій щодо запобігання витоку інформації через технічні канали та запобігання спробам НСД інформування під час створення КСЗІ;

6) організація робіт та участь у випробуваннях КСЗІ, проведення його експертизи;

7) відбір організацій-виконавців робіт зі створення КСЗІ, контроль за дотриманням встановленого порядку проведення робіт із захисту інформації, у взаємодії з підрозділом ТЗІ координація основних технічних та адміністративних документів, що супроводжують процес створення КСЗІ, технічні та робочі проекти, програма і методи випробувань, плани роботи тощо);

8) участь у розробці нормативно-правових актів, що діють в організації та ІТС, які встановлюють:

- дисциплінарна відповідальність за порушення вимог інформаційної безпеки та встановлених правил роботи КСЗІ;

- правила доступу користувачів до ресурсів ІТС, визначають порядок, норми, правила захисту інформації та контролю за їх дотриманням (інструкції, положення, накази, рекомендації тощо).

2. Функції СЗІ під час роботи:

1) організація процесу управління КСЗІ;

2) розслідування випадків порушення політики безпеки, небезпечних і непередбачених подій, аналіз причин, що їх призвели, ведення банку даних таких подій;

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

4) забезпечення контролю за цілісністю засобів інформаційної безпеки та швидкого реагування на їх вихід з ладу або порушення режимів роботи;

5) організація контролю доступу до ресурсів ІТС (розподіл серед користувачів необхідних реквізитів захисту інформації – паролів, привілеїв, ключів тощо);

6) ведення та оновлення бази даних інформаційної безпеки (матриць доступу, класифікаційних міток об'єктів, ідентифікаторів користувачів тощо);

7) спостереження (реєстрація та аудит подій в ІТС, моніторинг подій тощо) за функціонуванням КСЗІ та його складових;

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

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

10) участь у роботах з модернізації ІТС - узгодження пропозицій щодо впровадження нових компонентів в ІТС, нових функціональних завдань і режимів обробки інформації, заміни засобів обробки інформації тощо;

11) забезпечення супроводу та оновлення довідкових, архівних та резервних копій програмних компонентів КСЗІ, забезпечення їх зберігання та тестування;

12) проведення аналітичної оцінки поточного стану інформаційної безпеки в
ІТС (прогнозування появи нових загроз та їх врахування в моделі загрози, визначення необхідності її коригування, аналіз відповідності технології обробки інформації та реалізованої політики безпеки до поточна модель загроз тощо);

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

14) негайне втручання в процес ІТС у разі нападу на КСЗІ, здійснюючи в таких випадках виявлення порушника;

15) регулярне подання керівництву організації-власника (керівника) ІТС звітів про дотримання користувачами ІТС вимог щодо захисту інформації;

16) аналіз інформації про технічні засоби захисту інформації нового покоління, обґрунтування пропозицій щодо придбання коштів для організації;

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

18) контроль за охороною та зберіганням документів (носіїв інформації), що містять інформацію, що підлягає захисту;

19) розроблення та впровадження спільно з РСО (підрозділ ТЗІ, служба безпеки) організації комплексних заходів із забезпечення інформаційної безпеки під час діяльності науково-технічного, економічного, інформаційного

співробітництва з іноземними компаніями, а також під час зустрічей, переговорів тощо. , здійснення їх технічного та інформаційного забезпечення. [13]

3. Функції СЗІ для організації навчання персоналу з інформаційної безпеки:

1) розробка планів підготовки та перепідготовки спеціалістів СЗІ та ІТСперсоналу;

2) розробка спеціальних навчальних програм, які б враховували особливості технології обробки інформації в організації (ІТС), необхідний рівень її безпеки тощо;

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

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

5) участь в організації навчально-виховного процесу з необхідною матеріальною базою, підручниками, положеннями, положеннями, методичною літературою тощо.

Повноваження та відповідальність СЗІ включають:

1. Права:

- здійснювати контроль за діяльністю будь-якого структурного підрозділу організації (ІТС) з дотриманням вимог нормативно-правових актів із захисту інформації;

- надавати керівництву організації пропозиції щодо призупинення процесу обробки інформації, заборони обробки, зміни режимів обробки тощо у разі виявлення порушень політики безпеки або у разі реальної загрози порушення безпеки;

- складати та подавати керівництву організації акти про виявлені порушення політики безпеки, готувати рекомендації щодо їх усунення;

- проводити службові розслідування у справах про порушення;

- отримати доступ до робіт і документів структурних підрозділів організації, необхідних для оцінки вжитих заходів щодо захисту інформації та підготовки пропозицій щодо їх подальшого вдосконалення;

- готувати пропозиції щодо залучення на договірних засадах до виконання робіт із захисту інформації інших організацій;

- готувати пропозиції щодо забезпечення ІТС необхідними технічними та програмними засобами захисту інформації та іншим спеціальним обладнанням, дозволеним до використання в Україні з метою забезпечення захисту інформації;

- звертатися до керівництва організації з пропозиціями щодо подання заяв до відповідних державних органів на проведення державної експертизи КСЗІ або сертифікації окремих засобів захисту інформації;

- погоджувати умови включення нових компонентів до ІТС та подавати керівництву пропозиції щодо заборони їх включення, якщо вони порушують політику безпеки або рівень захисту ресурсів ІТС;

- надавати висновки з питань, що належать до компетенції СЗІ, які необхідні для виробничої діяльності організації, особливо технологій, доступ до яких обмежений, інших проектів, які потребують технічної підтримки з боку співробітників СЗІ;

- звертатися до керівництва організації з пропозиціями щодо узгодження планів і регламентів відвідування ІТС сторонніми особами;

- інші права, надані СЗІ відповідно до специфіки та специфіки організації.

2. Обов'язки:

- організувати забезпечення повноти та якісного виконання організаційнотехнічних заходів із захисту інформації в ІТС;

- своєчасно та в повному обсязі доводити до користувачів ІТС та персоналу інформацію про зміни у сфері захисту інформації, які їх стосуються;

- перевіряти відповідність прийнятих в ІТС (організації) правил, інструкцій з обробки інформації, здійснювати контроль за дотриманням цих вимог;

- здійснювати контрольні перевірки стану захисту інформації в ІТС;

- забезпечити конфіденційність робіт з встановлення, експлуатації та обслуговування засобів захисту інформації, встановлених в ІТС (організації);

- сприяти і, за необхідності, брати безпосередню участь у проведенні вищими органами перевірок стану захисту інформації в ІТС;

- сприяти (технічні та організаційні заходи) створенню та дотриманню умов збереження інформації, отриманої організацією на договірній, договірній чи іншій основі від партнерських організацій, постачальників, замовників та фізичних осіб;

- періодично, не рідше одного разу на місяць (інший термін), подавати керівництву організації звіт про стан інформаційної безпеки в ІТС та дотримання користувачами та персоналом ІТС встановленого порядку та правил захисту інформації;

- негайно інформувати керівництво ІТС про виявлені атаки та виявлених порушників;

- інші обов'язки, покладені на керівника та працівників СЗІ відповідно до специфіки та особливостей ІТС (організації).

3. Відповідальність. Керівництво та персонал СЗІ за дисциплінарне чи неналежне виконання посадових обов’язків, порушення встановленого порядку захисту інформації в ІТС несуть дисциплінарну, адміністративну, цивільноправову та кримінальну відповідальність згідно із законодавством України.

Персональна відповідальність керівника та працівників СЗІ визначається посадовими інструкціями.

