Міністерство освіти і науки, молоді та спорту України
Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

«До захисту допущено»
Завідувач кафедри
комп'ютерної інженерії
к.т.н., доц. О.М.Березький
_____
"____"_____20__ р.

ДИПЛОМНИЙ ПРОЕКТ

освітньо-кваліфікаційного рівня "Спеціаліст"
зі спеціальності 7.05010201 "Комп'ютерні системи та мережі"
на тему:

ARIS-МОДЕЛЬ СТРАТЕГІЇ ЗАХИСТУ ІНФОРМАЦІЇ OCTAVE

Студент групи КСМзс-51
_____Левчук Л.Й.
(підпис)
Керівник: викладач
_____ Якименко І.З.
(підпис)
Нормоконтроль
к.т.н., доцент
_____Васильків Н.М.
(підпис)

Консультант
з охорони праці
доцент
_____Сапожник Г.В.
(підпис)

2012

Міністерство освіти і науки, молоді та спорту України
Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

спеціальність 7.05010201 – "Комп'ютерні системи та мережі"

"Затверджую"
завідувач кафедри
комп'ютерної інженерії
к.т.н., доц. О.М.Березький
_____
"____"_____20__ р.

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЕКТ СТУДЕНТА
Левчук Людмили Йосипівни

1. **Тема проекту:** "ARIS-модель стратегії захисту інформації OCTAVE" затверджена наказом університету № 475 від 14 жовтня 2011 р.

2. **Термін здачі студентом закінченого проекту** "___"_____20__ р.

3. **Вихідні дані для проекту:** Технічне завдання.

4. **Перелік задач, які мають бути вирішені:**

- провести аналіз існуючих рішень та загального підходу OCTAVE;
- провести огляд та аналіз існуючих моделей ARIS;
- розробити принципи побудови критеріїв OCTAVE;
- розробити атрибути процесу оцінювання;
- описати дії по оцінці ризиків;
- виконати моделювання в ARIS 5.0;
- побудувати модель дерева функцій (Function Tree);
- побудувати модель ланцюжка доданої вартості (Value-Added chain Diagram)
- побудувати модель подійно–керованого процесу (eEPC).

5. **Перелік графічного матеріалу** (з точним вказанням обов'язкових креслень)

- Фази загального підходу. Схема структурна
- Відношення між статичними та динамічними моделями
- Модель дерева функцій (Function Tree)
- Модель ланцюжка доданої вартості (VAD)

6.Консультанти по проекту (із зазначенням розділів):

Розділ	Консультант	Підпис
Охорона праці	Сапожник Г.В.	

КАЛЕНДАРНИЙ ПЛАН

№	Назва розділів дипломного проекту	Термін виконання	Позначки керівника про виконання завдань
1	Характеристика загального підходу OCTAVE	15.09.2011 – 5.11.2011	
2	Структура критеріїв OCTAVE	6.11.2011 – 31.01.2012	
3	Побудова ARIS–моделей процесу вироблення стратегії захисту інформації OCTAVE	1.02.2012 – 14.04.2012	
4	Охорона праці	15.04.2012 – 23.04.2012	

Завдання прийняв до виконання _____

(підпис)

Керівник дипломного проекту _____

(підпис)

АНОТАЦІЯ

Робота виконана на 92 сторінках, з них 85 сторінок основного тексту, містить 8 рисунків, 4 таблиці, 18 джерел посилань на 2 сторінках, 5 додатків.

Метою дипломного проекту є розробка ARIS–моделі стратегії захисту інформації OCTAVE.

У проекті розглянуто три моделі: діаграма дерева функцій, діаграма ланцюжка доданої вартості та діаграма подійно-керований процесу. Діаграми відображають метод OCTAVE. Моделі в ARIS сприяють розумінню нової ідеології стратегічного управління безпекою інформації керівниками підприємств та підрозділів безпеки інформації.

Дипломний проект містить структурну схему фаз загального підходу; відношення між статичними та динамічними моделями; модель дерева функцій (Function Tree); модель ланцюжка доданої вартості (VAD), які подані в графічній частині.

Дипломний проект має практичну спрямованість і його результати плануються до впровадження.

ANNOTATION

The work performed at 92 pages, including 85 pages main text, contains 8 figures, 4 tables, 18 references sources on 2 pages, 5 applications.

The aim of the diploma project is to develop ARIS-model strategy for information security OCTAVE.

The project considered three models: tree chart features, chart and chain added sale diagram modulo event-driven process. Charts display method OCTAVE. ARIS–Models is help understanding of the new ideology security information management leaders of business enterprise and information security departments.

The degree project includes phase diagram of the general approach, the relationship between static and dynamic models, model tree functions (Function Tree); model chain of value added (VAD), which are presented in graphical part.

The diploma project is practically oriented and its results are planned for implementation.

Технічне завдання

1. НАЙМЕНУВАННЯ ТА ОБЛАСТЬ ЗАСТОСУВАННЯ

1.1 ARIS-модель стратегії захисту інформації OCTAVE

1.2 Область застосування – державні установи, комп'ютерні фірми та магазини, провайдери Інтернет, які використовують різноманітні системи захисту інформації.

2. ОСНОВА ДЛЯ РОЗРОБКИ

Основою для розробки є завдання на дипломний проект, затверджене кафедрою комп'ютерної інженерії факультету комп'ютерних інформаційних технологій Тернопільського національного економічного університету.

3. ПРИЗНАЧЕННЯ РОЗРОБКИ

Метою дипломного проекту є розробка ARIS-моделі стратегії захисту інформації OCTAVE

4. ДЖЕРЕЛА РОЗРОБКИ

Джерелами даної розробки є матеріали навчальної та реферативної наукової літератури, технічна документація, існуючі програмні та програмно-апаратні системи, журнали, науково-дослідні роботи вітчизняних та закордонних вчених.

5. ТЕХНІЧНІ ВИМОГИ

5.1 Вимоги до апаратних засобів

5.1.1 Функціональні вимоги до апаратних засобів.

5.1.1.1 Система повинна працювати на IBM-сумісних робочих станціях.

5.1.1.2 Мінімальні вимоги до робочих станцій: процесор від 1 ГГц, оперативна пам'ять від 512 Мб, відеокарта від 32 Мб, об'єм пам'яті на жорсткому диску до 100 Мб, клавіатура, маніпулятор «миша».

5.1.1.3 Відеореєструюча апаратури (відеокамера, фотокамера та їх роздільна здатність, сумісність програмного забезпечення).

5.2 Вимоги до програмної системи

5.2.1 Функціональні вимоги до програмної системи

5.2.1.1 Оператор системи повинен мати змогу виконувати наступні функції:

- інтеграція з іншими інженерними і комунікаційними системами об’єкта;

- здійснення управління згідно стратегії захисту інформації OCTAVE;

- формування звітів на основі проведених досліджень у табличному та графічному форматах.

5.2.1.2 Вхідна інформація отримується шляхом:

– завантаження файлів із цифрових носіїв даних: жорстких дисків, гнучких дисків, flash-карт тощо;

– отримання файлів за допомогою відповідної апаратури у реальному часі згідно стратегії захисту інформації OCTAVE.

5.2.1.3 Вихідна інформація:

– вихідна інформація повинна подаватись у простому та інтуїтивно зрозумілому для користувача форматі;

– формування звітів повинно відбуватись у реальному часі;

– вихідна інформація виводиться у текстовому, табличному, графічному (графіки, діаграми) форматах;

5.2.2 Вимоги до надійності.

5.2.2.1 Передбачити контроль введеної інформації.

5.2.2.2 Розробити комплекс заходів контролю коректності дій користувача під час роботи з системою.

5.2.2.3 Забезпечити можливість відновлення роботи системи після збоїв.

5.2.3 Вимоги до програмного забезпечення:

5.2.3.1 Операційна система сімейства Windows;

5.2.3.2 Графічна бібліотека OpenGL.

5.2.3.4 Сумісність з сучасними форматами даних:

– вхідна інформація подається у форматах «*.doc» та «*.docx»;

– вихідна інформація подається у форматах «*.txt», «*.doc» та «*.docx» для текстової інформації, «*.xls» для табличної інформації та «*.bmp», «*.jpg» для графічної.

5.2.4 Вимоги до програмної документації

5.2.4.1 Код програмних модулів повинен містити необхідні для його розуміння коментарі;

5.2.4.2 Розроблене програмне забезпечення повинно включати довідкову систему

5.2.5 Вимоги експлуатації

5.2.5.1Кліматичні вимоги до експлуатації, при яких забезпечується робота програми повинні відповідати кліматичним умовам експлуатації наявних технічних засобів

5.2.5.2 Вимоги до кваліфікації та численності персоналу. Мінімальна кількість персоналу, необхідного для роботи програми, може складати одну штатну одиницю – кінцевого користувача.

5.2.6 Вимоги до захисту:

5.2.6.1 Мінімальна довжина пароля - 10 символів.

6. ВИМОГИ ОХОРОНИ ПРАЦІ

В розділі “Охорона праці ” дипломного проекту повинен бути даний аналіз умов праці в приміщенні де працює розробник апаратно–програмного засобу та користувач.

7. ПОРЯДОК КОНТРОЛЮ І ПРИЙОМКИ

7.1 Представлення дипломного проекту на попередній захист

7.2 Представлення дипломного проекту на захист

ЗМІСТ

ВСТУП

На сучасному стані інформатизації діяльності підприємств, організацій та відомств з’явилася потреба стратегічного погляду на шлях розвитку систем забезпечення безпеки інформації, які забезпечать стан зростання рівня безпеки інформації у довгостроковій перспективі [1, 2]. У зв’язку з цим в практиці управлінської діяльності захисту інформації пропонується застосувати методологію стратегічного управління безпекою [3]. Необхідність уведення в практику захисту інформації такого поняття та інструменту, як стратегія захисту інформації з метою чіткого обґрунтування принципових підходів до забезпечення безпеки інформації вказують роботи російських фахівців [4, 5], а також у міжнародному стандарті ISO/IES13335. Але у відомій літературі ці поняття глибоко не проаналізовані, не визначено їх роль у практичній діяльності та в управлінні безпекою не розглядається питання розроблення стратегій захисту та ефективного застосування стратегічного управління безпекою за допомогою моделювання [6]. Таким чином актуальним стає задача розробка стратегії захисту інформацій, яка буде адекватна реальному рівню загроз безпеці інформації.

Складність полягає в тому, що необхідно сформувати єдиний підхід до забезпечення безпеки інформації на адміністративному рівні або на рівні керування організацією [7, 8]. У цьому випадку необхідно розглядати проблему інформаційної безпеки з погляду інфраструктури організації [9] та добре представляти інфраструктурну сутність цієї проблеми.

ARIS (Architecture of Integrated Information Systems, архітектура інтегрованих інформаційних систем) являє собою цілісний підхід до розробки, а також аналізу моделей бізнес−процесів [10, 11]. Структурний аналіз як сукупність моделей складних систем внаслідок великої розмірності розв'язуваних завдань повинен опиратися на потужні засоби комп'ютерної підтримки, що має забезпечити автоматизацію праці системних аналітиків

[12]. У даній роботі для моделювання стратегії безпеки інформації обраний програмний продукт ARIS 5.0. Мета моделювання полягає в перетворенні загальних, розпливчастих знань про вихідну предметну область (стратегію захисту інформації OCTAVE [13) у точні моделі, що можуть описувати різні підсистеми.

1. ХАРАКТЕРИСТИКА ЗАГАЛЬНОГО ПІДХОДУ OCTAVE

1.1 Основні положення підходу

На сьогоднішній день відсутні комплексні системні методики й методи, формального або неформального характеру, які дозволяють на систематичній основі вирішувати задачі по розробці концепції інформаційної безпеки або корпоративної політики безпеки у великих організаціях. Найбільш конструктивним щодо цього підходом є підхід OCTAVE [13], розроблений Software Engineering Institute і Carnegie Mellon University. Він має достатню спільність, що дозволяє розробити практичні методи й системні методики для вирішення перерахованих вище задач. Підхід OCTAVE був узятий за основу для створення системної методики й відповідного науково-методичного апарата, що дозволяє формалізувати процеси розробки стратегії забезпечення безпеки інформації організації.

Метод оперативної оцінки критичних ресурсів, погроз, активів і уразливостей (Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)) – це підхід, що визначає стратегію оцінки й планування дій по забезпеченню безпеки інформації на основі оцінки ризиків (risk–based).

OCTAVE є загальним підходом по оцінці погроз, ресурсів, і вразливостей на рівні організації в цілому. Основною посилкою (передумовою) є те, що ефективна оцінка ризиків повинна розглядатися як з організаційної, так і технологічних точок зору, відображати те, як співробітники організації використовують інформаційно–телекомунікаційну інфраструктуру у своїй щоденній діяльності.

Оцінка ризиків є життєво важливим елементом для прийняття рішень по забезпеченню безпеки інформації [14]. Саме результати оцінки ризиків дозволяють сформувати єдину системну позицію керівництва організації на ризики безпеки, а також формують основу для формування й реалізації стратегії безпеки.

Розглянутий підхід є стратегією оцінки й планування захисту інформації, що опирається на концепцію ризиків і забезпечення безпеки інформації. Принциповим моментом підходу є принцип внутрішнього керування процесами оцінки (принцип самоврядування), що означає, що в процесах вироблення корпоративної стратегії безпеки особисту участь приймають співробітники організації. Опираючись на свої знання співробітники дають реальну оцінку стану практичної діяльності по забезпеченню безпеки інформації (практики безпеки). Виявлені при цьому ризики для найбільш критичних активів (ресурсів) організації використовуються для визначення пріоритетних напрямків забезпечення безпеки інформації й загальної стратегії безпеки організації.

Більшість існуючих методик аналізу ризиків орієнтуються на технологічні ризики й на тактичні проблеми (захист інформації в конкретній системі або мережі). При цьому упускаються стратегічні цілі організації. У такий спосіб часткове рішення завдань захисту інформації стає видно у мережі (системі). Рішення приймаються незалежно від реальних потреб у забезпеченні безпеки інформації й від реальних потреб організації в таких задачах. Це порушує основні принципи забезпечення безпеки інформації: про єдність цілей організації й цілей захисту інформації.

Саме тому, особливо у великих компаніях, необхідно мати ефективні методики, які дозволять погоджувати задачі організації, а також завдання захисту інформації. Підхід OCTAVE орієнтований на організаційні ризики і тому в якості свого фокуса розглядає стратегічні проблеми інформаційної безпеки, пов'язані з організацією практичної діяльності установи по забезпеченню безпеки інформації. На інфраструктурному рівні при виробленні рішень необхідно забезпечити баланс між трьома ключовими аспектами: операційні ризики, практика безпеки та технології, що схематично представлено на рисунку 1.1.

