НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Дослідження проблем оцінки відповідності функціональних компонентів систем захисту інформації»

Виконав:
студент ІІ курсу, групи ТС-71мп
Некраш Іван Іванович _____

Керівник:
доктор технічних наук, професор кафедри ТС
Горицький В. М. _____

Рецензент:
Посада, науковий ступінь, вчене звання,
Прізвище, ініціали _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент (-ка) _____

Київ – 2018

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (спеціалізація) – 172 «Телекомунікації та радіотехніка» (172.3620.1 «Телекомунікаційні системи та мережі»)

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Л.О. Уривський

«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Некрашу Івану Івановичу

1. Тема дисертації «Дослідження проблем оцінки відповідності функціональних компонентів систем захисту інформації», науковий керівник дисертації Горицький Віктор Михайлович професор кафедри ТС, затверджені наказом по університету від «___»_____ 20__ р. №_____

2. Термін подання студентом дисертації _____

3. Об’єкт дослідження неструктурована інформація.

4. Предмет дослідження алгоритми аналізу неструктурованої інформації.

5. Перелік завдань, які потрібно розробити:

6. Орієнтовний перелік графічного (ілюстративного) матеріалу

Плакат №1 «Тема, мета та завдання магістерської дисертації»

Плакат №2 «Актуальність та постановка задачі»

Плакат №3 «»

Плакат №4 «»

Плакат №5. «»

Плакат №6. «Висновки»

7. Орієнтовний перелік публікацій

8. Дата видачі завдання 21 жовтня 2017.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Ознайомлення з існуючими стандартами в сфері інформаційної безпеки.		
2	Аналіз стандартів в сфері ІБ та їх застосування: ISO/IEC 15408-1:2009; ISO/IEC 15408-2:2008; ISO/IEC 15408-3:2008; ISO/IEC 18045:2008		
3	Дослідити ключові поняття функціональних вимог інформаційної безпеки, які можуть бути предявлені до обєкту оцінки.		
4	Дослідити структуру функціонального класу (сімейства, компоненту) інформаційної безпеки		
5	Підготовка статей по темі роботи		
6	Доповідь по темі роботи на		

	науково-технічних конференціях		
7	Дослідження вимог та їх реалізація у відповідності до ISO:15408		
8	Розрахунок кількісного показника захищеності інформаційної системи від несанкціонованого доступу		
9	Узагальнення і оцінювання результатів досліджень, підготовка підсумкового звіту. Подання роботи до приймання, та її захист.		

Студент Некраш І.І.

Науковий керівник дисертації Горицький В.М.

РЕФЕРАТ

Обсяг магістерської дисертації складає 93 сторінки, зокрема 33 ілюстрації, 2 таблиці та 12 джерел інформації.

Актуальність теми. Не викликає жодних сумнівів, що в наш час ключове місце в діяльності як окремої людини, так і суспільства в цілому займає інформація та все, що з нею пов’язано: створення, обмін, використання, знищення. Мабуть, вона є одним з найцінніших ресурсів, якими оперує людство.

Володіння певною інформацією може відкрити пепред людиною незвідані можливості, а втрата до невиправних наслідків. Отже, однією з найсерйозніших проблем пов’язаних з оперуванням інформацією є забезпечення безпеки цих операцій. Інформація може бути викраденою чи неправомірно зміненою, або навіть втраченою під впливом великої кількості факторів.

З метою мінімізації ризиків в різних куточках світу постійно створюються та вдосконалюються методи для попередження та протидії негативним факторам, які впливають на інформацію. Як результат створюються різноманітні нормативні документи та стандарти у яких одна мета – підвищити рівень інформаційної безпеки.

Метою випускної роботи є проведення дослідження найвідоміших стандартів у сфері інформаційної безпеки, аналіз їх переваг та недоліків. Дослідити повноту покриття вимог функціональними компонентами, визначеними в ISO/IEC:15408. Виконати розрахунок показника, котрий дозволить кількісно оцінити ступінь відповідності проектованої системи при різних вимогах до безпеки до вимог, що вимагаються обраним стандартом.

Відповідно до поставленої мети були сформульовані такі **завдання:**

- Розглянути основні стандартив сфері інформаційної безпеки та вибрати один з них для подальшого дослідження;
- Проаналізувати вибраний стандарт
- Виконати розрахунок кількісного показника, який дозволить провести оцінку відповідності інформаційної системи до вимог стандартів.

Об’єктом дослідження є інформаційна безпека

Предметом дослідження є стандарти в сфері інформаційної безпеки

Методи дослідження. В ході роботи були використані: методи теоретичного дослідження.

Апробація результатів дисертації. Основні результати дисертаційного дослідження оприлюднено в ході Міжнародної конференції "Проблеми телекомунікацій" на базі Інституту телекомунікаційних систем і НДІТ НТУУ "КПІ"., 2018. (м. Київ)

Публікації. Основні положення і результати дисертаційної роботи знайшли своє відображення на Міжнародній конференції "Проблеми телекомунікацій" на базі Інституту телекомунікаційних систем і НДІТ НТУУ "КПІ"., 2018. (м. Київ).

ABSTRACT

The work contains 93 pages, 33 illustrations, 2 tables and 12 sources.

Relevance of the topic There is no doubt that in our time the key place in the activity of both an individual and society as a whole has information and everything connected with it: creation, exchange, use, destruction. Apparently, it is one of the most valuable resources mankind uses.

Possession of certain information may open a lot of possibilities to person, and loss to irreparable consequences. Hence, one of the most serious problems with operating information is to ensure the security of these operations. Information may be stolen or improperly modified, or even lost under the influence of a large number of factors.

Methods for preventing and reacting to negative factors that affect information are constantly being created and improved in different parts of the world. As a result, various normative documents and standards are created which have one common goal - to increase the level of information security.

The **purpose** of the thesis is to research of the most famous standards in the field of information security, analysis of their advantages and disadvantages. Explore the completeness of the requirements coverage with the functional components defined in ISO/IEC:15408. Perform calculation of the indicator, which will allow to quantify the degree of conformity of the designed system with different safety requirements to the requirements required by the chosen standard.

In accordance with the stated goal, the following **objectives** were formulated:

Consider the main information security standard and select one for further research;

Analyze the selected standard;

Perform a calculation of the quantitative indicator, which will allow assessing the compliance of the information system with the requirements of the standards.

The **object** of research is an information security.

The **subject** of research are standarts in field of information security.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

COBIT	Control Objectives for Information and Related Technologies
IEC	Міжнародна електротехнічна комісія
ISO	Міжнародна організація зі стандартизації
ITL	Лабораторії інформаційних технологій
АС	Автоматизована система
ЗК	Загальні критерії
ІБ	Інформаційна безпека
ІС	Інфромаційна система
ІТ	Інформаційні технології
ІТС	Інформаційно-телекомунікаційні системи
КСЗІ	Комплексна система захисту інформації
ОО	Об'єкт оцінки
ПЗ	Профіль захисту
СУІБ	Система управління інформаційною безпекою
ФБО	Функції безпеки об'єкта

ВСТУП

В ході бурхливого розвитку наукового прогресу, відбувається невпинне підвищення значущості інформації в житті людства. Все більший відсоток даних переходить з паперового вигляду до електронного. Для обслуговування всієї цієї інформації необхідні системи, котрі зможуть забезпечити необхідний рівень захищеності даних, адже найменша вразливість може бути використана зловмисниками для досягнення, не завжди, добрих цілей.

Є великий перелік факторів, що впливають на інформаційні системи, від єлементарного людського фактору, іншими словами помилки, до навмисного втручання у фізичні середовищ розповсюдження сигналів, для подальшого спотворення або викрадення інформації, яку вони несуть.

Проводячи точкові дії в рамках однієї компанії чи установи, звісно, можна досягти певних успіхів у вирішенні даної проблеми, але в такому випадку нічого не зміниться глобально. Саме з метою вирішення глобальної проблеми спеціалісти почали описувати загальні підходи щодо вирішення проблеми, які виливаються у стандартизовані рішення.

Отже, актуальність дослідження стандартів у сфері інформаційної безпеки є дуже високою. Правильне та осмислене їх використання дозволить будувати інформаційні системи з високим рівнем захищеності, в чому є зацікавленість як простих людей, так і державних установ або великих корпорацій.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ ІСНУЮЧИХ СТАНДАРТІВ ЩОДО ПОБУДОВИ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Основні стандарти в сфері забезпечення інформаційної безпеки

Будь-яке забезпечення інформаційної безпеки потребує контролю і перевірки, які не можуть бути проведені тільки методом індивідуальної оцінки, без урахування міжнародних і державних стандартів.

Формування стандартів інформаційної безпеки відбувається після чіткого визначення її функцій і меж. Інформаційна безпека - це конкретний стан систем, пов’язаних з обробкою та зберіганням даних, при якому забезпечується конфіденційність, цілісність та доступність останніх.

Для визначення стану інформаційної безпеки найбільш застосовна якісна оцінка, так як висловити ступінь захищеності або уразливості в процентному співвідношенні можливо, але це не дає повної і об'єктивної картини. [1]

Для оцінки і аудиту безпеки інформаційних систем можна застосувати ряд інструкції і рекомендацій, які і мають на увазі під собою нормативне забезпечення.

Контроль і оцінка стану безпеки здійснюється шляхом перевірки їх відповідності стандартам державним і міжнародним (ISO, Common criteris for IT security).

Міжнародний комплекс стандартів, розроблених Міжнародною Організацією по Стандартизації (ISO), являє собою сукупність практик і рекомендацій щодо впровадження систем і устаткування для забезпечення захисту інформації. [2]

Найвідомішими стандартами в сфері забезпечення інформаційної безпеки визнано:

- Критерій оцінки надійності комп'ютерних систем «Помаранчева книга» (США);
- Гармонізовані критерії європейських країн;
- Рекомендації X.800;
- Стандарт BSI;
- Стандарт BS 7799;
- Стандарт «Загальні критерії» ISO:15408;
- Стандарт ISO:17799;
- Стандарт COBIT
- Система стандартів NIST
- Стандарти НД ТЗІ

1.2 Огляд системи стандартів NIST

Національний інститут стандартів і технології — є національним органом США, відповідальний за проведення стандартизації.

NIST — некомерційна та не пов'язана з урядом організація, яка координує роботи, пов'язані з добровільною стандартизацією в приватному секторі економіки, слідкує за діяльністю організацій, що розробляють стандарти та приймає рішення щодо надання стандартам статусу національних (у випадку, коли в ньому є зацікавленість з боку різних фірм і стандарт набуває статусу міжгалузевого).

NIST це єдина організація в США, яка приймає (затверджує) стандарти національного рівня. Основним завданням NIST є допомога у вирішенні проблем, загальнодержавного значення (забезпечення економії енергоресурсів, захист оточуючого середовища, підвищення рівня безпеки життя людей і умов на виробництві).

Спеціальна публікація NIST 800-53 - це частина спеціальної публікації 800-серії, яка звітує про дослідження, керівні принципи та інформаційну діяльність лабораторії інформаційних технологій (ITL) в галузі безпеки інформаційної системи та про діяльність ITL з промисловістю, урядом та академічними організаціями.

Зокрема, NIST Special Publication 800-53 охоплює кроки в рамках управління ризиками, які стосуються вибору контролю безпеки для федеральних інформаційних систем відповідно до вимог безпеки в Федеральному стандарті обробки інформації (FIPS) 200. Це включає в себе вибір початкового набору базової безпеки контроль на основі аналізу найгіршого впливу FIPS 199, розробка базового контролю безпеки та доповнення контролю безпеки на основі організаційної оцінки ризику. Правила безпеки охоплюють 17 областей, включаючи контроль доступу, реакцію на інциденти, безперервність бізнесу та відновлення функціонування систем після аварій.

Ключовою частиною процесу сертифікації та акредитації для федеральних інформаційних систем є відбір та реалізація підмножини контролю (гарантій) з каталогу контролю безпеки (NIST 800-53, додаток F). Ці засоби контролю - це управління, оперативні та технічні гарантії (або контрзаходи), встановлені для інформаційної системи для захисту конфіденційності, цілісності та наявності системи та її інформації. Для здійснення необхідних гарантій або контролю агентства повинні спочатку визначити категорію безпеки своїх інформаційних систем відповідно до положень FIPS 199 "Стандарти для категоризації безпеки Федеральних інформаційно-інформаційних систем". Класифікація рівня безпеки інформаційної системи (низька, середня або висока) визначає базовий набір елементів керування, які треба впровадити та проводити контроль. Агентства

мають можливість регулювати ці елементи керування та адаптувати їх до більш точної відповідності до організаційних цілей організації або середовищу функціонування.

Даний стандарт описує контролі безпеки, та інструкції щодо того, як їх правильно використовувати. Всі контролі в даному стандарті поділено на сімейства, які відповідають різним сферам забезпечення інформаційної безпеки [3]. Сімейства контролів, визначених в NIST наведено в таблиці 1.1.

Таблиця 1.1 Сімейства контролів NIST

Скорочення	Сімейство контролю (оригінальна назва)	Переклад
AT	Awareness and Training	Обізнаність та навчання
AU	Audit and Accountability	Аудит та звітність
CA	Security Assessment and Authorization	Авторизація та оцінювання безпеки
CM	Configuration Management	Керування конфігурацією
CP	Contingency Planning	Планування неперервності бізнесу
IA	Identification and Authentication	Ідентифікація та автентифікація
IR	Incident Response	Реакція на інциденти
MA	Maintenance	Підтримка
MP	Media Protection	Захист носіїв інформації

Продовження таблиці 1.1

PE	Physical and Environmental Protection	Захист від впливу середовища
PL	Planning	Планування
PS	Personnel Security	Безпека персоналу
RA	Risk Assessment	Оцінювання ризиків
SA	System and Services Acquisition	Придбання систем та сервісів
SC	System and Communications Protection	Захист систем та комунікацій
SI	System and Information Integrity	Цілісність системи та інформації
PM	Program Management	Керування програмою ІБ

Опис конжного контроля підпорядкований шаблону. Перш за все зазначено код сімейства контролів та його номер, наприклад, AU-2. Далі вказано його назву.

Основна частина складається з наступних розділів:

- Control. Опис специфічних дій або активностей, які виконуються організацією або ІС та мають відношення до забезпечення безпеки. Для певних контролів передбачено можливость гнучкого налаштування, яке надає можливість для організацій визначати окремі з параметрів, пов'язаних з контролем. Для прикладу, в ролі такого параметра може бути частота проведення аудитів, тривалість зберігання журналу логування або кількість спроб користувачів

авторизуватися, що закінчились невдачею. Це дозволяє підлаштовувати контролі під потреби конкретной організації, спираючись на вимоги, запропоновані до забезпечення безпеки зі сторони цілей поставлених організацією, результатів оцінок рівня ризику та прийнятності його, також можна розглядати вимоги з боку закону і регуляторів.

- Supplemental Guidance. Додаткові відомості для певного контроля. Включає в себе роз'яснювальну інформацію стосовно імплементації та використання контролю і т.д. Додатково можна зазначити посилання на пов'язані з ним контролі.
- Control Enhancements. Дана секція визначає можливості для «покращення» контролів, додаючи до нього додаткову функціональность.
- References. Включає в себе посилання на закони, нормативні акти і т.д.
- Priority and Baseline Allocation. Має вигляд таблички, в якій зведено інформацію щодо рекомендованого пріоритету в ході прийняття рішенн про реалізацію контролів і стартовий розподіл контролів серед базових наборів для систем з різними рівнями критичності. Пріоритизація імплементації дає змогу організаціям проводити реалізацію контролів ефективніше та в правильній послідовності, спочатку імплементуючи основоположні заходи.

Для впорядкування та забезпечення структурності підходу проведено розподіл контролів за різними типами. Він залежить від призначення контроля:

- Common. Загальні контролі, такі, що можуть бути успадкованими різноманітними системами і можуть бути використаними поза

межами окремої ІС. Контроль безпеки успадковується в тому разі, коли він виконує свої функції безпеки в ІС, проте був розроблений, реалізований, оцінений, авторизований за межами цієї ІС

- System-specific. Контроль створено та реалізованоконкретної для використання в конкретній ІС.
- Hybrid. Контроль частково функціонує як загальний, і частково в ролі специфічного для системи.

1.3 Критерій оцінки надійності комп'ютерних систем «Помаранчева книга» (США)

Офіційною назвою данного стандарту є «Критерії визначення безпеки комп'ютерних систем»

Даний стандарт розроблений Міністерством оборони США. Він встановлює основні умови для оцінки ефективності засобів комп'ютерної безпеки, що містяться в комп'ютерній системі. Критерії використовуються для визначення, класифікації та вибору комп'ютерних систем, призначених для обробки, зберігання та пошуку важливої або секретної інформації.

При розробці критеріїв переслідувались три мети:

- запропонувати користувачам критерій, використовуючи який можна було б оцінити ступінь довіри до обчислювальної системи розглядаючи забезпечення безпеки обробки секретної та іншої критично важливої інформації;
- створити керівництво, покликане допомогти виробникам вибрати з широкого діапазону пристроїв ті, які доцільно вбудовувати в їх нові, широко представлені на ринку перевірені комерційні продукти;
- забезпечити основу для оцінки вимог до захищеності в специфікаціях придбаних продуктів

"Помаранчева книга" дає наступне визначення безпечної системи, як такої, що "використовуючи відповідні засоби курує доступом до інформаційних ресупсів, таким чином, щоб отримували право на читання, запис, створення та видалення інформації лише авторизовані користувачі або процеси, які працюють від їх імені ".

