ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ:

КСЗІ	комплексні системи захисту інформації;
ІБ	інформаційна безпека;
ІС	інформаційна система;
ISO	international Organization for Standardization міжнародна організація по стандартизації;
СМІБ	системи менеджменту інформаційної безпеки;
HAZOP	hazard and Operability Study - аналіз небезпеки і працездатності;
HACCP	Hazard Analysis and Critical Control Point - аналіз ризиків и критичні контрольні точки;
SWIFT	structured what-if technique - структурований аналіз сценаріїв методом «що, якщо»;
CRAM	risk analysis and management method;
CCTA	central computer and telecommunications agency;
ГКУ	Господарський кодекс України
ОС	Операційна система
ПК	Персональний комп’ютер

ВСТУП

Нові інформаційні технології бурхливими темпами впроваджуються в усі сфери діяльності людини. Розвиток інформаційних технологій призвів до збільшення цінності інформації, що циркулює в автоматизованих системах управління, суспільство поступово переходить на електронний документообіг, зростає популярність інформаційно-пошукових систем. Це призвело до зростання загроз, спрямованих на нанесення шкоди даним в інформаційних системах (розголошення, зміна, витік, несанкціонований доступ, блокування доступу і т.д.) [1]. Як наслідок, актуалізувалася потреба захисту даних в інформаційних системах, а також розробки систем захисту інформації які дозволяють забезпечити потрібний рівень інформаційної безпеки.

Комплексні системи захисту інформації (КСЗІ) - це системи складаються з сукупності органів і (або) виконавців, а також технік захисту що ними використовуються, організованих і функціонуючих за правилами, встановленими правовими, розпорядчими і нормативними документами в галузі захисту інформації[1]. КСЗІ складаються з різноманітних технологій, методів, а також засобів захисту даних.

Технології захисту інформації в КСЗІ ґрунтуються на застосуванні сучасних методів, які запобігають втраті і витоку інформації, гарантують її цілісність. Основними способами захисту є: перешкода, маскування, регламентація, управління, примус, і спонукання.

Під перешкодою розуміється спосіб фізичного захисту інформаційних систем, завдяки якому зловмисники не мають можливість потрапити на територію, що охороняється.

Маскування - способи захисту інформації, що передбачають перетворення даних в форму, не придатну для сприйняття сторонніми особами. Для розшифрування потрібне знання принципу.

Регламентація - найважливіший метод захисту інформаційних систем, що передбачає введення особливих інструкцій, згідно з якими повинні здійснюватися всі маніпуляції з охоронюваними даними.

Управління - способи захисту інформації, при яких здійснюється управління над усіма компонентами інформаційної системи.

Примус - методи захисту інформації, тісно пов'язані з регламентацією, які передбачають введення комплексу заходів, при яких працівники змушені виконувати встановлені правила.

Якщо використовуються способи впливу на працівників, при яких вони виконують інструкції з етичних і особистісним міркувань, то мова йде про спонукання.

Способи захисту інформації передбачають використання певного набору засобів. Для запобігання втрати і витоку конфіденційних відомостей використовуються такі засоби: фізичні, програмні і апаратні, організаційні, а також законодавчі і психологічні.

Фізичні засоби захисту інформації запобігають доступ сторонніх осіб на територію, що охороняється. Фізичні засоби використовуються для охорони даних як на паперових, так і на електронних носіях. Апаратні засоби представлені пристроями, які вбудовуються в апаратуру для обробки інформації.

Програмні засоби - це сукупність програмних продуктів використовуваних для вирішення різних завдань із захисту інформації, в тому числі попередження витоку і забезпечення безпеки інформації, що захищається. Включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та ін. Апаратні засоби - це різні за типом пристрою (механічні, електромеханічні, електронні та ін.), які апаратними засобами вирішують завдання захисту інформації. Вони перешкоджають доступ до інформації, в тому числі за допомогою її маскування[2].

Організаційні засоби пов'язані з наступними методами захисту: регламентацією, управлінням, примусом. До організаційних засобів відноситься розробка посадових інструкцій, бесіди з працівниками, комплекс заходів покарання і заохочення. При ефективному використанні організаційних засобів працівники підприємства добре інформовані про використання засобів захисту інформації, чітко виконують свої обов'язки і несуть відповідальність за надання недостовірної інформації.

Законодавчі засоби - визначаються законодавчими актами країни, якими регламентуються правила користування, обробки і передачі інформації обмеженого доступу і встановлюються міри відповідальності за порушення цих правил[3].

Психологічні засоби - комплекс заходів для створення особистої зацікавленості працівників у збереженні та автентичності інформації. До психологічних засобів відноситься і побудова корпоративної культури, при якій кожен працівник відчуває себе важливою частиною системи і зацікавлений в успіху підприємства.

Підсумувавши, екосистема систем захисту інформації численна і різноманітна, базується на різних технологіях і методах захисту. Такі системи можуть мати різну ефективність, складність і співвідношення ціна/якість. КСЗІ переважно, будуються індивідуально для конкретного об'єкту захисту. Відповідно від характеристик об'єкта, вимог замовника і фінансування, із великої кількості технологій, методів і засобів, необхідно обрати чи побудувати ефективну КСЗІ. Чисельність і різноманітність КСЗІ, а також індивідуальність потреб замовника, потребують ефективного підбору технологій, методів і засобів захисту інформації, які максимально задовольнятимуть вимогам замовника. Найбільш об'єктивним показником для замовника є оцінка зниження ризику від впровадження КСЗІ. У цьому нам допомагають методики оцінки ризиків, вони дозволяють оцінити цінність інформації, загрози витоку, так і наслідки її втрати. Методи оцінки ризиків входять до складу систем захисту інформації.

1. Аналіз методик оцінки ризиків

1.1Оцінка інформаційних ризиків

Поняття інформаційної безпеки нерозривно пов'язане з ризиками для інформаційних ресурсів. Під ризиками розуміється можливість нанесення шкоди інформаційних ресурсів, зниження рівня їх захищеності. Ризики можуть мати різну природу і характеристики; однією з основних класифікацій ризиків для інформаційної безпеки є їх поділ:

- на системні ризики - некеровані ризики, пов'язані з тією середовищем і технічною інфраструктурою, в якій функціонують інформаційні системи;
- операційні ризики - керовані ризики, пов'язані з особливостями використання певних інформаційних систем, їх технічної реалізації, застосовуваними алгоритмами, апаратними засобами і тому подібне[4].

Для того щоб ефективно протидіяти ризикам, їх треба дослідити. Дослідження ризикив виконується завдяки оцінці інформаційних ризиків.

Оцінка інформаційних ризиків полягає в розрахунку ризиків, який виконується з урахуванням відомостей про критичність активів, а також ймовірностей реалізації вразливостей.

Класична формула оцінки ризиків:

$$R=D \times P(V) \qquad 1.$$

де R - інформаційний ризик;

D - критичність активу (збиток);

P (V) - ймовірність реалізації уразливості [5].

Під критичністю розуміється ступінь впливу інформації на ефективність функціонування процесів компанії. Критичність інформації правильніше оцінювати з точки зору трьох загроз - конфіденційності, цілісності і доступності, тому що збиток компанії від реалізації цих загроз може сильно відрізнятися, і оцінка загального збитку призведе до неадекватних результатів аналізу ризиків[6].

Імовірність реалізації уразливості – це можливість створення іншої загрози по відношенню до будь-якій системі, процесу або ресурсу. Імовірність реалізації загрози оцінюється експертом в області інформаційної безпеки на підставі власного досвіду і особливостей

інформаційної системи компанії. Як правило, основними факторами при визначенні ймовірності реалізації загрози є такі параметри, як частота виникнення загрози і простота її реалізації[6].

Результати оцінки ризиків, як правило, представляються в «Звіті про оцінку інформаційних ризиків компанії» [5].

«Звіт про обробку інформаційних ризиків компанії» детально описує способи обробки ризиків. Крім цього, складається «План зниження ризиків», де чітко описуються конкретні заходи щодо зниження ризиків, співробітники, відповідальні за виконання кожного положення плану, терміни виконання плану.

Сфера інформаційної безпеки нерозривно пов'язана з ризиками для інформаційних ресурсів. Для того щоб ефективно протидіяти ризикам, їх треба дослідити. Дослідження ризиків виконується завдяки оцінці інформаційних ризиків. Оцінка інформаційних ризиків є однією з найважливіших частин КСЗІ, вона допомагає зрозуміти, які ризики найбільш актуальні для певної інформаційної системи. Як правило оцінка ризиків є експертною оцінкою що в свою чергу накладає певні недоліки що впливають на якість оцінки. Це відбувається тому що кожен експерт визначає ймовірності і збитки по своєму, спираючись на свій досвід і інші вподобання. Програмна ж реалізація методик оцінки ризиків дозволяє уникнути цих проблем і є більш доступною для користувача ніж експертна.

1.2 Огляд стандарту ISO/IEC 27001

ISO / IEC 27001: 2005 «Системи управління інформаційної безпеки. Вимоги», - це міжнародний стандарт підготовлений для реалізації вимог по створенню, впровадженню, підтримці і постійного поліпшення системи менеджменту інформаційної безпеки. Визначає вимоги до засобів контролю безпеки, спеціально розроблені для потреб організації, або її частини.

Стандарт застосовується при виборі адекватних і пропорційних засобів контролю інформаційної безпеки, які захищають інформаційні активи і надають впевненість зацікавленим сторонам. Призначенням стандарту є встановлення вимог до системи управління інформаційною безпеки для демонстрації здатності організації захищати свої інформаційні ресурси.

Система управління ризиками стандарту дозволяє отримувати відповіді на наступні питання:

- На якому напрямку інформаційної безпеки потрібно зосередити увагу?
- Скільки часу і коштів можна витратити на дане технічне рішення для захисту інформації? Менеджмент ризиків відбувається за класичною схемою: пошук, класифікація, ранжування, оцінка, план по зниженню ризиків, прийняття залишкових ризиків і регулярний перегляд ризиків[4].

Стандарт ISO визначає інформаційну безпеку як: «збереження конфіденційності, цілісності та доступності інформації; крім того, можуть бути включені і інші властивості, такі як справжність, неможливість відмови від авторства, достовірність».

Основним завданням інформаційної безпеки є захист інформаційних ресурсів компанії від внутрішніх і зовнішніх умисних і ненавмисних загроз (підробка, вандалізм, крадіжка, пожежа, системний збій та ін.).

Метою інформаційної безпеки є забезпечення безперервності бізнесу компанії і мінімізація бізнес-ризиків шляхом попередження інцидентів безпеки і зменшення розмірів потенційного збитку.

Стандарт декларує два основних принципи управління:

- Процесний підхід до управління безпекою, який розглядає управління як процес - набір взаємозв'язаних безперервних дій, акцентує увагу на досягненні поставлених цілей, а також ресурсах, витрачених для досягнення цілей.
- Застосування PDCA - моделі як основи для всіх процедур управління ІБ. PDCA - модель визначає чотири етапи, які повинні виконуватися послідовно для кожного процесу (Рисунок 1.1).

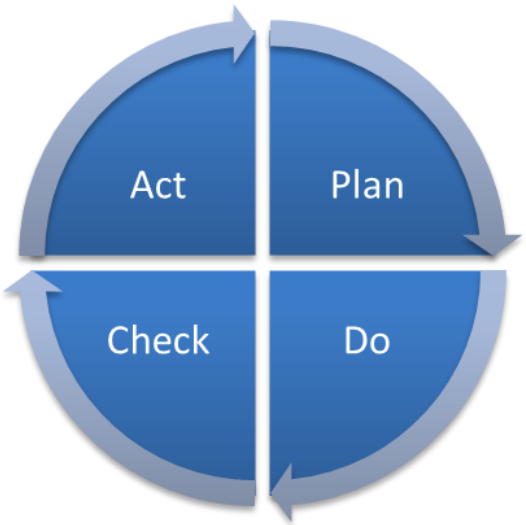

Рисунок 1.1 - PDCA модель

Процесна модель включає 4 групи процесів[7]:

- планування - забезпечується правильне завдання контексту і масштабу СУІБ, оцінюються ризики інформаційної безпеки, пропонується відповідний план обробки цих ризиків;
- реалізація - впроваджуються прийняті рішення, які були визначені на стадії планування;
- перевірка - збір інформації та контроль результату на основі ключових показників ефективності, встановлення причин відхилень;
- дія - вжиття заходів щодо усунення причин відхилень від запланованого результату, зміни в плануванні і розподілі ресурсів.

В стандарті наводяться вимоги до документації, яка в повинна включати[7]:

- положення політики СУІБ;
- опис області функціонування;
- опис методики;
- звіт про оцінку ризиків;
- план обробки ризиків;
- документування пов'язаних процедур.

Процес управління документами СУІБ, повинен включати[7]:

- актуалізацію;
- використання;
- зберігання;
- знищення.

Стандарт ISO/IEC 27001 визначає, що керівництво організації несе відповідальність за забезпечення і управління ресурсами, необхідними для створення СУІБ, а також організацію підготовки персоналу.

Поряд з елементами управління для комп'ютерів і комп'ютерних мереж, стандарт приділяє велику увагу питанням[7]:

- розробки політики безпеки;
- роботі з персоналом (прийом на роботу, навчання, звільнення з роботи);
- забезпечення безперервності виробничого процесу;
- юридичним вимогам.

У стандарті передбачаються методика оцінки ризиків, і також присутній перелік обов'язків організації для впровадження процесу оцінки ризиків ІБ який відповідатиме потребам стандарту.

Організація повинна визначити і впровадити процес оцінки ризиків інформаційної безпеки, на підставі якого[7]:

- встановити і підтримувати критерії для ризиків інформаційної безпеки, які включають в себе:
  - критерії прийняття ризиків;
  - критерії для проведення оцінки ризиків інформаційної безпеки;
- гарантувати, що повторна оцінка ризиків інформаційної безпеки дозволить отримати логічні, обґрунтовані і зіставні результати;
- визначити ризики інформаційної безпеки:
  - застосувати процес оцінки ризиків інформаційної безпеки для виявлення ризиків, пов'язаних з втратою конфіденційності, цілісності та доступності інформації в рамках системи менеджменту інформаційної безпеки;
  - визначити власників ризиків;
- проаналізувати ризики інформаційної безпеки:
  - визначити потенційні наслідки, які можуть виникнути в разі виникнення ризиків;
  - визначити реалістичну ймовірність виникнення ризиків;
  - визначити рівні ризику;
- оцінити ризики інформаційної безпеки:
  - порівняти результати аналізу ризиків з критеріями для ризиків;
  - встановити пріоритети по обробці ризиків для проаналізованих ризиків.

Організація повинна зберігати документовану інформацію про процес оцінки ризиків інформаційної безпеки.

Стандарт описує методику оцінки ризиків яка відповідає його вимогам, але не має описання реалізації цієї методики, це зумовлено

різноманітністю систем оцінки ризику інформації. Такі системи можуть мати різну ефективність, складність і співвідношення ціна/якість.

Згідно стандарту важливим поняттям є ідентифікація загроз, їх аналіз і оцінка. Загрози - реально або потенційно можливі дії або умови навмисного або випадкового порушення режиму функціонування підприємства шляхом нанесення шкоди, що приводить до фінансових втрат, включаючи і упущену вигоду. Загрози виникають в наслідок халатного відношення до правил побудування ІС, а також правил поведінки у цих системах. Критичність та ймовірність реалізації, визначаються експертами в залежності від характеру підприємства.

