Techniques and tools
for evaluation of IT security assurance
Training

A. Lenshin, O. Illiashenko, A.Potii
Edited by V.S. Kharchenko

Methodology and techniques of security assurance case

Tools for security assurance case

Assurance case for industry systems

Assurance case for standard IEC15408

Techniques and tools for evaluation of IT security assurance. Training

Tempus
2013 SEREIN 2016

TRAINING

TECHNIQUES AND TOOLS FOR EVALUATION OF IT SECURITY ASSURANCE

2017

Co-funded by the
Tempus Programme
of the European Union

Міністерство освіти та науки України
Національний аерокосмічний університет
ім. Н.Е. Жуковского «ХАІ»

А. В. Лєншин, О. О. Ілляшенко, О. В. Потій

Методи та засоби оцінки гарантій IT безпеки

Techniques and tools for evaluation of IT security assurance

Тренінг

За редакцією В. С. Харченко

Проект
SEREIN 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR
Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains

2017

Викладено матеріали практичної частини тренінг-курсу «Методи і засоби оцінювання гарантій безпеки» (CT3.Security and Resilience Assurance Cases), підготовленого в рамках проекту TEMPUS SEREIN «Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains» (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR).

Наведені описи тренінгів, які призначені для вивчення з технологіями та засобами оцінки гарантій безпеки, у відповідності до міжнародних стандартів та вимог. Надається навчальна програма курсу і опис лабораторних робіт і тренінгів.

Призначено для інженерів, які займаються проектуванням, розробленням та впровадженням систем захисту інформації, для груп верифікації і фахівців у галузі оцінювання якості та безпеки ІТ-систем, для магістрів і аспірантів університетів, які навчаються за напрямами інформаційної безпеки, комп'ютерних наук, комп'ютерної та програмної інженерії, а також для викладачів відповідних курсів.

Рецензенты:

– Prof. Todor Tagarev, Centre for Security and Defence Management, Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences;

– Prof. Stefano Russo, Consorzio Interuniversitario Nazionale per l'Informatica (Naples, Italy)

А.В. Леншин, О. А. Ильяшенко, А.В. Потий

Методы и средства оценки гарантий IT безопасности. Тренінг / под ред. В.С. Харченко – Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ». 2017. – 100 с.

Изложены материалы практической части тренинг-курса «Методы и средства оценки гарантий безопасности» (CT3.Security and Resilience Assurance Cases), подготовленного в рамках проекта TEMPUS SEREIN «Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains» (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR).

Приведены описания тренингов, которые предназначены для изучения технологий и средств оценки гарантий IT-безопаности, в соответствии с требованиями международных стандартов. Предоставляется учебная программа курса и описание лабораторных работ и тренингов.

Предназначено для инженеров, занимающихся проектирования, разработкой и внедрением систем защиты информации, для групп верификации и специалистов по оценке качества и безопасности ИТ-систем, для магистров и аспирантов университетов, обучающихся по направлениям информационной безопасности, компьютерных наук, компьютерной и программной инженерии, а также для преподавателей соответствующих курсов.

Библиогр.: 47 наименований, рисунков – 53.

Утверждено на заседании ученого совета Национального аэрокосмического университета имени Н.Е. Жуковского «ХАИ» (протокол № 6 от 22 февраля 2017 г.).

СПИСОК СКОРОЧЕНЬ

ITC	–	Інформаційно-телекомунікаційні системи
ASSET	–	Automated Security Self-Evaluation
IT	–	Інформаційна технологія
TOE	–	(Target of Evaluation) – об’єкт оцінки
SFP	–	(Security function policy) політика функції безпеки
TSP	–	(TOE security policy) політика безпеки об’єкту оцінки
SF	–	(security function) функція безпеки
TSF	–	(TOE security function) функції безпеки об’єкту оцінки
TSFI	–	(TOE security function interface) інтерфейс функцій
CC PKB	–	база знань Common Criteria Profiling Knowledge Base

ВСТУП

У посібнику викладено матеріали практичної частини тренінг-курсу «Методи і засоби оцінювання гарантій безпеки» (CT3.Security and Resilience Assurance Cases), підготовленого в рамках проекту TEMPUS SEREIN «Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains»[1] (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR). Курс присвячено метода та засобами оцінки гарантій безпеки та проектування вимог безпеки формації в ИТ-системах.

Тренінг «Методи і засоби оцінювання гарантій безпеки» входить до циклу тренінгів модуля CT3.Security and Resilience Assurance Cases. Основною метою тренінгу є отримання студентами необхідних навичок зі стандартизації і сертифікації продукції та послуг захисту інформації, знань основних вимог нормативних документів та формування практичних навичок їх застосування під час проектування систем захисту інформації.

Практикум №1 «Оцінка рівня зрілості процесів захисту інформації в організації» спрямована на формування практичних навичок з проведення елементів аудиту безпеки, первинного обстеження об'єктів інформаційної діяльності, оцінки зрілості процесів захисту інформації із застосування автоматизованої системи експертної оцінки «Радник».

Практикум №2 „Розроблення елементів профілю захисту у відповідності до вимог міжнародного стандарту ISO/IEC 15408" спрямована на вивчення студентами методології та порядку розроблення профілю захисту, з використанням засобів та систем автоматизованого проектування, а саме Profiling Knowledge Base та Common Criteria Tools.

Практикуми є одним із основних видів занять та призначені для вирішення таких навчальних задач:

- закріплення теоретичних знань, які отримані слухачами на лекціях;
- ознайомлення з методиками проектування систем захисту інформації, аудиту безпеки, спеціальних досліджень;
- набуття практичних навичок у використанні спеціалізованого програмного забезпечення;

[1] *Этот проект финансируется при поддержке Европейской комиссии. Эта публикация (сообщение) отражает мнения только авторов, и Комиссия не может нести ответственность за любое использование содержащейся в нем информации.*

This project has been funded with support from the European Commission. This publication (communication) reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- набуття навичок роботи з нормативними документами.

Виконання кожної роботи складається з трьох етапів:

- самостійна підготовка до роботи;
- виконання досліджень;
- аналіз отриманих результатів.

Під час самостійної підготовки до роботи студент повинен ознайомитися з метою та завданням роботи, вивчити основні теоретичні положення, які лежать в основі виконання роботи, ознайомитися з рекомендованою літературою та підготувати бланк звіту.

Для підготовки бланку звіту необхідно: (1) записати у звіт назву та мету роботи; (2) скласти і записати в звіт програму та порядок дослідження; (3) дати стислу характеристику лабораторної установки, спеціалізованого програмного забезпечення, його призначення, можливості і порядок використання; (4) провести, за необхідністю, попередні розрахунки і скласти графіки та таблиці; (5) помістити в звіт основні аналітичні співвідношення.

Виконання експериментальної частини здійснюється на ПЕОМ відповідно до розділу „Програма та порядок роботи", що є в описанні кожної роботи.

Кожен студент отримує індивідуальне завдання і виконує відповідні дослідження, самостійно формує висновки та пропозиції. Обробка результатів виконується безпосередньо на робочому місці в години, які відведені для виконання роботи. Результати обробляються відповідно до вказівок, що наведені в описі роботи, викладені в лекційному матеріалі або зроблені викладачем безпосередньо на заняттях.

Підсумком кожної роботи є звіт, що оцінюється відповідно до розділу „Зміст звіту". Всі проведені дослідження та результати відповідним чином інтерпретуються та оцінюються.

Практикум підготовлений співробітниками кафедри комп'ютерних систем і мереж Національного аерокосмічного університету ім. Н.Е. Жуковського «ХАІ»: старшим викладачем Ілляшенком О.О., професором Потієм О.В. та інженером – дослідником приватного акціонерного товариства "Інститут інформаційних технологій" Лєншиним А.В.. Загальне редагування здійснено доктором технічних наук, професором, заслуженим винахідником України Харченко В.С.

Автори висловлюють подяку рецензентам, колегам та співробітникам кафедр університетів, індустріальним партнерам за корисну інформацію, методичну допомогу та конструктивні пропозиції, які висловлювалися у процесі обговорення програми курсу та матеріалів посібника.

2. ОЦІНКА РІВНЯ ЗРІЛОСТІ ПРОЦЕСІВ ЗАХИСТУ ІНФОРМАЦІЇ В ОРГАНІЗАЦІЇ

2.1 Мета роботи

Закріпити знання вимог стандарту в сфері захисту інформації NIST SP 800-26, розглянути основні положення суб'єктивної логіки та навчитися використовувати системи підтримки прийняття рішень (систему експертної оцінки "Радник") для проведення внутрішнього аудиту безпеки інформації.

2.2 Методичні вказівки з організації самостійної роботи студентів

Під час підготовки та проведення лабораторної роботи студенти мають:

- повторити матеріал щодо вимог стандарту NIST SP 800-26 та ідеології проведення самооцінки згідно нього;
- ознайомитися з моделлю зрілості процесів по забезпеченню безпеки інформації;
- розглянути основні положення суб'єктивної логіки;
- розглянути оператори суб'єктивної логіки;
- ознайомитися з поняттям зон базових думок;
- вивчити документацію на систему експертної оцінки „Радник";
- підготувати бланк звіту;
- підготувати відповідь на контрольні запитання.

2.3 Основні теоретичні положення

2.3.1 Характеристика підходу до оцінки захищеності Національного інституту по стандартизації та технологіям США (NIST SP 800-26)

Забезпечення безпеки інформації в інформаційно-телекомунікаційних системах (ІТС) пов'язано з виконанням досить великого комплексу різних заходів, упровадженням спеціальних засобів захисту інформації. Адміністратори безпеки і керівники служби захисту інформації зустрічаються із труднощами при здійсненні реальної оцінки рівня захищеності ІТС, планування комплексу робіт із захисту інформації. Одним зі шляхів рішення цих задач є проведення періодичних атестацій системи захисту інформації на ступінь відповідності вимогам безпеки.

У 2001 році NIST розробив рекомендації SP 800-26, що містять методику самооцінки безпеки ІТС. Відповідно до рекомендацій, задачі забезпечення безпеки здійснюються на адміністративному, процедурному і програмно-технічному рівнях.

На адміністративному рівні реалізуються заходи загального характеру, що здійснюється керівництвом підрозділу.

На процедурному рівні запроваджуються заходи безпеки, що реалізуються технічним персоналом та особовим складом.

На програмно-технічному рівні впроваджуються конкретні технічні, фізичні та програмно-апаратні засоби захисту інформації.

Усі заходи щодо забезпечення безпеки інформації в ІТС розподілені на 17 областей (таблиця 2.1), які у свою чергу містять Критичні елементи (сукупність визначених практичних задач) (Рис. 2.1).

Таблиця 2.1 Контрольні області згідно NIST SP 800-26

№	Назва рівнів	Назва контрольних областей
1.	Адміністративний	Управління ризиками.
2.		Аналіз заходів щодо забезпечення безпеки інформації.
3.		Підтримка життєвого циклу.
4.		Сертифікація, атестація та акредитація.
5.		Розробка плану захисту.
6.	Процедурний	Захист від персоналу.
7.		Фізичний захист.
8.		Управління виробництвом і вхідний/вихідний контроль.
9.		Планування безперебійної роботи .
10.		Експлуатація апаратного і системного програмного забезпечення.
11.		Цілісність даних.
12.		Документація.
13.		Навчання, тренування, інформування.
14.		Реагування на інциденти.
15.	Програмно-технічний	Ідентифікація та автентифікація.
16.		Управління доступом.
17.		Протоколювання та аудит.

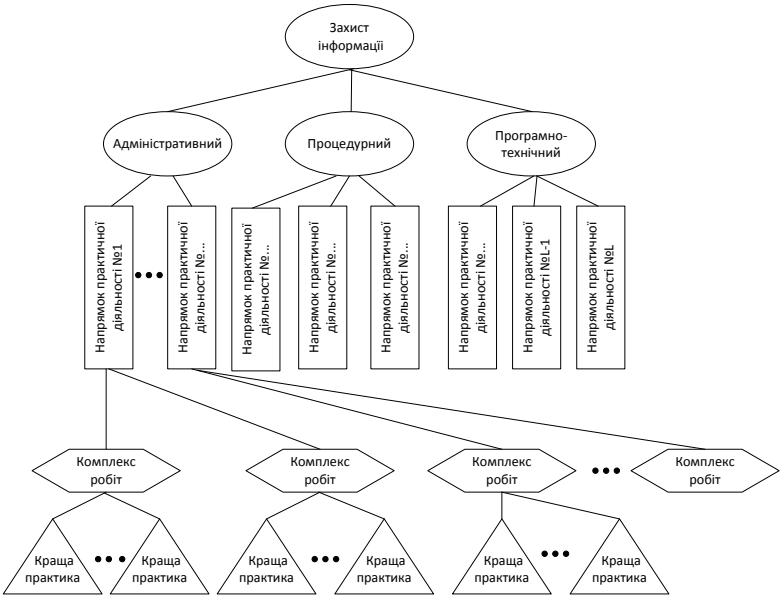


Рисунок 2.1 – Структура вимог безпеки NIST SP 800-26

Оцінка Критичного елемента здійснюється шляхом оцінки ступеня виконання кожної з задач наданням на запитання відповідей (Так/Ні). Критичний елемент може бути оцінений по одному з п'яти рівнів.

Рівень 1. Задокументовано у політиці безпеки

На цьому рівні передбачається, що:

- правила безпеки, що охоплюють верхній рівень керування організації й основних підрозділів (департаменти, керівництво, відділи), формально задокументовані і доведені до всього персоналу. Правила можуть розглядатися як спеціальний ресурс;
- правила безпеки містять більшість базових вимог безпеки, які визначаються в нормативно-правових документах.

Рівень 2 Задокументовано у виді процедур (робіт)

На даному рівні передбачається, що вимоги безпеки є формальними, повними, добре задокументованими процедурами (роботи)

для реалізації правил безпеки, уведених на першому рівні. Базові вимоги формуються на основі нормативно-правових документів

Рівень 3 Процедури захисту інформації виконані

На цьому рівні передбачається, що:

- процедури, які визначені на другому рівні, виконані.
- призначені відповідальні особи для виконання визначених процедур.

Ресурсом на третьому рівні є заходи безпеки інформації, які виконуються у встановленому порядку та і посилені через навчання персоналу.

Рівень 4 Процедури безпеки і засоби захисту протестовані та оцінені

На четвертому рівні вважається, що:

- здійснюється періодична оцінка адекватності та ефективності правил безпеки, процедур безпеки та засобів захисту інформації;
- надаються гарантії того, що в організації розпочато ефективні коригувальні дії, спрямовані на усунення виявлених недоліків у тому числі і тих, котрі проявилися як результат потенційних чи реальних інцидентів безпеки, а також виявлених за допомогою повідомлень спеціальних служб (наприклад, служби FedCIRC), постачальників та інших довірених джерел.

Рівень 5. Процедури безпеки і засоби захисту цілком інтегровані

На п’ятому рівні вважається, що

- здійснюється всеохоплююча програма забезпечення безпеки інформації, яка є невід'ємною частиною корпоративної культури;
- прийняття рішень засноване на економічній доцільності, ризику і впливі на місію організації.

Процедура оцінки Критичного елемента складається з відповідей на питання, що містяться в ньому. Відповіді на питання по кожному з рівнів надаються з урахуванням критеріїв висунутих до цього рівня. Висновок щодо виконання Критичного елемента здійснюється за мажоритарним принципом, який передбачає, що загальна відповідь про виконання Критичного елемента буде «Так» у випадку, якщо

більше ніж половина відповідей на його супідрядні питання будуть «Так». Інакше, Критичний елемент оцінюється як не виконаний на відповідному рівні.

Після проведення атестації Критичних елементів на відповідність рівням виконання, проводиться атестація Контрольних областей. Область може бути оцінена як вирішена на заданому рівні тільки в тому випадку, якщо всі Критичні елементи, що входять до її складу виконані на цьому рівні. Після атестації контрольної області будується профіль (Рис. 2.2), що дозволяє визначити області безпеки, які потребують першочергової уваги.

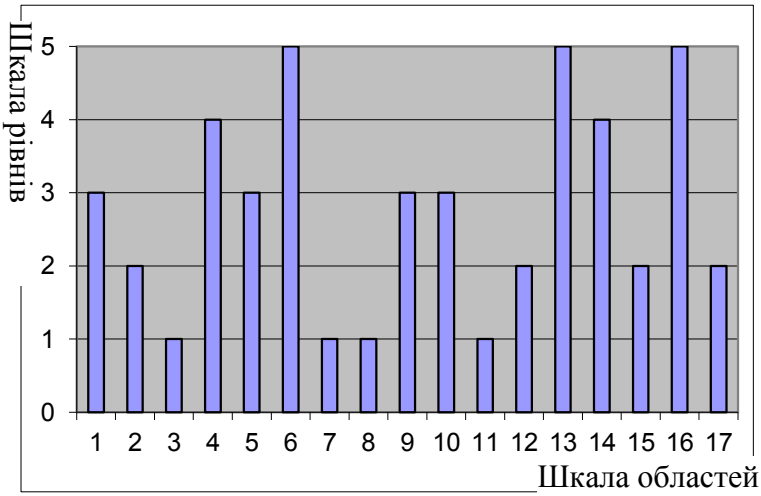


Рисунок 2.2 – Профіль виконання контрольних областей

2.3.2 Методика оцінки NIST

Згідно рекомендацій NIST SP 800-26, що містять методику самооцінки безпеки інформації в ІТС, задачі забезпечення безпеки інформації здійснюються на адміністративному, процедурному і програмно-технічному рівнях. Усі заходи щодо забезпечення безпеки ІТС розподілені на 17 областей, які у свою чергу містять Критичні елементи (сукупність визначених практичних задач). Оцінка Критичного елемента здійснюється шляхом надання відповіді, чи виконана кожна із задач (Так/Ні). Висновок щодо Критичного елемента здійснюється по мажоритарному принципу.

Обчислимо думку експерта по Критичному елементу 2.1 та Критичному елементу 7.2 по запропонованому мажоритарному принципу (питання відповідних Критичних елементів наводяться в таблиці 2.2).

Таблиця 2.2 – Критичні елементи

Критичний елемент 2.1. Чи проводиться аналіз заходів щодо забезпечення безпеки в даній системи, а також у взаємодіючих з нею системах ?
Чи проводиться періодичний аналіз даної системи, а також границь мереж ?
Якщо відбулись значні зміни у системі, чи проводиться незалежна експертиза ?
Проводиться, чи ні періодична самооцінка системи ?
Чи регулярно проводяться іспити і перевірка ключових об'єктів, наприклад, сканування мережі, аналіз установок маршрутизотора і комутатора, перевірка можливості проникнення (вторгнення) ?
Чи проводиться аналіз інцидентів, порушень безпеки і чи застосовуються необхідні коригувальні дії?
Критичний елемент 7.2 Дані захищені від перехоплення?
Чи впевненні ви, що монітори комп'ютерів розміщені таким чином, який виключає перегляд даних сторонніми особами, а також перехоплення електромагнітних випромінювань.
Проводиться контроль фізичного доступу до ліній передачі даних?

Використовуємо стандартний підхід, відповідаючи на питання «так» або «ні». В таблиці 2.3 приведені результати оцінки двох Критичних елементів.

Таблиця 2.3

№	2.1 1	2.1 2	2.1 3	2.1 4	2.1 5	2.1 разом	7.2.1	7.2.2	7.2 разом
Відповідь	Так	Ні	Так	Так	Ні	Так	Так	Ні	?

Прийняття рішення за мажоритарним принципом:

Нехай n - загальне число поставлених питань, r - кількість отриманих позитивних відповідей. Тоді функція ухвалення рішення $G(n)$ має вид:

$$G(n)=\begin{cases}1, & r > n/2\\ 0, & r < n/2\\ ?, & r = n/2\end{cases}$$

Процес ухвалення рішення по Критичному елементі з використанням мажоритарного принципу зображений на рисунку 2.3.

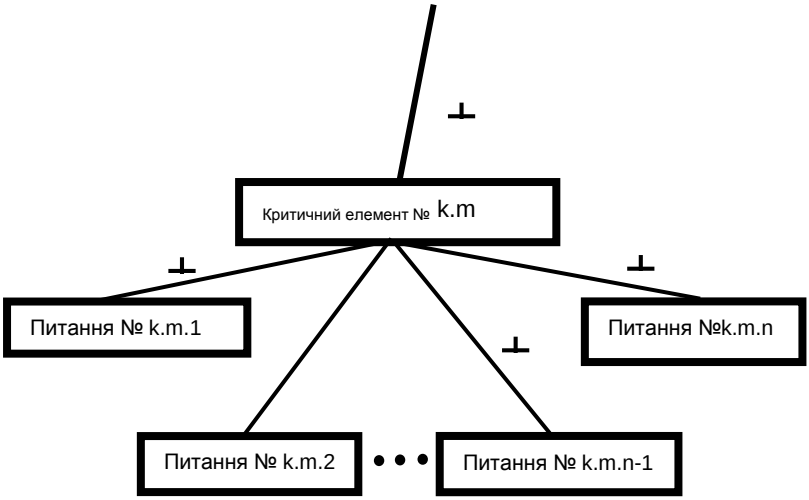


Рис. 2.3 - Використання мажоритарного принципу

Використовуючи мажоритарний принцип, дійдемо такого висновку: Критичний елемент 2.1 виконується, а рішення щодо виконання Критичного елемента 7.2 прийняти неможливо. Ситуація невизначеності викликана непарною кількістю елементів, і може бути вирішена введенням/виключенням питання. Але це вимагає втручання в систему питань NIST. Друге рішення полягає у віднесенні випа-

дку з рівною кількістю негативних і позитивних відповідей до однієї з областей позитивних/від'ємних відповідей, що неминуче приведе до огрубіння оцінки.

Незаперечною перевагою методики одержання оцінки шляхом надання відповідей «Так» і «Ні» з наступною обробкою по мажоритарному принципу є її простота, але при цьому одержана інформація не є повною. Результати, отримані по Критичному елементі 2.1, були такими ж, як і у випадку отримання позитивних відповідей на будь-які три питання, і при 4-х, 5-ти позитивних відповідях.

Методика самооцінки запропонована NIST безперечно має дуже високу цінність. Системний підхід застосовуваний при оцінці захищеності інформації в ІТС та грамотно підібрані задачі захисту дозволяють всебічно охопити питання безпеки інформації особі, що проводить процедуру самооцінки. При цьому від неї не вимагається дуже глибоких знань у галузі захисту інформації. Але використання бінарних відповідей та мажоритарного принципу не дозволяє дати точну відповідь на питання в якому обсязі виконана та чи інша процедура (робота) і не дає можливості сформувати обґрунтовані (бажано кількісні) висновки відносно ступеня виконання Критичного елемента.

Вище приведені фактори викликали думку використовувати математичний апарат суб'єктивної логіки, запропонований норвезьким вченим А. Джосангом (Audun Jøsang). Застосування операторів суб'єктивної логіки дозволяють поєднувати думки двох осіб, формуючи думку, що характеризує спільну істинність тверджень з урахуванням різних умов, дозволяє упорядкувати думки, чи виробити рекомендацію відносно наданої оцінки.

2.3.3 Основні теоретичні положення суб'єктивної логіки

У даному підрозділі розглядається математичний апарат суб'єктивної логіки, застосування якого дозволяє висловлювати і оброблювати думки експерта, за допомогою спеціальних операторів, які моделюють розумову діяльність людини.

Стандартна логіка оперує на двійкових змінних, які можуть приймати дискретні значення «ІСТИНА» та «БРЕХНЯ». Суб'єктивна логіка оперує з думками, представленими у вигляді вектору $\omega_p = \{b_p, d_p, u_p, a_p\}$.

Думки, як і свідчення, розглядаються індивідуально і таким чином, вони обов'язково належать комусь і виносяться до чогось (чи когось). Думка експерта A про істинність (правдивість, вірогідність) твердження p позначається як ω_p^A.

У суб'єктивній логіці визначено 7 операторів обробки думок:
- кон'юнкція (об'єднання) думок;
- диз'юнкція (роз'єднання) думок;
- заперечення думки;
- незалежний консенсус;
- залежний консенсус;
- частково залежний консенсус;
- рекомендація.