В "Помаранчевій книзі" довірену систему визначено як "систему, що використовує необхідні апаратні та/або програмні засоби, для забезпечення одночасної обробки інформаційних потоків різних ступенів секретності групами користувачів не порушуючи права на доступ". ІС розбивають на чотири широких ієрархічних класи підвищеного забезпечення секретності. Вони є основою для оцінки ефективності засобів управління захистом, вбудованих в продукти типу автоматизованих систем обробки даних.

Розглянуті Критерії оцінюють, як безпеку, так і довіру тільки в площині управління доступом до даних, що являється засобом забезпечення конфіденційності і цілісності (статичності). Проблеми доступності в "Помаранчевій книзі" не розглядаються.

Найважливішими критеріями для оцінки ступеню довіри є:

- Політика безпеки – перелік правил поведінки, що описують те, яким чином організації обробляють, захищають і поширюють інформацію. Наприклад, вони визначають, випадки, коли користувачі можуть працювати з конкретним набором даних. З підвищенням ступіню довіри до системи, мають ставати суворішими та різноманітнішими політики безпеки. В залежності від політики, яка сформульована є можливість обирати конкретний механізм забезпечення безпеки. Політика безпеки являється активним аспектом захисту, який містить в собі аналіз вірогідних загроз і перелік дій для боротьби з ними.

- Рівнем гарантованості є ступінь довіри, який можна надати для архітектури та реалізації ІС. Довіра безпеки виникає за результатами тестування або після перевірки основного задуму та реалізації системи або компонент, з яких вона складається. Рівень гарантованості вказує на те, чи відповідають нормам обрані механізми, відповідальні за реалізацію політики безпеки. Являється пасивним аспектом захисту.

Вимоги, що пред'являються до інформаціної системи в ході процесу оцінювання, можна поділити на наступні типи вимог: націлені на впровадження послідовної політики безпеки, до ведення обліку використання системи, довіри до системи та вимоги до ведення документації на систему.

Згідно TCSEC, для оцінювання комп'ютерних систем виділено чотири основних групи безпеки, які в свою чергу діляться на класи безпеки:

- группа D - Minimal Protection (мінімальний захист) - об'єднує інформаційні системи, які не можуть задовольнити вимогам безпеки більш високих класів. В даном випадку група та клас співпадають;
- група C - Discretionary Protection (виборчий захист) - об'єднує системи, що забезпечують набір засобів захисту, що застосовуються користувачем, включаючи засоби загального контролю і обліку суб'єктів та їх дій. Ця група має два класи:
    - клас C1 - Discretionary Security Protection (виборчий захист безпеки) - об'єднує системи з поділом користувачів і даних;
    - клас C2 - Controlled Access Protection (захист контрольованого доступу) - об'єднує системи, що забезпечують більш тонкі засоби захисту в порівнянні з системами класу C1, що роблять користувачів індивідуально помітними в їх діях за допомогою

процедур контролю входу та контролю за подіями, що зачіпають безпеку системи і ізоляцію даних.

- група B - Mandatory Protection (обов’язковий захист) - має три класи:
    - клас B1 - Labeled Security Protection (захист безпеки з використанням міток) - об'єднує системи, що задовольняють всім вимогам класу C2, додатково реалізуючу заздалегідь визначену модель безпеки, що підтримують мітки суб'єктів і об'єктів, повний контроль доступу. Вся видана інформація реєструється, всі виявлені при тестуванні недоліки повинні бути усунені;
    - клас B2 - Structured Protection (структурований захист) - об'єднує системи, в яких реалізована чітко визначена і задокументована формалізована модель забезпечення безпеки, а механізм міток, поділу і контролю доступу, реалізований в системах класу B1, поширюється на всіх користувачів, всі дані і на всі види доступу. У порівнянні з класом B1 посилені вимоги щодо ідентифікації користувачів, контролю за виконанням команд керування, посилена підтримка адміністратора і операторів системи. Повинні бути проаналізовані і перекриті всі можливості обходу захисту. Системи класу B2 вважаються "відносно невразливими" для несанкціонованого доступу;
    - клас B3 - Security Domains (області безпеки) - об'єднує системи, що мають спеціальні комплекси безпеки. У системах цього класу повинен бути механізм реєстрації всіх видів доступу будь-якого суб'єкта до будь-якого об'єкту. Повинна бути повністю виключена можливість несанкціонованого доступу. Система безпеки повинна мати невеликий обсяг і прийнятну складність

для того, щоб користувач міг у будь-який момент протестувати механізм безпеки. Системи цього класу повинні мати засоби підтримки адміністратора безпеки; механізм контролю повинен бути поширений аж до сигналізації про всі події, які зачіпають безпеку; повинні бути кошти відновлення системи. Системи цього класу вважаються стійкими до несанкціонованого доступу.

- група A - Verified Protection (захист перевіряється) - об'єднує системи, характерні тим, що для перевірки реалізованих в системі засобів захисту оброблюваної або інформації, що зберігається застосовуються формальні методи. Обов'язковою вимогою є повне документування всіх аспектів проектування, розробки і виконання систем. Виділено єдиний клас:
  - клас A1 - Verified Desing (перевіряється розробка) - об'єднує системи, функціонально еквівалентні системам класу B3 і не потребують будь-яких додаткових коштів. Відмінною рисою систем цього класу є аналіз формальних специфікацій проекту системи і технології виконання, що дає в результаті високий ступінь гарантованості коректної роботи системи. Крім цього, системи повинні мати потужні засоби управління конфігурацією і засоби підтримки адміністратора безпеки.

1.4 Загальні критерії ISO/IEC:15408

Загальні критерії є основою, з використанням якої користувачі комп'ютерної системи можуть визначати свої функціональні вимоги щодо безпеки та вимоги забезпечення у цільовому забезпеченні безпеки і можуть бути взяті з профілів захисту. Постачальники можуть потім реалізувати або

подавати заяви про атрибути безпеки своєї продукції, а тестові лабораторії можуть оцінити продукти, щоб визначити, чи дійсно вони відповідають вимогам. Іншими словами, Загальні критерії забезпечують впевненість, що процес специфікації, впровадження та оцінки продукту комп'ютерної безпеки був проведений строго, стандартно та повторюваним чином на рівні, який відповідає цільовому середовищу, де планується її використовувати. Основні характері риси Загальних критеріїв зазначено нижче:

- Вони зібрали нйбільш повну на сьогодні сукупність вимог до безпеки інформаційних технологій.
- Чітко поділяють вимоги безпеки на функціональні та вимоги довіри до безпеки. Функціональні треба асоціювати з функціями безпеки (ідентифікація, аутентифікація, управління доступом, аудит і т.д.). Вимоги ж довіри з технологіями розробки, перевірки, аналізу вразливостей, постачання, підтримки, іншими словами з усіма етапами життєвого циклу інформаційних технологій.
- Систематизує та класифікує вимоги згідно до ієрархії "клас" - "сімейство" - "компонент" - "елемент", використовуючи унікальні ідентифікатори вимог, що забезпечує зручне їх використання.
- Ранжирує компоненти вимог в родинах і класах відповідно зі ступенем повноти та жорсткості, групує їх в пакети функціональних вимог і оціночні рівні довіри.
- Додає гнучкість і динамізм в задачі задання вимог безпеки до різних видів інформаційних технологій та умов їх використання, що можна забезпечити шляхом формування переліку обов’язкових вимог у вигляді визначеному в ЗК стандартизованих структур (профілів захисту і завдань з безпеки).
- Відкритість для подальшого нарощування переліку вимог.

Предметом розгляду в ЗК є програмно-технічні та технологічні способи забезпечення безпеки ІТ. [4] До аспектів забезпечення безпеки ІТ, які знаходяться поза рамками ЗК, відносяться:

- адміністративні (організаційні) заходи забезпечення безпеки, не пов'язані безпосередньо із забезпеченням безпеки ІТ. Адміністративні заходи розглядаються в тій мірі, в якій вони здатні вплинути на можливості функцій безпеки протистояти загрозам безпеки ІТ;
- оцінка технічних аспектів забезпечення безпеки (таких, як захист від перехоплення інформації в технічних каналах, що виникають за рахунок побічного електромагнітного випромінювання і наведень). Разом з тим, багато положень ЗК застосовні і в цій області;
- методологія оцінки, адміністративна та правова система застосування критеріїв оцінки органами, що здійснюють оцінку. Однак очікується, що ОК будуть використовуватися для цілей оцінки в контексті такої системи і такої методології;
- процедури використання результатів оцінки при атестації виробів ІТ;

Серед користувачів ЗК можна виділити наступні групи :

- системні фахівці, що відповідають за визначення і виконання політики і вимог безпеки організації в області ІТ;
- аудитори, які контролюють адекватність заходів безпеки системи;
- проектувальники систем безпеки, що визначають специфікацію функцій безпеки виробів ІТ;
- особи, які здійснюють атестацію систем ІТ в конкретному середовищі функціонування;
- замовники виробів ІТ, що визначають вимоги до оцінки і підтримують її проведення;

- органи сертифікації, що здійснюють керівництво і нагляд за програмами проведення оцінок. [5]

Фахівці в сфері інформаційної безпеки, визнають Загальні критерії, з його універсальністю, гнучкістю, деталізацією, повнотою та рівнем систематизації, як один з найдосконаліших стандартів в галузі. Враховуючи особливост пов'язані з його побудовою, можна сказати, що він має практично необмежені можливості до розвитку та представляє собою базовий стандарт, який містить методологію опису вимог безпеки ІТ, а також систематизований перелік вимог безпеки. В якості функціональних стандартів, в яких формулюються вимоги до безпеки певних типів продуктів і систем ІТ, передбачається використання профілів захисту (ПЗ), що створюються за методологією і на основі каталогу вимог ЗК. У ПЗ можуть бути включені і будь-які інші вимоги, які є необхідними для забезпечення безпеки конкретного типу продуктів або систем ІТ.

1.5 Рекомендації X.800

Рекомендації x.800 визначають сервіси, характерні для розподілених систем, рівня семирівневої моделі, на якій можуть бути реалізовані механізми безпеки, функції безпеки, а також адміністрування засобів безпеки.

Стандарт виділяє наступні сервіси безпеки і ролі, які вони виконують:

- Автентифікація. Цей сервіс перевіряє автентичность партнерів і проводить перевірку автентичності джерела даних. Автентифікацію партнерів використовують при встановленні з'єднання і можна також використовувати, періодично під час сеансу. Її основна задача це протидія таким загроз, як маскарад і повтор попереднього сеансу

зв'язку. Автентифікація буває односторонньою (коли користувач доводить свою оригінальність серверу) і двосторонньою (взаємною).

- Управління доступом. Даний засіб забезпечує захист від несанкціонованого використання ресурсів, до яких є доступ через мережу.
- Політика приватності. Забезпечує захист від несанкціонованого отримання інформації. Окремо слід згадати конфіденційність трафіку (це захист інформації, яка може бути отриманою, шляхом аналізу мережевих потоків даних).

Цілісність даних розділено на підвиди в залежності від того, який тип сеансу використовують партнери - з встановленням з'єднання або без нього, підлягають захисту всі дані або тільки окремі поля, чи має забезпечуватися відновлення в разі порушення цілісності.

Невідмовність (тобто неможливість відмовитися від своїх дій) забезпечує два види послуг: неспростовність з підтвердженням оригінальності джерела даних і неспростовність з підтвердженням доставки. Побічним продуктом неспростовності являється аутентифікація джерела даних.

1.6 Німецький стандарт BSI

В 1998 р. в Німеччині було опубліковано "Керівництво по захисту інформаційних технологій для базового рівня". Пізніше він був представлений як стандарт BSI. В основу покладено загальну методологію та компоненти керування інформаційною безпекою, які наведено нижче:

- Загальний спосіб управління безпекою інформації (організація системи менеджменту у сфері інформаційної безпеки)
- Опис компонент IT

- Найважливіші компоненти (рівень процедур, організація дій, повязаних з захистом, планування дій в форсмажорних випадках)
- Інфраструктура
- Різнотипні компоненти клієнтів (такі як: DOS, Windows, UNIX, мобільні девайси та інше)
- Різні види мереж («точка-точка», Novell NetWare, побудовані на базі ОС UNIX і Windows, різнорідні мережі)
- Різні компоненти системи передачі даних (такі як комутатори, модеми, роутери та інше).
- Телекомунікаційні системи
- Стандартне ПО
- Бази даних
- Визначення головних компонент налагодження режиму інформаційної безпеки.
- Параметри об'єктів, які підлягають інформатизації
- Опис доступних інформаційних ресурсів певної компанії(до них відносять, для прикладу, апаратне і програмне забезпечення, таке як комп'ютери та сервери під керуванням ОС DOS, Windows або UNIX)
- Параметри комп'ютерних мереж заснованих на різних технологіях
- Технічні характеристики ТК обладнання (враховується як активне, так і пасивне)
- Вичерпні каталоги з переліком загроз безпеці та заходами контролю (кожний визначає більш ніж 600 найменувань)

Стандарт BSI поділив усі загрози на класи, наведені нижче:

- Форс-мажорні та надзвичайні обставини
- Нестача заходів, пов'язаних з організацією

- Людський фактор
- Технічні несправності
- Дії, вчинені навмисно

Схожим чином прокласифіковано заходи протидії:

- Покращення інфраструктури
- Адміністративні контрзаходи
- Процедурні контрзаходи
- Програмно-технічні контрзаходи
- Зниження вразливості комунікацій; розробка плану дій в надзвичайних ситуаціях

1.7 COBIT

1.7.1 Моделі зрілості

Управління IT - складова частина успіху в управлінні підприємством, яка гарантує раціональне і ефективне вдосконалення всіх взаємопов'язаних процесів підприємства. Управління IT надає основу, яка пов'язує IT-процеси, IT-ресурси і інформацію із стратегією та цілями установи, що дозволяє максимально ефективно використати інформацію, при цьому підвищивши капіталізацію і отримуючи конкурентоспроможні переваги.

Принципи управління створені для того, щоб допомогти керівнику IT відповісти на три стратегічних питання:

1. Чи існують зараз в організації інформаційні технології, при керуванні якими "задовольняються" всі інформаційні потреби організації?
2. Як організація забезпечує інфраструктуру та керує ризиками, наскільки організація залежить від цього?

3. З якими проблемами організація стикається при управлінні IT?

Щоб отримати відповіді на ці стратегічні питання необхідно безперервно відповідати на "тактичні" питання:

- Що є результатом IT-процесів?
- Що є рішенням проблем в IT?
- З чого складаються ці рішення?
- Чи будуть працювати ці рішення?
- Як їх реалізувати?

Для отримання відповідей на "тактичні" питання до принципів управління CobiT, включені такі розділи як моделі зрілості, критичні фактори успіху (КФУ), ключові індикатори цілі (КІЦ) і ключові показники результату (КПР), це доповнення дало змогу отримати якісно покращений підхід до питань управління IT, який відповідає потребам керівників в частині управління і контролю.

Моделі зрілості в стандарті CobiT призначаються для контролю над IT-процесами в установі. Вони базуються на визначені ступеню розвитку компанії від неіснуючої до оптимізованої (від 0-го до 5-го рівня моделі зрілості). Цей підхід був привнесений в CobiT з Моделей Зрілості, розроблених Інститутом проектування і розробки програмного забезпечення (Software Engineering Institute), створених для оцінки рівня зрілості розробки програмного забезпечення.

Моделі зрілості не підказують як поліпшити роботу компанії і не пояснюють, як працювати з персоналом, також немає готових посібників і по застосуванню моделей зрілості. Рекомендується для кожної компанії розробити подібне керівництво для свого бізнесу або запросити сторонніх консультантів для вирішення цього питання. Моделі зрілості призначені для організації ефективного управління. Вони визначають ключові дії, які

вказують, що треба зробити для досягнення необхідної якості і містять способи контролю над правильністю виконання ключових IT-процесів і методи їх коригування. Ключові дії детально описані в Керівництві на абстрактному рівні, а в процесі використання моделей зрілості компанія може вибрати довільний ступінь їх формалізації.

Шкала моделей зрілості:

- 0. Система управління безпекою не створена. Повністю відсутні будь-які процеси управління IT. Організація не визнає факт існування проблем в IT, які треба вирішувати, а отже немає ніяких відомостей про проблеми.
- 1. Початок. Організація визнала існування проблем в управлінні IT та необхідність вирішувати їх. При цьому не створено ніяких стандартизованих рішень. Є випадкові рішення, прийняті кимось персонально або випадково. Підхід керівництва щодо вирішення проблем в IT хаотичний, визнання наявності проблем випадкове і непослідовне.
- 2. Повторення. Є загальне усвідомлення наявності проблем в управлінні IT. Показники діяльності та IT-процесів розвиваються, охоплюючи при цьому процеси планування, функціонування та моніторингу за IT. Дії з управління інформаційними технологіями описані та інтегровані в процес управління установою. Вибрані для покращення та/або контролю такі IT-процеси, які можуть вплинути на основні бізнес-процеси в підприємстві. Ефективно здійснюється планування і управління інвестиціями. Керівництво організації регламентувало заходи з управління IT і методи з управління та оцінки, але процес не було прийнято в установі. Вся відповідальність покладена на співробітників. Вони повинні контролювати процеси

управління з використанням проектів та IT-процесів. Вибрано і впроваджено обмежені інструменти для відбору метрик управління, але їх не вдається використати в повному обсязі, бо є недоліки в оцінці їх функціональності.