ISO 27001: 2005 є стандартом, за яким проводиться офіційна сертифікація СУІБ. Стандарт являє собою перелік вимог, обов'язкових для сертифікації.

Під сертифікацією системи управління інформаційною безпекою (СУІБ) організації за вимогами стандарту ISO 27001: 2005 розуміється комплекс організаційно-технічних заходів, що проводяться незалежними експертами, в результаті чого підтверджується наявність та належне функціонування всіх рекомендованих стандартом механізмів контролю, які застосовуються в даній організації.

В більшості випадків сертифікація повністю виправдовує вкладені кошти і час. По-перше, офіційна реєстрація СУІБ організації в реєстрі авторитетних органів, таких як служба акредитації Великобританії (UKAS), що зміцнює імідж компанії, підвищує інтерес з боку потенційних клієнтів, інвесторів, кредиторів та спонсорів.

По-друге, в результаті успішної сертифікації розширюється сфера діяльності компанії за рахунок отримання можливості участі в тендерах і розвитку бізнесу на міжнародному рівні. У найбільш чутливих до рівню інформаційної безпеки областях, такий, наприклад, як фінанси, наявність сертифіката відповідності ISO 27001 починає виступати як обов'язкова вимога для здійснення діяльності.

Також дуже важливо, що процедура сертифікації чинить серйозний мотивуючий і мобілізуючий вплив на персонал компанії: підвищується рівень обізнаності співробітників, ефективніше виявляються і усуваються недоліки і невідповідності в системі управління інформаційною безпекою, що в перспективі означає для організації зниження середньостатистичного шкоди від інцидентів безпеки, а також скорочення накладних витрат на експлуатацію інформаційних систем. Цілком можливо, наявність сертифіката дозволить застрахувати інформаційні ризики організації на більш вигідних умовах.

Система управління інформаційною безпекою на основі стандарту ISO 27001 дозволить[7]:

- Зробити більшість інформаційних активів найбільш зрозумілими для управління компанії;
- Виявляти основні загрози безпеці для існуючих бізнес процесів;
- Розраховувати ризики і приймати рішення на основі бізнес-цілей компанії;
- Забезпечити ефективне управління системою в критичних ситуаціях;
- Проводити процес виконання політики безпеки (знаходити і виправляти слабкі місця в системі інформаційної безпеки);
- Чітко визначити особисту відповідальність;
- Досягти зниження і оптимізації вартості підтримки системи безпеки;
- Продемонструвати клієнтам, партнерам, власникам бізнесу свою прихильність до інформаційної безпеки;
- Отримати міжнародне визнання і підвищення авторитету компанії, як на внутрішньому ринку, так і на зовнішніх ринках;
- Підкреслити прозорість і чистоту бізнесу перед законом завдяки відповідності стандарту.

1.3 Стандарт ISO / IEC 27005

ISO / IEC 27005 «Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки» Стандарт забезпечує рекомендації для менеджменту ризиком інформаційної безпеки в організації, особливо підтримуючи вимоги системи менеджменту інформаційної безпеки (ISMS) згідно ISO / IEC 27001. Однак цей стандарт не забезпечує певної методології для менеджменту ризиків інформаційної безпеки. Цей стандарт призначений для визначення в організації підходу до менеджменту ризиків в залежності, наприклад, від області дії СМІБ, області застосування менеджменту ризиків або сектора промисловості. Щоб здійснити вимоги СМІБ багато існуючих методології можуть скористатися структурою, описаною в цьому інтернаціональному стандарті.

Даний стандарт призначений для керівників і персоналу, що займається в організації питаннями менеджменту ризику інформаційної безпеки, а також, при необхідності, для зовнішніх сторін, що мають відношення до цього виду діяльності.

Стандарт забезпечує рекомендації для менеджменту ризиків інформаційної безпеки, які включають інформацію і менеджмент ризиків телекомунікаційних технологій. Він застосовується для організацій всіх типів (наприклад, комерційних підприємств, державних установ, некомерційних організацій), які планують здійснювати менеджмент ризиків, які можуть скомпрометувати інформаційну безпеку організації.

Згідно стандарту повинні розроблятися критерії для оцінювання ризиків інформаційної безпеки організації, з огляду на наступне:

- стратегічна цінність обробки бізнес-інформації;
- критичність порушених інформаційних активів;
- правові та регулюючі вимоги і договірні зобов'язання;
- операційна важливість і важливість для бізнесу доступності, конфіденційності і цілісності;
- очікування сприйняття причетних сторін, а також негативні наслідки для репутації[8].

Крім того, критерії оцінювання ризиків можуть використовуватися для визначення пріоритетів для обробки ризиків.

Критеріями впливу повинні розроблятися і визначатися, виходячи зі ступеня збитку або витрат для організації, що викликаються подією, пов'язаною з інформаційною безпекою, з огляду на наступне:

- рівень класифікації інформаційного активу, на який виявляється вплив;
- порушення інформаційної безпеки (наприклад, втрата конфіденційності, цілісності і доступності);
- погіршені операції (внутрішні або третіх сторін);
- втрата цінності бізнесу та фінансової цінності;
- порушення планів і кінцевих термінів;
- збиток для репутації;
- порушення законодавчих, регулюючих або договірних вимог[8].

Критерії прийняття ризику повинні бути розроблені і визначені. Критерії прийняття ризику найчастіше залежать від політик, намірів, цілей організації та інтересів причетних сторін.

Організація повинна визначати власні шкали для рівнів прийняття ризику. При розробці слід враховувати наступне:

- критерії прийняття ризику можуть включати багато порогові значення, з бажаним цільовим рівнем ризику, але за умови, що при певних обставинах вище керівництво буде приймати ризики, що знаходяться вище зазначеного рівня;
- критерії прийняття ризику можуть виражатися як співвідношення кількісно оціненої вигоди (або іншої вигоди бізнесу) до кількісно оцінений ризику;
- різні критерії прийняття ризику можуть застосовуватися для різних класів ризику, наприклад, ризики, які можуть мати результатом невідповідність директивам і законам, не можуть бути прийняті, в той час як прийняття ризиків високого рівня може бути дозволено, якщо це визначено в договірному вимозі;
- критерії прийняття ризику можуть включати вимоги, що стосуються майбутньої додаткової обробки, наприклад, ризик може бути прийнятий, якщо є схвалення і згода на здійснення дії по його зниженню до прийнятного рівня в рамках певного періоду часу[8].

Критерії прийняття ризику можуть відрізнятися в залежності від того, наскільки довго, імовірно, ризик буде існувати, наприклад, ризик може бути пов'язаний з тимчасової або короткочасною діяльністю. Критерії прийняття ризику повинні встановлюватися з урахуванням наступного[8]:

- критеріїв бізнесу;
- правових та регулюючих аспектів;
- операцій;
- технологій;
- фінансів;
- соціальних і гуманітарних чинників.

Уразливості можуть бути ідентифіковані в наступних областях[8]:

- організація робіт;
- процеси і процедури;
- сталі норми управління;
- персонал;
- фізичне середовище;
- конфігурація інформаційної системи;
- апаратні засоби, програмне забезпечення та апаратура зв'язку;
- залежність від зовнішніх сторін.

Слід зазначити, що невірно реалізований або неправильно функціонуючий засіб контролю або засіб контролю, який неправильно використовується, і сам може бути вразливістю. Засіб контролю може бути ефективним чи неефективним в залежності від середовища, в якому він функціонує. І навпаки, загроза, яка не має відповідної уразливості, може не призводити до ризику. Уразливості можуть бути пов'язані з властивостями активу, які можуть використовуватися способом і з метою, що відрізняються від тих, які планувалися при придбанні або будівництві активу. Уразливості, що виникають з різних джерел, підлягають розгляду, наприклад, ті які є зовнішніми або внутрішніми по відношенню до активу.

Організації повинні визначати операційні наслідки сценаріїв інцидентів на основі (але не обмежуючись) [8]:

- часу на розслідування і відновлення;
- втрат (робочого) часу;
- втрачену можливість;
- охорони праці та безпеки;
- фінансових витрат на специфічні навички, необхідні для усунення несправності;
- репутації і іншого "невловимого капіталу.

Форма аналізу повинна узгоджуватися з критеріями оцінювання ризику, розробленими як частина встановлення контексту. Далі більш докладно описуються деталі методології оцінки:

Якісна оцінка

Якісна оцінка використовує шкалу кваліфікації атрибутів для опису величини можливих наслідків (наприклад, низький, середній і високий) і ймовірності виникнення цих наслідків. Перевага якісної оцінки полягає в

простоті її розуміння всім відповідним персоналом, а недоліком є залежність від суб'єктивного вибору шкали.

Такі шкали можуть бути адаптовані або скориговані таким чином, щоб задовольняти вимогам обставин, а для різних ризиків можуть використовуватися різні описи. Якісна оцінка може використовуватися:

- як початкова діяльність по ретельній перевірці для ідентифікації ризиків, які потребують більш детального аналізу;
- там, де цей вид аналізу є відповідним для прийняття рішення;
- там, де числові дані або ресурси є неадекватними для кількісної оцінки.

Якісний аналіз повинен використовувати фактичну інформацію і дані, де вони доступні;

Кількісна оцінка

Кількісна оцінка використовує шкалу з числовими значеннями (а не описові шкали, які використовуються в якісній оцінці) і наслідків, і ймовірності, застосовуючи дані з різних джерел. Якість аналізу залежить від точності і повноти числових значень і від обгрунтованості використовуваних моделей. В більшості випадків кількісна оцінка використовує фактичні дані за минулий період, забезпечуючи перевагу в тому, що вона може бути безпосередньо пов'язана з цілями інформаційної безпеки та проблемами організації. недоліки кількісного підходу можуть мати місце тоді, коли фактичні перевіряються дані недоступні, тому створюється ілюзія цінності і точності оцінки ризику.

Спосіб вираження наслідків та ймовірності і способи їх об'єднання для забезпечення відомостей про рівень ризику змінюються відповідно до виду ризику і метою, для якої повинні використовуватися вихідні дані оцінки ризику. невизначеність і змінність наслідків і ймовірності слід враховувати при аналізі і повідомляти про них ефективним чином.

Визначення цінності активів починається з класифікації активів відповідно до їх критичності, з точки зору важливості активів для здійснення бізнес-цілей організації. Потім визначається цінність з використанням двох заходів: відновної вартості активу:

- вартості очищення з метою відновлення і заміни інформації (якщо це можливо);

- наслідки для бізнесу від втрати або компрометації активу, наприклад, можливі несприятливі ділові та / або законодавчі або регулюють наслідки розкриття, модифікації, недоступності і / або руйнування інформації та інших інформаційних активів[8].

Цінність визначається наслідками для бізнесу, зазвичай значно вище просто відновної вартості і залежить від важливості активу для організації при виконанні її бізнес-цілей.

Вихідні дані: Перелік оцінених наслідків сценарію інцидентів, виражених по відношенню до активів і критеріям впливу[8].

1.4 Класифікація методів оцінки ризиків

Нерідко ситуація на підприємстві є унікальною, і потребує індивідуальних дій. Унікальність підприємств, а також їх фінансове забезпечення і потреби, породжують необхідність розвитку методів оцінки ризиків і їх різновидність.

1.4.1 Метод оцінки ризику «Мозковий штурм»

«Мозковий штурм» - це методика, яка націлена на сприяння вільному обговоренню і його заохочення в групі обізнаних осіб для ідентифікації потенційних видів відмов і пов'язаних з ними небезпек, ризиків, критеріїв прийняття рішень та (або) способів обробки. Термін «мозковий штурм» часто необгрунтовано застосовується для позначення будь-якого типу групового обговорення. Насправді ж «мозковий штурм» передбачає застосування спеціальних методик, щоб активувати творче мислення учасників ідеями і висловлюваннями інших членів групи.

У методі «мозкового штурму» велике значення має творче мислення. Тому його застосування особливо доцільно для ідентифікації ризиків, пов'язаних з новою технологією, коли відсутні дані або коли необхідні новаторські рішення проблем.

«Мозковий штурм» має наступні переваги:

- заохочує творче мислення, яке сприяє виявленню нових ризиків і оригінальних рішень;
- залучає ключові зацікавлені сторони і тому сприяє загальному обміну інформацією;
- простий у застосуванні і не вимагає великих витрат часу.

Метод має такі недоліки:

- учасники можуть бути недостатньо досвідченими і обізнаними для результативного участі в дослідженні;
- оскільки метод є порівняно неструктурованих, то буває важко обгрунтувати, що процес був всебічним, тобто що були ідентифіковані всі потенційні ризики;
- може існувати певна динаміка в конкретній групі, коли одні фахівці з цінними ідеями недостатньо беруть участь в обговоренні, а інші переважають. Даного недоліку можна уникнути за допомогою комп'ютеризованого «мозкового штурму» із застосуванням чат-форумів або методу номінальної групи. Комп'ютеризований «мозковий штурм» може бути анонімним, і не зачіпати персональні або політичні аспекти, які можуть негативно вплинути на вільне формування ідей. При застосуванні методу номінальної групи ідеї надходять модератору анонімно і потім обговорюються всіма учасниками групи[9].

1.4.2 Метод оцінки ризиків "Структуровані або напів структуровані опитування"

У структурованому опитуванні опитуваним особам індивідуально задають підготовлені питання, наявні в допоміжному аркуші, які сприяють аналізу ситуації опитуваною особою в іншому аспекті і, тим самим, ідентифікації ризиків в даному аспекті. Напів структуроване опитування проводиться подібним чином, але забезпечує велику свободу при обговоренні питань, що виникають.

Метод структурованих опитувань має такі переваги:

- структуровані опитування надають експертам час для роздумів над заданим питанням;
- обмін інформацією один на один може забезпечити більш глибоке розгляд питань;
- структуровані опитування дозволяють залучати більшу кількість зацікавлених осіб, ніж «мозковий штурм», який проводиться порівняно невеликою групою.

Метод має такі недоліки:

- координатору потрібна значна кількість часу на збір думок таким шляхом;
- упередженість допускається і не усувається в ході групового обговорення;
- може бути не досягнута ступінь творчого мислення, характерна для «мозкового штурму»[9].

1.4.3 Метод оцінки ризиків "Метод Делфі"

Метод Делфі - це процедура досягнення достовірного консенсусу думок групи експертів. Хоча в даний час цей термін широко застосовується для позначення будь-якої форми «мозкового штурму», важливою відмітною особливістю методу Делфі, згідно первісної формулюванні, було те, що експерти висловлювали свої думки індивідуально і анонімно, отримуючи доступ до думок інших експертів в ході процесу.

Метод Делфі має такі переваги:

- оскільки думки є анонімними, ймовірний вираз непопулярних думок;
- всі думки мають однакову вагомість, що запобігає проблему переважання окремих експертів;
- отримання права власності на результати;
- відсутність необхідності збирати всіх експертів в одному місці і в один час.

Метод має такі недоліки:

- великі витрати часу і висока трудомісткість;
- необхідність того, щоб учасники могли чітко висловлювати свої думки в письмовій формі[9].