2.3.3.1 Кон'юнкція

Формування кон'юнкції двох тверджень з сфокусованих фреймів розрізнення полягає у виробленні з двох думок стосовно кожного твердження, нової думки, що буде виражати віру в істинність обох тверджень одночасно. Цей оператор є аналогом "AND" у бінарній логіці.

Теорема 3 (Кон'юнкція тверджень**)**

Нехай θ_x та θ_y це два бінарних сфокусованих фрейму розрізнення, x та y - відповідно твердження стосовно станів в θ_x та θ_y. Тоді $\omega_x=(b_x,d_x,u_x,a_x)$ та $\omega_y=(b_y,d_y,u_y,a_y)$, це думки відносно цих станів, нехай $\omega_{x\wedge y}=(b_{x\wedge y},d_{x\wedge y},u_{x\wedge y},a_{x\wedge y})$ така думка, що

1. $b_{x\wedge y}=b_x b_y$;
2. $d_{x\wedge y}=d_x+d_y-d_x d_y$;
3. $u_{x\wedge y}=b_x u_y+u_x b_y+u_x u_y$
4. $a_{x\wedge y}=\dfrac{b_x u_y a_y+u_x a_x b_y+u_x a_x u_y a_y}{b_x u_y+u_x b_y+u_x u_y}$;

Тоді $\omega_{x\wedge y}$ має назву кон'юнкція тверджень думок ω_x та ω_y і виражає думку особи, яка приймає рішення стосовно того, що обидва твердження x та y є істинними. Для позначення цього оператора використовується символ $\wedge$ таким чином $\omega_{x\wedge y} \equiv \omega_x \wedge \omega_y$

2.3.3.2 Диз'юнкція

Формування диз'юнкції двох тверджень зі сфокусованих фреймів розрізнення полягає у визначенні з двох думок стосовно кожного твердження нової думки, яка буде виражати віру в істинність або одного твердження або їх одночасну істинність. Цей оператор є аналогом "OR" у бінарній логіці.

Теорема 4 (Диз'юнкція тверджень**)**

Нехай θ_x та θ_y це два бінарних сфокусованих фрейму розрізнення, x та y - відповідно твердження стосовно станів в θ_x та θ_y. Тоді $\omega_x = (b_x, d_x, u_x, a_x)$ та $\omega_y = (b_y, d_y, u_y, a_y)$ це думки відносно цих станів. Нехай $\omega_{x\vee y} = (b_{x\vee y}, d_{x\vee y}, u_{x\vee y}, a_{x\vee y})$ така думка, що

1. $b_{x\vee y} = b_x + b_y - b_x b_y$;
2. $d_{x\vee y} = d_x d_y$;
3. $u_{x\vee y} = d_x u_y + u_x d_y + u_x u_y$;
4. $a_{x\vee y} = \dfrac{u_x a_x + u_y a_y - b_x u_y a_y - u_x a_x b_y - u_x a_x u_y a_y}{u_x + u_y - b_x u_y - u_x b_y - u_x u_y}$.

Тоді $\omega_{x\vee y}$ має назву кон'юнкція тверджень думок ω_x та ω_y і виражає думку особи, яка приймає рішення стосовно того, що або обидва одне з тверджень x або y є істинними, або вони істині разом.

Для позначення цього оператора використовується символ $\vee$ таким чином $\omega_{x\vee y} \equiv \omega_x \vee \omega_y$

2.3.3.3 Заперечення

Заперечення думки щодо твердження x визначає думку, що x буде неістинне. Ця операція є аналогом заперечення "NOT" у бінарній логіці.

Теорема 5 (Заперечення)

Нехай $\omega_x = (b_x, d_x, u_x, a_x)$ це думка відносно x. Тоді $\omega_{\neg x} = (b_{\neg x}, d_{\neg x}, u_{\neg x}, a_{\neg x})$ це заперечення ω_x де:

1. $b_{\neg x} = d_x$;
2. $d_{\neg x} = b_x$
3. $u_{\neg x} = u_x$
4. $a_{\neg x} = 1 - a_x$.

Заперечення є інволютивним, тобто $\neg(\neg\omega_p) = \omega$ вірно для будь-якої думки ω.

2.3.3.4 Консенсус між незалежними думками

Консенсус між двома думками об'єднує їх, вважаючи, що вони незалежні та мають однакове значення. Наприклад, якщо два експерта спостерігали за певним явищем у два проміжки часу, що не перекриваються, вони можуть мати про нього різні думки. Консенсус дозволяє сформувати нову думку, що повинна дорівнювати думці третього експерту (віртуального експерту), який нібито спостерігав це явище у обидва проміжки часу.

Теорема 6 (Заперечення)

Нехай $\omega_x^A = \{b_x^A, d_x^A, u_x^A\}$ і $\omega_x^B = \{b_x^B, d_x^B, u_x^B\}$ думки, що належать відповідно експертам *A* и *B*, відносно твердження *p*. Нехай $\omega_x^{A,B} = \{b_x^{A,B}, d_x^{A,B}, u_x^{A,B}\}$ буде думкою такою, що

1. $b_x^{A,B} = \left(b_x^A u_x^B + b_x^B u_x^A\right) / k$;
2. $d_x^{A,B} = \left(d_x^A u_x^B + d_x^B u_x^A\right) / k$;
3. $u_x^{A,B} = \left(u_x^A u_x^B\right) / k$.
4. $a_x^{A,B} = \dfrac{a_x^B u_x^B + a_x^A u_x^B - \left(a_x^A + a_x^B\right) u_x^A u_x^B}{u_x^A + u_x^B - 2u_x^A u_x^B}$;

де $k = u_x^A + u_x^B - u_x^A u_x^B$ причому $k \neq 0$ та $a_x^{A,B} = \left(a_x^A + a_x^B\right) / 2$.

Операція консенсусу є комутативною й асоціативною, отже порядок комбінування думок не важливий. Передбачається, що думки незалежні. Не можна врахувати думки більш ніж один раз.

Дві думки, що містять нульову невизначеність, відповідно до теореми 1 не можуть комбінуватися. Це можна пояснити через ітерацію невизначеності "як кімната для впливу", тобто виникає можливість уплинути на думки, які ще не були висловлені ні за, ні проти твердження. Ситуація з незалежними абсолютно визначеними думками, з філософської точки зору, безглузда, по-перше тому, що думки не можуть бути абсолютно визначеними і по-друге, вони тоді повинні бути обов'язково однаковими.

2.3.3.5 Консенсус між залежними думками

Припустимо, що два експерти *A* и *B* одночасно спостерігають об'єкт, що породжує бінарні результати визначену кількість разів. Оскільки їхні спостереження ідентичні, то їхні думки будуть залежними і консенсус у змісті Теореми 6 не має сенсу.

Теорема 7 Нехай $\omega_x^{A_i} = \left\{b_x^{A_i}, d_x^{A_i}, u_x^{A_i}\right\}$, де $i \in \{1,\ldots,n\}$ це n залежних думок експертів $A_1,\ldots A_n$ відносно твердження x. Нехай $\omega_x^{\overline{A_1,..,A_n}} = \left\{b_x^{\overline{A_1,..,A_n}}, d_x^{\overline{A_1,..,A_n}}, u_x^{\overline{A_1,..,A_n}}\right\}$ це така думка, що

$$b_h^{\overline{A_1,..,A_n}} = \frac{\sum_{i=1}^n \left(b_p^{A_i} / u_p^{A_i}\right)}{\sum_{i=1}^n \left(b_p^{A_i} / u_p^{A_i}\right) + \sum_{i=1}^n \left(d_p^{A_i} / u_p^{A_i}\right) + n};$$

$$d_h^{\overline{A_1,..,A_n}} = \frac{\sum_{i=1}^{n}\left(d_p^{A_i} / u_p^{A_i}\right)}{\sum_{i=1}^{n}\left(b_p^{A_i} / u_p^{A_i}\right)+\sum_{i=1}^{n}\left(d_p^{A_i} / u_p^{A_i}\right)+n};$$

$$u_h^{\overline{A_1,..,A_n}} = \frac{n}{\sum_{i=1}^{n}\left(b_p^{A_i} / u_p^{A_i}\right)+\sum_{i=1}^{n}\left(d_p^{A_i} / u_p^{A_i}\right)+n}.$$

Тоді $\omega_x^{\overline{A_1,..,A_n}}$ називається залежним консенсусом між усіма n думками. Для позначення операції використовується символ $\overline{\oplus}$, тобто $\omega_x^{\overline{A_1,..,A_n}} = \omega_x^{A_1} \overline{\oplus} ... \overline{\oplus}\, \omega_x^{A_n}$.

Операція $\overline{\oplus}$ є і комутативною, і асоціативною. Отже порядок комбінування думок не важливий. Думки, що не містять невизначеності не можуть бути скомбіновані.

2.3.3.6 Консенсус між частково залежними думками

Якщо два експерти *A* и *B* спостерігають ті самі події протягом двох частково непересічних проміжків часу, то їх відповідні думки будуть частково залежними. Консенсус між частково залежними думками експертів *A* и *B* можна записати у виді:

$$\omega_x^{\mathrm{Ai}(B)} : \begin{cases} b_x^{\mathrm{Ai}(B)} = b_x^A \mu_x^{AB}; \\ d_x^{\mathrm{Ai}(B)} = d_x^A \mu_x^{AB}; \\ u_x^{\mathrm{Ai}(B)} = u_x^A \mu_x^{AB} / \left(1-\gamma_x^{AB}\right). \end{cases},$$

де $\mu_x^{AB} = \dfrac{1-\gamma_x^{AB}}{\left(1-\gamma_x^{AB}\right)\left(b_x^A + d_x^A\right)+u_x^A}$.

Для позначення консенсусу між частково залежними думками використовується символ $\widetilde{\oplus}$. Консенсус між думками експертів *A* и *B* може бути записаний у виді

$$\omega_x^A \tilde{\oplus} \omega_x^B = \omega_x^{A,\tilde{B}} = \omega_x^{\overline{Ad(B),BdA},Ai(B),Bi(A)} =$$
$$= \left(\omega_x^{Ad(B)} \bar{\oplus} \omega_x^{Bd(A)}\right) \oplus \omega_x^{Ai(B)} \oplus \omega_x^{Bi(A)} .$$

Для будь-якої думки ω_x^A з коефіцієнтом залежності γ_x^{AB} з будь-якою іншою думкою ω_x^B справедливе співвідношення

$$\omega_x^A = \omega_x^{A_1(B)} \otimes \omega_x^{A_{d_i}(B)}.$$

2.3.3.7 Рекомендація

Припустимо, що існують два експерти *A* и *B*, причому експерт *A* має деяку думку про експерта *B*, а експерт *B* має думку щодо твердження X.

Рекомендація цих двох думок полягає в комбінуванні думки експерта *A* відносно експерта *B* з думкою експерта *B* відносно твердження x.

Не існує такої речі як рекомендація в чистому виді. Рекомендація думок у загальному випадку піддається різним інтерпретаціям. Основними труднощами є опис результату невір'я експерта *A* в те, що експерт *B* буде давати добру пораду. Що насправді це означає? Існує три різних інтерпретації.

1. Схильність до невизначеності. Недовіра експерта *A* в рекомендації, які надає експерт *B,* полягає в тому, що *A* вважає, що *B* має невизначеність (не знання) щодо істинного значення X. У результаті *A* також буде невизначений щодо істинного значення X.

2. Схильність до обману. Недовіра експерта *A* в рекомендації експерта *B* спирається на те, що *A* вважає, що *B* послідовно намагається (пробує) зменшити інформованість *A* через злий намір. У результаті експерт *A* не вірить експерту *B*.

3. Схильність до припущення про погані поради. Невір'я експерта *A* в рекомендації експерта *B* означає, що *A* вважає, що *B* послідовно дає ради зворотні від його реальної думки щодо істинного значення X. У результаті експерт *A* не тільки не вірить у X зі ступенем, з яким *B* рекомендує вірити, але також і вірить у X зі ступенем, з

яким *B* рекомендує не вірити в x. Таким чином, комбінація двох результатів приводить до довіри.

Теорема 8. Нехай *A* и *B* два експерти, а $\omega_B^A = \left\{b_B^A, d_B^A, u_B^A\right\}$ думка експерта *A* щодо рекомендацій експерта *B*. Нехай x є твердження, а $\omega_x^B = \left\{b_x^B, d_x^B, u_x^B\right\}$ є думка експерта *B* відносно твердження x, яка виражена у формі рекомендації для експерта *A*. Нехай $\omega_x^{AB} = \left\{b_x^{AB}, d_x^{AB}, u_x^{AB}\right\}$ буде думка така, що

$$b_x^{AB} = b_B^A b_x^B;$$
$$d_x^{AB} = b_B^A d_x^B;$$
$$u_x^{AB} = d_B^A + u_B^A + b_B^A u_x^B$$

Тоді ω_x^{AB} називається думкою що виражає, думку експерта *A* щодо твердження x, яка сформована в результаті рекомендацій, отриманих від експерта *B*. Для позначення цієї операції будемо використовується символ ⊗, тобто

$$\omega_x^{AB} = \omega_B^A \otimes \omega_x^B.$$

Операція ⊗ є асоціативною, але не комутативною. Отже, комбінування думок не може починатися з якого-небудь кінця ланцюга. Порядок, у якому комбінуються думки, важливий. У ланцюгу, що містить більш одного рекомендуючого об'єкта, думки передбачаються незалежними. Це значить, що в ланцюжку не може бути об'єкта, що дає більш ніж одну рекомендацію.

Рекомендація B повинна інтерпретуватися як те, що експерт B рекомендує експерту A, але не обов'язково відбиває реальну думку відносно твердження x.

Правило рекомендації може бути виправданим тільки в припущенні того, що рекомендація транзитивна, тобто експерти в ланцюзі не можуть змінювати свого поводження (тобто того, що вони рекомендують) у залежності від того, які об'єкти з ними взаємодіють. Од-

нак, це не завжди вірно, оскільки свідомо невірні рекомендації можуть бути мотивовані, наприклад, протиріччями (конфліктами) між експертами. Правило рекомендації необхідно застосовувати з обережністю і тільки тоді, коли передбачається інваріантне поводження експертів.

2.4 Опис лабораторної установки

В якості лабораторної установки використовується ПЕОМ із інстальованим програмним забезпеченням – системою експертної оцінки „Радник”. В цьому розділі наводиться її стислий опис.

2.4.1 Призначення

Програмний продукт призначений для автоматизації процедури проведення самооцінки і періодичної атестацій системи на ступінь відповідності вимогам безпеки, згідно нормативними документами у сфері захисту інформації, зокрема рекомендаціям NIST SP 800-26. З його допомогою здійснюється оцінка зрілості процесів по забезпеченню безпеки інформації та планування комплексу робіт із захисту інформації.

2.4.2 Основні принципи функціонування

У логіку функціонування Автоматизованої експертної системи оцінки, «Радник» закладені наступні принципи:

- збір первинної інформації про об'єкт оцінки (ідентифікація системи, рівень критичності ресурсів і інформації, приналежність системи і т.д.)
- збір експертної інформації, її обробка, графічне і вербальне представлення результатів оцінки експертизи;
- розмежування доступу користувачів - експертів до результатів оцінки;
- ведення журналу оцінок;
- підготовка інформації для прийняття рішень щодо планування захисту в ІТС.

Для збору та обробки експертної інформації використані методи суб'єктивної логіки, що дозволяють експерту винести більш точне судження про оцінюваний елемент.

«Радник» надає можливість інтерактивної роботи зі змістом областей, критичних елементів, тверджень, візуального винесення

думки експерта в просторі суб'єктивної логіки. Розвинена система закладок і заміток полегшує переміщення по перелікові елементів оцінки (містить більш 200 елементів оцінки) і збору додаткової інформації про оцінювану систему.

Результати оцінки представляються в графічному вигляді, шляхом побудови профілю рівнів критичних елементів і областей, у вигляді вектору, що містить чисельні значення ступеня довіри, недовіри і рівня невизначеності, а також у вербальному вигляді, шляхом надання вербальної інтерпретації отриманої векторної оцінки.

2.4.3 Вимоги функціонування

Програмний продукт однаково добре працює під управлінням операційних систем Windows 98, Windows 2000, Windows XP. Для установки на одному з логічних дисків потрібно вільний простір 2 Mb. Подальший розмір робочих файлів залежить від кількості експертів притягнутих до оцінки.

2.4.4 Режими роботи системи

«Радник» функціонує в семи основних режимах:

1) Відомості про систему – додавання нової системи, відкриття вже існуючої системи, ознайомлення і редагування зведень про систему, перегляд даних «Журналу історій» (Рис. 2.4)

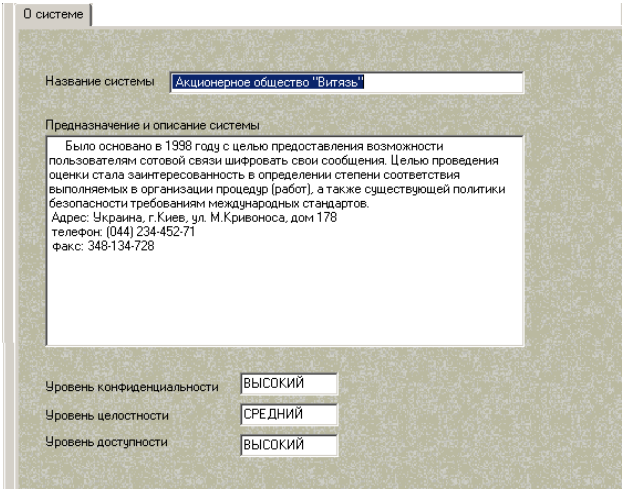


Рисунок 2.4 – Режим «Відомості про систему»

2) Експерти – додавання нового оцінювача, реєстрація оцінки і початок процесу оцінки шляхом надання особистого пароля існуючого оцінювача, знищення облікового запису оцінювача, перегляд зведень про оцінювачів (Рис. 2.5).

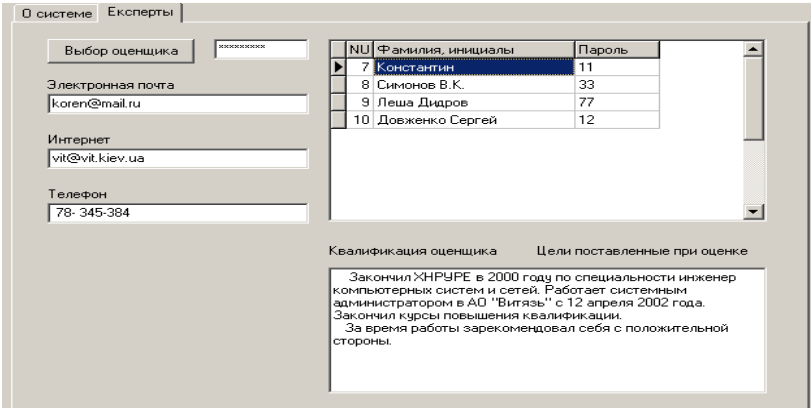


Рисунок 2.5 – Режим « Експерти »

3) Політика – докладне ознайомлення зі змістом контрольних областей, вибір контрольних областей, оцінка яких буде проводитися в плині даної експертизи (Рис. 2.6).

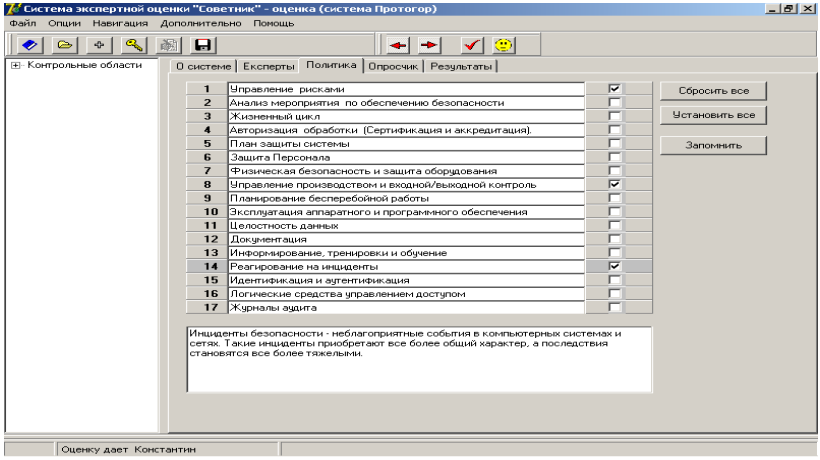


Рисунок 2.6 – Режим «Політика»

4) Опитувач – ознайомлення з інформацією про Контрольні області підлеглих їм Критичних елементах і твердженнях, висловлення думок щодо істинності запропонованих тверджень, додавання, знищення і переміщення між закладками, внесення своїх заміток щодо ступеня виконання тих чи інших задач інформаційної безпеки, і порядку рішення виникаючих проблем ІБ, прийняття думки інших експертів, що вже проводили оцінку по даному питанню (обмежено правами поточного оцінювача) (Рис. 2.7).

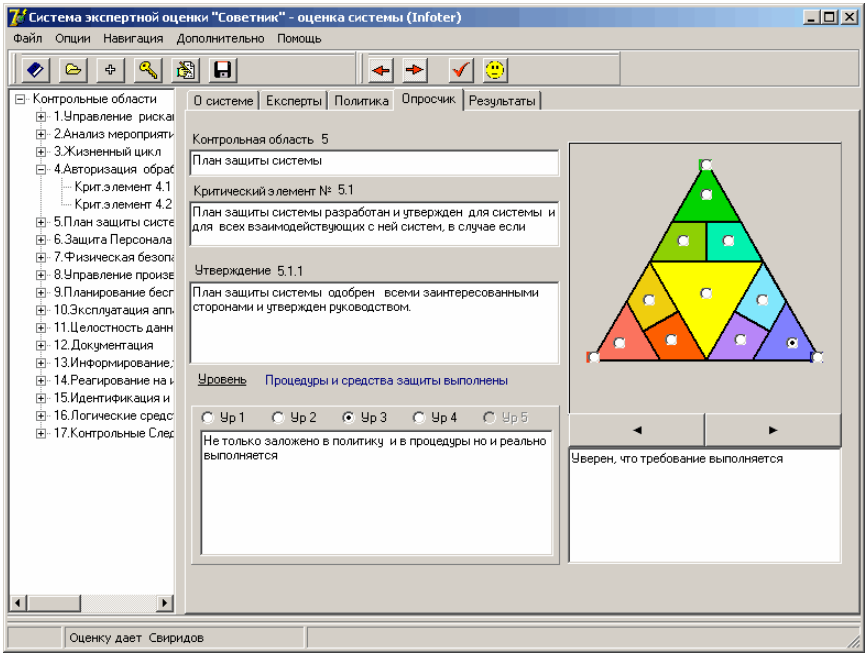


Рисунок 2.7 – Режим «Опитувач»

5) Результати – розрахунок значень Критичних елементів за результатами висловлень думок щодо істинності супідрядних тверджень (режим «Опитувач»), графічне і векторне уявлення отриманих результатів, ознайомлення з вербальним описом ступеню виконання Критичних елементів. Побудова профілю виконання контрольних областей (Рис. 2.8).

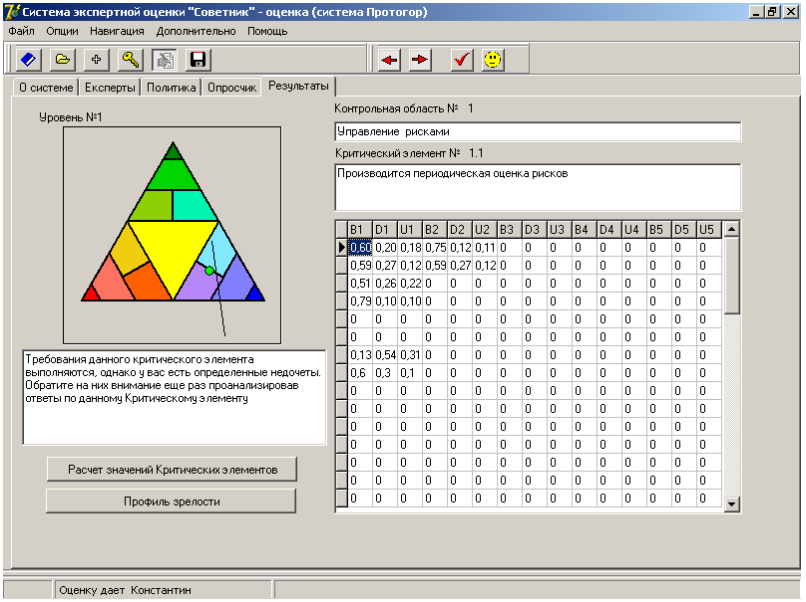


Рисунок 2.8 – Режим «Результати»

6) Аналіз та побудова профілю зрілості

Побудова профілю зрілості Напрямків практичної діяльності (Контрольних областей) на основі даних зібраних у попередніх режимах. Аналіз результатів по кожному напрямку, вивчення пропозицій, які надані „Радником” відносно порядку виконання необхідних процедур (робіт) та спрямованих на забезпечення виконання вимог безпеки діючого стандарту (Рис. 2.9).