Начальник СЗІ відповідає за:

- організація роботи із захисту інформації в ІТС, ефективність захисту інформації відповідно до чинних нормативно-правових актів;

- своєчасна розробка та впровадження «плану захисту інформації в ІТС»;

- якісне виконання працівниками 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;

- узгодження планів діяльності підрозділів і служб ІТС (захист інформації);

- створення системи навчання працівників, користувачів, персоналу ІТС з інформаційної безпеки;

- виконання персональних і розпоряджень керівника організації, правил внутрішнього трудового розпорядку, встановленого режиму, правил охорони праці та протипожежного захисту;

Співробітники СЗІ відповідають за:

- дотримання вимог нормативних документів, що визначають організацію роботи із захисту інформації, інформаційних ресурсів і технологій;

- повнота та якість розробки та впровадження організаційно-технічних заходів із захисту інформації в ІТС, точність та достовірність отриманих результатів та висновків з питань, що належать до компетенції СЗІ;

- дотримання термінів проведення контролю, перевірки, перевірки та інших заходів щодо оцінки стану інформаційної безпеки в ІТС, які включені до плану роботи СЗІ;

- якість та законність документування результатів робіт окремих етапів створення КСЗІ, документування результатів перевірок;

- інші питання персональної відповідальності, які покладаються на керівника та працівників СЗІ відповідно до специфіки та особливостей ІТС (організації).

СЗІ взаємодіє, координує та зв’язується з:

- організації РСО;

- служба безпеки організації;

- підрозділи служб безпеки іноземних компаній, їх представництва;

- підрозділ ТЗІ організації;

- зовнішні організації, які є партнерами, користувачами, постачальниками, підрядниками;

- адміністрація ІТС тощо підрозділи організації, виробнича діяльність яких пов'язана із захистом інформації або її автоматизованою обробкою; - іншими суб’єктами діяльності у сфері захисту інформації.

СЗІ координує свою діяльність з аудиторською службою під час проведення аудитів.

СЗІ — це штатний підрозділ організації, безпосередньо підпорядкований керівнику організації або його заступнику, який відповідає за інформаційну безпеку, або є структурним (штатним або сумісним) підрозділом служб безпеки організації.

Структура СЗІ, її склад і чисельність визначаються фактичними потребами ІТС для виконання вимог політики інформаційної безпеки та затверджуються керівництвом організації. Кількість і склад СЗІ мають бути достатніми для виконання всіх завдань із захисту інформації ІТС.

З метою ефективного функціонування та управління захистом інформації в ІТС СЗІ має штатний розклад, який включає перелік функціональних обов’язків усіх працівників, необхідні вимоги до рівня їх знань та навичок.

СЗІ безпосередньо контролює її керівник. У разі, коли СЗІ є структурним підрозділом підрозділу ТЗІ (служби безпеки організації) - керівник цього підрозділу. Призначення та звільнення з посади керівника СЗІ здійснюється керівництвом організації за погодженням з особами, відповідальними за інформаційну безпеку (начальник ТЗІ, начальник служби безпеки та ін.).

Штат СЗІ укомплектований спеціалістами зі спеціальною технічною освітою та практичним досвідом, навичками розробки, впровадження, експлуатації КСЗІ та засобів інформаційної безпеки, а також впровадження організаційних, технічних та

інших заходів із захисту інформації, знаннями та навичками щодо застосовувати нормативні акти. у сфері захисту інформації. [13]

Функціональні обов'язки працівників визначаються переліком і характером завдань, покладених на СЗІ керівництвом ІТС (організації).

Залежно від обсягу та особливостей завдань СЗІ до його складу можуть входити спеціалісти (групи спеціалістів, відділи тощо) різних спеціальностей:

- спеціалісти із захисту інформації від витоку через технічні канали;
- спеціалісти із захисту каналів зв'язку та комутаційного обладнання, налагодження та управління активним мережевим обладнанням;
- спеціалісти з адміністрування засобів захисту, управління базами даних захисту;
- фахівці з безпечних технологій обробки інформації.

Категорії співробітників СЗІ за посадами:

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

Трудові відносини в СЗІ ґрунтуються на законодавстві України з урахуванням положень статуту організації, правил внутрішнього трудового розпорядку та встановлених в організації охорони праці, гігієни та санітарії, інших розпорядчих документів організації. організація. [13]

СЗІ здійснює свою роботу щодо виконання основних організаційно-технічних заходів щодо створення та забезпечення функціонування КСЗІ відповідно до планів роботи. Основою розробки планів роботи є «план захисту інформації в ІТС».

Плани включають такі основні заходи:

- одноразові (одноразові, необхідність повторення яких виникає за умови повного перегляду прийнятих рішень щодо захисту інформації);

- постійно виконуються (заходи, які необхідно виконувати безперервно або дискретно у випадковий або визначений час);
- періодично виконується (із заданим інтервалом часу);
- впроваджуються в міру необхідності (заходи, які необхідно впровадити під час впровадження або настання певних змін в ІТС або зовнішньому середовищі).

Основні види планів робіт СЗІ:

1) Календар планів роботи (для виконання заходів щодо проектування, реалізації, оцінки, впровадження, обслуговування, експлуатації КСЗІ та інше);

2) План дій щодо швидкого реагування на непередбачені ситуації (у тому числі надзвичайні та надзвичайні ситуації) та відновлення роботи ІТС;

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

4) Перспективний план розвитку та вдосконалення діяльності СЗІ із захисту інформації (до 5 років);

5) план заходів із забезпечення інформаційної безпеки під час виконання окремих важливих робіт, нарад, укладення договорів, угод тощо; 6) Бізнес-план створення та функціонування СЗІ.

Плани роботи складаються керівником СЗІ після обговорення на виробничій нараді організаційно-технічних питань, що належать до його 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. Процедура реорганізації або ліквідації здійснюється відповідною комісією, яка створюється наказом (розпорядженням) керівника організації.

З метою забезпечення конфіденційності виконуваної роботи працівниками СЗІ при прийомі на роботу (звільненні) вони дають письмове зобов’язання не

розголошувати відомості, що становлять службову, комерційну чи іншу таємницю, і які стали відомі їм під час роботи в організація.

Матеріально-технічною базою для СЗІ є засоби захисту майна (оперативне управління, повне економічне управління), засоби захисту інформації, програмне забезпечення, технічне та інженерне обладнання, вимірювальне та контрольне обладнання, відповідна документація, а також інші інструменти та обладнання, необхідні для виконання покладених на нього завдання СЗІ.

Засоби захисту інформації та захищені засоби, які використовуються працівниками СЗІ під час виконання службових обов'язків, повинні мати належним чином отриманий документ, що засвідчує їх відповідність вимогам нормативних документів.

СЗІ фінансується:

- кошти, що виділяються в організації на утримання органів управління;
- прибуток організації (ІТС) та інші кошти за рішенням керівництва організації або рішенням загальних зборів акціонерів;
- кошти, отримані за виконання СЗІ договірних робіт і послуг;
- інші джерела фінансування, не заборонені законодавством.

1. Проектна документація на КСЗІ повинна включати:

- технічний проект для КСЗІ та ІТС;
- робоча документація по КСЗІ;
- класифікація інформації;
- класифікація користувачів за рівнем повноважень та їх місцезнаходженням;
- загальний опис КСЗІ;
- модель загроз інформаційної безпеки та модель потенційних порушників;
- опис політики інформаційної безпеки;
- план технічного захисту;
- опис технічних засобів захисту.

2. Експлуатаційна документація на КСЗІ повинна включати:

- накази про створення комісії з перевірки (категоризації) ІТС;
- акт категоризації ІТС;
- наказ про створення СЗІ, призначення адміністратора безпеки та інших адміністраторів;
- наказ про створення комісії з проведення попередніх випробувань КСЗІ;
- програма та методи випробувань;
- протокол попередніх випробувань КСЗІ;
- акт про переведення КСЗІ в дослідну експлуатацію;
- наказ про дослідну експлуатацію;
- журнал навчання користувачів;
- акт завершення дослідної експлуатації;
- політика інформаційної безпеки;
- положення про службу захисту інформації в ІТС;
- план захисту інформації в ІТС;
- інструкції щодо забезпечення режиму безпеки при роботі в ІТС;
- інструкції щодо забезпечення антивірусного захисту інформації в ІТС;
- інструкції для користувачів в ІТС, системного адміністратора;
- інструкції з тестування системи;
- інструкції з поточних і ремонтних робіт;
- інструкції про порядок введення КСЗІ в експлуатацію;
- інструкції про порядок модернізації КСЗІ;
- бланк паспорта на ІТС.