1.4.4 Метод оцінки ризиків "Контрольні листи"

Контрольні листи являють собою переліки небезпек, ризиків або помилок при управлінні, розроблені, як правило, на основі накопиченого досвіду: за результатами попередньої оцінки ризику, або відмов в минулому. Контрольні листи можуть застосовуватися для ідентифікації

небезпек і ризиків або для оцінки результативності заходів управління. Вони можуть застосовуватися на будь-якому етапі життєвого циклу продукції, процесу або системи. Контрольні листи можуть застосовуватися як частина інших методик оцінки ризику, але більш доцільно їх застосовувати для перевірки того, що все було враховано після застосування більш творчої методики, яка застосовувалася для виявлення нових проблем.

Контрольні листи мають наступні переваги:

- можуть застосовуватися особами, які не є експертами;
- будучи належним чином розробленими, вони об'єднують широкий діапазон дослідження в одну просту в застосуванні систему;
- можуть сприяти забезпеченню повноти обліку загальних проблем.

Контрольні листи мають наступні недоліки:

- мають тенденцію стримувати творче мислення при ідентифікації ризиків;
- розглядають «те, про що відомо, що воно відомо», а не «те, про що відомо, що воно невідомо» або «те, про що невідомо, що воно невідомо»;
- сприяють формальному типу поведінки («проставлення відміток в клітинах»);
- мають тенденцію грунтуватися на спостереженні, тому існує ймовірність упустити проблеми, які не очевидні при спостереженні[9].

1.4.5 Метод оцінки ризиків "Попередній аналіз небезпек або метод PHA"

Попередній аналіз небезпек - це простий індуктивний метод аналізу, метою якого є ідентифікація небезпек і небезпечних ситуацій і подій, які можуть завдати шкоди діяльності, обладнанню або системі. Зазвичай даний метод застосовується на початковій стадії розробки проекту, коли є недостатньо інформації про проект або процедурах функціонування, і часто передує подальшого вивчення або застосовується для отримання інформації з метою встановлення вимог до проекту системи. Його застосування також доцільно при проведенні аналізу існуючих систем для визначення пріоритету небезпек і ризиків для подальшого аналізу, або тоді, коли обставини створюють перешкод для застосування більш докладних і всебічних методик.

Метод PHA має такі переваги:

- застосуємо при наявності обмеженої інформації;
- дозволяє розглядати ризики на ранньому етапі життєвого циклу системи.

Метод має такі недоліки:

- PHA надає тільки попередню інформацію;
- він не є всебічним і не забезпечує детальною інформацією про ризики і про те, як їх можна найкращим чином запобігати[9].

1.4.6 Метод оцінки ризиків "Дослідження небезпеки і працездатності або метод HAZOP"

HAZOP - акронім словосполучення «дослідження небезпеки і працездатності» (HAZard and OPrability study) - є структурованим і систематизованим дослідженням планованих або існуючих продукції, процедури або системи. Ця методика призначена для ідентифікації ризиків для персоналу, обладнання, навколишнього середовища і (або) цілей організації. Від дослідницької групи також очікується, де це можливо, вироблення рішень по обробці ризику.

Процес HAZOP є якісною методикою, заснованою на застосуванні керуючих слів, за допомогою яких сформулюються питання про те, як завдання проектування або умови функціонування можуть бути не досягнуті на кожному етапі проекту, процесу, процедури або системи. Процес зазвичай проводить група фахівців різних областей в ході декількох засідань.

Метод HAZOP має такі переваги:

- забезпечує кошти для систематичного і повного дослідження системи, процесу або процедури;
- проводиться за участю групи фахівців різних областей, які мають практичний досвід роботи, і тих, які, можливо, будуть здійснювати дії по обробці ризиків;
- дозволяє виробити рішення і дії по обробці ризиків;
- застосуємо до різноманітних систем, процесів і процедур;

- дозволяє в явному вигляді враховувати причини та наслідки помилок персоналу;
- забезпечує фіксування процесу в письмовій формі, що можна використовувати для підтвердження належної ретельності дослідження.

Метод має такі недоліки:

- детальний аналіз може зажадати великих витрат часу і, отже, бути дорогим;
- детальний аналіз вимагає високого рівня документованого або технічного опису системи або процесу і процедури;
- спрямований скоріше на знаходження конкретних рішень, а не дослідження основних припущень (дані прояви можна зменшити при поетапному підході);
- обговорення може зводитися до конкретних аспектів конструкції, не враховуючи більш загальні або зовнішні аспекти;
- обмежений (попередніми) проектом, а також метою проектування, областю застосування і цілями, встановленими групою;
- дослідження ґрунтується більшою мірою на компетентності розробників, для яких об'єктивне виявлення недоліків власних проектів може становити певні труднощі[9].

1.4.7 Метод оцінки ризиків "Аналіз небезпек і критичні контрольні точки або метод HACCP"

Аналіз небезпек і критичні контрольні точки (HACCP) - структурований метод виявлення небезпек і встановлення заходів управління на всіх розглянутих частинах процесу для запобігання небезпек і підтримки стабільності якості і безпеки продукції. Метою HACCP є забезпечення мінімізації ризиків в більшій мірі за допомогою встановлення управління протягом усього процесу, а не за допомогою перевірки кінцевої продукції.

HACCP має такі переваги:

- є структурованим процесом, що забезпечує документоване свідоцтво управління якістю, а також ідентифікацію та зменшення ризиків;

- основними є практичні аспекти того, як і де в даному процесі можна запобігти небезпеці і управляти ризиками;
- переважне забезпечення поліпшеного управління ризиком в ході всього процесу, а не перевірки кінцевої продукції;
- можливість виявлення небезпек, що виникають в результаті діяльності персоналу, і визначення методів управління ними в точці виникнення або в подальшому.

Метод має такі недоліки:

- для HACCP потрібно, щоб небезпеки були виявлені, ризики, які вони представляють - визначено, а їх значущість розглядалася як вхідні дані аналізу. Також необхідно, щоб відповідні заходи управління були визначені. Дана інформація необхідна для встановлення критичних контрольних точок і параметрів управління при здійсненні HACCP; також може знадобитися поєднання такої інформації з іншими методами для досягнення даної мети;
- застосування заходів тільки в тому випадку, коли параметри управління виходять за встановлені межі, може привести до того, що поступові зміни в параметрах управління, які є статистично значущими, і, отже, вимагають відповідних заходів, можуть бути втрачені[9].

1.4.8 Структурована методика «Що, якщо ...?» (SWIFT)

Методика «Що, якщо ...?» (SWIFT) спочатку була розроблена як спрощений альтернативний варіант HAZOP. Вона є систематичним дослідженням, проведеним групою фахівців із застосуванням ряду допоміжних слів або фраз, які використовує координатор на засіданнях для сприяння ідентифікації ризиків учасниками. Координатор і група використовують стандартні фрази типу «Що, якщо ...?» В поєднанні з допоміжними фразами, щоб дослідити, як на систему, виробничу одиницю, організацію або процедуру вплинуть відхилення від нормального функціонування і поведінки. SWIFT зазвичай застосовують на більшості рівнів систем, що мають більш низький рівень деталізації, ніж HAZOP.

SWIFT має такі переваги:

- широко застосовується до всіх видів матеріального виробництва та систем, ситуацій і обставин, організаціям і видам діяльності;

- вимагає мінімальної підготовки групи;
- не вимагає великих витрат часу на проведення, основні небезпеки та ризики швидко виявляються в ході засідання групи;
- дослідження орієнтоване на систему і дозволяє учасникам розглядати реакцію системи на відхилення, а не наслідки відмови окремих компонентів;
- може застосовуватися для виявлення можливостей для вдосконалення процесів і систем і, в загальному випадку, для визначення дій, які призводять до необхідного результату і збільшують його ймовірність;
- передбачає участь в засіданнях осіб, відповідальних за існуючі заходи управління і за подальші дії по обробці ризиків, підсилює їх відповідальність;
- дозволяє скласти реєстр ризиків і, при незначного доопрацювання, - план обробки ризиків;
- дозволяє проводити ідентифікацію ризиків і небезпек таким чином, щоб результати можна було застосовувати для кількісного дослідження, тоді як зазвичай для оцінки ризику і для визначення пріоритету щодо відповідних дій використовують якісну і напівкількісну форму ранжирування ризику.

Методика має такі недоліки:

- для результативного застосування потрібен досвідчений і кваліфікований координатор;
- необхідна ретельна підготовка, щоб не витрачати час на засіданнях групи;
- якщо в групі фахівців відсутня досить великий досвід або якщо система допоміжних фраз не повна, деякі ризики або небезпеки можуть бути не ідентифіковані;
- застосування методики на високому рівні узагальнення може не дозволити виявити складні, докладні або взаємопов'язані причини[9].

1.4.9 Аналіз сценаріїв

Аналіз сценарію - це процес розробки описових моделей того, що може статися в майбутньому. Він може застосовуватися для ідентифікації ризиків за допомогою розгляду можливих варіантів розвитку подій і

дослідження їх можливих наслідків. Групи сценаріїв, що відображають, наприклад, «найкраща нагода», «найгірший випадок» і «очікуваний випадок», можуть застосовуватися для аналізу можливих наслідків і їх ймовірностей для кожного сценарію як форма аналізу чутливості при проведенні аналізу ризику.

Ефективність аналізу сценарію підтверджується розглядом значних змін за останні 50 років в технології, переваги споживачів, соціальних позиціях і тому подібного. Аналіз сценарію не дозволяє прогнозувати ймовірність таких змін, але може розглядати наслідки і сприяти організаціям у розвитку переваг і гнучкості, необхідних для адаптації до прогнозованих змін.

Аналіз сценаріїв розглядає ряд можливих ситуацій в майбутньому, що може бути кращим у порівнянні з традиційному підходом, заснованим на прогнозах різного ступеня довгострокове, в яких передбачається, на підставі накопичених даних, що майбутні події, ймовірно, триватимуть, слідуючи минулими тенденціям. Це важливо для ситуацій, коли є недостатньо поточної інформації, на якій можна засновувати прогноз, або в яких розглядаються ризики в більш віддаленому майбутньому.

Дана перевага має відповідний недолік, що полягає в тому, що при високій невизначеності деякі сценарії можуть бути нереалістичними.

Основні труднощі при застосуванні аналізу сценаріїв пов'язані зі ступенем наявності даних і здатністю аналітиків та осіб, які приймають рішення, розробляти реалістичні сценарії, які придатні для дослідження можливих результатів.

Недолік застосування аналізу сценаріїв як засіб обґрунтування прийняття рішення полягає в тому, що застосовувані сценарії можуть не мати відповідного підстави; що дані можуть бути гіпотетичними і що ні реалістичність результатів може бути не виявлено[9].

1.4.10 Марковський аналіз

Марковський аналіз застосується в ситуації, коли майбутній стан системи залежить тільки від її поточного стану. Даний метод зазвичай використовують для аналізу ремонтопридатності систем, які можуть працювати у багатьох режимах, і в ситуаціях, коли застосування аналізу надійності окремих блоків системи недоцільно. Метод може бути застосований до більш складних систем, використовуючи більш високий порядок процесів Маркова, і обмежений тільки моделлю, математичними обчисленнями і припущеннями.

Процес Марковського аналізу є кількісним методом і може бути дискретним (використання ймовірностей переходу між станами) або безперервним (використання коефіцієнтів інтенсивності переходу зі стану в стан).

Марковський аналіз може бути виконаний вручну, однак характеристики методу дозволяють використовувати для нього комп'ютерні програми.

Перевагою Марковского аналізу є можливість обчислення ймовірностей станів систем з відновленням і множинними станами деградації.

Недоліками Марківського аналізу є наступні:

- метод заснований на припущенні про постійність ймовірностей переходу та наявністю тільки двох можливих станів елементів системи (відмови і відновлення);
- у методі використано припущення, що всі розглянуті події статистично незалежні, т.є. майбутні стани не залежать від минулих станів, за винятком безпосередньо попереднього стану;
- для застосування методу необхідно знати всі ймовірності переходу.
- робота з методом неможлива без знання операцій з матрицями;
- отримані результати важкі для розуміння персоналом, які не мають відповідних технічних знань, навичок і досвіду[10].

1.4.11 Аналіз дерева неполадок

Аналіз дерева неполадок FTA - метод ідентифікації та аналізу факторів, які можуть сприяти виникненню досліджуваного небажаної події (званого кінцевим подією).

За допомогою дедукції досліджувані фактори ідентифікують, вибудовують їх логічним чином і представляють на діаграмі у вигляді дерева, яке відображає ці фактори і їх логічний зв'язок з кінцевим подією.

Факторами, зазначеними в дереві неполадок, можуть бути події, пов'язані з відмовами компонентів комп'ютерного обладнання, помилками людини або іншими подіями, які можуть привести до небажаного події.

Перевагами FTA є наступні:

- надання точного, систематизованого і гнучкого підходу дозволяє аналізувати різноманітні фактори, включаючи дії персоналу і фізичні явища;
- застосування підходу «зверху вниз» дозволяє розглядати впливу тих відмов, які безпосередньо пов'язані з кінцевим подією;
- застосування особливо доцільно для аналізу систем, що допускають підключення великої кількості пристроїв і взаємодія з ними (систем, що мають множинні інтерфейси);
- графічне представлення дозволяє спростити розуміння функціонування системи і розглянутих факторів, але оскільки деревовидні схеми найчастіше досить громіздкі, їх обробка може зажадати застосування комп'ютерних програм, що забезпечує можливість розгляду більш складних логічних взаємозв'язків (наприклад, з використанням логічних операцій «І-НЕ» і « НЕ-І »), але при цьому ускладнює верифікацію дерева неполадок;
- логічний аналіз дерева неполадок і визначення набору мінімальних перетинів корисні при ідентифікації простих шляхів відмови в складних системах, де комбінації подій можуть призвести до виникнення кінцевого події.

Недоліками методу є наступні:

- невизначеність оцінок ймовірностей базисних подій впливає на оцінку ймовірності виникнення кінцевого події. Це може привести до високого рівня невизначеності в ситуації, коли ймовірність відмови для кінцевого події точно невідома, але достовірність оцінок істотно вище для добре вивченою системи;
- у деяких ситуаціях початкові події не пов'язані між собою, і часом важко встановити, чи враховані всі важливі шляхи до кінцевої події. Наприклад, недостатнє дослідження всіх джерел загоряння може привести до невірної оцінки ризику виникнення пожежі (кінцевого події). У цій ситуації аналіз ймовірності із застосуванням методу FTA неможливий;
- дерево неполадок є статичною моделлю, в якій фактор тимчасової залежності не враховують;
- дерево неполадок може бути застосоване лише до бінарним станів (працездатного / непрацездатному);
- не дивлячись на те що помилки людини можуть бути враховані у схемі дерева неполадок на якісному рівні, невідповідності ступеня і якості,

часто характеризують помилки людини, в дереві неполадок врахувати досить складно;

- дерево неполадок не дозволяє легко врахувати і досліджувати ланцюгові реакції (ефект доміно) і умовні відмови[10].