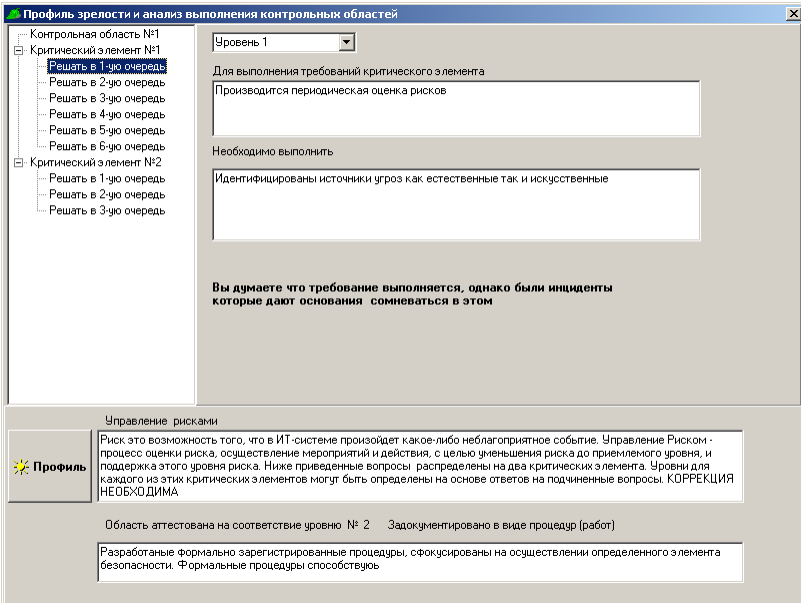


Рисунок 2.9 а)– Режим «Аналіз та побудова профілю зрілості »

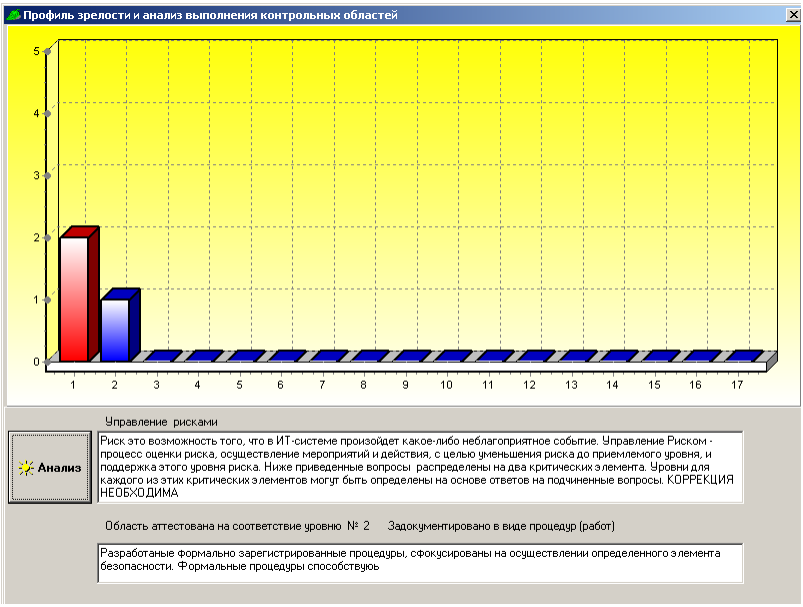


Рисунок 2.9 б) – Режим «Аналіз та побудова профілю зрілості »

7) Формування звіту

Вивід в документ Microsoft Word інформації щодо об’єкту оцінки, про експерта, що проводить оцінку, а також про умови її проведення. Представлення отриманих результатів у вигляді таблиць та графіків (Рис. 2.10).

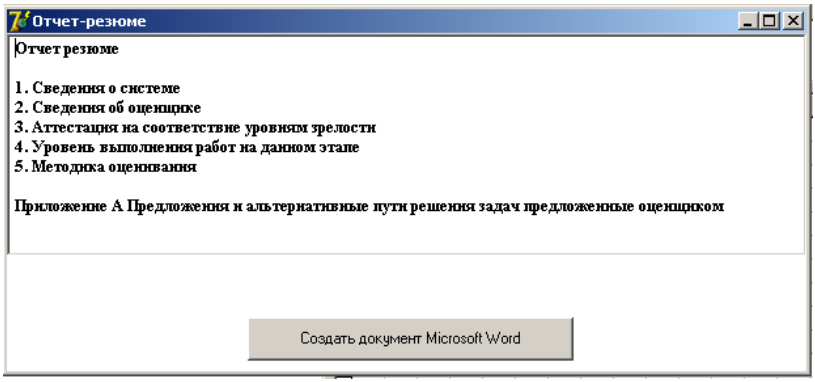


Рисунок 2.10 – Режим « Формування звіту »

2.5 Завдання на лабораторну роботу

Протягом виконання лабораторної роботи необхідно виконати такі основні завдання.

2.5.1 Дослідити методологію стандарту NIST SP 800-26.

2.5.2 Розібратися з основними положеннями та операторами суб’єктивної логіки.

2.5.3 Вивчити програмну документацію та керівництво користувача на систему експертної оцінки „Радник”.

2.5.4 Відпрацювати практичні завдання.

2.5.5 Скласти звіт

2.6 Порядок виконання роботи

Для виконання роботи використовуйте керівництво користувача на систему “Радник”. Виконайте нижче наведенні завдання, це надасть вам змогу пройти всю процедуру самооцінки згідно стандарту NIST SP 800-26 від реєстрації системи до складання звіту. Слід занотувати, що лише послідовне виконання завдань допоможе сфор-

мувати цілісну картину проведення внутрішнього аудиту безпеки інформації на підприємстві.

Завдання до практичного виконання

1. Створіть власну систему надавши їй умовну назву своєї групи.
2. Відкрийте систему шляхом вибору відповідної опції меню.
3. Заповніть інформацію про уявлену систему на вкладці “Про систему”. Та збережіть усі внесені зміни.
4. Додайте обліковий запис експерта, що буде проводити оцінку. (Заповніть інформацію стосовно одного студента з вашої групи). Усі поля мають бути обов’язково заповнені.
5. Перейдіть у режим “Експерти”. Виберіть там свій обліковий запис. Перевірте, чи було збережено інформацію про вашого експерта.
6. Ознайомтесь із інформацією по інших експертах. Якщо такі зареєстровані.
7. Виберіть свій обліковий запис. Введіть пароль доступу, що ви призначили на етапі додавання облікового запису експерта.
8. Спробуйте, змінити свій пароль за допомогою опції меню “Змінити пароль”.
9. Призначте пароль довіри.
10. Перейдіть у режим “Політика”. Позначте ті області які будуть вами оцінюватися протягом даного сеансу оцінки. Підтвердить внесені зміни натиском кнопки “Запам’ятати”.
11. Перейдіть у режим “Опитувач”.
12. Дослідить типові відповіді вибираючи точки у зонах базових думок, на які поділено трикутник думок.
13. Виберіть опцію меню “Параметри”. Виставте параметри згідно свого світогляду. Перевірте як змінюється зовнішній вигляд трикутника думок.
14. Поверніть стандартні настройки параметрів.
15. Дайте відповіді на твердження, що відносяться до обраних контрольних областей.
16. Спробуйте дати відповіді на різних рівнях. Чи це завжди можливо? Чому?
17. Ознайомтесь із змістом рівнів.
18. Натисніть кнопку “Нотування”. Занотуйте свої міркування, пропозиції по одному із тверджень. Запам’ятайте зміни вибравши

відповідну опцію контекстного меню (натиск правої кнопки миші у вікні для нотування).

19.Скрийте вікно де було внесено записи повторним натиском кнопки “Нотування”.

20.Відкрийте діалогове вікно “Закладки”. Додайте закладку, вказавши таким чином на твердження по якому ви вносили свої замітки.

21.Використайте дерево навігацій для переходу між критичними елементами. Чому деякі елементи не доступні?

22.Скориставшись добавленою вами закладкою перейдіть до твердження і переконайтеся, що внесені вами нотатки, та пропозиції збереглися.

23.Знаходячись у режими “Опитувач” виберіть опцію “Ознайомитися із точкою зору”. Виберіть серед переліку, експерта “Максим” введіть у відповідне вікно його пароль довіри (77), та дізнайтеся як він оцінив це твердження.

24.Перейдіть у режим “Результати” та виконайте розрахунки натиснувши кнопку “Розрахунок значень Критичних елементів”.

25.Після закінчення розрахунку подивіться яку оцінку тримали Критичні елементи:

- у просторі думок;
- вербальну.

26.Перегляньте профіль зрілості натиснувши кнопку із відповідною назвою.

27.Ознайомтесь із аналізом однієї із оціненою вами контрольної області.

28.Поверніться у режим “Результати”.

29.Виберіть опцію меню “Створити звіт”.

30.Створеному файлу надайте назву своєї системи та збережіть на диску. Він буде одним із складових отриманої Вами оцінки за лабораторну роботу.

31.Закрийте “Радник”

32.Запустить систему ще раз. Відкрийте Вашу систему та перегляньте журнал історій.

33.Уважно проаналізуйте створений звіт і підготуйтеся до захисту.

2.7 Зміст звіту

Під час підготовки до роботи студент має підготувати бланк звіту по роботи . Для цього необхідно:

- записати у звіті назву та мету роботи;
- зарисувати загальну структуру вимог безпеки стандарту NIST SP 800-26;
- викласти основі співвідношення суб'єктивної логіки;
- скласти й занести у звіт програму експериментальних досліджень;
- дати стислу характеристику апаратного й програмного забезпечення, їхнє призначення, можливості та порядок використання;
- внести до звіту отриманий у ході розрахунків профіль зрілості напрямків по забезпеченню безпеки інформації;
- зробити висновки.

2.8 Контрольні запитання та завдання

2.8.1 Теоретичні питання

2.8.1.1 Для чого призначена система "Радник"?

2.8.1.2 Поясніть ідеологію стандарту NIST SP 800-26.

2.8.1.3 Для чого потрібний профіль зрілості Контрольних областей? Скільки усього налічується Контрольних областей?

2.8.1.4 Поясніть сутність суб'єктивної логіки.

2.8.1.5 Які оператори математичного апарату суб'єктивної логіки ви знаєте?

2.8.1.6 Перерахуйте рівні зрілості. Поясніть сутність кожного з них.

2.8.2 Практичні питання

2.8.2.1 Створіть нову систему.

2.8.2.2 Поясніть призначення закладок. Наведіть приклад їх використання створивши власну.

2.8.2.3 Перегляньте яку відповідь на одне із запитань надав інший експерт за умови що вам відомий його пароль довіри.

2.8.2.4 Чи може пароль довіри надати змогу провести оцінку від імені його власника.

2.8.2.5 Внесіть нотатки по одному із тверджень. Збережіть внесені зміни.

2.8.2.6 Скористайтеся деревом навігацій для переходу до вказаного Вам викладачем Критичного елементу.

2.8.2.7 Змініть пароль. Призначте пароль довіри.

2.8.2.8 Скільки разів була оцінена подана система? Доведіть свою думку використовуючи засоби системи “Радник”.

2.8.2.9 Додайте новий обліковий запис експерта. Зареєструєте факт проведення оцінки.

2.8.2.10Докладіть структуру звіту, що може бути сформований за допомогою системи “Радник”.

2.8.2.11 Виберіть Контрольні області, що будуть оцінюватися протягом даного сеансу оцінки.

2.8.2.12 Чи можна надати відповідь на рівень якщо, рівні з меншими номерами ще не були оцінені? Якщо ні, то чому?

2.8.2.13 Побудуйте профіль зрілості за допомогою АСЕО “Радник”. Що він позначає?

Рекомендована література для самостійної роботи

1. ISO/IEC 17779:2000 Code of practice for information security management
2. ISO/IEC 21827: 2002 Information technology - Systems Security Engineering - Capability Maturity Model
3. NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems
4. Managing information security risks. Operationally Critical Threat, Asset and Vulnerability. Christopher Alberts and Audrey Dorofee, James Stevens, August, 2003.
5. A. Jøsang. A Logic for Uncertain Probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 9(3):279–311, June 2001.
6. A. Jøsang., S.J. Knapskog. A Metric for Trusted Systems. In Reinhard Posh, editor, Proceedings of the 15th IFIP/SEC International Information Security Conference. IFIP, 1998
7. A. Jøsang An Algebra for Assessing Trust in Certification Chains. In J. Kochmar, editor, Proceedings of the Network and Distributed Systems Security Symposium (NDSS'99). The Internet Society, 1999.
8. A. Jøsang. The Consensus Operator for Combining Beliefs, Distributed System Technology Centre, email: ajosang@dstc.edu.au
9. A. Jøsang. Prospectivies for Modelling Trust in Information Security, Distributed System Technology Centre, email: ajosang@dstc.edu.au.
10. Леншин А.В. Применение аппарата субъективной логики для оценки безопасности банковских ИТ-систем // Актуальні проблеми та перспективи розвитку фінансово-кредитної системи України: Збірник наукових статей. Харків: Фінарт, 2002, с.410-412.
11.Леншин А.В., Потий А.В. Применение оператора попарной усредненной конъюнкции для оценки уровня защищенности ИТ-систем // Збірник наукових статей за матеріалами VI міжнародної науково практичної конференції "Безпека інформації в інформаційно-телекомунікаційних системах",- Київ, 2003, с 57-58.
12. Потий А.В, Леншин А.В. Оценка защищенности информационно-телекоммуникационных систем с использованием математического аппарата субъективной логики //7-я Научно - практическая конференция «Безопасность информации в информационно – телекоммуникационных системах», Киев. 2004 р.

13. Потий А.В., Леншин А.В. Принципы построения системы экспертной оценки защищенности ИТ-систем «Советник» //Збірник наукових статей за матеріалами VI міжнародної науково практичної конференції “Безпека інформації в інформаційно-телекомунікаційних системах”,.- Київ, 2003, с 25-26. 14. Потій О.В., Лєншин А.В. Практичні рекомендації по використанню системи “Радник” при оцінці рівня організаційного захисту інформації в ІТС //7-я Научно - практическая конференция «Безопасность информации в информационно – телекоммуникационных системах», Киев. 2004 р.
15. A.Hunter. Uncertainty in information systems McGraw-Hill, London, 1996.
16. A. Motro and Ph. Smets. Uncertainty management in information systems: from needs to solutions. Kluwer, Boston, 1997.
17. G.Shafer A Mathematical Theory of Evidence. Princeton University Press, 1976. 18. Ph. Smets, R. Kennis The transferable belief model. Artificial Intelligence, 66:191-1-234, 1994.
19.G. de Cooman, D. Ayles. Supremum preserving upper probabilities. Information Sciences, 1998.
20. Daniel Ellsberg. Risk, ambiguity, and the Savage axioms. Quarterly Journal of Ecomonics

3. РОЗРОБЛЕННЯ ЕЛЕМЕНТІВ ПРОФІЛЮ ЗАХИСТУ У ВІДПОВІДНОСТІ ДО ВИМОГ МІЖНАРОДНОГО СТАНДАРТУ ISO/IEC 15408

3.1 Мета роботи

Закріпити теоретичні знання вимог міжнародного стандарту ISO/IEC 15408. Вивчити порядок розроблення, структуру та зміст профілю захисту засобу (системи) захисту інформації. Набути практичних навичок застосування інструментарію з розробки профілю захисту.

3.2 Методичні вказівки з організації самостійної роботи студентів

Під час підготовки до лабораторної роботи необхідно:

- ознайомитися з основними положеннями стандарту ISO/IEC 15408 за допомогою літератури, що надається у переліку;
- вивчити тему, програму виконання робіт, а також опис спеціалізованого забезпечення СС РКВ;
- підготувати бланк звіту, відповідно до розділу „Зміст звіту”;
- підготувати відповіді на контрольні запитання.

3.3 Основні теоретичні положення

3.3.1 Загальні положення

У 2000 році був прийнятий міжнародний стандарт ISO/IEC 15408 „Загальні критерії оцінки безпеки інформаційних технологій”. Це узгоджений стандарт, що розроблений на основі існуючих нормативних документів різних держав та з урахуванням досвіду в галузі захисту інформації.

Мета стандарту – створення єдиної методологічної основи для висування вимог безпеки до систем інформаційних технологій та здійснення оцінки властивостей (характеристик) безпеки цих продуктів.

Інформаційна технологія (ІТ) визначається як сукупність прийомів, способів та методів, застосування обчислюваної техніки та програмного забезпечення під час здійснення функцій збору, зберігання, обробки, передачі та використання даних.

Безпека інформаційних технологій характеризує захищеність інформації та ресурсів інформаційних технологій від впливу об'єктивних та суб'єктивних, зовнішніх та внутрішніх, випадкових та навмисних загроз, а також спроможність інформаційних технологій виконувати задані функції без нанесення втрат (шкоди) суб'єктам інформаційних взаємовідносин.

Безпека інформації це стан захищеності інформації, у якому забезпечується зберігання визначених політикою безпеки властивостей інформації.

Основними завданнями забезпечення безпеки інформації є:

- запобігання несанкціонованого розкриття інформації, тобто конфіденційності інформації;
- запобігання несанкціонованої модифікації інформації та ресурсів інформаційних технологій (ІТ-ресурсів), тобто забезпечення цілісності;
- забезпечення своєчасного санкціонованого отримання інформації та послуг інформаційних технологій, тобто забезпечення доступності;
- забезпечення спостережливості за діями суб'єктів та процесів.

Під час розгляду проблеми забезпечення (Рис.3.1) безпеки інформаційних технологій об'єктом забезпечення безпеки є інформація та ІТ-ресурси, які позначаються як активи. Суб'єктом забезпечення безпеки є власник активів, для кого вони представляють певну цінність. Важливим елементом моделі є зловмисник, який має певні мотиви, знання та можливості для незаконного використання активів. Це може призвести до нанесення втрат інтересам власника активів. Зловмисник розглядається як джерело загроз безпеки (агент загроз), тобто можливих подій, дій (впливів), процесів та явищ, які є потенційною небезпекою для активів. Реалізація загроз може призвести до втрат (шкоди) інтересам власника активів.

У зв'язку з цим власник активів вимушений вживати заходів, спрямованих на запобігання загрозам або зменшення ступеню небезпеки. Для ефективної протидії зловмиснику, власник активів має здійснити аналіз загроз. У якості загроз розглядаються загрози, які обумовлені яка **випадковими так і навмисними діями людей.**

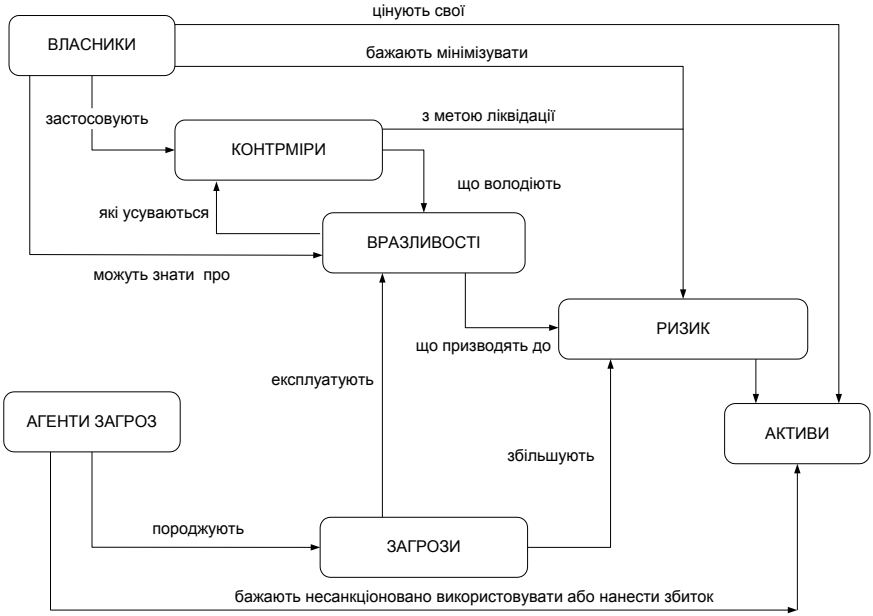


Рисунок 3.1 – Процес забезпечення безпеки ІТ

Загрози та існуючі вразливості є основними факторами ризику власника активів для зменшення або усунення якого він вживає заходи безпеки. Забезпечення безпеки інформаційних технологій це система заходів, які спрямовані на запобігання або нейтралізацію впливів загроз безпеки та на здійснення встановленої політики безпеки під час створення, функціонування та експлуатації систем та продуктів інформаційних технологій.

Продукти інформаційних технологій – це сукупність програмних, програмно-апаратних засобів інформаційних технологій, що являє собою визначені функціональні можливості та призначена як для безпосереднього (самостійного) використання, так і для включення у різноманітні системи інформаційних технологій.

Система інформаційних технологій –це конкретна реалізація інформаційних технологій з визначеним призначенням та умовами експлуатації, яка призначена для рішення задач автоматизації в конкретній області застосування.

3.3.2 Загальна модель об’єкту оцінки

Продукт або система інформаційних технологій разом із документацією (наприклад керівництв адміністратора та користувача) є предметом оцінки безпеки та називається об’єктом оцінки.

Сукупність правил, процедур, практичних прийомів та керівних принципів в галузі безпеки, якими керується організація у своєї діяльності, складає політику безпеки організації.

Сукупність правил, які регулюють управління ресурсами, їх захист та розподіл в середині продукту або системи інформаційних технологій та які виражаються за допомогою функціональних вимог безпеки, складають політику безпеки продукту (системи) інформаційних технологій.

Політика безпеки продукту (системи) ІТ, у свою чергу, включає множину політик функцій безпеки. Функція безпеки характеризує функціональні можливості частини або частин ІТ-продукту (системи), що забезпечують виконання підмножини правил політики безпеки ІТ-продукту (системи). Кожна політика функції безпеки має свою область застосування та можливості управління.

Сукупність всіх апаратних, програмно-апаратних та програмних засобів ІТ-продукту (системи), які реалізують сукупність всіх функцій безпеки ІТ-продукту (системи) та здійснюють політику безпеки, складає комплекс засобів захисту ІТ-продукту (системи).

Сукупність інтерфейсів, як інтерактивних (чоловічо-машинні інтерфейси), так і програмні (інтерфейси прикладних програм) з використанням яких здійснюється доступ до ресурсів ІТ-продукту (системи) за допомогою функцій безпеки складають інтерфейси функцій безпеки об’єкта.

На рисунку 3.2 надається загальна модель об’єкту оцінки.

