Міністерство освіти і науки України
Державний університет «Одеська політехніка»

Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

Батечко Сергій Вікторович,

студент групи РЗ - 161

# КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Розробка методики оцінки захищеності інформаційної системи за умовами стандартів

Спеціальність:

125 Кібербезпека

Керівник:

Лебедєва Олена Юріївна,

к.т.н., доцент

Одеса – 2021

Міністерство освіти і науки України
Державний університет «Одеська політехніка»

Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

Рівень вищої освіти другий (магістерський)
Спеціальність 125 – Кібербезпека
Освітня програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри КБПЗ

_____

д.т.н.,проф. А.А.Кобозєва
_____2021р.

**ЗАВДАННЯ**

**НА КВАЛІФІКАЦІЙНУ РОБОТУ**

*Батечку Сергію Вікторовичу*

1.Тема роботи: *Розробка методики оцінки захищеності інформаційної системи за умовами стандартів*

керівник роботи *Лебедєва Олена Юріївна, к. т. н., доцент,*

затверджені наказом ректора університету від „25” жовтня 2021 р. № 372-в.

2.Зміст роботи*: аналіз проблемної області, постановка задачі, аналіз принципів побудови методики оцінки захищеності інформаційної системи, розробка програмного продукту для оцінки захищеності інформаційної системи за умовами стандарту ISO 15408.*

3. Перелік ілюстративного матеріалу: *слайди презентації*.

5. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| Охорона праці | Ярова І.А. | Завдання видав | Завдання прийняв |
| | | | |

6. Дата видачі завдання "_____"_____20___ р.

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання | Примітка |
|---|---|---|---|
| *1* | *Аналіз джерел з теми випускної кваліфікаційної роботи* | *15-07-2021* | *виконано* |
| *2* | *Обґрунтування вибору рішення. Збір даних* | *15-08-2021* | *виконано* |
| *3* | *Аналіз та вибір стандарту для оцінки захищеності* | *11-09-2021* | *виконано* |
| *4* | *Аналіз структури стандарту ISO 15408 та побудови методики оцінки захищеності інформаційної системи* | *22-10-2021* | *виконано* |
| *5* | *Розробка програмного продукту для оцінки захищеності інформаційної систем* | *15-11-2021* | *виконано* |
| *6* | *Підготовка тексту роботи* | *26-11-2021* | *виконано* |
| *7* | *Підготовка презентації та доповіді* | *01-12-2021* | *виконано* |
| *8* | *Попередній захист* | *03-12-2021* | *виконано* |
| *9* | *Нормоконтроль, рецензування* | *03-12-2021* | *виконано* |
| *10* | *Занесення роботи в електронний архів* | *18-12-2021* | *виконано* |
| *11* | *Допуск до захисту* | *20-12-2021* | *виконано* |

**Здобувач вищої освіти** _____ *Батечко С.В.*

**Керівник роботи** _____ *Лебедєва О.Ю.*

**ЗАВДАННЯ**

на розробку розділу «Охорона праці та безпека в надзвичайних ситуаціях»

Батечка Сергія Вікторовича

Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій

Кафедра кібербезпеки та програмного забезпечення

Тема роботи: Розробка методики оцінки захищеності інформаційної системи за умовами стандартів.

Зміст розділу:

1. Аналіз умов праці і вибір заходів і засобів захисту від небезпечних і шкідливих виробничих факторів.
2. Аналіз техногенних небезпек і вибір заходів і засобів забезпечення безпеки у надзвичайних ситуаціях.
3. Дослідження працездатності спеціаліста з інформаційної безпеки.

Керівник роботи
к.т.н., доцент Лебедєва О.Ю.

_____
(підпис)

« __ » _____2021 р.

Консультант з охорони праці та БНС
к.т.н., доцент Ярова І.А.

_____
(підпис)

« __ » _____2021 р.

# АНОТАЦІЯ

Кваліфікаційна робота на тему “Розробка методики оцінки захищеності інформаційної системи за умовами стандартів” на здобуття другого (магістрського) рівня вищої освіти за спеціальністю 125 – Кібербезпека спеціалізація, освітня програма: кібербезпека містить 40 рисунків, 9 таблиць, 42 літературних джерела за переліком посилань. Робота виконана на 94 сторінках тексту.

*Метою* дипломної роботи є розробка методики оцінки захищеності інформаційної системи шляхом використання стандарту ISO 15408.

*Об’єктом дослідження* роботи є оцінка захищеності інформаційної системи.

*Предметом дослідження* є стандарти для оцінки захищеності інформаційної системи.

На основі стандарту ISO 15408 було розроблено методику оцінки захищеності інформаційної системи. Було розроблено програмний додаток, який реалізує розроблену методику оцінки захищеності інформаційної системи. Запропонований додаток має зручний інтерфейс, за допомогою якого користувач може знайти потрібний клас вимог безпеки, потрібний компонент і поставити відмітку виконання конкретної вимоги захисту інформаційної системи згідно зі стандартом.

*Ключові слова*: стандарт, методологія, інформаційна система, ISO 15408, клас, додаток, оцінка захищеності, управління ризиками, вимога.

# SUMMARY

Qualification work "Development of methods for assessing the security of information systems in terms of standards" for the second (master's) level of higher education in specialty 125 – Cybersecurity specialization, educational program: cybersecurity contains 40 figures, 9 tables, 42 literature sources on the list of references. The work is performed on 94 text pages.

The *aim* of the thesis is to develop a methodology for assessing the security of the information system using the ISO 15408 standard.

The *object* of the study is to assess the security of the information system.

The *subject* of the study is the standards for assessing the security of the information system.

Based on the ISO 15408 standard, a methodology for assessing the security of the information system was developed. A software application was developed that implements the developed methodology for assessing the security of the information system. The proposed application has a user-friendly interface through which the user can find the desired class of security requirements, the desired element and mark the implementation of a specific requirement for the protection of information systems in accordance with the standard.

*Keywords*: standard, methodology, information system, ISO 15408, class, application, security assessment, risk management, requirement.

ЗМІСТ

ВСТУП ..... 8
1 ОГЛЯД ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ..... 11
1.1 Інформаційна система та важливість її захисту. ..... 11
1.2 Аналіз загроз безпеки та їх класифікація. ..... 12
1.3 Найвідоміші стандарти безпеки та найкращі практики захисту інформації і сфери їх застосування. ..... 16
1.4 Готові програмні рішення для оцінки захищеності. ..... 19
2 РОЗРОБКА МЕТОДИКИ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ..... 37
2.1 Політики безпеки та основні принципи запобігання порушення безпеки. ..... 37
2.2 Стандартизація у сфері інформаційної безпеки. ..... 47
2.3 Стандарт ISO/IEC 15408. ..... 48
2.4 Методика оцінки захищеності інформаційних систем. ..... 57
3 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ..... 60
3.1 Мова програмування C#. ..... 60
3.2 Опис роботи розробленого програмного забезпечення ..... 64
3.3 Структура XML-файлів. ..... 70
4 ОХОРОНА ПРАЦІ І БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ ..... 73
ВИСНОВКИ ..... 89
ПЕРЕЛІК ПОСИЛАНЬ ..... 90
ДОДАТОК А. Таблиці залежностей сімейств класів в стандарті ISO/IEC 15408 ..... 94

# ВСТУП

На сьогоднішній день інформаційна безпека підприємства – один з провідних факторів його ефективного розвитку. Інформація має реальну вартісну вагу, яка чітко визначається прибутком, що отримується при її використанні, або шкодою, яку може бути завдано підприємству у разі використання її іншими особами.

Постійно зростає частка витрат організацій на забезпечення цілісності інформації та захисту її від можливих зовнішніх загроз. Проте підприємства не хочуть викидати гроші на вітер. Вони хочуть купувати тільки те, що справді необхідно для побудови надійної системи захисту інформації і при цьому з мінімальними витратами.

У зв'язку з цим гостро постає питання оцінки ефективності засобів захисту та оцінки захищеності всієї інформаційної системи в цілому. Зробивши таку оцінку, можна вибрати найбільш ефективну систему захисту як із функціонального, так і з економічного погляду у кожному конкретному випадку.

Ефективність роботи будь-якого підприємства безпосередньо залежить від захищеності його інформаційних ресурсів та безпеки всіх суб'єктів, що беруть участь у процесі виробництва та використовують ці ресурси. Вирішення цієї проблеми лише шляхом посилення рівня захищеності ресурсів не дозволяє досягти результату, що відповідає вимогам сучасного суспільства.

Побудова методики оцінки інформаційної безпеки, що забезпечує виконання таких вимог, можлива лише з використанням системного підходу для обліку всіх взаємопов'язаних факторів, що мають значення для вирішення проблеми безпеки об'єктів та суб'єктів підприємства, включаючи оцінки ризиків, економічну ефективність та ін.

Одним із найважливіших кроків посилення безпеки підприємства є привернення уваги людей до питань безпеки, усвідомлення співробітниками всієї серйозності проблеми та прийняття політики безпеки організації, вивчення та впровадження необхідних методів та дій для підвищення захисту інформаційного

забезпечення. Поінформованість має бути включена до всіх рівнів організації, починаючи з самого верхнього, де приймається політика безпеки. На основі цієї політики та розподілу відповідальності створюється модель оцінки захищеності інформаційної системи підприємства, тому тема роботи є актуальною.

*Метою* дипломної роботи є розробка методики оцінки захищеності інформаційної системи шляхом використання стандарту ISO 15408.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– Проаналізувати стан сучасних розробок в області оцінки захищеності;
– Провести аналіз сучасних стандартів безпеки;
– Розробити методику оцінки захищеності інформаційної системи;
– Розробити програмний продукт, який реалізує розроблену методику оцінки захищеності інформаційної системи.

*Об'єкт дослідження* – оцінка оцінки захищеності інформаційної системи.

*Предмет дослідження* – стандарти та методи для оцінки захищеності інформаційної системи.

Наукова новизна одержаних результатів полягає в наступному.

Було розроблено методику оцінки захищеності інформаційної системи шляхом використання стандарту ISO 15408. За результатами відповідей експертів наводиться оцінка захищеності інформаційної системи.

Практичне значення отриманих результатів. Практична цінність роботи полягає в розробці та реалізації методики оцінки захищеності інформаційної системи у вигляді програмного додатку зі зручним інтерфейсом. Розроблена методика може бути використаний як самостійний інструмент для оцінки захищеності інформаційних систем так і як складова частина комплексних систем оцінки.

У вступі обумовлена актуальність теми, сформульована мета, задачі, об'єкт та предмет досліджень.

В першому розділі була розглянута інформаційна система та важливість її захисту, розглянуті загрози безпеки та їх класифікація, найвідоміші стандарти безпеки та найкращі практики захисту інформації і сфери їх застосування, а також

існуючі програмні засоби які дозволяють вирішувати завдання оцінки захищеності інформаційної системи.

В другому розділі розглянуті політики безпеки та основні принципи запобігання порушення безпеки, розглянута тема стандартизації у сфері інформаційної безпеки та стандарт ISO/IEC 15408, також була розглянута методика оцінки захищеності інформаційних систем.

В третьому розділі розглянуто мову програмування C# як основний інструмент розробки додатків, було описано роботу розробленого програмного забезпечення, розглянуто структуру файлів XML.

В четвертому розділі проведено аналіз умов праці і вибір заходів і засобів захисту від небезпечних і шкідливих виробничих факторів, аналіз техногенних небезпек і вибір заходів і засобів забезпечення безпеки у надзвичайних ситуаціях, було досліджено працездатність спеціаліста з інформаційної безпеки.

В висновках описується отримані результати роботи.

# 1 ОГЛЯД ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

## 1.1 Інформаційна система та важливість її захисту.

Інформаційна система – інтегрований набір компонентів для збору, зберігання та обробки даних, а також для надання інформації, знань та цифрових продуктів. Бізнес-фірми та інші організації покладаються на інформаційні системи для здійснення та управління своїми операціями, взаємодії зі своїми клієнтами та постачальниками та конкуренції на ринку. Інформаційні системи використовуються для запуску міжорганізаційних ланцюгів поставок та електронних ринків. Наприклад, корпорації використовують інформаційні системи для обробки фінансових рахунків, управління людськими ресурсами та охоплення потенційних клієнтів за допомогою онлайн-реклами[1].

Багато великих компаній повністю побудовані навколо інформаційних систем. До них відноситься eBay, переважно аукціонний ринок; Amazon, електронний торговий центр, що розширюється, і постачальник послуг хмарних обчислень; Alibaba, електронний ринок для бізнесу; і Google, пошукова компанія, яка отримує більшу частину свого доходу від реклами за ключовими словами в Інтернеті.

Уряди впроваджують інформаційні системи для економічного надання послуг громадянам. Цифрові товари, такі як електронні книги, відеопродукти та програмне забезпечення, та онлайн-послуги, такі як ігри та соціальні мережі, постачаються разом із інформаційними системами. Люди покладаються на інформаційні системи, як правило, засновані на Інтернеті, для ведення більшої частини свого особистого життя: для спілкування, навчання, покупок, банківських послуг та розваг.

Сучасне суспільство зацікавлене у широкій доступності інформації з метою прискорення науково-технічного прогресу. У ринковій економіці інформація є товаром, та її отримання, зберігання, передача та використання повинні підпорядковуватися законам товарно-грошових відносин. Побудова економічно-

ефективної системи інформаційної безпеки безпосередньо залежить від того, наскільки точно проведена оцінка вартості захищеної інформації.

Можливі втрати від витоку інформації призводять до конкретної величини економічної шкоди. Витрати на захист такої інформації мають бути економічно обмежені сумою можливих втрат. Це зумовлено тим, що , наприклад, при зайвому засекречуванні комерційної інформації зростання витрат на дані цілі не є адекватним відносно зниження ймовірності витоку цінніших відомостей. Тому недоцільно охороняти як комерційну таємницю лише частину інформації підприємства, пов'язану з виробничим процесом.

## 1.2 Аналіз загроз безпеки та їх класифікація.

Інформаційні системи часто піддаються різним видам загроз, які можуть спричинити різні типи збитків, що може призвести до значних фінансових втрат.

Збитки інформаційної безпеки можуть варіюватися від невеликих втрат до повних руйнування інформаційної системи. Наслідки різних загроз значно відрізняються: деякі впливають на конфіденційність або цілісність даних, а інші впливають на доступність системи. Зараз організаціям важко зрозуміти які загрози є небезпечними для їх інформаційних активів і як отримати необхідні засоби для боротьби з ними[3].

У різних дослідженнях називаються системні проблеми безпеки інформаційних систем:

- маніпулювання доступом у внутрішній інформаційний простір;
- крадіжка інформації з корпоративних мереж і баз даних;
- зміна інформації, фальсифікація документів в електронному вигляді;
- промислове стеження;
- крадіжка засобів з банківських рахунків;
- вірусні загрози.

Деякі дослідження пропонують дещо глибшу класифікацію.

Список критеріїв класифікації:

- Джерело загрози безпеці: походження загрози внутрішнє або зовнішнє.
- Агенти загроз безпеки: агенти, які викликають загрози; виділено три основні класи: людські, екологічні і технологічні.
- Мотивація загрози безпеці: плани зловмисників на систему, які можуть бути зловмисними або нешкідливими.
- Намір загрози безпеці: намір людини, яка спричинила загрозу, навмисна або випадкова. Цей критерій дозволяє реконструювати поведінку атаки та повну шкідливу поведінку, щоб зрозуміти наміри зловмисника. Це є передбачуваним фактором, який допомагає слідчим завершити справу з високою точністю і, отже, зменшити ризики і допомогти прискорити прийняття рішень для відлову зловмисника.
- Вплив загроз: вплив загроз – це порушення безпеки, яке виникає внаслідок дії загрози. Визначено наступні впливи загроз: знищення інформації, пошкодження інформації, крадіжка/втрата інформації, розкриття інформації, відмова у використанні, підвищення привілеїв та незаконне використання.

Загроза може бути викликана внутрішніми, зовнішніми або як зовнішніми, так і внутрішніми суб'єктами.

Внутрішні загрози виникають, коли хтось має авторизований доступ до мережі за допомогою облікового запису на сервері або фізичний доступ до мережі. Загроза може бути внутрішньою для організації в результаті дій або невдач співробітників організаційного процесу.

Зовнішні загрози можуть виникати від окремих осіб або організацій, які працюють за межами компанії. Вони не мають авторизований доступ до комп'ютерних систем або мережі. Найбільш очевидні зовнішні загрози для комп'ютерних систем і резидентні дані – це стихійні лиха: урагани, пожежі, повені та землетруси. Зовнішні атаки відбуваються через підключені мережі (провідні та бездротові), фізичне вторгнення або партнерську мережу.

Агент загрози – це дійова особа або об’єкт/явище, яка створює загрозу системі. Є три класи для цієї класифікації: люди, стихійні лиха та технологічні

загрози. Запропонована класифікація охоплює повний набір потенційних агентів, оскільки ми включаємо людей, хімічні та фізичні реакції та створені людиною об'єкти (технологічні), і, природні, на які люди не мають жодного впливу.

Людські загрози – цей клас включає загрози, викликані діями людини, такими як інсайдери або хакери, які завдають шкоди або ризику в системах.

Наступний клас – фактори навколишнього середовища. Екологічні загрози – це загрози, викликані нелюдськими агентами. Це походить, по-перше, від загроз стихійного лиха, як землетруси, повені, пожежі, блискавки, вітер або вода, а також через тварин і дику природу, які завдають серйозної шкоди до інформаційних систем, таких як повені, блискавки, припливні хвилі (наприклад, цунамі) і пожежа. Також цей клас включає інші загрози, такі як заворушення, війни та терористичні атаки.

Технологічні загрози викликані фізико-хімічними процесами на матеріалі. До фізичних процесів належать використання фізичних засобів для проникнення в заборонені зони, такі як будівля, приміщення або будь-які інші призначені місця таких як крадіжка або пошкодження апаратного та програмного забезпечення. Однак хімічні процеси включають апаратні та програмні засоби технології. Він також включає обладнання для непрямої підтримки системи, наприклад джерела живлення.

Зловмисники зазвичай мають конкретну мету або мотив для атаки на систему. Ці цілі можуть викликати зловмисне або нешкідливі результати. Шкідливі загрози полягають у внутрішніх або зовнішніх атаках, спричинених працівниками чи непрацівниками, щоб заподіяти шкоду та пошкодити організація на кшталт вірусів, троянських коней або хробаків. Незловмисні атаки відбуваються через погані політики безпеки та засоби контролю, які дозволяють уразливості та помилки відбуватися. Це викликано необізнаними працівниками з метою не нашкодити системі.

Намір загрози представляє намір людини, яка спричинила загрозу:

– Навмисні загрози: це загрози, які є результатом шкідливого рішення. Наприклад, комп'ютерні злочини, або коли хтось навмисно завдає шкоди

майну чи інформації. Комп’ютерні злочини включають шпигунство, крадіжку особистих даних, дитяча порнографія та злочинність кредитних карток.

– Ненавмисні загрози: це загрози, які вводяться без усвідомлення. Ці загрози в основному включають несанкціонована або випадкова модифікація програмного забезпечення. Випадкова помилка включає пошкодження даних, викликане помилка програмування, помилка користувача або оператора.

Впливи загрози. Загроза безпеці може спричинити один або кілька шкідливих впливів на системи, на які вони поділяються. Їх є сім видів:

1) знищення інформації,
2) пошкодження інформації,
3) крадіжка або втрата інформації,
4) розкриття інформації,
5) відмова у використанні,
6) підвищення привілеїв,
7) незаконне використання.

Знищення інформації: навмисне знищення компонента системи для переривання роботи системи.

Пошкодження інформації – це будь-яка несанкціонована зміна файлів, що зберігаються на хост-комп'ютері, або даних, що передаються через мережу. Це також називається фальсифікацією інформації, до якої входять: додавання, видалення або зміна системи пам’яті, жорстких дисків та інших частин. Також сюди можна віднести імплантацію трояна, що призведе до змін, збільшення жорсткого диска, файлу, файлоподібне вірусне вторгнення, що призведе до відповідних змін у файлі.

Розкриття інформації – це розповсюдження інформації всім, хто не має до неї доступу. Ці загрози можуть спричинити несанкціоноване розкриття, перехоплення, вторгнення.

Крадіжка інформаціїї – це несанкціоноване використання комп'ютерних або мережевих служб без погіршення якості служби для інших користувачів. Крадіжка може статись через: крадіжку послуг, крадіжку функціональних можливостей, крадіжку даних, програмного та/або апаратного забезпечення, неправильне використання, зловживання даними.

Відмова в обслуговуванні – навмисне погіршення або блокування комп'ютерних або мережевих ресурсів.

Підвищення привілеїв – використання деяких засобів або використання слабких місць у системі; отримання дозволу на доступ до цільової системи.

Незаконне використання – використання звичайного функціоналу системи для зловмисних дій або інших цілей. Наприклад, зловмисник використовує звичайне мережеве підключення для атаки на інші системи, використовуючи вразливості звичайні системні служби для досягнення цілей зловмисника.

## 1.3 Найвідоміші стандарти безпеки та найкращі практики захисту інформації і сфери їх застосування.

Сімейство систем управління інформаційною безпекою ISO/IEC 27000 – цей документ надає огляд ISO/IEC 27000 сімейства систем управління інформаційною безпекою, який складається з взаємопов’язаних стандартів і рекомендацій, які вже опубліковані або знаходяться в стадії розробки, і містить ряд важливих структурних компоненти.

ISO/IEC 27001 – цей документ містить стандарти ISO щодо вимог щодо створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою в контексті організації. Стандарт ISO/IEC 27001 є першим загальновизнаним міжнародним стандартом системи управління інформаційною безпекою. Від багатьох інших стандартів у галузі захисту інформації його відрізняє те, що він може застосовуватись у будь-якій організації незалежно від роду її діяльності. Міжнародний стандарт інформаційної безпеки ISO 27001 описує будівництво системи інформаційної безпеки на підприємстві.

Загалом стандарт ISO 27001 – це опис вимог до системи управління інформаційною безпекою. Особливістю ISO 27001 є те, що він висуває вимоги не так до технічних засобів захисту, як до системи управління інформаційною безпекою. Це є головною особливістю стандарту і замовник повинен розуміти, що впровадження навіть невеликої частини вимог позначиться насамперед на процесах, а не технічному засобі. Область застосування стандарту ISO/IEC 27001 відрізняється від інших стандартів ІБ. Оскільки прибуток в організації приносить успішно функціонуючий бізнес-процес, то й захищає ISO 27001 також бізнес-процес в організації. Необхідно відзначити, що весь стандарт має на меті не досягнення певного рівня безпеки заради безпеки, а використання адекватних заходів захисту активів компанії, заснованому на критичності бізнесу компанії, тобто підвищення якості ІБ організації, що обов'язково призведе до підвищення якості ІС.

Недоліки ISO 27001:

1) відсутність чітких вказівок щодо документування системи управління інформаційною безпекою (немає загального переліку документів, ні інструкцій щодо його формування, ні вимог до змісту документів). Це спричиняє значні труднощі при запровадженні системи управління інформаційною безпекою, тому що думки про те, скільки має бути документів, якими вони мають бути, що треба, а що не треба документувати та як це робити, можуть сильно розходитися;
2) стандарт не визначає чіткої межі між системою управління інформаційною безпекою та системою забезпечення інформаційної безпеки, технічними та організаційними механізмами контролю. В результаті багато хто розглядає систему управління інформаційною безпекою як чисто організаційну складову системи забезпечення інформаційної безпеки, незважаючи на те, що в стандарті описуються обидва класи контролю, які, практично, неспроможні один без одного існувати;

3) не регламентовано, на відповідність яким критеріям/технічним стандартам потрібно перевіряти налаштування систем безпеки.

Всі перераховані вище недоліки при їх розгляді з іншого точки зору, є перевагами, тому що не накладають будь-які обмеження на вибрані дії виконавця.

ISO/IEC 27002 – Цей документ вводить кодекс практики для контролю інформаційної безпеки.

ISO/IEC 27017 – цей документ містить рекомендації, що підтримують впровадження засобів контролю інформаційної безпеки для споживачів і постачальників хмарних послуг. Вибір відповідних засобів контролю та застосування рекомендацій щодо впровадження базуються на оцінці ризиків та інших вимогах до використання хмарних сервісів.

Стандарт ISO/IEC 13355 – це посібник з управління безпекою інформаційних та телекомунікаційних технологій, встановлює концепцію та моделі, що лежать в основі базового розуміння безпеки, і розкриває загальні питання управління, які важливі для успішного планування, реалізації та підтримки безпеки. Метою цього стандарту є формування загальних понять та моделей управління безпекою. Наведені в ньому положення носять загальний характер і застосовуються до різних методів управління та організаціям. Цей стандарт розроблений так, що дозволяє пристосовувати його положення до потреб організації та властивого їй стилю управління.

Британський стандарт (BS) 7799, частина 3 – цей набір рекомендацій опубліковано BSI Group для управління ризиками інформаційної безпеки.

COBIT – цілі контролю для інформаційних та пов’язаних із ними технологій (COBIT) публікує Рада зі стандартів Асоціації аудиту та контролю інформаційних систем (ISACA), що забезпечує структуру контролю для управління та управління IT підприємства.

Загальні критерії (також відомі як ISO/IEC 15408) – це набір критеріїв оцінки розроблено та узгоджено з національними організаціями стандартів безпеки Австралії, Канади, Франції, Німеччини, Японії, Нідерландів, Нової Зеландії, Іспанії, Великобританії та США.

ITIL (або серія ISO/IEC 20000) – у цьому документі представлено набір найкращих практик з управління IT-послугами (ITSM), зосереджено на процесах обслуговування IT та розглядає центральну роль користувача.

Специфікація національних стандартів інформаційної безпеки – на цій веб-сторінці представлено набір національних стандартів інформаційної безпеки, сформульованих Технічним комітетом зі стандартів національної безпеки інформації. Ці стандарти включають управління інформаційною безпекою, оцінку інформаційної безпеки, аутентифікацію та авторизацію тощо.

Центр контролю безпеки в Інтернеті (CIS) (раніше відомий як Critical Security Controls) – це пріоритетний набір засобів захисту для пом’якшення найбільш поширених кібератак на системи та мережі. Вони зіставлені з різними правовими, нормативними та політичними рамками та посилаються на них.

## 1.4 Готові програмні рішення для оцінки захищеності.

На ринку існують готові програмні рішення для оцінки захищеності інформаційних систем. Усі вони розробляються на основі стандартів. Давайте розглянемо деякі з них.

Першим будемо розглядати додаток під назвою CRAMM.

Для кращого розуміння даного додатку необхідно ввести поняття стандарту BS 7799.

BS 7799 – стандарт , спочатку опублікований BSI Group (BSI) у 1995 році. Він був написаний Департаментом торгівлі та промисловості Уряду Сполученого Королівства і складається з кількох частин.

Оригінальний стандарт BS 7799 був розділений на дві частини:

Частина 1 була кодексом практики з управління інформаційною безпекою і включала низку потенційних засобів контролю, які, якщо вони є та працюють, забезпечать офіційно керовану інформаційну безпеку. Частина 1 була «супермаркетом» засобів контролю, деякі з яких були б доречними, інші – ні, залежно від бізнесу.

Частина 2 – це специфікація для введення в дію системи управління інформаційною безпекою (СУІБ). Так само, як ви можете керувати брандмауером, таким чином ви можете керувати загальною безпекою інформації.