1.4.12 Аналіз дерева подій

Метод ETA є графічним методом уявлення взаємовиключних послідовностей подій, наступних за появою вихідної події, відповідно до функціонування і не функціонування систем, розроблених для пом'якшення наслідків небезпечної події. Метод ETA може бути застосований для якісної і/або кількісної оцінки.

Послідовність подій легко уявити у вигляді дерева подій і тому за допомогою ETA легко встановити погіршують або пом'якшувальні наслідки події, беручи до уваги додаткові системи, функції або бар'єри.

Перевагами методу ETA є наступні:

- За допомогою методу ETA легко схематично зобразити сценарії розвитку подій після виникнення початкового події, провести аналіз працездатного стану або відмови допоміжних систем або функцій, призначених для зниження наслідків відмови, і оцінити їх вплив.
- Метод допомагає врахувати фактор часу, побачити взаємозв'язки і ланцюгові реакції, які складно досліджувати за допомогою методу дерева неполадок.
- Метод графічно представляє послідовність подій, що неможливо зробити за допомогою методу дерева неполадок.

Недоліками методу є наступні:

- Для використання методу ETA в якості складової частини загального процесу оцінки необхідно ідентифікувати всі можливі початкові події. Цього можна домогтися за допомогою використання інших методів аналізу (наприклад, HAZOP, PHA), проте завжди залишається ймовірність того, що не враховано деякі важливі початкові події.
- Метод дерева подій застосуємо тільки для двох станів системи (працездатного стану і відмови), в ньому важко врахувати відстрочене порушення працездатного стану системи або її відновлення.

- Кожен шлях реалізації обумовлений поєднанням подій, що сталися в попередніх точках розгалуження схеми дерева подій[10].

В таблиці 1.1 приведено аналіз найбільш поширених методик оцінки ризиків, серед показників були обрані як показники, які впливають на якість самої методики, так і показники які дають уявлення про можливість програмної реалізації методики.

Таблиця 1.1 – характеристика методик оцінки ризиків.

Методики оцінки ризиків	Показники порівнянь												
	характеристика застосовності					атрибути						Експертна реалізація	програмна реалізація
	ідентифікація ризику	аналіз ризику			порівняльна оцінка ризику	Підхід		аналіз		посилення аналізу			
		наслідок	ймовірнісні	рівень ризику		Дедуктивний	індуктивний	якісний	кількісний	якісний	кількісний		
Мозковий штурм	SA	NA	NA	NA	NA	C	NC	(NC)	C	high	high	+	+
Структуровані або напів структуровані опитування	SA	NA	NA	NA	NA	(NC)	C	C	(NC)	high	medium	+	+
Метод Делфі	SA	NA	NA	NA	NA	NC	C	(NC)	C	Low	High	+	-
Контрольні листи	SA	NA	NA	NA	NA	(NC)	C	NC	C		medium	+	+
Метод PHA	SA	NA	NA	NA	NA	NC	C	NC	NC	low	Low	+	-
Метод HAZOP	SA	SA	A	A	A	NC	C	(C)	C	low	High	+	+

Продовження таблиці 1.1

Метод HACCP	SA	SA	NA	NA	SA	(NC)	C	NC	(C)	medium	High	+	-
Метод SWIFT	SA	SA	SA	SA	SA	(NC)	NC	C	C	low	Medium	+	-
Аналіз сценаріїв	SA	SA	A	A	A	C	NC	C	(NC)	medium	High	+	-
Марковський аналіз	A	SA	NA	NA	NA	(NC)	C	C	C	high	Medium	+	+
Аналіз дерева неполадок	SA	NA	SA	A	A	C	NC	C	C	high	Medium	+	+
Аналіз дерева подій	A	SA	A	A	NA	C	C	(NC)	C	low	Low	+	-

SA – строго застосується. NC – метод не застосовується + – реалізується
NA – не застосується. C – метод застосовується - – не реалізується
A – застосується. ( ) – метод застосовується з обмеженнями

Оцінка ризиків - це процес, який охоплює ідентифікацію ризику, аналіз ризику і порівняльну оцінку ризику. Існує безліч систем оцінки ризику, які відрізняються між собою методиками виконання оцінки, але мають єдину мету: зрозуміти, які ризики найбільш актуальні для певної (ІС) [4]. Існує велика кількість методик оцінки ризиків, як програмних (COBRA, CRAMM), так і Експертних (Мозковий штурм, Аналіз сценаріїв), доволі часто вони використовуються разом.

2. Програмні методики оцінки ризиків

Методики оцінки ризиків для інформаційних систем переслідують одну і ту ж мету: зрозуміти, які ризики найбільш актуальні для інформаційної системи даної організації. Але слідувати до цієї мети вони можуть різними способами, відповідно, будуть і помітно відрізнятися одержувані результати. Ми розглянемо кілька найбільш актуальних для українських компаній методик, які популярні як в Україні, так і в світі, і можуть бути легко знайдені як в інтернеті, так і в спеціальній літературі.

2.1 Якісні методики управління ризиками

Якісні методики управління ризиками прийняті на озброєння в технологічно розвинених країнах численною армією внутрішніх і зовнішніх IT-аудиторів. Ці методики досить популярні і відносно прості, і розроблені, як правило, на основі вимог міжнародного стандарту ISO 17799. У вересні 2002 року основні положення ISO 17799 були переглянуті і доповнені з урахуванням розвитку сучасних інформаційних технологій і вимог до організації режиму ІБ. Сьогодні це найбільш поширений стандарт у всьому світі серед організацій і підприємств, які використовують подібні стандарти на добровільній основі. [4].

До якісних методикам управління ризиками на основі вимог ISO 17999 відносяться методики COBRA і RA Software Tool (Інструмент Програмного Забезпечення). Давайте коротко розглянемо названі методики.

2.2 COBRA

У другій половині 90-х років компанія C & A Systems Security Ltd. розробила однойменні методику і відповідний інструментарій для аналізу та управління інформаційними ризиками під назвою COBRA. Ця методика дозволяє виконати в автоматизованому режимі найпростіший варіант оцінювання інформаційних ризиків будь-якої компанії. Для цього пропонується використовувати спеціальні електронні бази знань і процедури логічного висновку, орієнтовані на вимоги ISO 17799. Істотно, що при бажанні перелік врахованих вимог можна доповнити різними вимогами вітчизняних нормативно-регулюючих органів. [4].

Методика COBRA представляє вимоги стандарту ISO 17799 у вигляді тематичних запитальників (check list's), на які слід відповісти в ході оцінки

ризиків інформаційних активів і електронних бізнес транзакцій компанії. [3].

Далі введені відповіді автоматично обробляються, і за допомогою відповідних правил логічного висновку формується підсумковий звіт с поточними оцінками інформаційних ризиків компанії та рекомендаціями щодо їх управління.

Гідність методики - в її простоті. Необхідно відповісти на кілька десятків питань, потім автоматично формується звіт.

Цей програмний продукт може застосовуватися при проведенні аудиту ІБ або для роботи фахівців служб, відповідальних за забезпечення інформаційної безпеки.

Простота, відповідність міжнародному стандарту, порівняно невелике число питань дозволяють легко адаптувати цей метод для роботи в вітчизняних умовах.

2.3 Кількісні методики управління ризиками

Другу групу методик управління ризиками становлять кількісні методики, актуальність яких обумовлена необхідністю вирішення різних оптимізаційних задач, які часто виникають в реальному житті. Суть цих завдань зводиться до пошуку єдиного оптимального рішення, з безлічі існуючих. Наприклад, необхідно відповісти на наступні питання: «Як, залишаючись в рамках затвердженого річного (квартального) бюджету на інформаційну безпеку, досягти максимального рівня захищеності інформаційних активів компанії?» Або «Яку з альтернатив побудови корпоративного захисту інформації (захищеного WWW сайту або корпоративної Email) вибрати з урахуванням відомих обмежень бізнес ресурсів компанії? »Для вирішення цих завдань і розробляються методи і методики кількісної оцінки і управління ризиками на основі структурних і рідше об'єктно-орієнтованих методів системного аналізу і проектування (SSADM - Structured Systems Analysis and Design). На практиці такі методики управління ризиками дозволяють[4]:

- Створювати моделі інформаційних активів компанії з точки зору безпеки;
- Класифікувати і оцінювати цінності активів;
- Складати списки найбільш значущих загроз і вразливостей безпеки;
- Ранжувати загрози і вразливості безпеки;
- Доводити засоби і заходи контролю ризиків;
- Оцінювати ефективність / вартість різних варіантів захисту;

• Формалізувати і автоматизувати процедури оцінювання та управління ризиками.

Однією з найбільш відомих методик цього класу є методика CRAMM.

2.4 Метод CRAMM

У 1985 році Центральне агентство з комп'ютерів і телекомунікацій (ССТА) Великобританії початок дослідження існуючих методів управління інформаційною безпекою для видачі рекомендацій по їх використанню в урядових організаціях, що обробляють конфіденційну інформацію. Жоден з розглянутих методів не підійшов. Тому спочатку був створений метод, а потім однойменна методика CRAMM (аналізу і контролю ризиків), що відповідає вимогам ССТА. Потім з'явилося кілька версій методики, орієнтованих на вимоги різних державних і комерційних організацій і структур. Одна з версій «комерційного профілю» широко поширилася на ринку засобів захисту інформації. [4].

Також хочу зазначити що методика CRAMM є найстаршою з розглянутих у цій роботі, і інші методики проектувались з оглядом на CRAMM, тому вона розглянута більш детально.

Основними цілями методики CRAMM є[4]:

• Формалізація і автоматизація процедур аналізу та управління ризиками;

• Оптимізація витрат на засоби контролю і захисту;

• Комплексне планування та управління ризиками на всіх стадіях життєвого циклу інформаційних систем;

• Скорочення часу на розробку і супровід корпоративної системи захисту інформації;

• Обгрунтування ефективності пропонованих заходів захисту і засобів контролю;

• Управління змінами та інцидентами;

• Підтримка безперервності бізнесу;

• Оперативне прийняття рішень з питань управління безпекою та ін.

Управління ризиками в методиці CRAMM здійснюється в кілька етапів (рис. 2.1).

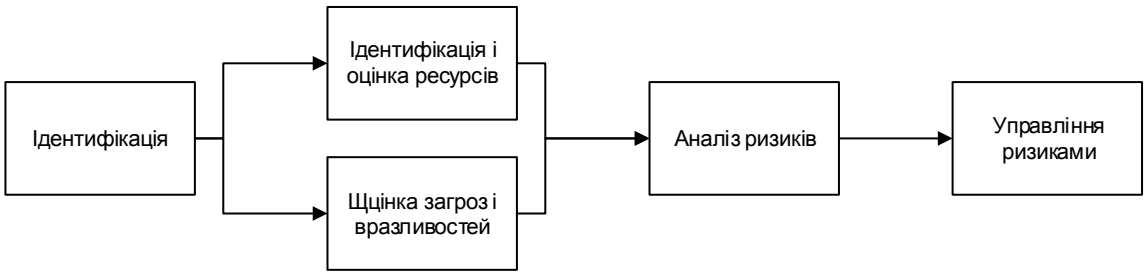

Рисунок 2.1 - Управління ризиками в методиці CRAMM.

На першому етапі ініціації - визначаються межі досліджуваної інформаційної системи компанії, склад і структура її основних інформаційних активів і транзакцій.

На етапі ідентифікації та оцінки ресурсів - чітко ідентифікуються активи, і визначається їх вартість. Розрахунок вартості інформаційних активів однозначно дозволяє визначити необхідність і достатність пропонованих засобів контролю і захисту.

На етапі оцінювання загроз і вразливостей - ідентифікуються і оцінюються загрози і вразливості інформаційних активів компанії.

Етап аналізу ризиків - дозволяє отримати якісні і кількісні оцінки ризиків.

На етапі управління ризиками - пропонуються заходи і засоби зменшення або ухилення від ризику.

Давайте тепер проведемо аналіз ризиків за допомогою методики CRAMM і запропонуємо деякі засоби контролю і управління ризиками, адекватні цілям і задачам бізнесу компанії. [4].

Визначення меж дослідження. Етап починається з рішення задачі визначення меж досліджуваної системи. Для цього збирається така інформація: відповідальні за фізичні і програмні ресурси; хто є користувачем і як користувачі застосовують або використовуватимуть систему; конфігурація системи. Первинна інформація збирається в процесі бесід з менеджерами проектів, менеджером користувачів або іншими співробітниками.

Ідентифікація ресурсів і побудова моделі системи з точки зору ІБ. Проводиться ідентифікація ресурсів: матеріальних, програмних і інформаційних, що містяться всередині кордонів системи. Кожен ресурс необхідно віднести до одного з визначених класів. Класифікація фізичних ресурсів наводиться в додатку. Потім будується модель інформаційної системи з точки зору ІБ. Для кожного інформаційного процесу, що має самостійне значення з точки зору користувача і званого призначеним для користувача сервісом (EndUserService), будується дерево зв'язків

використовуваних ресурсів. У розглянутому прикладі буде єдиний подібний сервіс (рис. 2.2). Побудована модель дозволяє виділити критичні елементи. [4].

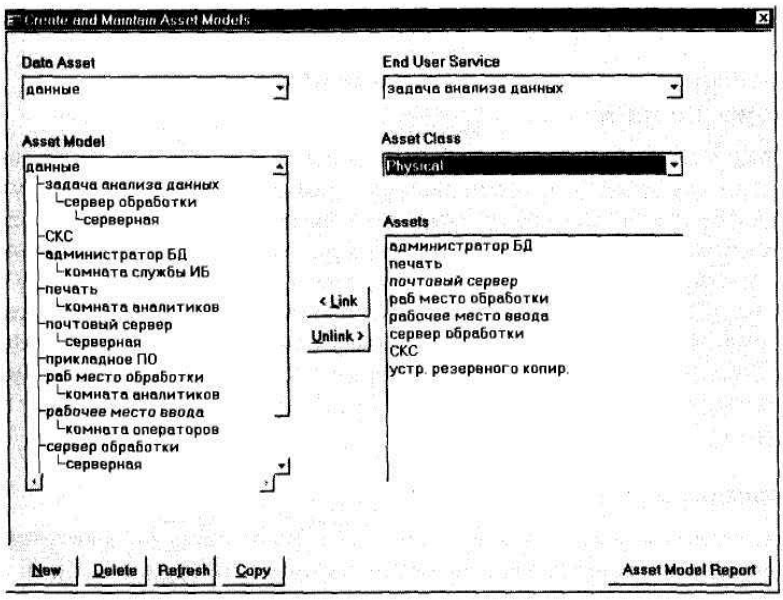

Рисунок 2.2 – Підборний сервіс

Цінність ресурсів. Цінність фізичних ресурсів в даному методі визначається ціною їх відновлення в разі руйнування.

Цінність даних і програмного забезпечення визначається в наступних ситуаціях:

• недоступність ресурсу протягом певного періоду часу;

• руйнування ресурсу - втрата інформації, отриманої з часу останнього резервного копіювання або її повне руйнування;

• порушення конфіденційності у випадках несанкціонованого доступу штатних співробітників або сторонніх осіб;

• модифікація розглядається для випадків дрібних помилок персоналу (помилки введення), програмних помилок, навмисних помилок;

• помилки, пов'язані з передачею інформації: відмова від доставки, недоставляння інформації, доставка по невірному адресою.