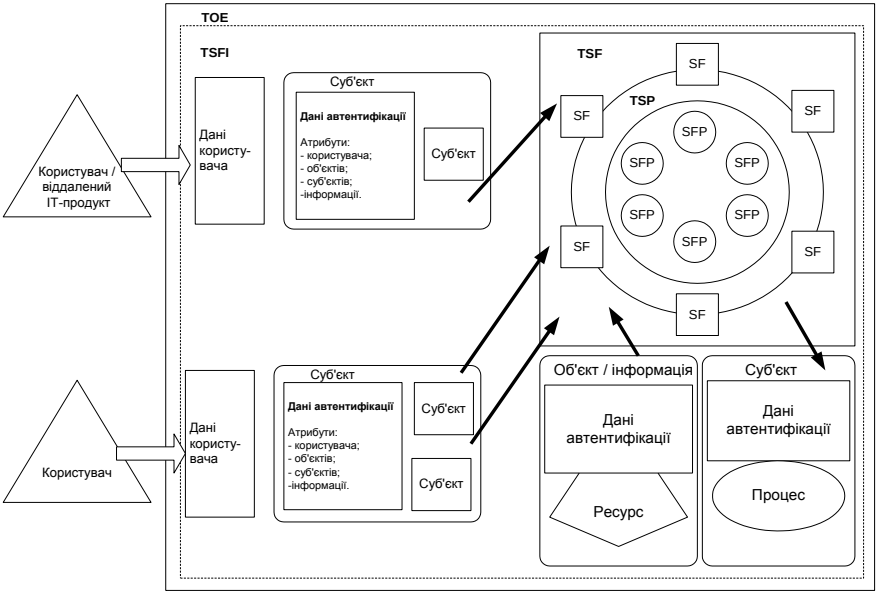


Рисунок 3.2 – Загальна модель об’єкту оцінки

TOE (Target of Evaluation) – об’єкт оцінки.

SFP (Security function policy) – політика функції безпеки.

TSP (TOE security policy) – політика безпеки об’єкту оцінки.

SF (security function) – функція безпеки.

TSF (TOE security function) – функції безпеки об’єкту оцінки.

TSFI (TOE security function interface) – інтерфейс функцій безпеки об’єкту оцінки.

3.3.3 Безпека у життєвому циклі ІТ-продуктів (систем)

Безпека інформаційних технологій досягається комплексним застосуванням законодавчих, організаційних та технологічних засобів безпеки, технічних та програмних засобів захисту на всіх етапах життєвого циклу ІТ-продуктів (систем). Міжнародний стандарт визначає основні процедури, заходи та методи, які мають використовуватися під час створення та застосування ІТ-продуктів (систем) з метою досягнення встановленого рівня гарантій безпеки.

Життєвий цикл ІТ-продукту (системи) складається з таких етапів:

- визначення призначення ІТ-продукту (системи), умов його застосування, формування цілей та вимог безпеки;
- проектування та розроблення ІТ-продукту (системи);
- впровадження та експлуатація ІТ-продукту (системи).

Формування вимог

Етап формування вимог безпеки ІТ-продукту (системи) є принципово важливим, оскільки від якісного його проведення залежить рівень всіх подальших проектних рішень та рівень безпеки, що буде досягнутий.

До множини вимог безпеки висуваються такі вимоги:

- повнота, якщо вимоги безпеки висунуті не в повній мірі, то ІТ-продукт (системи) не може відповідати своєму призначенню;
- узгодженість з цілями та умовами застосування ІТ-продукту (системи);
- відповідність вимогам нормативних документів (стандартів);
- перспективність, вимоги безпеки повинні враховувати перспективи розвитку можливостей зловмисників.

Підтримка життєвого циклу

Підтримка життєвого циклу це аспект встановлення дисципліни виконання та управління процесами вдосконалення ІТ-продукту (системи) під час його розроблення та супроводження. Гарантії відповідності ІТ-продукту (системи) вимогам безпеки більш надійні, якщо аналіз безпеки та формування відповідних свідчень (доказів) здійснюється на регулярній основі, як невід'ємна частина дій під час розроблення та супроводження.

Підтримка життєвого циклу здійснюється на основі прийняття повністю визначеної моделі життєвого циклу.

Розробка

Розробка – це процес створення зразка ІТ-продукту (системи), який задовольняє функціональним вимогам та вимогам гарантій.

Забезпечення безпеки у процесі розробки полягає у послідовній реалізації комплексу організаційно-технічних заходів у відповідності до технологічних етапів розробки на основі моделі життєвого циклу.

Оцінка безпеки

Оцінка безпеки ІТ-продукту (системи) здійснюється з метою перевірки можливостей функцій безпеки та вжитих під час розробки заходів забезпечення гарантій та відповідність вимогам, що визначені у технічному завданні з безпеки.

Експлуатація

Під час експлуатація безпека ІТ-продукту (системи) досягається:

- строгим виконанням оперативним персоналом вимог експлуатаційної документації на засоби захисту;
- додержанням всіх умов, які визначені для зовнішнього середовища;
- реалізацію розробниками заходів підтримки гарантій безпеки під час експлуатації.

На рисунку 3.3 надано структуру життєвого циклу ІТ-продукту (системи).

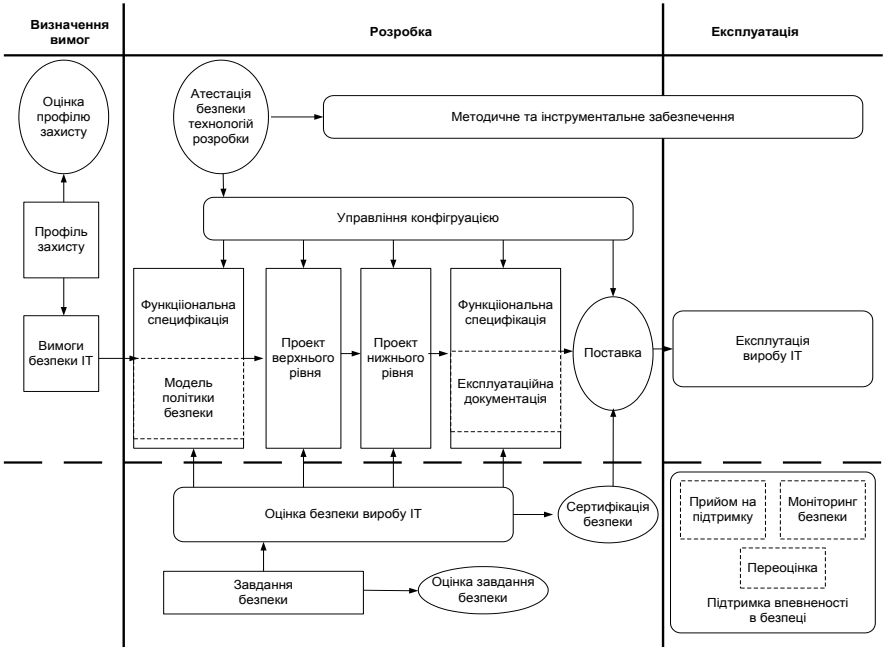


Рисунок 3.4 – Структура життєвого циклу ІТ-продукту

3.3.4 Загальний порядок формування вимог безпеки ІТ-продуктів (систем)

Міжнародний стандарт визначає загальний порядок формування вимог безпеки та базову структуру, в якій ці вимоги містяться.

На рисунку 3.4 надано загальний порядок формування вимог безпеки

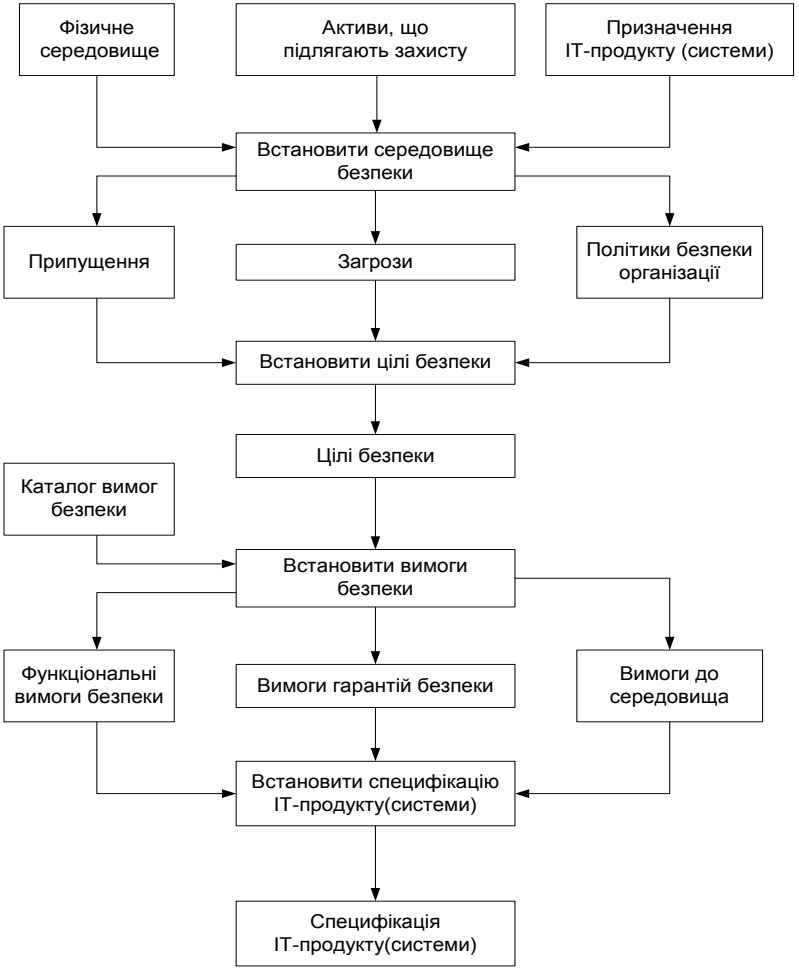


Рисунок 3.4 – Порядок формування вимог безпеки ІТ-продукту (системи)

Основними етапами формування вимог безпеки є:

I етап	Аналіз середовища безпека IT-продукту (системи)
II етап	Визначення та формулювання цілей безпеки
III етап	Встановлення вимог безпеки
IV этап	Розроблення специфікацій функцій безпеки

Аналіз середовища безпеки здійснюються з метою:

- відмежування комплексу засобів захисту IT-продукту (системи) від зовнішнього середовища;
- визначення ступеню небезпечності середовища для функціонування IT-продукту (системи);
- формування вихідних посилок для визначення цілей безпеки.

Середовище безпеки це сукупність фізичних, інформаційних, технічних об'єктів та систем, зовнішніх та внутрішніх по відношенню до IT-продукту (системи), а також організаційних заходів, правових норм, умов експлуатації та технологічних особливостей застосування IT-продукту (системи), що здійснюють фізичний, інформаційний, енергетичний та інші види впливу на функціонування IT-продукту (системи).

Таким чином, середовище безпеки визначає контекст застосування IT-продукту (системи), що передбачається. Під час визначення середовища безпеки мають бути враховані політики безпеки організації, відомі та потенційно можливі загрози безпеці, а також досвід розробників.

З метою встановлення середовища безпеки IT-продукту (системи), необхідно розглянути:

- фізичне середовище IT-продукту (системи), що визначає всі аспекти зовнішнього середовища, які мають відношення до безпеки, включаючи відомі умови безпеки фізичного розміщення IT-продукту (системи) та умови, які відносяться до персоналу;
- активи, що підлягають захисту з використанням функцій безпеки IT-продукту (системи). До активів відносяться інформаційні ресурси (файли, бази даних, електроні документи), а також інші ресурси, що забезпечують функціонування IT-продукту (системи), у тому числі технічні характеристики та область застосування.

Аналіз факторів зовнішнього середовища закінчується описом таких параметрів середовища:

- припущення про умови, які мають бути сформовані у середовищі, щоб ІТ-продукт (система) розглядався як безпечений;

- загрози безпеці, які можуть бути реалізовані по відношенню до ІТ-продукту (системи);

- заходи та правила поліпшення безпеки організації, які мають бути забезпечені по відношенню до ІТ-продукту (системи);

Таким чином, для встановлення середовища безпеки ІТ-продукту (системи) мають бути оцінені ризики та можливі втрати (шкода) від порушень безпеки. Ці оцінки є основою для визначення заходів та засобів протидії, які мають бути реалізовані під час розробки ІТ-продукту (системи).

Аналіз середовища безпеки здійснюється з метою формулювання цілей забезпечення безпеки ІТ-продукту (системи). Задачі захисту спрямовані на протидію загрозам безпеки, що виявлені та відповідають політиці безпеки організації та умовам, що визначені для середовища ІТ-продукту (системи). Задачі захисту явно виражають всі наміри суб'єкту захисту у відношення забезпечення безпеки ІТ-продукту (системи). Необхідно встановити, які Задачі захисту будуть реалізуватися функціями ІТ-продукту (системи), а які забезпечуються середовищем.

Вимоги безпеки є результатом перетворення цілей безпеки у сукупність вимог безпеки ІТ-продукту (системи) та вимог безпеки до середовища.

Вимоги безпеки ІТ-продукту (системи) складаються з функціональних вимог безпеки та вимог гарантій.

3.3.5 Представлення вимог безпеки. Профіль зрілості та завдання захисту

З метою забезпечення формалізованого встановлення вимог безпеки, вони представляються у вигляді ієрархічно впорядкованої системи груп вимог: клас – родина – компонент – елемент.

Клас використовується для найбільш загального групування вимог безпеки. Всі елементи класу мають загальну спрямованість.

Родина – групування вимог безпеки, які мають спільні задачі захисту, але відрізняються акцентуванням та суворістю вимог.

Компонент – специфічний набір вимог безпеки, який є мінімальним набором вимог для включення у профіль захисту.

Елемент – найнижчий неподільний рівень вимог безпеки, на якому здійснюється їх оцінка.

При встановлені вимог ІТ-продукту (системи) використовуються три типи конструкцій: пакет, профіль захисту та завдання захисту.

Пакет – це проміжний набір компонентів вимог безпеки, які задовольняють визначеної підмножині цілей безпеки. Пакет може використовуватися у структурі великих пакетів, профілів захисту та завдань захисту.

Профіль захисту – типовий набір вимог безпеки до сукупності ІТ-продуктів (системи), що не залежать від реалізації та відповідають визначеним цілям безпеки.

Завдання захисту - містить сукупність вимог безпеки до конкретного ІТ-продукту (системи), що забезпечують досягнення встановлених цілей безпеки.

На рисунку 3.5 а) наведено структуру профілю захисту. На рисунку 3.5 б) задана структура завдання захисту.

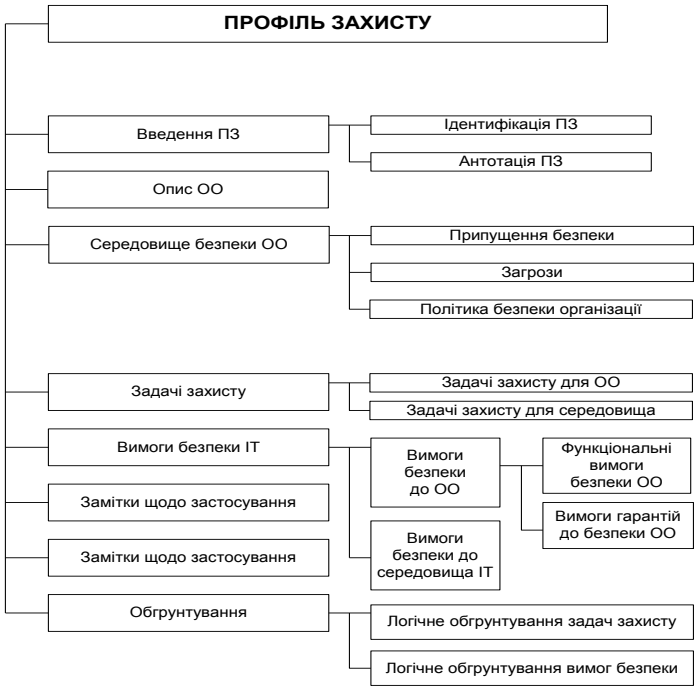


Рисунок 3.5 а) – Структура профілю захисту

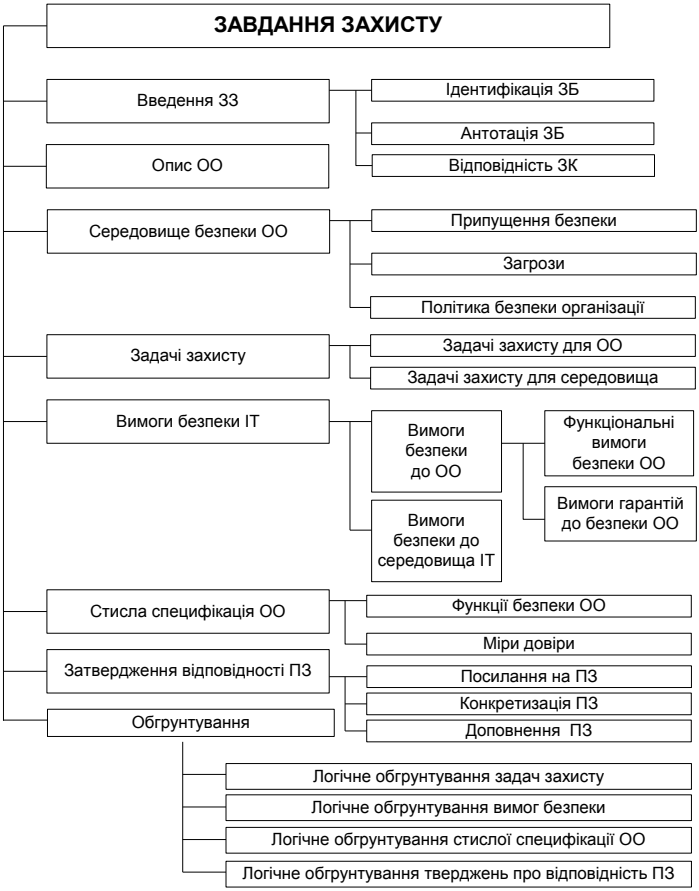


Рисунок 3.5 б) – Структура завдання захисту

З метою автоматизації процесу формування вимог безпеки розроблені спеціалізоване програмне забезпечення:

- база знань Common Criteria Profiling Knowledge Base (CC PKB);
- системи автоматизованого проектування CC Tools.

3.4 Стислий опис CC PKB

База знань CC PKB є базою даних, що розроблена у середовищі MS Access.

Призначення СС РКВ полягає у наданні інженеру з безпеки вихідних даних щодо загроз безпеки, цілей безпеки, положень та правил безпеки та вимог безпеки.

За допомогою СС РКВ можна:

- здійснити аналіз середовища ІТ-продукту (системи) та сформувати припущення щодо умов експлуатації;
- провести аналіз загроз безпеці та базових правил (положень) політики безпеки;
- визначити задачі захисту;
- визначити вимоги безпеки;

Таким чином СС РКВ здійснює інформаційне забезпечення процесу формування вимог безпеки.

Структура СС РКВ надана на рисунку 3.6

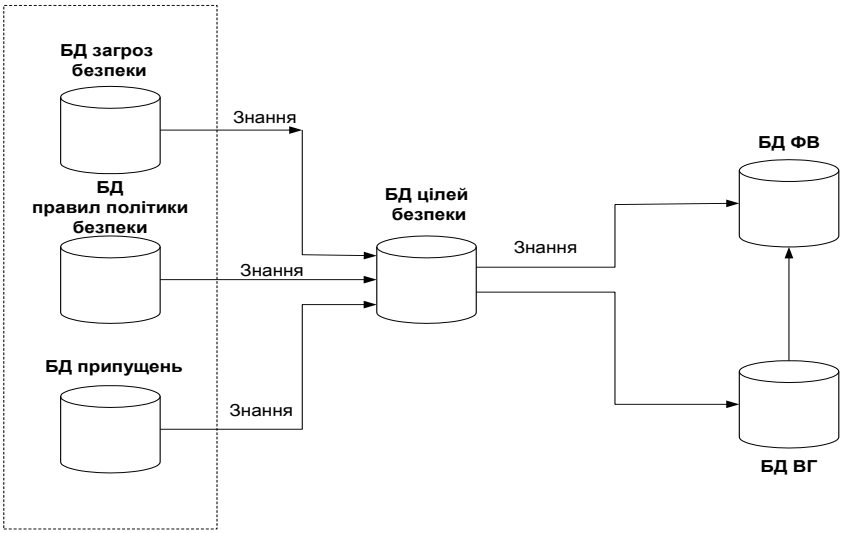


Рисунок 3.6 – Загальна структура СС РКВ

До складу СС РКВ входять:

- база даних загроз безпеки;
- база даних правил політик безпеки;
- база даних припущень з підказками;
- база даних цілей безпеки;
- база даних функціональних вимог та вимог гарантій

Між елементами бази даних встановлені логічні зв'язки, що відбивають знання експертів.

За допомогою основної форми (Рис. 3.7) можна отримати доступ до елементів будь-якої бази даних.

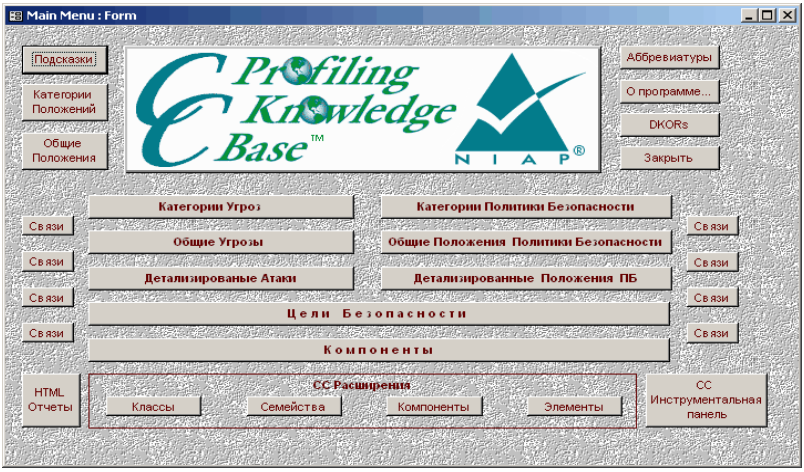


Рисунок 3.7 Зовнішній вигляд основної форми СС РКВ

База даних загроз безпеці складається з трьох баз даних: база даних джерел загроз, база даних загальних загроз, база даних атак. Елементи бази даних утворюють ієрархію загроз безпеці (Рис. 3.8)

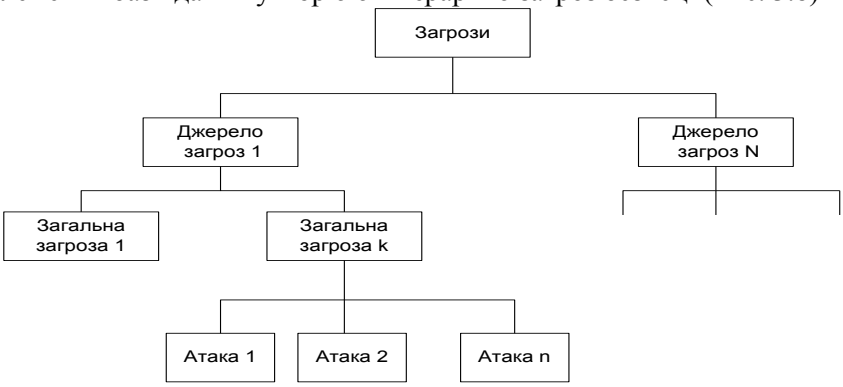


Рисунок 3.8 – Ієрархія загроз

На рисунках 3.9 -3.11 наведено форми, що надають доступ до баз даних джерела загроз, загальних загроз та атак відповідно.