Висновки до розділу.

У розділі було перелічено основні вимоги до створення технічного завдання на створення комплексної системи захисту інформації. Визначено основні загрози та

запропоновано вимоги щодо захисту від них. А також детально оглянуто процес створення та супроводження служби захисту інформації.

РОЗДІЛ 3. СТВОРЕННЯ, УПРАВЛІННЯ ТА ЕКСПЛУАТАЦІЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Процес створення та розробка політики безпеки 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».

Процес створення КСЗІ полягає у реалізації комплексу взаємоузгоджених заходів, спрямованих на розробку та впровадження інформаційної технології, що забезпечує обробку інформації в ІТС відповідно до вимог, встановлених нормативно-правовими актами та НД у сфері захисту інформації.

Порядок створення КСЗІ в ІТС – це сукупність організованих у часі, взаємопов’язаних, об’єднаних в окремі етапи робіт, виконання яких є необхідним і достатнім для створеного КСЗІ. Цей порядок не залежить від того, чи створюється КСЗІ у ІТС, що проектується, чи в існуючій ІТС, якщо є потреба у забезпеченні захисту інформації чи модернізації вже створеної ІТС.[14]

Етапи робіт, що виконуються під час створення КСЗІ в певній ІТС, їх зміст і результати, терміни виконання визначаються ТЗ на створення КСЗІ.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом АС, умовами роботи ІТС.

КСЗІ включає заходи та засоби, що реалізують методи, прийоми, механізми захисту інформації від:

- витоку по технічним каналам, до яких належать канали паразитного електромагнітного випромінювання та наведення, акустоелектричні та інші канали;

- несанкціоновані дії та несанкціонований доступ до інформації, які можуть бути здійснені шляхом підключення до обладнання та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту щодо використання інформації чи нав'язування неправдивої інформації, використання вбудованих пристроїв чи програм, використання комп'ютерних вірусів тощо;

- особливий вплив на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

У випадках, передбачених законодавством, роботи з проектування, розробки, виготовлення, випробування, експлуатації ІТС повинні виконуватися у поєднанні із заходами забезпечення конфіденційності, протидії технічній розвідці, а також режимними заходами щодо захисту ІзОД, що не є державною таємницею.

Створення комплексів ТЗІ від витоку по технічним каналам здійснюється у разі, якщо ІТС обробляє інформацію, що становить державну таємницю, або коли необхідність у цьому визначається власником інформації. [14]

Створення КЗЗ здійснюється в усіх ІТС, де обробляється інформація, що належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначена законом, та в ІТС, де така потреба визначається власником інформації. [14]

Роботу зі створення КСЗІ виконує організація-власник ІТС з дотриманням вимог нормативно-правових актів про діяльність у сфері захисту інформації.

З метою організації роботи зі створення КСЗІ в ІТС створюється служба захисту інформації, визначено порядок створення, завдання, функції, структуру та повноваження в НД ТЗІ 1.4-001-2000.

Якщо ІТС інтегрована, то КСЗІ рекомендується будувати на модульній основі, тобто кожен достатньо самостійний компонент ІТС повинен мати власний модуль КСЗІ, взаємодія між яким забезпечується єдиною підсистемою управління та

обміну інформацією. Вибір заходів та механізмів захисту кожного модуля здійснюється відповідно до політики інформаційної безпеки в ІТС та концепції побудови КСЗІ ІТС, що забезпечує їх узгодження між собою. Цей підхід спрямований на:

- реалізацію відкритої архітектури безпеки, зміст концепції, якої надано в ISO 7498-2-89

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

- уніфікація та оптимізація матеріальних витрат на проектування КСЗІ; ця процедура зводиться до розробки ряду типових компонентів, кожен з яких має лише власні дані (для створення бази даних безпеки), а не механізми захисту;

- можливість оцінювання кожної складової частини КСЗІ окремо (для будьякого виду випробувань).

- **Способи несанкціонованого доступу до інформації здійснюються шляхом**

- Застосування засобів підслуховування, фото, відеоапаратури, підкуп осіб, використання «троянських» програм;

- Використання недоліків мови програмування і недоліків в операційної системи, крадіжка носіїв інформації, копіювання інформації;

- Отримання захищених даних за допомогою запитів дозволу, реквізитів розмежування доступу, таємних паролів.

- **Технічні засоби істотно розширюють і доповнюють можливості людини з добування інформації, забезпечуючи**

- знімання інформації з носіїв, які недоступні органам почуттів людини;
- добування інформації без порушення кордонів контрольованої зони;
- передачу інформації практично в реальному масштабі часу в будь-яку точку земної кулі;
- аналіз і обробку інформації в обсязі і за час, недосяжних людині;
- консервацію і як завгодно довгий зберігання видобутої інформації.

- **Класифікація засобів добування інформації.** До технічних засобів ведення інформаційної боротьби відносять :

- знімання інформації з носіїв, які недоступні органам почуттів людини;
- добування інформації без порушення кордонів контрольованої зони;
- передачу інформації практично в реальному масштабі часу в будь-яку точку
-
-

земної кулі; аналіз і обробку інформації в обсязі і за час, недосяжних людині; консервацію і як завгодно довгий зберігання видобутої інформації.

- До програмних засобів ведення інформаційної боротьби відносять :

- ▪ комп'ютерний вірус (КВ)- спеціальна програма, що впроваджується в “чуже електронне середовище”. КВ спроможний передаватися по лініях зв'язку і мережам обміну інформацією, проникати в електронні телефонні станції і системи управління. У заданий час або по сигналу КВ стирає інформацію , що зберігається в БД, або довільно змінює її;

- ▪ логічна бомба (ЛБ)- так звана програмна закладка, що завчасно впроваджується в інформаційні системи і мережі. ЛБ по сигналу, або у встановлений час, приводиться в дію, стираючи або перекручуючи інформацію в інформаційних ресурсах і виводить їх з ладу;

- ▪ ”троянський кінь” (різновид ЛБ)- програма, що дозволяє здійснювати схований, несанкціонований доступ до інформаційних ресурсів для добування даних;

- ▪ засоби впровадження КВ і ЛБ в інформаційні ресурси ОУ і керування ними на відстані. Для цих засобів найбільш уразливими є інформаційні ресурси виявлення і управління, що постійно діють у встановлених режимах реального часу.

- ▪ ”нейтралізатори текстових програм,” це програми, що забезпечують невиявлення випадкових і навмисних хиб програмного забезпечення; ▪ засоби придушення інформаційного обміну в телекомунікаційних мережах, фальсифікації інформації в каналах.

- **Шкідливе програмне забезпечення**

- **Зловмисний програмний засіб** або **зловмисне програмне забезпечення** (англ. Malware - скорочення від malicious - зловмисний і software - програмне забезпечення) — програма, створена зі злими намірами. До зловмисних програмних засобів належать віруси, рекламне ПЗ, хробаки, троянці, руткіти,

клавіатурні логери, дозвонювачі, шпигунські програмні засоби, здирницькі програми, шкідливі плаґіни та інше зловмисне програмне забезпечення.

- Класифікація:

- . За видом програмного забезпечення:

- ▪ програми, що вимагають програм-носіїв - люки; - логічні бомби; троянські коні; - віруси.

- ▪ програми, що є незалежними. - черв’яки, - зомбі; - утиліти прихованого адміністрування; - програми-крадії паролів; - “intended”-віруси; конструктори вірусів; - поліморфік-генератори.