У 2000 році частина 1 стала стандартом ISO. Зміст залишився в основному кодексом практики, але, звісно, неможливо бути сертифікованим відповідно до кодексу практики.

Частина 2 залишилася британським стандартом, і організації можуть бути сертифіковані на нього. Сертифікація доводить всім зацікавленим особам, що організація керує своєю інформаційною безпекою.

На основі методології оцінки ризиків уряду Великобританії, CRAMM був повністю перероблений компанією Insight Consulting, щоб перетворитися на повний інструментарій інформаційної безпеки, який включає:

- комплексний інструмент оцінки ризиків, який повністю відповідає стандартам BS7799 та ISO 17799;
- ряд допоміжних інструментів для підтримки інформаційної безпеки менеджери для планування та керування безпекою Майстри для швидкого створення проформальних політик інформаційної безпеки та іншої відповідної документації Інструменти, які підтримують ключові процеси в управлінні безперервністю бізнесу
- базу даних із понад 3000 засобів контролю безпеки, які посилаються на відповідні ризики та ранжуються за ефективністю та вартістю Основні інструменти для допомогти отримати сертифікацію або відповідність стандарту BS7799.

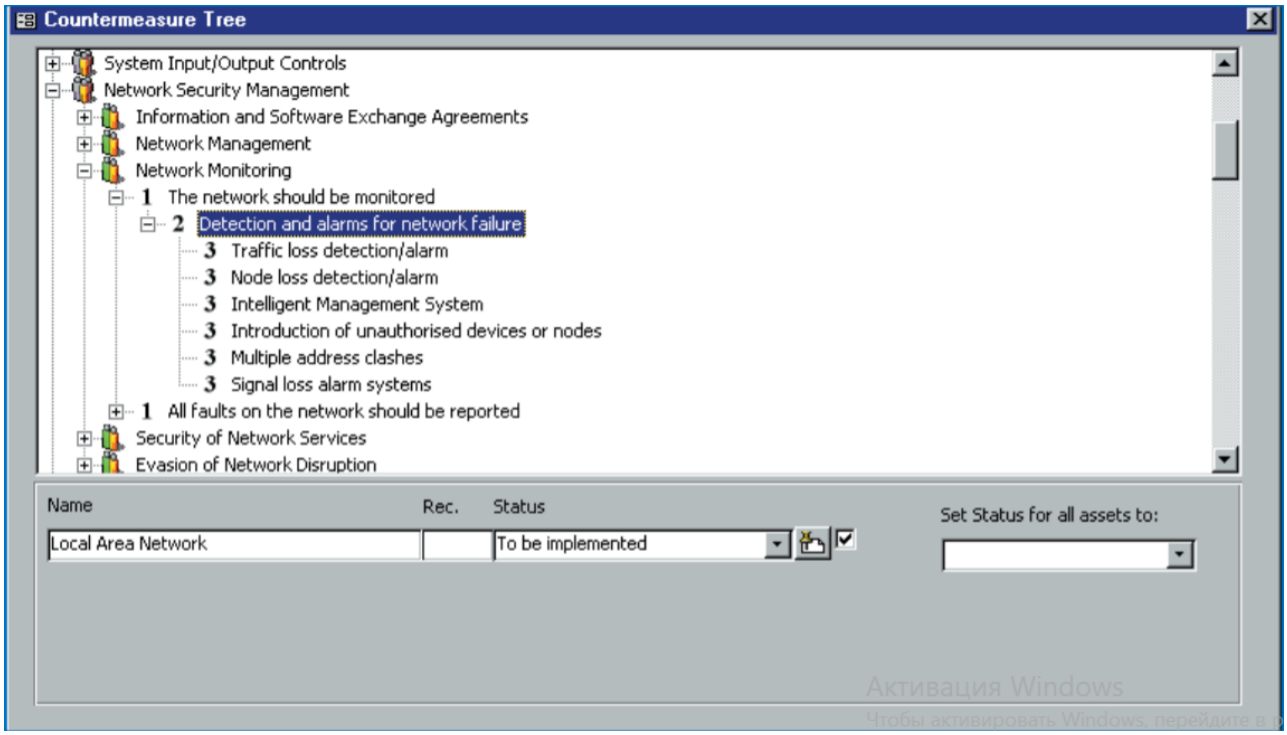


Рисунок 1.1 – Дерево контрзаходів, що ілюструє ієрархічну структуру бази даних елементів керування CRAMM

Користувачі можуть переглядати базу даних елементів керування, щоб визначити елементи керування, які можуть мати значення для їхнього бізнесу та додатків, а потім досліджувати їх із зростаючим рівнем деталізації. Крім того, інструменти оцінки ризику CRAMM можуть бути використані для визначення того, чи потрібні засоби контролю та чи можуть бути виправдані, на основі оцінених ризиків.

База даних контролю CRAMM регулярно оновлюється, щоб підтримувати її у відповідності з швидкими розвитками процесів, стандартів і технологій інформаційної безпеки.

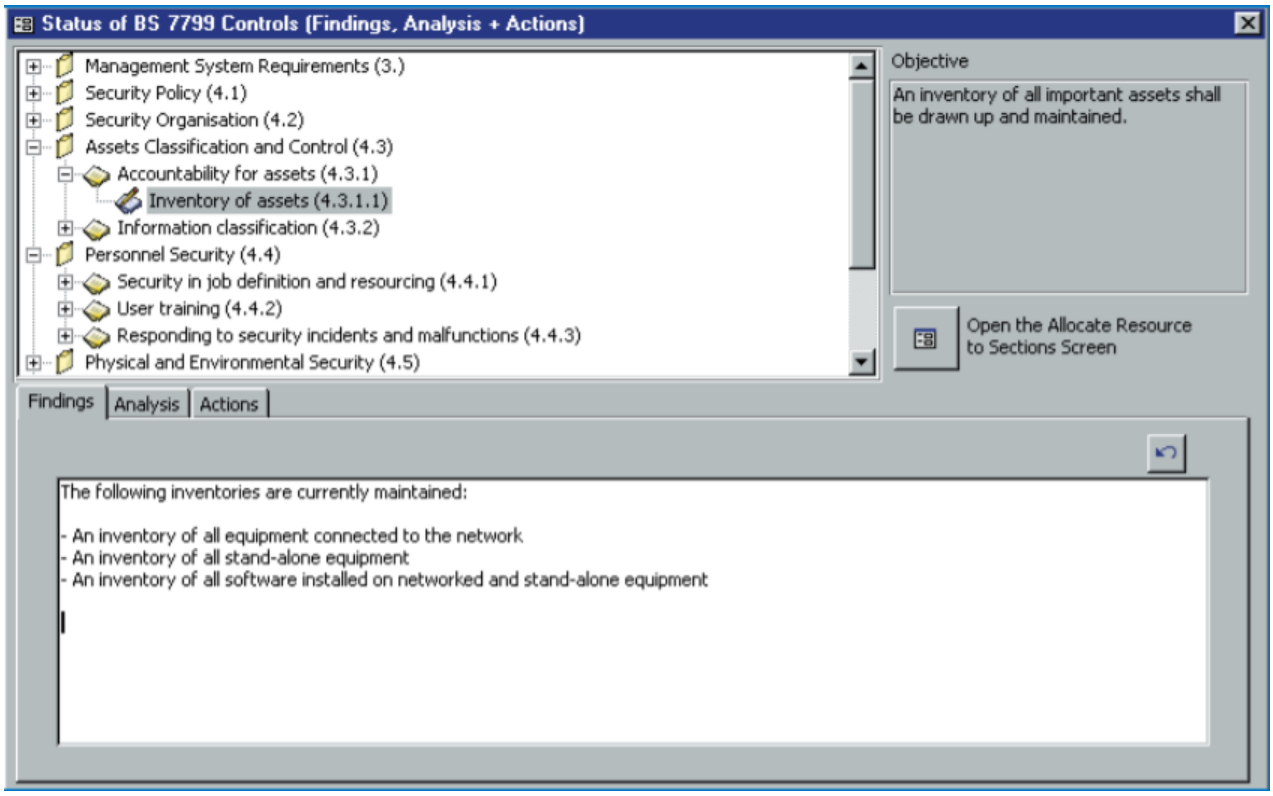


Рисунок 1.2 – Екран  для запису результатів аналізу прогалин

Інструменти оцінки ризиків CRAMM можна використовувати, щоб відповісти на окремі запитання, подивитися на організації, процеси, додатки чи системи, або для дослідження цілісної інфраструктури цілих організації. Користувачі мають на вибір інструмент швидкої оцінки ризику або повний, більш суворий аналіз.

Інструменти оцінки ризиків надзвичайно гнучкі, що дозволяють досліджувати різні проблеми та відповісти на багато різних питань.

Нижче наведені приклади застосування інструментів оцінки ризиків CRAMM:

- визначити, чи є вимоги до конкретних засобів контролю, наприклад, надійна аутентифікація, шифрування, захист живлення або апаратне резервування;
- визначити функціональні можливості безпеки, необхідні для нової програми;
- допомогти в розробці вимог безпеки для угоди про аутсорсинг/керовану послугу;

– переглянути вимоги до фізичної та екологічної безпеки на новому місці;
– вивчити наслідки дозволу користувачам підключатися до Інтернету;
– продемонструвати відповідність законодавству, такому як “Закон про захист даних”, який вимагає забезпечення належної безпеки;
– розробити політику безпеки для нової системи;
– провести аудит придатності та стану засобів контролю безпеки в існуючій системі.

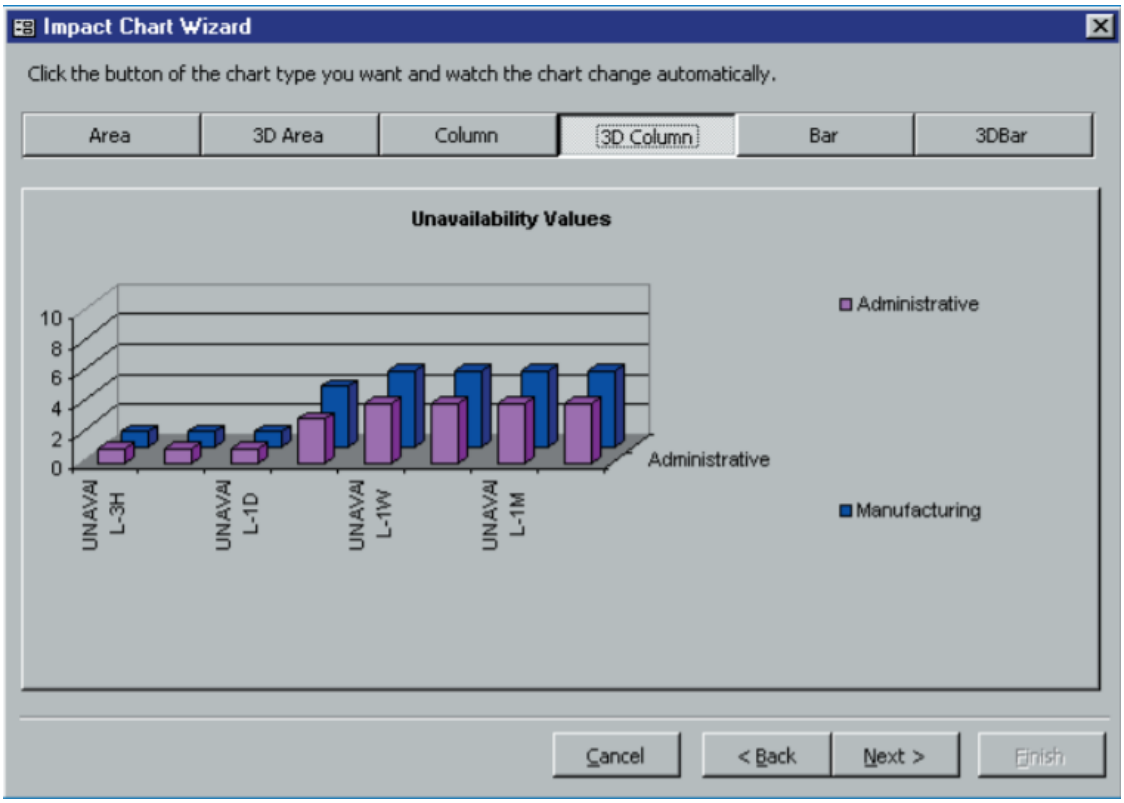


Рисунок 1.3 – Графічний звіт аналізу впливу на бізнес

CRAMM містить різноманітні інструменти, які допомагають оцінити результати оцінки ризику, в тому числі:

– визначити відносного пріоритету контролю;
– записати розрахункові витрати на впровадження контролю;
– моделювати зміни до оцінки ризику з використанням розрахунків «що, якщо?»;

– відстежувати через оцінку ризику, щоб показати обґрунтування конкретних засобів контролю.

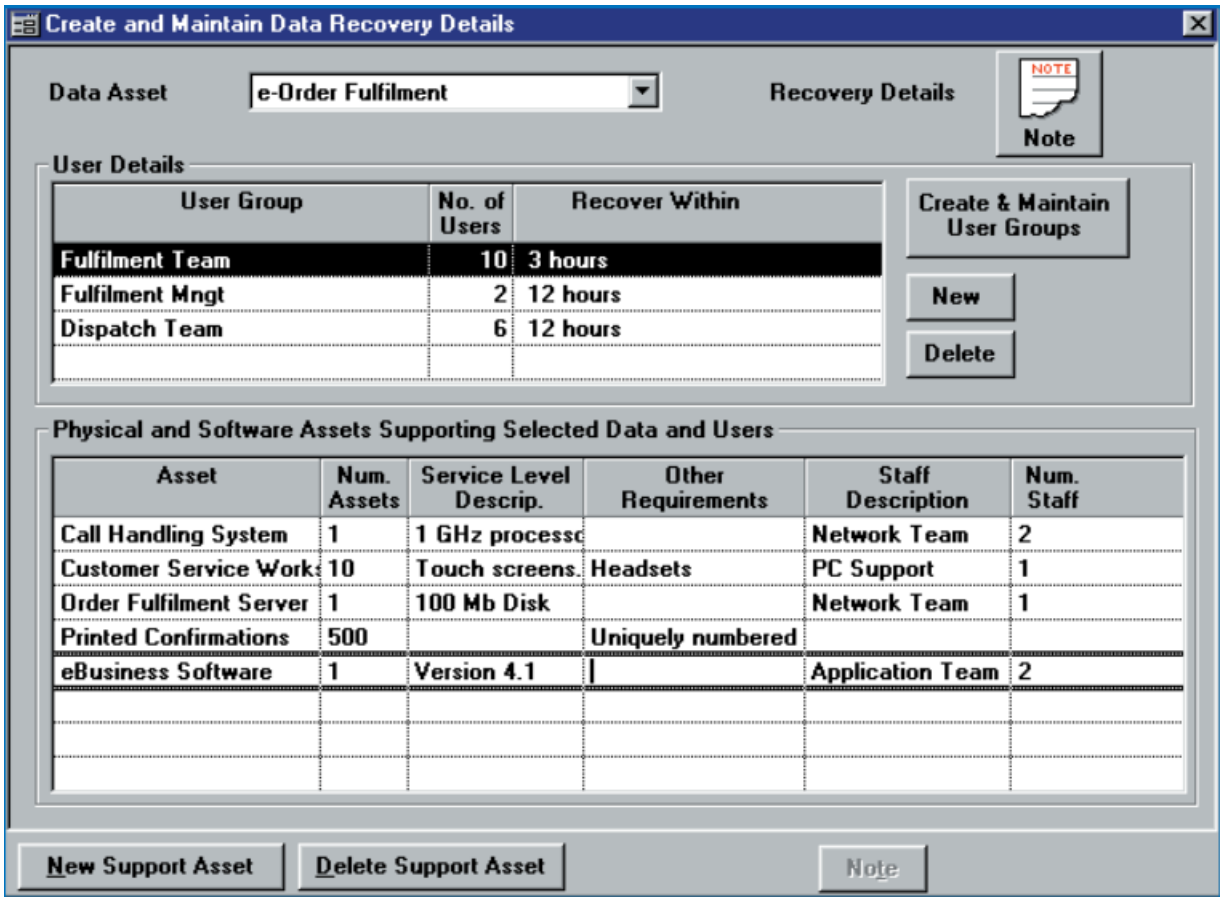


Рисунок 1.4 – Екран для запису вимог безперервності

Іншим популярним рішенням для оцінки захищеності інформаційної системи є COBRA.

Першою метою цього продукту є допомога та підтримка організації який запроваджує критерії з BS ISO/IEC 17799. Цей метод має два основних програмні модулі, COBRA Risk Consultant та ISO Compliance Analyst.

COBRA Risk Consultant надає підтримку процесу оцінки безпеки ризику шляхом: ідентифікації системні загрози, вразливості, вимірювання ступенів ризику та зв'язку з впливів на бізнес, надаючи детальні рішення та рекомендації щодо зменшення ризик.

Цей метод використовує стандартні форми структурованих запитів і включає оцінку три кроки:

1) запити,
2) оцінка ризику,
3) створення звіту.

Для кожного кроку метод COBRA дає модифікацію запиту, яка є мірою і експертиза після заповнення, завдяки адаптованій базі даних, яка забезпечує відновлення нових критеріїв, щоб кожна область могла бути адаптована до потреб користувачів. Метод COBRA містить бібліотеку контрзаходів і захисні рекомендації. Основними перевагами цього методу є: велика база загроз, адаптивна база знань, можливість часткової оцінки окремого модуля та простота оцінки. Основними недоліками цього методу є: застаріле програмне забезпечення, тривала оцінка, погана структура та заплутана оцінка процесу.

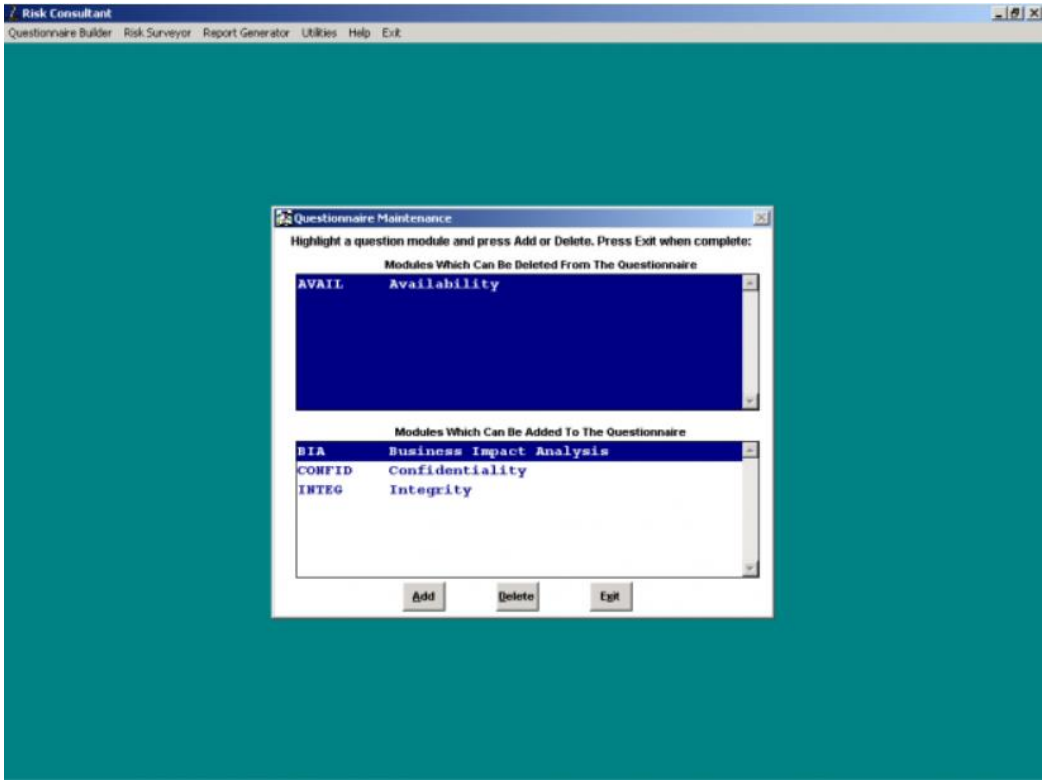


Рисунок 1.5 – Зовнішній вигляд COBRA Risk Consultant

Використовуючи ISO Compliance Analyst користувач на першому етапі розділ стандарту, на питання якого він буде відповідати.

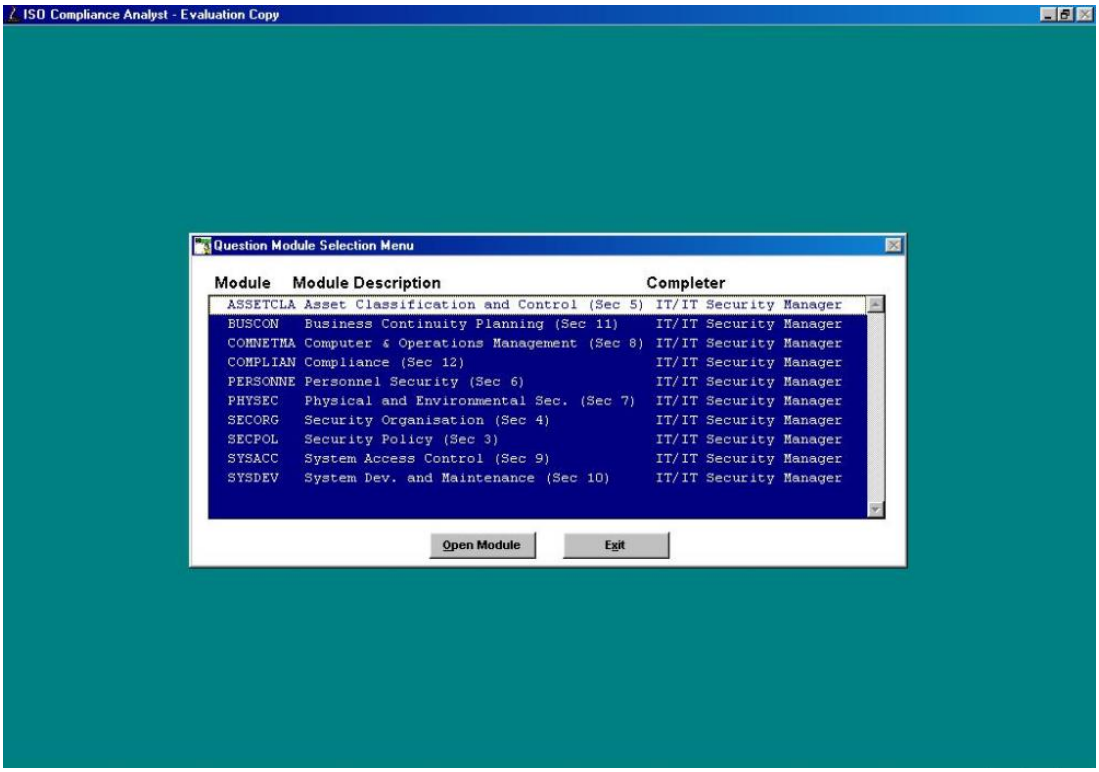


Рисунок 1.6 – Вибір розділу стандарта в ISO Compliance Analyst

Далі користувач відповідає на всі запитання по кожному розділу.

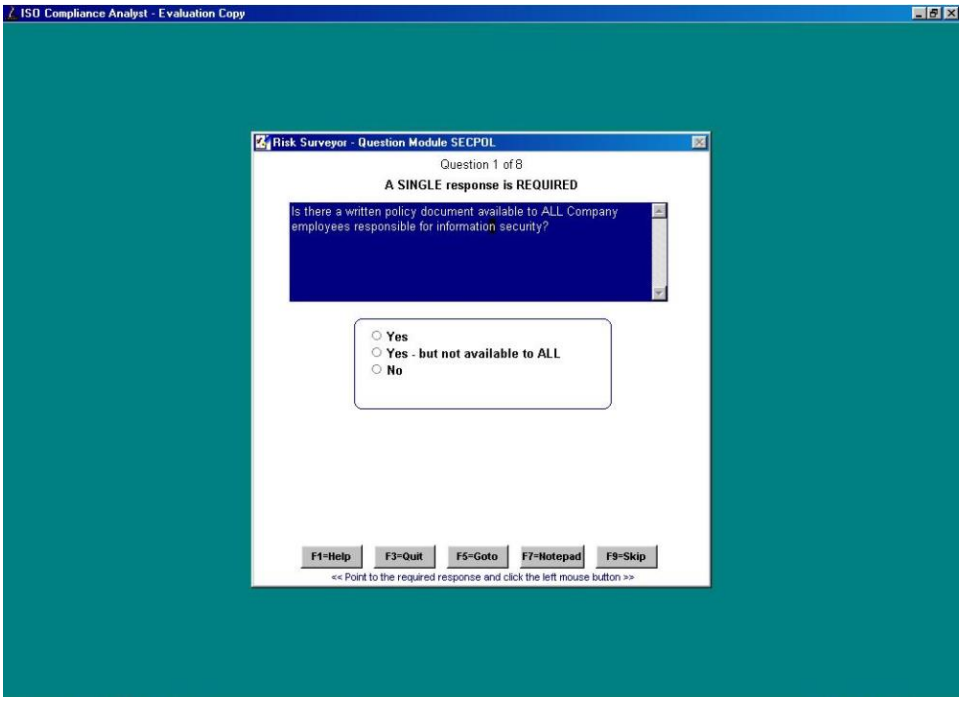


Рисунок 1.7 – Вікно із запитанням та варіантами відповіді

Пройшовши всі розділи та відповівши на всі запитання, користувач налаштовує параметри майбутнього звіту.

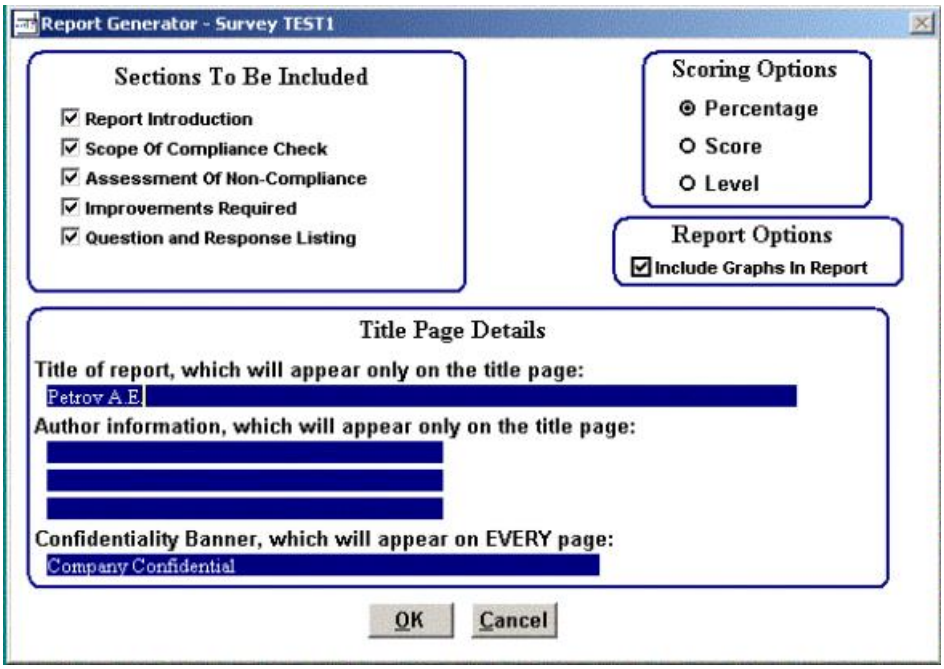


Рисунок 1.8 – Параметри звіту

На виході користувач отримує звіт згідно з яким він може оцінити ступінь відповідності існуючої політики безпеки згідно зі стандартом.