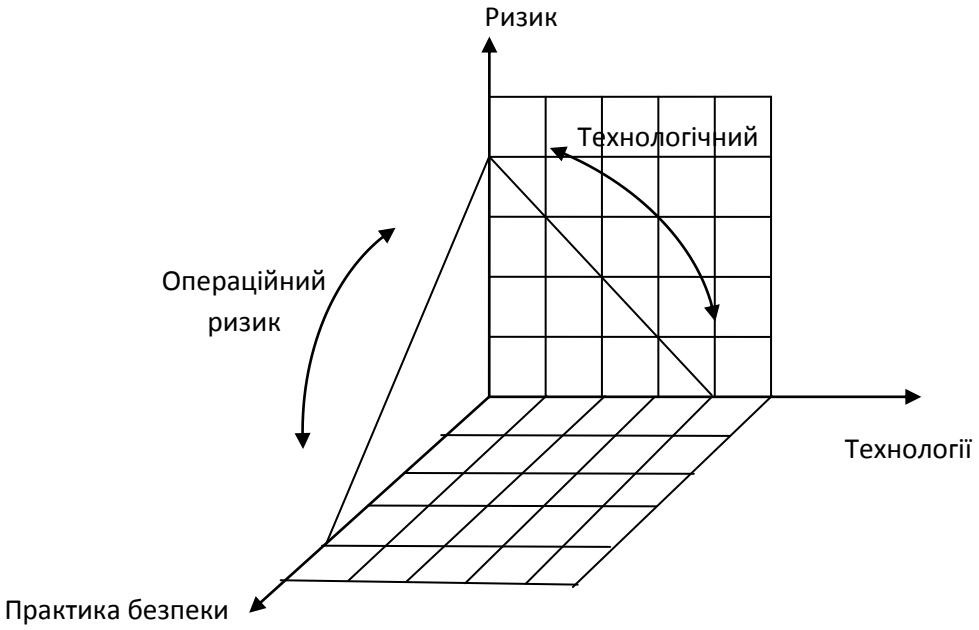


Рисунок 1.1 – Тривимірна модель взаємодії

При роботі на рівні організації переважаючу роль грає два аспекти: ризик і практика безпеки (площина операційного ризику). Технологія розглядається тільки у зв'язку з реалізацією практики безпеки, що дозволяє організації уточнити своє бачення поточної практики безпеки, що утворилася в організації. Таким чином, чим нижчий рівень (якість, ефективність, культура) практичної діяльності по забезпеченню безпеки, тим вищий операційний ризик.

Опираючись на підхід OCTAVE, можна розробити системну методику, що дозволяє організації виробити рішення по забезпеченню безпеки інформації, засноване на ризиках конфіденційності, цілісності й доступності критичних інформаційних активів і пов'язаних з ними інших ресурсів організації. Всі аспекти ризиків (активи, погрози, уразливості несприятливі для організації наслідку (збиток) є основними факторами, що мають вплив на прийняття рішень, і дозволяють організації виробити практично значиму стратегію захисту від цих ризиків безпеки.

Поняття ризику містить у собі три основних компоненти: актив (ресурс) − об'єкт ризику, погрози й уразливість. Таким чином, при оцінці ризиків як мінімум необхідно розглядати ці три компоненти. Загальний підхід повинен бути орієнтований на ресурси, що підлягають захисту. Саме тому група аналітиків повинна, принаймні, виконати такі процедури:

1) ідентифікувати інформаційні активи й пов'язані з ними ресурси, які являють цінність для організації й важливі для успішного функціонування організації;

2) основну увага приділити процесам аналізу ризиків для тих активів, які є найбільш критичними для організації;

3) таким чином група аналітиків повинна розглядати взаємозв'язки між критичними активами, погрозами для цих активів і уразливостями (як організаційними, так і технологічними), які дають можливість реалізувати погрози. Отже оцінка ризиків повинна здійснюватися в операційному контексті.

Іншими словами, даний підхід залежить від того, як ті або інші системи (інформаційно−телекомунікаційні системи) використовуються для досягнення бізнес−цілей організації, підтримки її діяльності і, оскільки ці системи піддаються ризикам, − безпека.

Реалізація підходу дозволить сформувати стратегію безпеки організації (у вигляді концепції) і план (або плани) зниження існуючих ризиків (планів захисту інформації) для практичних ресурсів організації. Таким чином, описаний підхід OCTAVE дозволяє об'єднати стратегічну й тактичну точки зору.

Організаційний, технологічний та аналітичний аспекти оцінки ризиків забезпечення безпеки інформації реалізуються шляхом виділення трьох основних фаз, які схематично представлені в Додатку А. Це дозволяє скласти повну картину усіх наявних потреб організації в забезпеченні безпеки інформації.

Перша фаза (побудова профілю погроз безпеки) відображає організаційний аспект. По суті, на цій фазі здійснюється оцінка практики безпеки організації. Група аналітиків у взаємодії з керівництвом компанії визначає, які ресурси найбільш важливі для організації і яким чином у даний момент організований захист цих ресурсів. Потім здійснюється вибір тих ресурсів, які є найбільш критичними та важливими для організації й формулюються вимоги безпеки до кожного ресурсу (у термінах конфіденційності, цілісності, а також доступності). Нарешті, здійснюється ідентифікація погроз до кожного критичного ресурсу та створюється профіль погроз.

Друга фаза (ідентифікація вразливостей інформаційно-телекомунікаційної інфраструктури) відображає технологічний аспект підходу. Об'єктом аналізу виступає інформаційно–телекомунікаційна інфраструктура організації. Група аналітиків розглядає шляхи доступу до критичних ресурсів, ідентифікує класи виробів інформаційних технологій, пов'язаних з якістю практичних ресурсів. Потім здійснюється аналіз стійкості цих компонентів до різних видів атак.

Третя фаза (розробка стратегії безпеки й планів захисту) відображає аналітичний аспект підходу. Група аналітиків ідентифікує ризики для критичних ресурсів і розробляє рішення щодо усунення цих ризиків. Опираючись на зібрану інформації, формується стратегія безпеки організації й розробляють плани усунення ризиків критичним активам.

1.2 Місце процесів оцінки в загальному циклі. Керування безпекою інформації

З загальної моделі керування безпекою інформації [15] видно, що в організації реалізується безперервний цикл керування. Методики, які базуються на OCTAVE, формують загальну (на рівні організації в цілому)

точку зору на поточні ризики безпеки інформації. Це знімок, зріз у часі й основа для подальших дій по поліпшенню стану питань забезпечення безпеки інформації. З погляду задач керування безпекою в ході реалізації підходу група аналітиків здійснює:

– ідентифікацію ризиків інформаційної безпеки організації;

– аналіз ризиків з метою визначення пріоритетів;

– планування дій по забезпеченню безпеки інформації шляхом розробки стратегії безпеки й планів захисту зі зменшенням ризиків.

Реалізація цих планів уже не є об'єктом OCTAVE. Після розробки стратегії й планів захисту в загальному випадку необхідно:

– розробити робочий план дій по реалізації стратегії безпеки. Ці дії повинні включати докладний аналіз економічної доцільності стратегії;

– реалізувати план дій;

– відслідковувати виконання планів з метою розподілу ресурсів і оцінки їхньої ефективності; це також включає відстеження (моніторинг) будь-яких вимірів ризиків;

– контроль змін у виконанні планів шляхом виконання коригувальних (коректованих) дій.

Таким чином, оцінка ризиків інформаційної безпеи є елементом керування ризиками, на якому базується керування безпекою. Якщо керування ризиками безперервний процес, то оцінка – процес скінчений. Періодично організація повинна переглядати результати оцінки ризиків. Такий перегляд повинен здійснюватися, наприклад, щорічно або у встановлених випадках (наприклад, при реорганізації, модифікації інформаційно–телекомунікаційної інфраструктури і т.д.).

Кожна організація з метою досягнення своїх цілей реалізує унікальний набір ділових, управлінських і виробничих процесів або практик.

При рішенні завдань захисту інформації й у ході вироблення стратегії безпеки важливо не загубити зв'язок між організаційними або діловими

завданнями й технологічними завданнями. Інформація, що буде отримана в ході реалізації загального підходу й рекомендації, сформульовані на основі цієї інформації, повинні в кінцевому підсумку впізнавати вплив на загальні виробничі й інші процеси в організації.

1.3 Архітектура інтегрованих інформаційних систем

Моделювання реальних ситуацій у роботі організації та відпрацьовування комплексних бізнес−процесів стали темою усе більше широких обговорень. Поява зовсім різних методів моделювання підсилює цю тенденцію, а їхня величезна кількість приводить до ще більших ускладнень і плутанини. Унаслідок цього вживають спроби створити стандартизовані концепції (архітектури) для процесу розробки інформаційних систем і методів моделювання.

Однієї з таких з є Архітектура інтегрованих інформаційних систем − ARIS (Architecture of Integrated Information Systems), розроблена професором А.В. Шеєром [6]. Ця концепція має дві основних переваги:

1) дозволяє вибрати методи та інтегрувати їх, опираючись на основні особливості об'єкта, який моделюємо;

2) служить базою для керування складними проектами, оскільки завдяки структурним елементам містить побудовані моделі процедур для розробки інтегрованих інформаційних систем.

Подібна архітектура дає можливість вводити в застосовувані методи деякі елементи стандартизації. Нові методи моделювання, а також ті, в основі яких лежить концепція ARIS, були інтегровані в рамках архітектури, що дозволило створити комплексний метод моделювання відповідних бізнес−процесів.

Інструментарій ARIS дозволяє проводити побудову, аналіз і оцінку робочих процесів організації в термінах методології організації

бізнес–процесів. Крім того, ARIS надає досить прості засоби для документування й моделювання процесів.

1.4 Моделі ARIS

Для структуризації елементів підходу всі моделі розділені на п'ять категорій:

1) організаційні моделі – це статичні моделі, структури організації. Містять у собі організаційні ланки та людські ресурси, представлені в ієрархічних організаційних діаграмах;

2) інформаційні моделі – статичні моделі інформації бізнесу. Містять у собі моделі даних, структури знань і навичок, інформаційних носіїв і баз даних;

3) функціональні моделі – статичні моделі дій процесів. Містять у собі ієрархію функцій, цілей, прикладних систем;

4) модель товарів і послуг – статичні моделі товарів і послуг, які перетворюються та отримуються у результаті бізнесової діяльності відповідної компанії.

5) процесні моделі – це динамічні моделі, які показують поводження процесів і їх залежність від ресурсів, даних і функцій оточення бізнесу. Містять у собі подійно–керовані моделі (eEPC), моделі оточення функції (FAD), модель доданої вартості (VAD).

Перші чотири категорії концентруються на структурі організації, тим часом як процесні моделі концентруються на поведінці процесів у часі.

Всі п'ять категорій з'єднуються в так званий "будинок" APIC, що допомагає наочно представити відносини між статичними та динамічними моделями, представлений у Додатку Б.

Проект моделювання бізнес–діяльності організації включає наступні фази:

– визначення цілей: навіщо, що, хто й коли;

– збір вимог моделювання;

– концепція моделювання;

– детальне моделювання;

– реалізація;

– верифікація й перевірка адекватності.

Концепція ARIS грунтується на ідеї інтеграції, що є складовою частиною комплексного аналізу бізнес–процесів. Перший крок при створенні архітектури складається в розробці моделі бізнесу–процесу, що описує всі його основні функції. Отримана в такий спосіб надзвичайно складна модель розділиться на підмоделі або типи моделей, відповідно до типів представлення. Це дозволяє істотно знизити ступінь її складності. Зміст типів моделей може бути описаний методами, призначеними для конкретного типу представлення. Численні взаємозв'язки між типами моделей при цьому не враховуються. Згодом ці взаємозв'язки інкорпоруються в загальну модель для аналізу всього.

Другим підходом, що зменшує складність побудови моделі бізнесу–процесу, має бути аналіз кожного типу моделей на різних рівнях. Відповідно до концепції моделі життєвого циклу, різні методи опису інформаційних систем диференціюються по ступені їхньої близькості до інформаційних технологій. Це гарантує цілісність опису на всіх етапах, починаючи від проблем керування бізнесом до технічної реалізації інформаційної системи.

Архітектура ARIS створює основу для розробки й оптимізації інтегрованих інформаційних систем, а також для опису їхньої реалізації. Вибір рівнів і типів описів формує архітектуру ARIS, що використається як модель для побудови процесів, пов'язаних з керуванням бізнесом, їхнього аналізу й оцінки.

1.5 Зміст вхідних і вихідних інформаційних об'єктів, постановка задачі

Розкриємо зміст вхідних та вихідних інформаційних об'єктів у такому вигляді:

1) неформалізовані знання співробітників організації можуть містити у собі колективні знання, уміння, навички, а також здатності усіх співробітників організації, які сприяють більш глибокому розумінню ресурсів, поточних вимог безпеки й процедурних уразливостей. Носіями знань є співробітники з різних підрозділів організації – керуючі, інженерно–технічний склад і т.д., а також керівники різних рівнів управління;

2) неформалізовані знання членів групи аналізу містять у собі колективні знання, уміння, навички й здатності членів групи аналізу та будь–яких інших осіб, які додатково залучаються до роботи для виконання окремих дій;

3) неформалізовані знання інженерно–технічного складу IT–підрозділів – це спеціальні колективні знання, уміння, навички й здатності співробітників IT–підрозділів, які беруть ключову участь при виконанні дій другої фази. Ці особи мають глибоке розуміння інформаційно–телекомунікаційної інфраструктури організації, а також проблем забезпечення безпеки інформації в інформаційно–телекомунікаційній системі;

4) ресурси – це перелік інформаційних активів, а також пов'язаних з ними інших ресурсів організації. Активи – це щось, що представляє цінність для організації. Визначимо наступні категорії активів та розглянемо їх докладніше.

{Ресурси}={інформація}{системи}{програмне забезпечення}{апаратне забезпечення}{люди}

Інформація – це задокументовані дані в електронному або паперовому виді або інтелектуальні активи, які використовуються для досягнення місії (стратегічної мети) організації.

Системи – це інформаційно–телекомунікаційні системи, призначені для обробки й зберігання інформації. Система є сукупністю інформаційних об'єктів (активів), програмного й апаратного забезпечення. Будь–який хост, клієнт або сервер може бути розглянутий як система.

Програмне забезпечення – це програмні додатки й послуги (служби) (операційні системи, системи управління базами даних, мережне програмне забезпечення, офісні додатки, додатки користувачів й т.д.).