- 3. Опис (Стандартизація). Необхідність діяти у відповідності до принципів управління IT усвідомлена керівництвом і впроваджується. У розвитку знаходиться базовий набір показників управління IT: є визначеним зв'язок між результатами та показниками продуктивності, він зафіксований та впроваджений в стратегічні процеси при плануванні та моніторингу. Процедури стандартизовані і задокументовані, проводиться навчання працівників щодо виконання цих процедур. Показники продуктивності всіх видів діяльності зафіксовано і їх значення відслідковуються, що в результаті призводить до підвищення ефективності функціонування всієї компанії. Процедури самі по собі не складні, вони являються формалізацією існуючої в компанії практики. Відповідальними за вивчення, виконання та використання стандартів покладено на робітників організації. Більшість процесів працюють відповідно до деяких основних метрик, і, як правило, контролюються окремими співробітниками, тому про деякі відхиленнях керівництво може не знати. Проте загальна звітність щодо виконання ключових процесів є доволі чіткою, і керівництво може заохочувати співробітників на основі оцінки ключових результатів.
- 4. Управління. Є повне розуміння проблем в управлінні IT на всіх рівнях компанії, постійно відбувається підвищення рівня кваліфікації співробітників. Угоди щодо рівня обслуговування визначено і вони підтримуються в актуальному стані. Є чітке розподілення відповідальності, встановлено рівень володіння процесами. В першу

чергу покращення в процесах управління ІТ грунтуються на вимірюваних кількісних показниках. Є можливість керувати процедурами та метриками процесів, проводити вимірювання їх відповідності. Керівництвом організації визначено допустимі відхилення, за яких процеси мають продовжувати працювати. Процеси постійно вдосконалюються, їх результати відповідають "найкращим практикам". Формалізований порядок аналізу першопричин. Присутнє розуміння необхідності постійного вдосконалення. Обмежено застосовуються передові технології, засновані на сучасній інфраструктурі і стандартних інструментах, які модифіковано. В бізнес-процеси залучаються всі необхідні ІТ-фахівці. Управління ІТ переростає в процес рівня усієї організації. Діяльність з управління ІТ інтегровано в процес керування організацією.

- 5. Оптимізація. В організації є глибоке розуміння того як управляти ІТ, вирішувати проблеми, а також шляхи розвитку. Комунікація та навчання підтримуються на високому рівні, за допомогою найсучасніших засобів. Як результ безперервного покращення, процеси відповідають моделям зрілості, які побудовано на підставі "кращих практик". Першопричини проблем і відхилень, що виникають ретельно аналізуються, і за результатами цього аналізу виконуються відповідні дії. Інформаційні технології інтегровано в бізнес-процеси, є повна їх автоматизація, яка надає можливість підвищувати якість та ефективність роботи організації.

1.7.2 Критичні Фактори Успіху (КФУ)

Критичні Фактори Успіху (КФУ) дають визначення найбільш важливим проблемам або діям керівництва і спрямовані на досягнення повного контролю над IT-процесами. КФУ мають бути керованими, з орієнтацією на успіх і мати опис того, як виконувати стратегічні, технічні, організаційні і процедурні дії щоб досягти успіху.

Як приклади критичних факторів успіху можна зазначити наступні:

- Дії з управління процесами в IT інтегровано в процеси управління організацією і стиль роботи керівництва;
- Управління IT зосереджується на цілях компанії: стратегічні ініціативи, технологій для забезпечення розвитку бізнесу, достатність ресурсів і задоволення бізнес-вимогам;
- Дії по управлінню процесами в IT чітко визначено, формалізовано і відбувається їх здійснення на основі потреб компанії з відповідною звітністю;
- Методики управління розроблено для підвищення продуктивності, досягнення оптимальності використання ресурсів і підвищенняя ефективності IT-процесів;
- Методи аудиту визначені таким чином, щоб уникнути збоїв і помилок в системі внутрішнього контролю;
- Можна спостерігати інтеграцію і розвиток взаємодії складних IT-процесів, наприклад, управління проблемами, змінами та конфігурацією;
- Засновано контрольний комітет, який призначає і спостерігає за незалежним аудитом, який приділяє пильну увагу IT при складанні

планів аудиту, а також приймає до уваги результати досліджень сторонніх організацій і аудіторов

1.7.3 Ключові Індикатори Цілі (КІЦ)

Ключові Індикатори Цілі (КІЦ) описують комплекс вимірювань, які за фактом повідомляють керівництву, що ІТ-процес досяг пропонованих бізнес-вимог. КІЦ виражаються в наступних термінах інформаційних критеріїв:

- Придатність інформації, яка необхідна для підтримки бізнесу;
- Ризики, пов'язані з відсутністю цілісності та конфіденційності;
- Рентабельність процесів і операцій;
- Підтвердженна надійність, ефективність та узгодженість.

1.7.4 Ключові Індикатори Результату (КІР)

Ключові Індикатори Результату містять в собі опис комплексу дій, необхідних для того щоб визначити, наскільки ІТ-процеси можуть досягти поставлених цілей. КІР є основними індикаторами, які відображають імовірність досягнення поставленої мети. А також індикаторами, які вказують на адекватність способів, методів і навичок, використовуваних для досягнення результату.

Ключовими Індикаторами Результату (КІР), можуть бути:

- Підвищення рентабельності ІТ-процесів;
- Покращення роботи і планування дій з вдосконалення ІТ-процесів;
- Збільшення навантаження на інфраструктуру ІТ;
- Підвищення ступеня задоволеності користувачів (опитування користувачів та відстежування кількості скарг);

- Покращення взаємодії та комунікації між керівниками ІТ і керівництвом компанії
- Підвищення продуктивності робітників.

1.7.5 Управління ІТ відповідно до CobiT

Потреби бізнесу визначаються Ключовими Індикаторами Цілі, чому сприяє організація постійного контролю над усіма ресурсами ІТ. Досягнення необхідного рівня контролю вимірюється Ключовими Показниками Результату, які враховують Критичні Фактори Успіху.

Модель Зрілості використовується для оцінки рівня управління ІТ в даній організації - від неіснуючого (найнижчий рівень) до оптимізованого (найвищий рівень).

Для досягнення п'ятого, "оптимізованого" рівня зрілості в управлінні ІТ організація повинна бути, принаймні, на п'ятому рівні в домені моніторингу і як мінімум на четвертому рівні моделей зрілості для всіх інших доменів.

1.8 Стандарти НД ТЗІ

1.8.1 Огляд стандарту НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»

Даний стандарт дає наступне визначення ІТС. Це така система, що належить до якоїсь із перелічених далі систем: ІС, ТК система, інтегрована система.

ІС це система, що поєднує організаційні та технічні аспекти і в якої реалізовано технології обробки інформації, які використовують засоби обчислювальної техніки та ПЗ;

ТКС система, яка забезпечує обмін інформацією за допомогою технічних і програмних засобів, та в якій інформація має вигляд сигналів, знаків, звуків, зображень;

Інтегрована система являє собою набір декількох взаємозв'язаних ІС та/або ТКС, де робота певних з них залежна від результату роботи інших, у випадку, якщо їх поєднання під час роботи можна розглянути як одну цілу систему. [6]

Стандарт визначає процес побудови КСЗІ, як для новостворюваних систем, так і для вже існуючих, котрі вимагають впровадження або вдосконалення КСЗІ.

КСЗІ розроблена згідно до рекомендацій даного стандарту має складатися з заходів та засобів, які забезпечать захист інформації від:

- Потрапляння її до технічних каналів, наприклад, до каналів побічних ЕМВ і наведень, акустико-електричні та інші види каналів;
- неправомірного доступу до інформаційних ресурсів з метою використати її, який може бути здійснено методом підключення до лінії зв'язку або приладів даної лінії, видавання себе як авторизованого користувача;
- впливів на дані, які можуть бути здійснені формуванням полів та сигналів, що має на меті порушити цілісность інформації та/або подолання системи захисту.

В НД ТЗІ 3.7-003 визначено ряд етапів проектування та впровадження КСЗІ. Процес розробки починається з формулювання вимог до системи, що має бути побудована, обґрунтовується необхідність її створення, вивчення

середовища в якому функціонує ІТС. Результатом є перелік об’єктів, що мають бути захищеними, перелік потенційних загроз для даних, моделі загроз та порушників. В результаті формується завдання на створеня КСЗІ.

На другому етапі розробляються політики інформаційної безпеки в ІТС. З переліку варіантів побудови вибирається самий оптимальний. Пізніше відбувається оформлення політики безпеки, де вибираються способи захисту від усіх суттєвих загроз, формуються загальні вимоги, правила та обмеження.

В результаті отримують документ, який описує вимоги щодо захисту інформації, оброблюваної в ІТС, послідовність створення КСЗІ, проведення випробувань та інтеграції у склад ІТС.

На основі складеного ТЗ проводять розробку проекту КСЗІ, під час чого відбувається обґрунтування та прийняття проектних рішень для реалізації вимог, зазначених в технічному завданні, розроблюється, оформлюється та затверджується робоча та експлуатаційна документація КСЗІ. [7]

Наступним етапом є введення КСЗІ в експлуатацію та оцінювання ступеню захищеності даних в ІТС. Тут відбуваються підготовчі роботи для переведення системи в робочий стан, навчання персоналу, роботи з розгортання системи, пусконалагоджувальні роботи, випробувальна екслуатація. Після дослідної експлуатації проводиться державна експертиза.

1.8.2 Огляд станарту НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»

Даний стандарт визначає перелік критеріїв, використовуваних при оцінці рівня захищеності інформації, яка оброблюється в інформаційних

системах, при спробах неправомірного доступу. Являється основою для визначення вимог до ІС і засобів захисту, оцінки рівня захищеності даних в таких системах та їх придатність для роботи з критичною інформацією.

Стандарт розглядає два види вимог при оцінці здатності ІС провадити захист інформації, що оброблюється, при спробах неправомірного доступу, а саме вимоги:

- до функції захисту
- до гарантій

Критерії розглядають ІС як сукупність функціональних послуг. Сама послуга є набором функцій, що дозволяють протистояти певним загрозам. В кожної послуги може бути декілька рівнів. Чим вищим є рівень послуги, тим більш повно вона забезпечує захист від певних видів загроз. Рівні послуг мають ієрархію за ступенем повноти захисту, проте не обов'язково представляють собою точну підмножину один одного.

Для зручност зіставлення проведено поділ функціональних критеріїв на чотири групи:

- Критерії конфіденційності. Загрози, що пов’язані з несакціонованим перегдядом інформації.
- Критерії цілісності. Загрози, які зв’язані з несанкціонованою зміною інформації.
- Доступність. Такі загрози, які порушують можливість використання ІС або інформації, що оброблюється.
- Критерії спостережності. Розглядає ідентифікацію та контроль за діями користувача, керованість комп’ютерною системою.

Кожна група описує вимоги до сервісів, які впроваджують захист від конкретного типу загрози.

Окремою ланкою виділено критерії гарантій, які дають змогу кількісно оцінити коректність впровадження послуг. До них можна віднести вимоги до архітектури рішення, середовища розробки, послідовності розробки, випробування системи захисту та середовища функціонування. [7]

Структурне представлення критеріїв наведено на рисунку 1.1.

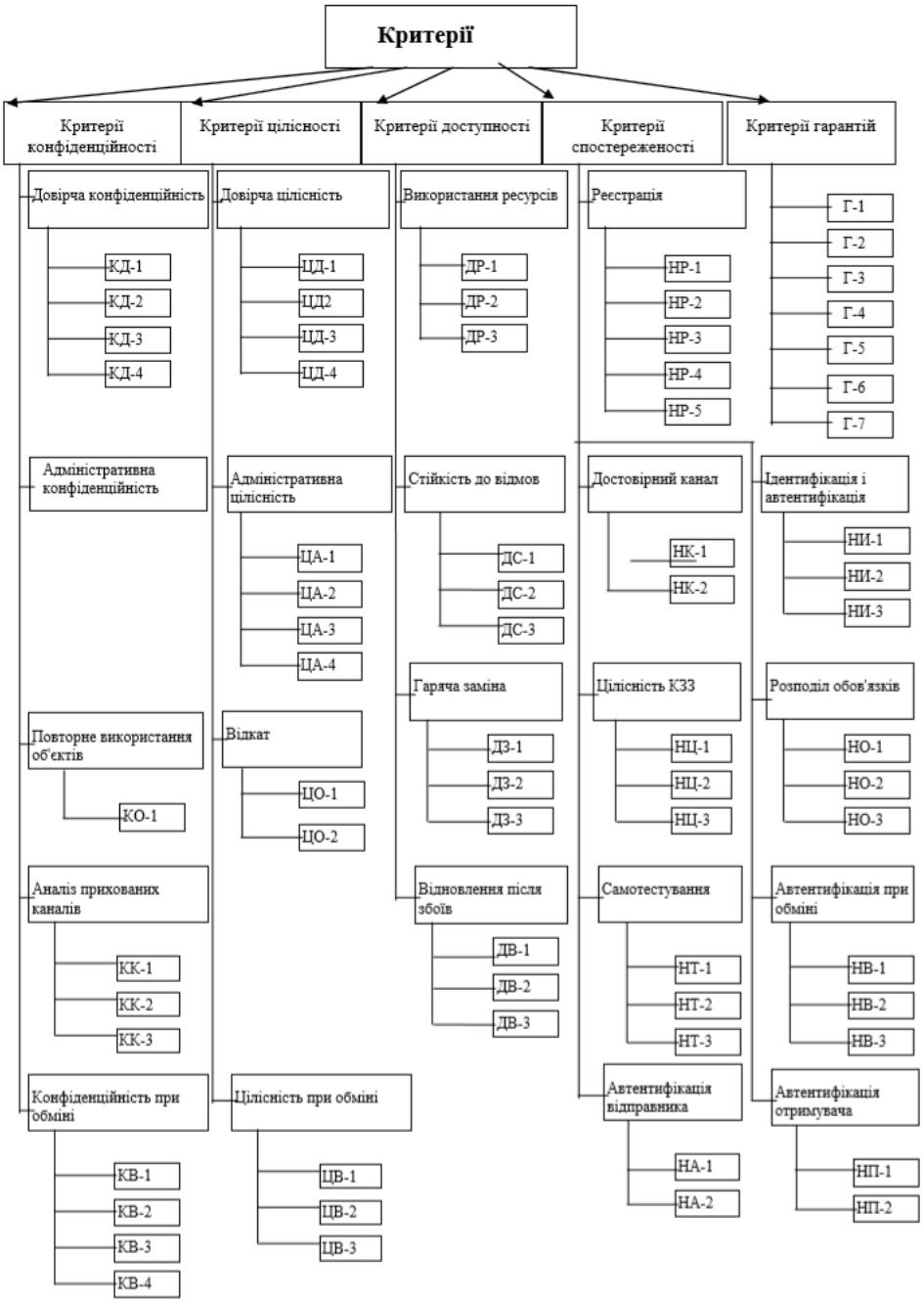

Рисунок 1.1 Структурне представлення критеріїв НД ТЗІ 2.5-004-99

1.9 Стандарт BS 7799

Британський стандарт BS 7799 це один з перших міжнародних стандартів управління інформаційною безпекою. Перший його розділ, BS 7799-1 «Практичні правила управління інформаційною безпекою» - був розроблений в 1995 році Британським інститутом стандартів за замовленням уряду Великобританії.

Відповідно до стандарту будь-яка служба безпеки, IT-відділ, вищий менеджмент компаній мають почати працювати у відповідності з загальним регламентом. Не важливо, буде відбуватись захист паперових документів чи електронних даних. Зараз стандарт BS 7799 підтримують в 27 країнах світу. В 2000 році Міжнародний інститут стандартів ISO розробив міжнародний стандарт управління безпекою ISO/IEC:17799, спираючись на BS 7799. Зараз можна побачити, що BS 7799 та ISO:17799 мають однаковий сенс та визнаний у світі.

Перша частина "Управління інформаційною безпекою. Практичні правила", містить систематичний, вельми повний, універсальний перелік регуляторів безпеки, який може бути корисним для організації практично будь-якого розміру, структури і сфери діяльності. Ця частина призначена для використання її як довідкового документа керівництвом і рядовими робітниками, що відповідають за планування, реалізацію і підтримку внутрішньої системи захисту інформації.

Згідно зі стандартом, мета інформаційної безпеки - забезпечити безперервну роботу організації, по можливості запобігти і/або мінімізувати збитки від порушень безпеки.

Управління інформаційною безпекою дозволяє сумісно користуватися даними, одночасно забезпечуючи захист самих даних та обчислювальних ресурсів.

Підкреслюється, що захисні заходи виявляються значно дешевшими і ефективними, якщо вони закладені в інформаційні системи і сервіси на стадіях завдання вимог і проектування.

Регулятори безпеки, визначені в першій частині BS7799 поділено на десять груп:

- політика безпеки;
- загальноорганізаційні аспекти захисту;
- класифікація активів і керування ними;
- безпека персоналу;
- фізична безпеки і безпека навколишнього середовища;
- адміністрування систем і мереж;
- керування доступом;
- розробка і підтримка інформаційних систем;
- керування безперебійною роботою організацій;
- контроль на відповідністю вимогам

У стандарті виділяється десять ключових регуляторів, які або є обов'язковими відповідно до чинного законодавства, або їх прийнято як основні структурні елементи інформаційної безпеки. До них відносяться:

- документ про політику інформаційної безпеки;
- поділ зобов'язань із забезпечення інформаційної безпеки;
- навчання і підготовка працівників, які підтримуватимуть режим інформаційної безпеки;
- сигналізація при випадках порушення захисту;

- антивірусні засоби;
- процес планування безперервної роботи організацій;
- нагляд за створенням копій ПЗ, котре захищене авторськими правами;
- захист супровідних документів;
- захист даних;
- контроль за відповідністю до політики безпеки.