Для оцінки можливого збитку пропонується використовувати наступні критерії[4]:

• шкоди репутації організації;

• порушення чинного законодавства;

• збитки для здоров'я персоналу;

• збитки, пов'язані з розголошенням персональних даних окремих осіб;

• фінансові втрати від розголошення інформації;

• фінансові втрати, пов'язані з відновленням ресурсів;

• втрати, пов'язані з неможливістю виконання зобов'язань;

• дезорганізація діяльності.

Наведена сукупність критеріїв використовується в комерційному варіанті методу (профіль Standard). В інших версіях сукупність буде інший, наприклад, у версії, використовуваної в урядових установах, додаються параметри, що відображають такі області, як національна безпека і міжнародні відносини.

Для даних і програмного забезпечення вибираються застосовні до даної ІС критерії, дається оцінка збитку за шкалою зі значеннями від 1 до 10.

Наприклад, якщо дані містять подробиці комерційної конфіденційної (критичною) інформації, експерт, який проводить дослідження, задає питання: як може вплинути на організацію несанкціонованого доступу сторонніх осіб до цієї інформації?

Можливий такий відповідь: провал відразу за кількома параметрами з перерахованих вище, причому кожен аспект варто було б розглянути докладніше і привласнити найвищу з можливих оцінок.

Потім розробляються шкали для обраної системи параметрів. Вони можуть виглядати наступним чином.

Шкоди репутації організації[4]:

• 2 - негативна реакція окремих чиновників, громадських діячів;

• 4 - критика в засобах масової інформації, що не має широкого громадського резонансу;

• 6 - негативна реакція окремих депутатів Верховної Ради України;

• 8 - критика в засобах масової інформації, що має наслідки у вигляді великих скандалів, парламентських слухань, широкомасштабних перевірок і т. П .;

• 10 - негативна реакція на рівні Президента і Уряду.

Збиток для здоров'я персоналу[4]:

• 2 - мінімальний збиток (наслідки не пов'язані з госпіталізацій або тривалим лікуванням);

• 4 - збиток середнього розміру (необхідне лікування для одного або декількох співробітників, але тривалих негативних наслідків немає);

• 6 - серйозні наслідки (тривала госпіталізація, інвалідність одного або декількох співробітників);

- 10 - загибель людей.

Фінансові втрати, пов'язані з відновленням ресурсів[4]:

- 2 - менш $ 1000.;
- 6 - від $ 1000 до $ 10 000;
- 8 - від $ 10 000 до $ 100 000;
- 10 - понад $ 100 000.

Дезорганізація діяльності в зв'язку з недоступністю даних[4]:

- 2 - відсутність доступу до інформації до 5 хвилин;
- 4 - відсутність доступу до інформації до 1 години;
- 6 - відсутність доступу до інформації до 3 годин;
- 8 - відсутність доступу до інформації від 12 годин;
- 10 - відсутність доступу до інформації більше доби.

Далі розглядаються основні сценарії, що призводять до різних негативних наслідків, описуваних в термінах обраних параметрів (рис.2.3 - Оцінка цінності інформаційних ресурсів).

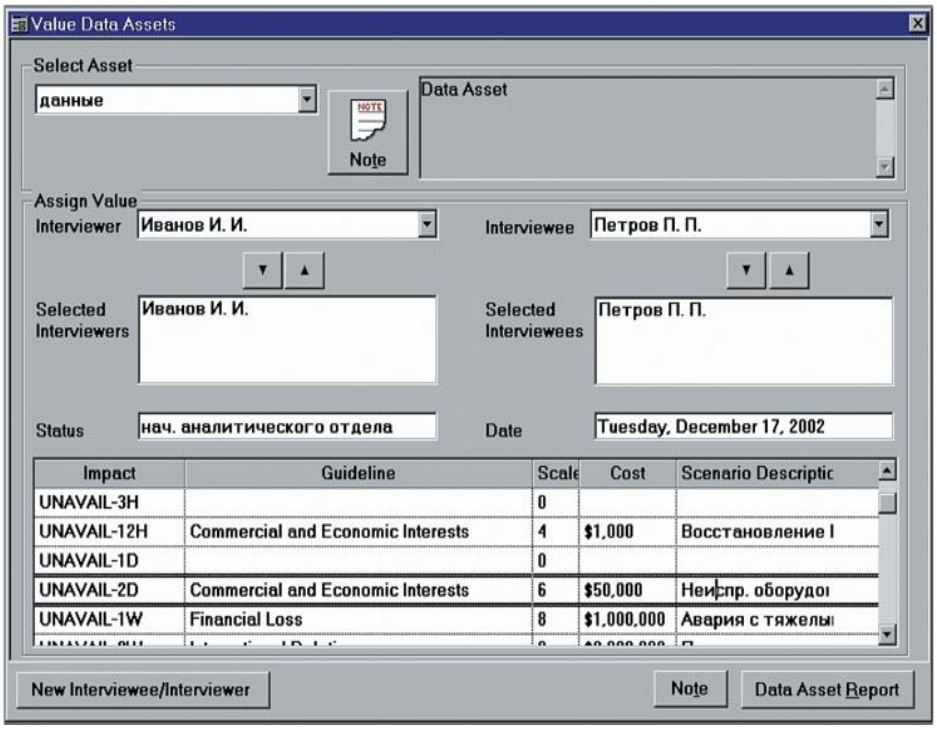

Рисунок 2.3 - Оцінка цінності інформаційних ресурсів.

На цьому етапі може бути підготовлено кілька типів звітів (межі системи, модель, визначення цінності ресурсів). Якщо цінності ресурсів низькі, можна використовувати базовий варіант захисту. В такому випадку

дослідник може перейти від цієї стадії відразу до стадії аналізу ризиків. Однак для адекватного врахування потенційного впливу будь-якої загрози, вразливості або комбінації загроз і вразливостей, які мають високі рівні, слід використовувати скорочену версію стадії оцінки загроз і вразливостей. Це дозволяє розробити більш ефективну систему захисту інформації компанії.

На етапі оцінювання загроз і вразливостей оцінюються залежно призначених для користувача сервісів від певних груп ресурсів і існуючий рівень загроз і вразливостей.

Далі активи компанії групуються з точки зору загроз і вразливостей. Наприклад, у разі наявності загрози пожежі або крадіжки, як група ресурсів розумно розглянути всі ресурси, що знаходяться в одному місці (серверний зал, кімната засобів зв'язку і т. Д.).

Програмне забезпечення CRAMM для кожної групи ресурсів і кожного з 36 типів загроз генерує список питань, що допускають однозначну відповідь. Рівень загроз оцінюється, в залежності від відповідей, як дуже високий, високий, середній, низький і дуже низький. Рівень уразливості оцінюється, в залежності від відповідей, як високий, середній і низький. [4].

На основі цієї інформації розраховуються рівні ризиків в дискретної шкалою з градаціями від 1 до 7. Отримані рівні загроз, вразливостей і ризиків аналізуються і узгоджуються з замовником.

CRAMM об'єднує загрози і вразливості в матриці ризику. Розглянемо, як виходить ця матриця, і що кожен з рівнів ризику означає.

Основний підхід, для вирішення цієї проблеми полягає в розгляді[4].:

• рівня загрози (шкала наведена в табл. 2.1);

• рівня вразливості (шкала наведена в табл. 2.2);

• розміру очікуваних фінансових втрат (приклад на рис. 2.1).

Таблиця 2.1 [4].

Таблиця 2.1 Шкала оцінки рівнів загрози (частота виникнення).	
Описання	Значення
інцидент відбувається в середньому, не частіше, ніж кожні 4 роки	дуже низький
інцидент відбувається в середньому один раз в 2 роки	низький
інцидент відбувається в середньому раз на рік	середній

Продовження таблиці 2.1	
інцидент відбувається в середньому один раз в чотири місяці	високий
інцидент відбувається в середньому раз на місяць	дуже високий

Таблиця 2.2 [3].

Таблиця 2. Шкала оцінки рівня вразливості (ймовірність успішної реалізації загрози).	
Описання	Значення
У разі виникнення інциденту, ймовірність розвитку подій за найгіршим сценарієм менше 0,33	низький
У разі виникнення інциденту, ймовірність розвитку подій за найгіршим сценарієм від 0,33 до 0,66	середній
У разі виникнення інциденту, ймовірність розвитку подій за найгіршим сценарієм вище 0,66	високий

Виходячи з оцінок вартості ресурсів, що захищається ІС, оцінок загроз і вразливостей, визначаються "очікувані річні втрати". На рис.2.4 наведено приклад матриці оцінки очікуваний втрат. У ній другий стовпець зліва містить значення вартості ресурсу, верхній рядок заголовка таблиці - оцінку частоти виникнення загрози протягом року (рівня загрози), нижня рядок заголовка - оцінку ймовірності успіху реалізації загрози (рівня вразливості).

		0.1	0.1	0.1	0.34	0.34	0.34	1	1	1	3.33	3.33	3.33	10	10	10
		0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1
1	1000	1.0E+01	5.0E+01	1.0E+02	3.4E+01	1.7E+02	3.4E+02	1.0E+02	5.0E+02	1.0E+03	3.3E+02	1.7E+03	3.3E+03	5.0E+03	5.0E+03	1.0E+04
2	10000	1.0E+02	5.0E+02	1.0E+03	3.4E+02	1.7E+03	3.4E+03	1.0E+03	5.0E+03	1.0E+04	3.3E+03	1.7E+04	3.3E+04	5.0E+04	5.0E+04	1.0E+05
3	30000	3.0E+02	1.5E+03	3.0E+03	1.0E+03	5.1E+03	1.0E+04	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.0E+04	1.0E+05	1.5E+05	1.5E+05	3.0E+05
4	100000	1.0E+03	5.0E+03	1.0E+04	3.4E+03	1.7E+04	3.4E+04	1.0E+04	5.0E+04	1.0E+05	3.3E+04	1.7E+05	3.3E+05	5.0E+05	5.0E+05	1.0E+06
5	300000	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.1E+04	1.0E+05	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.0E+05	1.0E+06	1.5E+06	1.5E+06	3.0E+06
6	1000000	1.0E+04	5.0E+04	1.0E+05	3.4E+04	1.7E+05	3.4E+05	1.0E+05	5.0E+05	1.0E+06	3.3E+05	1.7E+06	3.3E+06	5.0E+06	5.0E+06	1.0E+07
7	3000000	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.1E+05	1.0E+06	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.0E+06	1.0E+07	1.5E+07	1.5E+07	3.0E+07
8	1E+07	1.0E+05	5.0E+05	1.0E+06	3.4E+05	1.7E+06	3.4E+06	1.0E+06	5.0E+06	1.0E+07	3.3E+06	1.7E+07	3.3E+07	5.0E+07	5.0E+07	1.0E+08
9	3E+07	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.1E+06	1.0E+07	3.0E+06	1.5E+07	3.0E+07	1.0E+07	5.0E+07	1.0E+08	1.5E+08	1.5E+08	3.0E+08
10	1E+08	1.0E+06	5.0E+06	1.0E+07	3.4E+06	1.7E+07	3.4E+07	1.0E+07	5.0E+07	1.0E+08	3.3E+07	1.7E+08	3.3E+08	5.0E+08	5.0E+08	1.0E+09

Рисунок 2.4 - Матриця очікуваних річних втрат.

Значення очікуваних річних втрат (англ. Annual Loss of Expectancy) переводяться в CRAMM в бали, що показують рівень ризику, відповідно до шкали, представленої на рис.2.5 (в цьому прикладі розмір втрат наводиться в фунтах стерлінгів).

CRAMM Measure of Risk	"Annual Loss of Expectancy"
1	<£1,000
2	<£10,000
3	<£100,000
4	<£1,000,000
5	<£10,000,000
6	<£100,000,000
7	<£1,000,000,000

Рисунок 2.5 - Шкала оцінки рівня ризиків.

Відповідно до наведеної нижче матрицею, виводиться оцінка ризику (рис.2.6) рівні ризиків розраховуються в дискретної шкалою з градаціями від 1 до 7 (етап аналізу ризиків). Отримані рівні загроз, вразливостей і ризиків аналізуються і узгоджуються з замовником. Тільки після цього можна переходити до заключної стадії методу.

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln.	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
Asset Value															
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	3	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Рисунок 2.6 - Матриця оцінки ризику.

Третя стадія дослідження полягає в пошуку адекватних контрзаходів. По суті, це пошук варіанту системи безпеки, найкращим чином задовольняє вимогам замовника.

На цьому етапі CRAMM генерує кілька варіантів заходів протидії, адекватних виявленим ризикам і їх рівнями. Контрзаходи розбиваються на групи і підгрупи за наступними категоріями[4]:

- Забезпечення безпеки на мережевому рівні.
- Забезпечення фізичного захисту.
- Забезпечення безпеки підтримуючої інфраструктури.
- Заходи безпеки на рівні системного адміністратора.

В результаті виконання даного етапу формується кілька видів звітів.

Таким чином, розглянута методика аналізу та управління ризиками повністю застосовна і в наших умовах, незважаючи на те, що показники захищеності від несанкціонованого доступу до інформації та вимоги щодо захисту інформації різняться в українських нормативних документах і зарубіжних стандартах. Особливо корисним є використання

інструментальних засобів типу методу CRAMM при проведенні аналізу ризиків інформаційних систем з підвищеними вимогами в області ІБ. Це дозволяє отримувати обгрунтовані оцінки існуючих і допустимих рівнів загроз, вразливостей, ефективності захисту.

CRAMM має засоби генерації звітів, необхідні при проведенні аудиту інформаційної безпеки відповідно до ISO 17799.

Це такі звіти[4]:

- політика інформаційної безпеки;
- система управління інформаційною безпекою;
- план забезпечення безперебійної роботи;
- відомість відповідності.

Метод CRAMM в даний час застосовується найбільш часто, якщо потрібно провести аудит відповідно до вимог Британського стандарту.

Його переваги полягають у використанні технології оцінки загроз і вразливостей за непрямими факторів з можливістю верифікації результатів, зручною системі моделювання інформаційної системи з позиції безпеки, великій базі даних по контрзаходів. Цей метод - самий «потужний» і самий трудомісткий з розглянутих в цьому огляді, він дозволяє досить детально оцінити ризики і різні варіанти контрзаходів.

Його недолік з полягає великому обсязі вихідних документів (сотні сторінок). Аналітик (аудитор) зазвичай змушений на основі отриманих документів сам писати звіт для замовника.

Таким чином, CRAMM - приклад методики розрахунку, при якій первинні оцінки даються на якісному рівні, і потім проводиться перехід до кількісної оцінки (в балах) [4].