Апаратне забезпечення – це фізичні пристрої інформаційних технологій (робочі станції, сервера, мережне обладнання і т.д.)

Люди – співробітники організації, включаючи їх знання, уміння, навички й досвід;

5) дані про організації – це інформація, яка включає:

– структуру організації;

– задокументовану політику й процедури забезпечення безпеки інформації в організації;

6) нормативні та правові вимоги – закони й інші нормативно–правові акти, документи, які визначають законні зобов'язання організації відносно безпеки;

7) еталонна модель практики безпеки – модель практичної діяльності по забезпеченню безпеки інформації, на основі якої формується нормативна модель практики безпеки;

8) нормативна модель практики безпеки – це модель формування шляхом модифікації еталонної моделі, і у відповідність до якої здійснюється оцінка поточного стану практичної діяльності по забезпеченню безпеки інформації в організації;

9) поточні стани практики безпеки – це оцінка поточного стану практичної діяльності по забезпеченню безпеки інформації в організації. Містить у собі процеси й процедури по забезпеченню безпеки інформації, які в даний момент представлені, реалізовані й підтримуються в організації;

10) поточні процедурні уразливості – це недоліки в організації проведення заходів (робіт) по забезпеченню безпеки інформації, наявність яких сприяє реалізації неавторизованих дій. Уразливості вказують або на відсутність, або на неадекватність заходів безпеки;

11) критичні активи – це активи, які прийнято вважати найбільш важливими активами для організації (добавився новий атрибут – критичність). Організації може бути нанесений значний збиток, якщо властивості безпеки (або вимоги безпеки) даних активів будуть порушені;

12) вимоги безпеки для критичних активів – вони підкреслюють їх якість, що є важливо для організації. Вимоги безпеки зазвичай включають: конфіденційність, цілісність, доступність;

13) еталонний профіль погроз – він визначає діапазон загальних погроз, які повинні бути розглянуті для кожного критичного ресурсу;

14) профіль погроз для критичного активу – він визначає діапазон погроз, які можуть вплинути на критичний актив. Профіль погроз містить категорії, які згруповані відповідно до джерел погроз. Атрибут погроз:

{Погроза}={актив}{доступ}{фактор}{мотив}{результат}

15) поточна топологія мережі – це документи, що відбивають логічну й фізичну схему мережі та визначають взаємозв'язок системних і мережних компонентів;

16) технологічна інформація – докладна інформація про інформаційно–телекомунікаційну інфраструктуру організації і включає в себе сервери, компоненти безпеки, доменну структуру, автоматизовані функції, завдання тощо;

17) компоненти інформаційно−телекомунікаційної інфраструктури, які підлягають обстеженню − компоненти, які обрані для обстеження й оцінки. Дані компоненти оцінюються на наявність технологічних уразливостей;

18) обрані підходи для оцінки кожного компонента інформаційно−телекомунікаційної інфраструктури − підходи, які вибрані для оцінки компонентів інформаційно−телекомунікаційної інфраструктури і установлюють вимоги для обсягу оцінки уразливостей. Підхід повинен обов'язково встановлювати такі дані: хто буде виконувати оцінку та які засоби аналізу й оцінки уразливостей будуть використовуватися;

19) ключові класи компонентів − це типи пристроїв, які можуть відігравати важливу роль при обробці, зберіганні й передачі критичної інформації. Ресурси пов'язані із критичними активами. Визначимо наступні типові класи:

− сервера − це можуть бути відповідні хости всередині інформаційно−телекомунікаційної інфраструктури організації, які надають ІТ−служби в організації;

− мережні компоненти − це пристрої, які є важливими для мережі організації;

− засобу захисту − це пристрої, які в якості основної функції мають деяку функцію безпеки (наприклад, firewall);

− робочі станції − це хости в мережі організації, які співробітники використовують для виконання своїх службових обов'язків;

− домашні комп'ютери − це комп’ютери, які співробітники організації можуть використовувати для віддаленого доступу до мережі організації та інформаційних ресурсів;

− мобільні комп'ютери − це комп'ютери, які співробітники організації можуть використовувати для віддаленого доступу до інформації через мережу організації;

– пристрої зберігання – це пристрої, на яких забезпечується зберігання інформації з метою резервування;

– бездротові компоненти – це пристрої, які співробітники організації можуть використовувати для доступу до інформації (наприклад, електронна пошта);

– інші – це будь–які інші типи пристроїв, які можуть бути частиною сценарію погроз, але не ввійшли в перераховані вище класи;

20) каталог уразливостей – це множина уразливостей різних платформ і додатків, розміщених у спеціальній базі. Він використовується для оцінки технологічних уразливостей інформаційно–телекомунікаційної інфраструктури організації;

21) технологічні уразливості – слабості (недоліки) у системах, які безпосередньо ведуть до реалізації неавторизованих дій. Технологічні уразливості представляються й застосовуються до мережних служб, архітектури, операційних систем і додатків. Типи уразливостей: конструкції, реалізації, конфігурації;

22) попередні пропозиції по технологічним уразливостям. Підсумкові пропозиції містять наступну інформацію з кожного оцінюваного компонента інформаційно–телекомунікаційної інфраструктури:

– кількість уразливостей, які підлягають негайному усуненню (високий рівень);

– кількість уразливостей, які підлягають усунення найближчим часом (середній рівень);

– кількість уразливостей, які підлягають усунення в останню чергу (низький рівень).

23) підсумкові пропозиції щодо технологічних уразливостей. Додатково до інформації, що втримується в попередніх пропозиціях, підсумкові пропозиції містять специфічні дії про рекомендації з усунення виявлених уразливостей.

24) відновлення профілю погроз для критичних ресурсів;

25) опис збитку від реалізації погроз критичним ресурсам − опис збитку визначає ефект (результат, наслідки) реалізації погроз для місії організації й цілей (завдань) організації;

26) імовірнісні характеристики погроз критичним ресурсам − вони описують мотиви, засоби й умови для людини, що використовують або мережний, або фізичний доступ; поєднують будь−яку "історію" всіх типів погроз; ураховує будь−які незвичні поточні умови, які можуть вплинути на погрози;

27) критерії оцінки збитку − множина якісних (кількісних) заходів (показників), відповідно до яких здійснюється оцінка ризиків. Критерії визначають високий, середній і низький рівні збитку для організації. Зазвичай розробляються критерії для наступних сфер: репутація/довіра споживачів, безпека/здоров'я, штрафи/санкції, фінансовий збиток, ефективність;

28) критерії оцінки ймовірності – множина заходів (показників), відповідно до яких здійснюється оцінка ризику. Критерії визначають зміст високої, середньої та низької імовірності для погроз критичним ресурсам;

29) величина збитку від погроз для критичних активів – це якісна оцінка (низького, середнього або високого) збитку, що може бути нанесений організації в результаті реалізації погрози;

30) значення ймовірності погроз – це кількісна оцінка (низький, середній, високий) імовірності настання загрозливої події;

31) ризик−профіль для критичних ресурсів − він визначає діапазон ризиків, які можуть вплинути на ресурс. Основними складовими ризику−профілю є:

− профіль погроз для критичних ресурсів;

− вимоги безпеки для критичних ресурсів;

− опис збитку від реалізації погрози із профілю погроз;

– величина збитку від реалізації погрози;

– компоненти інформаційно–телекомунікаційної інфраструктури, які підлягають обстеженню;

– підсумковий результат по технологічним уразливостям для кожного дослідженого компонента;

– імовірнісні характеристики погроз;

– значення ймовірності погроз;

32) проект стратегії безпеки (концепції та політики безпеки). Проект визначає основні напрямки діяльності організації для реалізації та підтримки робіт із забезпечення безпеки інформації. Проект містить пропозиції групи аналізу для керівництва організації;

33) проекти планів усунення ризиків (або захисту). Проект містить дії по усуненню виявлених ризиків з метою зменшення ризиків критичним ресурсам організації. Проект містить відповідні пропозиції групи аналізу для керівництва організації. Розроблені плани мають тенденцію до інтегрування з діями або контрзаходами, які розробляються для запобігання конкретних погроз. Дії визначаються відповідно до нормативної моделі практичної діяльності;

34) стратегія (концепція й політика) безпеки визначає основні напрямки й стратегію, що реалізує організація для забезпечення безпеки організації і затверджуються керівництвом;

35) плани усунення ризиків (дотримання плану захисту) – вони містять конкретні дії, спрямовані на зниження ризиків критичним ресурсам;

36) наступні дії – вони визначають, що збирається робити організація в плані реалізації результатів оцінки. Зазвичай даний інформаційний об'єкт включає такі параметри:

– що збирається виконувати організація для реалізації результатів оцінки;

– що збираються робити старші керівники для поліпшення безпеки в організації;

– чи існують які–небудь подальші дії для поліпшення безпеки, які необхідно розглянути;

– які підходи буде застосовувати організація в майбутньому для процесів оцінки.

2 СТРУКТУРА КРИТЕРІЇВ OCTAVE

2.1 Принципи побудови критеріїв OCTAVE

Під критеріями в OCTAVE розуміють сукупність принципів, атрибутів і виходів.

Для моделювання в ARIC фази методу позначимо як функції (процеси), вихід − це товар або послуга, що забезпечує досягнення мети (це для функції вхід, якщо стрілка направлена на функцію, і результат, якщо інакше). Будемо використовувати події, які являють собою зміну в навколишньому світі в результаті виконання процесу.

Принципи − це фундаментальні концептуальні точки зору, які визначають природу оцінки. Вони визначають філософію процесів оцінювання.

Вимоги до оцінки відображуються в атрибутах і результатах. Під атрибутами розуміють різні якісні ознаки або характеристики процесів оцінки. По суті атрибути визначають базові елементи підходу й визначають, що необхідно виконати для успішної оцінки. Атрибути визначаються принципами.

Вихід це потрібний результат по кожній функції процесу оцінювання. Вони визначають кінцевий результат, що повинен бути отриманий аналітиками по кожній функції.

Оцінка безпеки ґрунтується на наступних принципах, які можна розбити на три групи:

− принцип оцінки ризиків безпеки інформації;

− принцип керування ризиками;

− принцип корпоративної культури.

Оцінка ризиків безпеки інформації здійснюється у відповідності з наступними принципами:

1) принцип внутрішнього керування(або самоврядування), суть якого полягає в тому, що оцінка ризиків організації здійснюється безпосередньо співробітниками організації. Ці співробітники несуть повну відповідальність за якість оцінки, організацію процесів оцінки й прийняття рішень щодо рівня безпеки інформації в організації. Даний принцип вимагає:

– прийняття відповідальності за забезпечення безпеки інформації шляхом організації й безпосереднього керівництва процесами оцінювання ризиків безпеки інформації й керування процесами оцінки;

– ухвалення остаточного рішення щодо зусиль організації по забезпеченню безпеки інформації, включаючи визначення напрямків робіт з поліпшення стану по забезпеченню безпеки інформації в організації;

2) принцип адаптації полягає в тому, що гнучкі процеси оцінки можуть бути легко адаптовані до швидко змінюваних технологій і вдосконалень інформаційно–телекомунікаційних систем організації. У таких умовах організація повинна мати набір (шкалу) параметрів (показників, метрик і т.п.), які можуть бути оцінені не залежно від обстановки, що змінилася. Даний принцип вимагає:

– мати інформаційні каталоги, які містять (визначають) набір базових практик безпеки, відомі джерела погроз і відомі технологічні уразливості;

– використати процеси оцінки, які пристосовані до будь-яких змін в інформаційних каталогах.

3) принцип визначеності процесів, суть якого полягає в тому, що оцінка здійснюється на основі чітко визначених і стандартизованих процедур. Застосування стандартизованих процесів забезпечує їх інституалізацію, певний рівень повноти і самостійності. Даний принцип вимагає:

– призначення конкретних осіб, які відповідають за оцінку;

– чіткого визначення всіх процедур, робіт та дій по оцінці;

– специфікації всіх інструментів, робочих таблиць (форм) і інформаційних каталогів, необхідних для оцінювання;

– розробку й створення єдиних форматів для документування й подання результатів оцінки;

4) принцип опори на безперервний процес, згідно якого організація повинна реалізовувати практичну стратегію безпеки й плани захисту на основі безперервних процесів забезпечення безпеки інформації. Результати оцінки ризиків безпеки інформації забезпечують основу для безперервного поліпшення практичної діяльності по забезпеченню безпеки інформації. Принцип висуває наступні вимоги:

– ідентифікація ризиків безпеки інформації повинна здійснюватися на основі використання строго визначених процесів;

– реалізація результатів оцінки ризиків безпеки інформації;

– забезпечення можливості безперервного керування ризиками безпеки інформації;

– реалізація стратегії безпеки й планів захисту таким чином, щоб забезпечити застосування найкращих практичних підходів до забезпечення безпеки інформації;

5) принцип керування ризиками є більше широким по сфері дії й опирається на базові принципи забезпечення безпеки інформації;

6) принцип перспективної точки зору вимагає від співробітників організації стати вище поточних проблем і сфокусувати свою увага на ризики, найбільш критичні для ресурсів організації. Основним завданням повинно бути керування невизначеністю через використання взаємозв'язків між активами, погрозами й уразливостями, через точну оцінку збитку, що може бути нанесений місії й задачам організації. Даний принцип вимагає:

– враховувати майбутні події, концентрувати свою увагу на зниженні невизначеності, що обумовлена безліччю ризиків;

– управляти ресурсами й роботами;

7) принцип концентрації на критичних активах вимагає від організації сконцентрувати свою увагу на найбільш критичних проблемах забезпечення безпеки інформації. Перед будь–якою організацією стоїть безліч проблем, у тому числі й у сфері забезпечення безпеки інформації. Таким чином організація повинна забезпечити ефективний розподіл і використання своїх ресурсів для вирішення цих проблем, у тому числі й задач оцінки ризиків. Для цього дуже важливо визначити головне в цих проблемах. З даного принципу випливає:

– необхідність використання методів цільового збору інформації про ризики безпеки;

– ідентифікацію найбільш критичних для організації активів і вибір тих практик безпеки, які забезпечать захист саме цих активів;

8) принцип єдності керування потребує, щоб політика й стратегія безпеки були сумісні з корпоративною бізнес–політикою та стратегією. Менеджмент організації повинен оцінити й розглянути всі залежності між бізнес–проблемами й проблемами безпеки, забезпечити баланс між цілями захисту й загальних цілями організації. Принцип вимагає:

– інтеграції завдань по забезпеченню безпеки інформації в бізнес–процесах організації;

– розгляд бізнес–стратегії й цілей під час розробки й перегляду стратегії та політики безпеки.