Друга частина BS 7799-2: 2002 "Системи управління інформаційною безпекою" розглядає систему управління інформаційною безпекою. Під якою мається на увазі частина всієї системи управління, яка опирається на аналіз ризиків і основним призначенням якої є проектування, реалізація, контроль, підтримка та вдосконалення заходів у сфері ІБ. Дана система складається з організаційних структур, політик, дій по плануванню, обов'язків, процедур, процесів і ресурсів.

1.10 Висновки до розділу 1

В даному розділі було проведено аналіз стандартів в сфері інформаційної безпеки. Розглянуто те, яким чином кожен з них трактує основні поняття, такі як власне інформаційна безпека, стан захищеності, засоби захисту. В цілому зважаючи на те, що стандарти працюють в одній сфері ці трактування дуже схожі між собою, але є певні відмінності в структурі самих документів та підходах до розгляду та класифікації засобів. Так, наприклад, “Критерії визначення безпеки комп'ютерних систем” проводять розділення безпеки на чотири групи, а груп в свою чергу на класи безпеки; в той же час COBIT вимагає перевірки стану інформаційної системи на відповідність певному ріню зрілості, та впроваджує поняття ключових індикаторів результату (КІР) та ключових індикаторів цілі (КІЦ); вітчизняні

стандарти НД ТЗІ проводять розділення критеріїв до безпеки на декілька груп і всередині групи виділяють рівні.

За результатами порівняльного аналізу для подальшого дослідження було вибрано стандарт ISO/IEC:15408 “Загальні критерії”. Основними причинами для прийняття такого рішення стало широке використання та визнання даного стандарту в світі, продуманість його структури, наприклад, поділ на класи, сімейства, компоненти, що робить його універсальнішим.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ВИМОГ ДО СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ ТА ЇХ РЕАЛІЗАЦІЯ У ВІДПОВІДНОСТІ ДО ISO:15408

2.1 Структура стандарту ISO/IEC:15408

Щоб зрозуміти логіку побудови стуктури даного стандарту, треба переглянути основні цілі, які було поставлено при розробці даного стандарту:

- Зведення стандартів в сфері оцінки захищеності ІС до уніфікованого вигляду
- Підняти ступінь довіри оцінці захищеності ІТ
- Мінімізація витрат на оцінювання ІТ

Для забезпечення правильної стурктури та прослідовності викладення стандарт було розділено на три частини:

- Введення та загальна модель
- Функціональні вимоги безпеки
- Вимоги щодо гарантій

У першій частині «Загальних критеріїв» містяться визначення основних понять, концепції, опис моделей та методик проведення оцінок захищеності ІТ. В ній введено основні поняття та визначено принципи щодо того як формалізувати предметну область.

В другій частині наведено вимоги до функціональної складової засобів захисту. Їх можна використати для аналізу захищеності та для оцінки повноти реалізації функцій безпеки в проектованій системі.

В третій частині міститься клас вимог щодо аналізу вразливостей засобів захисту, що називається AVA: Vulnerability Assessment. Цей клас описує методи, які треба використовувати щоб попередити, виявити і ліквідувати наступні типи вразливостей:

- існування каналів, що призводять до витоку даниї
- конфігураційні помилки, або використання систем, невірним шляхом, що може призвести до переходу її в небезпечний стан
- низька надійність засобу забезпечення безпеки, який реалізує відповідну функцію безпеки
- наявність вразливих точок в механізмах захисту інформації, які можуть дозволити користувачу отримати несанкціонований доступ до інформації, обходячи існуючі механізми захисту.

Основні відмітні риси ОК:

- використання визначених методологій ти системи створення вимог при оцінці захищеності ІТ. Можна простежити системність починаючи з термінів та рівнів абстракції вимог до того як вони використовуються при проведенні оцінки захищеності на всіх етапах життєвого циклу системи;
- містять в собі найбільш повну на сьогодні сукупність вимог щодо безпеки ІТ
- чітко поділяють вимоги безпеки на вимоги до функціональних частин та вимоги довіри до безпеки. Вимоги до функціональних компонент відносять до сервісів безпеки, а вимоги довіри - до технологій розробки, проведення перевірки, аналізу вразливостей, передачі користувачам, підтримки, іншими словами до кожного з етапів життєвого циклу системи
- в склад стандарту включено шкалу довіри до безпеки, яку можна використати при створенні різних рівнів упевненості в безпечності систем

- вони систематизують і класифікують вимоги згідно з ієрархією «клас - сімейство - компонент - елемент» використовуючи унікальні ідентифікатори вимог, що забезпечує зручне їх використання
- ранжування компонентів вимог в сімействах і класах за ступенем повноти і жорсткості, і групування в пакети вимог
- відкриті для подальшого нарощування сукупності вимог

В порівнянні з іншими стандартами, по рівню систематизованості, здатності поглибити деталізацію вимог та їх повноті, ISO: 15408 можна визнати одним із самих досконалих серед існуючих зараз стандартів. При цьому, зважаючи на особливості його побудови, можна зазначити, що стандарт має багато можливостей для продовження розвитку. ISO:15408 являється не просто функціональним стандартом, а методологією завдання, оцінки та перелік вимог безпеки ІТ, який можна нарощувати та уточнювати.

2.2 Вимоги щодо архітектурних рішень при побудові інформаційних систем для безпечного її функціонування

Ідеї запропоновані моделлю відкритих систем сильно вплинули на розвиток складних інформаційних систем. Основою є суворе фактичне дотримання сукупності профілів, протоколів і стандартів. Всі складові системи, як програмні, так і апаратні мають відповідати самим важливим вимогам щодо здатності до переносу та можливості спільної співпраці з віддаленими складовими. Це дає змогу впровадити сумісність різнорідних компонентів ІС, і засобів передавання даних. Задачу можна звести до максимізації можливості повторно використовувати розроблені та перевірені програмні та інформаційні компоненти при заміні платформ, операційних систем та процесів взаємодії.

Під час створення великих, розподілених ІС, розробці архітектурних зішень, виборі компонент і зв'язків між ними треба врахувати не лише загальні концептуальні вимоги, а також ряд специфічних вимог, основна задача яких - забезпечити безпеку функціонування, серед них можна виділити наступні:

- архітектурні рішення повинні бути гнучкими, тобто має бути можливість відносно просто, не роблячи великих змін у структурі, розвивати інфраструктуру та змінювати конфігурацію засобів, що використовуються, нарощувати функції та ресурси ІС у відповідності до розширення сфер та завдань поставлених перед нею;
- необхідність в забезпеченні безпеки при функціонуванні системи під час діх на неї різних типів загроз і надійного захисту даних від внесення помилок, зміни або втрати. Також є необхідність в проведенні авторизації користувачів, управлінні робочим навантаженням, резервуванні даних і апаратних ресурсів, максимально швидкому відновленні функціонування ІС;
- необхідно запровадити доступ до сервісів, який буде максимально комфортний та спрощений для користувача, використовуючи для цього сучасні графічні засоби, мнемосхеми та зрозумілих інтерфейсів користувача;
- необхідно підтримувати супровідну документацію в максимально актуальному стані

Треба зауважити, що незалежно від потужності систем безпеки, вони невзмозі гарантувати надійний захист на програмно-технічному рівні. Лише перевірені архітектурні рішення здатні зробити ефективне об'єднання сервісів, запровадити керованість інформаційною системою, забезпечити їй здатність до розвитку та протистояння новим типам загроз при цьому

зберігаючи наступні властивості: висока продуктивність, просте та зручне використання. [10]

З точки зору практики для забезпечення безпеки самими важливими є наступні принципи щодо того як будувати архітектуру ІС:

- дотримання принцпів запропонованих ідеологією відкритих систем, використання визнаних стандартів, перевірених рішень
- захист має бути безперервним в просторі та часі. Не повинно бути можливості подолати засоби захисту. За будь-яких обставин система має правильно обробляти позаштатні випадки, продовжуючи цілком виконувати свої функції, або блокувати доступ до всієї системи чи її частини.
- система має передбачати розподіл ролей і відповідальності таким чином, щоб один користувач не зміг порушити критично важливий для установи процес чи обійти систему захисту. На програмно-технічному рівні цей принцип вимагає давати користувачам та адміністраторам лише необхідні для їх потреб права доступу. Це дозволит мінімізувати можливі збитки від хибних дій користувача або адміністратора, незалежно від того чи були ці дії випадковими, чи зловмисними;

Загальний принцип простоти та керованості ІС як цілої системи так і окремого засобу захисту є дуже важливим. Лише проста та керована система може перевіряти узгодженість конфігурацій різних компонент і здійснювати централізоване управління. У цьому випадку інтегруюча роль належить web-сервісу, що приховує різноманіття об'єктів, які треба обслуговувати, та надає єдиний, зрозумілий інтерфейс. Нарпиклад, у випадку, коли певні об'єкти (наприклад, таблиці баз даних) повинні бути доступними через Інтернет,

треба заборонити доступ до них напряму, бо в такому випадку ІС стане вразливою, зросте її складність і вона стане складною в керуванні.

Добре спроектована структура програмних засобів, баз даних, топологій мереж прямо відображається на досягнення високих показників якості та безпеки в ІС, і на складність її створення. У випадку строгого дотримання правил структурованої побудови можна дуже полегшити досягнення високих показників якості і безпеки, через скорочення числа можливих помилок в програмах, що реалізуються, зменшення кількості відмов апаратной частини, стає можливим спрощення діагностики та локалізації проблем. В системі з правильною структурою, коли є чітко виділені компоненти можна чітко виділити контрольні точки, що допоможе вирішити задачу гарантування того, що застосованих засобів захисту достатньо для забезпечення неможливості обходу їх порушниками.

Основною причиною висування жорстких вимог до розробки архітектури та інфраструктури під час проектування ІС, є те, що саме протягом цієї стадії є можливість значно зменшити кількість вразливостей, зв'язаних з ненавмисними факторами дестабілізації, що можуть впливати на безпеку програмних засобів, баз даних і систем комунікації.

Проаналізувати безпеку ІС за відсутності впливів злочинного характеру можна опираючись на модель взаємодії компонентів ІС, що зображено на рисунку 2.1. [10]

Об'єктами вразливості розглядають:

- динамічні обчислювальні процеси пов'язані з обробкою даних, автоматизованою підготовкою рішень;
- програмний код, що виконується системою в процесі роботи ІС;
- дані та інформація, що накопичується в базах даних;
- дані, які видаються користувачам.

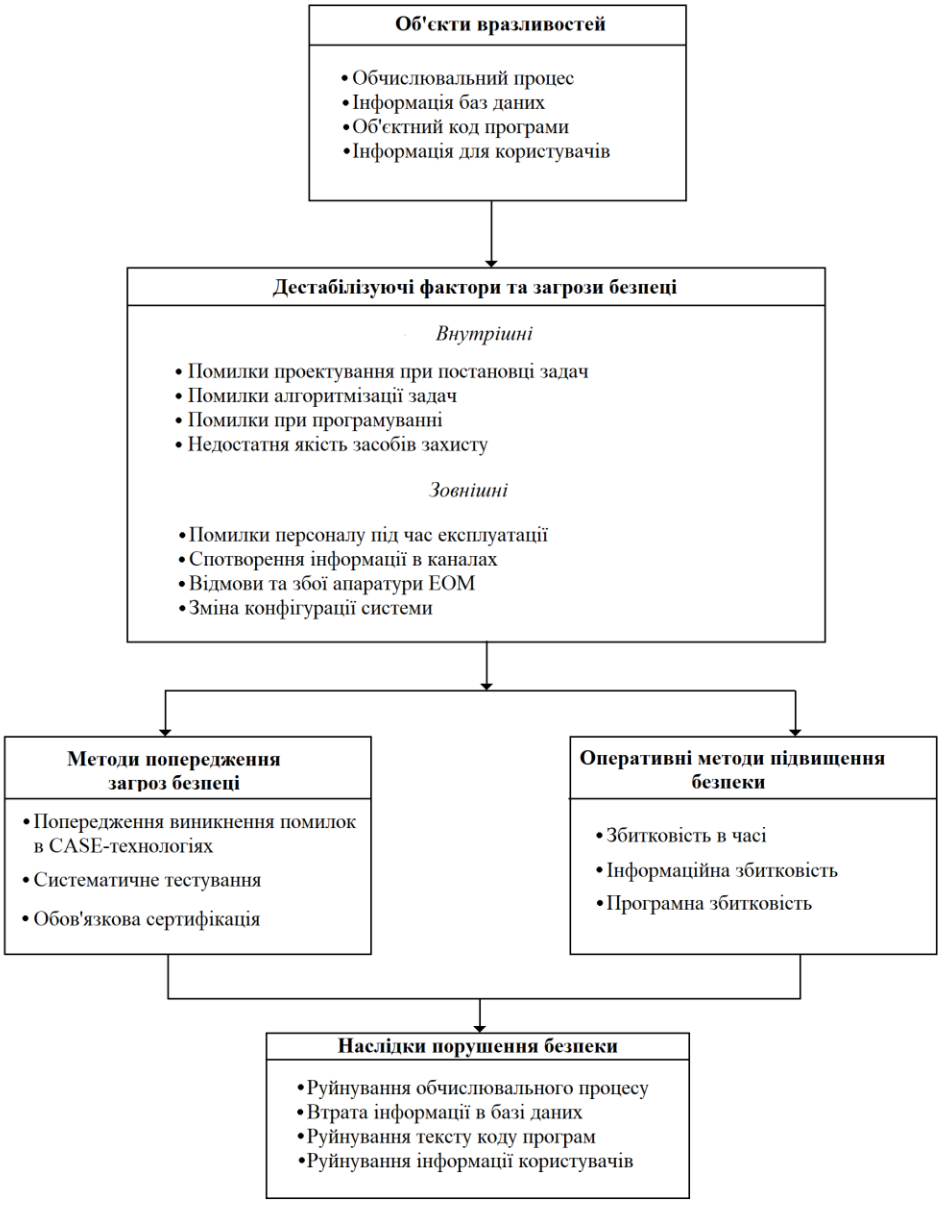

Рисунок 2.1 Модель аналізу безпеки ІС при відсутності злочинних загроз

2.3 Етапи побудови системи безпеки ІС

Концепція інформаційної безпеки пропонує поділяти етапи побудови системи інформаційної безпеки відповідно до стандартизованого життєвого циклу ІС: аудит безпеки для існуючої системи захисту, етап аналізу ризиків,

етап висування вимог і вироблення першочергових заходів щодо захисту, етапи проектування, впровадження, атестація та супроводу системи. Ниже розглянуто коротко зміст деяких з етапів.

Аудит безпеки. Він має включати в себе, хоча б, чотири різні групи дій.

До *першої групи* відносяться тестові зломи ІС. Вони застосовуються, як правило, на початкових етапах обстеження захищеності ІС. Причиною малої ефективності таких зломів полягає в самій постановці завдання. Основним завданням зловмисника є виявлення вразливостей з подальшим їх використання для доступу в систему. Неуспішність злому може означати мірі як захищеність системи, так і недостатню кількість тестів.

Другу групу називають експрес-обстеженням. В її рамках проводяться, звичайно нетривалі роботи з оцінки загального стану механізмів безпеки в обстежуваній ІС на базі стандартизованих перевірок. Таке обстеження зазвичай проводять у разі, якщо необхідно визначити пріоритетні напрями, які дозволять забезпечити мінімальний рівень захисту інформації. Основою для нього слугують списки контрольних питань, які заповнюються в результаті перевірки або, навіть, тестової роботи автоматизованих сканерів рівня захищеності.

Третя група робіт з аудиту це атестація систем на відповідність до вимог захищеності інформаційних ресурсів. Тут відбувається формальна перевірка набору вимог організаційного і технічного аспектів, розглядають повноту і достатність реалізації механізмів безпеки. Зазвичай методика аналізу корпоративної інформаційної захищеності представляє собою сукупність наступних методів:

- аналіз вихідних даних за структурою, аналіз архітектури, інфраструктури та конфігурацій ІС на момент проведення обстеження;

- попередня оцінка ризиків, що пов'язані зі здійсненням загроз відносно апаратних та інформаційних ресурсів;
- аналіз механізмів забезпечення безпеки на організаційному рівні, аналіз політик безпеки організації і організаційно-распорядчих документів щодо забезпечення режиму ІБ та оцінка відповідності цих режимів вимогам існуючих стандартів і нормативних документів та їх адекватності з урахуванням існуючих ризиків;
- аналіз конфігурації маршрутизаторів і проксі-серверів, поштових і DNS-серверів, шлюзів віртуальних приватних мереж (VPN) та інших критично важливих елементів інфраструктури мережі;
- проведення сканування зовнішніх мережевих адрес з локальної мережі;
- сканування ресурсів локальної мережі зсередини;
- проведення аналізу конфігурації серверів і робочих станцій з використанням спеціалізованих програмних агентів.

Наведені технічні методи передбачають використання як активного, так і пасивного тестування систем захисту інформації. Активне тестування має на увазі моделювання дій потенційного зловмисника; а *пасивне* - спирається на аналіз конфігурації ОС і встановлених додатків з використанням шаблонів та списків перевірки. Обидва види тестування можна проводити вручну або з використанням спеціальних програмних засобів.