- . За наявністю матеріальної вигоди:

- *що не приносять пряму матеріальну вигоду тому, хто розробив (встановив) шкідливу програму:*
  - ▪ - хуліганство, жарт;
  - ▪ - самоствердження, прагнення довести свою кваліфікацію; *що приносять пряму матеріальну вигоду зловмисникові:*

- ▪ крадіжка конфіденційної інформації, включаючи діставання доступу до систем банк-клієнт, отримання PIN кодів кредитних карток і таке інше; ▪ отримання контролю над віддаленими комп'ютерними системами з метою розповсюдження спаму з численних комп'ютерів-зомбі;

- За метою розробки програмне забезпечення, яке з самого початку розроблялося спеціально для забезпечення несанкціонованого доступу до інформації, що зберігається на ПК з метою спричинення шкоди (збитку) власникові інформації і/або власникові ПК.

- ▪ програмне забезпечення, яке з самого початку не розроблялися спеціально для забезпечення діставання несанкціонованого доступу до інформації

- ***Різновиди шкідливих програм***

- **Люк (trapdoor)** – це прихована, недокументована точка входу в програмний модуль, яка дозволяє кожному, хто про неї знає, отримати доступ до програми в обхід звичайних процедур, призначених для забезпечення безпеки КС. Люк вставляється в програму в більшості випадків на етапі налагодження для полегшення роботи – даний модуль можна буде викликати в різних місцях, що дозволяє налагоджувати окремі його частини незалежно одна від одної.

- **Логічна бомба** – це код, що поміщається в деяку легальну програму. Він влаштований таким чином, що при певних умовах “вибухає”. Умовою для включення логічної бомби може бути наявність або відсутність деяких файлів, певний день тижня або певна дата, а також запуск додатку певним користувачем.

- **Хробаки** – вид вірусів, які проникають на комп'ютер-жертву без участі користувача. Хробаки використовують так звані «дірки» (уразливості) у програмному забезпеченні операційних систем, щоб проникнути на комп'ютер. Вразливості – це помилки і недоробки в програмному забезпеченні, які дозволяють віддалено завантажити і машинний код, в результаті чого вірусхробак потрапляє в операційну систему і, як правило, починає дії по зараженню інших комп'ютерів через локальну мережу або Інтернет. Зловмисники використовують заражені комп'ютери користувачів для розсилки спаму або для DDoS-атак.

- Так само як для вірусів, життєвий цикл хробаків можна розділити на певні стадії:

- . Проникнення в систему

- . Активація

- . Пошук "жертв"

- . Підготовка копій

- . Поширення копій

- *На етапі проникнення в систему хробаки діляться переважно по типах використовуваних протоколів:*

- ▪ Мережні хробаки - хробаки, що використовують для поширення протоколи Інтернет і локальні мережі. Зазвичай цей тип хробаків поширюється з використанням неправильної обробки деякими

- додатками базових пакетів стека протоколів tcp/ip

- ▪ Поштові хробаки - хробаки, що поширюються у форматі повідомлень електронної пошти

-

▪IRC-хробаки - хробаки, що поширюються по каналах IRC (Internet Relay

- Ch**Е**at)**лектронний посібник**

- ▪ P2P-хробаки - хробаки, що поширюються за допомогою пірінгових (peerto-peer) файлообмінних мереж

- ▪ IM-хробаки - хробаки, що використають для поширення системи миттєвого обміну повідомленнями (IM, Instant Messenger - ICQ, MSN Messenger, AIM й ін.)

- Аналогічно, хробаки можуть міняти тему й текст інфікованого повідомлення, ім'я, розширення й навіть формат вкладеного файлу - виконує модуль, що, може бути прикладений як є або в заархівованому виді.

Віруси – трояни

- **Троян (троянський кінь)** — тип шкідливих програм, основною метою яких є шкідливий вплив стосовно комп'ютерної системи. Трояни відрізняються відсутністю механізму створення власних копій. Деякі трояни здатні до автономного подолання систем захисту КС, з метою проникнення й зараження

системи. У загальному випадку, троян попадає в систему разом з вірусом або хробаком, у результаті необачних дій користувача або ж активних дій зловмисника.

- *У силу відсутності в троянів функцій розмноження й поширення, їхній життєвий цикл украй короткий - усього три стадії:*

- . Проникнення на комп'ютер

- . Активація

- . Виконання закладених функцій

- Троян може тривалий час непомітно перебувати в пам'яті комп'ютера, ніяк не видаючи своєї присутності, доти, поки не буде виявлений антивірусними засобами.

- *Способи проникнення на комп'ютер користувача трояни вирішують звичайно одним із двох наступних методів.*

- **Маскування** — троян видає себе за корисний додаток, що користувач самостійно завантажує з Інтернет і запускає. Іноді користувач виключається із цього процесу за рахунок розміщення на Web-сторінці спеціального скрипта, що використовуючи діри в браузері автоматично ініціює завантаження й запуск трояна.

До даної групи шкідливих програм відносять:

- програми-вандали,
- «дроппери» вірусів, «злі жарти»,
- деякі види програм-люків;
- деякі логічні бомби,
- програми вгадування паролів;
- програми прихованого адміністрування.

- **Зомбі** - це програма, яка приховано під’єднується до інших підключених в Інтернет комп’ютерів, а потім використовує цей комп’ютер для запуску атак, що ускладнює відстеження шляхів до розробника програми-зомбі.

- **"Жадібні" програми (greedy program)**. - це програми, що намагаються монополізувати який-небудь ресурс, не даючи іншим програмам можливості

використовувати його. Доступ таких програм до ресурсів системи призводить до порушення її доступності для інших програм.

- **Захоплювачі паролів** - це спеціально призначені програми для крадіжки паролів.

- **Утиліти схованого адміністрування (backdoor).** Цей вид шкідливого програмного забезпечення у деяких випадках можна віднести до групи троянських коней. Вони по своїй суті є досить могутніми утилітами віддаленого адміністрування комп'ютерів у мережі

- Під час запуску трояну програма встановлює себе в системі і потім стежить за нею, при цьому користувачу не видається ніяких повідомлень про дії такого трояна в системі.

3.2 Управління та експлуатація КСЗІ

Управління – це:

- функція комплексних систем різного характеру, що забезпечує збереження їх специфічної структури, забезпечення режиму роботи, виконання програми, цілей;

- процес інформаційних впливів на об’єкти управління для формування їх цілеспрямованої поведінки;

- процес планування, організації, мотивації та контролю, необхідні для формулювання та досягнення цілей організації;

- функція системи управління, що забезпечує організацію цілеспрямованої діяльності керованої системи.

Сенс і мета управління в КСЗІ - такі зміни організаційної структури, сил і засобів захисту інформації, їх стану, способів і способів застосування, які забезпечують максимальну ефективність їх використання для досягнення цілей захисту інформації.

Управління можливо тільки в тих системах, які мають властивості:

- інформаційні зв'язки відіграють вирішальну роль у збереженні системи в цілому;

- система здатна переходити в різні стани відповідно до керуючих дій;

- існує кілька прийнятних форм поведінки системи, з яких за певними критеріями орган управління обирає найбільш прийнятний;

- процес функціонування системи цілеспрямований;

- система відкрита для зовнішньої дії, тобто вплив зовнішніх дій може мати різноманітний характер і наслідки.

Особливості системи управління КСЗІ:

1) призначені для дії в конфліктних ситуаціях, оскільки захист інформації є складним двостороннім процесом (КСЗІ та порушник);

2) інформація, на основі якої здійснюються управлінські дії (вибір засобів, методів і методів захисту інформації), характеризується значною неповнотою, неточністю та непослідовністю;

3) порушники постійно змінюють засоби і методи дії на систему, тактику своїх дій.