Важливу роль при проведенні робіт з розробки стратегії безпеки грає корпоративна культура організації. Сьогодні вплив корпоративної культури на всі сфери діяльності організації не можна заперечувати. Фахівці в області захисту інформації також вважають, що забезпечення безпеки інформації повинно бути справою кожного співробітника організації.

Розглянемо необхідні принципи, які лежать в основі формування корпоративної культури й безпосередньо впливають на ефективність керування ризиками:

1) принцип відкритості (комунікації), суть якого полягає в тому, що керування ризиками безпеки інформації не може бути успішним без відкритого й всебічного обговорення питань, пов'язаних із забезпеченням безпеки інформації. Фундаментальним і концептуальним підходом, що забезпечує найбільшу ймовірність успіху реалізації програми керування ризиками, є формування корпоративної культури, яка підтримує відкритість обговорення ризиків. З даного принципу випливають наступні вимоги:

– реалізація процесів (робіт) по оцінці, які будуються на кооперації різних фахівців (тобто виконуються в складі робочих груп);

– організація ефективного обміну інформацією про стан безпеки й рівень ризиків між різними рівнями керування організації;

– застосування процесів, побудованих на базі принципів консенсусу прийняття рішень;

2) принцип глобальної перспективи, який вимагає у співробітників організації формувати загальний погляд щодо того, що є цінним для організації. Окремі, приватні перспективи, що відносяться до ризиків безпеки інформації, поєднуються й формують загальну картину ризиків безпеки інформації на рівні організації в цілому. З даного принципу випливає:

– необхідність ідентифікації безлічі перспектив ризиків безпеки інформації, які існують в організації;

– розгляд ризиків безпеки інформації в рамках загального контексту місії організації й загальних задачах, що стоять перед організацією;

3) принцип групової роботи полягає в тому, що окремий (один) фахівець не здатний усвідомити й зрозуміти сутність і зміст усієї різноманітності існуючих ризиків безпеи інформації, з якими зіштовхується організація. Керування ризиками безпеки інформації вимагає міждисциплінарного підходу. Сутність міждисциплінарного підходу полягає в тому, що на різних етапах аналізу й оцінки ризиків, у виробленні й

прийнятті рішень беруть участь фахівці різних підрозділів організації. Обов'язковим є участь фахівців підрозділів, що забезпечують впровадження інформаційних технологій, фахівців основних підрозділів організації (бізнес−підрозділів) і співробітників служби захисту інформації. Таким чином, керування ризиками має на увазі колективне прийняття рішень. Даний принцип вимагає:

– формування міждисциплінарної робочої групи для організації й проведення оцінки;

– знати, коли необхідно включати додаткові перспективи в процеси оцінки;

– здійснення робіт у кооперації;

– максимального використання творчих способів, навичок і знань членів робочої групи й інших співробітників.

2.2 Атрибути процесу оцінювання

Під атрибутом у цьому випадку розуміємо якості або характеристику процесу оцінювання. Атрибут визначається через дві сутності:

– вимог, тобто істотних елементів (якісні відмінні сутності, вимірні показники й т.п.) атрибута;

– обґрунтування важливості атрибута для процесу оцінювання.

По суті атрибути визначають вимоги, яким повинні задовольняти процес (роботи) оцінки або сутності, які необхідні для досягнення успіху оцінки.

Атрибути процесу оцінювання будемо позначати RA.X, де X – порядковий номер атрибута. Розглянемо їх детальніше:

1) RA.1 – група аналізу, яка повинна відповідати таким вимогам:

− група аналізу комплектується зі складу штатних співробітників організації й забезпечує керівництво роботами по оцінці;

– група аналізу повинна бути сформована на основі міждисциплінарного підходу й включати співробітників основних підрозділів інформаційних технологій і захисту інформації;

– група аналізу повинна управляти й направляти оцінку ризиків безпеки інформації своєї організації і відповідає за прийняття рішень, які основані на інформації, зібраної в ході процесу оцінки.

Важливість атрибута визначається необхідністю встановлення однозначної відповідальності за здійснення оцінки ризиків, що покладається на членів групи аналізу, сформованої зі співробітників організації. Формування такої групи забезпечить те, що:

– для поліпшення стану безпеки інформації в організації будуть залучені особи, які добре розуміють бізнес–процеси та задачі інформатизації цих процесів, які працюють спільно;

– методи послідовно застосовуються на всіх рівнях керування організацією;

– співробітники організації відчувають особисту відповідальність за результати оцінки, що в остаточному підсумку сприяє успішній реалізації сформованих стратегій і класів;

2) RA.2 – кваліфікація групи аналізу. До неї ставляться відповідні вимоги, оскільки процес оцінки повинен передбачати можливість підвищення кваліфікації групи аналізу шляхом залучення осіб, що володіють специфічними навичками й знаннями, які потрібні для проведення тих або інших видів робіт або експертиз. Дозволяється додаткове залучення осіб з різних підрозділів організації або зовнішніх експертів. Група аналізу безпосередньо відповідає за аналіз інформації й прийнятті рішень у ході проведення оцінки. Однак ядро групи (основні члени групи) можуть не мати достатнього обсягу знань або навичок, необхідних для проведення тих або інших робіт у ході оцінки. У будь–якій контрольній точці процесу оцінки члени групи аналізу можуть прийняти рішення про залучення додаткових

фахівців або зовнішніх експертів, якщо вони будуть вважати, що у них недостатній рівень знань або навичок. Важливість атрибута визначається тим, що забезпечується необхідний рівень кваліфікації (знань і вмінь) групи аналізу для досягнення успіху оцінки ризиків. Атрибут дає можливість організації виконати оцінку ризиків безпеки інформації в тому випадку, якщо вона не має співробітників необхідної кваліфікації для формування групи аналізу. Таким чином це забезпечує можливість здійснення оцінки через залучення зовнішньої організації;

3) RA.3 − модель практичної діяльності по забезпеченню безпеки інформації (еталонна модель практики безпеки). До неї ставляться відповідні вимоги, оскільки у ході процесу оцінки повинна бути отримана оцінка ефективності поточної практики безпеки організації в різних сферах (напрямках) забезпечення безпеки інформації. Звідси повинна бути визначена модель практичної діяльності по забезпеченню безпеки інформації й спосіб оцінки ефективності цієї діяльності. Модель повинна бути сумісна із чинним законодавством, нормативно−правовими документами та стандартами відповідно до вимог, згідно з якими здійснюється захист інформації в організації. Її важливість полягає в тому, що використання моделі практичної діяльності по забезпеченню безпеки інформації є важливим тому, що це дозволяє організації здійснювати самооцінку системи захисту інформації на відповідність вимогам нормативних документів і на основі добре відомих і загальноприйнятих показників. Це допоможе організації усвідомити, що в цей момент виконується й на якому рівні, і які уразливості існують. Модель також формує структуру стратегії безпеки організації й нарешті є основою для визначення конкретних дій, які включаються в план захисту;

4) RA.4 − загальна модель погроз, згідно якої процес оцінки повинен дати оцінку погроз критичним активам організації в широкому діапазоні потенційних джерел погроз, які формально визначені в загальній моделі погроз:

– модель повинна представити зручний спосіб надання потенційних погроз і забезпечити вичерпну інформацію про погрози критичним активам;

– модель повинна надати простий спосіб захисту й обміну інформацією про погрози.

Застосування загальної моделі погроз дозволить організації ідентифікувати погрози своїм критичним активам;

5) RA.5 – модель (каталог) вразливостей, оскільки процес оцінювання повинен оцінити технологічні слабості (уразливості) у ключових компонентах інформаційно–телекомунікаційній інфраструктурі організації шляхом розгляду широкого діапазону технологічних вразливостей на основі застосування сучасних методів виявлення й аналізу вразливостей. Застосовуваний інструментарій (програмне забезпечення, контрольні місця й т.д.) повинні перевірити компоненти інфраструктури на наявність вразливостей, які втримуються в загальнодоступних каталогах (базах), наприклад CERT Knowledgebase або Common Vulnerabilities and Exploits (CVE).

Застосування каталогу є важливим, оскільки це дозволить організації оцінювати свої технології з погляду відсутності відомих вразливостей. Визначення того, які уразливості існують у ключових компонентах, дозволяє одержати інформацію про уразливість інформаційно–телекомунікаційної інфраструктури організації в цілому;

6) RA.6 – визначення функцій по оцінки, суть якого полягає в тому, що всі процедури для виконання будь–яких функцій по оцінці та артефакти, що використовуються під час виконання будь–якої функції, повинні бути чітко й однозначно визначені й задокументовані. Це припускає:

– визначення процедур по підготовці й проведенню оцінки;

– визначення процедур оцінки;

– визначення процедур для завершення кожної функції;

– специфікацію всіх інструментів і робочих таблиць (форм), необхідних для проведення оцінки;

– специфікацію всіх інформаційних каталогів (моделей), які визначають практику безпеки, відомі погрози безпеки, відомі вразливості (слабості).

Застосування певних функцій по оцінці дозволяє інституалізувати процеси оцінки в організації й забезпечити при цьому деякий рівень сумісності процесів. Це також формує основу для адаптації функцій під потреби конкретних підрозділів або базис груп.

7) RA.7 – документування результатів оцінки. Організація повинна документувати результати оцінки в паперовому або електронному виді. Як мінімум, підлягає документуванню й архівації інформація наступного типу:

– ризики критичним активам організації;

– стратегія безпеки й плани захисту.

Для організації важливо забезпечити постійне бачення записів результатів оцінки. Інформаційна база надалі служитиме вихідним матеріалом для виконання послідовних функцій оцінки, будучи корисною для планів і функцій, виконуваних після оцінки. Інформація також може використовуватися з метою навчання й інформування співробітників;

8) RA.8 – обсяг оцінки, який вказує на можливі границі оцінки. Процес оцінки повинен включати рекомендації, які дозволяють організації прийняти рішення щодо того, які сфери діяльності (або підрозділів) повинні бути включені для оцінювання. Встановлення обсягу оцінки важливе тому, що це забезпечує максимальну потужність результату для організації. Якщо границя оцінки дуже широка, то це приведе до істотних труднощів при аналізі отриманої інформації. Визначення прийнятного обсягу оцінки зменшить розміри оцінки, зробить цей процес більше легким для адміністрування й виконання різних дій. Крім того, необхідно відранжирувати сфери діяльності організації для виконання оцінювання;

9) RA.9 – наступні кроки. Процес оцінки повинен включати функції, коли співробітники організації визначають наступні кроки, необхідні для реалізації стратегії безпеки й планів захисту. Ці функції дуже часто вимагають активної підтримки й участі вищого керівництва організації. Наступні кроки звичайно визначають:

– що організація збирається будувати на підставі результатів оцінки ризиків;

– хто буде залучений для реалізації стратегії безпеки й планів захисту;

– плани щодо майбутніх дій по оцінці ризиків безпеки інформації.

Визначення наступних кроків, які повинні виконати співробітники організації для реалізації стратегії безпеки й планів усунення ризиків, є істотним для поліпшення стану по забезпеченню безпеки інформації. Співробітникам організації необхідно планувати й здійснювати свою діяльність, опираючись на результати оцінки. Одержання підтримки з боку вищого керівництва є першим важливим і критичним кроком на шляху до успіху такої діяльності;

10) RA.10 – фокуси на ризик. Процес оцінки повинен бути сфокусований на оцінку ризиків безпеки інформації організації через облік взаємозв'язків між ресурсами та погрозами і ресурсами та уразливостями (включає організаційні і технологічні вразливості).

Важливість даного атрибута обумовлена тим, що він вимагає від співробітників організації концентрувати свою увагу на проблемах безпеки й на його впливі на бізнес–цілі та задачі організації. Співробітники повинні розглядати насамперед організаційні недоліки й технологічні уразливості, які в даний момент мають місце в організації й перевіряти, яким чином ці слабості пов'язані із критичними ресурсами організації, а також виявляти погрози цим ресурсам.

11) RA.11 – цілеспрямованість функцій. Процес оцінки повинен включати рекомендації по забезпеченню цілеспрямованості функцій. Наприклад:

– колективні методи, які забезпечують ефективне одержання інформації, пов'язаної із забезпеченням безпеки інформації від керівників різного рівня;

– методи аналізу, які на основі використання інформації про ресурси забезпечують фокус на функції по визначенню погроз і ризиків;

– методи аналізу, які використовують інформацію про ресурси й погрози для визначення обсягу оцінки вразливостей;

– планування функцій, що забезпечують ранжування ризиків на основі його показників;

12) RA.12 – організаційні та технологічні проблеми. Процес оцінки повинен розглядати як організаційні, так і технологічні проблеми. Оцінка ризиків безпеки інформації повинна включати:

– відомості про поточний стан практики безпеки;

– відсутність або неадекватність практики безпеки (або організаційні (процедурні) уразливості);

– технологічні слабості представлення в ключових системах і компонентах інформаційних технологій.

Оскільки безпека містить у собі і організаційний, і технологічний компоненти, важливо, щоб у ході оцінки були розглянуті як організаційні, так і технологічні проблеми. Група аналізу повинна проаналізувати обидва типи проблем у взаємозв'язку з місією та бізнес–задачами організації (при розробці стратегії безпеки й планів захисту). Виконавши це, аналітики будуть здатні сформувати загальну картину щодо ризиків безпеки інформації, які насправді мають місце в організації.

13) RA.13 – участь співробітників основних та IT–підрозділів. Процес оцінки повинен припускати участь представників як від основних (базисних)

підрозділів, так і департаменту інформаційних технологій, а також служби безпеки. Це забезпечує міждисциплінарний характер групи аналізу. Необхідність участі співробітників із ключових сфер діяльності організації обумовлена вимогою інтеграції різних точок зору на проблеми забезпечення безпеки інформації. До роботи також можуть залучатися співробітники, що представляють різні рівні керування організації (вище керівництво, середній рівень керівництва, рядові співробітники).