2.5 RiskWatch

Інший метод із зарубіжними країнами, RiskWatch, може бути використаний окремо для аналізу фізичних і програмних ризиків. На відміну від CRAMM, даний метод більшою мірою орієнтований на те, щоб ще на етапі проектування тієї чи іншої інформаційної системи врахувати всі загрожують їй ризики. Рекомендації в даному випадку видаються на підставі відомої аксіоми про те, що вартість захисту не повинна перевищувати вартість втрат компанії від реалізації того чи іншого ризику в реальному житті. В даному методі спочатку визначаються категорії захищаються ресурсів, потім описуються можливі втрати і класи

інцидентів. Для цього використовується спеціальний опитувальник, який містить понад шістсот питань, що дозволяють максимально повно і точно описати ризики для інформаційної системи організації. Потім встановлюються зв'язки між ресурсами, втратами і ризиками, на підставі чого проводиться кількісний розрахунок очікуваних втрат і видаються рекомендації по конкретним заходам захисту. Метод дозволяє прораховувати ризики як при відсутності засобів захисту, так і при їх впровадженні, що робить можливим визначення рентабельності впровадження того чи іншого технічного рішення в організації. На жаль, є у RiskWatch і свої недоліки. Перший і найголовніший - це труднощі обліку та кількісного опису адміністративного та організаційного чинника, який часто не менш важливий, ніж технічні засоби захисту від інформаційних ризиків. [4].

2.6 ГРИФ

Альтернативою є розробка російських спеціалістів з інформаційної безпеки, метод ГРИФ. На відміну від статичних CRAMM і RiskWatch, він аналізує рухомі у середині компанії інформаційні потоки, що доповнюється потім вже знайомим нам по двом попереднім методам аналізом загроз і вразливостей. При аналізі інформаційних потоків будується повна модель всієї інформаційної системи організації, що включає в себе всі інформаційні ресурси, їх користувачів і наявні у цих користувачів права доступу, а також засобів захисту ресурсів; на підставі даної інформації потім будується карта зв'язків користувачів і ресурсів в корпоративній інформаційній системі. Далі за допомогою спеціальних опитувальників проводиться визначення адекватності комплексної політики безпеки реальній структурі інформаційної системи, що є відправною точкою для подальшого аналізу в термінах загроз і вразливостей. На даному етапі визначаються загрози і вразливості для кожного з інформаційних ресурсів організації, після чого оновлена модель прораховується за допомогою добре відомих імовірнісних математичних моделей, що потім дає можливість визначити рекомендації для кожного з корпоративних інформаційних ресурсів. До плюсів даної методики, безсумнівно, можна віднести облік «динаміки» у вигляді існуючих всередині організації інформаційних потоків, а також можливість обліку комплексних політик інформаційної безпеки, однак є і свої мінуси, які полягають в помітно меншій базі типових рішень, що може помітно збільшити тривалість і вартість аналізу інформаційних ризиків організації,

а також відсутність достатньої кількості консалтерів, які в повній мірі володіють даною методикою. [4].

2.7. Порівняльна характеристика методик оцінки ризиків.

Таблиця 2.1

Показники порівняння	**CRAMM**	**ГРИФ**	**RiskWatch**	**COBRA**
Ризики				
Використання категорій ризиків	+	+	+	+
Використання поняття максимально допустимого ризику	+	+	+	+
Підготовка плану заходів щодо зниження ризиків	+	+	+	−
Управління				
інформування керівника	+	+	+	+
План робіт по зниженню ризиків	−	+	+	−
Включає проведення тренінгів, семінарів, зборів	−	+	+	−
Оцінка бізнес-ризиків / операційних ризиків / IT-ризиків	−	+	+	+
Оцінка ризиків на організаційному рівні	+	+	−	+
Оцінка ризиків на технічному рівні	+	+	+	+
Пропоновані способи зниження ризиків				
Обхід (виняток) ризику	−	+	+	−
зниження ризику	+	+	+	+
прийняття ризику	−	+	−	+
Процеси використання елементів ризику				
Матеріальні активи	+	+	+	+
Нематеріальні активи	+	+	+	+
Загрози	+	+	+	+
цінність активів	+	+	+	+
Уразливості	+	+	+	+
Заходи безпеки	+	+	+	−
потенційний збиток	+	+	+	+
Матеріальні активи	+	+	+	+
Розглядаємі типи ризиків				
Бізнес-ризики	−	+	+	+
Ризики, пов'язані з порушенням законодавчих актів	−	+	−	−
Ризики, пов'язані з використанням технологій	−	+	−	+
комерційні ризики	+	+	+	+
Ризики, пов'язані з залученням третіх осіб	+	+	+	+
Ризики, пов'язані з залученням персоналу	+	+	−	+

Продовження таблиці 2.1				
Повторні оцінки ризиків	−	+	+	−
Визначення правил прийняття ризиків	−	+	−	−
Способи вимірювання величин ризиків				
якісна оцінка	+	+	+	+
кількісна оцінка	−	+	+	−
Способи управління				
Якісне ранжування ризиків	+	+	+	+
Кількісне ранжирування ризиків	−	+	+	−
Використання незалежної оцінки	−	+	−	+
Розрахунок повернення інвестицій	−	+	−	−
Розрахунок оптимального балансу між різними типами заходів безпеки, такими як:				
заходи запобігання	−	+	+	−
заходи виявлення	−	+	+	−
Заходи щодо виправлення	−	+	+	−
Заходи по відновленню	−	+	+	−
Інтеграція способів управління	−	+	−	−
Опис призначення способів управління	−	+	+	+
Процедура прийняття остаточних ризиків	+	+	−	−
Управління залишковими ризиками	−	+	−	−
Моніторинг ризиків	−	+	+	+
Застосування моніторингу ефективності заходів ІБ	−	+	+	−
Проведення заходів щодо зниження ризиків	−	−	+	+
Використання процесу реагування на інциденти в області ІБ	−	+	−	−
Структуроване документування результатів оцінок ризиків	−	+	+	−

Оцінка CRAMM

Дана методика не враховує супровідної документації, такої як описання бізнес-процесів або звітів по проведеним оцінками ризиків. Відносно стратегії роботи з ризиками CRAMM передбачає використання тільки методів їх зниження. Такі методи управління ризиками, як обхід або прийняття, чи не розглядаються. У методиці відсутні: процес інтеграції способів управління і опис призначення того чи іншого способу; моніторинг ефективності використовуваних способів управління і способів управління залишковими ризиками; перерахунок максимально допустимих величин ризиків; процес реагування на інциденти.

Практичне застосування CRAMM пов'язане з необхідністю залучення фахівців високої кваліфікації; трудомісткістю і тривалістю процесу оцінюки ризиків. Крім того, слід зазначити високу вартість ліцензії. [12].

Оцінка ГРИФ

Методика ГРИФ використовує кількісні і якісні методи оцінки ризиків, а також визначає умови, при яких останні можуть бути прийняті компанією, включає в себе розрахунок повернення інвестицій на впровадження заходів безпеки. На відміну від інших методик аналізу ризиків, ГРИФ пропонує всі способи зниження ризиків (обхід, зниження і прийняття). Дана методика враховує супровідну документацію, таку як опис бізнес-процесів або звітів по проведеним оцінками ризиків ІБ. [12].

Оцінка RiskWatch

Ця методика використовує кількісні і якісні методи оцінки ризиків. Трудомісткість робіт з аналізу ризиків з використанням цього методу порівняльно невелика. Такий метод підходить, якщо потрібно провести аналіз ризиків на програмно-технічному рівні захисту без урахування організаційних і адміністративних чинників. Істотним достоїнством RiskWatch є інтуїтивно зрозумілий інтерфейс і велика гнучкість методу, що забезпечується можливістю введення нових категорій, описів, питань і т. д. [12].

Оцінка COBRA

COBRA не передбачає такого ефективного заходу з управління ризиками, як «Програма підвищення інформованості співробітників в області інформаційної безпеки». Така програма дозволяє знизити ризики ІБ, пов'язані з порушеннями режиму інформаційної безпеки співробітниками компанії через їх необізнаність щодо корпоративних вимог в цій області і правил безпечного використання інформаційних систем. Також в COBRA не передбачена періодичність проведення оцінки ризиків та оновлення їх величин, що свідчить про те, що методика придатна для виконання разових оцінок і не годиться для регулярного використання.

Позитивною стороною COBRA є те, що програмний продукт, реалізуючий цю методику, поширюється безкоштовно і не вимагає значних ресурсів для установки і застосування [12].

Висновок до розділу

Розглянуті методики добре відповідають вимогам груп «Ризики» і «Процеси (Використання елементів ризику)», але деякі з них (CRAMM, COBRA) мають недоліки у відповідності до розділів «Моніторинг» і «Управління», а також з багатьма підрозділами «Процеси» . Мало хто (ГРИФ, RiskWatch,) дають докладні рекомендації з приводу складання розкладу проведення повторних оцінок ризиків.

У тих випадках, коли потрібно виконати тільки разову оцінку рівня ризиків в компанії середнього розміру, доцільно рекомендувати використання методики COBRA. Для управління ризиками на базі періодичних оцінок на технічному рівні найкраще підходить CRAMM. Методики ГРИФ і RiskWatch кращі для використання у великих компаніях, де імовірність впровадження управління ризиками (ІБ) на базі регулярних оцінок, на рівні не нижче організаційного, і потрібна розробка обґрунтованого плану заходів щодо їх зниження.

3. Блок оцінки ризиків

Ця частина роботи передбачає розробку програмного продукту, що дозволяє підібрати максимально підходящу методику оцінки ризиків, для обраного підприємства, з обраними особливостями проведення оцінки ризиків. Вид підприємства а також особливості проведення оцінки ризиків, встановлює сам замовник проходячи простий тест. На основі тесту програма визначає підходящу методику оцінки.

Ідентифікація підприємства виконується згідно з ст.6. Господарського кодексу України «Загальні принципи господарювання». Згідно з статтею було розроблено тестові питання класифікуючи підприємства згідно ГКУ.

Ідентифікація потреб замовника а також його фінансова спроможність, визначається методом подібним до ідентифікації підприємства. Розроблено тестові питання за допомогою яких замовник може обрати потрібну, як на його розсуд, оцінку інформаційних ризиків.

Згідно аналізу проведеного у таблиці Таблиці 2.1, найбільш універсальною є програма ГРИФ, тому їй назначена найвища кількість балів, відповідно були назначені кількості балів для інших методик.

Кожен варіант відповідей має свій коефіцієнт, сума цих коефіцієнтів відповідає методикам оцінки інформаційних ризиків (таблиця 3.1).

Таблиця 3.1 - Кількості балів програмних методик

Методики	Бали
1. ГРИФ	76 - 90
2. RiskWatch	61 - 75
3. CRAMM	46 - 60
4.COBRA	31 – 45
5.CORAS	16 – 30
6.MSAT	1 – 15

Програмний продукт відповідно до результату тесту замовника, пропонує найбільш підходящу систему оцінки ризиків, яка краще за інших підходитиме типу підприємства і потребам замовника.

3.1 Алгоритм роботи програми

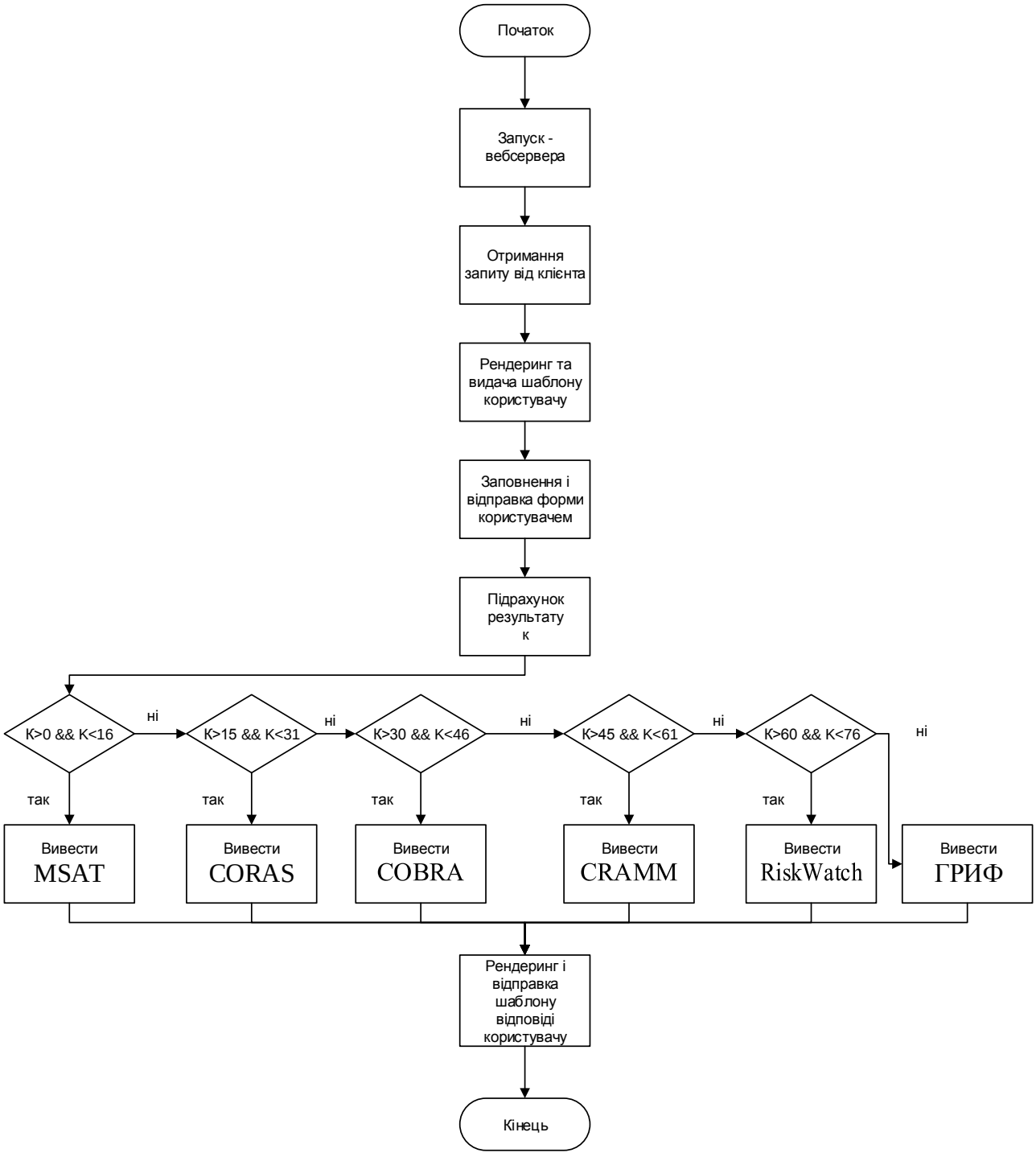

Рисунок 3.1 – Алгоритм роботи програми

3.2 Проектування

3.2.1 Вибір мови програмування

Згідно ТЗ, в даному курсовому проекті буде використовуватися мова програмування Python 3.

Python 3. - високорівнева мова програмування загального призначення, орієнтований на підвищення продуктивності розробника і читання коду. Синтаксис ядра Python мінімалістичний. У той же час стандартна бібліотека включає великий обсяг корисних функцій, таких як:

Math - стандратний модуль, що дозволяє проводити розширені арифметичні операції над змінними.

Time - стандартний модуль, що дозволяє працювати програмі з тимчасовими значеннями.

Fractions - модуль, що дозволяє проводити операції над раціональними числами, в тому числі пошук найбільшого загального дільника.

Numpy - модуль, що полегшує роботу з простими числами.