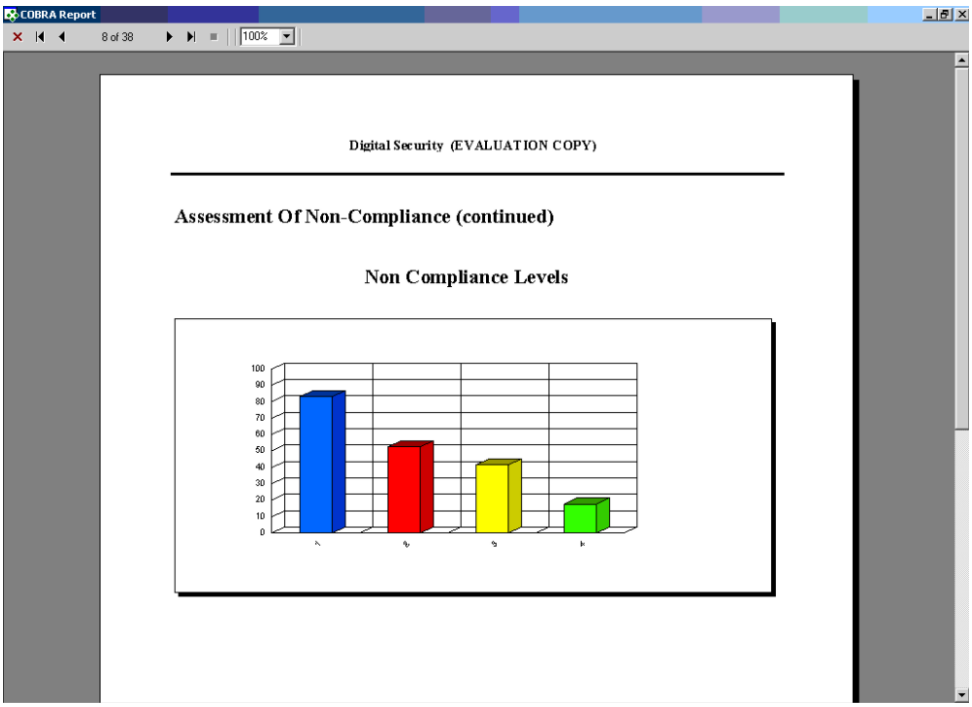


Рисунок 1.9 – звіт COBRA (сторінка 1)

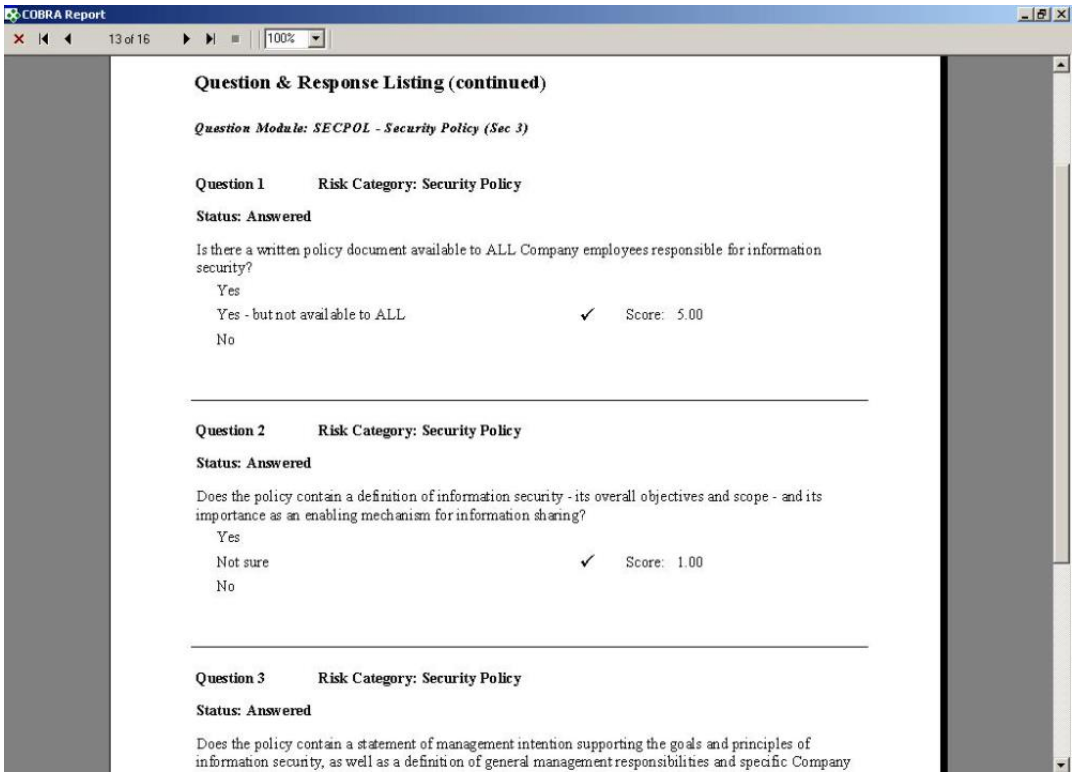


Рисунок 1.10 – Звіт COBRA (сторінка 2)

Останнім розглядатимемо RiskWatch.

RiskWatch представляє собою сімейство програмних продуктів, які призначені для управління різними видами ризиків та підтримки різних стандартів.

Розглянемо детальніше продукт RiskWatch for Information Systems.

RiskWatch for Information Systems – це рішення компанії RiskWatch для управління ризиками інформаційної системи. Цей інструмент проводить автоматизований аналіз ризиків та оцінку вразливості інформаційних систем. Бази даних знань, які надаються разом із продуктом, повністю налаштовуються користувачем, включаючи можливість створення нових категорій активів, категорій загроз, категорій уразливостей, засобів захисту, категорій запитань та наборів запитань. Інструмент містить елементи керування за стандартами ISO 17799 і US-NIST 800-26.

Крім того продукт має такі переваги:

– програмний інтерфейс (API) для роботи з базою знань, а також засоби імпорту інформації, наприклад, даних по активах;

– модуль оцінки ризиків, що реалізує алгоритми аналізу та оцінювання ризиків на підставі даних з бази знань та результатів опитувань;
– інтерфейсні модулі, призначені для формування та заповнення опитувальників користувачами продукту, а також створення звітів за результатами оцінки ризиків.

Оцінка ризиків відбувається протягом чотирьох етапів. Спочатку визначаються параметри обстеження. Після цього проводиться інтерв'ю та вводяться дані. Далі розраховуємо величини ризиків. На останньому етапі формується звіт.

На етапі визначення параметрів (Definition) задаються область оцінки, категорії збитків, категорії активів, аналізовані загрози, вразливості та контрзаходи, що застосовуються. Можна використовувати стандартні параметри або додавати власні.

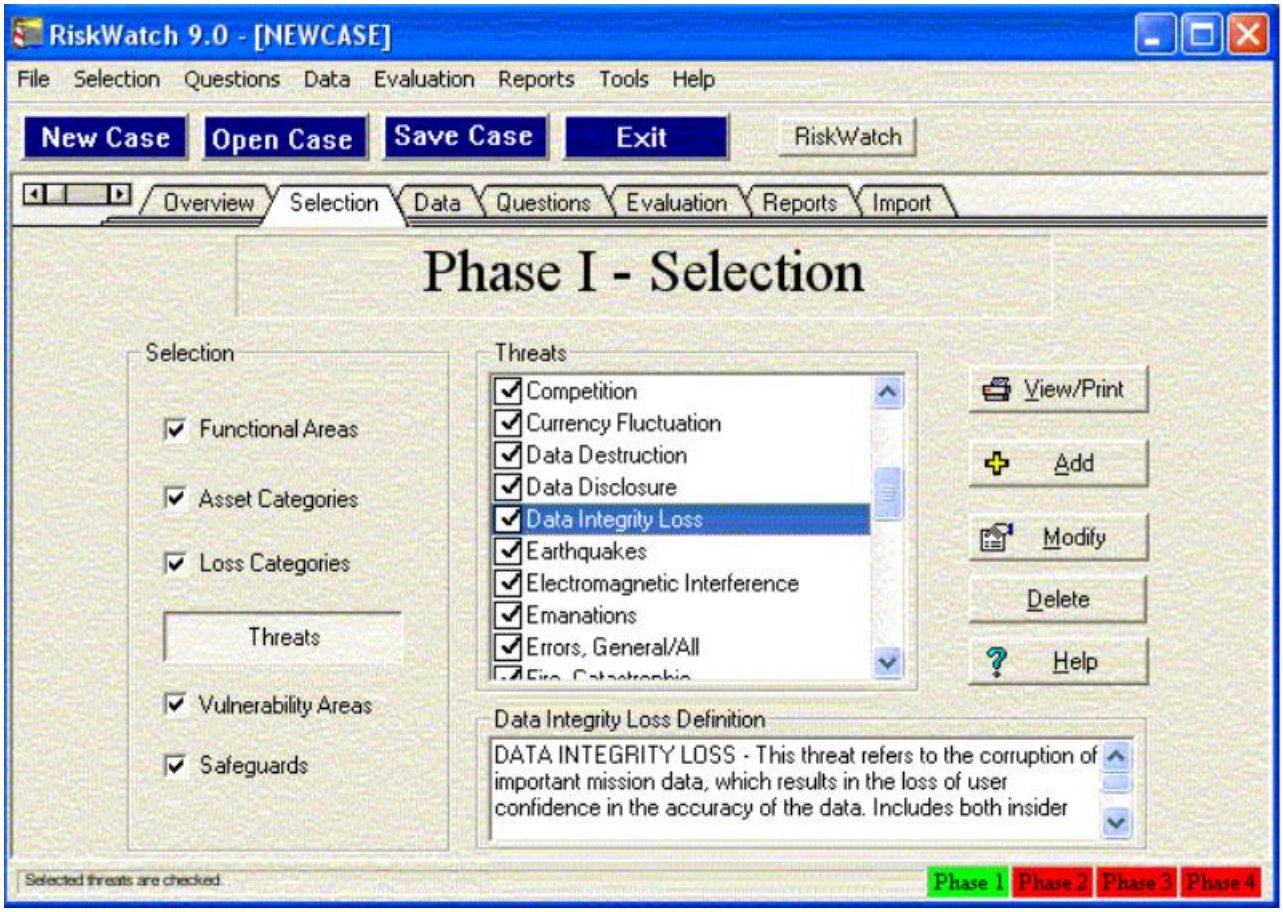


Рисунок 1.11 – Опис ресурсів інформаційної системи

На етапі введення даних (Data) до системи заносяться дані про цінність активів, ймовірність загроз, величину вразливостей та вартості контрзаходів.

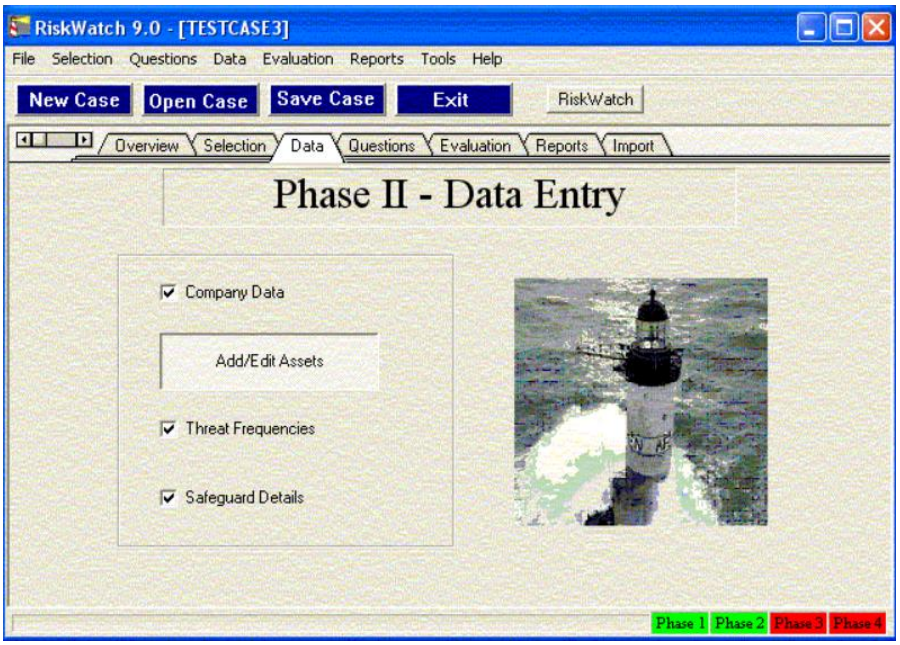


Рисунок 1.12 – Етап введення даних

Цінності активів, що визначаються величиною збитків внаслідок порушення конфіденційності, цілісності та доступності активів, відповідають певні оціночні грошові величини.

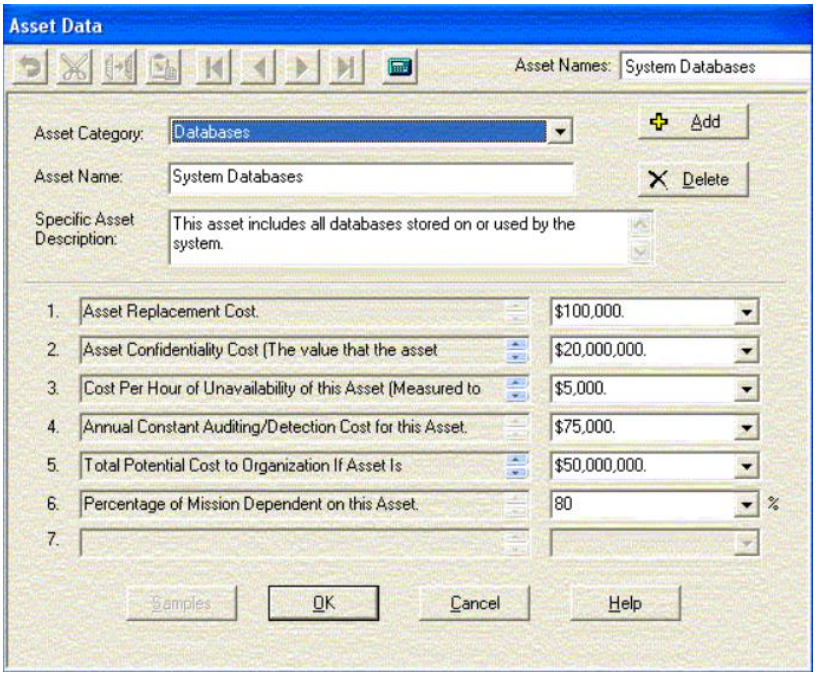

Рисунок 1.13 – Цінність активів

Очікувана частота реалізації загроз визначається термінах середньорічної оцінної частоти загрози (Annual Frequency Estimate). База знань RiskWatch визначає для кожної загрози стандартну частоту оцінки (StandardAnnualFrequencyEstimate, SAFE).

Для обчислення ризиків використовується локальна оцінна частота загрози (Local Annual Frequency Estimate, LAFE), яку користувач визначає сам, використовуючи базове значення SAFE.

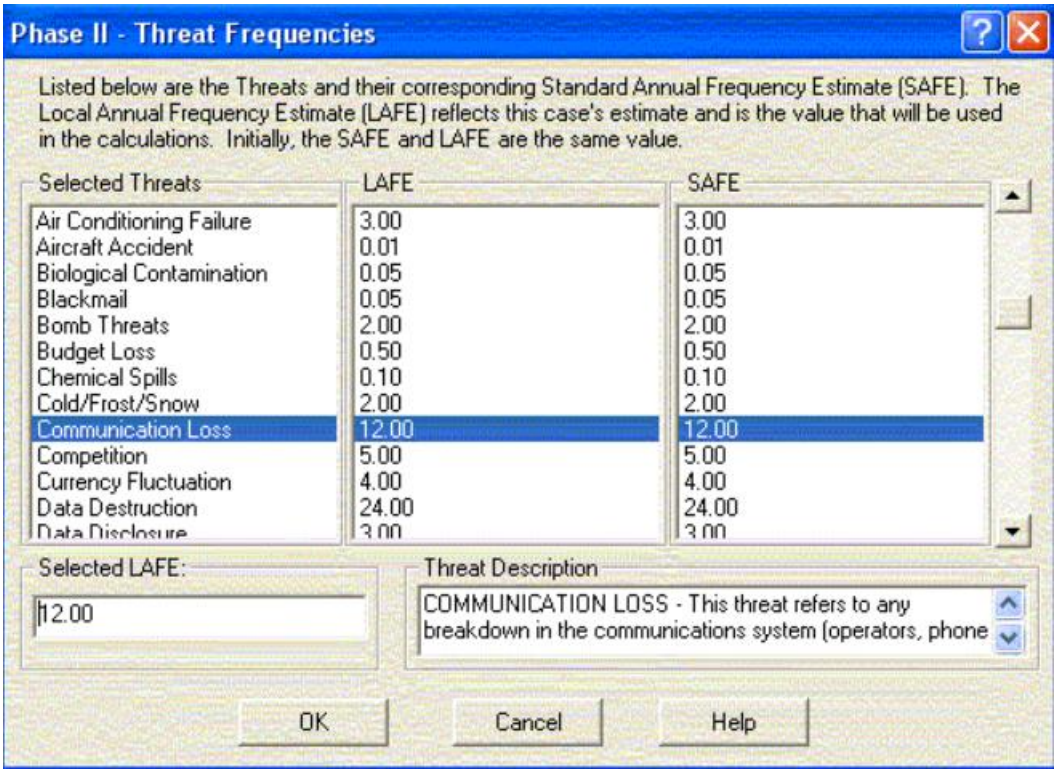


Рисунок 1.14 – Оцінка параметрів загроз з використанням статистичних даних

Для кожної контрзаходи задається її вартість, яка визначається вартістю впровадження та супроводу. Також враховується, на якій стадії знаходиться реалізація контрзаходу, тривалість її життєвого циклу та наскільки цей контрзахід зменшує оцінну частоту реалізації загрози (LAFE).

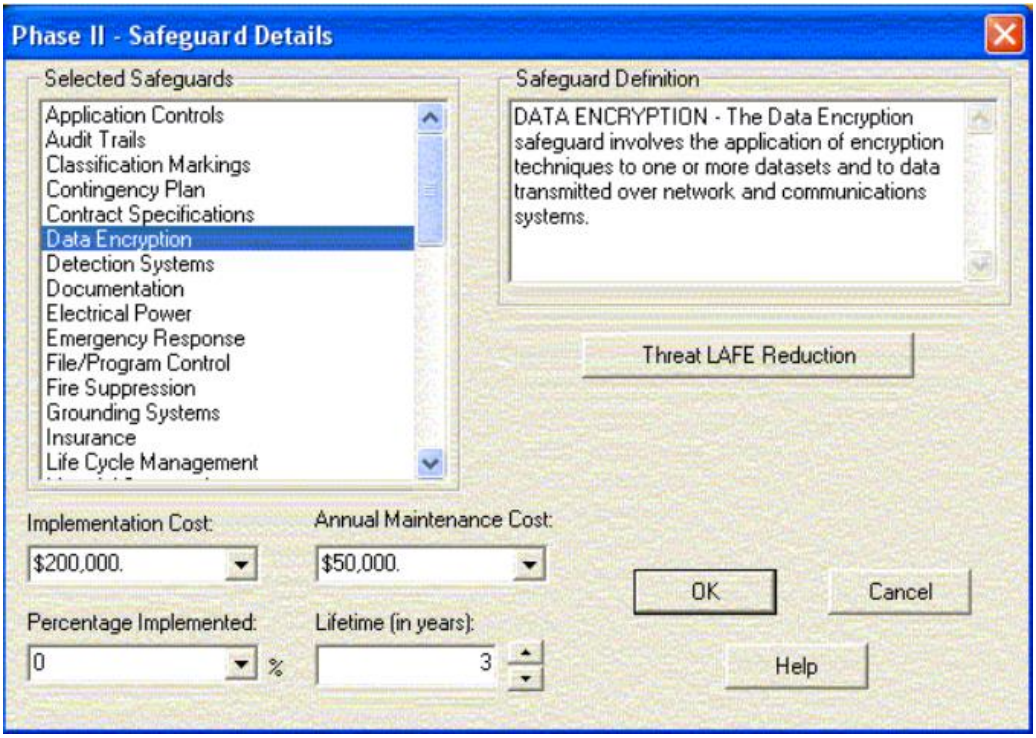


Рисунок 1.15 – Деталі захисту

На даному етапі також здійснюється формування опитувальних листів, які використовуються для отримання інформації від власників активів, представників бізнесу та експертів предметної галузі.

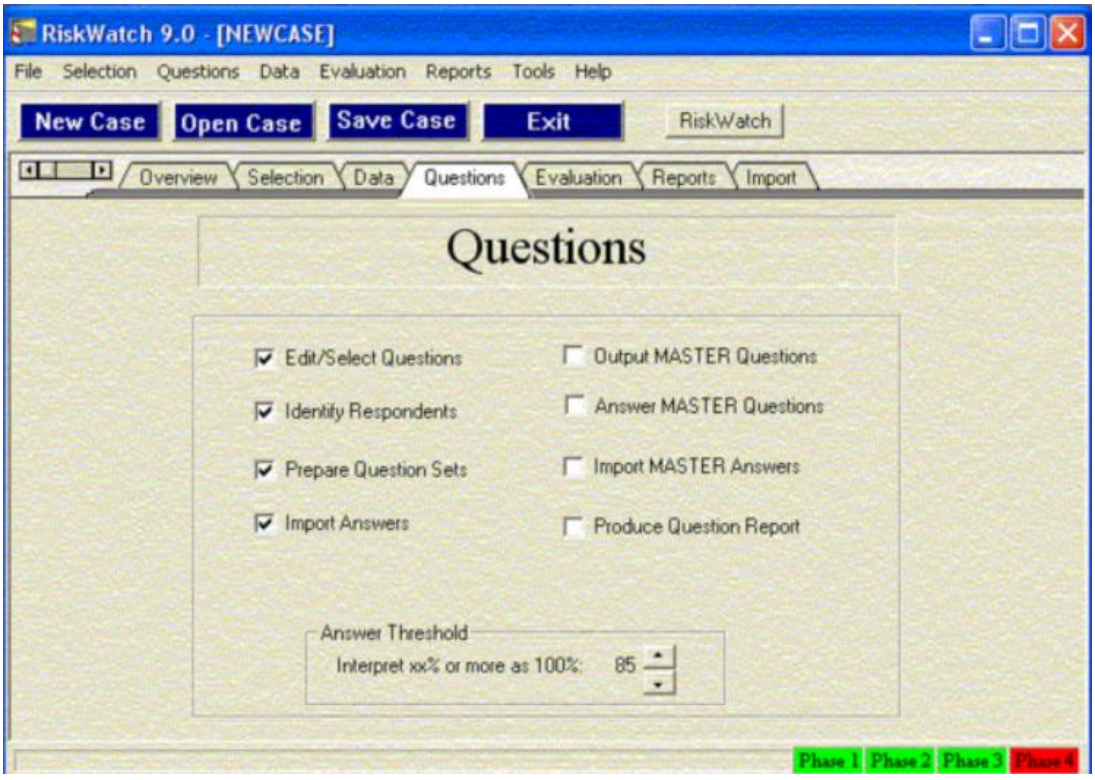

Рисунок 1.16 – Формування опитувальних листів

Інтерв'ю проводиться за допомогою веб-інтерфейсу за допомогою якого можна опитати будь-яку кількість експертів у віддаленому режимі.

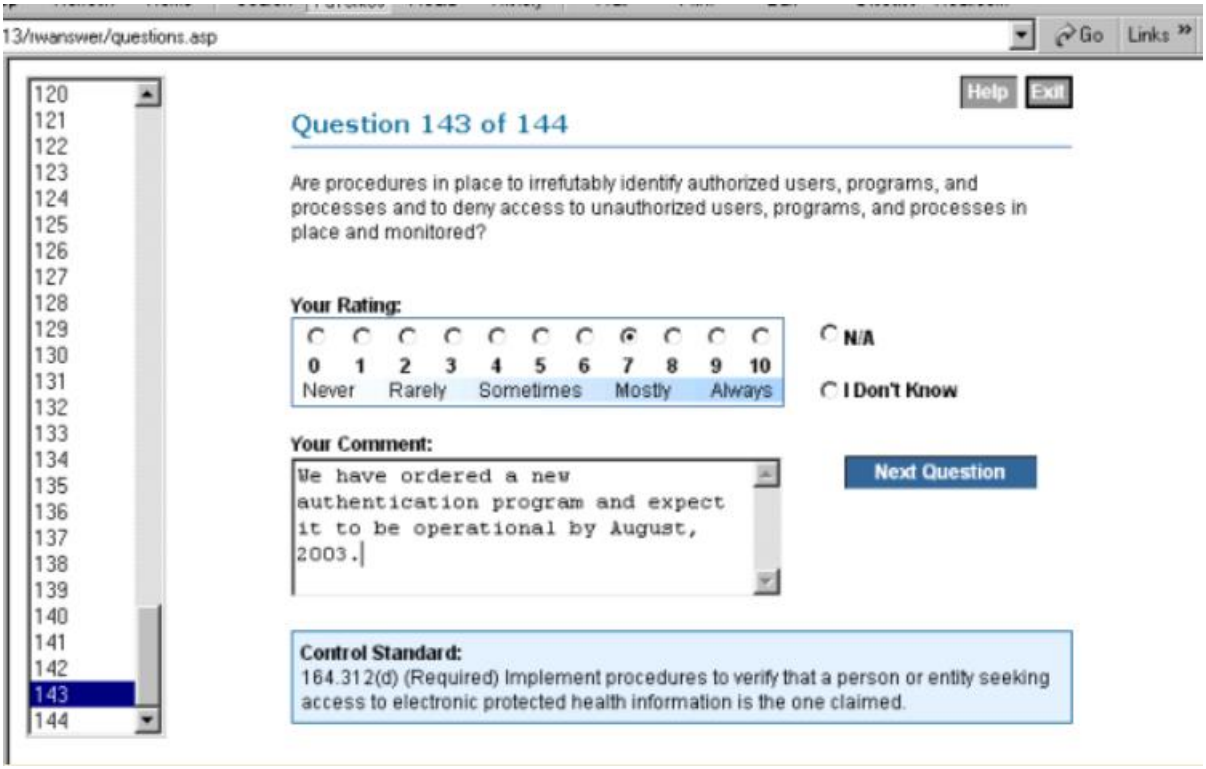


Рисунок 1.17 – Процес опитування

На етапі оцінки ризиків (Evaluation) проводиться зв'язування між собою даних про цінність активів, частоту загроз і величину вразливостей. В результаті проводиться розрахунок кількісних значень очікуваного середньорічного збитку (Annual Loss Expectancy, ALE) для кожної комбінації актив-загроза-вразливість. На даному етапі також розраховується коефіцієнт ROI для контрзаходів та розгляд сценаріїв «А що якщо?» (What Ifs), що дозволяють вибрати для зменшення ризиків оптимальну комбінацію контрзаходів.