Об'єднання різних точок зору і їх бачення є істотним, оскільки необхідно розглянути широкий діапазон факторів ризику. Співробітники, які працюють у лінійних підрозділах організації, добре розуміють важливість ділових процесів і операцій, а також систему і інформацію, яка підтримує ці операції. Вони краще розуміють суть несприятливих наслідків (збитку), які можуть наступити в результаті порушень у роботі різних систем. Співробітники IT–підрозділів, включаючи експертів по захисту інформації, краще розуміють архітектуру існуючих систем і збиток, можливий при використанні технологічних вразливостей. Вони перебувають у кращій позиції щодо оцінки впливу злочинних дій на працездатність систем;

14) RA.14 – участь вищого керівництва. Вище керівництво організації повинне брати участь і займати активну позицію під час реалізації процесу оцінки. Вище керівництво повинно:

– демонструвати й надавати активну підтримку процесу оцінки;

– брати участь у роботі з одержання й відображення поглядів та виділяти проблеми забезпечення безпеки і їхній вплив не бізнес–процеси;

– розглядати й затверджувати стратегію безпеки й плани захисту;

– визначати наступні функції щодо реалізації стратегії безпеки й планів захисту.

Це єдиний і найбільш важливий фактор успіху оцінки ризиків безпеки інформації. Участь вищого керівництва організації демонструє підтримку процесів оцінки в організації. Такий рівень підтримки забезпечить:

– реальну участь рядових співробітників у процесі оцінки;

– серйозне, мотивоване й сумлінне відношення рядових співробітників до виконання робіт з оцінки ризиків;

– дієвість результатів оцінки.

Активна участь вищого керівництва в оцінці ризиків безпеки інформації також важлива для забезпечення успіху цієї ініціативи. Старші керівники допоможуть визначити обсяг оцінки й склад учасників. Якщо керівники підтримують проведення оцінки, співробітники організації приймають більше активну участь у цьому процесі. У противному випадку рядові співробітники досить швидко втрачають інтерес до цих робіт.

15) RA.15 – концепція співробітництва. Кожна функція процесу оцінки повинна опиратися на взаємодію й співробітництво між співробітниками, які беруть участь у виконанні цієї функції. Високий рівень співробітництва може бути досягнутий через використання колективних методів аналізу проблем і прийняття рішень, та інших інтерактивних методів. Концепція співробітників є істотним атрибутом оцінки ризиків безпеки інформації. Оскільки проблема безпеки по своїй природі міждисциплінарна, то виконання дій по оцінці вимагає різних знань і навичок. Таким чином, дуже важливо, щоб кожна функція по оцінці вимагала від всіх учасників максимальної взаємодії й співробітництва. Тільки в цьому випадку буде забезпечене ефективне використання знань і вмінь для успішного виконання конкретної функції.

Очікувані результати по кожному процесу (або функції) оцінки ризиків будемо називати виходами. Група аналізу повинна добре представляти остаточні результати й прагнути до їхнього досягнення. Виходи в основному являють собою ту або іншу інформацію (дані), на підставі якої приймають проміжні й остаточні рішення. Ці дані можуть бути розбиті на три категорії:

– організаційні дані;

– технологічні дані;

– дані по аналізі ризику і його усуненню.

Як уже було сказано вище, процес оцінки ризиків складається з підготовчої й трьох основних функцій (процесів) (див. рисунок 1.2). Ці функції відбивають міждисциплінарну природу проблем забезпечення безпеки інформації.

Розглянемо виходи кожної функції процесу оцінки ризиків. Опис результату представляється у вигляді двох сутностей:

– вимоги або істотні характеристики (показники) кожного результату;

– важливість результату для процесу оцінки.

2.3 Процеси (функції) оцінки

Організаційний, технологічний і систематичний аспекти оцінки ризику безпеки інформації становлять концептуальну основу для опису процесу оцінки і його результатів. Процес оцінки складається із трьох основних процесів (функцій):

1) процес 1: побудова профілю погроз безпеки;

2) процес 2: ідентифікація вразливостей;

3) процес 3: розробка стратегії безпеки й планів захисту.

На сучасному етапі розвитку виробничої та ділової діяльності організації інформаційно–телекомунікаційна інфраструктура пронизує всі рівні керування організації і впливає практично на всі сфери господарювання. Більшість виробничих, технологічних, управлінських і бізнес–процесів мають таку відмітну рису, як розподіленність, що приводить до спеціалізації робочих функцій, виконуваних рядовими співробітниками організації. Звідси випливає те, що співробітники організації відіграють немаловажну роль у забезпеченні безпеки інформації. Кожна людина має унікальні знання про те, яка інформація важлива для виконання тієї або іншої роботи, функції, завдання. Кожний співробітник має своє унікальне бачення перспектив організації, у тому числі й у сфері захисту інформації, має свій

погляд щодо поточного стану практики безпеки в організації, своє думку й оцінку щодо рівня ефективності або неадекватності того або іншого виду практичної діяльності по забезпеченню безпеки інформації.

2.3.1 Побудова профілю погроз безпеки

У ході виконання першого процесу виконуються функції, які дозволяють з'ясовувати що думають і знають співробітники організації щодо проблем безпеки інформації. Збір цих знань, їхня консолідація і аналіз можуть бути здійсненні тільки шляхом розробки й застосування неформальних методів системного аналізу (організації опитувань, анкетування, семінарів і нарад). У ході цих дій співробітники організації повинні висловити свою думку щодо їхнього бачення того:

– що є важливим для організації (ресурси (активи) пов'язані з інформацією);

– яким чином у даний момент здійснюється захист цих ресурсів (стан практичної діяльності по забезпеченню безпеки інформації);

– недоліки або неадекватність тих або інших практик безпеки (організаційна (процедурна) уразливість).

Дії по збору цієї інформації вимагають репрезентативної групи представлення різних підрозділів організації, включаючи основні підрозділи, включаючи IT–підрозділи. Крім того, повинні бути представники від різних рівнів керування організацією. Члени групи аналізу організують проведення таких дій і забезпечують їхнє виконання.

У ході об'єднання й аналізу аналітики виконують такі функції:

– визначають найбільш інформативні дані в ході дії по виявленню знань співробітників;

– вибирають ресурси, які є найбільш важливими для організації (критичні ресурси);

– описують (формулюють) вимоги безпеки для критичних ресурсів;

– ідентифікують погрози критичним ресурсам.

Аналіз специфіки перерахованих вище завдань визначає вимоги до знань і вмінь аналітиків, яких включають до складу групи аналізу.

Виходами першого процесу є:

1) RO 1.1 – критичні ресурси. Процес оцінки повинен визначити які ресурси є критичними. Актив – це що–небудь, що представляє цінність для організації. Критичні активи – це активи, які є найбільш важливими для організації. Організації може бути нанесений певний збиток у результаті порушення критичних активів. Критичні активи є фокусом (основним об'єктом) для всіх інших дій оцінки ризиків безпеки інформації;

2) RO 1.2 – вимоги безпеки для критичних активів. Вони відбивають важливі властивості активів, які повинні бути визначені для кожного критичного активу. Основними вимогами безпеки є конфіденційність, цілісність та доступність. Вимоги безпеки забезпечують основу для розробки планів захисту;

3) RO 1.3 – погрози критичним ресурсам. Процес повинен включати спосіб визначення й опису погроз безпеки. Погроза безпеки – це потенційна несприятлива подія. Розуміння сутності погроз критичним активам допомагає сформувати основу для дослідження ІТІ й визначення аналізу ризиків;

4) RO 1.4 – поточний стан практики безпеки. Процес оцінки повинен визначити поточний стан практичної діяльності по забезпеченню безпеки інформації. Практика безпеки – це дії, роботи, процедури й заходи щодо захисту інформації, що у даний момент ініційована, реалізована і підтримується в організації. Практика безпеки в основному відображає організаційний аспект захисту інформації Визначення того, які заходи щодо забезпечення безпеки інформації здійснюються в конкретний момент в організації, допомагає співробітникам зрозуміти, що вони виконують і які

заходи вони повинні підтримувати. Поточна практика безпеки – це та основа, на якій формується майбутня стратегія безпеки організації;

5) RO 1.5 – поточні організаційні уразливості. Процес оцінки повинен визначити організаційні (процедурні) уразливості організації. Процедурна уразливість − це недоліки в організації робіт із забезпечення безпеки інформації. Ці уразливості визначаються відсутністю або неадекватністю практик безпеки. Визначення того, які процедурні уразливості властиві організації та зрозуміти які заходи (роботи, дії) необхідно поліпшувати. Ці напрямки по поліпшенню повинні бути інтегровані в стратегію безпеки інформації.

Основним завданням функцій при зборі інформації є ідентифікація того, який реальний вплив на діяльність організації роблять проблеми захисту інформації. Основними завданнями функцій при аналізі зборів інформації є формування реальної картини по забезпеченню безпеки інформації в організації. Важливість сформулювати виходи визначається тим, що надалі вони використаються в якості вхідних даних для виконання другого та третього процесів й створюють основу для розробки стратегії безпеки й планів захисту.

2.3.2 Ідентифікація вразливостей

Змістом другого процесу є оцінка інформаційно−телекомунікаційної системи з погляду захисту інформації. У ході другого процесу група аналізу виконує такі функції:

− здійснює дослідження інформаційно−телекомунікаційної інфраструктури, практичних ресурсів та погроз для цих ресурсів;

− ідентифікує ключові компоненти систем інформаційних технологій і компоненти, які пов'язані з кожним практичним ресурсом;

− застосовує спеціальний інструментарій для визначення вразливостей ключових компонентів;

– аналізує результуючі дані для визначення вразливостей, які можуть привести до неавторизованих дій стосовно критичних ресурсів.

Основними учасниками другого процесу є безпосередньо члени групи аналізу. Крім того, до складу групи повинні бути введені співробітники IT–підрозділів, що володіють необхідним знаннями й уміннями в сфері застосування й експлуатації (адміністрування) систем інформаційних технологій. При необхідності можуть бути залучені зовнішні експерти. Важливо забезпечити достатню глибину дослідження проблем, пов'язаних із застосуванням інформаційних технологій і комп'ютерних систем.

Розглянемо основні виходи другого процесу:

1) RO 2.1 – ключові компоненти. Процес оцінки повинен визначити ключові компоненти інфраструктури для проведення аналізу технологічних вразливостей. Ключові компоненти – це пристрої, які важливі для обробки, зберігання, запису або передачі інформації. Вони представляють активи, пов'язані із критичними активами. Ключові компоненти вибираються зі складу компонентів ITI, які є об'єктами оцінки технологічних вразливостей. Ці компоненти визначать границі оцінки технологічних вразливостей.

2) RO 2.2 – поточні технологічні уразливості. У ході процесу оцінки повинні бути ідентифіковані технологічні уразливості в ITI. Технологічна уразливість − це слабість у системі, що може безпосередньо привести до неавторизованих дій. Уразливості представлені в службах мереж, архітектурі, операційних системах і додатках. Типи – конструктивні (архітектурні), реалізаційні та конфігураційні. Важливість технологічних вразливостей обумовлена тим, що вони визначають недоліки в ITI організації, які можуть бути використані зловмисником. Таким чином, визначення технологічних вразливостей допомагає відобразити дійсні стан ITI.

Додатково шаблони технологічних вразливостей можуть указати на проблеми, що мають місце в практиці безпеки організації.

Ідентифікація вразливостей відображає технологічний ступінь захисту інформації. Основний результат процесу – розуміння й усвідомлення технологічних вразливостей, які присутні в службах мережі, архітектурі мереж, операційних системах і додатках. Важливість другого процесу обумовлена тим, що:

– результати першого процесу переглядаються у взаємозв'язку з ІТІ;

– результати другого процесу, задокументовані у встановленому порядку, відображають стан ІТІ відповідно до технологічних слабостей, які можуть бути використані зловмисниками (фактор–людина).

2.3.3 Розробка стратегії безпеки й планів захисту

Змістом третього процесу є здійснення аналізу ризиків й функцій по усуненню виявлених ризиків. Під час здійснення аналізу ризиків група аналізу ідентифікує й аналізує ризики для критичних ресурсів організації.

Завдання процесу:

– зібрані дані використовуються для виміру ризиків критичним ресурсам (наприклад, опису збитку або визначення ймовірності);

– визначення критеріїв і показників оцінки ризиків, опираючись на загальне розуміння якісних метрик збитку (високий, середній, низький);

– оцінка ризику відповідно до критеріїв оцінки.

У результаті група аналізу приймає рішення щодо усунення кожного типу ризиків і розробляє стратегію безпеки, що опирається на зібрану інформацію. Зокрема, аналітики:

– розробляють стратегію безпеки й плани захисту ресурсів організації;

– визначають наступні дії, які повинні бути виконані для реалізації стратегії безпеки й планів захисту.

Члени групи аналізу є безпосередніми учасниками даного процесу. Якщо необхідно, то до складу групи додатково включаються співробітники, що мають необхідні знання й уміння.

Керівники організації розглядають і затверджують стратегію безпеки й плани захисту.

Виходами третього процесу є:

1) RO 3.1 – ризики критичним активам. Процес оцінки повинен включати метод опису ризиків. Ризик – це можливість завдання збитків або втрат. Він є потенційною реалізацією несподіваних негативних наслідків конкретних подій. Ризики стосуються тих ситуацій, коли особи можуть реалізувати які–небудь небажані дії або збої у функціонуванні систем або природних катаклізмів, реалізація яких приведе до негативних наслідків або збитку. Ідентифікація ризиків критичних активів характеризує вплив погроз безпеки на місію й цілі організації. Глибоке розуміння ризиків є важливим, оскільки це дозволяє розглянути й оцінити погрози безпеки в контексті цільових напрямків організації. Вони формують основу для визначення пріоритетів стратегії безпеки;

2) RO 3.2 – вимірювання ризиків. Процес оцінки повинен установити засоби вимірювання рівня ризику для кожного критичного ресурсу. Введення показників ризику важливо для визначення пріоритетів при формуванні стратегії безпеки.

3) RO 3.3 – стратегія безпеки. Вона повинна бути головним результатом процесу оцінки. Стратегія безпеки організації визначає основні напрямки прикладених зусиль по поліпшенню безпеки інформації. Вона включає підходи для організації, реалізації й підтримці практик безпеки в організації. Стратегія безпеки інтегрується в довгострокові ініціативи організації. Створення стратегії безпеки обумовлена тим, що вона є картою руху організації до необхідного рівня безпеки інформації.

4) RO 3.4 – плани захисту (усунення ризику) ресурсів повинні бути одним з результатів оцінки. Ці плани визначають конкретні дії, спрямовані на зниження ризиків для практичних активів організації. У ході розробки цих класів група аналізу повинна враховувати організаційні ресурси та

обмеження. Створення класів захисту є важливим тому, що вони визначають множину дій, необхідних для захисту критичних ресурсів організації. Важливість третього процесу обумовлена тим, що саме в ході виконання функцій цього процесу група аналізу глибоко усвідомлює проблеми безпеки інформації, в результаті чого розробляється діюча стратегія безпеки й практичних планів захисту. Третій процес включає функції і по аналізу ризиків, і по прийняттю рішень щодо їхнього усунення. Важливість дій по аналізі ризиків визначається такими факторами:

– оцінюють погрози безпеки інформації в контексті цільових напрямків організації, у результаті чого формулюється точне визначення й зміст ризику для критичних ресурсів;

– вводять критерії для виміру ризиків і основу для визначення пріоритетів при розробці планів захисту (класів усунення ризиків).