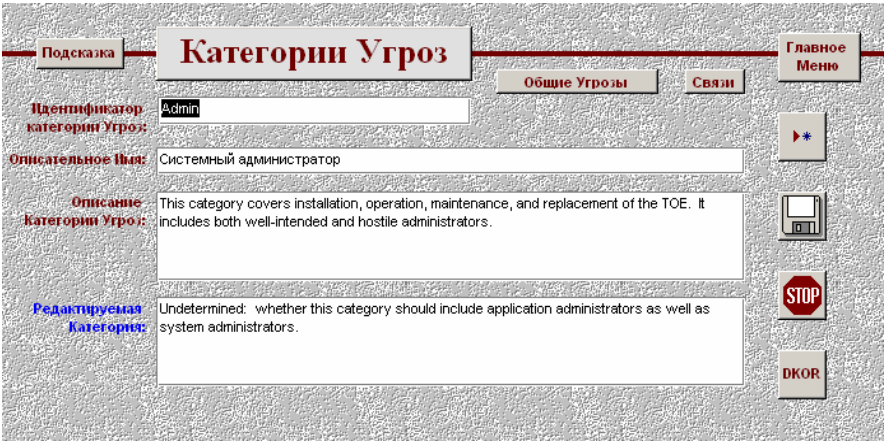


Рисунок 3.9 – Форма „Джерело загрози”

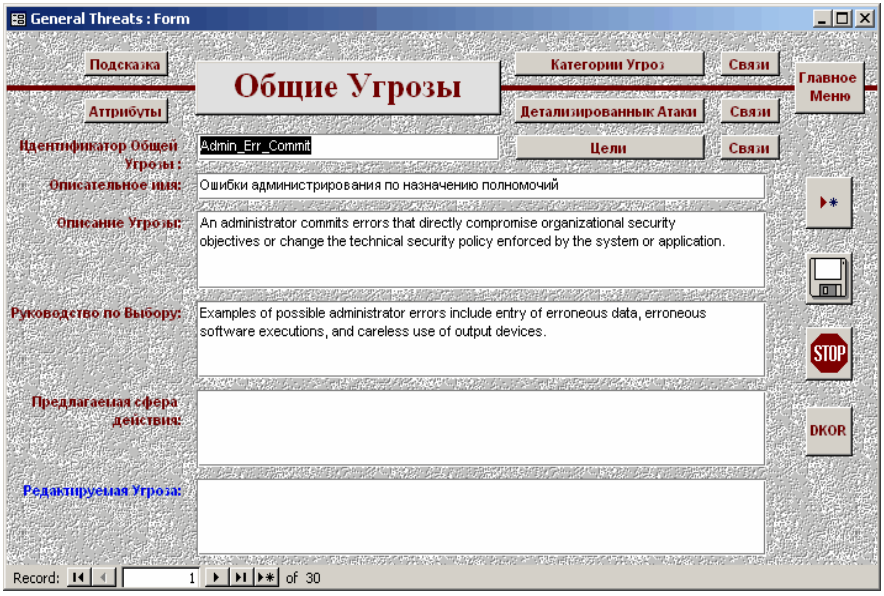


Рисунок 3.10 – Форма „Загальні загрози”

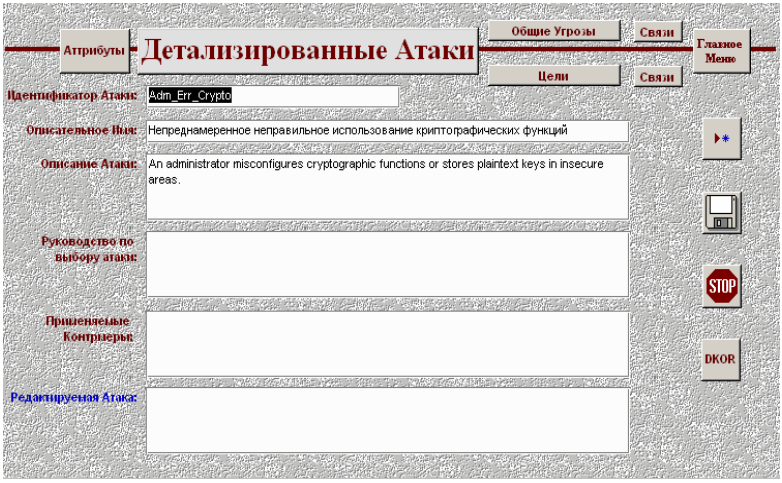


Рисунок 3.11 – Форма „Атаки”

Встановлено шість основних джерел загроз:

- системний адміністратор;
- неавторизована особа (зловмисник);
- фізичне середовище;
- розробник IT-продукту (системи);
- системне / апаратне / програмне забезпечення;
- авторизований користувач.

Для кожного джерела загроз визначені відповідні загальні загрози. Зв’язок між джерелом загроз та загальними загрозами можна визначити за допомогою форми-відображення зв’язків (Рис. 3.12)

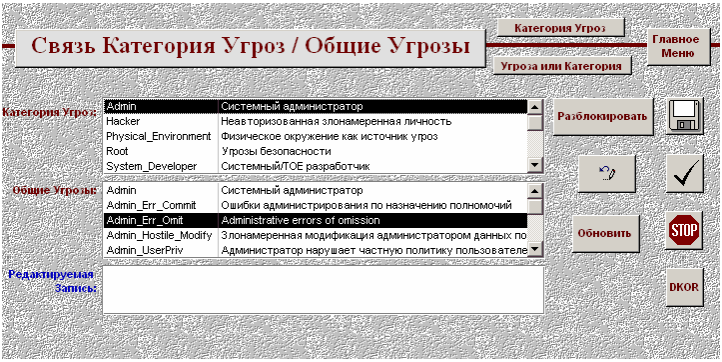


Рисунок 3.12 – Форма-відображення зв’язків „Джерело загроз/загальні загрози”

Для кожної загальної загрози встановлені відповідні атаки. Зв'язок встановлюється формою-відображенням зв'язків „Загальна-загроза/атака"(Рис. 3.13)

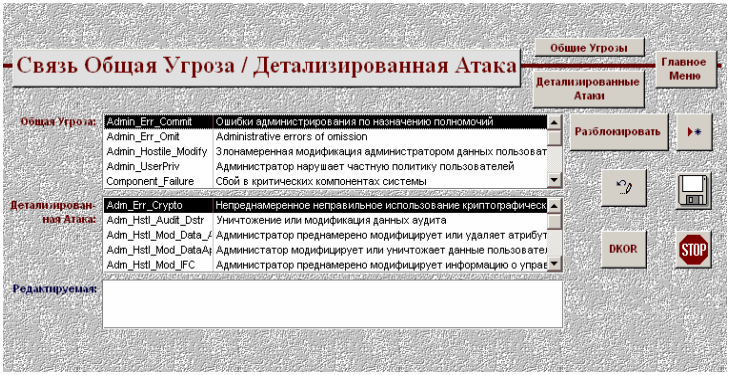


Рисунок 3.13 – Форма-відображення зв'язків „Загальна-загроза/атака"

Використовуючи ці форми можна проаналізувати та побудувати відповідне дерево загроз для IT-продукту (системи).

Аналогічну структуру побудови має база даних політик безпеки, яка складається з бази даних категорій політик (визначено дві категорії), бази даних положень політик безпеки та бази даних правил політик безпеки. На рисунках 3.14-3.16 наведено форми, що надають доступ до відповідних баз даних. На рис 3.17 та 3.18 надано відповідні форми-відображення зв'язків.

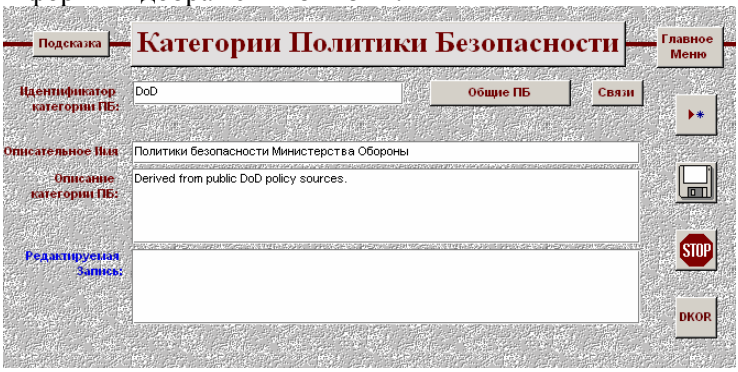


Рисунок 3.14 – Форма „Категорії політик"

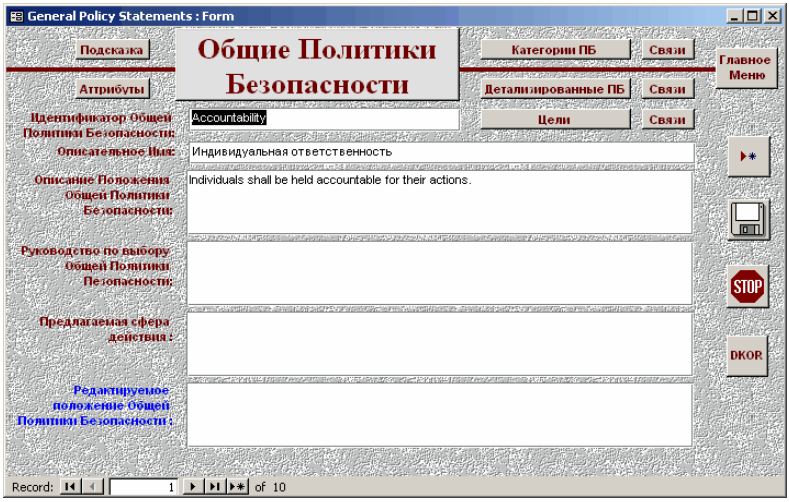


Рисунок 3.15 – Форма „Загальні положення політик безпеки”

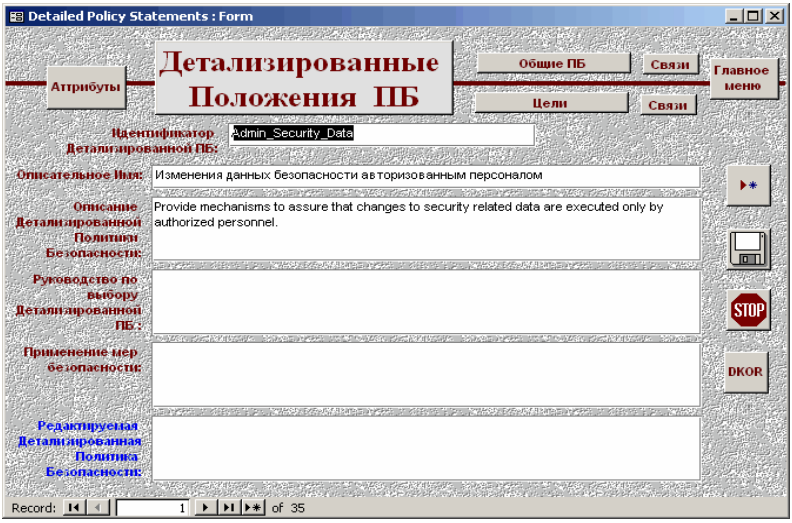


Рисунок 3.16 – Форма „Правила політик безпеки”

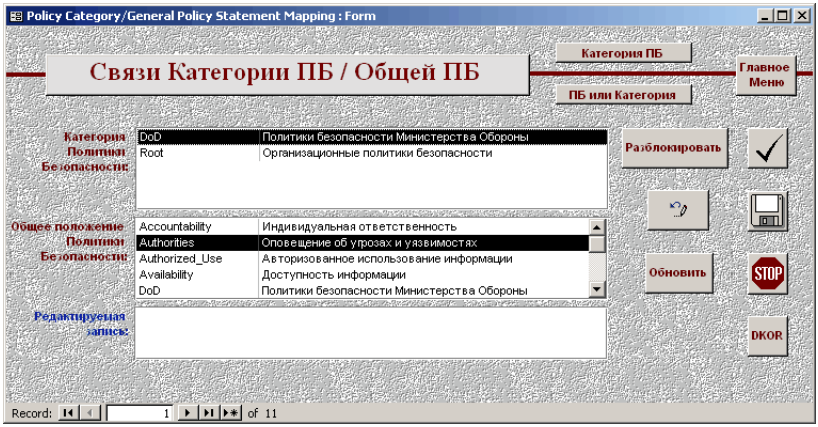


Рисунок 3.17 – Форма-відображення зв'язків „Категорії політик / Загальні положення політик безпеки"

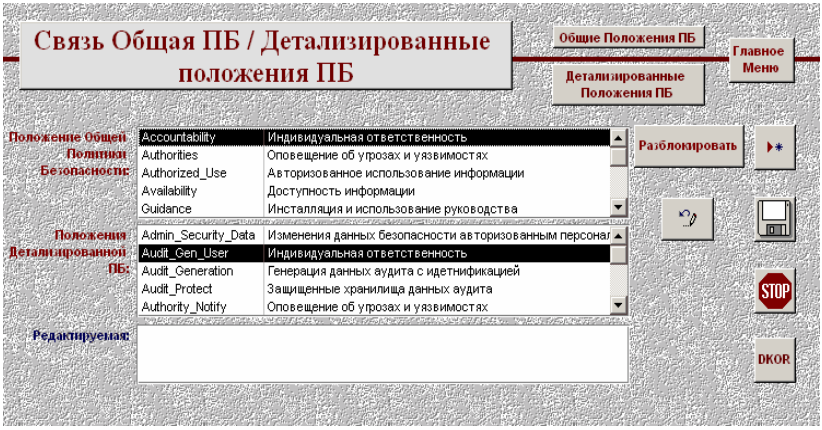


Рисунок 3.18 – Форма-відображення зв'язків „Загальні положення політик безпеки/ Правила політик безпеки"

Таким чином правила політик безпеки також організовані в ієрархію (Рис. 3.19). У поточній версії надана ієрархія правил безпеки міністерства оборони США, але користувач може власноруч визначити відповідну ієрархію правил безпеки.

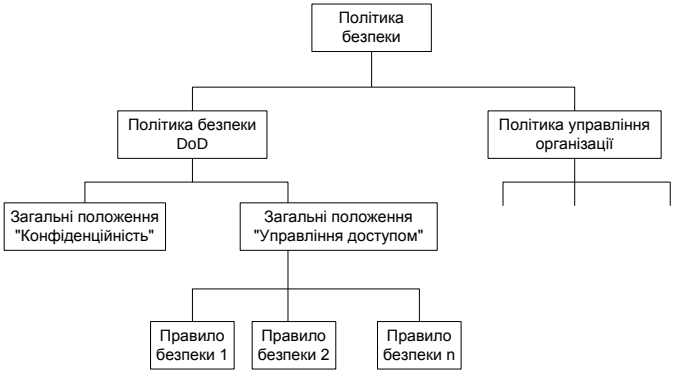


Рисунок 3.19 – Ієрархія правил політики безпеки

База даних „Задачі захисту” містить 155 визначених цілей безпеки. На рисунку 3.20 наведено форму „Задачі захисту”, за допомогою якої можна отримати доступ до елементів бази .

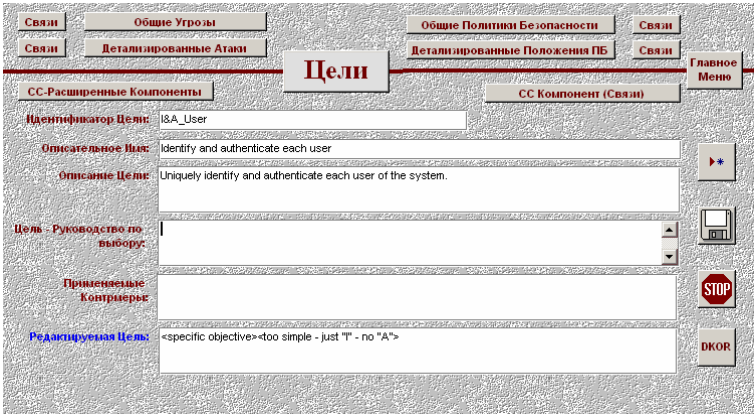


Рисунок 3.20 – Форма „Задачі захисту”

Елементи бази містять ідентифікатор задачі, унікальне ім’я задачі, опис задачі, рекомендації щодо вибору задачі, можливі напрямки досягнення задачі.

Формування цілей здійснюються на основі визначення загроз безпеці та аналізу положень та правил безпеки. На рисунку 4.16 наведено структуру логічних зв’язків між елементами баз даних загроз безпеки, політик безпеки та цілей безпеки.

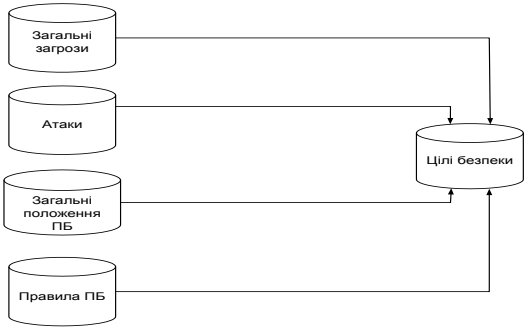


Рисунок 3.21 – Структура логічних зв’язків баз даних

На рисунках 3.21 -3.24 надано відповідні форми-відображення зв’язків, які допомагають встановити необхідні зв’язки між елементами баз даних.

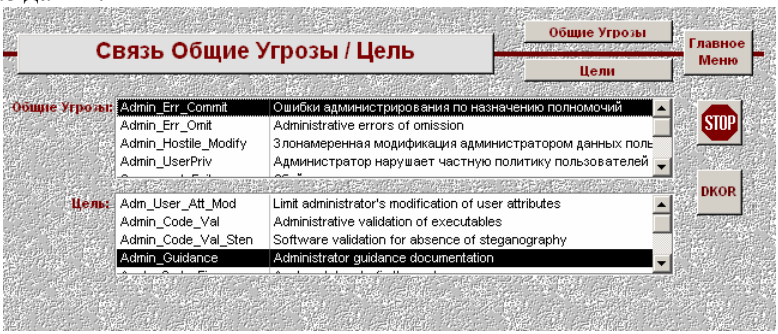


Рисунок 3.21 – Форма-відображення зв’язків „Загальні-загрози/ задачі захисту”

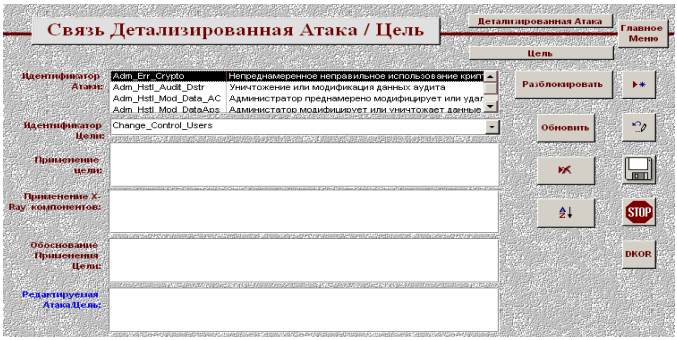


Рисунок 3.22 – Форма-відображення зв’язків „Атаки/ задачі захисту”

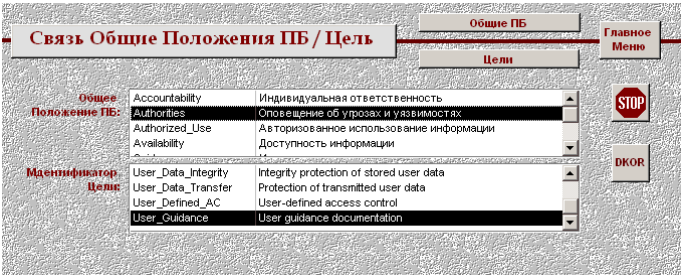


Рисунок 3.23 – Форма-відображення зв'язків „Положення ПБ/ задачі захисту"

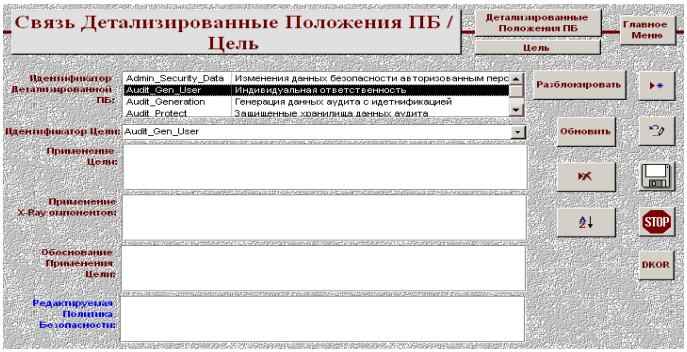


Рисунок 3.24 – Форма-відображення зв'язків „Правила ПБ/ задачі захисту"

База даних вимог безпеки відображає ієрархію вимог безпеки, що закріплена в міжнародному стандарті (Рис. 3.25)

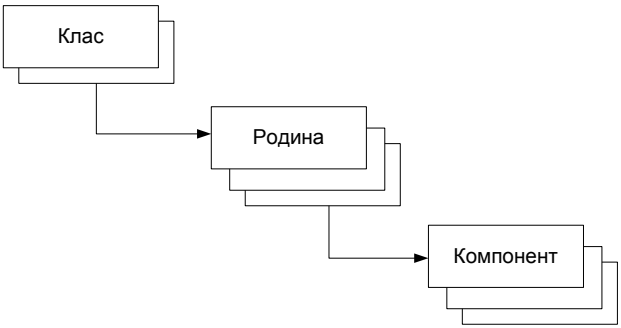


Рисунок 3.25 – Ієрархія вимог безпеки

На рисунках 3.26-3.28 наведено відповідні форми.

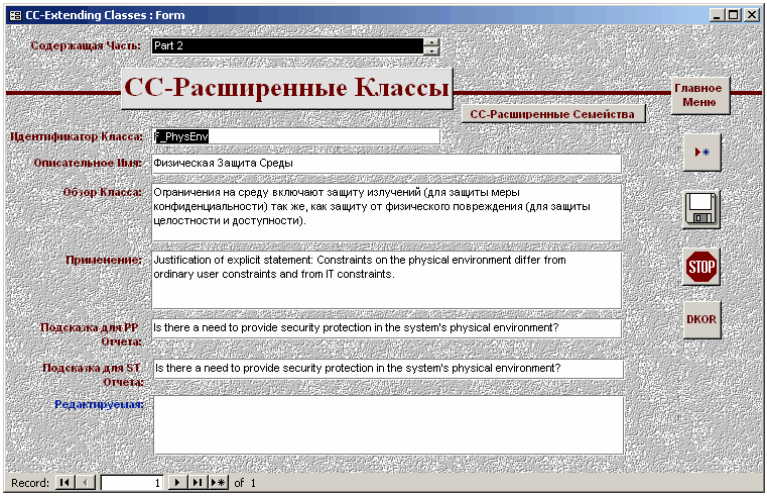


Рисунок 3.26– Форма „Класи вимог”

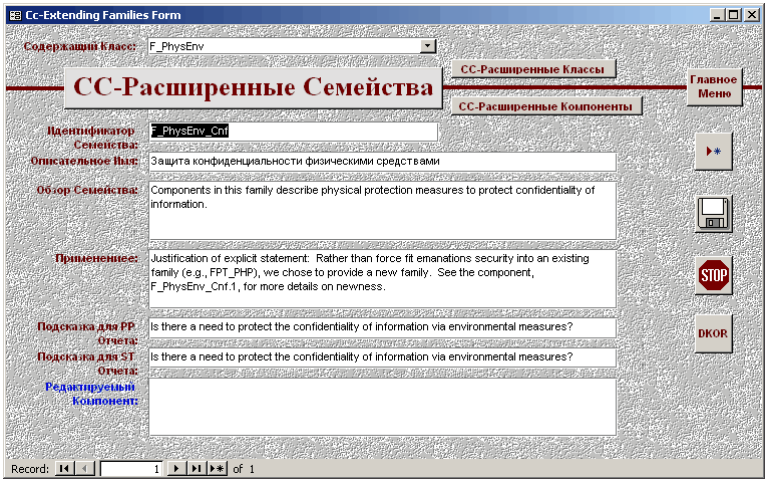


Рисунок 3.27– Форма „Родини вимог”

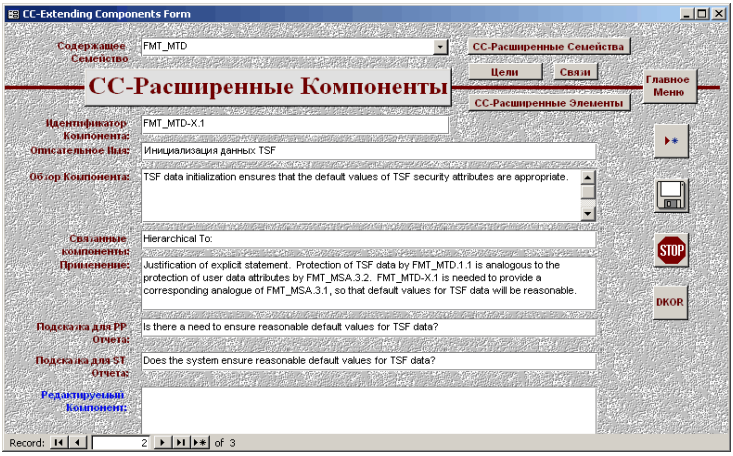


Рисунок 3.28– Форма „Компоненти”

Між елементами бази даних „Задачі захисту” та „Компоненти вимог” встановлені зв’язки, що визначають, які функціональні вимоги та вимоги гарантій необхідно обрати для досягнення задачі захисту. На рисунку 3.29 наведено форму-відображення зв’язків, яка допомагає відстежити такі зв’язки.