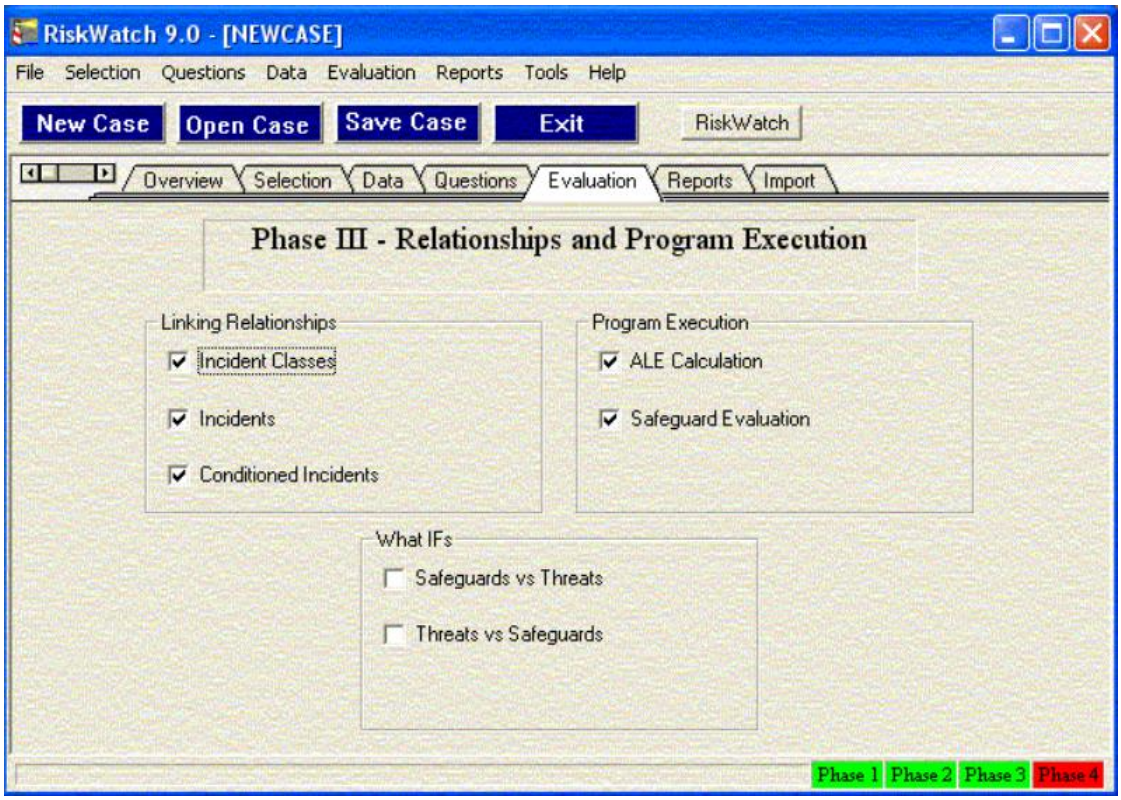


Рисунок 1.18 – Етап оцінки ризиків

На етапі формування звітів (Reports) роздруковується певний набір звітів за результатами оцінки ризиків.

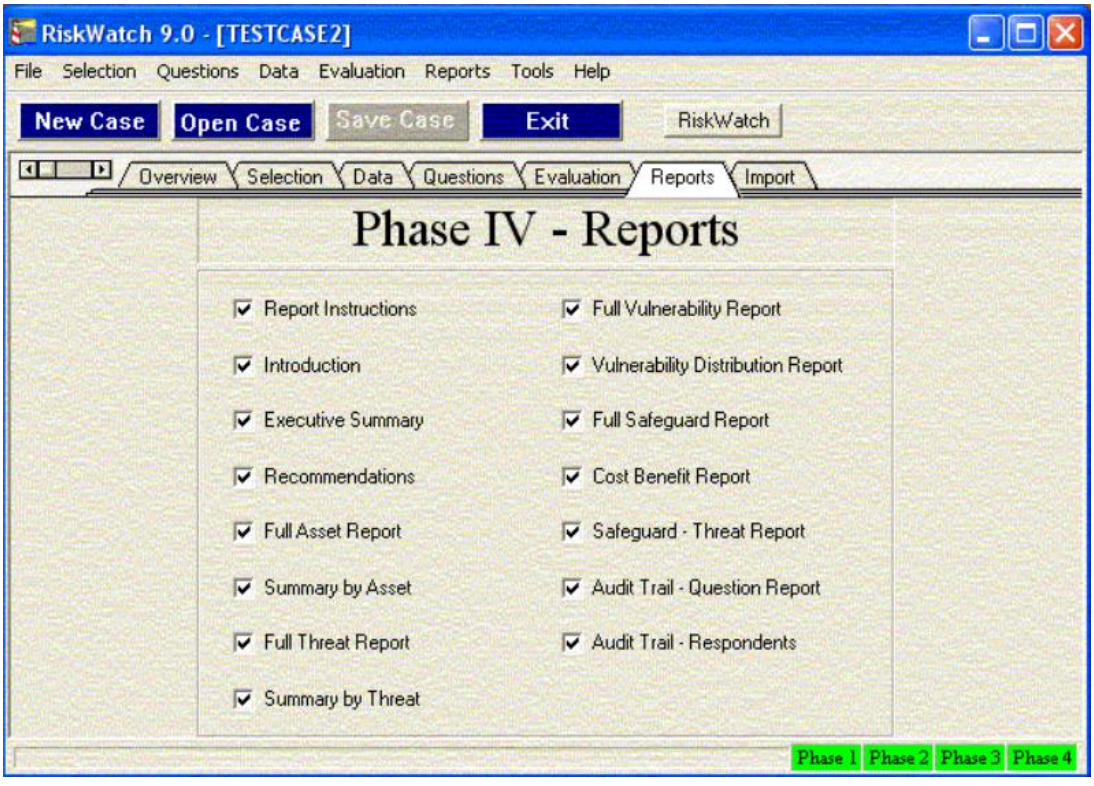

Рисунок 1.19 – Формування звіту

Графіки, що використовуються у звітах, представляють статистичну інформацію, наприклад, про розподіл вразливостей інформаційної системи по областях контролю.

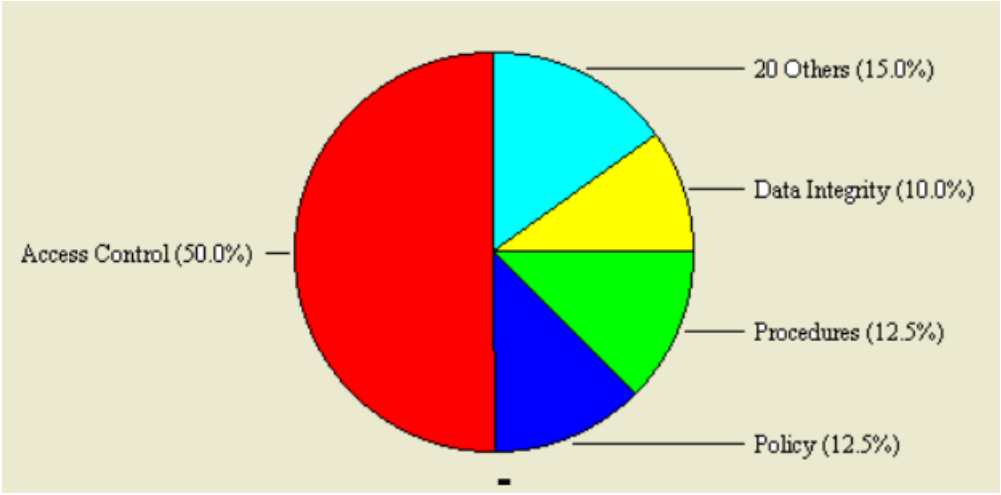


Рисунок 1.20 – Графік звіту з розподілом вразливостей інформаційної системи по областях контролю

Рекомендовані контрзаходи можуть бути відсортовані в порядку зменшення значення ROI, що є одним з основних показників для прийняття рішення щодо реалізації контрзаходів та відповідних пріоритетів їх реалізації.

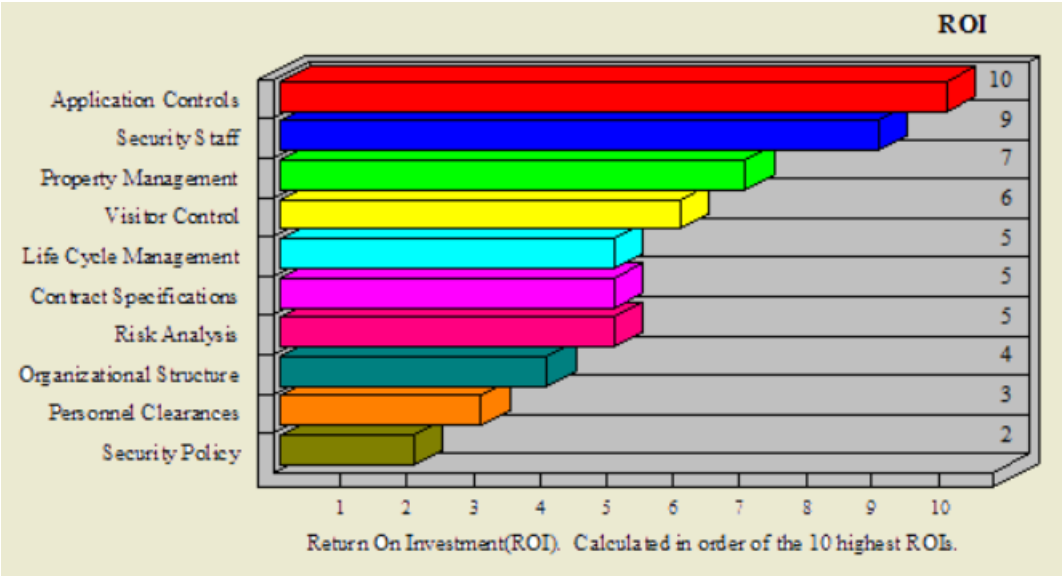


Рисунок 1.21 – Коефіцієнт ROI

Розглянувши цілий ряд програмних продуктів можна сказати, що багато країн впроваджують подібні рішення для оцінки захищеності інформаційних систем, адже це завдання є багатофакторним та вкрай необхідним. Програмні інструменти дозволяють отримати обгрунтовані результати, що допомагає виявити вразливості та вибудувати ефективний захист інформаційної системи. Використовуючи подібні додатки дослідити інформаційну систему можна у стислий термін із документуванням результатів.

На сьогоднішній день було розроблено стандарти для оцінювання безпеки інформаційних систем.

В них враховуються чотири типи вимог до комп'ютерних систем:

1) вимоги до проведення політики безпеки (security policy);
2) ведення обліку використання комп'ютерних систем (accounts);
3) довіру до комп'ютерних систем;
4) вимоги до документації.

Вимоги до проведення послідовної політики безпеки і ведення обліку використання комп'ютерних систем залежать одна від одної та забезпечуються засобами, закладеними в систему, тобто вирішення питань безпеки включається в програмні та апаратні засоби на стадії проектування.

Порушення довіри до комп'ютерних систем, як правило, буває викликано порушенням культури розробки програм: відмовою від структурного програмування, не виключенням заглушок, невизначеним введенням і т.д.

Для тестування на довіру потрібно знати архітектуру програми, правила стійкості її підтримки, тестовий приклад.

Вимоги до документації означають, що користувач повинен мати вичерпну інформацію з усіх питань. При цьому документація повинна бути лаконічною і зрозумілою. Тільки після оцінки безпеки комп'ютерної системи вона може надійти на ринок.

# 2 РОЗРОБКА МЕТОДИКИ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ

## 2.1 Політики безпеки та основні принципи запобігання порушення безпеки.

Інформаційна безпека на будь-якому рівні передбачає реалізацію трьох складових:

1) конфіденційність інформації або недоступність її третім особам;
2) цілісність або відсутність спотворення або підміни;
3) доступність або постійна можливість для користувача мати доступ до потрібних йому даних.

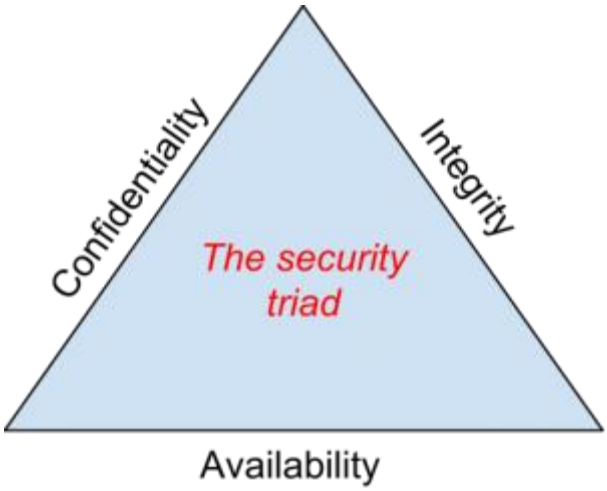


Рисунок 2.1 – Тріада безпеки

Цим трьом складовим може бути надане різне значення в програмах безпеки різних структур. Наприклад для системи національної оборони головною проблемою може бути забезпечення конфіденційності секретної інформації, тоді як система переказу коштів може вимагати жорсткого контролю цілісності. Вимоги до програм, підключених до зовнішніх систем, відрізнятимуться від вимог до програм без такого взаємозв’язку. Таким чином, конкретні вимоги та засоби контролю для інформаційної безпеки можуть відрізнятися.

Структура, в рамках якої організація прагне задовольнити свої потреби в інформаційній безпеці, кодифікується як політика безпеки. Політика безпеки – це стислий виклад тих, хто відповідає за систему (наприклад, вищого керівництва), про цінності інформації, відповідальність за захист та організаційні зобов'язання. Цю політику можна реалізувати, вживаючи конкретних дій, керуючись принципами контролю управління та використовуючи конкретні стандарти, процедури та механізми безпеки. І навпаки, вибір стандартів, процедур і механізмів має керуватися політикою, щоб бути найбільш ефективним.

Щоб бути корисною, політика безпеки повинна не лише вказувати потребу в безпеці (наприклад, конфіденційність – ці дані повинні бути розкриті лише уповноваженим особам), але й стосуватися діапазону обставин, за яких ця потреба має бути задоволена, і пов'язаних з ними стандартів роботи. Без цієї другої частини політика безпеки є настільки загальною, що стає марною (хоча друга частина може бути реалізована за допомогою процедур і стандартів, встановлених для реалізації політики). За будь-яких конкретних обставин деякі загрози є більш імовірними, ніж інші, і розважливий орган, який встановлює політику, повинен оцінити загрози, призначити рівень занепокоєння кожній і сформулювати політику, згідно з якою загрозам слід протистояти. Наприклад, до недавнього часу більшість політик безпеки не вимагали, щоб потреби безпеки були задоволені перед обличчям вірусної атаки, оскільки така форма атаки була незвичайною та широко не зрозуміла. Оскільки віруси переросли від гіпотетичної до звичайної загрози, виникла необхідність переглянути таку політику щодо методів розповсюдження та придбання програмного забезпечення. Неявним у цьому процесі є вибір керівництвом рівня залишкового ризику, з яким воно буде жити, рівня, який відрізняється в різних організаціях.

Управлінський контроль – це механізми та методи – адміністративні, процедурні та технічні – які впроваджуються для реалізації політики безпеки. Деякі засоби управління безпосередньо пов'язані із захистом інформації та інформаційних систем, але концепція засобів управління включає набагато більше, ніж конкретну роль комп'ютера у забезпеченні безпеки. Зауважте, що

засоби керування не лише використовуються менеджерами, а й користувачами. Необхідна ефективна програма управлінського контролю, щоб охопити всі аспекти інформаційної безпеки, включаючи фізичну безпеку, класифікацію інформації, засоби відновлення після порушень безпеки, і, перш за все, навчання, щоб прищепити обізнаність і сприйняття з боку людей. Між контролем існують компроміси. Наприклад, якщо технічні засоби контролю недоступні, то процедурні засоби контролю можуть використовуватися, поки не буде знайдено технічне рішення.

Одні лише технічні заходи не можуть запобігти порушенням довіри людей до окремих осіб, порушенням, які стали джерелом великої частини проблем комп'ютерної безпеки в промисловості на сьогоднішній день. Технічні заходи можуть перешкоджати людям робити несанкціоновані дії, але не можуть перешкодити їм робити те, що дають їм право виконувати їхні службові функції. Таким чином, щоб запобігти порушення довіри, а не просто виправити збиток, який спричиняє, потрібно в першу чергу залежати від усвідомлення людьми того, що роблять інші люди в організації. Але навіть технічно надійна система з інформованим і уважним керівництвом і користувачами не може бути позбавленою всіх можливих вразливостей. Залишковим ризиком необхідно керувати за допомогою процедур аудиту, резервного копіювання та відновлення, які підтримуються загальною пильністю та креативними реакціями. Більше того, організація повинна мати адміністративні процедури для доведення особливих дій до відома особи, яка може на законних підставах довідатися про доцільність таких дій, і ця особа має фактично зробити запит. У багатьох організаціях ці адміністративні положення є набагато менш задовільними, ніж технічні положення щодо безпеки.

Вага, що надається кожній із трьох основних вимог, що описують потреби в інформаційній безпеці – конфіденційності, цілісності та доступності – сильно залежить від обставин. Наприклад, негативні наслідки недоступності системи повинні частково бути пов'язані з вимогами до часу відновлення. Система, яку необхідно відновити протягом години після збою, являє собою і вимагає більш

вимогливого набору політик і засобів контролю, ніж подібна система, яку не потрібно відновлювати протягом двох-трьох днів. Аналогічно, ризик втрати конфіденційності щодо основного оголошення продукту зміниться з часом. Завчасне розкриття інформації може поставити під загрозу конкурентні переваги, але розкриття безпосередньо перед запланованим оголошенням може бути незначним. При цьому інформація залишається незмінною, а термін її оприлюднення істотно впливає на ризик втрати.

Розглянемо більш детальніше основні вимоги безпеки.

Конфіденційність – це вимога, метою якої є запобігання розголошенню конфіденційної інформації неавторизованим одержувачам. Секрети можуть бути важливими з міркувань національної безпеки (дані про ядерну зброю), правоохоронних органів (особи секретних наркоагентів), конкурентних переваг (витрати на виробництво або плани торгів) або конфіденційності (кредитні історії).

Оперативний контроль, який військові розробили на підтримку цієї вимоги, передбачають автоматизовані механізми обробки інформації, які мають вирішальне значення для безпеки. Такі механізми вимагають класифікації інформації на різних рівнях чутливості та в ізольованих відсіках, позначеної цією класифікацією та обробкою людей, які мають дозвіл на доступ до певних рівнів та/або відсіків. Усередині кожного рівня та відсіку особа з відповідним дозволом також повинна мати «потребу знати», щоб отримати доступ. Ці процедури є обов’язковими: для розсекречення інформації також необхідно дотримуватися детально розроблених процедур.

Політика класифікації існує в інших умовах, що відображає загальне визнання того, що для захисту активів корисно ідентифікувати та класифікувати їх. Деякі комерційні фірми, наприклад, класифікують інформацію як обмежену, конфіденційну та несекретну. Навіть якщо організація не має власних секретів, вона може бути зобов’язана за законом або загальною ввічливістю зберігати конфіденційність інформації про окремих осіб. Наприклад, медичні записи можуть потребувати більш ретельного захисту, ніж більшість конфіденційної

інформації. Таким чином, лікарня повинна вибрати відповідну політику конфіденційності, щоб підтримувати свою довірчу відповідальність щодо записів пацієнтів.

У комерційному світі конфіденційність зазвичай охороняється механізмами безпеки, менш суворими, ніж механізми національної безпеки. Наприклад, інформація призначається «власнику» (або опікуну), який контролює доступ до неї. Такі механізми безпеки здатні впоратися з багатьма ситуаціями, але не настільки стійкі до певних атак, як механізми, засновані на класифікації та обов'язковому позначенні, частково тому, що неможливо визначити, куди можуть надходити копії інформації. За допомогою атак троянських коней на, наприклад, навіть законних і чесних користувачів механізму власника можна обманом розкрити секретні дані. Комерційний світ переніс ці вразливості в обмін на більшу операційну гнучкість та продуктивність системи, пов'язану з відносно слабкою безпекою.

Цілісність – це вимога, яка гарантує, що інформація та програми змінюються лише визначеним та санкціонованим способом. Можливо, важливо підтримувати узгодженість даних (як у бухгалтерському обліку подвійного запису) або дозволяти змінювати дані лише затвердженим способом (наприклад, під час зняття коштів з банківського рахунку). Також може знадобитися вказати ступінь точності даних.

Деякі політики щодо забезпечення доброчесності відображають турботу про запобігання шахрайству та викладені з точки зору управлінського контролю. Наприклад, будь-яке завдання, пов'язане з можливістю шахрайства, має бути розділене на частини, які виконують окремі люди, такий підхід називається розділенням обов'язків. Класичним прикладом є система закупівель, яка складається з трьох частин: замовлення, отримання та оплати. Хтось повинен розписатися на кожному кроці, одна й та сама особа не може підписатися на двох кроках, і записи можна змінити лише за встановленими процедурами – наприклад, рахунок списується, а чек виписується лише на суму затвердженого та отриманого замовлення . У цьому випадку, хоча політика сформульована

оперативно, тобто з точки зору конкретних засобів управління, модель загроз також явно розкривається.

Інші політики доброчесності відображають занепокоєння щодо запобігання помилкам і упущенням, а також контролю за наслідками змін програми. Політика доброчесності вивчена не так ретельно, як політика конфіденційності. Комп'ютерні заходи, які були встановлені для захисту цілісності, як правило, є випадковими і не випливають із запропонованих моделей цілісності.

Цілісність – це впевненість у тому, що інформація, до якої здійснюється доступ, не була змінена і справді представляє те, що задумано. Подібно до того, як чесна людина означає те, їй можна довіряти, що вона послідовно представляє істину, інформаційна цілісність означає, що інформація справді представляє передбачуваний зміст. Інформація може втратити свою цілісність через зловмисні наміри, наприклад, коли хтось неуповноважений вносить зміни, щоб навмисно щось спотворити. Прикладом цього може бути, коли хакера наймають, щоб увійти в систему університету та змінити оцінку.

Цілісність також може бути втрачена ненавмисно, наприклад, коли стрибок напруги комп'ютера пошкоджує файл або хтось, уповноважений на внесення змін, випадково видаляє файл або вводить неправильну інформацію.

Доступність – це вимога, яка забезпечує оперативну роботу систем і відсутність відмов у сервісі для авторизованих користувачів. З операційної точки зору ця вимога стосується адекватного часу відгуку та/або гарантованої пропускної здатності. З точки зору безпеки, він представляє здатність захищатися від шкідливої події та відновлюватися після неї. Наявність належним чином функціонуючих комп'ютерних систем (наприклад, для маршрутизації міжміських дзвінків або обробки бронювання авіакомпаній) є важливою для роботи багатьох великих підприємств, а іноді і для збереження життя (наприклад, управління повітряним рухом або автоматизовані медичні системи). Планування на випадок надзвичайних ситуацій пов'язане з оцінкою ризиків і розробкою планів для запобігання чи відновлення після несприятливих подій, які можуть зробити систему недоступною.

Традиційне планування на випадок надзвичайних ситуацій для забезпечення доступності зазвичай включає реагування лише на дії Бога (наприклад, землетруси) або випадкові антропогенні події (наприклад, витік токсичного газу, що перешкоджає проникненню на об’єкт). Однак планування на випадок надзвичайних ситуацій має також включати забезпечення відповідей на зловмисні дії, а не просто дії Бога чи нещасні випадки, і, як таке, має включати явну оцінку загрози на основі моделі реального супротивника, а не імовірнісної моделі природи.

Наприклад, проста політика доступності зазвичай формулюється так: «У середньому термінал не працює менше ніж на 10 хвилин на місяць». Конкретний термінал (наприклад, банкомат або клавіатура та екран агента з бронювання) працює, якщо він правильно відповідає протягом однієї секунди на стандартний запит на обслуговування; в іншому випадку він знижений. Ця політика означає, що час роботи на кожному терміналі, усереднений для всіх терміналів, має становити щонайменше 99,98 відсотків.

Політика безпеки для забезпечення доступності зазвичай приймає іншу форму, як у наступному прикладі: «Жодні введення в систему будь-яким користувачем, який не є авторизованим адміністратором, не призведе до того, що система перестане обслуговувати інших користувачів». Зауважте, що ця політика нічого не говорить про системні збої, крім випадків, коли вони можуть бути викликані діями користувача. Натомість він визначає конкретну загрозу, зловмисний чи некомпетентний вчинок звичайного користувача системи та вимагає, щоб система пережила цей акт. У ньому нічого не сказано про інші способи, якими ворожа сторона може відмовити в наданні, наприклад, обірвавши телефонну лінію; для кожної такої загрози потрібне окреме твердження, що вказує на те, до якої міри опір цій загрозі вважається важливим.

Потреби до інформаційної системи можуть відрізнятися. Наприклад, автоматизована касова система повинна зберігати конфіденційність персональних ідентифікаційних номерів (ПІН) як у хост-системі, так і під час передачі транзакції. Він повинен захищати цілісність записів рахунків та окремих

транзакцій. Захист конфіденційності важливий, але не критично. Наявність хост-системи важлива для економічного виживання банку, але не для його відповідальності. У порівнянні з доступністю хост-системи, наявність окремих банкоматів викликає менше занепокоєння. З іншого боку, система телефонної комутації не має високих вимог до цілісності окремих транзакцій, оскільки час від часу втрата дзвінків або рахунків не буде завдана довготривалої шкоди. Однак цілісність керуючих програм і конфігураційних записів є критичною. Без них функція перемикання буде порушена, а найважливіший атрибут усіх – доступність – буде скомпрометований. Система телефонної комутації також повинна зберігати конфіденційність окремих дзвінків, не даючи одному абоненту підслухати іншого.

Потрібно звертати увагу на те, як використовується система. Наприклад, система верстки повинна забезпечувати конфіденційність, якщо вона використовується для публікації корпоративних запатентованих матеріалів, цілісність, якщо вона використовується для публікації законів, і доступність, якщо вона використовується для публікації щоденних газет. Можна очікувати, що система розподілу часу загального призначення забезпечить конфіденційність, якщо вона обслуговує різноманітну клієнтуру, цілісність, якщо вона використовується як середовище розробки програмного забезпечення або інженерних проектів, і доступність до такої міри, що жоден користувач не може монополізувати послугу і що втрачені файли можна буде відновити.

Засоби управління призначені для того, щоб направляти операції у належному напрямку, запобігати чи виявляти зло і шкідливі помилки, а також завчасно попереджати про вразливі місця. Організації майже в кожному напрямі діяльності встановили контроль на основі таких ключових принципів:

- індивідуальна відповідальність,
- аудит,
- розділення обов'язків.

Ці принципи, визнані в тій чи іншій формі протягом століть, є основою передкомп’ютерних операційних процедур, які дуже добре розуміють люди.