Виконуючи аналіз конфігурації засобів захисту для зовнішньої частини локальної мережі і управління міжмережними взаємодіями особливу увагу треба звернути на наступні аспекти:

- створення правил розмежування доступу;

- створення схем та проведення налаштування параметрів автентифікації;
- налаштування параметрів системи реєстрації подій;
- впровадження механізмів, які забезпечують приховування топології мережі, яку треба захистити (трансляція мережевих адрес);
- настроювання механізмів сповіщення про атаки;
- перевірка наявності та працездатності засобів контролю цілісності;

Аналіз конфігурації має на увазі перевірку правильності встановлення великої кількості різних параметрів. Щоб автоматизувати цей процес можуть використовуватися спеціалізовані програмні засоби аналізу ступеню захищеності, асортимент яких в даний час доволі широкий.

Одним із сучасних методів автоматизації процесів аналізу та контролю захищеності розподілених систем є використання технологій інтелектуальних програмних агентів. Для кожної з контрольованих систем встановлюють програмний агент, котрий виконує відповідні налаштування, робить перевірку їх правильності, контролює цілісність файлів, своєчасність встановлення оновлень, а також вирішує додаткові завдання з контролю захищеності ІС. Управляє агентами віддалена програма-менеджер, через мережу. Ці менеджери, які є центральними компонентами таких систем, розсилають керуючі команди до всіх агентів контрольованого ними домену і забезпечують зберігання всіх отриманих від агентів даних в центральній базі даних. Адміністратор може керувати менеджерами за допомогою графічного інтерфейсу, що дозволяє вибирати, змінювати та створювати нові політики безпеки, проводити аналіз змін стану системи, здійснювати ранжування вразливостей і т. п. Всі взаємодії між агентами, менеджерами і керуючою програмою здійснюються з використанням захищеного клієнт-серверного протоколу.

Четверта група включає в себе передпроектне обстеження. Це самий складний варіант аудиту. Він передбачає аналіз організаційної структури компанії, правил доступу робітників до тих або інших додатків. Потім треба виконати аналіз самих додатків. Також повинні бути врахованими конкретні служби доступу з одного рівня на інший і служби, які необхідні для інформаційного обміну. Також відбувається доповнення вбудованими механізмами безпеки, що при поєднанні з оцінками збитків у разі порушення ІБ дає підстави для проведення ранжування ризиків, що існують в ІС, і вироблення адекватних заходів протидії. Успішне проведення такого обстеження та подальшого аналізу ризиків і формування вимог визначать, в якій мірі прийняті заходи будуть адекватними загрозам, ефективними і економічно виправданими.

Проектування системи. На сьогодні є два підходи щодо побудови системи ІБ: продуктовий і проектний. Продуктовий підхід передбачає вибір набору засобів фізичного, технічного та програмного захисту, аналіз функцій, а вже на основі аналізу визначається політика доступу до інформаційних ресурсів. Можна діяти навпаки: спочатку опрацювати політику доступу, на основі якої визначити функції, необхідні для її реалізації, і здійснити вибір засобів і продуктів, що забезпечать виконання цих функцій. Вибір методів буде залежати від конкретних умов діяльності організації, її фізичного місцезнаходження, складу підсистем ІС, сукупності завдань, вимог до системи захисту і т. д. Більш дешевим з точки зору витрат на проектування є продуктовий підхід. Окрім того, в деяких випадках він виявляється єдиним можливим в умовах нестачі рішень або жорстких вимог нормативних документів (наприклад, для забезпечення криптографічного захисту інформації в мережах спеціального призначення та урядових телефонних мережах використовують тільки такий підхід).

Проектний підхід є більш повним, і рішення, побудовані на його основі, зручніші та простіші для атестації. Він виявляється кращим і при створенні великих гетерогенних розподілених систем, адже на відміну від продуктового підходу не зв'язаний якоюсь конкретною платформою. Також, він забезпечує більш "довгоживучі" рішення, бо допускає заміну продуктів і рішень не змінюючи політики доступу. А це, в свою чергу, забезпечує високий показник повернення інвестицій при розвитку ІС і системи ІБ.

Проектування архітектури системи інформаційної безпеки може відбуватись із застосуванням об'єктног, прикладного або змішаного підходів.

Об'єктний підхід вибудовує захист інформації на основі фізичної структури певного об'єкта (будівлі, підрозділу, підприємства). При застосуванні об'єктного підходу припускається використання набору універсальних рішень з метою забезпечення механізмів безпеки, підтримується однорідний набір організаційних заходів. Класичним прикладом такого підходу можна вважати побудову захищених інфраструктур зовнішнього інформаційного обміну, локальних мереж, систем телекомунікацій і т. д. З недоліків можна відзначити очевидну неповноту універсальних механізмів, особливо для організацій з великою кількістю складно зв'язаних між собою програм.

Прикладний підхід в свою чергу "прив'язує" механізми безпеки до певного додатку. Прикладом такого підходу може бути захист підсистеми або окремих зон автоматизації. Незважаючи на більшу повноту захисних заходів, у цього підходу є і недоліки, а саме: необхідність зв'язувати різні за функціональним можливостям засоби забезпечення безпеки для зменшення витрат на адміністрування та експлуатацію та необхідність задіяти вже існуючі засоби для збереження інвестицій.

Комбінацією двох описаних раніше підходів являє собою змішаний підход. В ньому ІС представляється як набір об'єктів, для кожного з яких застосовується об'єктний підхід, а для взаємозалежних об'єктів використовується прикладний. Цей метод є більш трудомістким на стадії проектування, проте часто дає хорошу економію коштів при впровадженні, використанні та підтримці системи захисту інформації.

Служби і механізми безпеки. Стратегія захисту може бути реалізована двома методами: ресурсним і сервісним. Ресурсний розглядає ІС як набір ресурсів, які "прив'язані" до конкретних компонент системи ІБ. Даний метод добре підходит для невеликих ІС з обмеженим набором задач. Розширюючи коло завдань і при розростанні ІС часто доводиться дублювати елементи захисту для однотипних ресурсів, що призводить до зайвих витрат. Сервісний підхід розглядає ІС як набір служб, програмних і телекомунікаційних сервісів, використовуваних для надання послуг користувачам. Тут один і той же елемент захисту може бути використаний для різних сервісів, побудованих на однакових технічних пристроях. Зараз сервісний підхід виглядає ефективнішим, оскільки припускає строгий функціональний аналіз існуючих служб, які забезпечують роботу ІС, і дозволяє виключати широкий клас загроз відмовляючись від служб, які не будуть використовуватись. Саме сервісний підхід покладено в основу сучасних стандартів щодо безпеки, зокрема ISO:15408.

Впровадження та атестація. Етап впровадження містить в собі комплекс послідовно проведених заходів, включаючи установку і конфігурування засобів захисту, навчання користувачів роботі із засобами захисту, попередні випробування і здачу в дослідну експлуатацію. Дослідна експлуатація дає змогу виявити і усунути можливі недоліки в функціонуванні підсистеми інформаційної безпеки, перед запуском системи в робочому

режимі. Якщо під час дослідної експлуатації було виявлено факти некоректної роботи компонентів, то проводиться коригування налаштувань засобів захисту, режимів в яких вони функціонують і т. п. За результатами дослідної експлуатації вносяться коригування, якщо в них є необхідность, і уточнюються налаштування засобів захисту. Далі слід провести приймально-здавальні випробування, а після введення в штатну експлуатацію і надалі надавати технічну підтримку і супровід.

Підтвердити функціональну повноту системи безпеки і забезпечення необхідного рівня захищеності ІС можна шляхом проведенням атестації системи ІБ відповідним акредитованими установами. Атестація має на меті комплексну перевірку захищеного об'єкта в реальних умовах експлуатації щоб оцінити відповідність застосовуваного комплексу заходів і засобів захисту до необхідного рівня безпеки. Атестація проводиться згідно відповідно до схеми, яка складається на підготовчому етапі спираючись на наступний перелік робіт:

- аналіз вихідних даних, попереднє ознайомлення з об'єктом атестації та інформатизації;
- експертне обстеження об'єкта інформатизації з аналізом документації з питань захисту інформації на відповідность вимогам;
- проведення випробувань окремих засобів і систем захисту інформації на базі випробувальних центрів;
- виконання комплексних атестаційних випробувань об'єкта інформатизації в реальних умовах експлуатації;
- аналіз результатів, отриманих в ході експертного обстеження та атестаційних випробувань з послідуючим затвердження висновку за результатами атестації об'єкта інформатизації.

За результатами випробувань створюється звітна документація, проводиться оцінка результатів випробувань і надається атестат відповідності встановленого зразка. Наявність атестату дає право обробляти інформацію зі ступенем конфіденційності та на період часу, встановленими цим атестатом.

Технічна підтримка та супровід. Для забезпечення підтримки працездатності підсистеми інформаційної безпеки та безперебійного виконання цією системою своїх функцій треба передбачити комплекс заходів пов'язаних з технічною підтримкою та супроводом програмного і апаратного забезпечення підсистеми інформаційної безпеки, до яких відносять поточне адміністрування, роботи, що проводяться в екстрених випадках, а також періодично профілактичні роботи. Цей комплекс заходів може включати в себе:

- адміністрування штатних засобів захисту та їх технічне обслуговування;
- контроль за станом системи, профілактичне обстеження конфігурації, виявлення можливих потенційних проблем;
- перевірка та встановлення випущених оновлень і програмних засобів захисту, а також ОС, СУБД і додатків, що використовуються;
- проведення регулярного пошуку і аналізу вразливостей в системі, що захищається. з використанням спеціальних засобів сканування;
- діагностику несправностей та проведення робіт з відновлення при виникненні аварійних і позаштатних ситуацій;
- проведення періодичного тестування системи інформаційної безпеки та оцінки ефективності захисту.

Технічна підтримка та супровід системи інформаційної безпеки потребує наявності у обслуговуючого персоналу певних знань і навичок та

може здійснюватися як штатними працівниками компанії, відповідальними за інформаційну безпеку, так і робітниками спеціалізованих організацій. [11]

2.4 Висновки до розділу 2

В другому розділі було більш детально проаналізовано структуру стандарту, призначення кожної з його частин. Визначено принципи, важливі для забезпечення високого ступеню безпеки, інформаційної системи на етапі розробки її архітектури, такі як безперервність захисту в просторі та часі, наявність розподілу ролей користувачів, проектування системи, яка буде не дуже складною, що підвищить рівень керованості. Досліджено основні об'єкти вразливостей. До них віднесено:

- обчислювальні процеси
- інформацію баз даних
- код програм
- користувацька інформація

Проаналізовано основні внутрішні та зовнішні дестабілізуючі фактори та загрози безпеці та методи протидії їм, а також можливі наслідки дії цих факторів.

Досліджено етапи, на які ISO:15408 радить розбивати процес побудови системи інформаціної безпеки.

- Етап аналізу ризиків
- Етап висування вимог
- Етап проектування
- Етап впровадження
- Етап атестації та супроводу системи

РОЗДІЛ 3. АНАЛІЗ ФУНКЦІОНАЛЬНИХ КЛАСІВ

3.1 Аудит безпеки (FAU)

Аудит безпеки включає в себе розпізнавання, запис, збереження та аналіз інформації, пов'язаної з діями, що стосуються безпеки (наприклад, з діями, контрольованими ПБО). Записи аудиту, одержувані в результаті, можуть бути проаналізовані, щоб визначити, які дії, пов'язані з безпекою, відбувалися і хто з користувачів за них відповідає. Декомпозиція класу представлена на рисунку 3.1.

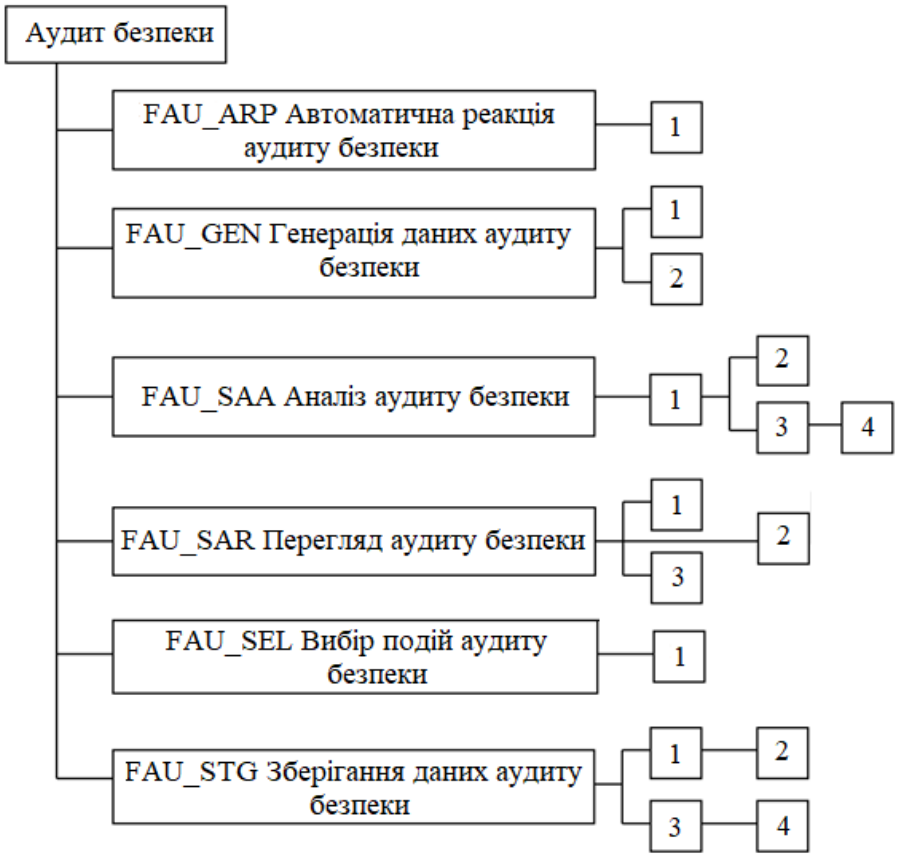

Рисунок 3.1 Декомпозиція класу FAU

Автоматична реакція аудиту безпеки (FAU_ARP)

Сімейство FAU_ARP визначає реакцію на виявлення подій, що вказують на можливе порушення безпеки.

В даному сімействі визначено одну компоненту FAU_ARP.1 “Сигнали порушення безпеки”. ФБО повинні вживати заходів у разі виявлення можливого порушення безпеки.

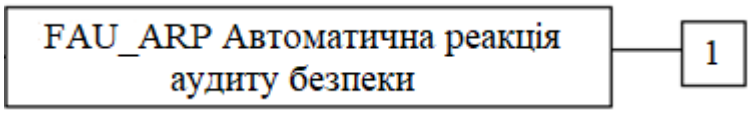

Рисунок 3.2 Ранжирування компонентів в FAU_ARP

Генерація даних аудиту безпеки (FAU_GEN)

Сімейство FAU_GEN визначає вимоги щодо реєстрації виникнення подій, що відносяться до безпеки, які підконтрольні ФБО. Це сімейство ідентифікує рівень аудиту, перераховує типи подій, які потенційно повинні піддаватися аудиту з використанням ФБО, і визначає мінімальний обсяг пов'язаної з аудитом інформації, яку слід подавати в записах аудиту різного типу.

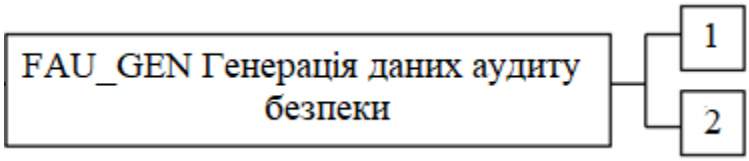

Рисунок 3.3 Ранжирування компонентів в FAU_ GEN

В FAU_GEN визначено наступні компоненти:

- FAU_GEN.1 «Генерація даних аудиту»
- FAU_GEN.2 «Асоціація ідентифікатора користувача»

FAU_GEN.1 визначає рівень подій, потенційно піддаються аудиту, і склад даних, які повинні бути зареєстровані в кожному записі.

Згідно до FAU_GEN.2 ФБО повинні асоціювати події, які потенційно піддаються аудиту, і особисті ідентифікатори користувачів.

Аналіз аудиту безпеки (FAU_SAA)

Сімейство FAU_SAA визначає вимоги до автоматичних засобів, які аналізують показники функціонування системи і дані аудиту з метою пошуку можливих або реальних порушень безпеки. Цей аналіз може використовуватися для підтримки як виявлення втручання, так і автоматичного реагування на очікуване порушення безпеки.

Дії, що вживаються при виявленні порушень, можуть бути при необхідності визначені з використанням сімейства FAU_ARP.

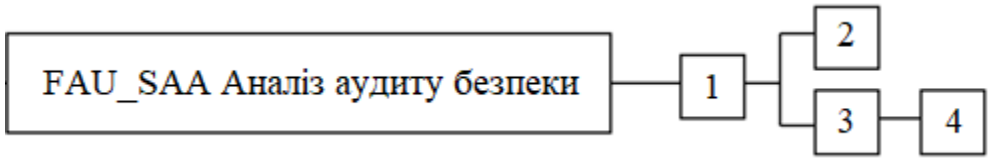

Рисунок 3.4 Ранжирування компонентів в FAU_ARP

Компонента FAU_SAA.1 «Аналіз потенційного порушення» визначає поріг виявлення на основі раніше визначеного набору правил.

У відповідності до FAU_SAA.2 «Виявлення аномалії, засноване на профілі» ФБО підтримують окремі профілі використання системи, де профіль являє собою шаблони передісторії використання, що виконувалися учасниками цільової групи профілю. Цільова група профілю може включати в себе одного або декількох учасників, які взаємодіють з ФБО. Кожному учаснику цільової групи профілю призначається індивідуальний рейтинг підозрілої активності, який показує, наскільки поточні показники дій учасника відповідають встановленим шаблонами використання, представленим в профілі. Цей аналіз може виконуватися під час функціонування ГО або при аналізі даних аудиту в пакетному режимі.