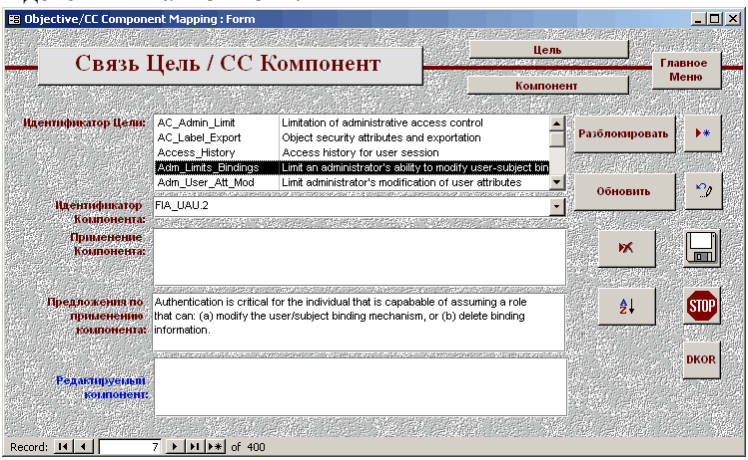
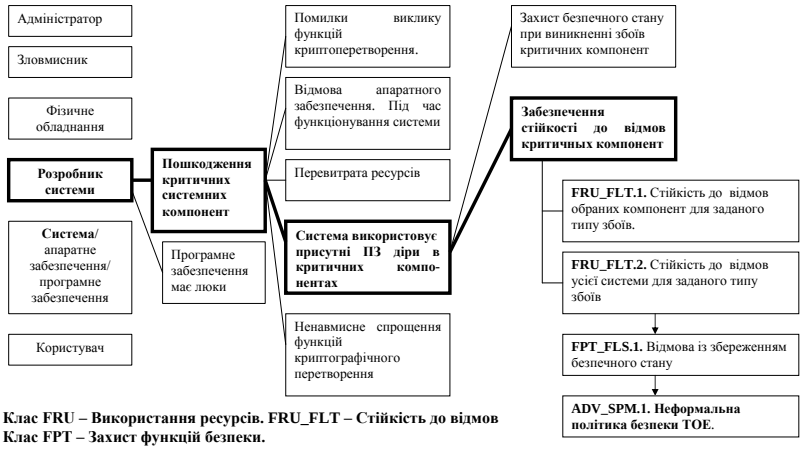


Рисунок 3.29 – Форма-відображення зв’язків „Задачі захисту / Компоненти вимог”

Таким чином, використовуючи базу знань СС РКВ можна провести аналіз середовища, загроз безпеці та політики безпеки, обрати

задачі захисту та відповідні функціональні вимоги безпеки, вимоги гарантій, а також здійснити опис всіх цих елементів.

На рисунку 3.30 наведено приклад формування вимог безпеки.



Клас FRU – Використання ресурсів. FRU_FLT – Стійкість до відмов
Клас FPT – Захист функцій безпеки.
Клас ADV – Вимоги до розробки
ADV_SPM – Моделювання політики безпеки. (Вимоги до розробника та завдання експерта).

Рисунок 3.30– Приклад формування вимог безпеки

3.5 Методика формування функціональних вимог безпеки та вимог гарантій

Розглянемо методику формування функціональних вимог безпеки та вимог гарантій за допомогою бази СС РКВ.

На рисунку 3.31 надано контекстна діаграма процесу формування вимог безпеки.

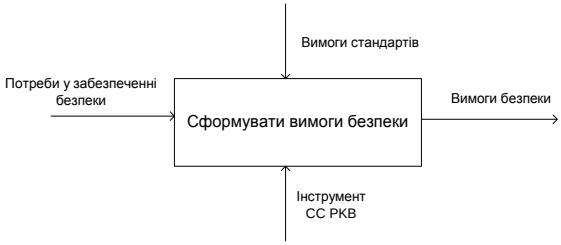


Рисунок 3.31 – Контекстна діаграма процесу формуванням вимог безпеки

Декомпозиція контекстної діаграми приводить до наступної функціональної діаграми (Рис. 3.32–3.33).

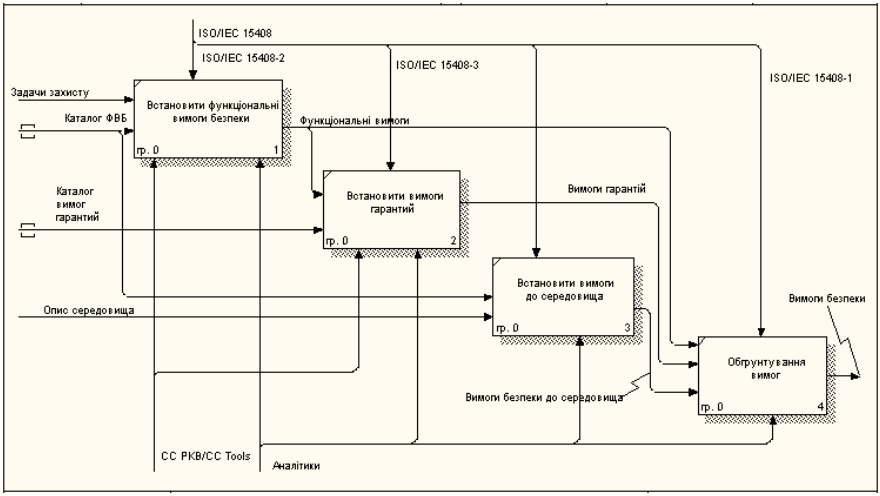


Рисунок 3.32 – Декомпозиція діаграми процесу формуванням вимог безпеки

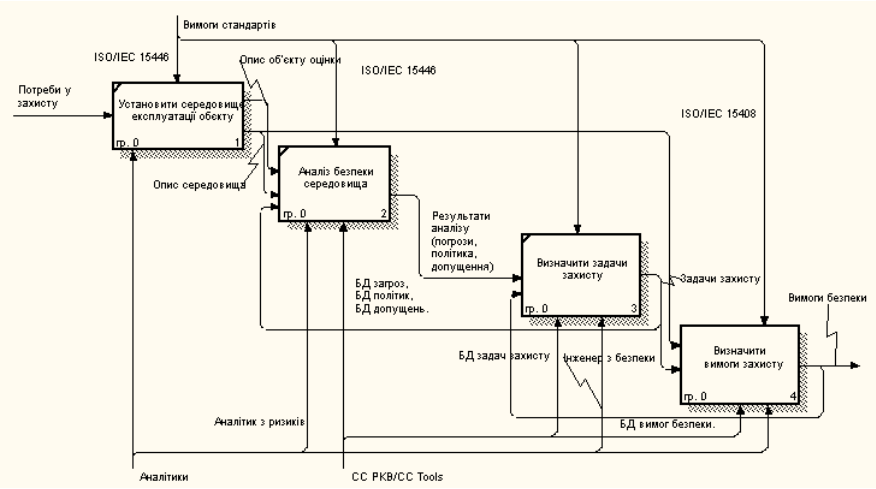


Рисунок 3.33 – Декомпозиція діаграми обґрунтування вимог

Вхідними даними для процесу формування вимог є потреби у забезпеченні безпеки, які напрдикінці будуть перетворені у вимоги безпеки.

Першим кроком є задача визначення середовища безпеки об'єкту оцінки. На основі загального уявлення про об'єкт оцінки інженер здійснює загальний опис об'єкту оцінки та середовища безпеки. Під час виконання цієї задачі інженер керується вимогами стандарту ISO/IEC 15408 та ISO/IEC 15466 (розділ 4). Результатами виконання задачі є:

- опис об'єкту оцінки, який як мінімум має містити визначення об'єкту оцінки, призначення та послуги (функції), що надаються об'єктом оцінки;
- первинний опис середовища безпеки який містить опис фізичного середовища, логічного середовища, опис взаємодії об'єкту оцінки з середовищем, суб'єктів які безпосередньо виконують функції об'єкту оцінки, характеристики потенційних порушників та ресурси (активи), які підлягають захисту.

Отримані дані беруться до уваги під час аналізу середовища безпеки.

Наступний крок – аналіз середовища.

Аналіз середовища здійснюється з метою встановлення потенційних загроз безпеці, визначення правил політики безпеки та допущення безпеки. Вхідними даними є відповідні каталоги, що містяться у базах даних СС РКВ. Керівні вказівки містяться в ISO/IEC 15466. Інструментарій, що використовується аналітиком ризиків, є відповідним базі даних СС РКВ.

Результатом виконання задач є:

- опис загроз безпеці;
- опис положень (правил) політики безпеки;
- опис допущень щодо безпеки.

Загрози безпеки, положення (правила) безпеки та опис допущень щодо безпеки є основою для визначення задач захисту. Задачі захисту формулюються у відповідності до рекомендацій ISO/IEC 15466 (розділ 5). Вхідними даними є каталог стандартних задач захисту. Враховуючи взаємозв'язок типу:

$$\{загроза\ безпеці\} \rightarrow \{задача\ захисту\}$$
$$\{правила\ безпеки\} \rightarrow \{задача\ захисту\}$$

$$\{допущення\ щодо\ безпеки\} \rightarrow \{задача\ захисту\}$$

що встановлюється СС РКВ формується вихідний результат роботи – множина задач захисту.

Останнім етапом є формування вимог безпеки. На рисунку 5.3 надано декомпозицію задачі „Визначити вимоги безпеки". Ця задача складається за таких підзадач:

- встановлення функціональних вимог безпеки до об'єкту оцінки;
- встановлення вимог гарантій безпеки;
- встановлення вимог безпеки до середовища;
- обґрунтування вимог безпеки .

Функціональні вимоги визначаються у відповідності до вимог ISO/IEC 15408 та ISO/IEC 15466 та з урахуванням задач захисту. Вхідними даними є каталог функціональних вимог безпеки. Сутність формування полягає у виборі функціональних вимог безпеки, які спрямовані на вирішення визначених задач захисту та адаптування їх стандартної форми до конкретного об'єкту оцінки. Проектування полягає у виконанні над стандартними вимогами встановлених операцій (призначення, вибір, уточнення, повторення). Відображення $\{задача\ захисту\} \rightarrow \{функціональна\ вимога\ безпеки\}$ визначається за допомогою СС РКВ.

Вхідними даними є стандартизований каталог вимог гарантій. Сутність формування полягає у виборі вимог гарантій безпеки, які спрямовані на вирішення визначених задач захисту.

Відображення $\{задача\ захисту\} \rightarrow \{вимога\ гарантій\ безпеки\}$ визначається за допомогою відповідної форми СС РКВ.

За необхідністю формується вимога безпеки для середовища об'єкту оцінки.

Останнім етапом формування вимог безпеки є їх обґрунтування. На етапі обґрунтування здійснюють:

- обґрунтування вибору задач захисту;
- обґрунтування вибору функціональних вимог безпеки;
- встановлення залежності обраних компонентів вимог безпеки.

Обгрунтування вибору задач захисту здійснюється шляхом встановлення того, що для визначених загроз безпеці, встановлених правил політики та допущень визначені відповідні задачі захисту. Тобто встановлюється відображення множин: $Thr \times Obj$; $Pol \times Obj$; $Ass \times Obj$

Thr - множина загроз безпеці

Pol - множина правил політики безпеки

Ass - множина допущень

Obj - множина задач захисту

Необхідно довести, що кожному елементу множини T, P, A відповідає один або декілька елементів з множини O

Таблиця 3.1 Відповідність загроз безпеці задачам захисту

Загрози безпеці	Задачі захисту			
	Obj.1	*Obj*.2	…	*Obj.N*
Thr.1	X			X
Thr.2		X		X
⋮				
Thr.M		X		

Таблиця 3.2 Відповідність політик безпеки задачам захисту

Правил безпеки	Задачі захисту			
	Obj.1	*Obj*.2	…	*Obj.N*
Pol.1	X			
Pol.2	X	X		
⋮		X		
Pol.K		X		

Таблиця 3.3 Відповідність допущень щодо безпеки задачам захисту

Допущення	Задачі захисту			
	Obj.1	*Obj*.2	…	*Obj.N*
Ass.1	X			
Ass.2	X			
⋮				
Ass.L		X		X

Обгрунтування вибору функціональних вимог безпеки полягає у логічному доведені того, що для вирішення конкретної задачі захисту необхідно виконання визначених функціональних вимог безпеки. Таким чином встановлюється відображення множини задач захисту Obj множині функціональних вимог безпеки Fsr

$$Obj \times Fsr$$

Обов'язковим є виконання принципу повноти покриття, тобто кожному елементу $\{Obj\}$ має бути встановлений у відповідність один або декілька елементів з $\{Fsr\}$.

Вимоги гарантії безпеки визначаються у відповідності до вимог ISO/IEC 15408 та ISO/IEC 15466 (розділ 6). Для визначення вимог гарантій необхідно врахувати:

- задачі захисту;
- рівень гарантій, що вимагається;
- встановлені функціональні вимоги безпеки.

3.6 Порядок виконання роботи

3.6.1 Запустити базу СС КВ та вивести на екран основну форму (Рис. 3.7)

3.6.2 Виконати повний цикл формування вимог безпеки з урахуванням методики

3.6.2.1 Складається опис визначеного джерела загроз (джерело загроз визначає викладач для кожної бригади окремо) (Рис. 3.9).

3.6.2.2 Визначити для джерела загроз повну множин загальних загроз безпеці (Рис. 3.12).

3.6.2.3 Обрати одну загальну загрозу безпеки (кожен член бригади обирає свою загальну загрозу) та скласти опис загальної загрози безпеці (Рис. 3.10).

3.6.2.4 Для обраної загальної загрози безпеці побудувати повну множину атак за допомогою форми „Загальні загрози/ атаки" (Рис. 3.13).

3.6.2.5 Обрати дві атаки та скласти їх опис за допомогою форми „Атаки" (Рис. 3.11).

3.6.2.6 Для обраних атак побудувати повну множину задач захисту та побудувати відповідне дерево (Рис. 3.34). Скласти опис всіх задач захисту за допомогою БД „Задачі захисту" (Рис. 3.20).

3.6.2.7 Із множини задач захисту обрати дві задачі захисту та скласти для них повну множину функціональних вимог безпеки та вимог гарантій. Побудувати відповідне дерево.

3.6.2.8 Скласти опис функціональних вимог безпеки за допомогою каталогу вимог (ISO/IEC 15408-2).

3.6.2.9 Здійснити обґрунтування вимог безпеки шляхом побудови:

- таблиці відповідності задачі захисту / функціональні вимоги безпеки;
- таблиці залежностей компонентів функціональних вимог безпеки.

3.6.3 Підготувати звіт за результатами роботи.

Звіт має містити:

- опис джерела загроз, обраної загальної загрози, обраних атак;
- опис задач захисту, які спрямовані на запобігання встановленим атакам;
- дерево загроз, задач захисту та вимог безпеки;
- опис вимог безпеки;
- таблиці відповідності п. 3.6.2.9.

3.7 Контрольні запитання та завдання

3.7.1 Нехай задана функціональна вимога безпеки Fsr . За допомогою СС РКВ визначте які задачі захисту можна вирішити за допомогою цієї вимоги безпеки.

Таблиця 3.4 Варіанти вимог безпеки.

№	Ідентифікатори вимоги	Вимоги безпеки
1	FCS_CKM.3	Доступ до криптографічних ключів
2	FCO_NRO.1	Вибірковий доказ відправлення
3	FDR_PSE.1	Псевдоанонімність
4	FTA_LSA.1	Обмеження області атрибутів, що обираються
5	FAU_SAA.3	Проста евристика атаки
6	FDP_ACF.1	Управління доступом на основі атрибутів безпеки
7	FDP_IFC.2	Повне управління інформаційними потоками

8	FDP_ACC.1	Обмежене управління доступом
9	FPT_RCV.1	Ручне відновлення
10	FPT_ RCV.2	Автоматичне відновлення без втрат
11	FPT_ITC.1	Конфіденційність даних функції безпеки, що експортується, під час передавання
12	FPT_ITI.1	Виявлення модифікації даних функцій безпеки, що експортуються
13	FMT_MOF.1	Управління режимом виконання функцій безпеки
14	FMT_MSA.3	Ініціалізація статичних атрибутів
15	FMT_REV.1	Відміна

3.7.2 Задана задача захисту Obj . За допомогою СС РКВ визначте:

а) на запобігання яких загроз безпеки спрямовано досягнення задачі захисту;

б) на задоволення яких правил політик безпеки спрямовано вирішення цієї задачі захисту.

Таблиця 3.5 Варіанти задач захисту

№	Ідентифікатори задачі захисту	Задачі захисту
1	Access_History	Забезпечення доступу до сесії користувачів
2	Admin_Code_Val_Sten	Перевірка програмного забезпечення на предмет відсутності стеганографічних закладок
3	Apply_Code_Fixes	Застосування програмних оновлень
4	EMSEC_Design	Забезпечення захисту від ПЕМІН
5	Encryption_Access	Захист шифрованого тексту
6	No_Residual_Info	Закриття допоміжної інформації
7	Security_Func_Mgt	Керівництво функціями безпеки
8	TSF_Snd_Err_ID_Rem	Віддалене визначення факту модифікації критичних даних в момент передачі по каналах зв’язку

3.7.3 Задано правила безпеки Pol . За допомогою СС РКВ визначте:

а) задачі захисту, які спрямовані на реалізацію правила безпеки;
б) на запобігання яких загроз безпеці спрямовані визначні задачі захисту.

Таблиця 3.6 Варіанти правил безпеки

№	Ідентифікатори правила	Правила безпеки
1	Admin_Security_Data	Зміна даних безпеки лише авторизованим персоналом
2	Audit_Protect	Захист сховищ даних аудиту
3	Change_Control_Users	Сповіщення про дані, що були модифіковані
4	Documented_Recovery	За документування плану відновлення
5	Integrity_Data/SW	Використання сильних механізмів забезпечення цілісності
6	Maintenance_Prvnt	Проведення профілактичного технічного обслуговування
7	Malicious_Code	Проведення профілактику по виявленню шкідливого коду
8	Screen_Lock	Блокування екрану користувача

3.7.4 Конфіденційна інформація організації обробляється на АСУ класу 1 (згідно НД ТЗІ 2.5-002-99). У відповідності до вимог ISO/IEC 15408 зробить опис середовища безпеки АС класу 1 та за допомогою СС РКВ визначте допущення щодо безпеки. Сформулюйте відповідний розділ профілю захисту.
3.7.5 Наведіть загальний порядок формування вимог безпеки та поясніть призначення кожного етапу формування вимог.
3.7.6 Здійсніть аналіз етапу „Аналіз середовища безпеки” побудуйте діаграму декомпозиції етапу.
3.7.7 Здійсніть аналіз етапу „Визначення задач захисту” та побудуйте діаграму декомпозиції етапу.
3.7.8 Наведіть структуру профілю захисту, розкрийте зміст елементів профілю захисту. Чим відрізняється за змістом та призначенням профіль захисту та завдання із захисту?
3.7.9 Наведіть структуру СС РКВ. Які основні бази даних входять до СС РКВ? У чому полягає зв’язок між базами даних?
3.7.10 Наведіть структуру БД „Загрози безпеці” та БД „Політики безпеки”

Рекомендована література для самостійної роботи

1. ISO/IEC 15408:2000 – Information technology – Security techniques – Evaluation criteria for IT security. – Part 1: Introduction and general model.

2. ISO/IEC 15408:2000 – Information technology – Security techniques – Evaluation criteria for IT security. – Part 2: Security functional requirements.

3. ISO/IEC 15408:2000 – Information technology – Security techniques – Evaluation criteria for IT security. – Part 3: Security assurance requirements.

4. ISO/IEC WD 15292 – Information Technology – Security techniques – Protection Profile registration procedures – 1999.

5. CEM-97/017 – Common Evaluation Methodology for Information Technology security. – Part 1: Introduction and general model. – Ver. 0.6 – 1997.

6. CEM-99/008 – Common Evaluation Methodology for Information Technology security. – Part 2: Evaluation Methodology. – Ver. 0.6 – 1999.

7. Горбенко И.Д., Потий А.В, Терещенко П.И. Критерии и методология оценки безопасности информационных технологий // Радиотехника. Всеукраинский межвед. научн.-техн. сб. – 2000. – Вып. 114. – С. 25-38.

8. Скрыпник Л.В, Потий А.В. Гибкость и специализация профиля защиты автоматизированной системы // Радиотехника. Всеукраинский межвед. научн.-техн. сб. – 2001. – Вып. 119. – С. 17-21.

9. Горбенко И.Д., Потий А.В., Терещенко П.И. Рекомендации международных стандартов по оценке безопасности информационных технологий //Материалы третьей международной научно-практической конференции «Безопасность информации в информационно-телекоммуникационных системах». – Киев 2000. – С. 150-160.

10.Бондаренко М.Ф., Черных С.П., Горбенко И.Д., Замула А.А., Ткач А.А. Методологические основы концепции и политики безопасности информационных технологий // Радиотехника. Всеукраинский межвед. научн.-техн. сб. – 2001. – Вып. 119. – С. 5-17.

11.ISO 7498-2:1989 – Information technology – Open Systems Interconnection – Basic reference model – Part 2: Security architecture.

12.ISO/IEC 10181-(1-7):1996 – Information technology – Open Systems Interconnection – Security frameworks for open systems.

13.Щербо В.К. Стандарты вычислительных сетей. Взаимосвязи сетей. Справочник. – М.:Кудиц-образ, 2000. – 198 с.

14.НД ТЗИ 1.1 – 002 – 99. Основные положения по защите информации в компьютерных системах от несанкционированного доступа.

15.НД ТЗИ 1.1 – 003 –99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа.

16.НД ТЗІ 2.5 – 004 – 99. Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа.

17.НД ТЗИ 3.7. – 001 – 99. Методические указания по разработке технического задания на создание комплексной системы защиты информации в автоматизированной системе.

18.НД ТЗИ 2.5. – 005 – 99. Классификация автоматизированных систем и стандартные профили защищенности обрабатываемой информации от несанкционированного доступа.

19.Концепция технической защиты информации в Украине. Постановление Кабинета министров Украины от 08.10.97 №1126.

20.Положение о технической защите информации в Украине. Указ Президента Украины от 27.09.99 №1229.

21.Положение о порядке осуществления криптографической защиты информации в Украине. Указ Президента Украины от 22.05.1998 №505/98.

22.ISO/IEC 13335-(1-3): 1998 – Information technology –Guidelines of IT Security.

23.ISO/IEC 17799:2001 – Information technology. – Information Security Management – Code of Practice for Information Security Management.

24.BS 7799: 1995 – Code of Practice for Information Security Management.

25.Bundesmat fur Sicherheit in der Informationstechnik. IT Baseline Protection Manual. – 1998.

26.Анищенко В.В. Оценка информационной безопасности // PC Magazine/RE – №2. – 2000. – С. 7-11.

27.Анищенко В.В., Фисенко В.К. Проблемы и перспективы стандартизации в области безопасности информационных технологий в Республике Беларусь // Материалы Международной НТК “Информационная безопасность” – Минск, 2000.

ДОДАТОК А. МЕТОДИКА ОЦІНКИ ЗА ДОПОМОГОЮ СУБ’ЄКТИВНОЇ ЛОГІКИ

У ході проведення внутрішнього аудиту, необхідно відповідати на питання які входять до складу так званого Критичного елемента. Критичний елемент являє собою один з аспектів проблеми забезпечення безпеки інформації, що висвітлюється в області, до якої він належить. Після відповіді на питання виникає проблема обробки отриманих результатів. Використовуючи мажоритарний принцип, запропонований у NIST можна оцінити Критичний елемент. Така оцінка є неточною. При проведенні оцінки експерту часто важко виразити свою думку однозначно «Так» чи «Ні». Складність може обумовлюватися як неповнотою знань, так і динамічністю досліджуваних процесів. Випадок абсолютної довіри чи недовіри є ідеальним і в реальності не зустрічається. Для вираження більш точного вираження своєї думки, і подальшої їхньої обробки використовуємо апарат суб'єктивної логіки.