Індивідуальна відповідальність відповідає на питання: хто несе відповідальність за цю заяву чи дію? Його мета – відстежувати те, що сталося, хто мав доступ до інформації та ресурсів і які дії були вжиті. У будь-якій реальній системі є багато причин, чому фактична робота не завжди може відображати початкові наміри власників: люди роблять помилки, система має помилки, система вразлива до певних атак, широка політика не була правильно переведена в детальні характеристики, власники передумали тощо. Коли щось йде не так, необхідно знати, що сталося, і хто є причиною. Ця інформація є основою для оцінки збитків, відновлення втраченої інформації, оцінки вразливостей та ініціювання компенсаційних дій, таких як судове переслідування, поза комп'ютерною системою.

Для підтримки принципу індивідуальної відповідальності необхідна послуга, яка називається аутентифікація користувача. Без надійної ідентифікації не може бути відповідальності. Таким чином, аутентифікація є важливою основою інформаційної безпеки. Багато систем були проникнуті, коли слабкі або погано керовані служби аутентифікації були скомпрометовані, наприклад, через вгадування погано підібраних паролів.

Основна послуга, яку надає аутентифікація, – це інформація про те, що заява або дія були зроблені певним користувачем. Іноді необхідно переконатися, що користувач пізніше не зможе стверджувати, що приписувана йому заява була підроблена і що він ніколи її не робив. У світі паперових документів це є метою нотаріального засвідчення підпису; нотаріус надає незалежні та дуже достовірні докази, які будуть переконливими навіть через багато років, що підпис справжній, а не підроблений. Ця суворіша форма аутентифікації, яка називається невідмовністю, сьогодні пропонується нечисленними комп'ютерними системами, хоча юридичну потребу в ній можна передбачити, оскільки комп'ютерно-опосередковані транзакції стають все більш поширеними в бізнесі.

Аудиторські послуги підтримують підзвітність і тому є цінними для керівництва та внутрішніх чи зовнішніх аудиторів. Враховуючи реальність того, що кожна комп'ютерна система може бути скомпрометована зсередини, і що

багато систем також можуть бути скомпрометовані, якщо можна отримати прихований доступ, відповідальність є життєво важливим останнім засобом. Аудиторські служби створюють та ведуть записи, необхідні для забезпечення підзвітності. Зазвичай вони тісно пов’язані з аутентифікацією та авторизацією (сервіс для визначення того, чи є користувач або система довіреною для певної мети – дивіться обговорення нижче), так що кожна автентифікація записується, як і кожна спроба доступу, незалежно від того, авторизована чи ні. Враховуючи важливу роль аудиту, пристрої аудиту іноді стають першою ціллю зловмисника і повинні бути захищені відповідним чином.

Записи аудиту системи, які часто називають аудиторським слідом, мають інші потенційні можливості, крім встановлення підзвітності. Наприклад, можна проаналізувати аудиторський слід на наявність підозрілих моделей доступу і таким чином виявити неналежну поведінку як законних користувачів, так і фейків. Основними недоліками є обробка та інтерпретація даних аудиту.

Системи можуть постійно змінюватися, оскільки персонал та обладнання приходять і зникають, а програми розвиваються. З точки зору безпеки, система, що змінюється, навряд чи буде системою, яка покращується. Щоб зайняти активну позицію проти поступового знищення заходів безпеки, можна доповнити динамічно зібраний журнал аудиту (який корисний для визначення того, що сталося) статичними аудитами, які перевіряють конфігурацію, щоб переконатися, що вона не відкрита для атак. Служби статичного аудиту можуть перевіряти, чи програмне забезпечення не змінилося, чи належним чином налаштовано контроль доступу до файлів, чи вимкнено застарілі облікові записи користувачів, чи правильно ввімкнено вхідні та вихідні лінії зв’язку, що паролі важко вгадати тощо. Окрім засобів перевірки на віруси, на ринку існує кілька інструментів статичного аудиту.

Встановлена практика поділу обов’язків уточнює, що важливі операції не може виконуватися однією особою, а вимагає згоди (принаймні) двох різних осіб. Таким чином, розділення обов’язків посилює безпеку, запобігаючи будь-якому

підриву органів управління однією рукою. Це також може допомогти зменшити кількість помилок, забезпечивши незалежну перевірку дій однієї особи іншою.

Поділ обов'язків є прикладом більш широкого класу засобів контролю, які намагаються вказати, кому довіряють для певної мети. Цей вид контролю зазвичай відомий як авторизація користувача. Авторизація визначає, чи є певний користувач, який був аутентифікований як джерело запиту щось зробити, довіреним для цієї операції. Авторизація також може включати контроль часу, коли щось можна зробити (тільки в робочий час), або комп'ютерного терміналу, з якого це можна зробити (тільки на столі менеджера).

Подібно до того, як мета індивідуальної підзвітності вимагає механізму нижчого рівня для аутентифікації користувачів, так само й засоби контролю авторизації, такі як розподіл обов'язків, вимагають механізму нижчого рівня, щоб гарантувати, що користувачі мають доступ лише до правильних об'єктів. Всередині комп'ютера ці механізми застосування зазвичай називають механізмами контролю доступу.

## 2.2 Стандартизація у сфері інформаційної безпеки.

Стандартизація – це діяльність, що направлена на розробку та встановлення вимог, норм та правил, характеристик, що є обов'язковими до виконання або рекомендованими.

Самі стандарти – це нормативні документи, що розроблені на основі консенсусу, затвердженого признаним органом та направлені на досягнення оптимального ступеня упорядкованості у певній області. В стандарті встановлюють для загального та багатократного використання загальні принципи, правила і характеристики, що стосуються змісту різних видів діяльності або їх результатів. Стандарти мають за мету досягнення оптимального ступеня упорядкованості в тій або іншій області діяльності за допомогою широкого та багатократного використання встановлених положень, вимог та норм для рішення реально існуючих, запланованих або потенціальних задач.

Стандарти в галузі інформаційної безпеки покликані виробити чіткий набір критеріїв, за якими можна звести до мінімуму можливі загрози системі. При оцінці безпеки інформаційних систем слід враховувати думку трьох груп фахівців: розробників інформаційних систем, замовників або користувачів інформаційних систем, спеціалістів – аналітиків з інформаційної безпеки.
Розглянемо, за допомогою яких стандартів та нормативних документів можна оцінити якість інформаційної системи чи окремі показники.

## 2.3 Стандарт ISO/IEC 15408.

Стандарт ISO/IEC 15408 – один з найпоширеніших стандартів безпеки. У його створенні взяли участь організації із багатьох країн. У стандарті, який отримав назву «Загальні критерії оцінки безпеки інформаційних технологій» (The Common Criteria for Information Technology Security Evaluation), детально розглянуті загальні підходи, методи та функції забезпечення захисту в організаціях. Функції системи інформаційної безпеки забезпечують виконання вимог конфіденційності, цілісності, достовірності та доступності інформації.

ISO/IEC 15408 складається з наступних частин під загальною назвою Інформаційні технології – Методи безпеки – Критерії оцінки IT-безпеки:

- Частина 1: Вступ і загальна модель;
- Частина 2: Функціональні вимоги безпеки;
- Частина 3: Вимоги до забезпечення безпеки.

Оцінка інформаційної безпеки ґрунтується на моделях системи безпеки, що складаються з перелічених у стандарті функцій. В ISO 15408 міститься ряд зумовлених моделей (так званих профілів), що описують стандартні модулі безпеки. З їх допомогою можна не створювати моделі поширених засобів захисту самостійно, винаходячи велосипед, а користуватися вже готовими наборами описів, цілей, функцій та вимог до цих засобів. Простим прикладом профілів може бути модель міжмережевого екрану або система управління базами даних.

Особливості ISO 15408 в порівнянні з іншими стандартами безпеки:

- стандарт дозволяє визначити повний перелік вимог до засобів безпеки, а також критеріїв їхньої оцінки (показники захищеності інформації);
- стандарт визначає повний перелік об'єктів аналізу та вимог до них, не загострюючи уваги на методах створення, управління та оцінки системи безпеки;
- стандарт дозволяє оцінити повноту системи інформаційної безпеки з технічного погляду, не розглядаючи при цьому комплекс організаційних заходів із забезпечення захисту інформації.

ISO/IEC 15408 має 3 частини. Давайте детальніше розглянемо другу його частину.

ISO/IEC 15408-2 визначає зміст і представлення функціональних вимог безпеки, які підлягають оцінці під час оцінки безпеки з використанням ISO/IEC 15408. Він містить повний каталог попередньо визначених функціональних компонентів безпеки, які відповідатимуть найбільш поширеним потребам безпеки. ринок. Вони організовані з використанням ієрархічної структури класів, сімейств і компонентів і підтримуються вичерпними примітками користувача.

ISO/IEC 15408-2 також містить вказівки щодо специфікації індивідуальних вимог безпеки, коли не існує відповідних попередньо визначених функціональних компонентів безпеки.

Усі функції представлені у вигляді чотирирівневої ієрархічної структури: клас - сімейство - компонент - елемент. За аналогією представлені вимоги якості. Подібна градація дозволяє описати будь-яку систему інформаційної безпеки та зіставити створену модель із поточним станом справ. У стандарті ISO/IEC 15408–2 виділено 11 класів функцій: аудит, ідентифікація та аутентифікація, криптографічний захист, конфіденційність, передача даних, захист даних, управління безпекою, захист функцій безпеки системи, використання ресурсів, доступу до системи, надійність коштів.

Назва класу надає інформацію, необхідну для ідентифікації та категоризації функціонального класу. Кожен функціональний клас має унікальну назву.

Категоріальна інформація складається з короткої назви з трьох символів. Коротка назва класу використовується в специфікації коротких імен сімейства цього класу.

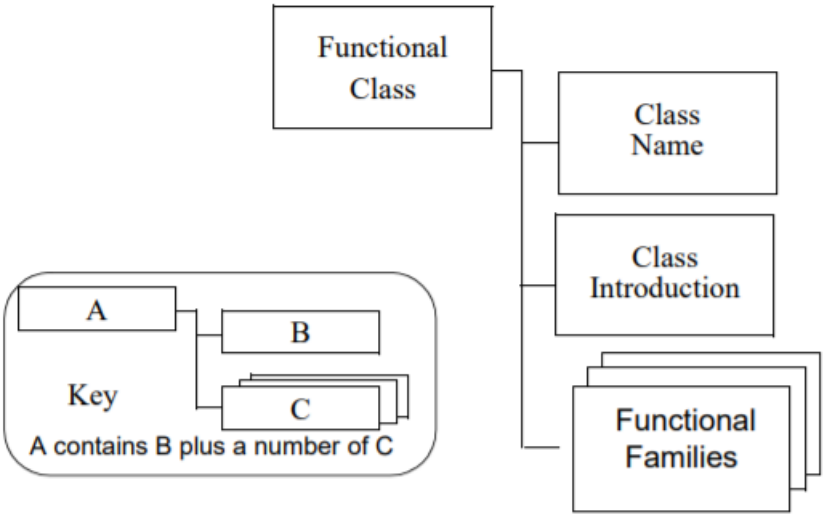


Рисунок 2.2 – Структура функціонального класу

Назва сім'ї надає категоріальну та описову інформацію, необхідну для ідентифікації та категоризації функціональної сім'ї. Кожна функціональна сім'я має унікальну назву. Інформація про категорію складається з короткої назви з семи символів, причому перші три ідентичні короткій назві класу, за якими слідує символ підкреслення та коротка назва сімейства, як показано нижче XXX_YYY. Унікальна коротка форма назви надає основне посилання для компонентів.

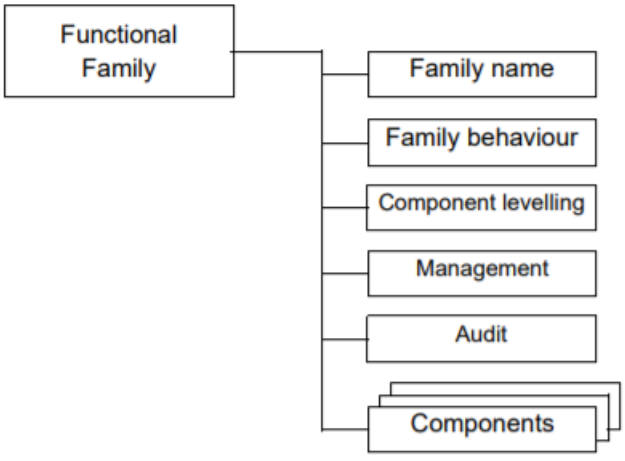


Рисунок 2.3 – Структура функціонального сімейства

Функціональні сімейства містять один або більше компонентів, будь-який з яких можна вибрати. Метою цього розділу є надання інформації користувачам при виборі відповідного функціонального компонента після того, як сімейство було визначено як необхідну або корисну частину їхніх вимог безпеки. Цей розділ опису функціонального сімейства описує доступні компоненти та їх обґрунтування. Точні відомості про компоненти містяться в кожному компоненті. Відносини між компонентами всередині функціонального сімейства можуть бути ієрархічними, а можуть і не бути такими. Компонент є ієрархічним щодо іншого, якщо він забезпечує більшу безпеку.

Ідентифікація компонента надає описову інформацію, необхідну для категоризації. У складі кожного функціонального компонента надається наступне:

– Унікальна назва. Назва відображає призначення компонента.
– Коротка назва. Унікальна коротка форма назви функціонального компонента. Це коротке ім'я служить основним довідковим ім'ям для категоризації, реєстрації та перехресних посилань компонента. Ця коротка назва відображає клас і сімейство, до якого належить компонент, а також номер компонента в сімействі.
– Ієрархічний список. Список інших компонентів, для яких цей компонент є ієрархічним і для яких цей компонент можна використовувати, щоб задовольнити залежності від перерахованих компонентів.

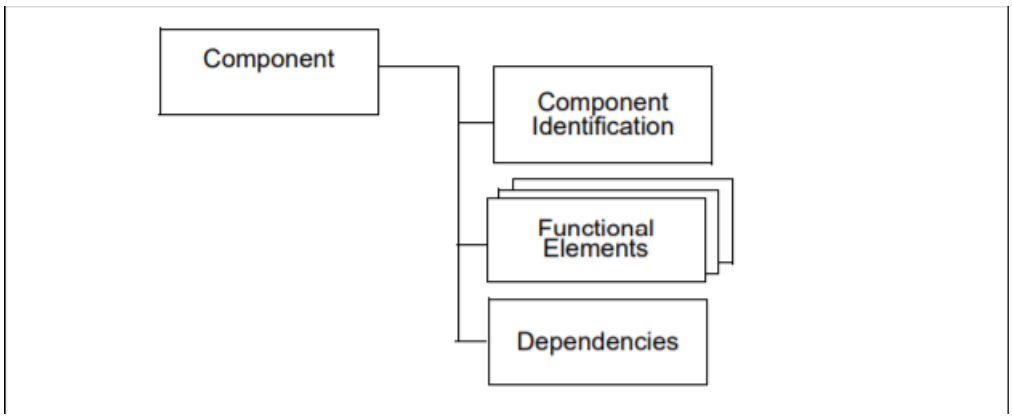


Рисунок 2.4 – Структура функціонального компонента

Для кожного компонента надається набір елементів. Кожен елемент визначається окремо і є самостійним. Функціональний елемент – це функціональна вимога безпеки, подальше розділення якої не дасть значущого результату оцінки. Це найменша функціональна вимога безпеки, визначена та визнана в ISO/IEC 15408.

Не дозволяється вибирати лише один або більше елементів із компонента. Повний набір елементів компонента повинен бути обраний.

Надається унікальна коротка форма назви функціонального елемента. Наприклад, назва вимоги FDP_IFF.4.2 звучить так: F – функціональна вимога, DP - клас "Захист даних користувача", _IFF – сімейство "Функції керування інформаційними потоками", .4 – 4-й компонент під назвою "Часткове усунення незаконних інформаційних потоків" , .2 – 2-й елемент компонента.

Розглянемо залежності між функціональними компонентами стандарту ISO 15408-2.

Залежності між функціональними компонентами виникають, коли компонент не є самодостатнім і покладається на функціональність або взаємодію з іншим компонентом для свого належного функціонування.

Кожен функціональний компонент має повний список залежностей від інших функціональних компонентів і компонентів забезпечення. У деяких компонентах може бути зазначено «Немає залежностей». Компоненти, від яких залежить, можуть, у свою чергу, залежати від інших компонентів. Список, наданий у компонентах, задає прямі залежності. Це лише посилання на функціональні вимоги, які необхідні для належного виконання цієї вимоги. Непрямі залежності, тобто залежності, які є результатом залежних компонентів, можна знайти в Додатку А. Зазначається, що в деяких випадках залежність є необов’язковою, оскільки надається ряд функціональних вимог, де кожна з них бути достатнім для задоволення залежності.

Розглянемо таблиці залежностей. Кожному компоненту, від якого залежать функціональні компоненти, у таблиці відведений стовпець. Кожному функціональному компоненту відведено рядок. Знаки на перетині рядків та

стовпців таблиці вказують на характер залежності відповідних компонентів. "x" – пряма залежність; "-" – непряма, а "O" – залежність, що вибирається.

Залежність, що вибирається розглянемо на прикладі компонента FDP_ETC.1 "Експорт даних користувача без атрибутів безпеки", що вимагає присутності або компонента FDP_ACC.1 "Обмежене управління доступом", або компонента FDP_IFC.1 "Обмежене управління інформаційними потоками". Так, якщо обраний компонент FDP_ACC.1 "Обмежене керування доступом", то присутність FDP_IFC.1 "Обмежене керування інформаційними потоками" необов'язкова і навпаки. Якщо перетин рядка та стовпця таблиці порожній, тоді компонент рядка не залежить від компонента зі стовпця.

Список залежностей визначає мінімальні функціональні або впевнені компоненти, необхідні для задоволення вимоги безпеки, пов'язані з ідентифікованим компонентом. Компоненти, які є ієрархічними щодо ідентифікованого компонента, також можуть використовуватися для задоволення залежності. Залежності, зазначені в ISO/IEC 15408-2, є нормативними.

Ієрархічність компонентів можна пояснити за допомогою наступного рисунка.

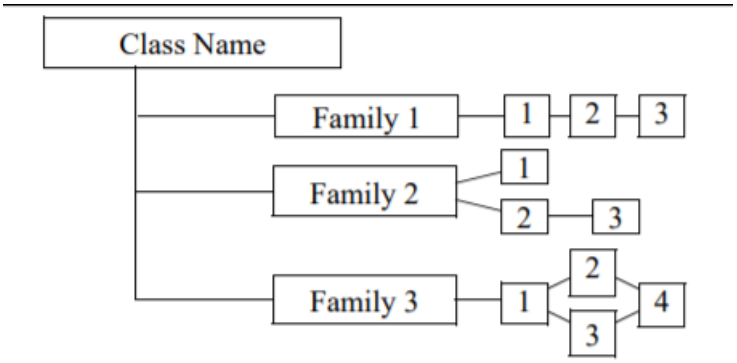


Рисунок 2.5 – Зображення класу та його складових

На рисунку перше сімейство, Сімейство 1, містить три ієрархічні компоненти, де компонент 2 і компонент 3 можуть використовуватися для задоволення залежностей від компонента 1. Компонент 3 є ієрархічним

компонентом до компонента 2, а також може використовуватися для задоволення залежностей від компонента 2.

У Сімействі 2 є три компоненти, не всі з яких є ієрархічними. Компоненти 1 і 2 не є ієрархічними для інших компонентів. Компонент 3 є ієрархічним компонентом до компонента 2 і може використовуватися для задоволення залежностей від компонента 2, але не для задоволення залежностей від компонента 1.

У Сімействі 3 компоненти 2, 3 і 4 ієрархічні до компонента 1. Компоненти 2 і 3 ієрархічні до компонента 1, але непорівнянні. Компонент 4 є ієрархічним як для компонента 2, так і для компонента 3.

Таблиця 1 – Функціональні класи та сімейства стандарту ISO/IEC 15408-2

| Клас | Назва класу | Сімейства класу |
|---|---|---|
| FAU | Аудит безпеки | FAU_ARP – Автоматична реакція аудиту безпеки<br>FAU_GEN – Генерація даних аудиту безпеки<br>FAU_SAA – Аналіз аудиту безпеки<br>FAU_SAR – Перегляд аудиту безпеки<br>FAU_SEL – Вибір подій аудиту безпеки<br>FAU_STG – Зберігання даних аудиту безпеки |

Продовження табл.1

| Клас | Назва класу | Сімейства класу |
|---|---|---|
| FCO | Інформаційний обмін | FCO_NRO – Невідмовність відправлення<br>FCO_NRR – Невідмовність отримання |
| FCS | Криптографічна підтримка | FCS_CKM – Керування криптографічними ключами<br>FCS_COP – Криптографічні операції |
| FDP | Захист інформації користувача | FDP_ACC – Політика контролю доступу<br>FDP_ACF – Функції контролю доступу<br>FDP_DAU – Аутентифікація даних<br>FDP_ETC – Експорт у зовнішній контроль функцій безпеки об’єкта оцінки |

| | | |
|---|---|---|
| | | FDP_IFC – Політика контролю інформаційних потоків<br>FDP_IFF – Функції керування потоком інформації<br>FDP_ITC – Імпорт поза контролем функцій безпеки об’єкта оцінки<br>FDP_ITT – Внутрішня передача в межах об’єкта оцінки<br>FDP_RIP – Захист залишкової інформації<br>FDP_ROL – Відкат<br>FDP_SDI – Цілісність збережених даних<br>FDP_UCT – Захист конфіденційності передачі даних користувача між функціями безпеки об’єкта оцінки<br>FDP_UIT – Захист передачі цілісності даних користувача між функціями безпеки об’єкта оцінки |
| FIA | Ідентифікація й автентифікація | FIA_AFL – Помилки автентифікації<br>FIA_ATD – Визначення атрибута користувача<br>FIA_SOS – Специфікація секретів<br>FIA_UAU – Аутентифікація користувача<br>FIA_UID – Ідентифікація користувача<br>FIA_USB – Прив'язка користувач – суб’єкт |

Продовження табл.1

| Клас | Назва класу | Сімейства класу |
|---|---|---|
| FMT | Керування безпекою | FMT_MOF – Управління функціями в функціях безпеки об’єкта оцінки<br>FMT_MSA – Управління атрибутами безпеки<br>FMT_MTD – Управління даними функцій безпеки об’єкта оцінки<br>FMT_REV – Відкликання<br>FMT_SAE – Термін дії атрибута безпеки<br>FMT_SMR – Ролі керування безпекою |

| | | |
|---|---|---|
| FPR | Конфіденційність доступу до системи | FPR_ANO – Анонімність<br>FPR_PSE – Псевдонімність<br>FPR_UNL – Відключення<br>FPR_UNO – Неспостережливість |
| FRU | Контроль за використанням ресурсів | FRU_FLT – Відмовостійкість<br>FRU_PRS – Пріоритет обслуговування<br>FRU_RSA – Розподіл ресурсів |
| FTA | Контроль доступу до системи (об’єкта оцінки) | FTA_LSA – Обмеження області вибору атрибутів<br>FTA_MCS – Обмеження на декілька одночасних сеансів<br>FTA_SSL – Блокування сеансу<br>FTA_TAB – Банери доступу до об'єкта оцінки<br>FTA_TAH – Історія доступу до об'єкта оцінки<br>FTA_TSE – Відкриття сеансу з об'єктом оцінки |
| FTP | Забезпечення прямої взаємодії | FTP_ITC – Довірений канал передачі між функціями безпеки об'єкта оцінки<br>FTP_TRP – Довірений шлях |

Продовження табл.1

| Клас | Назва класу | Сімейства класу |
|---|---|---|
| FPT | Захист функцій безпеки | FPT_AMT – Тестування базової абстрактної машини<br>FPT_FLS – Безпека під час бою<br>FPT_ITA – Доступність експортованих даних функцій безпеки об'єкта оцінки<br>FPT_ITC – Конфіденційність експортованих даних функцій безпеки об'єкта оцінки |

| | | |
|---|---|---|
| | | FPT_ITI – Цілісність експортованих даних функцій безпеки об'єкта оцінки<br>FPT_ITT – Передача даних функцій безпеки об'єкта оцінки в рамках об'єкта оцінки<br>FPT_PHP – Фізичний захист функцій безпеки об'єкта оцінки<br>FPT_RCV – Надійне відновлення<br>FPT_RPL – Виявлення повторного відтворення<br>FPT_RVM – Посередництво при зверненнях<br>FPT_SEP – Розділення домену<br>FPT_SSP – Протокол синхронізації стану<br>FPT_STM – Позначки часу<br>FPT_TDC – Узгодженість даних функцій безпеки об'єкта оцінки з іншими функціями безпеки об'єкта оцінки<br>FPT_TRC – Узгодженість даних функцій безпеки об'єкта оцінки при дублюванні в рамках об'єкта оцінки<br>FPT_TST – Самотестування функцій безпеки об'єкта оцінки |

## 2.4 Методика оцінки захищеності інформаційних систем.

Для конкретної інформаційної системи не всі класи можуть знадобитися для оцінки захищеності. У програмній реалізації необхідні класи ми помічаємо на початку роботи з додатком.

Після того, як ми відмітили класи, необхідні нам для оцінки захищеності, нам необхідно провести процедуру ранжування класів за важливістю його вкладу в загальну оцінку.

Потім потрібно визначити вагові коефіцієнти та пронормувати їх. Обчислення вагових коефіцієнтів $C_i$ для кожного і-го класу безпеки відбувається за формулою: $C_i = 1 - \frac{R_i - 1}{M}$, де $R$ – ранг, а $M$ – число функціональних класів.

Далі проводимо нормування коефіцієнтів, використовуючи формулу: $C_k = \frac{C_i}{\sum_{i=1}^{M} C_i}$.

Наступним кроком для нас є проведення ранжування сімейств класів. Цей процес відбувається за наступною формулою: $F_i = 1 - \frac{R_i - 1}{M}$.

Нормування коефіцієнтів: $F_k = \frac{F_i}{\sum_{i=1}^{M} F_i}$.

У результаті виконання показників ми можемо отримати 3 різних поведінки: “–1” – якщо показник не виконано, “0” – якщо він не використовується і “1” – якщо показник виконано.

Наприклад, виконання показника FAU_GEN.2, що має пряму залежність від показників FAU_GEN.1 і FIA_UID.1 розраховуємо таким чином:

$$F_k = \frac{F_{FAU\_GEN} * w_{FAU\_GEN.1} + F_{FIA\_UID} * w_{FIA\_UID.1}}{F_{FAU\_GEN} + F_{FIA\_UID}}$$

Виконання показника FDP_ETC.2, що має вибіркову залежність між показниками FDP_ACC.1 або FDP_IFC.1 будемо рахувати за формулою:

$$F_k = max[F_{FDP\_ACC} * w_{FDP\_ACC.1} ; F_{FDP\_IFC} * w_{FDP\_IFC.1}]$$

Для розв’язування задачі оцінки захищеності інформаційної системи обрано метод результуючого показника, відповідно до якого визначається адитивний показник:

$$X_j = \sum_{k=1}^{n} C_k w_{kj},$$

де $0 \le C_j \le 1$ $\sum_{j=1}^{n} C_j = 1$, $C_j$ – ваговий коефіцієнт важливості j-го класу;

$w_{kj}$ – підсумковий показник по всім сімействам j-го класу

Підсумкова оцінка захищеності визначається за формулою:

$$Y = \sum_{j} X_j$$

Розроблена методика оцінки захищеності інформаційних систем має наступні кроки:

1. Визначення класів, що беруть участь в оцінці;
2. Ранжирування класів та розрахунок вагових коефіцієнтів класів;
3. Ранжирування сімейств кожного класу та розрахунок вагових коефіцієнтів сімейств;
4. Відмітка про виконання дій зазначених в компонентах кожного сімейства серед класів, що беруть участь в оцінці;
5. Формування матриці вагової функції по відміткам про виконання;
6. Розрахунок залежностей для кожної компоненти сімейства, якщо така залежність присутня у стандарті;
7. Розрахунок узагальнених показників по кожному класу;
8. Розрахунок підсумкової оцінки;
9. Розрахунок залежностей, узагальнених показників та підсумкової оцінки для класів, що беруть участь в оцінці в ситуації що стоять всі позитивні відмітки про виконання дій зазначених в компонентах кожного сімейства;
10. Порівняння результатів, отриманих на кроках 8 та 9 та формування рекомендацій по підвищенню захищеності інформаційної системи, що оцінюється.