Сутністю управління КСЗІ є цілеспрямована діяльність керівництва організації, посадових осіб та служби захисту інформації, спрямована на досягнення цілей захисту інформації. Які цілі?

1) Забезпечення захисту інформації від несанкціонованого доступу, знищення, зміни, блокування, копіювання, надання, поширення, а також інших протиправних дій щодо такої інформації.

2) Дотримання конфіденційності ІзОД.

3) Реалізація права на доступ до інформації.

4) Забезпечення спостереженості та керованості ІТС.

Керування КСЗІ покликане забезпечити ефективне вирішення наступних завдань:

- недопущення НСД інформації та передачі її особам, які не мають права на доступ до інформації;

- блокування витоку захищеної інформації через технічні канали та канали спеціального впливу;

- своєчасне виявлення фактів НСД до інформації;

- запобігання можливості несприятливих наслідків порушення порядку доступу до інформації;

- запобігання впливу на технічні засоби обробки інформації, внаслідок чого порушується їх функціонування;

- негайне відновлення інформації, зміненої або знищеної в результаті НСД до неї;

- постійний контроль за забезпеченням рівня інформаційної безпеки та гарантій безпеки.

Досягнення основних цілей захисту інформації пов'язане з вирішенням кола завдань, що становлять зміст управління КСЗІ. Основними є:

1) безперервне вилучення, збір, вивчення та аналіз ситуаційних даних;

2) підтримання системи в постійній готовності до виконання завдань із захисту інформації;

3) прийняття рішень щодо захисту інформації;

4) доведення завдань до підлеглих;

5) планування заходів із захисту інформації;

6) організація та забезпечення взаємодії структурних підрозділів організації;

7) комплексне забезпечення заходів із захисту інформації;

8) організація управління, що означає створення системи управління, забезпечення її ефективного функціонування (включаючи захист системи управління від усіх видів дій порушників), а також удосконалення цієї системи із застосуванням нових інформаційних технологій;

9) управління підготовкою підрозділів захисту інформації;

10) організація і здійснення контролю і допомоги підлеглим.

Процес функціонування КСЗІ можна розділити на використання системи за цільовим призначенням, що передбачає реалізацію всього комплексу заходів, безпосередньо пов’язаних із захистом інформації в ІТС, і технічну експлуатацію. Цільове використання передбачає організацію доступу до ресурсів ІТС та забезпечення їх цілісності.

Функції системи розмежування доступу:

- впровадження ПРД суб'єктів та їх процесів до даних;

- впровадження ПРД суб'єктів та їх процесів до механізмів створення друкованих копій;

- відокремлення програм процесу, що виконується в інтересах суб'єкта, від інших суб'єктів;

- контроль потоків даних з метою недопущення запису даних на носії невідповідного штампа;

- реалізація правил обміну даними між суб'єктами для ІТС, побудованих на мережевих принципах.

Правила обмеження доступу передбачають наявність засобів для СРД, які виконують такі функції:

- ідентифікація та автентифікація суб'єктів та підтримка прив'язки суб'єкта до виконуваного для суб'єкта процесу;

- реєстрація дій суб'єкта та його процесу;

- надання можливостей для виключення та включення нових суб'єктів та об'єктів доступу, а також зміни повноважень суб'єктів;

- реагування на спроби НСД, такі як тривога, блокування, відновлення після НСД;

- тестування;

- очищення оперативної пам'яті та робочих зон на магнітних носіях після закінчення роботи користувача із захищеними даними;

- облік оригінальних друкованих і графічних форм та друкованих копій в ІТС;
- контроль цілісності програмно-інформаційної частини як СРД, так і засобів, що її забезпечують.

Ефективність СРД залежить від надійності механізмів автентифікації, яка здійснюється за допомогою криптографічних методів. Під час роботи механізмів автентифікації основними завданнями є:

- створення або виготовлення ідентифікаторів;
- їх облік і зберігання;
- передача ідентифікаторів користувачеві;
- контроль за правильністю проведення процедур автентифікації в ІТС.

При компрометації атрибутів доступу (пароль, персональний код тощо) потрібне їх негайне виключення зі списку дозволених. Ці дії виконує наступний оператор СРД.

Розповсюдження секретних ключів шифрування має здійснюватися за межами захищеної ІТС. Значення ідентифікаторів користувачів не повинні зберігатися та передаватися в системі у відкритому вигляді.

Засоби розмежування доступу до технічних засобів запобігають несанкціонованим діям порушника:

- включення технічних засобів;
- завантажити операційну систему;
- інформація введення-виведення;
- використання нестандартних пристроїв тощо.

Розмежування доступу здійснюється оператором СРД за допомогою використання апаратних та програмних засобів. Він керує використанням ключів блокування блоків живлення безпосередньо на апаратному забезпеченні або на всіх пристроях в окремому приміщенні, дистанційно

керує блокуванням блокування живлення на пристрої або блокуванням завантаження операційної системи.

На апаратному або програмному рівні оператор може змінити технічну структуру інструментів, які може використовувати конкретний користувач.

Апаратно-програмні засоби розмежування доступу до програм і даних використовуються найбільш інтенсивно і значною мірою визначають характеристики СРД. Вони налаштовуються посадовими особами СЗІ і змінюються при зміні повноважень користувача або при зміні програмної та інформаційної структури.

Доступ до файлів регулюється диспетчером доступу. Доступ до записів та окремих полів записів у файлах бази даних також регулюється СКБД.

Ви можете підвищити ефективність СРД, шифруючи файли, що зберігаються на зовнішніх пристроях зберігання даних, а також повністю стираючи файли при їх знищенні та видаляючи тимчасові файли.

У розподілених ІТС доступ між підсистемами регулюється міжмережевими екранами. Брандмауер необхідно використовувати для контролю обміну між захищеними та незахищеними комп’ютерними системами.

Якщо атрибути суб’єкта доступу або алгоритм його дій для цього суб’єкта не дозволені, то подальша робота в ІТС такого порушника припиняється до втручання оператора КСЗІ. Інструменти блокування усувають або значно ускладнюють автоматичний вибір атрибутів доступу.

Журнали подій записують дані про вхід та вихід користувачів із системи, про всі спроби вчинення несанкціонованих дій, про доступ до певних ресурсів тощо. Журнал налаштований на запис певних подій, а його вміст періодично аналізується оператором на чергові та старші посадові особи відділу СЗІ. Процес створення та аналізу журналу має бути автоматизований за допомогою програмного забезпечення.

Безпосереднє управління СРД здійснює черговий оператор КСЗІ, який, як правило, виконує і функції наступного адміністратора ІТС. Він завантажує систему, забезпечує необхідну конфігурацію та режими ІТС, вводить в СРД повноваження та атрибути користувачів, контролює та керує доступом користувачів до ресурсів ІТС.

Підтримка працездатності здійснюється шляхом обслуговування, постійного контролю працездатності та її відновлення у разі відмови. Ефективність засобів захисту інформації постійно контролюється за допомогою апаратно-програмного вбудованого контролю та періодично працівниками служби безпеки та комісіями. Умови контролю та обсяги робіт визначені в керівних документах.

Успіх технічної експлуатації залежить від якості підтримки, яка включає:

- матеріально-технічне забезпечення - дозволяє задовольнити потребу в витратних матеріалах, запасних виробах і пристроях, інструментах та інших матеріальних засобах, необхідних для функціонування КСЗІ;
- транспортування та зберігання захищених ІТС-пристроїв повинні забезпечувати захист від НСД пристроїв у дорозі та на зберіганні. Для забезпечення необхідних умов транспортування та зберігання готуються заходи щодо підготовки приладів відповідно до вимог експлуатаційно-технічної документації;
- метрологічне забезпечення - дозволяє підтримувати засоби вимірювальної техніки в справному стані;
- забезпечення безпеки експлуатації - під час експлуатації важливо забезпечити безпеку персоналу та користувачів, особливо від загрози ураження електричним струмом, а також від можливих пожеж.