Ідея застосування суб’єктивної логіки полягає у тім щоб надати експерту можливості висловити своє відношення, щодо ступеня виконання робіт (процедур), а потім об’єднати отримані думки, таким чином, щоб утворювана узагальнена думка по Критичному елементу враховувала ступінь виконання усіх робіт (Рисунок А.1).

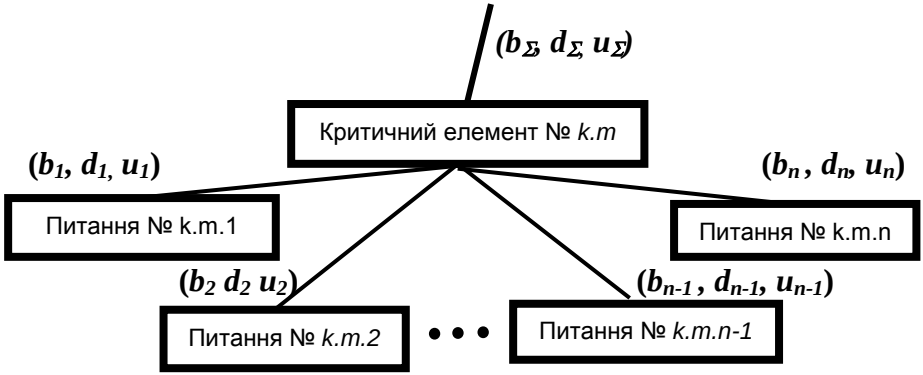


Рисунок А.1 Використання суб’єктивної логіки

Використання апарата суб'єктивної логіки, як інструмента для оцінки ступеня виконання Критичних елементів, вимагає рішення двох основних задач:

- формування думок з питань у просторі суб'єктивної логіки;
- формування об'єднаної оцінки по Критичному елементу в цілому.

Перша проблема в застосуванні суб'єктивної логіки складається у визначенні думок, що будуть використовуватися як вхідні параметри. Люди можуть вважати модель думок недостатньо визначеної і як наслідок давати конфліктуючі думки при оцінці тих самих подій. Нижче приведений опитувач призначений допомогти оцінювачу висловити свою думку щодо даного твердження. Ідея опитувача складається у винесенні думки по кожному параметру окремо.

Порядок переходу в простір інтуїтивних думок

1. Чи зрозумілий Вам зміст твердження, чи чітко воно сформульовано ?

«Так» перехід на крок (2).

«Ні» (уточніть зміст твердження і спробуйте ще раз).

2. Чи існують у Вас будь-які аргументи на користь чи проти даного твердження ?

«Так» перехід на крок (3).

«Ні» Висновок:

У Вас повна невизначеність $b = 0$, $d = 0$, $u = 1$.

Кінець.

3. Наскільки сильне почуття невизначеності ?

Дайте оцінку $0 \leq x < 1$ перехід на крок (4).

4. Наскільки сильні аргументи проти даного твердження ?

Дайте оцінку $0 \leq y < 1$ перехід на крок (5).

5. Наскільки сильні аргументи на користь даного твердження ?

Дайте оцінку $0 \leq z < 1$ перехід на крок (6).

6. Нормування результатів

$$\begin{cases} b = \dfrac{z}{z + y + (1 - x)} \\ d = \dfrac{y}{z + y + (1 - x)} \\ u = \dfrac{1 - x}{z + y + (1 - x)} \end{cases} \qquad \text{(A.1)}$$

перехід на крок (7).

7. Одержання вектору думки $\omega = \{b, d, u\}$

Застосування даного алгоритму дозволяє експерту коректно висловити свою думку у просторі суб'єктивної логіки. Сформована думка відображає ставлення експерта до запропонованого твердження у повній мірі, але при цьому алгоритм обтяжує розумову діяльність особи, що проводить процедуру аудиту. Експерту необхідно висловити ступінь своїх аргументів на користь та проти твердження в межах інтервалу (0;1), і таким же чином оцінити ступінь невизначеності. Така методика є математично строгою, але не зручною. Після проведення експерименту стало ясно, що зростання кількості тверджень, що належать до розгляду, призводить до зниження якості відповідей, що надаються. Людина не мислить цифрами, чи відсотками, їй легше надавати відповіді таким чином, як у житі - вербально. Сформулювати перелік найбільш типових відповідей, не складно. Важче розробити модель переводу цих суджень у простір суб'єктивної логіки.

У суб'єктивній логіці множина всіх думок являє собою трикутник. Вершини трикутника визначають абсолютну довіру, недовіру або невизначеність до твердження, що розглядається. Основа трикутника являє собою простір який є еквівалентним простору бінарної логіки, тобто відповіді є аналогічними нормованим судженням у бінарній логіці.

Більше детальний розгляд простору думок виявив, що весь простір можливо розбити на зони, які будуть являти собою геометричну інтерпретацію базових суджень. (Рис. А.2)

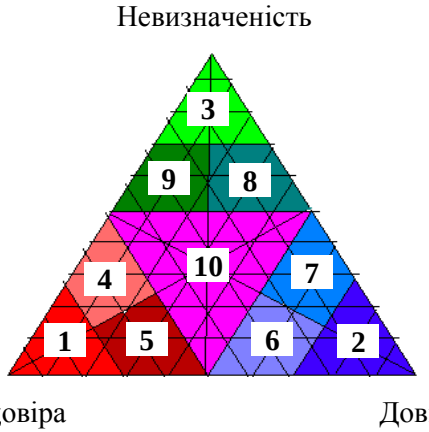


Рисунок А.2 Зони базових думок у просторі суб'єктивної логіки

Вибір границь цих зон не є випадковим і математично описано в таблиці (А.1)

Таблиця А.1 – Математичний опис зон базових думок

№ зони	Математичний вираз	Вербальний опис думки
1	$d \succ (b+u),\ b \approx u$	Переважає недовіра, при цьому ступінь довіри близька до невизначеності.
2	$b \succ (d+u),\ d \approx u$	Переважає довіра, при цьому ступінь недовіри близька до невизначеності.
3	$u \succ (d+b),\ d \approx b$	Переважає невизначеність, при цьому ступінь довіри близька до недовіри.
4	$d \succ (b+u),\ b \prec u$	Переважає недовіра, при цьому ступінь довіри менше від невизначеності.
5	$d \succ (b+u),\ b \succ u$	Переважає недовіра, при цьому ступінь довіри більше ніж невизначеність.
6	$b \succ (d+u),\ d \succ u$	Переважає довіра, при цьому ступінь недовіри більше ніж невизначеність.

7	$b \succ (d+u),\ d \prec u$	Переважає довіра, при цьому ступінь недовіри менше від невизначеності.
8	$u \succ (d+b),\ d \prec b$	Переважає невизначеність, при цьому ступінь недовіри менше від довіри.
9	$u \succ (d+b),\ d \succ b$	Переважає невизначеність, при цьому ступінь недовіри більше ніж довіра.
10	$b \approx d \approx u$	Ступені недовіри, довіри та невизначеності близькі

З метою більш точного надання математичного опису зон були використані положення теорії відношень. З їх допомогою формально задаються и описуються „переваги". Основними відношеннями переваг є:

- відношення строгої переваги $\succ$;
- відношення байдужості $\approx$;

У цьому випадку запис $d^1 \succ d^2$ позначає що елемент d^1 строго більш пере важніше ніж елемент d^2, тобто за умови пред'явлення особі, що приймає рішення (ОПР) двох цих елементів її вибір завжди буде за елемент d^1. Запис $d^1 \approx d^2$ позначає, що елементи не переважають один одного і за умови пред'явлення тільки цих двох елементів ОПР не зможе зробити вибір.

Наприклад, вираз $u \succ (d+b), d \approx b$ позначає, що ОПР вважає: твердження, яке розглядається, має високу ступінь невизначеності, яка значно переважає по зрівнянню зі ступенем недовіри та довіри. В свою чергу довіра та недовіра приблизно однакові, тобто експерт вважає не доцільним надавати перевагу одній з них. Вербально, в загальному випадку це можна описати так „Переважає невизначеність, при цьому ступінь довіри близька до довіри". А за умови інтерпретації до конкретних задач, що буде вирішувати експертна система, це можна описати так: „Питання потребує подальшого вивчення, оскільки маються значні сумніви стосовно його реалізації, або воно недостатньо вивчено". Такий підхід до визначення зон найбільш типових відповідей дозволяє не тільки перевести свою оцінку в простір суб'єктивної логіки із їх подальшою обробкою, але при цьому отримавши результат, представити його у вербальному вигляді.

Слід зазначити, що оскільки кожна людина має можливість власноруч визначити, випадки у яких вона надає ті чи інші типові відповіді, то і отримана відповідь по проблемі, буде також належати до зон, зміст яких буде зрозумілим для експерта. Таким чином, створювана на таких засадах система є адаптованою під конкретну людину і дозволяє підвищити ефективність застосування отриманих за її допомогою відповідей.

Розрахуємо значення Критичних елементів з використанням математичного апарату суб'єктивної логіки. З цією метою перефразуємо питання таким чином, щоб вони мали вид тверджень (таблиця А.2).

Таблиця А.2

Критичний елемент 2.1. Проводиться аналіз заходів щодо забезпечення безпеки в даній системи, а також у взаємодіючих з нею системах.	
2.1.1	Дана система, а також границі мереж піддаються періодичному аналізу.
2.1.2	У випадку значних змін у системі проводиться незалежна експертиза.
2.1.3	Проводиться періодична самооцінка системи.
2.1.4	Регулярно проводяться іспити і перевірка ключових об'єктів, наприклад, сканування мережі, аналіз установок маршрутизотора і комутатора, перевірка можливості проникнення (вторгнення).
2.1.5	Інциденти і порушення безпеки аналізуються і починаються коригувальні дії.
Критичний елемент 7.2. Захист даних від перехоплення.	
7.2.1	Монітори комп'ютерів розміщені таким чином, який виключає перегляд даних сторонніми особами, а також перехоплення електромагнітних випромінювань.
7.2.2	Контролюється фізичний доступ до ліній передачі даних.

Виразимо свою думку (висловлюючи базові судження у просторі думок) щодо вищенаведених тверджень. Результати оцінки приведені в таблиці А.3

Таблиця А.3

№	Довіра	Недовіра	Невизначеність	Відповідь
2.1 1	0.8	0.1	0.1	Так
2.1 2	0.4	0.4	0.2	Ні
2.1 3	0.9	0.05	0.05	Так
2.1 4	0.65	0.15	0.2	Так
2.1 5	0.4	0.3	0.3	Ні
7.2.1	0.6	0.2	0.2	Так
7.2.2	0.3	0.4	0.3	Ні

Відповідно до формул кон'юнкції обчислимо значення *b, d, u* для Критичних елементів 2.1 і 7.2. Об'єднання думок будемо проводити методом ітерацій, тобто параметр (довіра, недовіра, невизначеність) першого поєднується з параметром другого, а їхній результат з параметром наступного.

Після проведення обчислень маємо:

Критичний елемент 2.1: $b = 0{,}075$; $d = 0{,}69$; $u = 0{,}235$.

Критичний елемент 7.2: $b = 0{,}18$; $d = 0{,}52$; $u = 0{,}3$.

Аналіз отриманого результату вказує на те, що Критичний елемент 7.2 заслуговує більшої довіри (більш ніж у 2 рази),а рівень недовіри в нього нижче, ніж у Критичного елемента 2.1, при майже однакових значеннях параметра невизначеності. Така оцінка не є правомірною. У дійсності, твердження Критичного елемента 2.1 оцінювалися як ті що заслуговують більш високого рівня довіри, з низьким рівнем невизначеності.

Дана помилка показує, на некоректність застосування операції кон'юнкції для $n>2$. Таким чином, необхідно вирішити другу проблему використання апарата суб'єктивної логіки.

Постановка задачі на розробку оператора об'єднання

Нехай кількість тверджень n, ω_p – думка оцінювача відносно p-го твердження, що можна уявити у виді $\omega_p = \{b_p, d_p, u_p\}$, де b_p - рівень довіри до p-ого твердження, d_p - рівень недовіри до p-ого твердження, u_p - рівень невизначеності, наявної відносно p–ого твердження. Нехай $\omega_{\Sigma n}$ - об'єднана адекватна думка по n твердженнях, що можна уявити у виді

$$\omega_{\Sigma n} = \{b_{\Sigma n}, d_{\Sigma n}, u_{\Sigma n}\},$$

де $b_{\Sigma n}$ - рівень довіри до n тверджень;

$d_{\Sigma n}$ - рівень недовіри до n тверджень;

$u_{\Sigma n}$ - рівень невизначеності відносно n тверджень.

Необхідно знайти такий оператор об'єднання $f(W_n)$ – де W_n – безліч думок відносно n тверджень, що $\omega_{\Sigma n} = f(W_n)$.

Рішення даної задачі можливо за допомогою наступних шляхів:

1) Введення деякого поправочного коефіцієнта k як функції від числа (n);
2) Застосування замість кон'юнкції середнього значення параметрів;
3) Знаходження середнього значення кон'юнкції для n думок.

Рішення задачі має задовольняти ти таким вимогам:

- результат має залежати від чисельних значень параметрів думок, а не від їхньої кількості;
- результат не повинний суперечити положенням суб'єктивної логіки.

Введення поправочного коефіцієнта.

Нехай $\omega^1_{\Sigma n} = \{b^1_{\Sigma n}, d^1_{\Sigma n}, u^1_{\Sigma n}\}$ - об'єднана думка отримана методом послідовних ітерацій, а $\omega_{\Sigma n}$ - думка така, що адекватно відображає істинність Критичного Елемента, що включає n – тверджень. Тоді суть уведення поправочного коефіцієнта полягає в обчисленні таких коефіцієнтів $K_b(N)$, $K_d(N)$, $K_u(N)$, що

$$\omega_{\Sigma n} = \{K_b(N)* b_{\Sigma n}, K_d(N)* d_{\Sigma n}, K_u(N)* U_{\Sigma n}\}$$

Залежність поправочних коефіцієнтів від кількості поєднуваних тверджень буде носити нелінійний характер. Складність знаходження і той факт, що такі коефіцієнти швидше за все будуть нівелювати значення окремих параметрів, фактично спираючись на мінімальні і максимальні значення параметрів, не дозволяє використовувати даний метод у якості прийнятного оператора об'єднання

Середнє значення параметрів

Використання даної методики має на увазі застосування середнього арифметичного значення параметрів. Обчислення підсумкових значень параметрів відбувається по формулах

$$\begin{aligned} b_{n\Sigma} &= \frac{1}{n}\sum_{i=1}^{n} b_i \\ d_{n\Sigma} &= \frac{1}{n}\sum_{i=1}^{n} d_i \\ u_{n\Sigma} &= \frac{1}{n}\sum_{i=1}^{n} u_i \end{aligned} \qquad \text{(A.2)}$$

Після проведення обчислень маємо наступні оцінки:
Критичний елемент 2.1: $b = 0{,}63$; $d = 0{,}2$; $u = 0{,}17$.
Критичний елемент 7.2: $b = 0{,}45$; $d = 0{,}3$; $u = 0{,}25$.

Даний метод хоча і позбавлений від недоліку методу послідовних ітерацій – залежності об'єднаних кон'юнкції від кількості поєднуваних думок, але при цьому він не відповідає положенням суб'єктивної логіки. Тому що подібна оцінка не враховує залежностей між твердженнями і не відповідає жодному визначеному для суб'єктивної логіки оператору.

Усереднена попарна кон'юнкція

Нехай n–кількість поєднуваних тверджень, b_i, d_i, u_i – параметри думки відносно I-го твердження, k – кількість можливих пар кон'юнкцій. Тоді математична модель оператору попарної кон'юнкції має вид:

$$\bar{b}_{n\Sigma} = \frac{1}{k}\sum_{l,j}(b_i * b_j) \;\forall\; (i = \overline{1, n-1};\quad j = \overline{1, n};\quad j > i);$$

$$\bar{d}_{n\sum} = \frac{1}{k}\sum_{l,j}(d_i + d_j - d_i * d_j) \forall \ (i = \overline{1, n-1};\ \ j = \overline{1, n};\ j > i);$$

$$\bar{u}_{n\sum} = \frac{1}{k}\sum_{i,j}(u_i * b_j + u_j * b_i + u_i * u_j) \ \forall \ \ (i = \overline{1, n-1};\ j = \overline{1, n};\ j > i);$$

$$k = \frac{n(n-1)}{2}.$$

З метою кращого розуміння даного методу розглянемо алгоритм розрахунку усередненої попарної кон'юнкції параметрів

<u>Алгоритм розрахунку усередненої кон'юнкції для n думок.</u>

1. *Розрахунок кон'юнкції параметрів за принципом кожний з кожним*

$$\begin{aligned} b_j &= b_i \wedge b_j, \quad i = \overline{1, n-1};\ \ j = \overline{i+1, n} \\ d_j &= d_i \wedge d_j, \quad i = \overline{1, n-1};\ \ j = \overline{i+1, n} \\ u_j &= u_i \wedge u_j, \quad i = \overline{1, n-1};\ \ j = \overline{i+1, n} \end{aligned} \qquad \text{(A.3)}$$

де *n* - загальне число думок, які необхідно об'єднати

2. *Знаходження кількості (k), по парних кон'юнкцій використовуючи* формулу:

$$k = \frac{n(n-1)}{2} \qquad \text{(A.4)}$$

3. *Обчислення суми по кожному параметру окремо:*

$$b_\sum = \sum_{i=1}^{k} b_i;\ \ d_\sum = \sum_{i=1}^{k} d_i;\ \ u_\sum = \sum_{i=1}^{k} u_i. \qquad \text{(A.5)}$$

4. *Обчислення середньоарифметичного по кожному з параметрів:*

$$b_{n\sum} = \frac{1}{k} b_{\sum} \; ; \; d_{n\sum} = \frac{1}{k} d_{\sum} \; ; \; u_{n\sum} = \frac{1}{k} u_{\sum} \; . \qquad \text{(А.6)}$$

Обчислимо значення попарної усередненої кон'юнкції для вже висловлених думок щодо Критичних елементів 2.1 та 7.2. Для зручності результати обчислень першого пункту алгоритму для Критичного елемента 2.1 представимо у вигляді квадратної таблиці розмірністю (*n***n*), де *n* - кількість питань, що містяться у ньому. На головній діагоналі даної таблиці відсутні значення, тому що об'єднання думки самого із собою позбавлено змісту. У зв'язку з тим, що операція кон'юнкції є комунікативною досить обчислити тільки частину таблиці розташовану над головною діагоналлю. Прорахунок даної таблиці здійснювався за допомогою електронних таблиць Excel Microsoft Office. На рисунку А.3 представлена таблиця експортована з цього додатка. У *i*–ому рядку і *j*-ому стовпці в стовпчик (*b, d, u*) записуються конюнкція *I*-ої думки з *j*–ою.

Довіра Недовіра Невизначеність		0,32 0,46 0,22	0,72 0,145 0,135	0,52 0,235 0,245	0,32 0,37 0,31
Довіра Недовіра Невизначеність			0,36 0,43 0,21	0,26 0,49 0,25	0,16 0,58 0,26
Довіра Недовіра Невизначеність				0,585 0,1925 0,2225	0,36 0,335 0,305
Довіра Недовіра Невизначеність					0,26 0,405 0,335
Довіра Недовіра Невизначеність					

Рисунок А.3 – Таблиця попарних кон'юнкцій (Excel)
для Критичного елемента 2.1

2-ий етап.
Знайдемо кількість попарних кон'юнкція за формулою (А.4):

$$k = \frac{5*(5-1)}{2} = 10$$

3-ій етап
Знайдемо суму по кожному параметру окремо за формулою (А.5):

$$b_{\Sigma}= 3{,}865 \qquad d_{\Sigma}=3{,}6425 \qquad u_{\Sigma}=2{,}4925.$$

4-ий етап
Обчислимо середньоарифметичне по кожному з параметрів за формулою (А.6):

$$b_{n\Sigma}= 0{,}3865 \quad d_{n\Sigma}= 0{,}36425 \quad u_{n\Sigma}= 0{,}24925$$

У таблиці А.4 зведено результати отримані при використання всіх розглянутих методик. $\{b_{n\Sigma}, d_{n\Sigma}, u_{n\Sigma}\}$

Таблиця А.4 Зведені результати по обчисленню об'єднаної думки

Назва оцінюваного Критичного елементу	Значення об'єднаної думки при використанні різних методик			
	Бінарна логіка	Послідовні ітерації $\{b_{n\Sigma}, d_{n\Sigma}, u_{n\Sigma}\}$	Середнє значення параметрів $\{b_{n\Sigma}, d_{n\Sigma}, u_{n\Sigma}\}$	Усереднена кон'юнкція $\{b_{n\Sigma}, d_{n\Sigma}, u_{n\Sigma}\}$
Критичний елемент 2.1	Так	{0,075; 0,69; 0,235}	{0,63; 0,2; 0,17}	{0,39; 0,36; 0,25}
Критичний елемент 7.2	?	{0,18; 0,52; 0,3}	{0,45; 0,3; 0,25}	{,18; 0,52; 0,3}

Аналіз отриманих результатів вказує на те, що для обчислення кон'юнктивної вірності n думок доцільно використовувати метод усередненої кон'юнкції, оскільки він відповідає ідеології суб'єктивної логіки, а результат такого об'єднання залежить від значень параметрів усіх поєднуваних думок і не залежить від кількості даних думок.

ДОДАТОК Б. АНАЛІЗ АВТОМАТИЗОВАНОЇ СИСТЕМИ САМООЦІНКИ ASSET

Процес проведення самооцінки є рутинною роботою. З метою автоматизації процесу збору, збереження й обробки відповідей на питання, що дозволяють оцінити ступінь захищеності системи, відповідно до методики самооцінки запропонованої Національним інститутом по стандартизації та технологіям, був розроблений і підтримується програмний продукт ASSET (Automated Security Self-Evaluation).

Для роботи із системою автоматизованої самооцінки безпеки до апаратного і програмного забезпечення висуваються наступні мінімальні вимоги:

- Pentium II –450 MHz;
- 128 Mb RAM;
- 120 Mb вільного місця на твердому диску;
- на кожну наступну оцінку додатково виділяється додатково 3 Mb;
- операційна система Windows 2000 Professional;

Використання даного продукту вимагає проведення процедури інсталяції. Під час інсталяції створюється первинна база даних, у якій зберігаються питання, а також методика збору та обробки отриманих відповідей. Надалі дані по окремих проведених оцінках можуть зберігатися в локальну базу даних, або експортуватися у файл спеціального формату.