# 3 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ

## 3.1 Мова програмування C#.

Для реалізації програмного продукту для оцінки захищеності інформаційної системи у якості мови програмування було обрано C#. Чому саме C#?

Взагалі існує багато мов програмування загального призначення, але розробники, безумовно, можуть погодитися з тим, що C# є однією із найкращих. Це, ймовірно, пов’язано з тим, що C# дуже універсальна, пропонує м’яке навчання та об’єктно-орієнтована.

Спочатку C# була розроблена для конкуренції з Java. Це сучасна мова програмування, яка дозволяє програмістам створювати програми, що працюють в екосистемі .NET. Як ви можете собі уявити, він має міцні зв’язки з сімейством мов C, тому будь-який інженер, який добре розуміє C і C++, безсумнівно не матиме проблем із розумінням C#.

З моменту свого першого випуску, понад 20 років тому, C# стабільно залишається однією з найпопулярніших мов у світі програмування.

C# – це мова програмування загального призначення з багатопарадигмальним підходом, який охоплює кілька дисциплін програмування, таких як статична типізація, імперативне, декларативне, функціональне, об’єктно-орієнтоване та компонентно-орієнтоване програмування. Саме такий підхід дозволяє C# бути настільки універсальною, що її можна використовувати для багатьох різних проектів.

Розроблений Microsoft у 2000 році, C# був створений для того, щоб задовольнити зростаючий попит на веб-додатки. Хоча компанія Redmond мала Visual Basic і C++ для роботи над цим типом програм, реальність була такою, що обидві мови мали проблеми з випуском високопродуктивного програмного забезпечення. Ось чому мова C# так швидко знайшла своє місце серед кращих

мов, оскільки її архітектура відповідає найкращим практикам Java, щоб забезпечити кращий підхід до розробки додатків.

Інші відмінні особливості C# включають його здатність повторно використовувати компоненти для швидшої розробки та гнучкі типи даних без помилок. Наче цього було недостатньо, C# має широкий спектр компонентів, які можуть легко підвищити розвиток будь-якого проекту, будь то системно-орієнтований чи бізнес-орієнтований.

Як мову програмування загального призначення, ви можете використовувати C# для розробки майже всього, що тільки ви можете придумати, від мобільних і настільних додатків до корпоративного програмного забезпечення та хмарних платформ.

Однак C# сяє найяскравіше, коли ви використовуєте цю мову для 3 конкретних типів проектів:

- веб-розробка – як частина платформи .NET, C# ідеально підходить для створення динамічних веб-сайтів і програм. Його об’єктно-орієнтована природа робить його ідеальним для розробки веб-сайтів, які мають високу ефективність і легко масштабуються.
- програми Windows – оскільки C# був розроблений Microsoft, цілком природно, що він широко використовується для створення настільних програм Windows. Насправді, це може бути найсильнішим варіантом використання цієї мови – створення програм, спеціально розроблених для архітектури ОС Microsoft.
- розробка комп’ютерних ігор – C# був широко визнаний як одна з найкращих мов програмування для ігор, особливо для ігор Unity. C# інтегрується з двигуном Unity, щоб забезпечити найкраще середовище для розробки ігор, і ви навіть можете використовувати його для розробки консольних ігор з кросплатформними технологіями, такими як Xamarin.

Універсальність мови програмування C# може бути найважливішою особливістю, але є багато інших переваг для тих, хто працює з нею. Деякі з найважливіших включають:

- швидший час розробки – C# має кілька функцій, які дозволяють розробникам кодувати швидше, ніж з іншими мовами. Деякі з цих функцій включають статично типізовану та зручну для читання мову, синтаксис, схожий на розширену версію Java, і величезну бібліотеку, наповнену функціональними можливостями високого рівня.
- висока масштабованість – Статична природа кодування C# перетворює всі його програми на надійні продукти, які можна легко налаштувати та змінити. Це означає, що інженери можуть швидко вносити корективи та надбудовувати будь-яку програму C#, щоб розширити її функціональні можливості та підтримати більше користувачів.
- об'єктно-орієнтованість – C# прийняв об'єктно-орієнтоване програмування таким чином, що ця мова може краще використовувати його. Насправді, об’єктно-орієнтованість дозволяє C# бути високоефективним і надзвичайно гнучким, що робить розробку легшою та менш ресурсомісткою.
- м’який поріг входження – як мова високого рівня, C# дуже легка для вивчення і розуміння. І це без урахування багатьох вбудованих функцій, які дуже прості у використанні. Більш того, будь-який програміст, який вже знає C++ або Java, почуватиметься як вдома, коли вперше використає C#, оскільки ці мови мають багато тих самих функцій і загальний підхід до програмування.
- велика громада – C# є однією з найбільш широко використовуваних мов у світі, а це означає, що є багато розробників C#, які готові допомогти вам. Це ще не все. Будучи продуктом Microsoft, C# має підтримку технологічного гіганта, що означає допомогу експертів, додаткові ресурси та часті оновлення.

Незважаючи на приголомшливий список переваг C#, вона має ряд недоліків, що ви повинні враховувати, перш ніж використовувати його для своїх проектів. До найбільш помітних належать:

- функціонує на базі Windows – оскільки C# є частиною екосистеми .NET, його програми майже виключно призначені для систем на базі Windows. Якщо ви вирішите працювати з іншою ОС, ви можете виявити, що деякі функції C# не працюють або недоступні.
- залежність від .NET – хоча C# є універсальним і може обслуговувати досить багато проектів, ця здатність має застереження: вам потрібна платформа .NET, щоб усе працювало безперебійно.
- неможливість кодування низькорівневих рішень – C# це мова високого рівня, що означає не тільки те, що підходи до синтаксису та кодування є більш абстрактними, але й те, що взаємодія продуктів C# з апаратним забезпеченням неможлива.

Також у процесі розробки було використано Chart. За допомогою цього елемента керування можна вирішувати графічні задачі на зразок побудови діаграми. Chart у ASP.NET пропонує широкий набір типів діаграм та параметрів конфігурації. Елемент управління Chart був доступний як завантажуваний додатково в .NET версії 3.5 SP1, але тепер входить до складу .NET 4.0.

Створений додаток у процесі роботи взаємодіє з файлами XML.

XML (Extensible Markup Language) – це мова розмітки, що схожа на HTML, але без попередньо визначених тегів. Замість цього ви визначаєте власні теги, розроблені спеціально для ваших потреб. Це потужний спосіб зберігання даних у форматі, який можна зберігати, шукати та ділитися ним. Найважливіше, оскільки основний формат XML стандартизований, якщо ви передаєте XML між системами чи платформами, локально або через Інтернет, одержувач все одно може аналізувати дані завдяки стандартизованому синтаксису XML.

Для взаємодії з файлом у мові програмування C# є кілька відмінних бібліотек. Але ми використовуємо простір імен System.XML. Дана бібліотека дозволяє читати, так і зберігати дані в файли XML.

## 3.2 Опис роботи розробленого програмного забезпечення

Спочатку необхідно запустити додаток. У діалоговому вікні, що відкрилося користувач бачить 2 пункти меню – “Standarts” та “Estimate”.

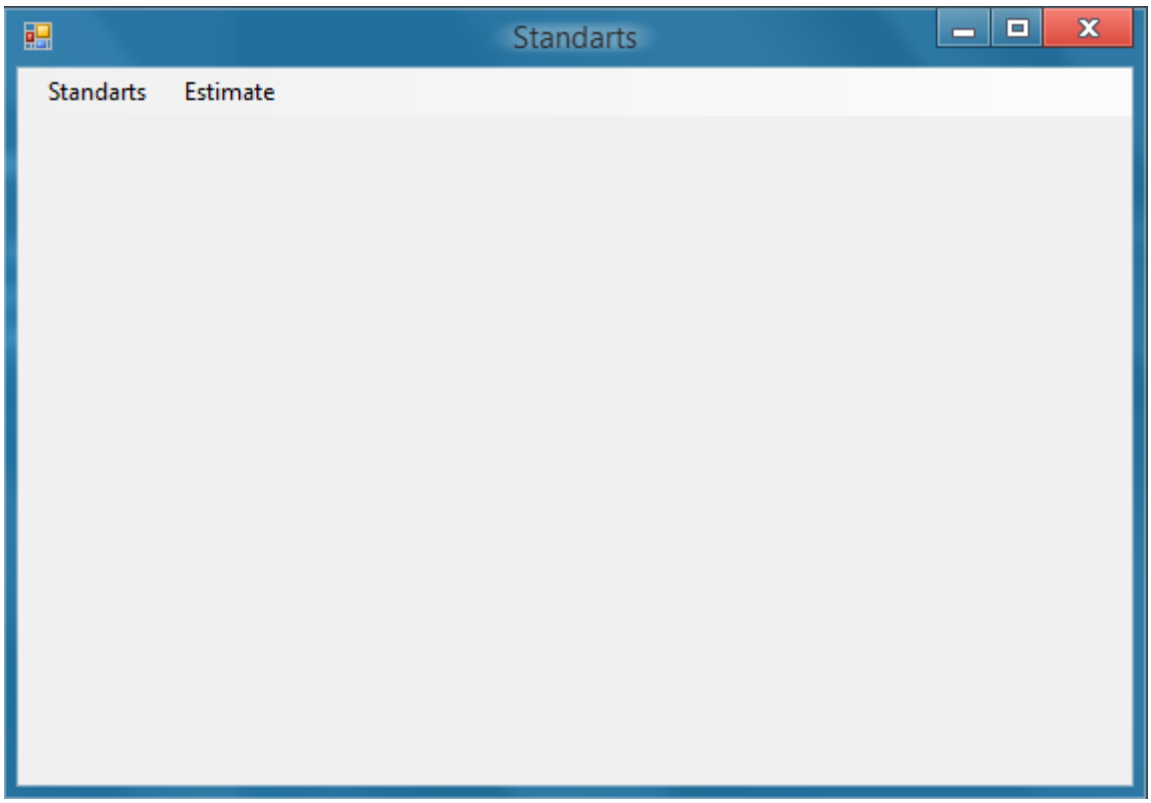


Рисунок 3.1 – Початкове вікно програми

Вкладка “Standarts” служить для вибору стандарта, з яким буде проводитись робота. Наразі ми працюємо зі стандартом ISO 15408, тому він вибраний за замовчуванням.

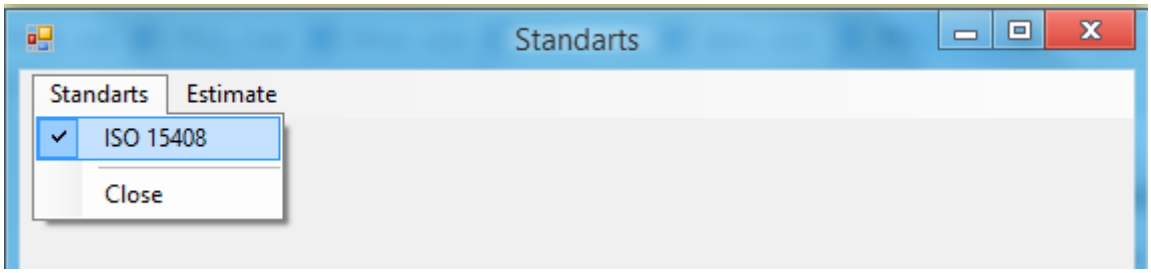


Рисунок 3.2 – Вибір стандарту

Після вибору стандарту користувач переходить до пункту меню “Estimate”. Він має вигляд як на рисунку 3.3.

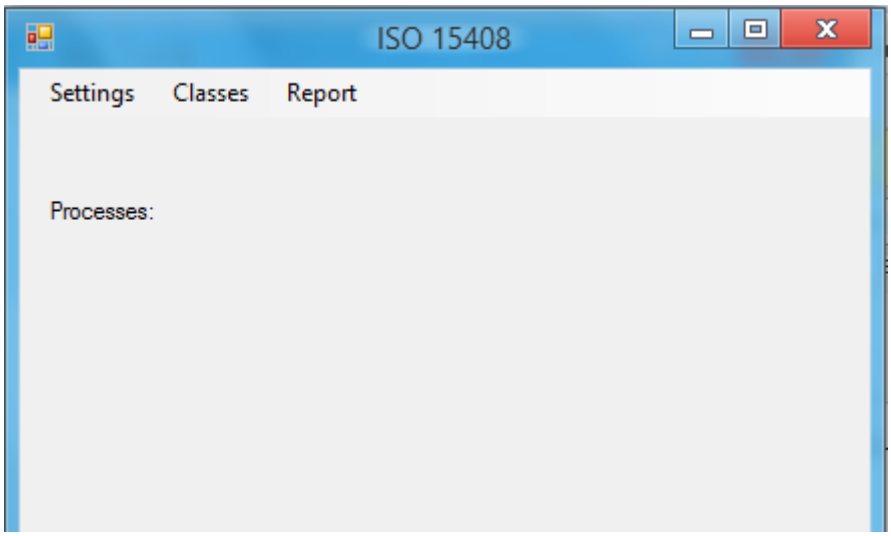


Рисунок 3.3 – Вікно “Estimate”

Спочатку необхідно виконати процедуру ранжування класів. Для цього необхідно перейти у пункт “Settings” та натиснути на кнопку “Rank classes”.

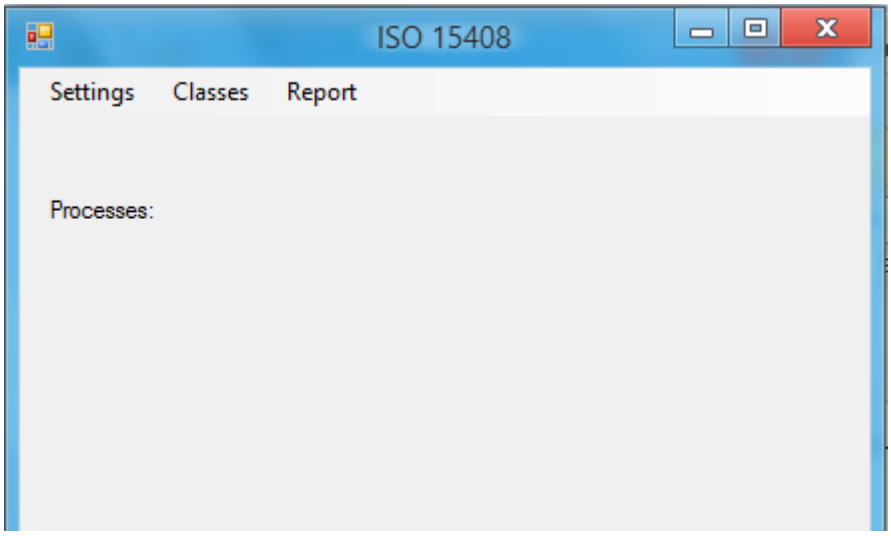


Рисунок 3.4 – Відкриття вікна ранжування класів

Відкривається діалогове вікно, у якому ми знаходимося у вкладці “Classes”.

За допомогою чекбоксів навпроти назви кожного класу, користувач відмічає класи, що є актуальними для нашої інформаційної системи. Щоб відмітити, що

конкретний клас не є актуальним для інформаційної системи необхідно зняти галочку навпроти конкретного класу й, у результаті, при розрахунку вагових коефіцієнтів, коефіцієнт даного класу буде дорівнювати 0.

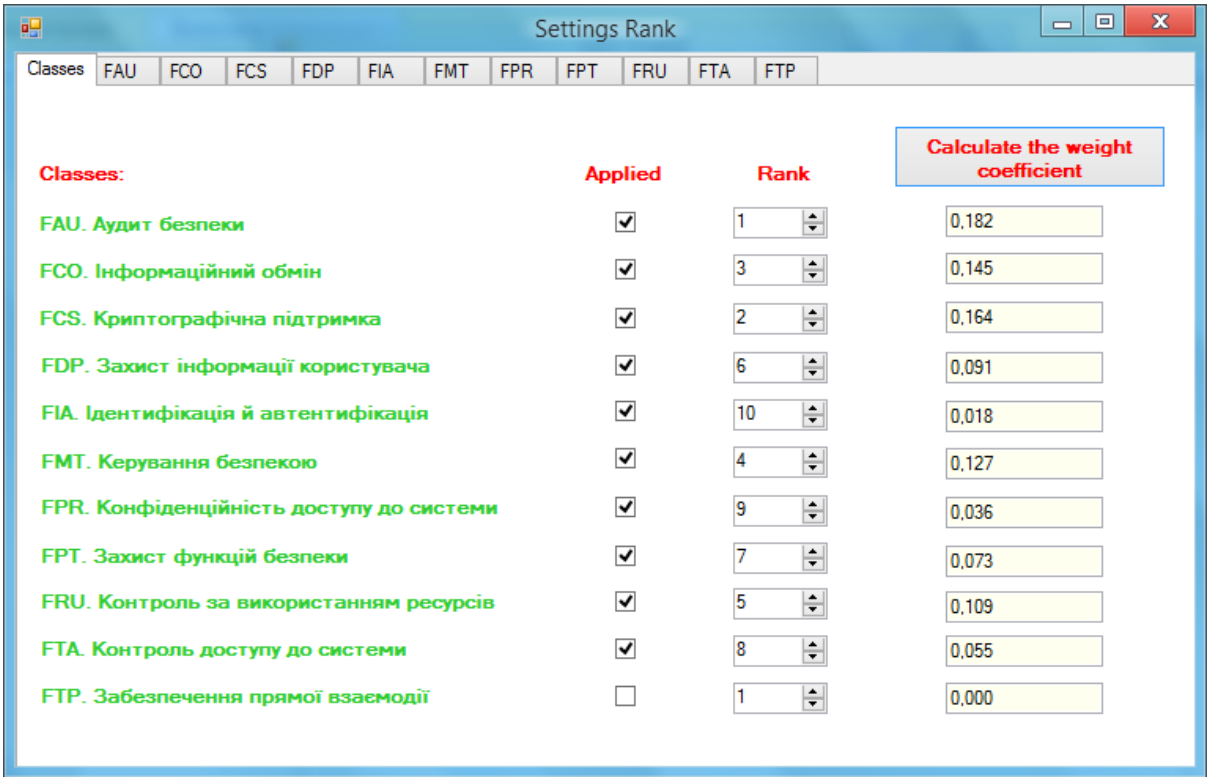


Рисунок 3.5 –Вікно ранжування класів

Користувач розставляє ранги для класів від 1 до 11. Вони означатимуть важливість вкладу кожного класу для загальної оцінки. Після цього необхідно натиснути кнопку “Calculate the weight coefficient” щоб отримати вагові коефіцієнти у відповідних полях .

Правіше від активної знаходяться вкладки для ранжування сімейств кожного класу. Це і буде наступним кроком.

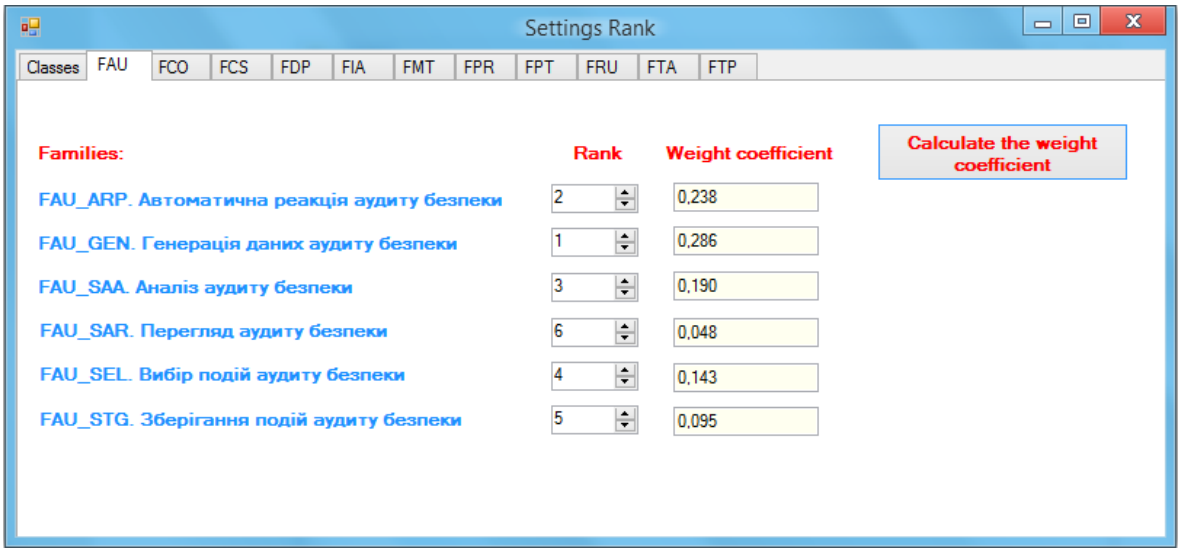


Рисунок 3.6 –Вікно ранжування сімейств класу FAU

Користувач обирає клас, наприклад – FAU та натискаємо на відповідну вкладку.

Дана вкладка має схожий інтерфейс управління. Спочатку необхідно проставити ранги кожного сімейства, а потім натиснути на кнопку “Calculate the weight coefficient”.

Сімейства усіх класів, що беруть участь в оцінюванні захищеності інформаційної системи мають бути також проранжовані, тому треба повторити дану процедуру з усіма класами, що є актуальними для конкретної інформаційної системи.

Далі користувач може закривати дане діалогове вікно. Результати пройдених кроків зберігаються для зручності. У будь-який момент можна повернутися до процедури ранжування та змінити вхідні дані для отримання інших вагових коефіцієнтів, або, якщо користувач не запам’ятав якусь інформацію зв’язану з ранжуванням.

Пункт меню “Classes” містить самі опитувальні листи, що містять конкретні вимоги для оцінки захищеності інформаційної системи. Користувач має пройти по всім опитувальним листам актуальних класів.

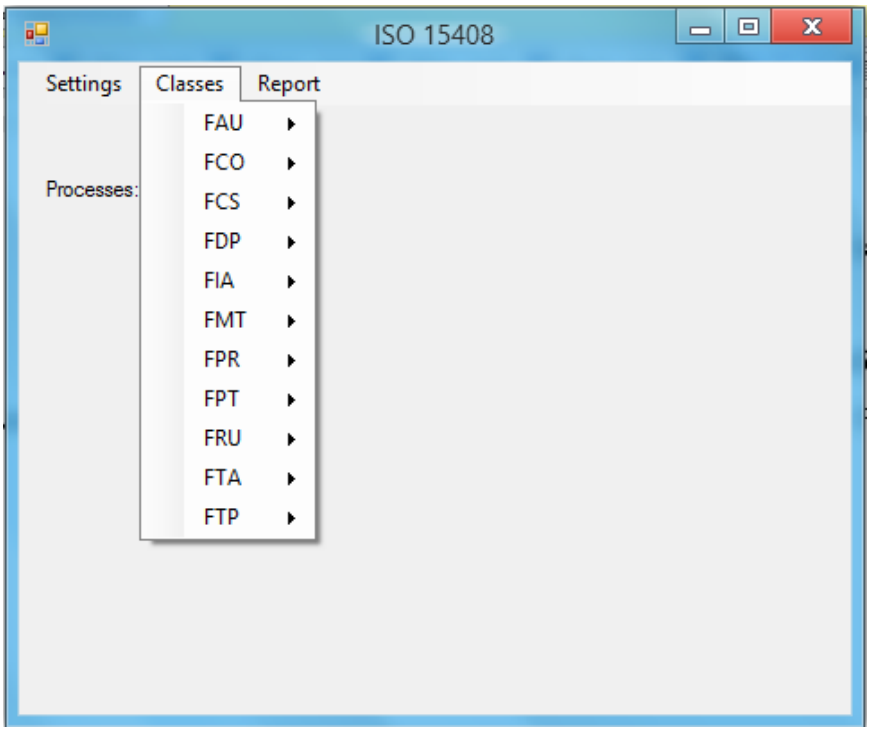


Рисунок 3.7 – Випадаючий список для вибору класу

Наводячи на назву класу, у випадаючому списку відображаються усі його сімейства. Користувач обирає клас та сімейство, наприклад – FAU_ARP.

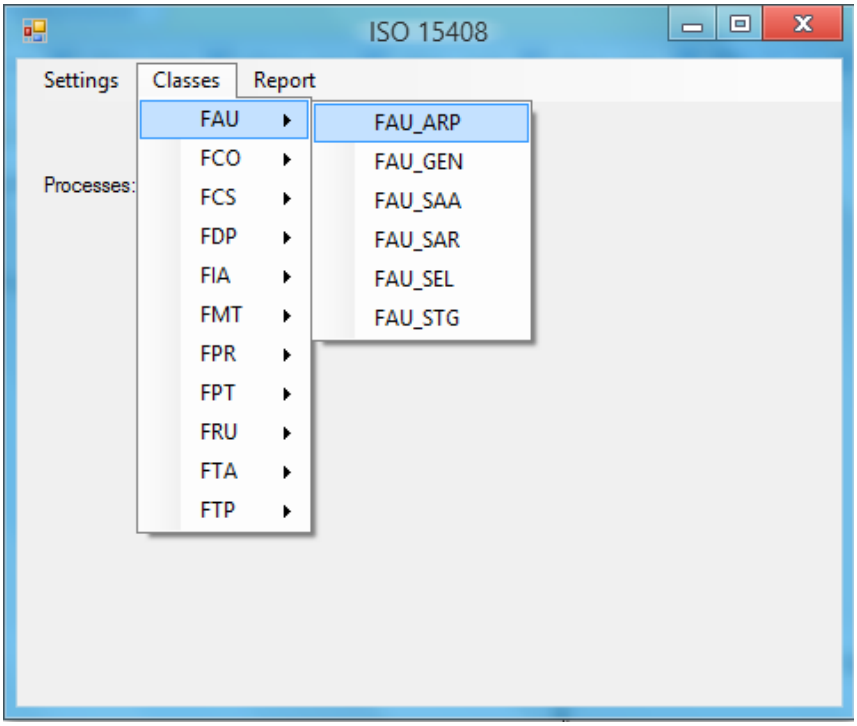


Рисунок 3.8 – Випадаючий список для вибору сімейства класу

Відкривається діалогове вікно, що містить інформацію про обраний клас, сімейство, кількість компонентів та конкретні вимоги до інформаційної системи. Користувач оцінює виконання вимоги відповідно до залежностей та ієрархічності компонентів та натискає на кнопку “Save results”.