3.2.2 Вибір середовища розробки

При написанні програми буде використане середовище розробки PyCharm 2016.3 Professional, яка дозволяє писати програми на мові Python 3. PyCharm - це інтегроване середовище розробки для мови програмування Python. Надає засоби для аналізу коду, графічний відладчик, інструмент для запуску юніт-тестів і підтримує веб-розробку на Django. PyCharm розроблена компанією JetBrains на основі IntelliJ IDEA.

можливості:

• Статичний аналіз коду, підсвічування синтаксису і помилок.

• Навігація по проекту і вихідного коду: відображення файлової структури проекту, швидкий перехід між файлами, класами, методами і використаннями методів.

• Рефакторинг: перейменування, вилучення методу, введення змінної, введення константи, підйом і спуск методу і т. Д.

• Інструменти для веб-розробки з використанням фреймворку Django

• Вбудований відладчик для Python

• Вбудовані інструменти для юніт-тестування

• Розробка з використанням Google App Engine

• Підтримка систем контролю версій: загальний користувальницький інтерфейс для Mercurial, Git, Subversion, Perforce і CVS з підтримкою списків змін і злиття.

В проекті буде використовуватися інтерфейс програмування додатків PyQt 5.

PyQt5 - це набір Python бібліотек для створення графічного інтерфейсу на базі платформи Qt5 від компанії Digia.і Він доступний для Python 2.x і 3.x.

Бібліотека Qt є однією з найпотужніших бібліотек GUI (графічного інтерфейсу користувача).

PyQt5 реалізований у вигляді набору python-модулів. Ця бібліотека має понад 620 класів і 6000 функцій і методів.

Це мультиплатформенна бібліотека, яка працює на всіх основних операційних системах, в тому числі Unix, Windows і Mac OS.

3.3 Розробка

3.3.1 Вибір системної архітектури

Системна архітектура додатка визначає, як взаємодіють елементи програми та які функції вони надають. Існують три типи системної архітектури: одноріvнева, дворівнева і багаторівнева. Багаторівневі додатки. Багаторівневі додатки реалізуються розподілом по безлічі комп'ютерів в мережі. Додатки цього типу називають також розподіленими або n-рівневим. Подібне додаток є особливим випадком трирівневого, у якого один і більше рівнів розбивається на додаткові рівні, що забезпечує більш високу масштабованість додатки. У багаторівневих додатках презентаційний сервіс, прикладна логіка, і сервіс даних відокремлені один від одного. Однак рівнів може бути не три, а більше. Логічні рівні не обов'язково повинні відповідати їх фізичному місцезнаходженням в мережі. У багаторівневому додатку клієнту надається тільки для користувача інтерфейс. Прикладна логіка реалізується проміжним рівнем, який розміщується між призначеним для користувача інтерфейсом і системою зберігання даних. Це і дозволяє виділяти кожен тип сервісу в окремий рівень. Перевага такої моделі в тому, що прикладна логіка зосереджена в одному місці і може бути легко модифікована. Презентаційний рівень відповідає фактично тільки за взаємодію з користувачем. У багаторівневому додатку покупець не звертається до системи зберігання даних безпосередньо. Поділ всіх сервісів дозволяє модифікувати будь-який рівень системи, не вносячи зміни в інші.

Одноріvнева архітектура - архітектура, що підтримує як призначений для користувача інтерфейс, так і прикладну логіку. До останньої належать різноманітні математичні функції: перевірка, правопису та ін. На тому ж рівні містяться і підпрограми, які забезпечують збереження і доступ до файлів даних. Одноріvнева системна архітектура не передбачає поділ на рівні.

Дворівнева архітектура - архітектура, що підтримує як призначений для користувача інтерфейс, так і прикладну логіку, які при цьому реалізовані на різних рівнях.

Для трирівневої архітектури характерна наявність призначеного для користувача інтерфейсу, реалізації рішення задачі, бази даних. Даний тип архітектури застосовується в програмному забезпеченні, яке здійснює роботу, з будь-якою базою даних.
Проаналізувавши види систем архітектури, найкращим рішенням є вибір дворівневої архітектури для програми так як програма повинна реалізовувати підрахунок результату і взаємодіяти з користувачем через веб-інтерфейс.

3.3.2 Діаграма прецедентів

Діаграма прецедентів (англ. Use case diagram, діаграма варіантів використання) в UML - діаграма, що відображає відносини між акторами і прецедентами і є складовою частиною моделі прецедентів, що дозволяє описати систему на концептуальному рівні.

Прецедент - можливість модельованої системи (частина її функціональності), завдяки якій користувач може отримати конкретний, вимірний і потрібний йому результат. Прецедент відповідає окремому сервісу системи, визначає один з варіантів її використання і описує типовий спосіб взаємодії користувача з системою. Варіанти використання зазвичай застосовуються для специфікації зовнішніх вимог до системи.

Відповідно до завдання на курсовий проект була побудована UML діаграма прецедентів рисунок 3.1.

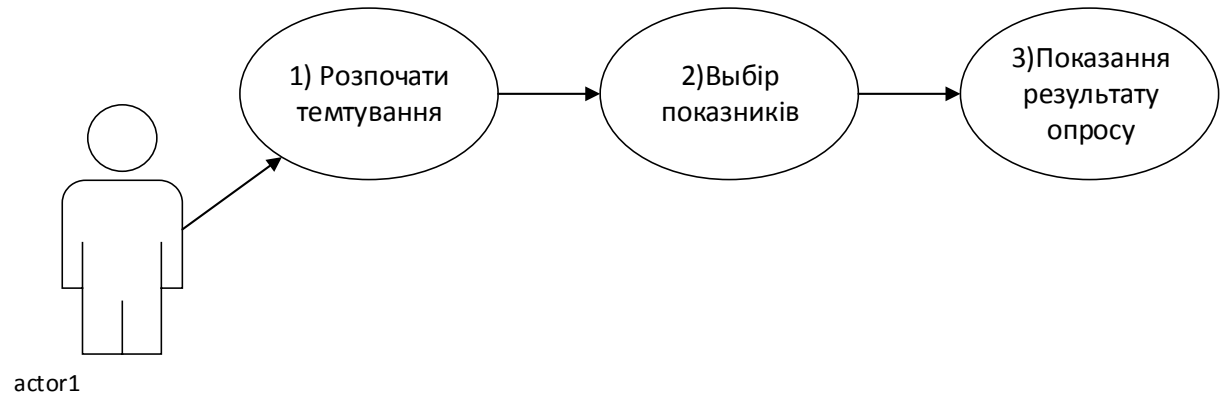

Рисунок 3.1-UML діаграма прецедентів

1) Користувач розпочинає проходження тесту.

2) В ході тестування користувач вибирає показники які підходять його випадку.

3) На основі показників вибраних клієнтом, видається результат опитування у вигляді назви методики.

3.4 Тестування і верифікація

Верифікація – це процес засвідчення, що програми та їх компоненти відповідають технічному завданню. Метод верифікації є засвідченням того, програмне забезпечення відповідає висунутим вимогам, у свою чергу тестування програмного забезпечення – це процес відповідності між реальною і очікуваною поведінкою програми що здійснюється на кінцевому наборі тестів. Результати тестування представлені в таблиці 3.1.

Таблиця 3.2 –Тестування програми

№	Призначення тесту	Очікуваний результат	Отриманий результат	Коментар
1	Зчитування тесту із файлу	Відображення тесту на веб-сторінці	Тест відобразився на веб-сторінці	Тест пройдено
2	Аналіз результату тестування і видання висновку	Отримання типу методики	Отримано методику	Тест пройдено
3	Аналіз коректності результату роботи програми	Результатом повинна бути методика відповідна до суми коефіцієнтів відповідей	Методика коректна	Тест пройдено

4.ЕКОНОМІЧНА ЧАСТИНА

4.1 Мета економічної частини

Мета економічної частини дипломного проекту бакалавра – розрахунок собівартості та економічне обґрунтування розробки засобу для порівнювального аналізу алгоритмів шифрування.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

1. Розрахунок трудомісткості проектування системи;

2. Розрахунок заробітної плати реалізаторів проект;

3. Розрахунок собівартості проекту;

4. Скласти кошторис витрат на розробку проекту.

4.2 Розробка переліку робіт з розробки програмного забезпечення

В даному підрозділі необхідно скласти перелік робіт для розробки програмного засобу аналізу методик оцінки ризиків розрахувати тривалість і трудомісткість робіт. Для проектування програмного засобу необхідний 1 програміст.

Під час обчислення тривалості тривалість окремого етапу визначається таким співвідношенням:

$$\mathrm{T} = \frac{t}{n}$$

де T - тривалість етапу, визначається у робочих днях, округляється до цілого;

t - трудомісткість етапу (людино-дні);

n - кількість виконавців, зайнятих одночасно виконанням етапів.

Результати розрахунку трудомісткості наведені у таблиці 4.1.

Таблиця 4.1- Перелік робіт і трудомісткість проектування систем

№ п/п	Етапи	Тривалість[дн]	Трудомісткість [людино-дні]	Посада	
				Аналітик захисту інформації	Програміст
1. Розробка ТЗ і постанова задачі					
1.1	Аналіз науково - технічної інформації	4	4	+	-
1.2	Формулювання завдання	1	1	+	-
1.3	Розробка технічного завдання	1	1	+	-
1.4	Розробка технічної моделі	2	2	-	+
2. Система проектування					
2.1	Розробка архітектури програми	4	4	-	+
2.2	Деталізація архітектури програми	5	5	-	+
2.3	Тестування	4	8	+	+
2.4	Обробка отриманих результатів	7	7	+	-
3. Підготовка та презентація результатів					
3.1.	Оформлення отриманих результатів	7	7	+	-
4. Впровадження результатів					
4.1	Здача в експлуатацію	1	2	+	+
Усього:		33	38	22	16

Для розробки програмного засобу аналізу систем оцінки ризиків аналітику потрібно 22 дні, а програмісту потрібно 16 дні.

Для проектування системи потрібен програміст, чия заробітна плата складає 7 854 грн.-міс та аналітика, чия зарплата складає 10 142 грн.-міс (таблиця 4.2).

Таблиця 4.2 Середня місячна зарплата і щоденні заробітні плати

№ п/п	Посада	Щомісячна ЗП, грн.	Щоденна ЗП, грн.
1	Аналітик	10 142	461
2	Програміст	7 854	357

Судячи із розрахунків щоденна заробітна плата аналітика складає 461 грн - день, а програміста 357 грн - день.

Зарплата аналітика систем та програміста складається з основної та додаткової заробітних плат.

Фонд основної заробітної плати визначається за формулою:

$$ЗП_{ОС} = ЗП_{АС} * Т_{АС} + ЗП_{П} * Т_{П} \quad (4.1)$$

Де $Т_{АС}$, $Т_{П}$ - трудомісткість роботи аналітика системи та програміста.

$ЗП_{АС}$, $ЗП_{П}$ - Щоденна середня заробітна плата аналітика системи та програміста:

Звідси

$$ЗП_{ОС} = 461*22 + 357*16 = 15\ 854 \text{ ГРН} \quad (4.2)$$

Для розрахунку додаткової заробітної плати ($ЗП_{ДОП}$), яка включає в себе доплату до додаткового робочого дня, премії, тощо., становить 15% від базової зарплати. Таким чином:

$$ЗП_{ДОП} = ЗП_{ОС} * \frac{Н_{ДОП}}{100} = 2\ 378 \text{ ГРН.} \quad (4.3)$$

Загальний фонд заробітної плати ($Ф_{ЗП}$) підраховується наступним чином:

$$Ф_{ЗП} = ЗП_{ОС} + ЗП_{ДОП} = 18\ 232 \text{ ГРН.} \quad (4.4)$$

Нарахування заробітної плати у відсотках від основної і додаткової заробітних плат (єдиний соціальний внесок) складає 22%.

$$З_{СОЦ} = Ф_{ЗП} * \frac{Н_{СОЦ}}{100} = 4\ 011 \text{ ГРН.} \quad (4.5)$$

Таблиця 4.3 представляє вартість матеріалів.

Таблиця 4.3-Вартість матеріалів

№ п/п	Матеріал	Призначення	Кількість, шт	Ціна за од., грн	Сума, грн
1	Флеш-накоплювач Kingston DataTraveler SE9 32GB (DTSE9H/32GB)	Зберігання інформації	1	399	399
2	Заправка картриджа	Друк документації	1	120	120
3	Папір офісний Папір Data Copy A4 80 г/м2 500 аркушів біла	Друк документації	1	104	104
4	Python 3.6.1	Написання програми	1	0	0
	Усього:	623 грн			

Таблиця 4.4 представляє вартість основних засобів.

Таблиця 4.4 - Основні засоби

№ п/п	Матеріал	Призначення	Кількість, шт	Ціна за од., грн	Сума, грн
1	Персональный компьютер Everest Home & Office 1020	Робота працівника	2	5 561	11 122
2	Монитор 18.5" Philips 193V5LSB2	Робота працівника	2	1 999	3998
3	Миш Logitech M90 USB	Робота працівника	2	169	338
4	Клавіатура Trust ClassicLine Multimedia USB (21200)	Робота працівника	2	299	598
5	Друкар HP DeskJet Ink Advantage 3775	Друк документації	1	1 733	1 733
6	Комп’ютерний стіл	Робота працівника	2	549	1 098
7	Комп’ютерний стілець	Робота працівника	2	370	740
8	Офісний пакет Microsoft Office	Оформлення документації,презентації , розрахунку витрат	1	2799	2799
Усього:		22 420 грн			

Таким чином, вартість матеріалів ($ОЗ_м$) для проектування системи складає 22 420 грн.

Щорічна норма амортизаційних відрахувань ($А_М$) розраховується за формулою 5.6:

$$Am = \frac{ОЗ_М * Н_А * N_{роб}}{100\% * N_{річ}} \quad (4.6)$$

де $ОЗ_М$ – вартість основних засобів, $Н_А$– відсоток річної норми амортизації, $N_{роб}$ – кількість витрачених робочих днів, $N_{річ}$– кількість робочих днів в році.

Тривалість проекту – 38 днів, загальна кількість робочих днів у 2017 році – 249 днів.

$$Am = \frac{22420 * 22\% * 33}{100\% * 249} = 855 \text{ ГРН} \quad (4.7)$$

Нарахування інших витрат у відсотках становить 40% від вартості основних засобів ($ЗП_{ОС}$) і складає $ЗП_{ОС}$ * 36% = 6 341 ГРН.

4.3 Собівартість проектування системи

Собівартість розробки буде дорівнювати сумі всіх вищезазначених витрат.

Враховуючи все вище зроблені підрахунки, зведена таблиця основних витрат на розробку системи буде виглядати наступним чином:

Таблиця 4.5 - Собівартість проектування системи

Стаття	Вартість, ГРН	Призначення
1. Основна заробітна плата	15 854	$ЗП_{ОС} = \Sigma N_i * ЗП_{ср}$
2. Додаткова заробітня плата	2 378	15% від $ЗП_{ОС}$
3. Єдиний соціальний внесок	4 011	22% від ($ЗП_{ОС}$+$ЗП_{ДОД}$)
4. Вартість матеріалів	623	см.табл.5.3
5.Амортизаційні відрахування	855	ОС(Таб.5.4)*25%*(кільк. робоч. днів) / (кільк. робоч. днів у році (249))*100%

Продовження таблиці **4.**5		
6. Інші витрати	6 341	40% від $ЗП_{ОС}$
7. Собівартість розробки	54 486	п.1+п.2+п.3+….п6

Так як програмний засіб являє собою ознайомлювальний продукт для досліджень, то прибуток від системи підраховувати недоцільно.