Функції по прийняттю рішення по усуненню ризиків є важливими тому, що вони:

– формують стратегію безпеки як напрямок поліпшення станів безпеки інформації в організації;

– формують класи захисту (усунення) ризиків для кожного критичного ресурсу;

– вимагають від вищого керівництва розглянути стратегії безпеки й плани захисту з погляду цільових перспектив організації, формуючи в такий спосіб підтримку керівництвом результатів оцінки;

– визначають, що повинна виконати організація в результаті оцінки, формуючи в такий спосіб послідовні рухи по поліпшенню безпеки інформації.

3. ПОБУДОВА ARIS–МОДЕЛЕЙ ПРОЦЕСУ ВИРОБЛЕННЯ СТРАТЕГІЇ ЗАХИСТУ ІНФОРМАЦІЇ OCTAVE

3.1 Опис дій по оцінці ризиків

Представимо загальну методику оцінки ризиків у вигляді моделі "чорного ящика". Процес оцінки ризиків ділиться на функції (процеси), які у свою чергу діляться на дії, а ті на процедури й роботи (рисунок 3.1).

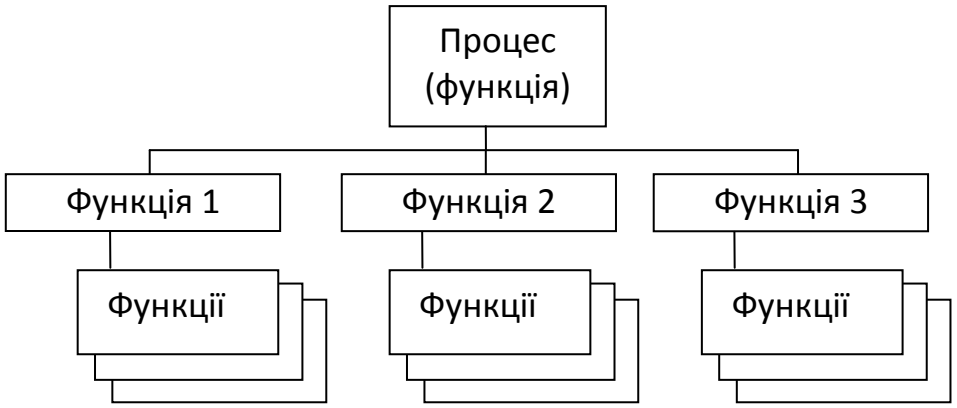


Рисунок 3.1 – Загальна методика оцінки ризиків

Розглянемо більш докладно зміст функцій абстрактного процесу оцінки ризиків. Основна увага на першому процесі оцінки приділяється персоналу організації. Необхідно забезпечити участь співробітників з різних підрозділів організації для з'ясування їхньої точки зору й представлення:

– про інформаційні активи й пов'язані з ними ресурси, які необхідні для виконання службових обов'язків;

– про поточний стан практичної діяльності по забезпеченню безпеки інформації, що здійснюється в організації;

– які організаційні уразливості є в цей час в організації.

Група аналізу аналізує отриману інформацію й формує загальну картину, що відображає безліч інформаційних активів і пов'язаних з ними

ресурсів організації, поточний стан практики забезпечення безпеки і процедурні уразливості організації.

Після цього група аналізу виконує такі функції:

– визначає активи й ресурси, які є найбільш важливими для досягнення головних цілей (місії) організації та рішення основних завдань, тобто критичні активи й ресурси;

– створює множину вимог безпеки для кожного критичного активу або ресурсу;

– розробляє унікальний профіль погроз (на основі еталонного профілю) для кожного типу критичних ресурсів, що описує діапазон погроз, які можуть бути реалізовані для критичних ресурсів.

Формально графічний опис абстрактних функцій процесу оцінки задається графом типу дерева, де коренева вершина Р (верхній або нульовий рівні) відповідає процесу в цілому. У цьому випадку під процесом будемо розуміти організовану сукупність функцій, що реалізуються з урахуванням зовнішніх і внутрішніх обмежень, і спрямовані на досягнення поставлених цілей.

Процес складається з функцій $F_1,...,\ F_n$, які пов'язані між собою об'єктами потоку (в основному, це інформаційні потоки). Кожна функція з 1–го рівня складається з функцій $F_{1.1}, F_{1.2},..., F_{1.m}$, що розкриває зміст функції (рисунок 3.2)

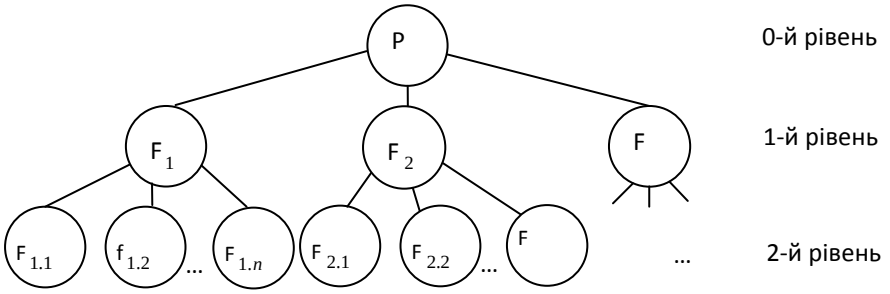


Рисунок 3.2 – Опис процесу

Дуги дерева визначають відносини на множині $\{P, F_1, ..., F_n, P_{1.1}, P_{1.2}, ..., P_{1.m} ..\}$.

Розглядаємо модель функцій, які співставляються з вершинами дерева (рисунок 6.3). Формально–графічний опис функцій складається з рамки (квадрат з округленими кутами), у яку:

– ліворуч входять стрілки, що позначають вхідні об'єкти дії. У загальному випадку вихідних об'єктів може бути декілька і вони утворюють множину вхідних об'єктів;

– зверху входять стрілки, що позначають ціль (цілі) виконуваної дії. Ціль може бути структурована на підцілі й задачі;

– знизу входять стрілки, що позначають ресурси, необхідні для виконання дії. У загальному випадку для виконання дій може знадобитися множина ресурсів;

– праворуч із рамки виходять стрілки, позначені вихідними об'єктами (інформаційними об'єктами). У загальному випадку на виході дії формується множина вихідних об'єктів.

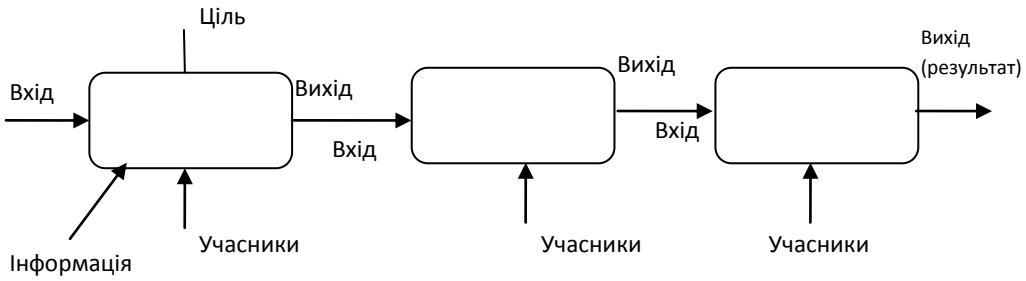


Рисунок 3.3 – Модель графічного опису стратегії функцій

У моделі процесу 1 реалізуються наступні функції:

– Р 1.1 – ідентифікація ресурсів;

– Р 1.2 – визначення поточної практики безпеки;

– Р 1.3 – визначення процедурних вразливостей організації;

– Р 1.4 – визначення критичних ресурсів;

– Р 1.5 – опис вимог безпеки для критичних ресурсів;

– Р 1.6 – розробка профілю погроз для критичних ресурсів.

Метою функції Р 1.1 є створення загально організаційного переліку інформаційних ресурсів. При виконанні функції визначаються інформаційні активи і ресурси, які важливі для досягнення головної мети і рішення різних задач організації. Вхідним інформаційним об'єктом є неформалізовані знання співробітників різних підрозділів організації, керівників різного рівня про інформаційні активи і ресурси, необхідні для виконання своїх службових обов'язків. Група аналізу, поєднуючи ці відомості, класифікує й обробляє їх, створює загальну картину, що відображає множину інформаційних активів і пов'язаних з ними ресурсів, необхідних для організації.

При виконанні цієї функції дуже важливо врахувати різні точки зору щодо цих ресурсів, урахувати наскільки вони необхідні й важливі для рішення конкретних задач. Саме тому, перш ніж приступити до формування загального бачення щодо активів, необхідно визначити приватні погляди. Основними учасниками функції є співробітники різних підрозділів організації й керівники різного рангу. Члени групи аналізу забезпечують організацію проведення функції. Важливість цієї функції визначається тим, що, знаючи, які активи (ресурси) є найбільш важливими для організації, керівництво може сконцентрувати обмежені ресурси на захист найбільш важливих інформаційних активів і пов'язаних з ними ресурсів.

Метою функції Р 1.2 є визначення стану практичної діяльності по забезпеченню безпеки інформації. Тобто визначення того, які заходи щодо забезпечення безпеки інформації здійснюються в організації і як вони виконуються. Основними учасниками функції є репрезентативна група співробітників і керівників організації.

Головною метою функції Р 1.3 є формування списку необхідних процедурних вразливостей організації. Виконання цієї функції дозволяє

визначити процедурні уразливості. Співробітники різних підрозділів організації й керівники різного рангу повинні висловити свою точку зору щодо існуючих процедурних вразливостей організації. Група аналізу аналізує різні відомості й формує загальне бачення цього питання.

Метою функції Р 1.4 є вибір тих активів і ресурсів, які є найбільш важливими для організації. Такі активи й з будуть називатися критичними.

Для цього група аналізу аналізує зібрану на процедурних функціях інформацію, а потім здійснюють вибір найбільш важливих активів (ресурсів). Кількість критичних активів повинна бути мінімізована. Ключовими учасниками функції є члени групи аналізу. Важливість функції обумовлена тим, що після її виконання наші критичні ресурси будуть у центрі уваги організації і є об'єктом виконання наступних функцій по оцінці ризиків.

Головною метою функції Р 1.5 є формулювання й опис вимог безпеки для кожного критичного активу (ресурсу). Основним результатом функції є опис (а при необхідності й формалізація) вимог безпеки для критичних ресурсів. Група аналізу повинна сформувати множину вимог безпеки для кожного критичного ресурсу. При виробленні цих вимог група аналізу розглядає аспекти конфіденційності, цілісності й доступності цих ресурсів, а також взаємозв'язок між вимогами безпеки. Ключовими учасниками функції є члени групи аналізу. До складу групи повинні входити особи, що мають необхідні знання й навички для рішення таких завдань. Вимоги безпеки для критичних ресурсів підкреслюють значимість і якісні характеристики цих активів (ресурсів). Вимоги формують основу для розробки стратегії безпеки інформації.

Метою функції Р 1.6 є визначення діапазону погроз, які можуть впливати на кожний критичний ресурс (актив). Результатом функції є визначення конкретної множини погроз, реалізованих для кожного критичного ресурсу. Група аналізу досліджує кожний критичний ресурс у контексті наявності для нього потенційних погроз (еталонний профіль

погроз) Приймає рішення які погрози із профілю застосовні до ресурсу. Таким чином формується унікальна модель погроз для критичних ресурсів організації. При розробці правила погроз, група аналізу також розглядає унікальні погрози, які можуть бути й не представлені в еталонній моделі.

Профіль погроз, створений у ході даної функції, допомагає сформувати основу для обстеження ІТІ організації (процес 2) і ідентифікації й аналізу ресурсів (процес 3).

При виконанні процесу 2 основна увага приділяється оцінці ІТІ організації. У ході другого процесу члени групи аналізу й співробітники ІТ-підрозділів:

– вибирають специфічні компоненти ІТІ для аналізу технологічних вразливостей;

– вибирають підходи для оцінки кожного компонента;

– узагальнюють результати оцінки технологічних вразливостей, що впливають на кожний критичний актив;

– обновляють профіль погроз для кожного критичного активу, опираючись на результати оцінки компонентів ІТІ.

Другий процес містить у собі наступні функції:

– Р 2.1 – вибір компонентів ІТІ для оцінки;

– Р 2.2 – оцінка вразливостей з використанням засобів аналізу;

– Р 2.3 – аналіз вразливостей і узагальнення результатів;

Ціллю Р 2.1 є вибір специфічних компонентів ІТІ для проведення оцінки технологічних вразливостей через перевірку мережного доступу до критичного ресурсу й вибору підходу для оцінки вразливостей.

На даному етапі необхідно знайти компромісне рішення пов'язане із забезпеченням балансу між глибиною й шириною оцінки (обсягом оцінки) і витратами (тимчасовими, людськими й т.д.) на проведення такої оцінки. Результатом є множина специфічних компонентів ІТІ, які підлягаються оцінці на наявність технологічних вразливостей.

Для кожного критичного ресурсу група аналізу розглядає погрози, пов'язані з можливістю мережного доступу неавторизованими особами. Ці погрози впливають на ресурси через злочинне використання технологічних вразливостей або злочинні дії людей. Опираючись на такі специфічні погрози критичним ресурсам, група аналізу визначає компоненти, які можуть бути використані легітимними користувачами для доступу до критичних ресурсів.

Для організації з великою ІТІ додатково проводять визначення ключових класів інфраструктурних компонентів. Потім для оцінки вразливостей вибираються окремі компоненти з кожного ключового класу. Після того здійснюється оцінка уразливості інфраструктури.

Важливість функції обумовлена необхідністю обґрунтування множини вимог для обсягу оцінки вразливостей. Обрані компоненти - ті компоненти, які підлягають подальшій оцінці на наявність технологічних вразливостей.

Метою функції Р 2.2 є визначення технологічних уразливостей, що мають місце в обраних компонентах, і створення їх попереднього переліку.

Співробітники проводять оцінку вразливостей обраних компонентів за допомогою спеціальних (автоматизованих) засобів. Після цього здійснюється перегляд докладної інформації про вразливості, сформовані цими засобами, інтерпретація результатів і формування попередніх узагальнених даних про технологічний вразливості для кожного ключового компонента. Важливість функції обумовлена тим, що вони допомагають визначити специфічні слабості ІТІ організації, які можуть бути використанні факторами погроз.