Загалом рівень технічної експлуатації багато в чому визначає ефективність використання КСЗІ.

3.3. Моделювання комплексної системи захисту інформації

Систему захисту інформації слід створювати разом із створеною ІТС. Одним з основних етапів розвитку КСЗІ є етап розробки технічного завдання. Саме на цьому етапі вирішуються практично всі специфічні завдання розвитку КСЗІ.

Процес розробки систем, який завершується розробкою технічного завдання, називається науково-дослідною роботою, а решта робіт зі створення складної системи — дослідженнями і розробкою технічного та програмного забезпечення, які проводяться за допомогою систем автоматизації проектування. [11]

При розробці та побудові КСЗІ в ІТС необхідно дотримуватися певних методичних засад дослідження, проектування, виробництва, експлуатації та розробки таких систем.

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

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

Науково-дослідна і дослідно-конструкторська розробка (НДДКР) – це комплекс робіт, спрямованих на отримання нових знань і практичне застосування при створенні нового продукту або технології.

Науково-дослідні роботи (НДР) - науково-дослідні, теоретичні та експериментальні роботи, що виконуються для визначення технічної доцільності створення нової техніки в установлені терміни. НДР поділяється на:

- фундаментальні дослідження (отримання нових знань);

- прикладні дослідження (застосування нових знань для вирішення конкретних проблем).

Дослідно-конструкторська робота (ДКР) і Технологічна робота (ТР) – комплекс робіт з розробки конструкторсько-технологічної документації на дослідний зразок системи, виготовлення та випробування дослідного зразка системи, виконаних за технічним завданням.

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

1) Основні технічні вимоги до КСЗІ:

- значення основних технічних характеристик;

- виконував функції;

- режими роботи;

- взаємодія із зовнішніми системами тощо.

2) Узгоджені взаємні зобов'язання замовника та забудовника.

Основою етапу науково-дослідної розробки КСЗІ є визначення оцінок характеристик апаратно-програмних засобів КСЗІ, а також складу функцій і режимів роботи засобів захисту, порядку їх використання та взаємодії з зовнішні системи. Для проведення досліджень на цьому етапі замовник може залучити підрядника або науково-дослідну установу, або організувати їх спільну роботу.

Розробка досліджень КСЗІ починається з аналізу:

1. Конфіденційність і важливість інформації в ІТС:

- визначаються потоки конфіденційної інформації, елементи ІТС, в яких вона обробляється та зберігається;

- розглянуто питання розмежування доступу до інформації окремих користувачів та сегментів ІТС;

- визначаються вимоги до інформаційної безпеки (шляхом присвоєння грифа конфіденційності, встановлення ПРД).

2. Загрози інформаційній безпеці в ІТС, вразливості в апаратно-програмному забезпеченні та технологіях обробки інформації:

- розробка моделі загроз інформаційної безпеки в ІТС (містить систематизовану інформацію про всі можливі випадкові та навмисні загрози, їх небезпеку, часові рамки дії, ймовірність реалізації).
- розробка моделі порушника, яка орієнтована на висококваліфікованого зловмисника-професіонала, оснащеного всім необхідним і має легальний доступ на всіх лініях захисту.

3. ІТС, що захищається:

- географічне розташування ІТС;
- тип ІТС (розподілений або зосереджений);
- структура ІТС (технічна, програмна, інформаційна);
- продуктивність і надійність елементів ІТС;
- види використовуваного технічного та програмного забезпечення та режими їх роботи;
- взаємодія із зовнішніми системами.

3.4. Методи моделювання КСЗІ

Ефективність захисту інформації — це ступінь відповідності результатів захисту інформації поставленій меті. Оцінка ефективності КСЗІ є складним науково-технічним завданням. У процесі оцінюється комплексна система інформаційної безпеки:

- розвиток ІТС;
- під час роботи ІТС;
- при створенні (модернізації) КСЗІ під існуючі ІТС шляхом моделювання.

Під час розробки КСЗІ поширеним методом проектування є синтез з подальшим аналізом: система синтезується шляхом узгодженого поєднання вузлів,

пристроїв, підсистем і аналізується (оцінюється) ефективність рішення. З множини синтезованих систем за результатами аналізу, який здійснюється за допомогою моделювання, вибирається найкраща.[11]

Моделювання КСЗІ полягає в побудові образу (моделі) системи, з певною точністю відтворюючи процеси, що відбуваються в реальній системі. Реалізація моделі дозволяє отримати та вивчити характеристики реальної системи.

Для подолання складнощів моделювання КСЗІ використовуються різні підходи:

1. Основою спеціальних методів неформального моделювання є застосування положень теорії систем. Основними компонентами теорії неформальних систем є:

1) Структурування архітектури та процесів функціонування КСЗІ – це розробка формального опису складних систем, поширеного на організаційнотехнічні системи.

Умови структурованого опису систем що досліджуються та процесів їх функціонування:

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

2) Неформальні методи оцінки полягають у залученні експертів у відповідних галузях знань для отримання деяких характеристик КСЗІ, які неможливо виміряти безпосередньо або розрахувати за допомогою аналітичних методів.

До таких характеристик КСЗІ відносяться:

- ймовірність реалізації деяких загроз;

- цінність захищеної інформації;

- деякі характеристики ефективності систем захисту тощо.

Найпоширенішими з неформальних методів оцінювання є методи експертних оцінок (асоціації, парні порівняння, вектор уподобань, серединна точка, експертні опитування, Delphi, мозковий штурм, ієрархічний аналіз тощо). Будь-який із методів експертних оцінок є алгоритмом відбору експертів, встановленням правил отримання незалежних оцінок кожним експертом та подальшої статистичної обробки результатів.

3) Неформальні методи пошуку оптимальних рішень поділяються на дві групи:

- методи неформального зведення складної задачі до формального опису та розв’язання задачі формальними методами (з використанням методів теорії нечітких множин, теорії конфліктів, теорії графів, формально-евристичних методів, еволюційного моделювання тощо);

- методи неформального пошуку оптимального рішення ґрунтуються на тому, що людина бере участь не тільки в побудові моделі, а й у процесі її реалізації.

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

Теорія конфлікту моделює конфлікт між правопорушником і системою захисту, який розгортається на тлі випадкових загроз. Обидві протиборчі сторони

переслідують суворо протилежні цілі. Конфлікт розвивається в умовах неоднозначності та поганої передбачуваності процесів, здатності сторін швидко змінювати цілі. Теорія конфліктів — це розвиток теорії ігор, що дозволяє структурувати завдання, вичерпно подати його, знайти сфери кількісної оцінки, упорядкування, переваги, визначити домінуючі стратегії, якщо вони існують.

З теорії графів для дослідження систем інформаційної безпеки ми переважно використовуємо апарат мереж Петрі. Управління станом у вузлах Петрі дозволяє моделювати процеси подолання захисту з боку порушника.

Формально-евристичні методи включають методи пошуку оптимальних рішень не на основі строгих математичних, логічних співвідношень, а на основі людського досвіду, наявних знань та інтуїції. Отримані рішення можуть бути далекі від оптимальних, але вони завжди будуть кращими за рішення, отримані без евристичних методів. Найпоширенішими з евристичних методів є лабіринтний і концептуальний методи.

У моделі лабіринту проблема подається людині у вигляді лабіринту можливих рішень. Передбачається, що фахівець має здатність швидко відрізати неперспективні шляхи лабіринту і серед шляхів, що залишилися, швидше за все, знайти спосіб вирішення проблеми.

Понятійний метод передбачає виконання дій з поняттями, що означає узагальнені елементи та зв’язки між ними. Поняття формуються в процесі побудови структурованої моделі. Фахівець проводить уявний експеримент зі структурованою моделлю і створює обмежену область лабіринту, в якій легко знайти рішення.