Робота з ASSET включає складається із п’яти основних етапів (Рис. Б.1):

1) ввід початкових даних;
2) ідентифікація системи;
3) визначення політики;
4) відповіді на питання;
5) генерація звітів;

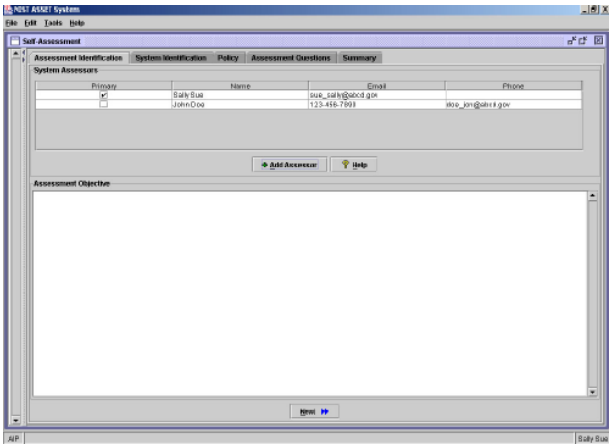


Рисунок Б.1 Основні етапи оцінки

Перед використанням ASSET необхідно створити свій обліковий запис (login). Під час цієї процедури буде потрібно ввести повне ім'я оцінювача, адресу електронної пошти. Уведення login на початку першої після інсталяції оцінки показує ASSET, що пред'явник є головним оцінювачем. Головний оцінювач наділений правами адміністратора, що дозволяє установлювати режими роботи інших оцінювачів. (Рис. Б.2)

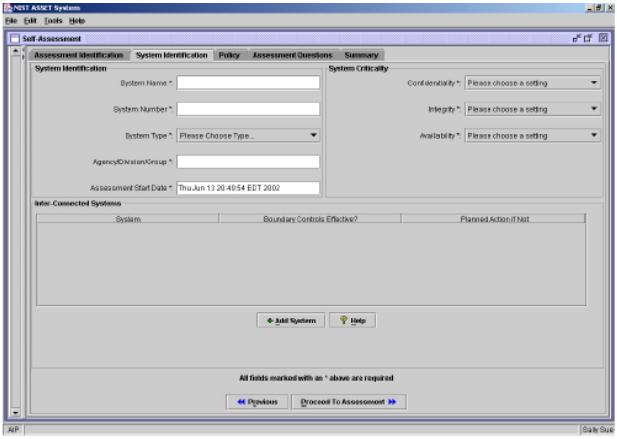


Рисунок Б.2 Ідентифікація експертів

Самооцінка є процедурою, що займає не один день. Враховуючи неможливість якісно оцінити стан безпеки за один сеанс по всіх контрольних областях, система дозволяє перед початком роботи вибрати саме ті області, що будуть оцінюватися в даному сеансі. (Рис. Б.3)

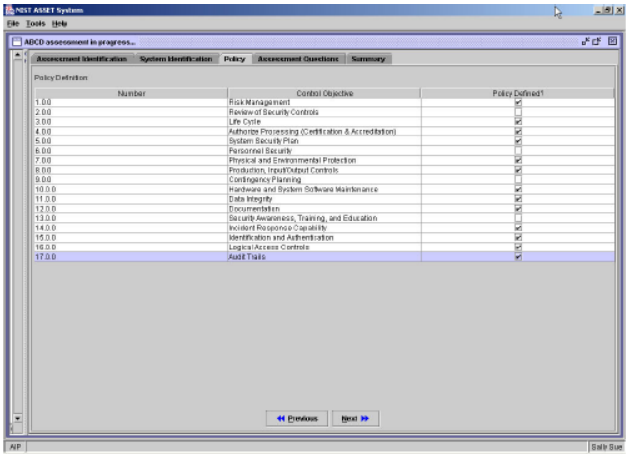


Рисунок Б.3 – Вибір областей, що оцінюються

Оскільки рівні в NIST SP 800-26 знаходяться в ієрархічній залежності, логіка функціонування ASSET не дозволяє дати відповідь на питання за рівнем, якщо воно не було атестовано на відповідність усім попереднім рівням. Перехід до наступного питання також передбачає відповідь на всі попередні питання, котрі входять у даний Критичний елемент. Навігація між Критичними елементами можлива двома способами – послідовно, або за допомогою дерева перегляду. (Рис. Б.4)

У ході проведення самооцінки може виявитися, що питання не було вивчено в достатній для відповіді мірі, у цьому випадку цей факт позначається відповідним прапорцем.

При відповіді на питання оцінювач відзначає чи був присутній ризик, а також визначити його ступінь і описати, чим він обумовлений і в чому полягав.(Рис Б.4)

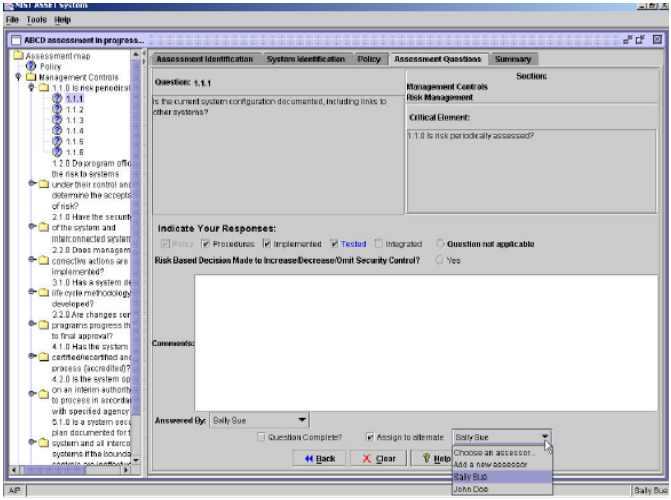


Рисунок Б.4 – Проведення процедури оцінки

Критичний елемент одержує позитивну оцінку за рівнем у тому випадку, якщо більше половини питань одержало позитивні відповіді і при цьому всі питання були атестовані на відповідність даному рівню (допускаються оцінки «рішення засноване на ризику», «вивчений у недостатньому обсязі»).

На останньому етапі ASSET представляє наступні дані (Рис. Б.5):

- відсоток виконання оцінки;
- список Критичних елементів, розгляд яких було довершено;
- список Критичних елементів, що містять не вивчені питання;
- список Критичних елементів що містять відповіді, засновані на ризику;
- рівні на відповідність яким були атестовані Критичні елементи.
-

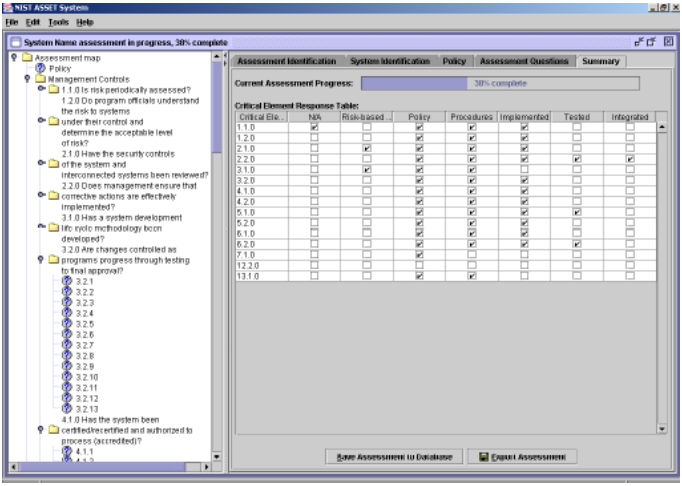


Рисунок Б.5 – Форма представлення результатів оцінки

Дана система є добрим засобом автоматизації процесу збору, збереження і відображення інформації про проведену оцінку. Але при цьому механізм збору та обробки відповідей дозволяє провести лише первину оцінку.

АНОТАЦІЯ

А.В. Лєншин, О. О. Ілляшенко, О.В. Потій, **Методи та засоби оцінювання гарантій ІТ безпеки. Тренінг** / під ред. В.С. Харченко – Міністерство освіти та науки України, Національний аерокосмічний університет ім. Н.Е. Жуковського «ХАІ». 2017. – 100 с.

Викладено матеріали практичної частини тренінг-курсу «Методи і засоби оцінювання гарантій безпеки» (СТ3.Security and Resilience Assurance Cases), підготовленого в рамках проекту TEMPUS SEREIN «Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains» (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR).

Наведені описи тренінгів, які призначені для вивчення з технологіями та засобами оцінки гарантій безпеки, у відповідності до міжнародних стандартів та вимог. Надається навчальна програма курсу і опис лабораторних робіт і тренінгів.

Призначено для інженерів, які займаються проектуванням, розробленням та впровадженням систем захисту інформації, для груп верифікації і фахівців у галузі оцінювання якості та безпеки ІТ-систем, для магістрів і аспірантів університетів, які навчаються за напрямами інформаційної безпеки, комп'ютерних наук, комп'ютерної та програмної інженерії, а також для викладачів відповідних курсів.

Бібл. – 47 найменувань, рисунків – 53.

ЗМІСТ

ABSTRACT

Lenshin A.V., Illiashenko O.A., Potii A.V., **Techniques and tools for evaluation of IT security assurance. Training.** / Edited by Kharchenko V. S. – Ministry of Education and Science of Ukraine, National Aerospace University named after N. E. Zhukovsky "KhAI", 2017. – 100 p.

The materials of the practical part of the training course "CT3.Security and Resilience Assurance Cases", developed in the framework of the TEMPUS SEREIN project "Modernization of Postgraduate Studies on Security Resilience for Human and Industry Related Domains" (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR) are described.

The descriptions of trainings, which are intended for studying with technologies and means of assessing security guarantees, are given in accordance with international standards and requirements. Course syllabus and description of laboratory work and training provided.

Dedicated for engineers who design, develop and implement information security systems, for verification teams and professionals in the field of quality assessment and security of IT systems, for masters and graduate students from universities which study in the areas of information security, computer science, computer and software engineering, as well as for lecturers of the corresponding courses.

Ref. – 47 items, figures – 53.

CONTENTS

ДОДАТОК В. НАВЧАЛЬНА ПРОГРАМА КУРСУ

DESCRIPTION OF THE MODULE

TITLE OF THE MODULE	Code
Security and Resilience Assurance Cases	**CT3**

Teacher(s)	Department
Coordinating: Oleg Illiashenko **Others: Oleksandr Potii, Anatolii Lenshin**	Computer systems and networks, Security of information and communication systems

Study cycle	Level of the module	Type of the module
Engineer	A	Full-time tuition. Compulsory

Prerequisites	
Prerequisites: Foundation of Information Security; Management of information Security; Formal Methods Foundation; Foundation of Modeling; Computer Systems and System Analysis.	**Co-requisites (if necessary):** Foundations of Dependability and Security System and Network Security and Resilience

Credits of the module	Total student workload	Contact hours	Individual work hours
4	108	36	72

Aim of the module (course unit): competences foreseeen by the study programme		
The aim of module is to create a knowledge base for multidisciplinary research on Secutiy Assurance Case and to provide a prerequisites for practical use of Security Assurance Evaluation. The study also expands the current research on Information Security Assurance in the context of the study of methods System Analysis.		
Learning outcomes of module (course unit)	**Teaching/learning methods**	**Assessment methods**
At the end of course, the successful student will be able to: 1. Define and interpret Security assurance requirements and Evaluation Assurance Level (EAL)	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire

on the basis of the international standards, for example ISO/IEC 15408, ISO/IEC 15443..		
2. Select appropriate method for evaluation Assurance Level.	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
3. Prepare Security assurance case and create scenarios to evaluate of Security assurance requirements and Evaluation Assurance Level (EAL).	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
4. Utilize different special tools for the examination EAL and analyze data to identify trends regarding security assurance activities and create reports of evaluation.	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
5. Perform evaluation of Security assurance requirements and Evaluation Assurance Level.	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire

Themes	Contact **work hours**							**Time and tasks for individual work**	
	Lectures	Consultations	Seminars	Practiacl work	Laboratory work	Placements	**Total contact work**	**Individual work**	**Tasks**
1. Introduction in Security assurance. International Standard ISO/IEC 15443 1.1.Concept of security assurance 1.2. The structure of security assurance 1.3. Security Assurance Conformity Assessment techniques.	2							7	1.4. Security Assurance Conformity Assessment methods. 1.5. Aspects of the Composition of Security Assurance.
2. Security assurance requirement for IT-systems. International Standard ISO/IEC 15408 2.1 Ontological model of security assurance. 2.2 Classification of Security assurance requirement. 2.3. Evaluation assurance Level.	2				4			8	2.4 Create Security profile with Security assurance requirements.
3. Basic concepts of Assurance Case methodology. 3.1. Toulmin's argument model. 3.2. Goal-structuring Notation (GSN). 3.3. Adelard safety Claims Argument Data (SCADA). 3.4. Trust Case (TC)	2				8			9	3.5 Construct and analyze an security assurance with the help of notations GSN and SCADA
4. NOR-STA platform for development of assurance cases 4.1. Trust-IT framework. 4.2 trust-IT argument model.	2				8			8	4.6 Building Trust case be models using NOR-STA

4.3. Trust case example. 4.4. Trust case development.									platform for
5. Standards Conformity Framework 5.1 Trust Case Templates. 5.2 SCF Application Process 5.3 Trust Case Template Structure	2				8			8	5.4 Appraisal Mechanism
6. Case Study. 6.1 Case Study 1 - Common Criteria 6.2 Case Study 2 – BS 7799-2. 6.3 Case Study 7 – ISO/IEC 27001 6.4 Case Study 10 – ISO/IEC 15408 6.5 Appraisal Mechanism Validation	2				8			8	6.5. Individual case Study
Iš viso	**20**				**32**			**72**	

Assessment strategy	**Weight in %**	**Deadlines**	**Assessment criteria**
Lecture activity, including fulfilling special self-tasks	30	7,14	85% – 100% Outstanding work, showing a full grasp of all the questions answered. 70% – 84% Perfect or near perfect answers to a high proportion of the questions answered. There should be a thorough understanding and appreciation of the material. 60% – 69% A very good knowledge of much of the important material, possibly excellent in places, but with a limited account of some significant topics. 50% – 59% There should be a good grasp of several important topics, but with only a limited understanding or ability in places. There may be significant omissions. 45% – 49% Students will show some relevant knowledge of some of the issues involved, but with a good grasp of only a minority of the material. Some topics may be answered well, but others will be either omitted or incorrect.

			40% – 44% There should be some work of some merit. There may be a few topics answered partly or there may be scattered or perfunctory knowledge across a larger range. 20% – 39% There should be substantial deficiencies, or no answers, across large parts of the topics set, but with a little relevant and correct material in places. 0% – 19% Very little or nothing that is correct and relevant.
Learning in laboratories	50	7,14	85% – 100% An outstanding piece of work, superbly organised and presented, excellent achievement of the objectives, evidence of original thought. 70% – 84% Students will show a thorough understanding and appreciation of the material, producing work without significant error or omission. Objectives achieved well. Excellent organisation and presentation. 60% – 69% Students will show a clear understanding of the issues involved and the work should be well written and well organised. Good work towards the objectives. The exercise should show evidence that the student has thought about the topic and has not simply reproduced standard solutions or arguments. 50% – 59% The work should show evidence that the student has a reasonable understanding of the basic material. There may be some signs of weakness, but overall the grasp of the topic should be sound. The presentation and organisation should be reasonably clear, and the objectives should at least be partially achieved. 45% – 49% Students will show some appreciation of the issues involved. The exercise will indicate a basic understanding of the topic, but will not have gone beyond this, and there may well be signs of confusion about more complex material. There should be fair work towards the laboratory work objectives. 40% – 44% There should be some work to-

			wards the laboratory work objectives, but significant issues are likely to be neglected, and there will be little or no appreciation of the complexity of the problem. 20% – 39% The work may contain some correct and relevant material, but most issues are neglected or are covered incorrectly. There should be some signs of appreciation of the laboratory work requirements. 0% – 19% Very little or nothing that is correct and relevant and no real appreciation of the laboratory work requirements.
Module Evaluation Quest	20	8,16	The score corresponds to the percentage of correct answers to the test questions

Author	**Year of issue**	**Title**	**No of periodical or volume**	**Place of printing. Printing house or intrenet link**
Compulsory literature				
	2012	ISO/IEC TR 15443-1, Information technology – Security techniques – Security assurance framework – Part 1: Introduction and concepts	ISO	
	2009	ISO/IEC 15408-1:2009, Informational technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model; Part 3: Security assurance requirement.	ISO	
	2011	15026-2:2011 Systems and Software Engineering-- Systems and Soft-	ISO	

		ware Assurance-- Part 2: Assurance Case		
	2008	ISO/IEC 18045, Informational technology – Security techniques – Methodology for IT security evaluation		
A. Potij. D. Komin, I. Rebriy	2012	An Ontological Modeling of Assurance Evaluation Process in Context of Functional-Linguistic Approach	Vol. 28, No. 1 — pp. 108-120.	Information & Security. An International Journal
O. Illiashenko, O. Potii, D. Komin	2015	Advanced security assurance case based on ISO/IEC 15408	Conference: DepCoS - RELCOMEX 2015	https://link.springer.com/chapter/10.1007/978-3-319-19216-1_37
R. E. Bloomfield, K. Netkachova, R. Stroud	2013	Security-Informed Safety: If it's not secure, it's not safe.	5th International Workshop on Software Engineering for Resilient Systems	http://openaccess.city.ac.uk/3097/1/Bloomfield_serene_2013.pdf
Łukasz Cyra	2008	A Method of Trust Case Templates to Support Standards Conformity Achievement and Assessment. PhD Thesis	Gdańsk University Of Technology, 146 p.	http://iag.pg.gda.pl/download/L_Cyra_PhD_Thesis.pdf
A. Ekelhart, S. Fenz, M. Klemen, E. Weippl	2007	Security Ontologies: Improving Quantitative Risk Analysis		https://www.sba-research.org/wp-content/uploads/publications/2007%20-%20Ekelhart%20-%20Security%20Ontologies%20Improving%

				20Quantitative%20Risk%20Analysis.pdf
Lukasz Cyra, Janusz Górski	2008	Expert Assessment of Arguments: a Method and Its Experimental Evaluation	Volume 5219, Berlin/Heidelberg, 2008, pp. 291-304	Lecture Notes in Computer Science. http://iag.pg.gda.pl/download/2008_Cyra_Gorski_Expert_Assessment_of_Arguments_a_Method_and_Its_Experimental_Evaluation.pdf
Rob Alexander, Richard Hawkins, Tim Kelly	2011	Security Assurance Cases: Motivation and the state of the Art	The University of York. CEGS/TR/2011/1	http://www-users.cs.york.ac.uk/~rda/York%20CESG%20security%20case%20report%20i1_1.pdf
Charles B. Weinstock Howard F. Lipson John Goodenough	2007	Arguing Security – Creating Security Assurance Cases	Software Engineering Institute	http://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_293637.pdf
Chris W. Johnson	2011	Using Assurance Cases and Boolean Logic Driven Markov Processes to Formalise Cyber Security Concerns for Safety - Critical Interaction with Global Navigation Satellite Systems	School of Computing Science, University of Glasgow,	http://www.dcs.gla.ac.uk/~johnson/papers/FMIS2011/Chris.pdf
Tomoko Kaneko, Shuichiro Yamamoto, Hidehiko Tanaka	2014	CC-Case as an Integrated Method of Security Analysis and Assurance over Life-cycle Process	Vol. 3(1): p. 49-62	International Journal of Cyber-Security and Digital Forensics (IJCSDF)
Peter Bishop, Robin Bloomfield, Sofia Guerra	2004	The future of goal-based assurance cases		http://www.adelard.com/papers/dsn2004v10.pdf
Jeffrey R. Williams, George F. Jelen	1998	A Framework for Reasoning about Assurance	National Security Agency Document Number:	http://www.sse-cmm.org/Papers/Framework.pdf

			ATR 97043	
Additional literature				
Nair, S., de la Vara, J. L., Sabetzadeh, M., Briand, L.:	2014	An Extended Systematic Literature Review on Provision of Evidence for Safety Certification	Vol. 56, pages 689–717,	Elsevier Science Information & Software Journal http://www.sciencedirect.com/science/article/pii/S0950584914000603
Mishchenko O.V., Pomorova O.V., Hovorushchenko T.O Kharchenko V. (edit)	2012	Case-assessment of critical software systems. Three-volume edition, Vol.1. Quality		National aerospace university named after N. Zhukovsky "KhAI", 2012. – 201 p.
Odarushchenko O.M., Kharchenko V.S., Maevskiy D.A., Ponochovniy Yu. L., Rudenko O.A., Odarushchenko O.B., Zasukha S.O., Zhadan V.O., Zhyvilo S.V. Kharchenko V. (edit)	2012	Case-assessment of critical software systems. Three-volume edition, Vol. 2. Reliability		National aerospace university named after N. Zhukovsky "KhAI", 2012. – 292 p.
Kharchenko V.S., Netkacheva K.I., Orekhova A.O., Tarasyk O.M., Gorbenko A.V., Sklyar V.V., Brezhnev E.V., Babeshko E.V., Illiashenko O.O. Kharchenko V. (edit)	2012	Case-assessment of critical software systems. Three-volume edition, Vol.3. Safety		National aerospace university named after N. Zhukovsky "KhAI", 2012. – 292 p.

ДОДАТОК Г. МЕТОДІЧНІ РЕКОМЕНДАЦІЇ ЗІ САМОСТІЙНОЇ РОБОТИ

4.1 Пояснення до навчальної програми

Самостійну роботу над дисципліною «Безпека та резільентність: приклади гарантій безпеки.» («Security and Resilience Assurance Cases») необхідно починати с вивчення навчальної програми, яка надається у додатку Б. Програма включає такі елементи.

Об'єкт вивчення – гарантії ІТ-безпеки.

Предмет вивчення – методи, технології та інструментальні засоби оцінювання гарантій ІТ-безпеки.

Вимоги до вихідних знань та навичкам, які необхідно мати на початку навчання:

- знання в області сучасних комп'ютерних систем та інформаційних технологій;
- основи проектування ІТ-систем;
- стандарті в сфери безпеки інформації;
- основи теорії гарантоспроможності та інформаційної безпеки;
- основи безпеки та стійкості комп'ютерних систем та мереж.

Метою вивчення є: засвоєння знань та навичко з використання засобів оцінки гарантій ІТ-безпеки; отримання навичок проектування систем захисту; засвоєння знань зі сертифікаційних випробування систем захисту.

У результаті вивчення студенті мають:

– проводити аналіз вимог безпеки та вимог гарантій безпеки;

– чітко та ясно формулювати питання, вміти формулювати відповіді;

– проектування профіль захисту ІТ-системи;

– проводити оцінку гарантій безпеки із застосуванням апарату суб'єктивної логіки;

– знати вимоги міжнародних стандартів з ІТ-безпеки;

– володіти базою знань зі проектування систем захисту;

– вмити проводити сертифікаційні випробування систем захисту;

– реалізувати спроможність до самостійного навчання, вивчати складу технічну документацію;

Структура та зміст модулів.

МОДУЛЬ 1. Характеристика міжнародних стандартів в сфері гарантій безпеки. У модулі розглядаються міжнародні та регіональні стандарті в сфері гарантій безпеки. Розглядаються вимоги гарантій до криптографічних модулів, криптографічних протоколів, моделі гарантій автентифікації та ідентичності тощо.

МОДУЛЬ 2. Моделі гарантій IT-безпеки (Model of IT-Security Assurance) розглядаються аналітична, онтологічна та формальні моделі гарантій безпеки. Формулюються вимоги до властивостей гарантій безпеки. Вивчається процес оцінки гарантій безпеки та його формалізована модель.

МОДУЛЬ 3. Методи функціонально-лінгвістичного підходу до оцінювання гарантій безпеки. Розглядається та вивчається функціонально-лінгвістичний підхід до оцінки гарантій безпеки. Формулюються рекомендації щодо використання методів процесного підходу до оцінки гарантій безпеки, використання положень теорії лінгвістичних змінних та нечіткої логіки для формулювання стверджень щодо виконання вимог гарантій безпеки.

По кожному з модулів передбачені практичні роботи та наданий список літературі

Методи оцінки

Іспит (100 %).

По закінченню курсу проводиться 90-хвилиний іспит.

Звітність включає звіти за практичні заняття, а також іспит, що містить типові питання та задачі.

4.2 Підготовка до занять та іспиту

Під час підготовки до практичних занять необхідно звернути увагу на з'ясування цілей та завдань, а також знань, що необхідні для практичної роботи. Під час виконання роботі, необхідно керуватися методичним вказівками, описом програмного забезпечення та спромогтися знайти відповіді на питання, що наведені наприкінці кожної роботи. Особливу уваги необхідно приділити формулювання висновків у формі звіту.

Під час самостійної підготовки до практичних завдань важливо здійснювати правильно планування індивідуально та колективну роботу, організувати відбір літератури та провести її аналіз.

Лєншин Анатолій Валерійович
Ілляшенко Олег Олександрович
Потій Олександр Володимирович

Методи та засоби оцінки гарантій ІТ безпеки

Тренінг

(українською мовою)

Редактор Харченко В.С.

Комп'ютерна верстка
О.О. Ілляшенко

Зв. план, 2017
Підписаний до друку 25.01.2017 Формат
60х84 1/16. Папір офс. №2. Офс. друк.
Умов. друк. арк. 21,89. Уч.-вид. л. 22,31. Наклад 100 прим.
Замовлення 2/2. Ціна вільна

Національний аерокосмічний університет ім. М. Є. Жуковського "Х а р к і в с ь к и й а в і а ц і й н и й і н с т и т у т"
61070, Харків-70, вул. Чкалова, 17
http://www.khai.edu