Ціллю функції Р 2.3 є розробка узагальнених результатів по технологічним уразливостям, які впливають на кожний критичний актив, і оновлення профілю погроз для кожного критичного активу, опираючись на результати оцінки ключових компонентів ІТІ. Її важливість полягає в узагальненні технологічних вразливостей, опису типів виявлених вразливостей (потрібна класифікація), які необхідно усунути й опис дій і рекомендації для їх усунення. Важливість функції обумовлена тим, що в

результаті формується загальна картина технологічних вразливостей, які можуть використатися зловмисниками.

Третій процес оцінки носить аналітичний характер. У його ході група аналізу визначає ризики критичним ресурсам організації й приймає рішення щодо їхнього усунення. У результаті група аналізу розробляє стратегію безпеки й плани усунення ризиків критичним ресурсам. Керівництво організації розглядає запропоновану стратегію й плани, вносить у них зміни, опираючись на наявні обмеження на ресурси організації. Далі визначаються наступні кроки, необхідні для реалізації стратегії. Третя фаза включає виконання наступних функції:

– Р 3.1 – визначення ризиків для критичних ресурсів;

– Р 3.2 – розробка критеріїв оцінки ризиків;

– Р 3.3 – оцінка ризиків для критичних ресурсів;

– Р 3.4 – розробка стратегії безпеки;

– Р 3.5 – розробка планів захисту;

– Р 3.6 – розгляд стратегії безпеки й планів захисту керівництвом;

– Р 3.7 – визначення плану наступних дій.

Метою функції Р 3.1 є опис потенційних збитків, завданих організації, як можливий результат реалізації погроз для кожного критичного ресурсу.

Група аналізу аналізує профіль погроз для кожного ресурсу. Для кожного результату реалізації погроз, представлених у профілі, аналітик дає оповідальний опис потенційного збитку.

Ризики можуть бути визначені у двох вимірах. Вимірюємо "збиток" і вимірюємо "імовірність". У випадку використання виміру "імовірність" необхідно описати мотив, засоби й сприятливі ситуації по використанню мережного або фізичного доступу. Потім необхідно розглядати будь–які історичні (архівні) дані по цьому типі погроз, відзначити будь–які незвичайні умови, які можуть впливати на погрози.

Дана функція є важливою тому, що вона зосереджує увагу на вплив погроз на організацію через розгляд погроз у контексті діяльності організації. Це формує основу для визначення пріоритетів при виконанні інших функцій. Дані щодо ймовірності погроз також корисні для уточнення пріоритетів.

Метою функції Р 3.2 є визначення критеріїв оцінки ризиків для виміру збитку, що забезпечують однозначне розуміння кількісного або якісного виміру збитку.

Група аналізу визначає, що становить високий, середній і низький рівень збитку в організації, розглядаючи різницю з потенційного збитку.

Використовуючи імовірнісні показники, в ході аналізу ризиків група аналізу повинна визначити змісту високої, низький і середній імовірності погрози. При розробці такого критерію необхідно враховувати інформацію про мотиви, засоби й умови, які сприяють фактору-людині використати мережний або фізичний доступ, історію погроз і інші фактори.

Важливість функції обумовлена тим, що вводяться критерії, для яких установлюється, що є високий, середній і низький збиток для організації. Види збитків, опис яких було отримано в попередній функції (Р 3.1), оцінюється з використанням критеріїв, розроблених у ході даної функції. Показники збитку використовуються для визначення пріоритетів під час усунення ризику. Таким чином важливо розробити й ввести в практику організації критерій корисних і значимих для організації.

У випадку застосування імовірнісних показників необхідно визначити і їхню сутність. Використання цих показників дозволить уточнити пріоритети.

Критерії оцінки є якісними. Вони розробляються в широкому діапазоні типів або категорій збитку. Звичайно розглядаються наступні категорії збитку: репутація організації/довіри споживачів, безпека/здоров'я споживачів, штрафи/санкції, фінансовий збиток, продуктивність.

Сфери збитку є контекстуальними і повинні адаптуватися для задоволення потреб організації. Перед виконанням оцінки група аналізу

повинна визначити унікальність сфер діяльності для організації, що підлягають розгляду. Одним зі способів визначення таких сфер є системний аналіз цілей організації і категорій збитку, пов'язаних із цими цілями.

Цілі функції Р 3.3 є такими:

1) визначити величину збитку для кожного типу збитку й розробити ризик–профіль для кожного ресурсу;

2) визначити ймовірність кожної погрози й уточнити ризик-профіль.

Для кожного описаного типу збитку вводиться (визначається) його величина. Група аналізу розглядає опис кожного збитку та його оцінку відповідно до введених критеріїв, призначаючи збитку конкретну величину:

Якщо додатково використовуються ймовірності оцінки, то група аналізу аналізує відповідні дані для кожної погрози й здійснює оцінку ймовірності погрози шляхом призначення відповідної величини.

Коли група аналізу призначить величину збитку для кожного типу збитку кожному ресурсу, а також призначить значення ймовірності кожної погрози для критичного ресурсу, здійснюється розробка профілю ризиків для цих критичних ресурсів.

Ризик–профіль для критичного ресурсу визначає діапазон ризиків, які впливають на ресурс. Ризик–профіль для критичного ресурсу складається з наступної інформації: профіль погроз для критичного ресурсу; вимоги безпеки для критичного ресурсу; опис збитку від реалізації погроз із профілю погроз; імовірнісні характеристики погроз із профілю погроз; величина збитку від погрози; значення ймовірності погрози; компоненти ІТІ, пов'язані із критичними ресурсами, які потребують розгляду; психологічні уразливості для кожного досліджуваного компонента інфраструктури.

Мета функції Р 3.4 є розробка стратегії забезпечення безпеки інформації в організації.

Група аналізу аналізує поточну практику безпеки організації, поточні організаційні уразливості й слабості організації, а також ризик–профіль для

кожного практичного ресурсу. Потім приступають до розробки стратегії забезпечення безпеки шляхом розгляду напрямків практичної діяльності з нормативної (еталонної) моделі. Аналітики розглядають стратегії, які допомагають організації підтримувати їхню поточну практику безпеки, звертаючи увагу на процедурні уразливості й на ризики з високим пріоритетом. Після цього аналітики розглядають основні напрямки практичної діяльності з еталонної моделі й визначають будь–які додаткові стратегії, які дозволяють співробітникам організації краще розуміти й виконувати свої обов'язки в даній сфері діяльності.

Важливість дії обумовлена тим, що в результаті розробляється стратегія, заснована на інформації, яка зібрана в ході оцінки, а не стратегія, що опирається на абстрактні моделі. У проекті стратегії представляються пропозиції для керівництва організації від групи аналізу. Надалі цей проект пропонується для розгляду й затвердження керівництву компанії.

Мета функції Р 3.5 є розробка проектів планів усунення ризиків з метою зменшення ризиків до критичних ресурсів.Група аналізу розглядає поточну практику безпеки організації, поточні процедурні уразливості організації й ризик–профіль для кожного критичного ресурсу.

Для кожного критичного ресурсу група аналізу визначає, які ризики організація буде активно усувати, а які ризики будуть прийняті організацією.

Група аналізу використає для цього значення збитку. Як додатковий фактор можуть бути використані значення ймовірностей. Для ризиків, щодо яких було ухвалене рішення про їхнє усунення, група розробляє плани, які встановлюють конкретні функції по запобіганню погроз Для ранжування функцій (установлення пріоритетів) використовуються величини збитку. Основна увага повинна приділятися усуненню погроз, реалізація яких приводить до найбільшого збитку місії організації або цілям (завданням) організації.

Якщо використовуються значення ймовірностей, вони застосовуються для уточнення пріоритетів, отриманих на основі аналізу збитку.

Плани усунення ризиків визначають функції, необхідні для зниження ризиків критичним ресурсам. Ці функції є важливими, оскільки вимагають, щоб група аналізу розробила плани для кожного критичного ресурсу на основі інформації, зібраної в ході процесу оцінки.

Проекти планів містять пропозиції групи аналізу для керівників організації. Плани надалі підлягають розгляду й затвердженню керівництвом організації. Дана функція має важливість тому, що жадає від керівників організації розглядати плани з урахуванням перспектив організації.

Керівництво вносить зміни в політику й плани, опираючись на розумінні ресурсів і обмеження для компанії в цілому. Цей етап важливий також і тому, що сприяє формуванню активної підтримки з боку керівництва.

Метою функції Р 3.7 є визначення для керівництва організації плану функцій, які необхідні для реалізації стратегії безпеки й планів захисту.

Вище керівництво організації визначає, що буде робити організація для реалізації результатів оцінки, і визначає, що будуть робити керівники для поліпшенню процесів забезпечення безпеки інформації.

Керівники організації також визначають, чи існують які–небудь інші функції по поліпшенню питань для забезпеченню безпеки й визначають підходи організації до проведення оцінки ризиків у майбутньому. Група аналізу забезпечує проведення цієї функції.

Важливість даної функції обумовлена тим, що в результаті визначається конкретний план функцій для реалізації розробленої стратегії. Без чіткого визначення цих функцій і без активної підтримки вищого керівництва малоймовірно, що ініціатива по поліпшенню забезпечення безпеки інформації досягне успіху.

3.2 Моделювання в ARIS 5.0

Після запуску з операційної системи Windows програмне середовище ARIS створює головне вікно, що містить всі інші робочі вікна, панелі, діалоги. Початковий вигляд головного вікна наведений на рисунку 3.4.

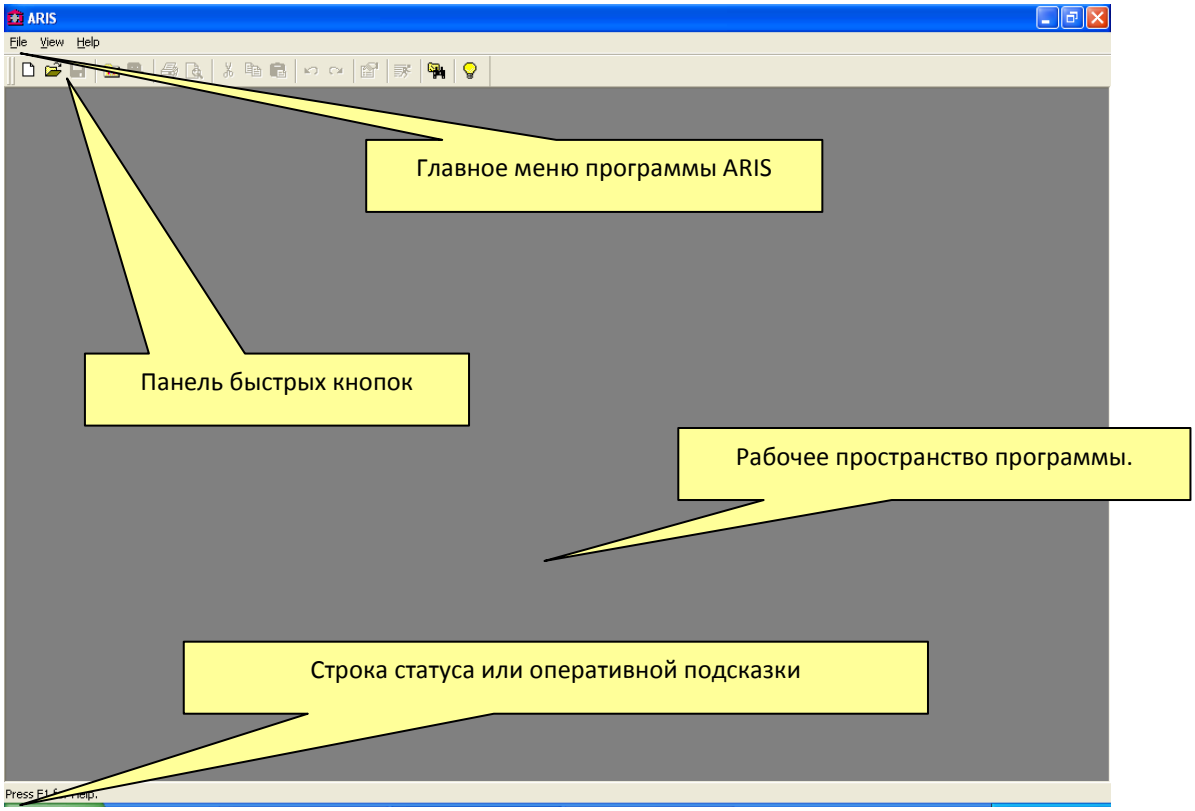


Рисунок 3.4 – Головне вікно програмної середовище ARIS

У головному вікні знаходяться елементи для керування ходом роботи в середовищі ARIS:

Головне меню – містить упорядкований список доступних пунктів–команд для керування елементами середовища ARIS (вікнами, об'єктами, моделями та ін.). Деякі пункти меню доступні при активному елементі.

Панель швидких кнопок (Tool Bar) – це набір кнопок, що "натискаються" за допомогою мишки. При цьому склад набору

конфігурується з дій, які найбільш часто використовуються у цей момент роботи в середовищі.

Рядок статусу (Status Bar) – невелике текстове повідомлення, що пояснює поточний стан програмного середовища ARIS. У деяких випадках містить рекомендації дій для данної ситуації.

Робочий простір – частина головного вікна програми, у якому з'являються робочі елементи середовища: вікна провідника, дизайнера моделей, діалогові вікна й т.д.

Закриття головного вікна приводить до завершення роботи в середовищі ARIS. При цьому можуть бути запити до користувача, якщо дані не збережені та необхідність їх відобразити в базі моделювання.

Зовнішній вигляд вікна провідника наведений на рисунку 3.5. Вікно провідника в будь–який момент можна показати, нажавши клавішу F9.