Еволюційне моделювання є різновидом моделювання. Його особливість полягає в тому, що в процесі моделювання вдосконалюється алгоритм моделювання.

2. Декомпозиція загального завдання оцінки ефективності КСЗІ. Для вирішення проблеми складності дослідження КСЗІ використано метод

декомпозиції (розподілу) загальної задачі оцінки ефективності ряду часткових задач:

- оцінка ефективності захисту від збоїв і збоїв технічних і програмних засобів;
- оцінка ефективності захисту від НСД;
- оцінка ефективності захисту від ПЕМВН;
- оцінка ефективності захисту від розголошення;
- оцінка ефективності захисту каналів зв'язку тощо.

Наприклад, при оцінці ефективності захисту від збоїв, що призводять до знищення інформації, ймовірність відмови системи P (t) за час t, яка розраховується за формулою:

$$\boldsymbol{P(t) = 1 - P_{від}(t)},$$

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

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

$$\boldsymbol{P_{від}(t) = e^{-\lambda \cdot t}},$$

де – інтенсивність відмов системи (число відмов в одиницю часу).

Просто вирішується задача оцінки ефективності методу шифрування за умови, що атака на шифр можлива тільки шляхом перебору ключів, і відомий метод шифрування. Середній час злому шифру за цих умов розраховується по формулі:

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

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.

Основна складність методу декомпозиції при оцінці КСЗІ полягає у врахуванні взаємозв’язку та взаємовпливу окремих завдань оцінки та оптимізації. Цей вплив враховується як при розв’язанні задачі декомпозиції, так і в процесі отримання інтегральних оцінок.

3. Для загальної оцінки системи проводиться макромоделювання КСЗІ. Завдання спрощується використанням при побудові моделі лише основних характеристик КСЗІ. Такі моделі використовуються в основному для отримання попередніх оцінок системи. [11]

Наприклад, якщо КСЗІ використовує k рівнів безпеки, а порушник не має жодного офіційного статусу на об’єкті ІТС, він чи вона повинні подолати всі k рівнів безпеки, щоб отримати доступ до інформації.. Для такого порушника ймовірність діставання несанкціонованого доступу до інформації $P_{\text{нсд}}$ може бути розрахована за формулою:

$$\boldsymbol{P}_{\text{нсд}} = \prod_{\boldsymbol{i}=\boldsymbol{1}}^{\boldsymbol{k}} \boldsymbol{P}\boldsymbol{i},$$

де $\boldsymbol{P}_{\boldsymbol{i}}$ – ймовірність подолання порушником i-го рівня захисту.

На макрорівні можна, наприклад, вивчити необхідну кількість рівнів захисту, їх ефективність по відношенню до передбачуваної моделі порушника з урахуванням особливостей ІТС та фінансових можливостей проектування та побудови КСЗІ.

3.5. Показники ефективності та оптимальності КСЗІ

Проектування та функціонування КСЗІ виявили проблеми, вирішення яких можливе лише на основі комплексної оцінки різноманітних факторів, неоднорідних взаємозв’язків, зовнішніх умов. У зв'язку з цим в системному аналізі є розділ, пов'язаний з визначенням якості систем та ефективності процесів, реалізованих у цих системах.

Цілі оцінки складних систем:

- оптимізація - вибір найкращого алгоритму з кількох, що реалізують закон роботи системи;

- ідентифікація - визначення системи, якість якої найкраще відповідає реальному об'єкту в заданих умовах;

- підготовка даних для прийняття рішень з управління системою.

Оцінка ефективності КСЗІ можлива за умови визначення показників її ефективності. Показник продуктивності системи є мірою якості вирішення системою проблеми, з якою вона стикається.

Вимоги до показників продуктивності системи:

1) обчислювальна потужність - значення можуть бути розмірними або безрозмірними значеннями, що дозволяють кількісно оцінити вплив системи;

2) адекватність - відповідність меті системи (адекватний показник дозволяє оцінити ефективність системи за ступенем досягнення її основного призначення);

3) зміст (повнота) - здатність індикатора досліджувати ефективність системи без залучення інших характеристик;

4) чутливість - здатність індикатора реагувати на зміни характеристик середовища і систем, що впливають на ефективність.

Ефективність системи є мірою її доцільності, пов'язаної з її призначенням, її рентабельністю, показником її здатності продуктивно працювати, а в кінцевому підсумку - мірою її життєздатності. [11]

Поняття ефективності завжди пов’язане з отриманням деякого корисного результату, який називається виграшем G. Прибуток одержується за рахунок енергії, інформації, грошей та інших витрат, що забезпечують функціонування системи, і називається виплатою С.

Необхідно створити або вибрати такі механізми захисту інформації та методи управління системою захисту, при яких забезпечується виконання всього набору необхідних функцій і досягається максимум або мінімум обраного критерію, а також обмеження на деякі показники ефективності. спостерігаються. [11]

Це твердження застосовне не тільки для вирішення загальної проблеми, а й часткових завдань оцінки ефективності комплексної системи захисту інформації.

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

1. Класичний підхід полягає у визначенні оцінки ефективності КСЗІ на основі використання критеріїв ефективності, отриманих за допомогою показників ефективності. Значення показників ефективності визначають шляхом моделювання або розрахунку характеристик реальних ІТС та систем безпеки в них.

Такий підхід використовується при розробці та модернізації КСЗІ. Проте можливості класичних методів комплексної оцінки ефективності щодо КСЗІ обмежені через ряд обставин:

- високий ступінь невизначеності вихідних даних;
- складність формалізації процесів функціонування;
- відсутність загально визначених методів розрахунку показників ефективності та вибору критеріїв оптимальності тощо.

2. Офіційний підхід пов’язаний із застосуванням системи нормативних актів чи стандартів держави, які визначають вимоги до захисту інформації різних категорій конфіденційності та важливості. Вимоги до КСЗІ встановлені переліком механізмів захисту інформації, які повинні мати ІТС для відповідності певному профілю безпеки. Використовуючи такі документи, можна оцінити ефективність КСЗІ. При цьому критерієм ефективності КСЗІ є відповідність його характеристик і можливостей заданому профілю безпеки, зазначеному в ТЗ. Безсумнівною

перевагою такого підходу до оцінки ефективності КСЗІ є простота його використання. Основним недоліком офіційного підходу до визначення ефективності систем захисту є те, що він не визначає ефективність того чи іншого механізму захисту, а констатує лише факт його наявності чи відсутності. Цей недолік певною мірою компенсується завданням у регламенті достатньо детальних вимог до цих механізмів захисту та вказівкою гарантій. [11]

3. Експериментальний підхід полягає в тому, що ефективність існуючих КСЗІ оцінюється за спробами подолати захисні механізми системи спеціалістами, які виступають у ролі порушників. Процедура експериментальної перевірки така:

- умовним порушником обрано одного або кількох спеціалістів у сфері інформаційної боротьби вищої кваліфікації;

- складається план експерименту, який визначає порядок та матеріальнотехнічне забезпечення проведення експериментів з виявлення слабких місць у системі захисту (це може імітувати дії порушників, що відповідають різним моделям їх поведінки: від некваліфікованого порушника до висококваліфікованого офіцер безпеки);

- служба захисту інформації впроваджує нові механізми захисту (замінює старі) в КСЗІ до тих пір, поки «порушники» не подолають захист, щоб уникнути «злому» системи захисту;

- «порушник», який використовує стандартні інструменти ІТС або впроваджує власне обладнання та програмне забезпечення, намагаючись «зламати» систему безпеки.

Такий підхід до оцінки ефективності дозволяє отримати об’єктивні дані про можливості існуючих КСЗІ, але вимагає високої кваліфікації виконавців та великих матеріальних і часових витрат. Для проведення дослідів необхідно мати найсучасніше обладнання (засоби інженерно-технічної розвідки, програмнотехнічні та випробувальні комплекси (стенди) тощо).