Згідно до FAU_SAA.3 «Проста евристика атаки» ФБО повинні бути здатні виявити виникнення характерних подій, які свідчать про значну загрозу здійсненню ПБО. Цей пошук характерних подій може відбуватися в режимі реального часу або при аналізі даних аудиту в пакетному режимі.

FAU_SAA.4 «Складна евристика атаки» стверджує, що ФБО повинні бути здатні визначити і виявити багатокрокові сценарії проникнення. Тут ФБО здатні порівняти події в системі (можливо, що виконуються декількома учасниками) з послідовностями подій, відомими як повні сценарії проникнення. ФБО повинні бути здатні вказати на виявлення характерного події або послідовності подій, які свідчать про можливе порушення ПБО.

Перегляд аудиту безпеки (FAU_SAR)

Це сімейство визначає вимоги до інструментів аудиту, які повинні бути доступними авторизованим користувачам для надання допомоги у перегляді даних аудиту.

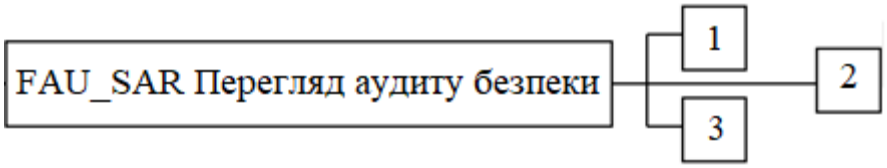

Рисунок 3.5 Ранжирування компонентів в FAU_SAR

FAU_SAR.1 Аудиторський огляд забезпечує можливість читання інформації з аудиторських записів.

FAU_SAR.2 Обмежений аудит вимагає, щоб не було інших користувачів, крім тих, що були ідентифіковані в FAU_SAR.1, які можуть читати інформацію.

FAU_SAR.3. Вибір аудиторського розгляду вимагає інструментів перевірки аудиту, щоб вибрати дані аудиту, які будуть переглянуті на основі критеріїв.

Вибір події з аудиту безпеки (FAU_SEL)

Це сімейство визначає вимоги до вибору події, яка повинна бути перевірена під час роботи ОО. Він визначає вимоги до включення або виключення подій із сукупності аудиторських подій.

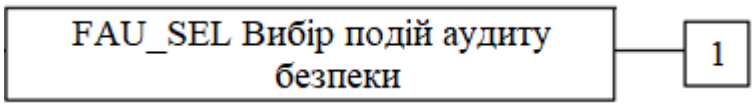

Рисунок 3.6 Ранжирування компонентів в FAU_SEL

FAU_SEL.1 “Вибірковий аудит” вимагає можливості включати чи виключати події з набору подій, що перевіряються, згідно до атрибутів, що визначаються автором ПЗ / ЗБ.

Зберігання даних, які отримані за результатами аудиту безпеки (FAU_STG)

Це сімейство визначає вимоги до ФБО, для отримання можливості створювати та підтримувати безпечну історію проведення аудиту.

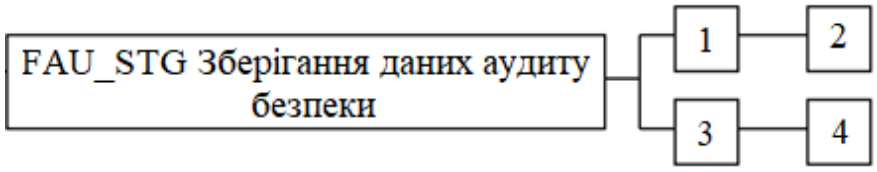

Рисунок 3.7 Ранжирування компонентів в FAU_STG

Відповідно до FAU_STG.1 “Захищені сховища журналів аудиту” журнали мають розміщуються так, аби вони були захищеними від несанкціонованого видалення та / або модифікації.

FAU_STG.2 “Гарантії доступності даних аудиту” вказує на те, що ФБО підтримує дані аудиту з урахуванням виникнення небажаного стану.

FAU_STG.3 “Дії у разі вірогідної втрати даних аудиту” описує дії, які слід вжити, якщо перевищено порогове значення наповнення журналу аудиту.

FAU_STG.4 “Попередження втрати даних аудиту” вказує на те, як слід чинити у разі переповнення журналу аудиту.

3.2 Зв’язок (FCO)

Цей клас включає два сімейства, які специфічно пов'язані з забезпеченням ідентичності сторони, яка бере участь у обміні даними. Ці сімейства пов'язані з забезпеченням ідентичності джерела переданої інформації (підтвердження походження) та забезпечення ідентифікації одержувача переданої інформації (підтвердження отримання). Ці сімейства гарантують, що автор не може заперечувати факт надсилання повідомлення, а одержувач не зможе заперечити, що отримав це повідомлення.

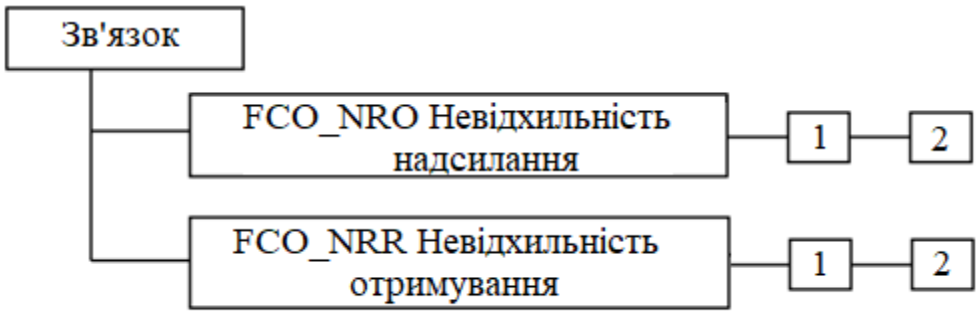

Рисунок 3.8 Декомпозиція класу FCO

В класі визначено два сімейства:

- Невідхильність надсилання (FCO_NRO)
- Невідхильність отримування (FCO_NRR)

Невідхильність надсилання (FCO_NRO)

Неможливість відмови від відправлення гарантує, що джерело інформації не зможе успішно відмовити у надсиланні інформації. Це сімейство вимагає, щоб ФБО забезпечували методи, які гарантували б, що

суб'єкт, який отримує інформацію під час обміну даними, має докази походження інформації.

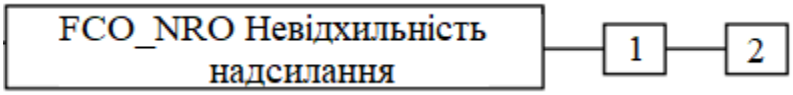

Рисунок 3.9 Ранжирування компонентів в FCO_NRO

FCO_NRO.1 “Вибіркове підтвердження походження” вимагає від ФБО надання суб'єктам можливості запитувати докази походження інформації.

FCO_NRO.2 “Примусовий доказ походження” вимагає, щоб ФБО завжди генерували докази походження для переданої інформації.

Невідхильність отримування (FCO_NRR)

Неможливість відмови від отримання гарантує, що одержувач інформації не зможе успішно відмовити в отриманні інформації. Це сімейство вимагає, щоб ФБО надавали методи, для гарантування того, що суб'єкт, який передає інформацію під час обміну даними, має докази отримання інформації.

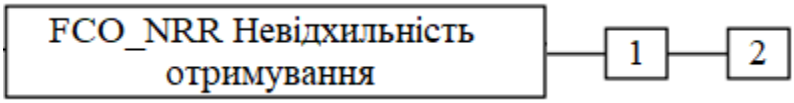

Рисунок 3.10 Ранжирування компонентів в FCO_NRR

FCO_NRR.1 “Вибіркове підтвердження отримання” вимагає, щоб ФБО надавали суб'єктам здатність подавати докази про отримання інформації.

FCO_NRR.2 “Примусове підтвердження отримання” вимагає, щоб ФБО завжди надавали докази отримання для отриманої інформації

3.3 Ідентифікація та аутентифікації (FIA)

Сімейства цього класу відповідають вимогам щодо функцій для встановлення та підтвердження заявленої ідентифікації користувача.

Ідентифікація та автентифікація необхідні для забезпечення відповідності користувача відповідним атрибутам безпеки (наприклад, ідентифікація, групи, ролі, рівні безпеки та цілісності).

Неодмінна ідентифікація авторизованих користувачів та правильне об'єднання атрибутів безпеки з користувачами та темами має вирішальне значення для забезпечення виконання передбачених правил безпеки.

Сім'ї в цьому класі займаються визначенням та перевіркою ідентичності користувачів, визначенням їх повноважень для взаємодії з ФБО та правильною асоціацією атрибутів безпеки для кожного авторизованого користувача. Інші категорії вимог (наприклад, захист даних користувачів, аудит безпеки) залежать від правильної ідентифікації та автентифікації користувачів, щоб вони були ефективними.

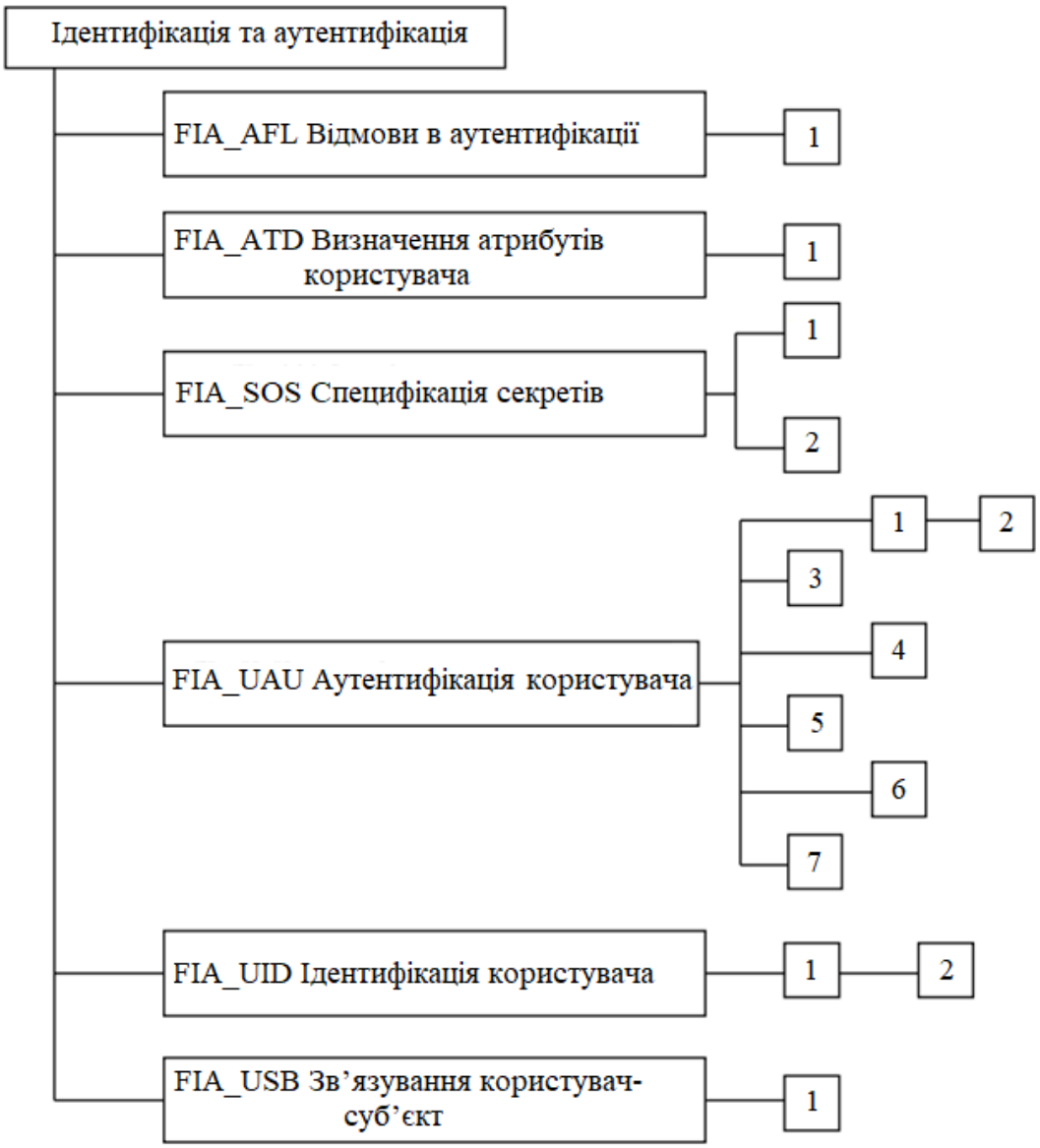

Рисунок 3.11 Декомпозиція класу FIA

Відмови в аутентифікації (FIA_AFL)

Це сімейство містить вимоги до визначення значень кількості невдалих спроб автентифікації та дій ФБО у випадках невдалих спроб автентифікації. Параметри включають (але не обмежуються) кількість невдалих спроб аутентифікації та порогові значення часу.

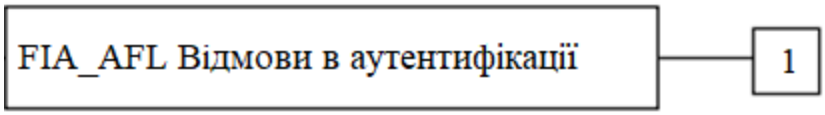

Рисунок 3.12 Ранжирування компонентів в FIA_AFL

FIA_AFL.1 “Обробка відмов аутентифікації” вимагає, щоб ФБО мали змогу припинити процес встановлення сесії після певної кількості невдалих спроб автентифікації користувача. Також вимагається, щоб після закінчення процесу встановлення сесії ФБО могли відключити обліковий запис користувача або точку входу (наприклад, робоча станція), з якої були зроблені спроби, поки адміністратор не прийме відповідне рішення.

Визначення атрибутів для користувачів (FIA_ATD)

Всі авторизовані користувачі можуть мати набір атрибутів безпеки, окрім ідентифікатора користувача, який використовується для забезпечення виконання ПБО. Це сімейство визначає вимоги щодо асоціації атрибутів захисту із користувачами, якщо це необхідно для підтримки ПБО.

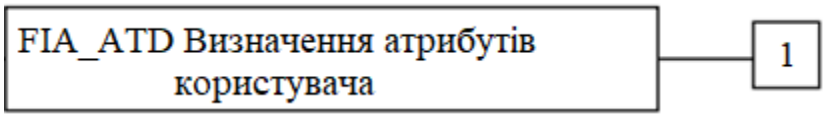

Рисунок 3.13 Ранжирування компонентів в FIA_ATD

FIA_ATD.1 “Визначення атрибута користувача”, дозволяє зберігати атрибути безпеки для кожного користувача індивідуально.

Специфікація секретів (FIA_SOS)

Це сімейство визначає вимоги до механізмів, що забезпечують встановлені показники якості на наданих секретах та створюють секрети для задоволення визначеної метрики.

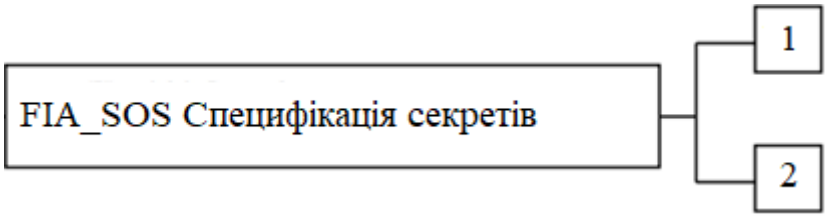

Рисунок 3.14 Ранжирування компонентів в FIA_SOS

FIA_SOS.1 “Перевірка секретності” вимагає, щоб ФБО перевірила, чи секрети відповідають визначеним показникам якості.

FIA_SOS.2 “Створення секретів” вимагає від ФБО генерувати секрети, які відповідають певним показникам якості.

Аутентифікація користувача (FIA_UAU)

Це сімейство визначає типи механізмів автентифікації користувачів, які підтримуються ФБО. Ця сім'я також визначає необхідні атрибути, на яких повинні базуватися механізми автентифікації користувача.

Рисунок 3.15 Ранжирування компонентів в FIA_UAU

FIA_UAU.1 “Терміни автентифікації”, дозволяють користувачеві виконувати певні дії до автентифікації користувача.

FIA_UAU.2 “Аутентифікація користувача перед будь-якою дією користувача“ вимагає, щоб користувачі самостійно автентифікувались, перш ніж вчинити дію ФБО дасть їм можливість виконвати якісь дії.

FIA_UAU.3 “Незаперечна автентифікація” вимагає, щоб механізм автентифікації мав можливість виявляти та запобігати використанню підроблених або скопійованих даних аутентифікації.

FIA_UAU.4 “Механізми одноразового автентифікації”, вимагає механізму автентифікації, який працює з одноразовими даними аутентифікації.

FIA_UAU.5. “Комбінування механізмів автентифікації” вимагає, щоб для автентифікації ідентифікацій користувачів для певних подій, було надано та використано різні механізми автентифікації.

FIA_UAU.6 “Повторна автентифікація” вимагається можливість вказати перелік подій, для яких користувачеві потрібно повторно перевірити автентичність.

FIA_UAU.7 “Автентифікації з захищеним зворотнім зв'язком” вимагає під час автентифікації надання користувачеві обмеженої інформації про неї.

Ідентифікація користувача (FIA_UID)

Це сімейство визначає умови, за яких користувачі повинні будуть самостійно ідентифікувати себе перед виконанням будь-яких інших дій, які повинні бути опосередковані ФБО і вимагають ідентифікації користувача.