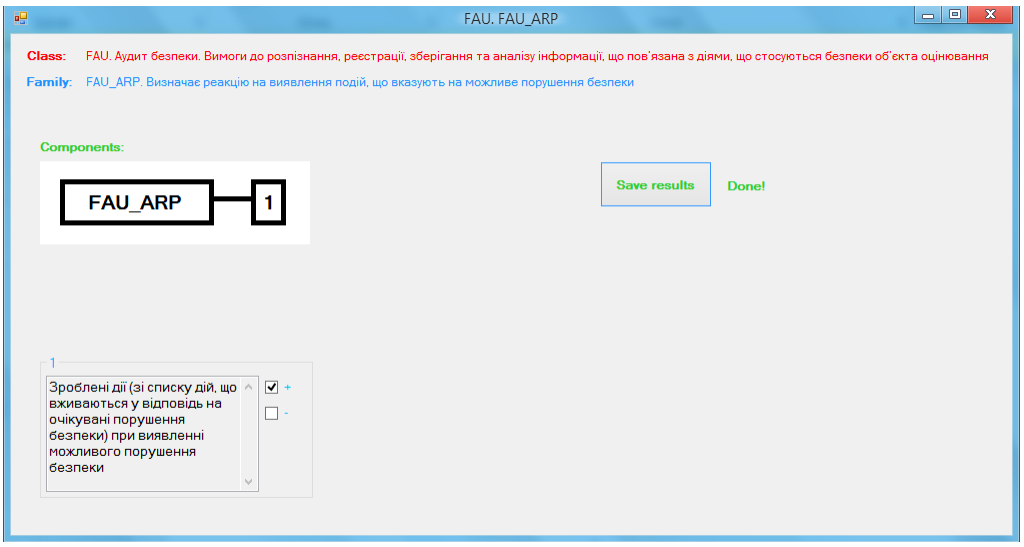


Рисунок 3.9 – Вікно для опитування

Користувач може відслідковувати, які сімейства класу були оцінені за допомогою історії переходів.

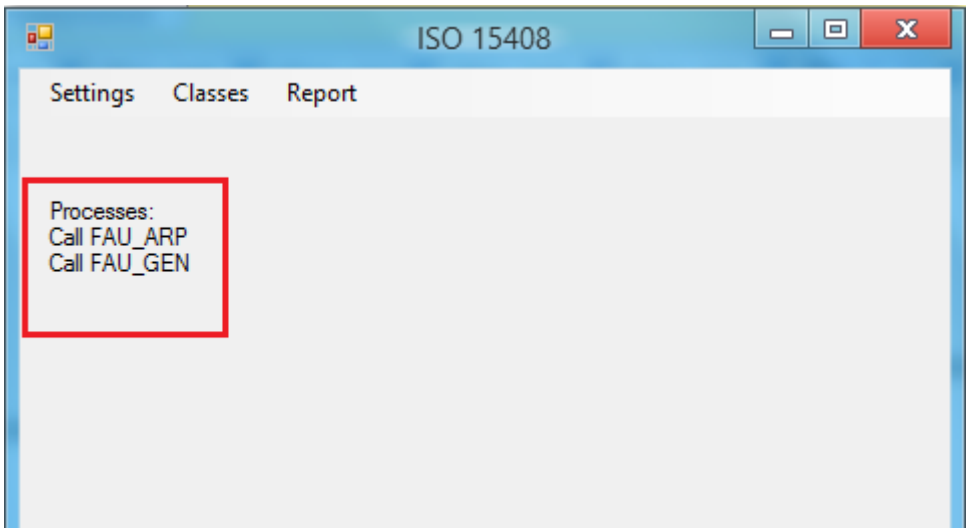


Рисунок 3.10 – Відображення історії переходів користувача

Після оцінки усіх класів, користувач натискає на вкладку “Report” та отримує оцінку захищеності конкретної інформаційної системи.

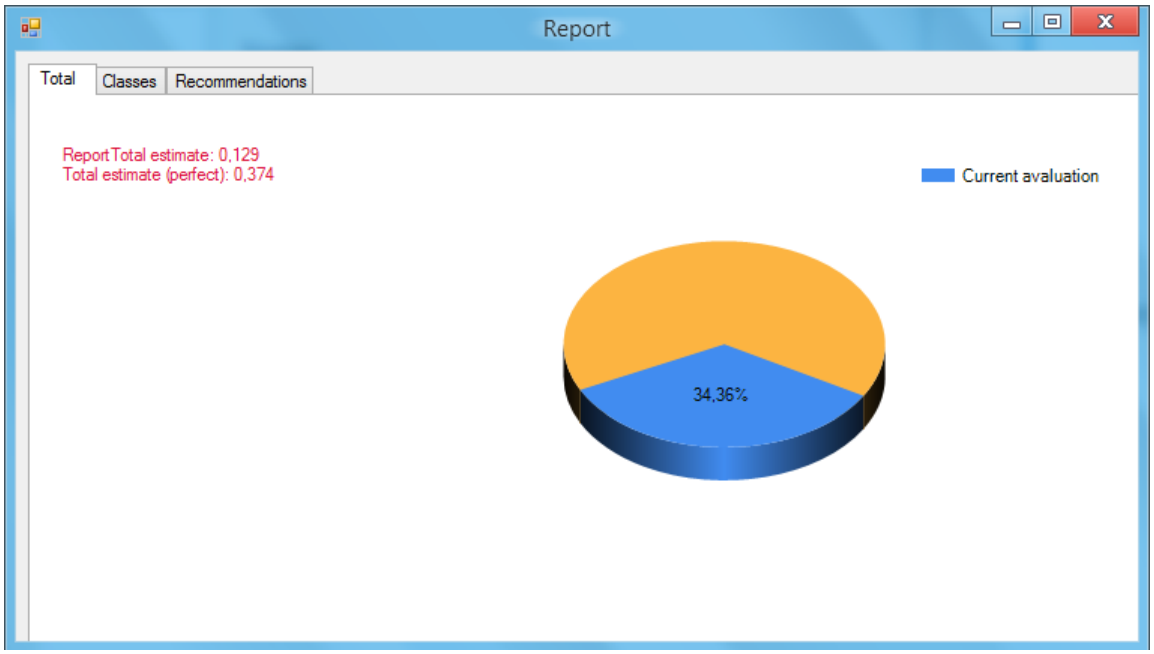


Рисунок 3.11 – Відображення результатів оцінювання

## 3.3 Структура XML-файлів.

Для зберігання інформації про введені ранги та вагові коефіцієнти для класів та сімейств класів та відповіді по компонентам для сімейств класів були розроблені два XML-файлу.

Формат xml відноситься до файлів мови розмітки, що розширюється. Являє собою звичайний текстовий документ, структура якого відображає опис документа та теги користувача. Приваблива особливість xml в тому, що він дозволяє прочитати і зрозуміти інформацію, що міститься, і для цього зовсім не обов'язково знати, в якій програмі файл створювався.

Подібний формат файлу зберігає найрізноманітніші види інформації. У форматі XML можуть міститися бази даних або певні налаштування програм. Застосування документа XML в Інтернеті, служить з метою обміну інформацією. Використовується мова розмітки, що розширюється, і для обміну даними між програмними комплексами.

Вміст XML-документа є набором елементів, секцій CDATA, директив аналізатора, коментарів, спецсимволів, текстових даних.

XML-документ може мати наступну структуру:

```
<?xml version="1.0" ?>
<кореневий_елемент>
     <елемент>
         Текст <елемент атрибут="значення" /> текст ...
     </елемент>
     Текст текст текст <елемент>текст текст... </елемент>  ...
</кореневий_елемент>
```

Для зберігання інформації про введені ранги та вагові коефіцієнтів класів та сімейств було розроблено XML-документ наступної структури:

```
<?xml version="1.0" encoding="UTF-8"?>
<settings>
  <classes>
    <class name="назва класу" mark="True або False" rank="число"
coef="число">
      <families>
        <family>
          <family_name>Назва сімейства</family_name>
          <family_rank>число</family_rank>
          <family_coef>число</family_coef>
        </family>
        … … … … … … …
      </families>
    </class>
  </classes>
</settings>
```

Для збереження та зчитування інформації з XML-файлу використовуються пункти меню “Open ranks” та “Save ranks” (рисунок 3.12).

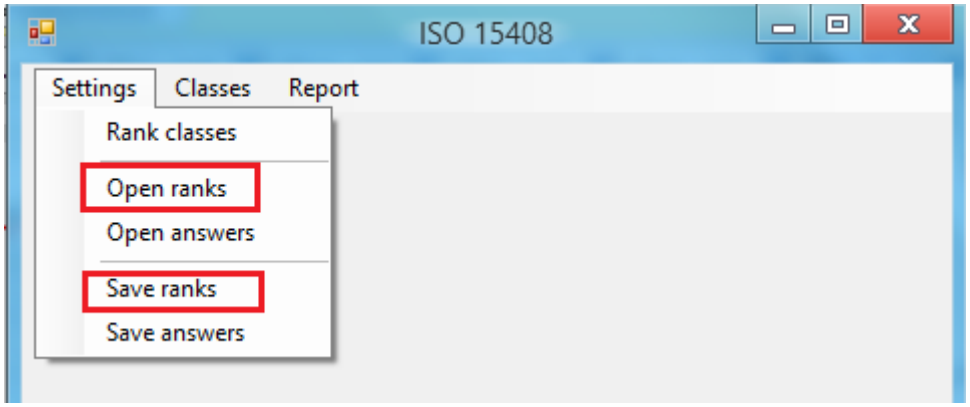


Рисунок 3.12 – Пункти меню для збереження інформації у вигляді XML-файлу

Для зберігання інформації про введені відповіді в компонентах сімейств було розроблено XML-документ наступної структури:

```
<?xml version="1.0" encoding="UTF-8"?>
<settings>
  <classes>
    <class name="Назва класу">
      <families>
        <family>
          <family_name>Назва сімейства</family_name>
          <num_component>Кількість компонент</num_component>
          <ans_component>відповідь 1 компонента; відповідь 2
компонента; … </ans_component>
        </family>
        … … … … … … …
      </families>
    </class>
  </classes>
</settings>
```

Для збереження та зчитування інформації з XML-файлу використовуються пункти меню “Open answers” та “Save answers”.

# 4 ОХОРОНА ПРАЦІ І БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Аналіз умов праці і вибір заходів і засобів захисту від небезпечних і шкідливих виробничих факторів.

Охорона праці – правові, соціально-економічні, організаційні, технічні, психофізичні, санітарно-гігієнічні, лікувально-профілактичні, реабілітаційні заходи, що створені для забезпечення безпеки життєдіяльності людини на підприємстві.

Метою охорони праці є організація безпеки життєдіяльності на робочому місці.

За умовами розробки методики захищеності інформаційної системи робочим місцем для спеціаліста з інформаційної безпеки є місце, обладнане персональним комп'ютером або ноутбуком.

Відомо, що комп'ютер створює певну небезпеку для здоров'я людини.

Ергономічні вимоги щодо робочого місця спеціаліста, що працює з комп'ютером викладені у серії стандартів ДСТУ ISO 9241 «Ергономічні вимоги до роботи з відео-терміналами в офісі».

Вимоги щодо забезпечення безпеки та здоров'я працівників під час роботи з екранними пристроями затверджені наказом Мінсоцполітики від 14.02.2018 № 207, що набули чинності 18 травня 2018 року й водночас втратили чинність Правила охорони праці під час експлуатації електронно-обчислювальних машин № 65 від 26.03.2010) та ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин».

Небезпечні та шкідливі виробничі фактори (НШВФ):

- відблиски від екрану комп'ютера;
- знижена або надлишкова яскравість зображення;
- мерехтіння зображення;
- іонізуючі випромінювання (дисплей);
- підвищений рівень шуму у робочому приміщенні;

- недостатня освітленість робочих поверхонь;
- психологічне та розумове перенапруження;
- підвищений рівень напруги в електричній мережі з імовірністю ураження електричним струмом.

Розглянемо детальніше найосновніші з НШВФ.

Іонізуюче та неіонізуюче випромінювання**.** Тема випромінювання є надзвичайно важливою, адже досі ведуться суперечки з приводу шкоди, що завдають людині випромінювання дисплеїв. Монітор є джерелом практично всіх видів електромагнітного випромінювання. Залежно від впливу на об'єкт, ці випромінювання, бувають іонізуючими і неіонізуючими. До іонізуючих відноситься рентгенівське випромінювання (діапазон частот 10нм – 0.01нм), до неіонізуючих – електромагнітне поле (випромінювання) наднизької (30-300Гц) і низької (30-300кГц) частоти.

Дослідження, що проводилися різними державами та виробниками інформаційного обладнання, свідчать, що рівень іонізуючого випромінювання при роботі з дисплеєм є суттєво нижчим за допустимий будь-яких національних стандартів безпеки. Загальна доза опромінювання при щоденній 8–годинній роботі становить 0,5 % дози, яку отримує людина від інших джерел (флюорографія, сонячне світло та ін.)

В Україні радіаційна безпека дисплеїв регламентується Нормами радіаційної безпеки України (НРБУ-97/Д-2000). Ними описано, що потужність експозиційної дози рентгенівського випромінювання на відстані 0,05 м від екрана та корпусу комп’ютера при будь-яких положеннях не повинна перевищувати 7,74·10–12 А/кг, що відповідає еквівалентній дозі 0,1 мбер/год (100 мкР/год)[4].

У підсумку варто сказати, що проблему випромінювання у данному випадку майже повністю вирішує дистанціювання від джерела хвиль та створення перерв у роботі.

Шум. Вплив шуму на організм людини залежить від рівня звукового тиску, частотних характеристик, тривалості дії, а також індивідуальних особливостей людини. Шум створює значне навантаження на нервову систему, причому шум,

що створюється самою людиною, її не турбує. Відсутність необхідної тиші, особливо у нічний час (нічні зміни), приводить до передчасної втоми, а часто і до захворювань. Підвищені рівні шуму при тривалій дії спричиняють швидку втому, погіршення самопочуття, зниження гостроти зору і врешті-решт за рахунок пере подразнення нервової системи викликають множинний розлад функцій внутрішніх органів (порушення кров'яного тиску, ритму серця та дихання, травлення та ін.) – «шумової» патології (віброшумове захворювання). Разом із тим надлишкова зашумленість приміщення заважає робочому процесу, порушуючи сконцентрованість та фокус уваги працівників.

Джерелами шуму в офісі можуть бути: принтери, комп'ютери (їх системи охолодження), кондиціонери та, звичайно ж, люди.

Допустимі рівні шуму нормуються ДСанПіН 3.3.2-007- 98, де вказано, що як нормативний рівень шуму в офісі запроваджено гранично допустимий рівень звуку 50 дБА, який забезпечує відсутність ризику втрати слуху і практично не впливає на працездатність та стан здоров'я.

Заходами для зниження впливу шуму на працівників є:

- зниження рівнів шуму в джерелі його утворення (при проектуванні);
- використання звукопоглинаючих та звукоізолюючих засобів;
- раціональне планування виробничих приміщень та робочих місць.

Для зниження рівнів шуму на робочих місцях з комп'ютерами друкуючі пристрої ударної дії розміщують в іншому приміщенні або застосовують звукоізолюючі екрани.

Зовнішні шуми знижують шляхом облицьовування стін звукопоглинаючими матеріалами. До засобів звукоізоляції належать звукоізолюючі відгородження , звукоізолюючі кабіни та пульти керування , звукоізолюючі кожухи та акустичні екрани.

Освітлення. Значний вплив на ефективність сприймання інформації має характер освітлення. Збільшення освітлення при прямому контрасті поліпшує умови сприймання інформації, оскільки яскравість фону зростає більше, ніж

яскравість об’єкта, а при зворотному контрасті – навпаки. Величина порогового контрасту залежить і від часу експозиції інформації.

Освітлення на робочому не має бути надлишковим або недостатнім. Є певні симптоми, що виникають після довгої роботи за комп’ютером. Серед них: головні болі, сухість та почервоніння очей, стомлюваність. Одним із основних негативних ефектів є часткова втрата зору. Для уникнення згубних впливів працівникам рекомендується робити перерви у роботі. Наразі багато компаній вже ввели обідні перерви, інтерактивні розваги персоналу, проведення корпоративів, спільні заняття у спортзалі та інші заходи, що допомагають зняти напругу з людини та покращити її емоційний стан.

Надлишкове освітлення може осліпити, викликати почервоніння, свербіння та різь у очах. Згідно з регламентоване ДСанПін 3.3.2.007-98 для правильної організації освітлення потрібно скомбінувати природне та штучне.

Раціональне виробниче освітлення повинне попереджати розвиток зорового і загального стомлення, забезпечувати психологічний комфорт при виконанні тих чи інших видів зорових робіт, сприяти збереженню працездатності, поліпшенню якості продукції, що випускається, зниженню виробничого травматизму, а також підвищенню безпеки праці. Нормований рівень освітленості на робочому столі – 300-500 лк.

При визначенні вимог до виробничого освітлення виходять з основних властивостей зору, а це передбачає створення таких умов, що виключають стомлення зору і виникнення причин виробничого травматизму та сприяють підвищенню продуктивності праці. Таким чином, основна задача освітлення на виробництві – створення найсприятливіших умов праці щодо зору[4].

Вимоги до освітлення:

- створювати на робочих місцях освітленість, що відповідає гігієнічним нормам;
- забезпечувати рівномірність і постійність рівня освітленості;
- не створювати на робочому місці різких і глибоких тіней;
- обмежувати пульсацію світлового потоку;

- не зменшувати необхідний контраст фону та об’єктів, зображених на екрані ЕОМ;
- застосувати на екрані ЕОМ найкращі за видимістю сполучення кольорів, а також чергувати фони.

Штучне освітлення приміщення з комп’ютерами має обладнуватися у вигляді загальної системи рівномірного освітлення. Допускається застосовувати світильники таких класів світлорозподілу: прямого світла, переважно прямого, переважно відбитого. Для штучного освітлення рекомендується застосовувати люмінесцентні лампи.

Для забезпечення відносної постійності природного освітлення необхідно вікна обкладати сонцезахисними регульованими жалюзі. Розташовувати робочі місця з комп’ютерами слід так, щоб у поле зору користувача не потрапляли вікна або світлі поверхні світильників. Окрім того, вони повинні знаходитися за його спиною, щоб уникнути відблисків на екрані.

Щоб зменшити пряму блискучість джерел природного та штучного освітлення яскравість їх поверхонь, що перебувають у полі зору та за спиною, не повинна перевищувати 200 кд/м2 , а яскравість виблисків на дисплеї – 40 кд/м2.

Потрібно унеможливити або мінімізувати відблиски від дисплея, адже вони є дуже небезпечними для зору людини. Цю проблему можна вирішити додатковим устаткуванням працівника – комп’ютерними окулярами, що завдяки спеціальним кольоровим фільтрам поглинають шкідливе світло.

Підвищений рівень напруги в електричній мережі з імовірністю ураження електричним струмом. Екрани на основі електронно-променевих трубок є джерелом електростатичних зарядів. Тривале перебування в такому електричному полі може бути причиною бронхо-легеневих захворювань, порушення серцево-судинної та нервової систем, ураження шкіри та ін. Ці заряди зосереджуються переважно на екрані монітора. Дія на користувача відбувається індуктивним або контактним шляхом, підвищуючи тим самим його електричний потенціал. Комп’ютери та інше устаткування,  електропроводи та кабелі за виконанням і

ступенем захисту мають відповідати класу зони за НПАОП 40.1-1.01-97, мати апаратуру захисту від струму короткого замикання та інших аварійних режимів.

Заходи щодо захисту від статичної електрики полягають у наступному :

– встановити нейтралізатори статичної електрики;

– підтримувати в приміщенні з екранами відносну вологість повітря не нижче 45–50 %;

– використовувати для покриття підлоги антистатичні матеріали і проводити вологе прибирання;

– протирати екран та робоче місце антистатичною серветкою;

– носити одяг, особливо першого шару, з натуральних матеріалів;

– кілька разів на день мити руки та обличчя водою, або торкатися заземлених металевих поверхонь.

Організація робочого місця.

Основним устаткуванням робочого місця є персональний комп'ютер або ноутбук, маніпулятор(комп'ютерна миша),клавіатура (якщо потрібна додаткова), робочий стіл, стілець (крісло).

Робоче місце повинно бути обладнаним відповідно до деяких вимог.

– Перш за все, стіл та стілець мають бути підібрані під працівника, а саме під його зріст.

– На робочому столі має бути простір. Ніщо не повинно заважати рухам під час роботи. Усі вкрай необхідні предмети мають бути легкодоступними. Це дуже важливо, тому що надлишкове захаращення робочого місця може призвести до певних травм або пошкодження працівником робочого обладнання.

– Монітор повинен бути встановленим не менш ніж на 50 см відстані від очей працівника.

– Стіл має бути оптимального розміру для роботи, тобто на ньому має вміщуватися все офісне обладнання та має бути простір для того, щоб робити робочі записи, розміщувати документи.

– Стілець або крісло мають забезпечувати можливість працівнику змінювати робочу позу та забезпечувати рівну посадку, щоб уникнути зайвого навантаження на хребет людини.

Площа робочого місця працівника має передбачати розміщення людини та всього обладнання, необхідного для роботи.

Одним із найважливіших аспектів є робоча поза, адже вона безпосередньо впливає на рівень втоми, що отримує працівник.

Опис правильної робочої пози працівника.

– Необхідно сидіти прямо, не сутулячись та спираючись на спинку крісла, що знизить навантаження на хребет і допоможе розслабитися.

– Поперек потрібно прогнути не назад, як робить більшість, а, навпаки, вперед.

– Руки мають бути розслабленими. Для цього можна тримати їх на підлокітниках крісла.

– Ступні маються лежати на підлозі або спеціальній підставці паралельно одна одній, або злегка розведеними в боки.

При дотриманні даної робочої пози можна уникнути швидкої стомлюваності.

Аналіз техногенних небезпек і вибір заходів і засобів забезпечення безпеки у надзвичайних ситуаціях.

Основною техногенною небезпекою у нашому випадку є пожежа, а природною – землетрус.

Розглянемо детальніше пожежну безпеку.

Пожежі у приміщеннях з ЕОМ можуть виникнути у разі: короткого замикання, перевантаження блоку живлення системного блоку, перегрівання тощо.

Згідно з ГОСТ 27331-87 можливу пожежу відносимо до класу Е, що визначає пожежі, що пов’язані з горінням електроустановок, тому що всі приміщення обладнані офісною технікою (комп’ютерами та іншим устаткуванням)

Для уникнення аварійних ситуацій, що можуть стати причинами пожежі потрібно:

- використовувати тільки справне обладнання. У разі виявлення несправності повідомити старшому за посадою працівнику.
- перед початком роботи перевіряти цілісність дротових з'єднань обладнання.
- звертати увагу на справність розетки.
- не використовувати трійники, не вмикати багато приладів у подовжувачі. краще не використовувати подовжувачі на робочому місці, щоб уникнути наявності дроту на підлозі.
- не переміщувати обладнання самотужки та без дозволу.
- оснащення приміщень приладами пожежної сигналізації;
- влаштування протипожежних перепон в системах вентиляції, опалювальних або кабельних комунікаціях;
- оснащення приміщень засобами пожежогасіння (порошковими та вуглекислотними вогнегасниками);
- оснащення приміщень автоматичними установками пожежогасіння (особливо – місць з великою кількістю електроприладів);
- проведення інструктажів з пожежної безпеки для персоналу.

На будь якому підприємстві є люди, відповідальні за проведення інструктажів працівникам з приводу пожежної безпеки. Усі працівники офісу мають бути проінформовані про їх дії при пожежі та про наявність аварійних виходів у будівлі.

Говорячи про землетрус потрібно мати на увазі, що основним уражаючим його фактором є пружні коливання земної поверхні. Саме вони руйнують будівлі, розривають трубопроводи, викликають зсуви ґрунту.

Кілька рекомендацій щодо безпеки під час землетрусів:

- необхідно намагатися зберігати спокій та пам'ятати, що найнебезпечнішими при землетрусі є ті предмети, що можуть впасти;
- якщо ви знаходитесь у малоповерховому будинку (до 2-го поверху) необхідно відразу за 25-30 секунд залишити та вийти на відкритий простір;

– якщо ви не можете залишити приміщення необхідно: вимкнути всі комунікації (світло, газ, воду); стати в прорізі дверей несучих стін (вони є стійкішими до коливань), біля внутрішньої капітальної стіни, під ліжком чи столом; необхідно пам’ятати, що найчастіше завалюються зовнішні стіни будинків; слід уникати місць біля вікон та важких предметів, які можуть перекинутися чи зрушити з місця; не поспішати до ліфтів чи сходів (під час землетрусу вони обвалюються найчастіше);

– після припинення підземних поштовхів покинути приміщення (ліфтом користуватись заборонено) та відійти на відкрите місце подалі від будинків і споруд, стовпів і ліній електропередач;

– опинившись у завалі, необхідно спокійно оцінити становище, надати собі першу допомогу, якщо вона потрібна; важливо подбати про встановлення зв’язку з тими, хто перебуває зовні завалу (голосом, стуком); людина без серйозних ушкоджень може зберігати життєздатність (без води і їжі) понад два тижні.

Дослідження працездатності спеціаліста з інформаційної безпеки.

Працездатність досліджуватимемо шляхом проведення теппінг-тесту.

Теппінг-тест – це нейропсихологічний тест, який досліджує рухове функціонування, зокрема, швидкість руху та латералізовану координацію.

Нервові процеси відображають загальну працездатність людини. Людина, яка має сильну нервову систему може витримати більш інтенсивний і тривалий тиск з боку подразників, ніж людина зі слабкою нервовою системою. Через слабку нервову систему стомлення внаслідок психічного або фізичного напруження виникає швидше, ніж за умови сильної.

Таблиця 2 – Діагностика властивостей нервової системи за психомоторними показниками о 8:00

| Номер поля | Проміжок часу, с | Кількість точок правою рукою $N$ | Темп руху правої руки $T$, точок/с | Кількість точок лівою рукою $N$ | Темп руху лівої руки $T$, точок/с |
|---|---|---|---|---|---|
| 1 | 0 – 5 | 39 | 7,8 | 35 | 7 |

| | | | | | |
|---|---|---|---|---|---|
| 2 | 6 – 10 | 29 | 5,8 | 32 | 6,4 |
| 3 | 11 – 15 | 32 | 6,4 | 30 | 6 |
| 4 | 16 – 20 | 27 | 5,4 | 24 | 4,8 |
| 5 | 21 – 25 | 31 | 6,2 | 24 | 4,8 |
| 6 | 26 – 30 | 24 | 4,8 | 29 | 5,8 |

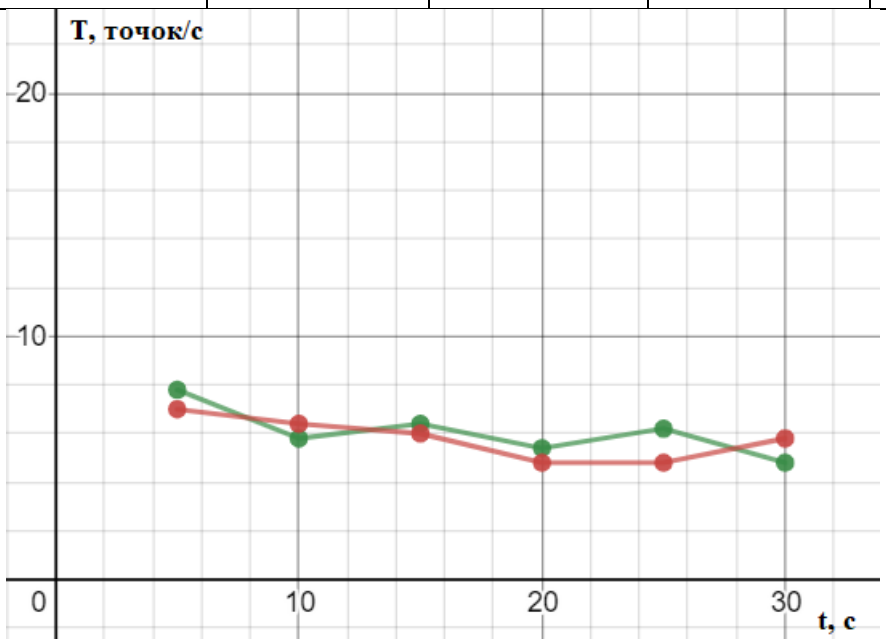


Рисунок 4.1 – Графік працездатності рук

На даному графіку зеленою лінією зображено динаміку працездатності правої руки, а червоною – лівої.