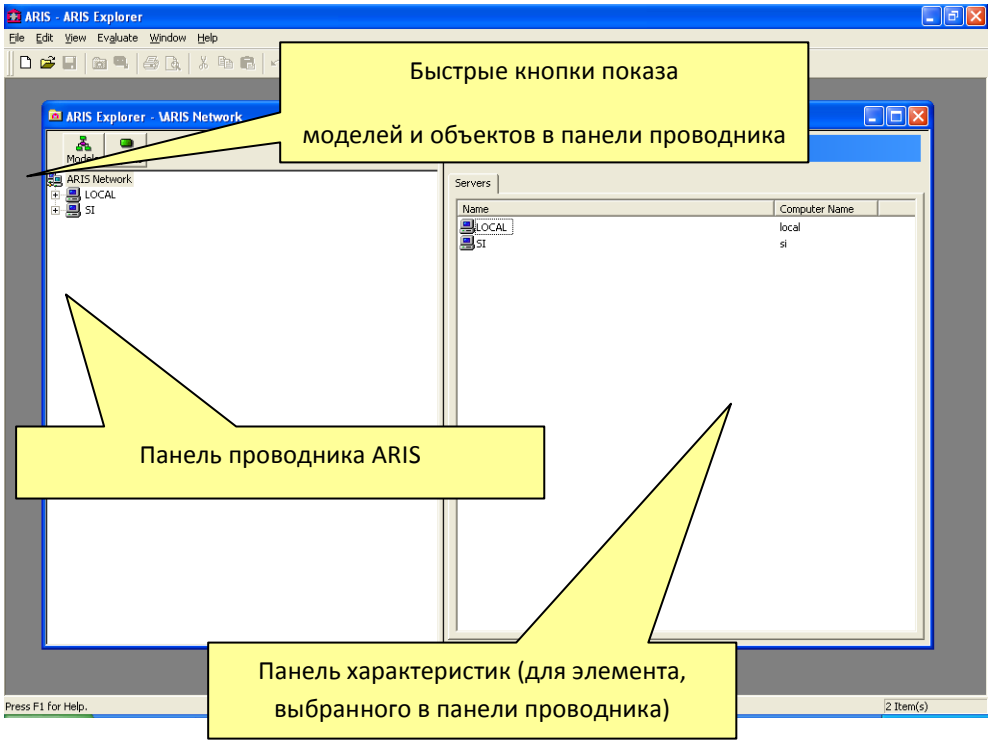


Рисунок 3.5 – Вікно провідника ARIS

Вікно провідника складається з декількох частин, що дозволяють оперативно переміщатися між робочими моделями й об'єктами, розташованими в базі моделювання бізнес–процесів.

Розташована ліворуч панель провідника ARIS містить перелік підключених серверів, баз даних на них і зміст баз даних моделювання. За допомогою панелі можна оперативно переключатися між вмістом груп, характеристиками моделей і об'єктів.

Розташована праворуч панель характеристик для обраного (активного) елемента в панелі провідника ARIS розкриває його вміст. Для групи це перелік внутрішніх груп і моделей з об'єктами. Для моделей або об'єктів дана панель показує взаємозв'язок з іншими елементами моделювання.

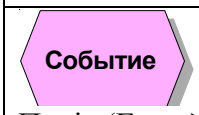
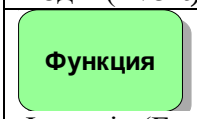
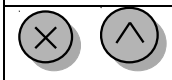
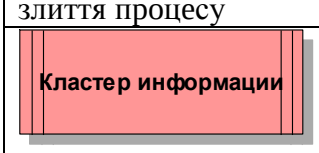
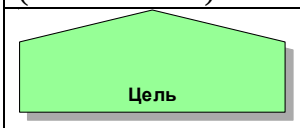
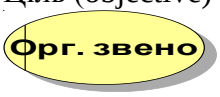
Для створення нової моделі вибирається група, усередині якої буде розташовуватися модель. Вибирається пункт "New\Model" у локальному меню для цієї групи. Після цього з'являється діалог створення нової моделі. Спочатку необхідно вибрати тип моделі. Далі в діалозі вводиться ім'я нової моделі. При успішному завершенні діалогу з'являється вікно з моделлю.

Перебуваючи у вікні дизайнера, за допомогою миші перетягуємо необхідні нам об'єкти з панелі об'єктів. При цьому не можна забувати про довідники об'єктів. Якщо необхідно вказати один з довідкових об'єктів, то його краще взяти з панелі провідника по моделях і об'єктам.

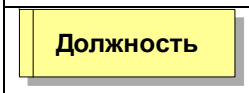
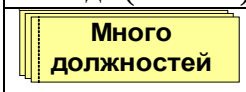
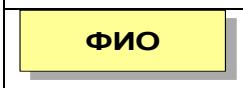
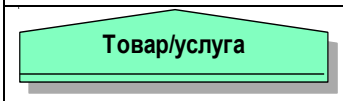
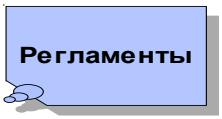
Після появи об'єктів на діаграмі проводимо зв'язки (відношення) між ними, дотримуючись їх адекватності реальному положенню речей. Зв'язок утвориться за допомогою миші (потрібно проконтролювати натискання кнопки активності проведення зв'язків). Для цього треба підвести курсор миші до краю символу об'єкта, від якого буде виходити зв'язок. З появою характерного покажчика можливості початку встановлення зв'язку треба натисніть один раз ліву кнопку миші. Далі потрібно вести курсор до символу об'єкта, на якому зв'язок закінчується. Якщо тип моделі й методологічний фільтр дозволяють проводити між обраними об'єктами відношення, то на

краю символу з'явиться розв'язний вид курсору. Натиснувши ліву кнопку миші, можна між об'єктами встановити відношення і на діаграмі з'явиться з'єднуюча лінія. У таблиці 3.1 наведено об’єкти та символи, які використовуються для побудови моделей.

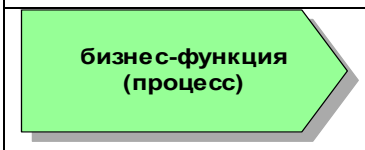
Таблиця 3.1 – Об'єкти й символи, необхідні для побудови моделей

Тип и символ об'єкта	Цільове використання	Правила іменування
1	2	3
 Подія (Event)	Відображення подій, що відбуваються при виконанні бізнесу-процесу.	Ім'я починається з імені об'єкта, стан або подія стосовно якого відбулася.
 Функція (Function)	Опис бізнес-функції в ланцюжку виконання бізнес-процесу.	Ім'я починається з дії або позначення процесу, істотні характеристики якого приводяться далі в імені.
 Правила розгалуження або злиття процесу	Вказівка крапок розгалуження або злиття в ході виконання бізнес-процесу.	Об'єкти даного типу не йменуються
 Набір даних (Cluster)	Опис абстрактного (на концептуальному рівні) набору формалізованих даних.	В імені необхідно згадати назву документа або джерела походження інформації
 Документ (Document)	Подання інформаційного носія даних у матеріалізованому виді (напр. на папері).	Ім'я повинно містити найменування документа.
 База даних (файл) (Database/File)	Подання інформаційного носія даних у нематеріальній формі (напр. на магнітному диску або флеш-пам’яті).	Іменується назвою файлу або ім'ям інформаційної бази даних
 Ціль (objective)	Вказівка однієї із цілей діяльності компанії.	Напівформальний опис досягає мети
 Організаційна одиниця (Organizational unit)	Позначення окремого штатного підрозділу.	Повна назва підрозділу

Продовження таблиці 3.1

1	2	3
 Юридична особа	Позначення юридичної особи	Повна назва юридичної особи
 Група (Group)	Група може відображати групу співробітників, що працюють разом протягом певного проміжку часу, наприклад, проектна група.	Повна назва тимчасового колективу (групи)
 Посада (Position)	Представлення посади.	Повна назва посади
	Множинна посада використовується для подання сукупності осіб, що виконують однотипну роботу	Повна назва посади
 Співробітник (internal person)	Співробітник є окремим службовцем компанії (ідентифікуємо, приміром, по його персональному коду) і може бути пов'язаний з організаційними одиницями (у які він входить), а також з функціями (які він виконує або за які відповідає).	Співробітник указується прізвищем і ініціалами (додатково, може вказуватися персональний номер)
 Товар, Услуга (Product/Service)	Об'єкт використовується для представлення результату людських дій або технічного процесу й може бути як матеріальним продуктом (тип матеріалу, тип операційного ресурсу, допоміжні технічні засоби, тип пакувального матеріалу), так і послугою.	Повне найменування товару або послуги
	Подання знань або вмінь, якими повинен володіти співробітник або необхідними для успішного виконання бізнесу-функції.	Напівформальне визначення необхідного обсягу знань
	Об'єкт використовується для ідентифікації формалізованого (задокументованого) обсягу знань, необхідних для виконання бізнес-функції.	Повна назва документа, що містить інформацію

Продовження таблиці 3.1

1	2	3
	Позначення бізнес-функції верхнього (концептуального) рівня опису діяльності організації.	Аналогічно іменуванню об'єкта "Функція"

3.3 Модель дерева функцій (Function Tree)

Функція – опис елемента роботи, що утворює один логічний етап у рамках процесу. В ARIS використається діаграма "Дерево функцій", за допомогою якої функції можуть бути описані з різними рівнями деталізації. При цьому функції представляються не обов'язково в хронологічному порядку.

На самому верхньому рівні описуються найбільш складні функції, що представляють собою повністю окремий бізнес–процес або відповідну процедуру. Деталізація функцій утворить ієрархічну структуру їх описів. Модель дерева функцій згідно стратегії захисту інформації OCTAVE наведена в Додатку В.

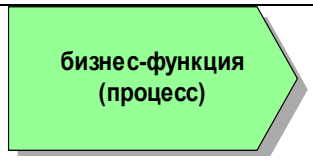
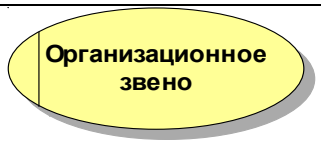
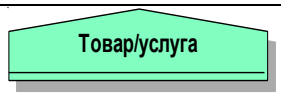
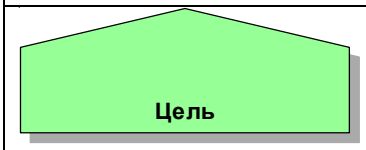
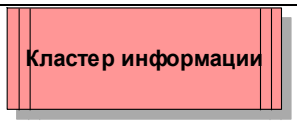
Діаграма складається з переліку функцій. Основні функції: побудова профілю загроз, ідентифікація ІТІ організації та розробка стратегії безпеки та планів захисту. Кожна з цих функцій декомпозується. Спосіб подання функцій у вигляді дерева дозволяє зменшити ступінь складності і є статичним описом функції.

3.4 Модель ланцюжка доданої вартості (Value-Added chain Diagram)

Діаграма ланцюжків доданої вартості описує функції організації, які безпосередньо впливають на реальний вихід її продукції. Перелік об'єктів діаграми ланцюжка доданої вартості наведено у таблиці 3.2.

В моделі VAD (Додаток Г) розглянуті всі функції (побудова профілю загроз, ідентифікація ITI організації, розробка стратегії безпеки та планів захисту), їх входи, виходи (вихід з першої функції поступає на вхід другої функції), цілі методу OCTAVE, організаційні структури та ін. Функції створюють послідовність дій, формуючи додані значення: вартість, кількість, якість і т.д. У даній моделі функції представлені в логічній послідовності головних процесів із вказівкою найближчого оточення.

Таблиця 3.2 – Перелік об'єктів діаграми ланцюжка доданої вартості

Тип і символ об’єкта	Характеристика об’єкта
	Бізнес-функція (процес) верхнього рівня, виконання якої спрямоване на досягнення мети.
	Організаційна ланка складу організаційної структури, що виконує функцію.
	Товар або послуга, що забезпечують досягнення мети
	Якісна або кількісна ситуація (стан), досягнення якої важливо для компанії
	Набір інформації

3.5 Модель подійно–керованого процесу (eEPC)

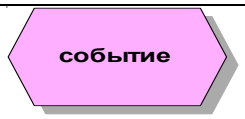
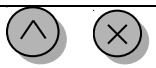
Цей тип моделей є центральним елементом для всього бізнес–моделювання в методології ARIC. eEPC є динамічною моделлю, що з'єднує разом статичні ресурси (організаційні одиниці, інформаційні системи,

продукти, послуги, і т.п.) і становить із них логічні послідовності бізнес–функцій або процесів.

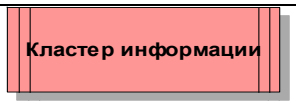
Концептуально діаграма eEPC складається з наступних типів об'єктів: подія (стан); функція; правила розгалуження; ресурси (організаційні одиниці, інформаційні системи, продукти, послуги, і т.п.) (можуть бути відсутніми або винесені в окрему діаграму оточення бізнес–функції).

У таблиці 3.3 наведено перелік об'єктів діаграми подійно–керованого процесу.

Таблиця 3.3 – Перелік об'єктів діаграми подійно-керованого процесу

Тип і символ об’єкта	Характеристика об’єкта
1	2
	Події являють собою зміну в навколишньому світі в результаті виконання процесу.
	Функції являють собою елементарні дії, спрямовані на здійснення бізнесу-процесу.
	Правила розгалуження процесу, у яких відбувається зміна напрямку послідовності виконуваних функцій
	Організаційна ланка, посада (у т.ч. множинна) складу організаційної структури, що виконує функцію
 	Інформаційні носії, як матеріальної форми (паперові документи,.....), так і електронного представлення інформації: бази даних, файли, електронні листи, ресурси Інтернет, ОЛАП
	Структурована (задокументована) або неформальна інформація, що втримується в навичках співробітника, необхідна для коректного виконання бізнесу-функції

Продовження таблиці 3.3

1	2
	Товар або послуга, що є результатом виконання бізнес-функції
	Якісна або кількісна ситуація (стан), досягнення якої важливо для компанії
	Описуваний на верхньому рівні набір інформації який або поступає на вхід бізнесу-функції, або являється її результатом

Події являють собою зміну в навколишньому світі в результаті виконання процесу. Це можуть бути:

1) зовнішні зміни(події), що приводять до початку процесу;

2) внутрішні зміни, викликані ходом виконання процесу;

3) завершальні (вихідні) зміни, що мають зовнішній ефект результату виконання.

Функції являють собою елементарні дії, спрямовані на здійснення бізнесу–процесу. Функції можуть виконуватися людьми або автоматизованими системами. Функції мають вхід та вихід (матеріальний, інформаційний тощо) і можуть споживати для свого здійснення деякі ресурси.

ВИСНОВКИ

В роботі розглянуто три моделі: діаграма дерева функцій, діаграма ланцюжка доданої вартості та діаграма подійно-керований процесу. Діаграми відображають метод OCTAVE. Моделі в ARIS сприяють розумінню нової ідеології стратегічного управління безпекою інформації керівниками підприємств та підрозділів безпеки інформації.

Побудовані моделі не охопили всі фактори для захисту інформації, оскільки це не є можливим. Завжди існують фактори, які можуть негативно вплинути на стратегію захисту інформації. Дуже складно все врахувати в процесі розробки та реалізації стратегії.

В останньому розділі був проведений аналіз питань охорони праці при впровадженні розробленої системи звукового забезпечення (Додаток Д).