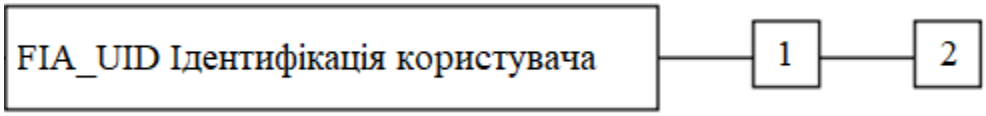

Рисунок 3.16 Ранжирування компонентів в FIA_UID

FIA_UID.1 “Терміни ідентифікації” дозволяють користувачам виконувати певні дії, перш ніж вони ідентифікуються за допомогою ФБО.

FIA_UID.2 “Ідентифікація користувача перед будь-якою дією” вимагає, щоб користувачі ідентифікували себе перед тим, як ФБО дозволять йому виконувати будь-які дії.

Пов’язування користувач-суб’єкт (FIA_USB)

Автентифікований користувач, для того, щоб використовувати ОО, зазвичай активує певний суб’єкт. Атрибути безпеки користувача пов'язуються (повністю або частково) з цим суб’єктом. Це сімейство визначає вимоги щодо створення і підтримки асоціації атрибутів безпеки користувача з суб’єктом, що діє від імені користувача.

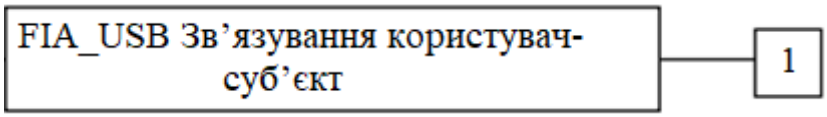

Рисунок 3.17 Ранжирування компонентів в FIA_USB

FIA_USB.1 “Зв’язування користувач-суб’єкт” вимагає підтримання зв'язку між атрибутами безпеки користувача та суб'єктом, що діє від імені користувача.

3.4 Приватність (FPR)

Цей клас містить вимоги щодо конфіденційності. Ці вимоги забезпечують захист користувачів від виявлення та неправильного використання ідентичності іншими користувачами.

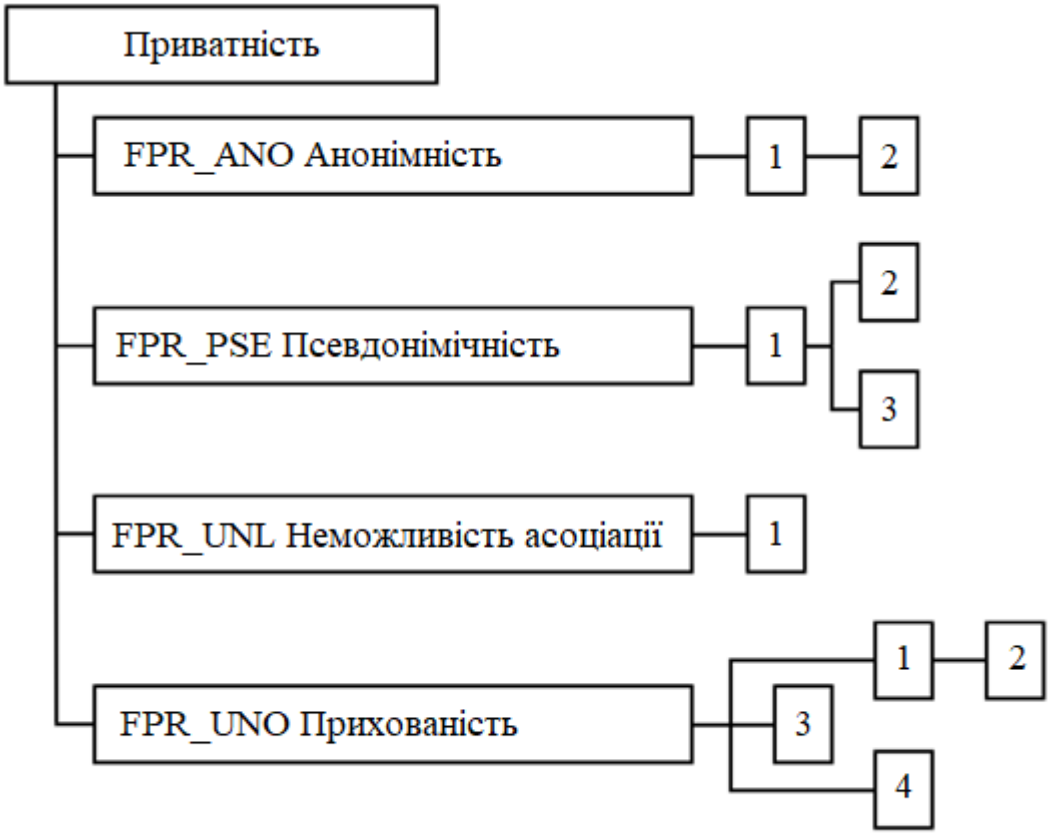

Рисунок 3.18 Декомпозиція класу FPR

Анонімність (FPR_ANO)

Це сімейство гарантує, що користувач може використовувати ресурс чи послугу, не розкриваючи себе. Вимоги до анонімності забезпечують захист ідентичності користувача. Анонімність не покликана захистити предметну ідентичність.

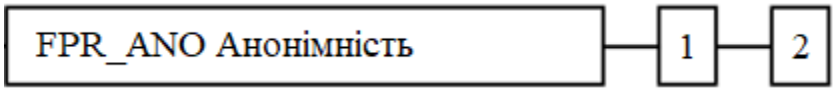

Рисунок 3.19 Ранжирування компонентів в FPR_ANO

FPR_ANO.1 “Анонімність” вимагає, щоб будь-який інший користувач або суб’єкт не зміг визначити особу користувача, пов'язаного з предметом або операцією.

FPR_ANO.2 “Анонімність без запиту інформації” накладає додаткові вимоги на FPR_ANO.1, забезпечуючи, що ФБО не вимагає ідентифікатор користувача.

Псевдонімічність (FPR_PSE)

Це сімейство гарантує, що користувач може використовувати ресурс чи послугу, не розкриваючи свого ідентифікатора, але все ще може бути відповідальним за виконані дії.

Рисунок 3.20 Ранжирування компонентів в FPR_PSE

FPR_PSE.1 “Псевдонімічність” вимагає, щоб набір користувачів та/або суб’єктів не зміг дізнатися ідентифікатор користувача, який пов'язаний з суб'єктом або операцією, але цей користувач все ще ніс відповідальність за виконані дії.

FPR_PSE.2 “Зворотна псевдонімічність” вимагає від ФБО надавати можливість визначати початковий ідентифікатор користувача на основі наданого псевдоніму.

FPR_PSE.3 “Альтернативна псевдонімічність” вимагає від ФБО дотримуватися певних правил побудови псевдоніму до ідентифікатора користувача.

Неможливість асоціації (FPR_UNL)

Це сімейство гарантує, що користувач може багаторазово використовувати ресурси чи послуги, при цьому інші користувачі не зможуть пов'язувати разом ці спроби.

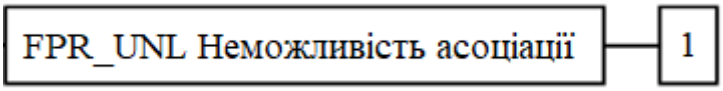

Рисунок 3.21 Ранжирування компонентів в FPR_UNL

FPR_UNL.1 “Неможливість асоціаці” вимагає, щоб користувачі та/або суб'єкти не мали змоги визначити, чи викликає один і той самий користувач певні операції в системі.

Прихованість (FPR_UNO)

Це сімейство гарантує, що користувач може використовувати ресурс чи послугу без необхідності повідомляти про це інших, особливо третіх сторін.

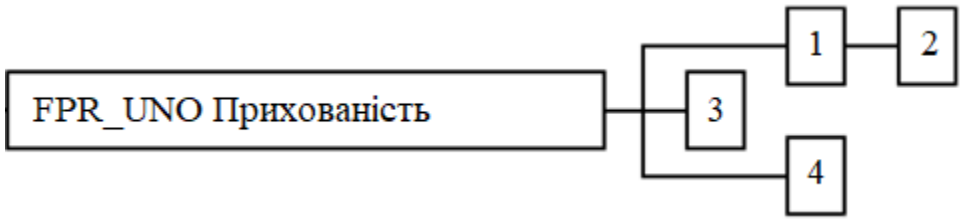

Рисунок 3.22 Ранжирування компонентів в FPR_UNO

FPR_UNO.1 “Прихованість” вимагає, щоб користувачі та/або суб'єкти не мали змоги визначити, чи виконується операція.

FPR_UNO.2. “Розподіл інформації, що впливає на прихованість”, вимагає, щоб в ФБО були передбачені спеціальні механізми, що дозволяють уникнути концентрації інформації, пов'язаної з конфіденційністю, в межах

ОО. Такі концентрації можуть вплинути на прихованість, якщо виникне порушення безпеки.

FPR_UNO.3 “Прихованість без запиту інформації” вимагає, щоб ФБО не намагалися отримати конфіденційну інформацію, яка зможе бути використаною для порушення прихованості.

FPR_UNO.4. “Відкритісь для уповноваженого користувача”. Для одного чи декількох таких користувачів ФБО повинні забезпечити здатність спостерігати за використанням ресурсів та/або послуг.

3.5 Криптографічна підтримка (FCS)

ФБО може використовувати криптографічні функції, щоб задовольнити декілька цілей безпеки високого рівня. До таких цілей можна віднести: ідентифікацію та автентифікацію, неповторність, довірений шлях, довірений канал та розділення даних. Цей клас використовується, коли ОО реалізує криптографічні функції, реалізація яких може здійснюватися в апаратно-програмними та/або програмними методами.

Клас FCS складається з двох сімейств: FCS_CKM – “управління криптографічними ключами” та “криптографічні операції” FCS_COP. Перше розглядає аспекти керування криптографічними ключами, тоді як FCS_COP стосується оперативного використання цих криптографічних ключів.

Рисунок 3.23 Декомпозиція класу FCS

Управління криптографічними ключами (FCS_CKM)

Управління криптографічними ключами повинно відбуватись протягом всього їх життєвого циклу. Це сімейство призначене для підтримки цього життєвого циклу і, отже, визначає вимоги до таких дій: генерація, розповсюдження, доступ та знищення криптографічного ключа. Це сімейство повинне бути включеним, коли є функціональні вимоги до управління криптографічними ключами.

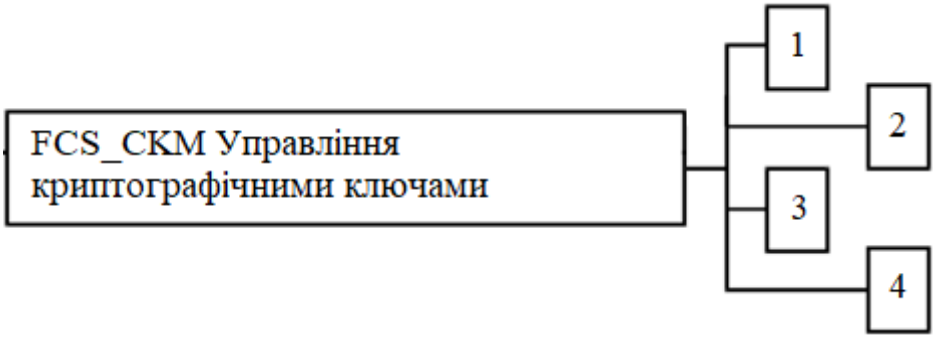

Рисунок 3.24 Ранжирування компонентів в FCS_CKM

FCS_CKM.1 “Створення криптографічного ключа” вимагає створювати криптографічні ключі у відповідності до заданого алгоритму та розмірів ключів, які базуються на відповідному стандарті.

FCS_CKM.2 “Розповсюдження криптографічного ключа” вимагає щоб криптографічні ключі розповсюджувались у відповідності до заданого методу розподілу, який базується на відповідному стандарті.

FCS_CKM.3 “Доступ до криптографічного ключа” вимагає щоб доступ до ключів відбувався у відповідності до заданого методу доступу, який базується на певному стандарті.

FCS_CKM.4 “Деструкція криптографічного ключа” вимагає знищення криптографічних ключів у відповідності до заданого методу знищення, який базується на певному стандарті.

Криптографічні операції (FCS_COP)

Для правильної роботи криптографічної операції операція повинна виконуватися у відповідності з заданим алгоритмом та криптографічним ключем заданого розміру. Це сімейство має бути включеним, коли існують вимоги щодо виконання таких операцій.

Типові криптографічні операції включають в себе шифрування та/або дешифрування даних, створення та/або перевірку цифрових підписів, генерацію криптографічної контрольної суми для цілісності та/або перевірки контрольної суми, безпечного хешування, шифрування та/або дешифрування ключа та угоду про криптографічні ключі .

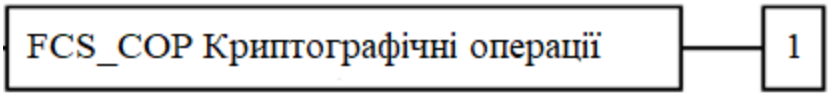

Рисунок 3.25 Ранжирування компонентів в FCS_COP

FCS_COP.1 “Криптографічні операції” вимагає виконання криптографічної операції у відповідності до заданого алгоритму та ключа з заданими розмірами. Вказаний алгоритм та розміри ключа взмозі базуватися на певному стандарті.

3.6 Довірені шляхи та канали (FTP)

Сімейства цього класу встановлюють вимоги до надійного шляху зв'язку між користувачами та ФБО, а також до надійного каналу зв'язку між ФБО та іншими довіреним IT-продуктами. Довірені маршрути та канали можна охарактеризувати наступним чином:

- Маршрут будується за допомогою внутрішніх та зовнішніх каналів зв'язку (відповідно до компоненту), які ізолюють ідентифіковану підмножину даних та команд ФБО від інших частин ФБО та даних користувача.
- Використання маршруту може ініціювати користувач та/або ФБО (відповідно до компоненту)
- Маршрут здатний забезпечити впевненість, що користувач обмінюється даними з правильними ФБО, і що ФБО виконує обмін з правильним користувачем (відповідно до компонента)

У цій парадигмі довіреним каналом є канал зв'язку, який може ініціювати будь-яка зі сторін каналу, що зв’язуються, і забезпечує неможливість відмови від ідентичності сторін каналу.

Довірений маршрут забезпечує можливості для користувачів виконувати функції прямо взаємодіючи з ФБО. Довірений шлях, як правило, бажаний для дій користувача, таких як початкова ідентифікація та/або автентифікація, але може також бути використаним і під час всього сеансу. Обміни по довіреному маршруту можуть ініціюватися користувачем або

ФБО. Довірений маршрут гарантує, що відповіді, отримані за його допомогою захищаються від модифікації або розголошення ненадійними програмами.

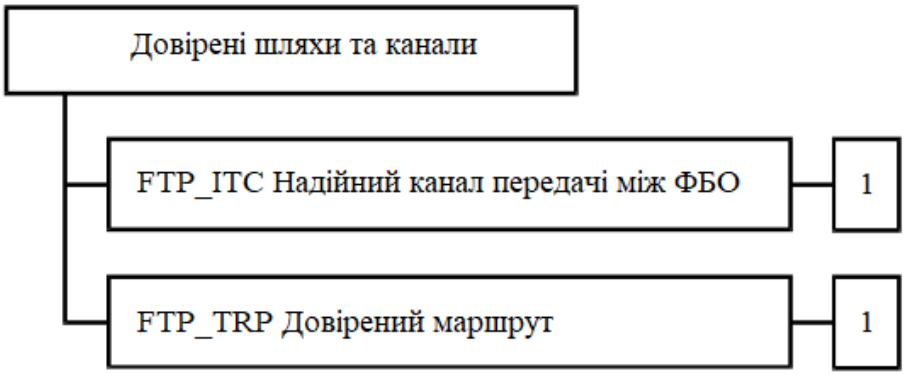

Рисунок 3.26 Декомпозиція класу FTP

Надійний канал передачі між ФБО (FTP_ITC)

Це сімейство визначає вимоги до створення надійного каналу між ФБО та іншими надійними ІТ-продуктами для виконання операцій, які критичні для безпеки. Дане сімейство слід включати, коли існують вимоги до безпечної передачі даних користувача або ФБО між ОО та іншими надійними ІТ-продуктами.

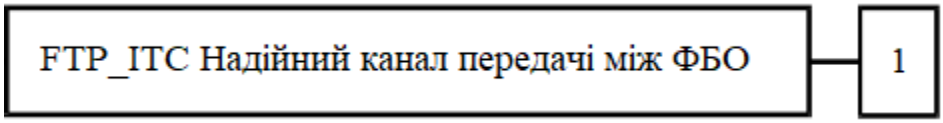

Рисунок 3.27 Ранжирування компонентів в FTP_ITC

FTP_ITC.1 “Довірений канал між ФБО“ вимагає, щоб ФБО забезпечували довірений канал зв'язку між собою та іншим надійними ІТ-продуктоми.

Довірений маршрут (FTP_TRP)

Це сімейство визначає вимоги щодо встановлення та підтримки довірених комунікацій між користувачами та ФБО. Довірений шлях може знадобитися для будь-якої взаємодії, що стосується безпеки. Обмін надійними шляхами може бути ініційований користувачем під час взаємодії з ФБО, або ФБО можуть встановити зв'язок з користувачем через довірений шлях.