Висновки до розділу.

У даному розділу наведено методи створення, управління та експлуатації комплексної системи захисту інформації відповідно до НД ТЗІ. Визначено цілі керуючого персоналу, їх склад та повноваження. Поставлені цілі були досягнуті, результати представлені. розділі наведено основні концепції науково-дослідної розробки систем захисту інформації. Розглянуто методи моделювання комплексних систем. Подані формули на визначення показників ефективності систем що були досліджені у ході роботи.

ВИСНОВКИ

У процесі виконання дипломного проєкту було систематизовано ключові терміни й визначення, що стосуються побудови комплексної системи інформаційної безпеки (КСІБ) у контексті комп’ютерно-інженерного підходу. Описано базові принципи її проектування з урахуванням вимог до архітектури обчислювальних систем та сучасних мережевих інфраструктур.

Були сформульовані функціональні завдання та цілі інформаційного захисту, а також визначено типові об’єкти захисту, серед яких — комп’ютерні вузли, мережеві інтерфейси, програмні компоненти та канали передавання даних. Очевидно, що в умовах стрімкої цифровізації та широкого використання систем обробки даних, необхідність у багаторівневому захисті критичної інформації з обмеженим доступом є фундаментальною для будь-яких сучасних організацій — як у сфері бізнесу, так і в державному секторі.

На основі аналізу актуальних векторів несанкціонованого втручання в інформаційні системи та комп’ютерні мережі здійснено їх класифікацію за параметрами походження, засобу реалізації, джерела загрози та вектору впливу. У процесі дослідження було виявлено типові вразливості, що виникають під час розробки інформаційної безпеки, зокрема: ризики деструктивних дій користувачів і шкідливого ПЗ, втрата даних, збої у функціонуванні обчислювальних систем, а також недоліки в адмініструванні комп’ютерних мереж.

Сформульовано концептуальні засади інженерного проєктування засобів кіберзахисту, враховуючи новітні підходи до моделювання цифрових систем, симуляції сценаріїв атак, а також структуризації процесів моніторингу та протидії загрозам. Запропоновано формалізовані математичні моделі для оцінювання ефективності функціонування компонентів КСІБ, з використанням кількісних показників доступності, надійності та цілісності інформації.

Розглянуто вимоги до розроблення технічного завдання на створення КСІБ з урахуванням стандартів НД ТЗІ, ISO/IEC 27001 та методологій побудови систем реального часу й вбудованих платформ. Також проаналізовано типові загрози — від соціотехнічних атак до мережевого сканування, — та розроблено інженерні вимоги до засобів захисту.

Окрему увагу приділено моделюванню цифрового контуру служби захисту інформації: від етапу впровадження до технічного супроводу і модернізації. Детально описано процедури управління, моніторингу та реагування на інциденти безпеки в умовах гібридної ІТ-інфраструктури.

Згідно з вимогами нормативно-правової бази (НД ТЗІ України), визначено повноваження та відповідальність керуючого персоналу, включаючи системних адміністраторів, фахівців з кібербезпеки та розробників, залучених до експлуатації й підтримки КСІБ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Основні засади розвитку інформаційного суспільства в Україні на 20072015 роки [Текст] : Закон України № 537-V від 09.01.2007 р. / Верховна Рада України // Відомості Верховної Ради України. – 2007, № 12, ст.102 – [Електронний ресурс] // Режим доступу: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=53716#n14

2. Про інформацію [Текст] : Закон України № 2658-XII від 02.10.1992 р. / Верховна Рада України // Відомості Верховної Ради України. – 1992. – №48. – [Електронний ресурс] // Режим доступу: https://zakon.rada.gov.ua/laws/show/265712#Text

3. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу – [Електронний ресурс] // Режим доступу: https://tzi.ua/assets/files/1.1_003_99.pdf

4. Про Державну службу спеціального зв'язку та захисту інформації України

[Текст] : Закон України № 3475-IV від 23.02.2006 р. / Верховна Рада України // Відомості Верховної Ради України. – 2006, № 30, ст. 258 – [Електронний ресурс] // Режим доступу: https://zakon.rada.gov.ua/laws/show/3475-15#Text

5. Про державну таємницю [Текст] : Закон України № 3855-XII від 21.01.1994 р. / Верховна Рада України // Відомості Верховної Ради України. – 1994, № 16, ст.

93 – [Електронний ресурс] // Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text

6. Про захист інформації в інформаційно-телекомунікаційних системах [Текст] : Закон України № 80/94-ВР від 05.07.1994 р. / Верховна Рада України // Відомості Верховної Ради України. – 1994, № 31, ст.286 – [Електронний ресурс] // Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

9. Гапак О. М., Балога С. І. Захист інформації в комп'ютерних системах: підручник для студентів спеціальності 123 «Комп'ютерна інженерія» / уклад. О. М. Гапак, С. І. Балога; рец. М. І. Глебена. – Ужгород: ПП «АУТДОР-ШАРК», 2021. – 184 с.

10. Вишняков В. М. Захист інформації в комп'ютерних системах: навчальний посібник / В. М. Вишняков. – Київ: КНУБА, 2022. – 119 с.

11. Ананьїн В. О., Горлинський В. В., Гангал А. В. Інформаційна безпека. Менеджмент інформаційної безпеки держави: курс лекцій / В. О. Ананьїн, В. В. Горлинський, А. В. Гангал. – Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2025. – 140 с.

12. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека: навчальний посібник. Ч. 2 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: ХНЕУ, 2008. – 196 с.

13. Вакалюк Т. А. Захист інформації в комп'ютерних системах: навчально-методичний посібник для студентів напряму 6.040302 «Інформатика» / Т. А. Вакалюк. – Житомир: Вид-во ЖДУ ім. І. Франка, 2012. – 120 с.

14. Конахович Г. Ф., Климчук В. П., Паук С. М., Потапов В. Г., Горбунов О. О. Захист інформації в телекомунікаційних системах / Г. Ф. Конахович та ін. – Київ: НАУ, 2016. – 240 с.

15. Гуржій А. М., Возненко Л. І., Поворознюк Н. І., Самсонов В. В. Основи інформаційних технологій: навчальний посібник для здобувачів професійної (професійно-технічної) освіти / А. М. Гуржій та ін. – Київ: Літера ЛТД, 2023. – 288 с.

16. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. – [Електронний ресурс] // Режим доступу: https://tzi.ua/assets/files/3.7-001-99.pdf

17. Завгородний В. И. Комплексная система защиты в компьютерных системах : Учебное пособие. - М. : Логос; ПБОЮЛ Н. А. Егоров, 2001. – 264 с.

18. 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.

19. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах – [Електронний ресурс] // Режим доступу: https://tzi.com.ua/downloads/2.6001-11.pdf

20. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі – [Електронний ресурс] // Режим доступу: https://tzi.com.ua/downloads/1.4-001-2000.pdf

21. НД ТЗІ 3.7-003 -2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі – [Електронний ресурс] // Режим доступу: https://tzi.com.ua/downloads/3.7-0032005.pdf

22. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. – [Електронний ресурс] // Режим доступу: https://tzi.com.ua/downloads/1.1-005-07.pdf

23. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення

24. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу – [Електронний ресурс] // Режим доступу: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf

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

26. Гайворонський М.В. Безпека інформаційно-комунікаційних систем / Гайворонський М.В., Новиков О.М. – К.: вид. група BHV, 2009. – 608 с.

27. Павлов І.М. Проектування комплексних систем захисту інформації / І.М.

Павлов, В.О. Хорошко. – К: – ВІТІ – ДУІКТ, 2011. – 245 с.

28. 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 – [Електронний ресурс] // Режим доступу: https://tzi.com.ua/downloads/3.6-001-2000.pdf