Коефіцієнт сили нервової системи для правої руки

$$K_{СНС}=\frac{(29-39)+(32-39)+(27-39)+(31-39)+(24-39)}{36} *100\% = -144.4\%$$

Коефіцієнт сили нервової системи для правої руки

$$K_{СНС}=\frac{(32-35)+(30-35)+(24-35)+(24-35)+(29-35)}{35} *100\% = -102.8\%$$

Коефіцієнт функціональної асиметрії працездатності лівої і правої рук:

$$K_{ФА}=\frac{182-174}{182+174} *100\% = 2.24\%$$

У результаті розбіжність графіків для правої та лівої рук не виявлена. Працездатність лівої руки є вищою ніж правої. Розряд і характеристика нервової системи належать до 5-ого розряду, характеристика якого – дуже висока вираженість сили або слабкості нервової системи.

Коефіцієнт функціональної асиметрії працездатності лівої і правої рук має знак “+”, що свідчить про зміщення балансу в бік збудження.

Визначення типу нервової системи за графіками працездатності правої та лівої рук. Обидва графіки є приблизно однаковими, мають рівний тип кривої: максимальний темп утримується приблизно на одному рівні протягом усього часу роботи. Цей тип кривої характеризує нервову систему досліджуваного як нервову систему стабільної середньої сили.

Таблиця 3 – Діагностика властивостей нервової системи за психомоторними показниками о 10:00

| Номер поля | Проміжок часу, с | Кількість точок правою рукою $N$ | Темп руху правої руки $T$, точок/с | Кількість точок лівою рукою $N$ | Темп руху лівої руки $T$, точок/с |
|---|---|---|---|---|---|
| 1 | 0 – 5 | 32 | 6,4 | 32 | 6,4 |
| 2 | 6 – 10 | 28 | 5,6 | 24 | 4,8 |
| 3 | 11 – 15 | 26 | 5,2 | 32 | 6,4 |
| 4 | 16 – 20 | 27 | 5,4 | 24 | 4,8 |
| 5 | 21 – 25 | 26 | 5,2 | 29 | 5,8 |
| 6 | 26 – 30 | 29 | 5,8 | 31 | 6,2 |

Таблиця 4 – Діагностика властивостей нервової системи за психомоторними показниками о 12:00

| Номер поля | Проміжок часу, с | Кількість точок правою рукою $N$ | Темп руху правої руки $T$, точок/с | Кількість точок лівою рукою $N$ | Темп руху лівої руки $T$, точок/с |
|---|---|---|---|---|---|
| 1 | 0 – 5 | 40 | 8 | 34 | 6,8 |
| 2 | 6 – 10 | 29 | 5,8 | 26 | 5,2 |
| 3 | 11 – 15 | 29 | 5,8 | 30 | 6 |

| | | | | | |
|---|---|---|---|---|---|
| 4 | 16 – 20 | 30 | 6 | 31 | 6,2 |
| 5 | 21 – 25 | 33 | 6,6 | 30 | 6 |
| 6 | 26 – 30 | 23 | 4,6 | 29 | 5,8 |

Таблиця 5 – Діагностика властивостей нервової системи за психомоторними показниками о 14:00

| Номер поля | Проміжок часу, с | Кількість точок правою рукою $N$ | Темп руху правої руки $T$, точок/с | Кількість точок лівою рукою $N$ | Темп руху лівої руки $T$, точок/с |
|---|---|---|---|---|---|
| 1 | 0 – 5 | 34 | 6,8 | 32 | 6,4 |
| 2 | 6 – 10 | 25 | 5 | 34 | 6,8 |
| 3 | 11 – 15 | 30 | 6 | 34 | 6,8 |
| 4 | 16 – 20 | 26 | 5,2 | 29 | 5,8 |
| 5 | 21 – 25 | 31 | 6,2 | 38 | 7,6 |
| 6 | 26 – 30 | 35 | 7 | 30 | 6 |

Таблиця 6 – Діагностика властивостей нервової системи за психомоторними показниками о 16:00

| Номер поля | Проміжок часу, с | Кількість точок правою рукою $N$ | Темп руху правої руки $T$, точок/с | Кількість точок лівою рукою $N$ | Темп руху лівої руки $T$, точок/с |
|---|---|---|---|---|---|
| 1 | 0 – 5 | 39 | 7,8 | 38 | 7,6 |
| 2 | 6 – 10 | 30 | 6 | 32 | 6,4 |
| 3 | 11 – 15 | 32 | 6,4 | 33 | 6,6 |
| 4 | 16 – 20 | 28 | 5,6 | 32 | 6,4 |
| 5 | 21 – 25 | 35 | 7 | 29 | 5,8 |
| 6 | 26 – 30 | 33 | 6,6 | 32 | 6,4 |

Таблиця 7 – Діагностика властивостей нервової системи за психомоторними показниками о 18:00

| Номер поля | Проміжок часу, с | Кількість точок правою рукою $N$ | Темп руху правої руки $T$, точок/с | Кількість точок лівою рукою $N$ | Темп руху лівої руки $T$, точок/с |
|---|---|---|---|---|---|
| 1 | 0 – 5 | 29 | 5,8 | 32 | 6,4 |
| 2 | 6 – 10 | 30 | 6 | 30 | 6 |
| 3 | 11 – 15 | 28 | 5,6 | 30 | 6 |
| 4 | 16 – 20 | 28 | 5,6 | 31 | 6,2 |
| 5 | 21 – 25 | 30 | 6 | 34 | 6,8 |
| 6 | 26 – 30 | 25 | 5 | 30 | 6 |

Таблиця 8 – Діагностика властивостей нервової системи за психомоторними показниками о 20:00

| Номер поля | Проміжок часу, с | Кількість точок правою рукою $N$ | Темп руху правої руки $T$, точок/с | Кількість точок лівою рукою $N$ | Темп руху лівої руки $T$, точок/с |
|---|---|---|---|---|---|
| 1 | 0 – 5 | 30 | 6 | 35 | 7 |
| 2 | 6 – 10 | 31 | 6,2 | 33 | 6,6 |
| 3 | 11 – 15 | 32 | 6,4 | 33 | 6,6 |
| 4 | 16 – 20 | 30 | 6 | 34 | 6,8 |
| 5 | 21 – 25 | 29 | 5,8 | 31 | 6,2 |
| 6 | 26 – 30 | 29 | 5,8 | 30 | 6 |

Таблиця 9 – Обробка результатів теппінг-тестів.

| Час виконання тесту | Середній темп руху правої руки Тср п, точок/с | Середній темп руху лівої руки Тср л, точок/с |
|---|---|---|
| 8:00 | 6,06 | 5,8 |
| 10:00 | 5,6 | 5,73 |
| 12:00 | 6,13 | 6 |
| 14.00 | 6,03 | 6,56 |
| 16.00 | 6,56 | 6,53 |
| 18.00 | 5,66 | 6,23 |
| 20.00 | 6,03 | 6,53 |

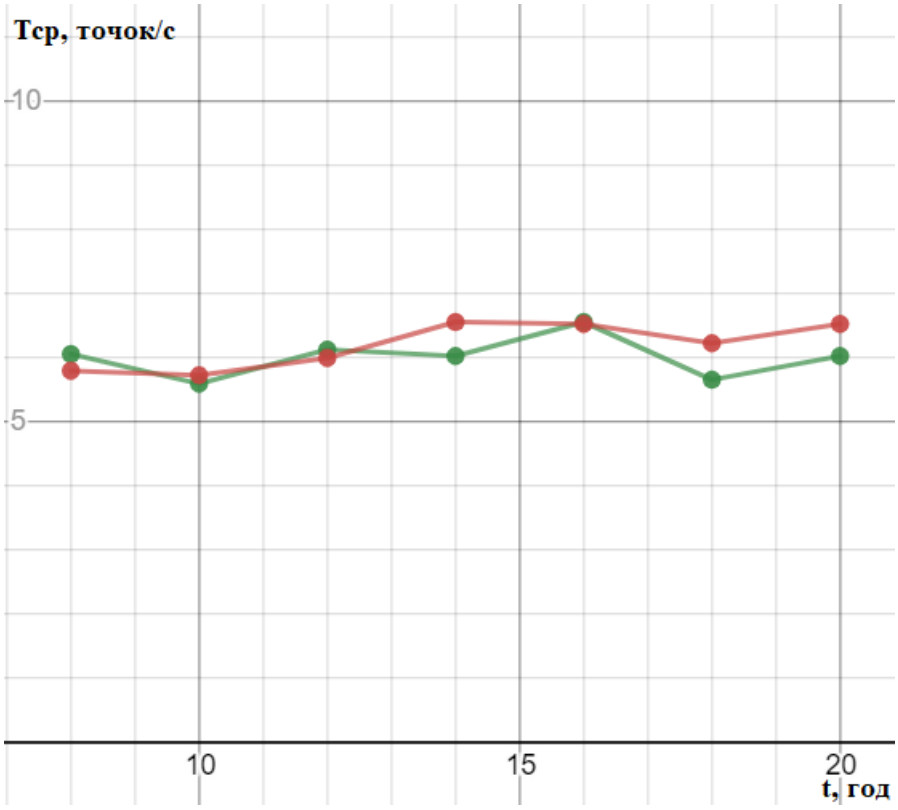


Рисунок 4.2 – Графік динаміки працездатності обох рук протягом дня

Підводячи підсумки результатів теппінг-тестів, що були проведені на протязі всього дня, можна сказати, що пік моєї продуктивності знаходиться у проміжку між 14:00 – 16:00 годинами, а також о 20:00 ввечері. Звичайно ж після 20:00 рівень працездатності швидко знижуватиметься. Планування робочого дня є дуже важливим і часто залежить від типу нервової системи людини. Тип моєї нервової системи – нервова система стабільної середньої сили, тому мені краще

розпочинати свій робочий день о 10:00 - 11:00 годині. Працездатність триматиметься приблизно на одному рівні до 20:00.

# ВИСНОВКИ

У першому розділі було розглянуто проблематику інформаційної безпеки. Виходячи із наданої в ньому інформації можна сказати, що потреби інформаційної системи безпеки будуть відрізнятися від додатку до додатку навіть у межах одного додатку. В результаті організації повинні як розуміти свої застосування, так і продумати відповідні варіанти для досягнення належного рівня безпеки. Потреби в безпеці визначаються більше тим, для чого використовується система, ніж тим, чим вона є.

У другому розділі розкривається тема стандартів у галузі інформаційної безпеки. Проаналізовано важливість наявності стандартів та використання їх для оцінки захищеності інформаційних систем. Описана розроблена методика оцінки захищеності інформаційних систем.

Третій розділ демонструє опис середовища розробки та програмну реалізацію додатку для оцінки захищеності інформаційної системи згідно з другою частиною стандарту ISO/IEC 15408.

У четвертому розділі кваліфікаційної роботи було проаналізовано умови праці та були визначені заходи і засоби захисту від небезпечних та шкідливих факторів на робочому місці. Також важливим було проаналізувати техногенні небезпеки, а саме пожежу та землетрус, та визначити засоби та заходи захисту у надзвичайних ситуаціях. Було досліджено працездатність спеціаліста з інформаційної безпеки. Дослідження було проведено з використанням теппінг тесту – засобу, що допомагає вивчити нервову систему людини.

# ПЕРЕЛІК ПОСИЛАНЬ


1. Information System. URL: https://www.britannica.com/topic/information-system
2. Bourgeois D., Bourgeois D.T. Information Systems Security. URL: https://bus206.pressbooks.com/chapter/chapter-6-information-systems-security/
3. Information Systems Security. URL: https://www.sciencedirect.com/science/article/pii/S1877050914006528
4. Березуцький В.В., Васьковец Л.А., Горбенко В.В., В.Ф. Райко В.Ф., Янчик О.Г. Основи професійної безпеки та здоров'я людини. Харків: НТУ "ХПІ", 2018. 553с.
5. RiskWatch Official Website. URL: http://www.riskwatch.com
6. COBRA Tool Identity Card. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_cobra.html
7. CRAMM Tool Identity Card. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_cramm.html
8. A tour of the C# language. URL: https://docs.microsoft.com/en-us/dotnet/csharp/tour-of-csharp/
9. ISO/IEC 15408-2. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components. URL: https://www.iso.org/standard/46414.html
10. Что такое XML. URL: https://habr.com/ru/post/524288/
11. Cyber Security Standarts. URL: https://www.educba.com/cyber-security-standards/
12. Введение в C#. URL: https://metanit.com/sharp/tutorial/1.1.php
13. Руководство по C# - Часть 1 URL: https://professorweb.ru/my/csharp/charp_theory/level1/index.php\
14. Cyber Security Threats and Attacks: All You Need to Know. URL: https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/

15. Руководство по C# - Часть 2 URL: https://professorweb.ru/my/csharp/charp_theory/level1/index1.php
16. Управление рисками. Метод CRAMM. URL: https://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf
17. CRAMM – Wikipedia. URL: https://en.wikipedia.org/wiki/CRAMM
18. Information Technology Risk Assessment Methodologies: Current Status and Future Directions. URL: https://www.ijser.org/researchpaper/Information-Technology-Risk-Assessment-Methodologies.pdf
19. Угрозы информационной безопасности. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/
20. Information System (IS). URL: https://www.techopedia.com/definition/24142/information-system-is
21. The risk assessment of information system security. URL: https://cuc.carnet.hr/cuc2004/program/radovi/a5_baca/a5_full.pdf
22. Для чего нужны политики информационной безопасности? URL: https://searchinform.ru/products/kib/politiki-informatsionnoj-bezopasnosti/
23. What is Cyber Threat? URL: https://www.upguard.com/blog/cyber-threat
24. CRAMM Version 5.1 User Guide; Insight Consulting: 2005. URL: https://pdfcoffee.com/cramm-version-51-userguide-pdf-free.html
25. Information System. URL: https://en.wikipedia.org/wiki/Information_system#:~:text=An%20information%20system%20(IS)%20is,%2C%20store%2C%20and%20distribute%20information.&text=A%20computer%20information%20system%20is,that%20processes%20or%20interprets%20information.
26. Chapter 1: What Is an Information System? URL: https://bus206.pressbooks.com/chapter/chapter-1/
27. What Are Information Systems? URL: https://saylordotorg.github.io/text_business-information-systems-design-an-app-for-that/s05-01-what-are-information-systems.html

28. Угрозы безопасности информации. URL: https://data-sec.ru/public/protect/information-threats/
29. Классификация угроз информационной безопасности. URL:https://rvision.pro/blog-posts/klassifikatsiya-ugroz-informatsionnoj-bezopasnosti/
30. What Are Cyber Threats and What to Do About Them. URL: https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/
31. Cyber Threat Source Descriptions. URL: https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions
32. ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT. URL: https://www.iso.org/isoiec-27001-information-security.html
33. ISO/IEC Standard 13335. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-13335
34. Политика информационной безопасности. URL: https://softline.ru/about/politika-informatsionnoy-bezopasnosti
35. Политика информационной безопасности — опыт разработки и рекомендации. URL: https://habr.com/ru/post/174489/
36. Standards for IT and cyber security. URL: https://www.bsigroup.com/en-GB/Cyber-Security/Standards-for-IT-and-cyber-security/#:~:text=ISO%2FIEC%2027001%20is%20used,for%20information%20and%20cyber%20security.&text=information%20security%20controls-,This%20standard%20is%20the%20latest%20version%20of%20the%20world's%20leading,specification%20of%20information%20security%20controls.
37. ISO Information Security Standard – 27001. URL: https://www.insightsassociation.org/get-support/iso-information-security-standard-27001
38. STANDARDS & GUIDELINES. URL: https://oneit.charlotte.edu/security/standards-guidelines

39. Five standardization bodies security professionals need to know. URL: https://resources.infosecinstitute.com/topic/5-standardization-bodies-security-professionals-need-know/
40. C# Programming Language. URL: https://www.geeksforgeeks.org/csharp-programming-language/
41. Learn C# Programming. URL: https://www.programiz.com/csharp-programming
42. Working with C#. URL: https://code.visualstudio.com/docs/languages/csharp

# ДОДАТОК А. Таблиці залежностей сімейств класів в стандарті ISO/IEC 15408

| | FAU_GEN.1 | FAU_SAA.1 | FAU_SAR.1 | FAU_STG.1 | FIA_UID.1 | FMT_MTD.1 | FMT_SMF.1 | FMT_SMR.1 | FPT_STM.1 |
|---|---|---|---|---|---|---|---|---|---|
| FAU_ARP.1 | - | x | | | | | | | - |
| FAU_GEN.1 | | | | | | | | | x |
| FAU_GEN.2 | x | | | | x | | | | - |
| FAU_SAA.1 | x | | | | | | | | - |
| FAU_SAA.2 | | | | | x | | | | |
| FAU_SAA.3 | | | | | | | | | |
| FAU_SAA.4 | | | | | | | | | |
| FAU_SAR.1 | x | | | | | | | | - |
| FAU_SAR.2 | - | | x | | | | | | - |
| FAU_SAR.3 | - | | x | | | | | | - |
| FAU_SEL.1 | x | | | | - | x | - | - | - |
| FAU_STG.1 | x | | | | | | | | - |
| FAU_STG.2 | x | | | | | | | | - |
| FAU_STG.3 | - | | | x | | | | | - |
| FAU_STG.4 | - | | | x | | | | | - |

Рисунок А.1 – Залежності класу FAU

| | FIA_UID.1 |
|---|---|
| FCO_NRO.1 | x |
| FCO_NRO.2 | x |
| FCO_NRR.1 | x |
| FCO_NRR.2 | x |

Рисунок А.2 – Залежності класу FCO

| | FCS_CKM.1 | FCS_CKM.2 | FCS_CKM.4 | FCS_COP.1 | FDP_ACC.1 | FDP_ACF.1 | FDP_IFC.1 | FDP_IFF.1 | FDP_ITC.1 | FDP_ITC.2 | FIA_UID.1 | FMT_MSA.1 | FMT_MSA.3 | FMT_SMF.1 | FMT_SMR.1 | FPT_TDC.1 | FTP_ITC.1 | FTP_TRP.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FCS_CKM.1 | - | O | x | O | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| FCS_CKM.2 | O | - | x | - | - | - | - | - | O | O | - | - | - | - | - | - | - | - |
| FCS_CKM.3 | O | - | x | - | - | - | - | - | O | O | - | - | - | - | - | - | - | - |
| FCS_CKM.4 | O | - | - | - | - | - | - | - | O | O | - | - | - | - | - | - | - | - |
| FCS_COP.1 | O | - | x | - | - | - | - | - | O | O | - | - | - | - | - | - | - | - |

Рисунок А.3 – Залежності класу FCS

| | FDP_ACC.1 | FDP_ACF.1 | FDP_IFC.1 | FDP_IFF.1 | FDP_ITT.1 | FDP_ITT.2 | FDP_UIT.1 | FIA_UID.1 | FMT_MSA.1 | FMT_MSA.3 | FMT_SMF.1 | FMT_SMR.1 | FPT_TDC.1 | FTR_ITC.1 | FTP_TRP.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FDP_ACC.1 | - | x | - | - | | | | - | - | - | - | - | | | |
| FDP_ACC.2 | - | x | - | - | | | | - | - | - | - | - | | | |
| FDP_ACF.1 | x | - | - | - | | | | - | - | x | - | - | | | |
| FDP_DAU.1 | | | | | | | | | | | | | | | |
| FDP_DAU.2 | | | | | | | | x | | | | | | | |
| FDP_ETC.1 | O | - | O | - | | | | - | - | - | - | - | | | |
| FDP_ETC.2 | O | - | O | - | | | | - | - | - | - | - | | | |
| FDP_IFC.1 | - | - | - | x | | | | - | - | - | - | - | | | |
| FDP_IFC.2 | - | - | - | x | | | | - | - | - | - | - | | | |
| FDP_IFF.1 | - | - | x | - | | | | - | - | x | - | - | | | |
| FDP_IFF.2 | - | - | x | - | | | | - | - | x | - | - | | | |
| FDP_IFF.3 | - | - | x | - | | | | - | - | - | - | - | | | |
| FDP_IFF.4 | - | - | x | - | | | | - | - | - | - | - | | | |
| FDP_IFF.5 | - | - | x | - | | | | - | - | - | - | - | | | |
| FDP_IFF.6 | - | - | x | - | | | | - | - | - | - | - | | | |
| FDP_ITC.1 | O | - | O | - | | | | - | - | x | - | - | | | |
| FDP_ITC.2 | O | - | O | - | | | | - | - | - | - | - | x | O | O |
| FDP_ITT.1 | O | - | O | - | | | | - | - | - | - | - | | | |
| FDP_ITT.2 | O | - | O | - | | | | - | - | - | - | - | | | |
| FDP_ITT.3 | O | - | O | - | x | | | - | - | - | - | - | | | |
| FDP_ITT.4 | O | - | O | - | | x | | - | - | - | - | - | | | |
| FDP_RIP.1 | | | | | | | | | | | | | | | |
| FDP_RIP.2 | | | | | | | | | | | | | | | |
| FDP_ROL.1 | O | - | O | - | | | | - | - | - | - | - | | | |
| FDP_ROL.2 | O | - | O | - | | | | - | - | - | - | - | | | |
| FDP_SDI.1 | | | | | | | | | | | | | | | |
| FDP_SDI.2 | | | | | | | | | | | | | | | |
| FDP_UCT.1 | O | - | O | - | | | | - | - | - | - | - | | O | O |
| FDP_UIT.1 | O | - | O | - | | | | - | - | - | - | - | | O | O |
| FDP_UIT.2 | O | - | O | - | | | O | - | - | - | - | - | | O | - |
| FDP_UIT.3 | O | - | O | - | | | O | - | - | - | - | - | | O | - |

Рисунок А.4 – Залежності класу FDP

| | FIA_ATD.1 | FIA_UAU.1 | FIA_UID.1 |
|---|---|---|---|
| FIA_AFL.1 | | x | - |
| FIA_ATD.1 | | | |
| FIA_SOS.1 | | | |
| FIA_SOS.2 | | | |
| FIA_UAU.1 | | | x |
| FIA_UAU.2 | | | x |
| FIA_UAU.3 | | | |
| FIA_UAU.4 | | | |
| FIA_UAU.5 | | | |
| FIA_UAU.6 | | | |
| FIA_UAU.7 | | x | - |
| FIA_UID.1 | | | |
| FIA_UID.2 | | | |
| FIA_USB.1 | x | | |

Рисунок А.5 – Залежності класу FIA

| | FDP_ACC.1 | FDP_ACF.1 | FDP_IFC.1 | FDP_IFF.1 | FIA_UID.1 | FMT_MSA.1 | FMT_MSA.3 | FMT_MTD.1 | FMT_SMF.1 | FMT_SMR.1 | FPT_STM.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FMT_MOF.1 | | | | | - | | | | x | x | |
| FMT_MSA.1 | O | - | O | - | - | - | - | | x | x | |
| FMT_MSA.2 | O | - | O | - | - | x | - | | - | x | |
| FMT_MSA.3 | - | - | - | - | - | x | - | | - | x | |
| FMT_MSA.4 | O | - | O | - | - | - | - | | - | - | |
| FMT_MTD.1 | | | | | - | | | | x | x | |
| FMT_MTD.2 | | | | | - | | | x | - | x | |
| FMT_MTD.3 | | | | | - | | | x | - | - | |
| FMT_REV.1 | | | | | - | | | | | x | |
| FMT_SAE.1 | | | | | - | | | | | x | x |
| FMT_SMF.1 | | | | | | | | | | | |
| FMT_SMR.1 | | | | | x | | | | | | |
| FMT_SMR.2 | | | | | x | | | | | | |
| FMT_SMR.3 | | | | | - | | | | | x | |

Рисунок А.6 – Залежності класу FMT

| | FIA_UID.1 | FPR_UNO.1 |
|---|---|---|
| FPR_ANO.1 | | |
| FPR_ANO.2 | | |
| FPR_PSE.1 | | |
| FPR_PSE.2 | X | |
| FPR_PSE.3 | | |
| FPR_UNL.1 | | |
| FPR_UNO.1 | | |
| FPR_UNO.2 | | |
| FPR_UNO.3 | | X |
| FPR_UNO.4 | | |

Рисунок А.7 – Залежності класу FPR

| | AGD_OPE.1 | FIA_UID.1 | FMT_MOF.1 | FMT_SMF.1 | FMT_SMR.1 | FPT_ITT.1 |
|---|---|---|---|---|---|---|
| FPT_FLS.1 | | | | | | |
| FPT_ITA.1 | | | | | | |
| FPT_ITC.1 | | | | | | |
| FPT_ITI.1 | | | | | | |
| FPT_ITI.2 | | | | | | |
| FPT_ITT.1 | | | | | | |
| FPT_ITT.2 | | | | | | |
| FPT_ITT.3 | | | | | | x |
| FPT_PHP.1 | | | | | | |
| FPT_PHP.2 | | - | x | - | - | |
| FPT_PHP.3 | | | | | | |
| FPT_RCV.1 | x | | | | | |
| FPT_RCV.2 | x | | | | | |
| FPT_RCV.3 | x | | | | | |
| FPT_RCV.4 | | | | | | |
| FPT_RPL.1 | | | | | | |
| FPT_SSP.1 | | | | | | x |
| FPT_SSP.2 | | | | | | x |
| FPT_STM.1 | | | | | | |
| FPT_TDC.1 | | | | | | |
| FPT_TEE | | | | | | |
| FPT_TRC.1 | | | | | | x |
| FPT_TST.1 | | | | | | |

Рисунок А.8 – Залежності класу FPT

| | FPT_FLS.1 |
|---|---|
| FRU_FLT.1 | x |
| FRU_FLT.2 | x |
| FRU_PRS.1 | |
| FRU_PRS.2 | |
| FRU_RSA.1 | |
| FRU_RSA.2 | |

Рисунок А.9 – Залежності класу FRU

| | FIA_UAU.1 | FIA_UID.1 |
|---|---|---|
| FTA_LSA.1 | | |
| FTA_MCS.1 | | x |
| FTA_MCS.2 | | x |
| FTA_SSL.1 | x | - |
| FTA_SSL.2 | x | - |
| FTA_SSL.3 | | |
| FTA_TAB.1 | | |
| FTA_TAH.1 | | |
| FTA_TSE.1 | | |

Рисунок А.10 – Залежності класу FTA