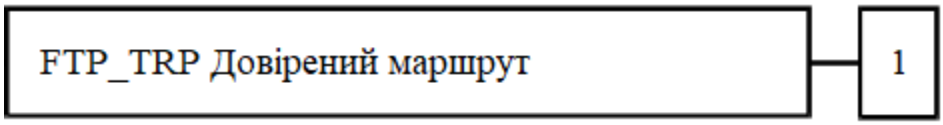

Рисунок 3.28 Ранжирування компонентів в FTP_TRP

FTP_TRP.1 “Довірені маршрути” вимагає, щоб надійний маршрут між ФБО і користувачем був забезпечений для набору подій, визначених автором ПЗ/ЗБ. Користувач та/або ФБО можуть мати можливість ініціювати довірений маршрут.

3.7 Висновки до розділу 3

В даному розділі було досліджено структуру та призначення найважливіших функціональних класів, запропонованих в ISO:15408. Проаналізовано сімейства, на які розділено класи та роль компонентів в кожному сімействі. Було проведено дослідження наступних класів:

- Аудит безпеки (FAU)
- Зв’язок (FCO)
- Ідентифікація та аутентифікація (FIA)
- Приватність (FPR)
- Криптографічна підтримка (FCS)
- Довірені шляхи та канали (FTP)

РОЗДІЛ 4. РОЗРАХУНОК КІЛЬКІСНОГО ПОКАЗНИКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

4.1 Розрахунок кількісного показника захищеності інформації від несанкціонованого доступу

Сьогодні більшість нормативних документів передбачає проведення оцінки захищеності автоматизованої системи від несанкціонованого доступу за якісним критерієм, з орієнтацією на статичні умови фунціонування систем захисту.

Для атестації АС і сертифікації засобів обчислювальної техніки відповідно до вимог чинних нормативних документів необхідні висока кваліфікація персоналу, обробка великих обсягів даних і значні витрати часу. У відомих вітчизняних та зарубіжних методик кількісного оцінювання захищеності інформації (підхід на основі аналізу інформаційних ризиків, підхід на основі моделі системи забезпечення безпеки Клементса) є ряд недоліків, що не дозволяють безпосередньо використовувати їх для оцінки захищеності, а саме:

- не враховується реальна структура АС;
- оцінюється вартість втрат від несанкціонованого доступу до інформації в грошових одиницях, що прийнятно не для всіх АС;
- не повністю враховуються варіативність сценаріїв реалізації несанкціонованого доступу (НСД) і динамічні характеристики процесу захисту інформації.

Захищеність інформації в АС від НСД визначається захищеністю її ресурсів. Для оцінки захищеності доцільно використовувати її комплексні показники, що враховують і процеси порушення безпеки ресурсів в АС, і

процеси контролю і відновлення їх захищеного стану. В якості такого показника пропонується використовувати коефіцієнт захищеності інформації АС від НСД, аналогічний використовуваному в теорії надійності коефіцієнту готовності. [12]

При наявності можливості відновлення захищеності тільки одного ресурсу для розрахунку коефіцієнта захищеності інформації від несанкціонованого доступу в АС може використовуватися наступна формула:

$$K_{зщАС} = \frac{1}{\sum_{i=0}^{N_{зр}} A_{N_{зр}}^{i} \left(\frac{\lambda_{нбi}}{\mu_{взi}} \right)^{i}}, \qquad (4.1)$$

Де $N_{зр}$ – кількість ресурсів, що підлягають захисту, $A_{N_{зр}^{i}} = \frac{N_{зр}!}{(N_{зр} - i)!}$ – кількість розміщень з $N_{зр}$ по i, $\lambda_{нб}$ – інтенсивність порушень безпеки ресурсів, $\mu_{вз}$ – інтенсивність відновлення захищеності ресурсів.

При умовно необмежених можливостях для відновлення захищеності ресурсів формула приймає наступний вигляд:

$$K_{зщАС} = \prod_{i=1}^{N_{зр}} \frac{\mu_{вз}}{\lambda_{нб} + \mu_{вз}}. \qquad (4.2)$$

Проведемо порівняльний аналіз захищеності інформації від несанкціонованого доступу на прикладі трьох АС, побудованих на основі локальних обчислювальних мереж і відрізняються масштабом і можливостями системи захисту. Кожен співробітник організації має робочу станцію, під керуванням ОС Windows, на якій знаходяться його користувацькі дані. Робочі станції об'єднані в обчислювальну мережу з декількома серверами, під керуванням ОС Windows Server, на яких функціонують поштовий сервер, СУБД, Web-сервер підприємства, миттєва система обміну повідомлень для співробітників і т. д. Нехай АС першого

підприємства має 50 критично важливих захищених ресурсів (5 загальних ресурсів, розташованих на серверах, 45 ресурсів – дані користувачів на їх робочих станціях), АС другого підприємства має 100 критично важливих ресурсів, що захищаються (10 загальних ресурсів, 90 ресурсів – дані користувачів), АС третього підприємства має 150 критично важливих ресурсів, що захищаються (15 загальних ресурсів, 135 ресурсів – дані користувачів).

У розрахунку на найгірший випадок припустимо, що порушник «ідеальний» (має високу кваліфікацію, постійно відстежує появу нових вразливостей, а також має можливість миттєво використовувати їх для здійснення несанкціонованого доступу до інформації, що обробляється в АС розглянутих організацій). При використанні такої моделі порушника інтенсивність порушень безпеки інформації АС відповідає інтенсивності появи вразливостей в програмному забезпеченні АС. Аналіз загальнодоступної статистики по виявленню вразливостей в АС на основі ОС Windows показав, що інтенсивність в середньому становить дев'ять порушень безпеки в місяць, тобто $\lambda_{нб} = 0{,}013$ / год.

Зазвичай адміністратор безпеки АС організації може в кожен момент часу відновлювати захищеність лише одного ресурсу. Тоді, використовуючи формулу (4/1), можна отримати залежність коефіцієнта захищеності інформації в АС від інтенсивності відновлення її захищеності в даних умовах, зображену на рисунку 4.1.

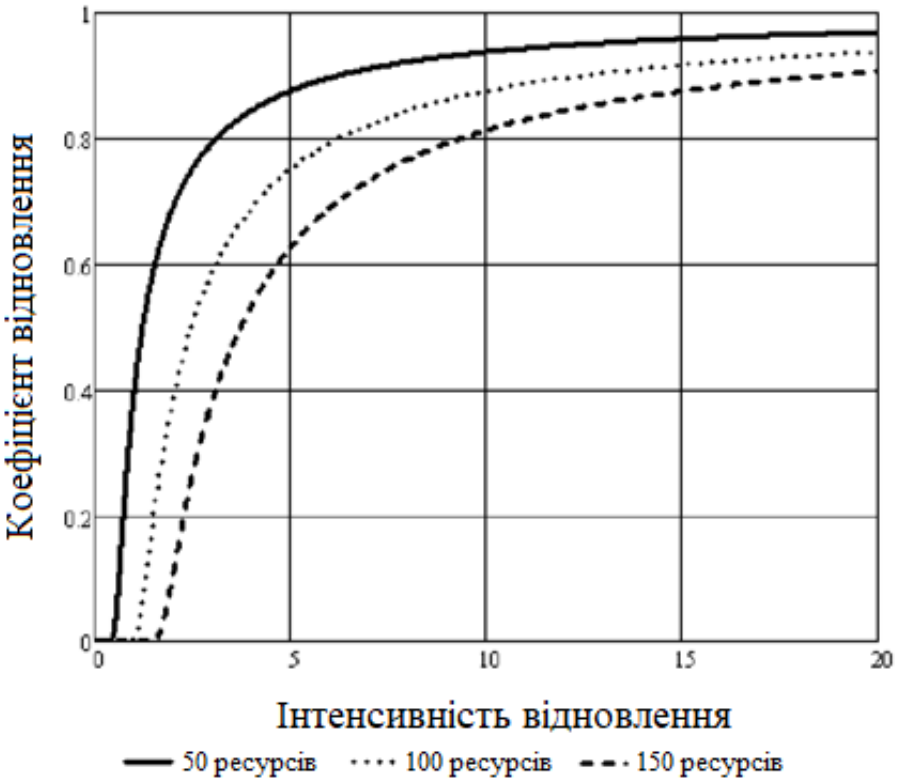

Рисунок 4.1 Залежність коефіцієнта захищеності інформації в АС від інтенсивності відновлення захищеності ресурсів при обмежених ресурсах на відновлення.

Припустимо, що в організації є практично необмежені можливості по відновленню захищеності інформації. Тоді, використовуючи формулу (4.2), можна отримати залежність коефіцієнта захищеності інформації в АС від інтенсивності відновлення захищеності ресурсів, зображену на рисунку 4.2.

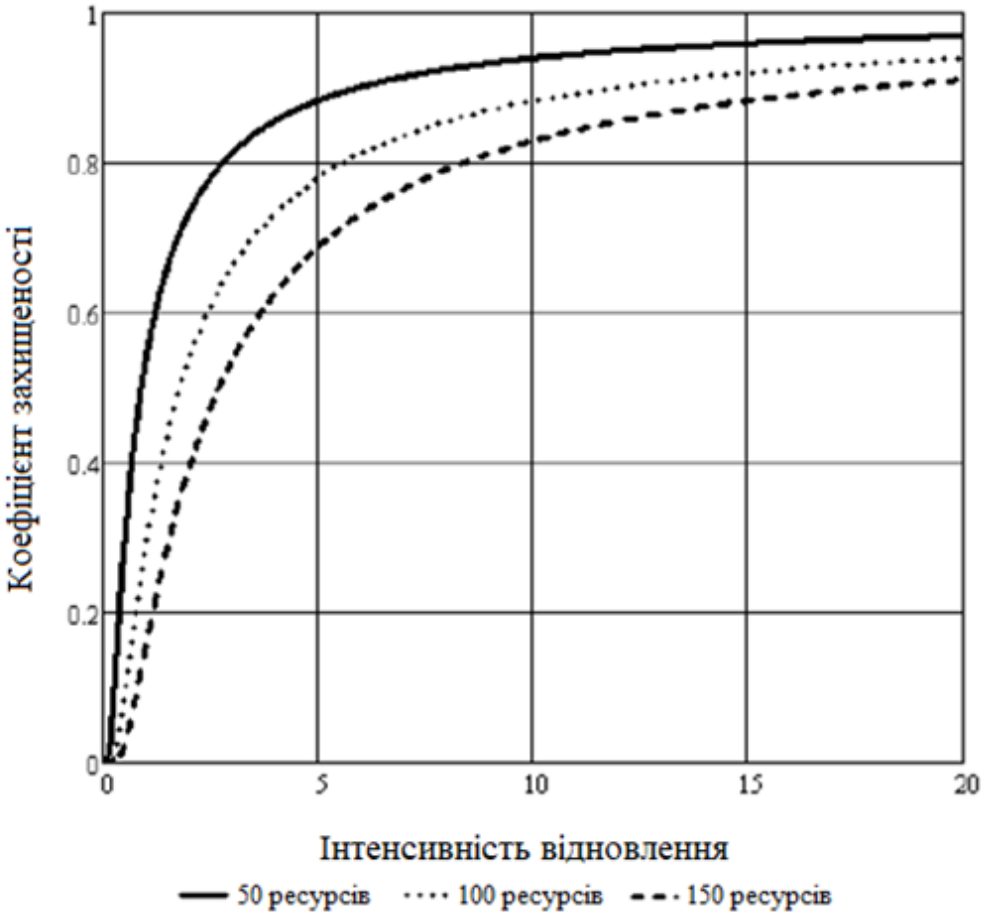

Рисунок 4.2 Залежність коефіцієнта захищеності інформації в АС від інтенсивності відновлення захищеності ресурсів при умовно необмежених ресурсах на відновлення.

З'ясуємо, яка повинна бути інтенсивність відновлення захищеності ресурсів в АС адміністратором безпеки середнього підприємства (100 ресурсів, які потребують захисту) при наступних необхідних значеннях коефіцієнта захищеності інформації від несанкціонованого доступу в АС:

$К_{зщ1АС} = 0.9$, $К_{зщ2АС} = 0.95$, $К_{зщ3АС} = 0.99$. Так як адміністратор безпеки АС реального підприємства має обмежені ресурси на відновлення захищеності інформації, то для розрахунків буде використовуватися формула (4.1). Результати розрахунків наведені на рисунку 4.3.

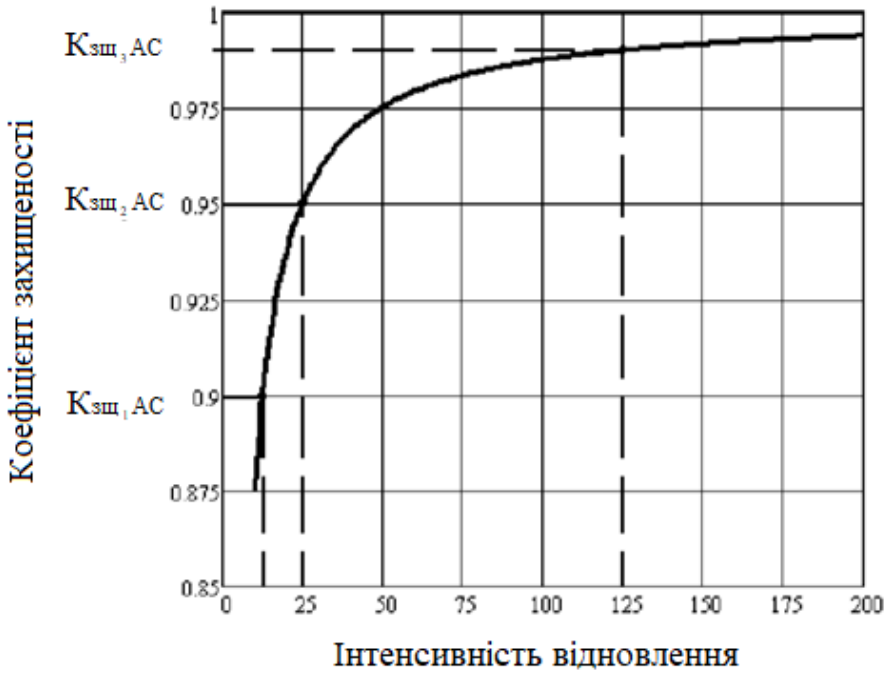

Рисунок 4.3 Інтенсивність відновлення захищеості ресурсів при $К_{зщ1АС}$ = 0.9, $К_{зщ2АС}$ = 0.95, $К_{зщ3АС}$ = 0.99

Результати розрахунку часу, необхідного для відновлення захищеності ресурсів адміністратором безпеки АС представлені в таблиці 4.1.

Таблиця 4.1 - Результати розрахунку часу на відновлення захищеності ресурсів

$К_{зщАС}$	$\mu_{вз}$, раз / год	Час необхідний на відновлення захищеності ресурсів
0.9	12.5	4.8 хв
0.95	25	2.4 хв
0.99	125	28.8 с

4.2 Висновки до розділу 4

Проаналізувавши результати розрахунків захищеності інформації в АС за критерієм придатності можна зробити наступні висновки:

- Залежність рівня захищеності інформації від несанкціонованого доступу в АС від ресурсів, що виділяються на відновлення захищеності, носить яскраво виражений нелінійний характер. Для кожної АС існує порогове значення виділених ресурсів, перевищення якого практично не призводить до підвищення рівня захищеності.
- Для забезпечення необхідного рівня захищеності необхідно використовувати додаткові і альтернативні засоби захисту.
- Без використання автоматичних засобів виявлення порушень безпеки ресурсів і відновлення захищеності ресурсів АС, здатних функціонувати в масштабі часу, близькому до реального, в умовах експлуатації буде складно досягти високий рівень захищеності.

ВИСНОВКИ

У даній роботі було проведено дослідження проблеми відповідності сучасних інформаційних систем вимогам, що встановлюються стандартами в сфері інформаційної безпеки. Було проаналізовані найвідоміші стандарти та нормативні документи, серед яких:

- “Критерій оцінки надійності комп'ютерних систем”;
- система стандартів NIST;
- ISO/IEC 15408 “Загальні критерії”;
- COBIT;
- стандарти НД ТЗІ;

Було проаналізовано основні вимоги щодо побудови систем захисту інформації, етапи їх проектування.

Досліджено вимоги до функціональних компонентів, визначених в ISO/IEC 15408, яким мають відповідати проектовані інформаційні системи, щоб забезпечувати високі показники захищеності.

Проведено визначення коефіцієнту захищеності інформаційної системи від несанкціонованого доступу при різних можливостях до відновлення ресурсів адміністратором системи та залежно від кількості ресурсів, що підлягають захисту. Після аналізу результату стало видно, що залежність коефіцієнту захищеності від інтенсивності відновлення носить нелінійний характер та кожна АС має своє порогове значення виділених ресурсів, перевищення якого практично не призведе до підвищення рівня захищеності.

СПИСОК ВИКОРИСТАНХ ДЖЕРЕЛ

1 Избачков С. Ю. Информационные системы. Учебни для вузов.2–е изд. / С. Ю. Избачков, В. Н. Петров. – СПб.: Питер, 2006. – 656 с.

2 Хорошко В.О. Основи інформаційної безпеки / В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест. – К.: ДУІКТ, 2008. – 186 с.

3 NIST SP 800-53 Revision 3

4 http://www.commoncriteriaportal.org.

5 ISO/IEC 15408–1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.

6 http://www.dsszzi.gov.ua/dsszzi/control/uk/index

7 НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

8 НД ТЗІ 3.7-003 -2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

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

10 ISO/IEC 15408–2:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components.

11 ISO/IEC 15408–3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components.

12 А.Ю. Щеглов Защита компьютерной информации от несанкционированного доступа – СПб.: Наука и Техника, 2004. – 384 с.