5. Висновки до розділу

В ході розрахунку економічної складової проекту була отримана собівартість, яка склала 54 486 грн. Розрахунки були зроблені з урахуванням всіх витрат, відрахувань до соціального фонду, урахуванням витрат на матеріали та інші витрати на оренду приміщення, електроенергію і оплату послуг інтернету. В ході виконання було розраховано: основну заробітну плату, яка склала 15 854 грн; додаткову заробітну плату, яка склала 2 378 грн, відрахування в єдиний соціальний фонд, які склали 4 011 грн, витрати на матеріали, які склали 623 грн, , амортизаційні відрахування, які склали 855 грн та інші витрати, які склали 6 341 грн.

Для зниження витрат, можливо запропонувати наступні рішення. Як видно найбільші витрати були зроблені на заробітну плату програміста та аналітика. Зниження цих витрат, можливо покращенням праці аналітика шляхом покращення зручності місця праці та покращенням ефективності програміста шляхом використання більш сучасних ЕВМ для роботи.

Висновок

Метою дипломної роботи бакалавра, було дослідження методик оцінки ризиків інформаційної безпеки.

В ході проведення аналізу методик оцінки ризиків, були виявлені їх недоліки і переваги. Серед переваг, слід зазначити можливість використання деяких методик не досвідченними користувачами, та можливість відмови від експертних оцінок, оскільки експертні оцінки вже додані у програму реалізацію, що дає можливіть залучити більш досвідчених експертів. Аналіз показав, що деякі методики мають погану програмну реалізацію. Адже саме програмна реалізація є найбільш прийнятною для користувача, оскільки такі методики найбільш легко використовувати. Саме тому був розроблений блок аналізу ризиків, який дозволяє не тільки обрати методику оцінки ризиків, а і її найбільш доцільну програмну реалізацію.

Список використаної літератури

1. Розробка моделі оцінки ризиків інформаційної безпеки корпоративної мережи [Електронний ресурс] Режим доступу: http://bibliofond.ru/view.aspx?id=552378

2.Засоби захисту інформації [Електронний ресурс] Режим доступу: http://cyclowiki.org/wiki/

3. Інформаційні технології в економіці. Автори: Моісеєнко Є.В., Лаврушина Є.Г. [Електронний ресурс] Режим доступу: https://abc.vvsu.ru/books/inform_tehnolog/page0025.asp

4. Лекційний матеріал по предмету "Управління інформаційною безпекою" лектор Цуранов М.В. [Електронний ресурс] Режим доступу: https://drive.google.com/drive/folders/0B_nqyQA3OP98LTdUS3ZMeHdGSTA

5. Наукова бібліотека [Електронний ресурс] Режим доступу: http://sernam.ru/ss_42.php

6. «Аналізуємо ризики власними силами». Автори: Медведовський И., Куканова Н. [Електронний ресурс] Режим доступу: https://dsec.ru/ipm-research-center/article/analyze_the_risks_by_own_forces/

7. «Системи управління інформаційної безпеки. Вимоги» ISO /I EC 27001 друге видання 2005. – 28 с.

8.«Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки» ISO / IEC 27005 друге видання 2011. - 94с.

9. Методи оцінки ризиків [Електронний ресурс] Режим доступу: http://metrology.com.ua/risk-menedzhment/metody-otsenki-riska

10. «Методи оцінки ризиків» ГОСТ Р ИСО/МЭК 31010 – 2011. – 74 с.

11. Блог про інформаційну безпеку [Електронний ресурс] Режим доступу: http://securityinform.blogspot.com/2013/10/blog-post_10.html

12. Методики аналізу оцінки ризиків інформаційної безпеки [Електронний ресурс] Режим доступу: http://cyberleninka.ru/article/n/metodiki-analiza-i-otsenki-riskov-informatsionnoy-bezopasnosti.pdf.

Додаток А. Технічне завдання

1. Введення

1.1Найменування роботи і підстави для виконання роботи

Проведеної по справжньому технічним завданням роботі присвоюється найменування: «Програмний підбір методик оцінки ризиків для підприємства»(далі по тексту – програма).

1.2 Коротка характеристика області застосування

Дана програма призначена для підбору найбільш підходящої методики оцінки ризиків, для конкретного підприємства з індивідуальними потребами в оцінці ризиків.

2. Підстави для розробки

2.1 Підстава для проведення розробки

Підставою для проведення розробки є завдання на дипломний проект бакалавра кафедри «Комп'ютерні системи і мережі» Національного аерокосмічного університету ім. Н.Є. Жуковського «Харківський авіаційний інститут» на тему «Системи захисту інформації з детальною розробкою блоку оцінки ризиків».

2.2 Найменування та умовне позначення теми розробки

Найменування теми розробки «Системи захисту інформації з детальною розробкою блоку оцінки ризиків»

Умовне позначення теми розробки (шифр теми) – «СЗІ РБОР».

3.Призначення розробки

3.1 Функціональне призначення розробки

Основним призначенням програми є ініціалізація тесту, підрахунок результату, виведення назви методики оцінки ризиків згідно результату тесту.

Розробляється програма для полегшення процесу визначення з застосуванням методик оцінки ризиків.

3.2 Експлуатаційне призначення

Програма призначена для експлуатації як на ПК так і на інших пристроях маючих можливість доступу до мережі Інтернет.

Для роботи з програмою потрібен браузер.

4. Вимоги до програми або програмного виробу

4.1 Вимоги до функціональних характеристик

4.1.1 Вимоги до складу виконуваних функцій

Програма повинна виконувати наступні функції:

- завантаження тесту з файлу;
- ініціалізація тесту;
- підрахунок балів тесту;
- Визначення результату.

4.1.2 Вимоги до організації вхідних даних

Вхідні данні не передбачені розробкою.

4.1.3 Вимоги до організаційних даних

Вхідні данні не передбачені розробкою.

4.1.4 Вимоги до тимчасових характеристик

Вимоги не пред’являються.

4.2 Вимоги до надійності

система повинна зберігати працездатність і забезпечити відновлення своїх функцій при виникненні наступних позаштатних ситуацій:

- при перебоях в системі електропостачання апаратної частини що призводять до перезавантаження ОС, відновлення програми має відбуватися після перезапуску ОС;
- при помилках в роботі апаратних засобів (крім носіїв даних і програм) відновлення функції системи покладається на ОС;
- при помилках пов’язаних с програмним забезпеченням (ОС і драйвери пристроїв), Відновлення працездатності покладається на ОС.
- для захисту апаратури від кидків напруги і комунікаційних перешкод повинні застосовуватися мережеві фільтри.

4.2.1 Забезпечення сталого функціонування програми

Стійке функціонування програми має бути забезпечене виконанням замовником сукупності організаційно-технічних заходів, перелік яких наведений нижче:

- організацією безперебійного живлення технічних засобів;

- використанням ліцензійного програмного забезпечення;
- регулярним виконанням вимог нормативних документів. Що стосуються захисту інформації шляхом випробування програмних засобів на наявність комп’ютерних вірусів;

- доступ до мережі Інтернет.

4.2.2 Відмови через некоректні дії оператора

Відмови програми можливі внаслідок некоректних дій користувача при взаємодії з ОС. Щоб уникнути виникнення відмов програми за вказаною вище причини слід забезпечити роботу кінцевого користувача без надання йому адміністративних привілеїв.

4.3 Умови експлуатації

4.3.1 Кліматичні умови експлуатації

Кліматичні умови експлуатації, при яких повинні забезпечуватися задані характеристики програми, повинні задовольняти вимогам, що пред’явлені до технічних засобів в частині умов їх експлуатації.

Програма призначена для користування на ПК і інших пристроях маючих доступ до мережі Інтернет.

4.3.2 Вимоги до видів обслуговування

Для використання програми необхідна наявність на комп’ютері браузера і доступу до мережі Інтернет.

4.3.3 Вимоги до чисельності та кваліфікації персоналу

Для експлуатації програми визначені наступні ролі – користувач. Для роботі з програмою потрібні базові знання для роботи з комп’ютером.

4.4 Вимоги до складу і параметрів технічних засобів

Технічне забезпечення системи повинно максимально забезпечувати технічні засоби. Вимоги до технічних характеристик ПК системного адміністратора і адміністратора баз даних:

- процесор з тактовою частотою не менш 1.5 ГГц;
- обсяг оперативної пам’яті – не менше 2 Гб:
- вільного дискового простору для зберігання програми не менше 1 Мб;
- дисплей і відеоадаптер будь-якого типу;
- клавіатуру і мишу.

4.5 Вимоги до програмної та інформаційної сумісності

4.5.1 Вимоги до інформаційних структур і методів розв’язання

Не пред’являються.

4.5.2 Вимоги до вихідного коду і мов програмування

Для розробки програми в якості мови програмування потрібно використовувати мову Python. Для проектування необхідно використовувати середовище розробки Edit with IDLE 3.6 і вище.

4.5.3 Вимоги до програмних засобів, які використовуються програмно

Програма повинна бути здатна виконуватися під керуванням ОС Windows 7 і вище, і інших систем з наявністю браузеру и виходу до мережі Інтернет. Системні програмні засоби, що використовуються програмою повинні бути представлені ліцензійної локалізованої версією ОС. Допускається використання відповідного пакета оновлень. Параметри ОС налаштовані таким чином, щоб виконання програми було можливим.

4.5.4 Вимоги до захисту інформації та програм

Програма використовує конфіденційні данні користувача, захист цих даних покладається на самого користувача.

4.6 Спеціальні вимоги

Робота з програмою здійснюється за наявності підключення до мережі Інтернет.

5. Вимоги до маркування та упаковки

5.1 Вимога до маркування

Диск, із записаною на ньому програмою, повинен мати маркування з найменуванням продукту, номера версії, порядкового номера, дати розробки. Маркування повинне бути нанесене на диск у вигляді наклейки виконаної поліграфічним способом з урахуванням вимог ГОСТ 9181-74.

5.2 Вимоги до упаковки

Упаковка диска з програмою повинна здійснюватися у пакувальну тару підприємства-виготовлювача, що представляє собою жорсткий футляр для DVD-дисків. Упаковка програмного виробу повинна проводитись в закритих приміщеннях при температурі від +15 до +40° С і відносній вологості не більше 80% при відсутності агресивних домішок у навколишньому середовищі.

5.3 Вимога до транспортування і зберігання

Програма поставляється на DVD-диску, який повинен бути поміщений в жорсткий футляр, що забезпечує тривале зберігання в складських приміщеннях

в умовах придатних для зберігання оптичних дисків протягом 5 років. Допускається транспортування програмного виробу в транспортній тарі усіма видами транспорту. При перевезенні в залізничних вагонах вид відправки - невеликий малотоннажний.

При транспортуванні і зберіганні програмного вироби повинен бути передбачений захист від попадання пилу і атмосферних опадів. Кліматичні умови транспортування:

- температура навколишнього повітря, ° С - від +5 до +50;
- атмосферний тиск, кПа - 101,3;
- відносна вологість повітря при +25 ° С - 40-60%.

6 Вимоги до програмної документації

6.1 Попередній склад програмної документації

Склад програмної документації повинен включати:

- технічне завдання;
- пояснювальна записка;
- керівництво користувача;
- код програми.

7 Стадії і етапи розробки.

7.1 Стадії розробки

Розробка повинна проводитися за такими стадіями:

- розробка технічного завдання;
- робоче проектування;
- отримання результатів.

7.2 Етапи розробки

На стадії розробки технічного завдання повинен бути виконаний етап розробки, узгодження і затвердження цього технічного завдання.

На стадії робоче проектування повинні бути виконані перераховані нижче види робіт:

- обґрунтування вибору алгоритму;
- розробка програми;
- тестування і верифікація.

На етапі отримання результатів повинні бути проведені відповідні тести і дійшли висновку про виконану роботу та її результати.

Додаток Б. Код програми

Лістинг Б.1 – код програми

```
import copy
import flask
import json
import os
from random import choice as make_selection

app = flask.Flask(__name__)
quiz_dir = 'quizzes'

quizzes = {}
for quiz in os.listdir(quiz_dir):
    print('Loading', quiz)
    quizzes[quiz] = json.loads(open(os.path.join(quiz_dir, quiz)).read())

@app.route('/')
def index():
    return flask.render_template('index.html', quiz_names=zip(quizzes.keys(),
map(lambda q: q['name'], quizzes.values())))

@app.route('/quiz/<id>')
def quiz(id):
    if id not in quizzes:
        return flask.abort(404)
    quiz = copy.deepcopy(quizzes[id])
    questions = list(enumerate(quiz["questions"]))
    random.shuffle(questions)
    quiz["questions"] = map(lambda t: t[1], questions)
    ordering = map(lambda t: t[0], questions)

    return flask.render_template('quiz.html', id=id, quiz=quiz,
quiz_ordering=json.dumps(list(ordering)))

@app.route('/check_quiz/<id>', methods=['POST'])
def check_quiz(id):
```

```
    ordering = json.loads(flask.request.form['ord'])
    quiz = copy.deepcopy(quizzes[id])
    quiz['questions'] = sorted(quiz['questions'], key=lambda q: ordering.index(quiz['questions'].index(q)))
    answers = dict( (int(k), quiz['questions'][int(k)]['options'][int(v)]) for k, v in flask.request.form.items() if k != 'ord' )


    if not len(answers.keys()):
        return flask.redirect(flask.url_for('quiz', id=id))

    for k in range(len(ordering)):
        if k not in answers:
            answers[k] = [None, False]

    answers_list = [ answers[k] for k in sorted(answers.keys()) ]
    decision = make_selection(["GRAMM",
                "ГРИФ",
                "RiskWatch",
                "COBRA",
                "CORAS",
                "MSAT"])

    decision = len(list(filter(lambda t: t[1], answers_list)))

    return flask.render_template('check_quiz.html', quiz=quiz, answer=decision)


if __name__ == '__main__':
    app.run(debug=True)
```

Додаток В. Інструкція користувача

1. Призначення програми

Данна програма призначена для роботи з Системами оцінки ризиків.

Програма може працювати в необслугованому режимі. Відмова програми не тягне за собою критичних наслідків. Програма поставляється у виді здійснених кодів (.ру-файлів).

2. Апаратні та програмні вимоги

До складу технічних засобів повинен входити x64-сумісний персональний комп’ютер, що включає в себе:

- процесор з тактовою частотою 1.5 Гц;
- оперативна пам’ять 2 Гб;
- вільного дискового простору, не менше 1 Мб;
- ОС Windows 7 і вище;
- Edit with IDLE 3.6 і вище
- клавіатуру, мишу, монітор.

3.Установка програми

Програма поставляється у вигляді виконуваного файлу (.py). Встановлюється на даний комп’ютер шляхом копіювання в відповідну директорію.

4. Опис інтерфейсу

Інтерфейсом програми є інтерфейсом будь-якого браузеру.

5. Покроковий опис роботи програми

1) Після установки запустіть quiz_site.py

2) далі програма відкриє тест у браузері.

3) по завершенню тесту користувачем програма автоматично розрахує і видає результат.

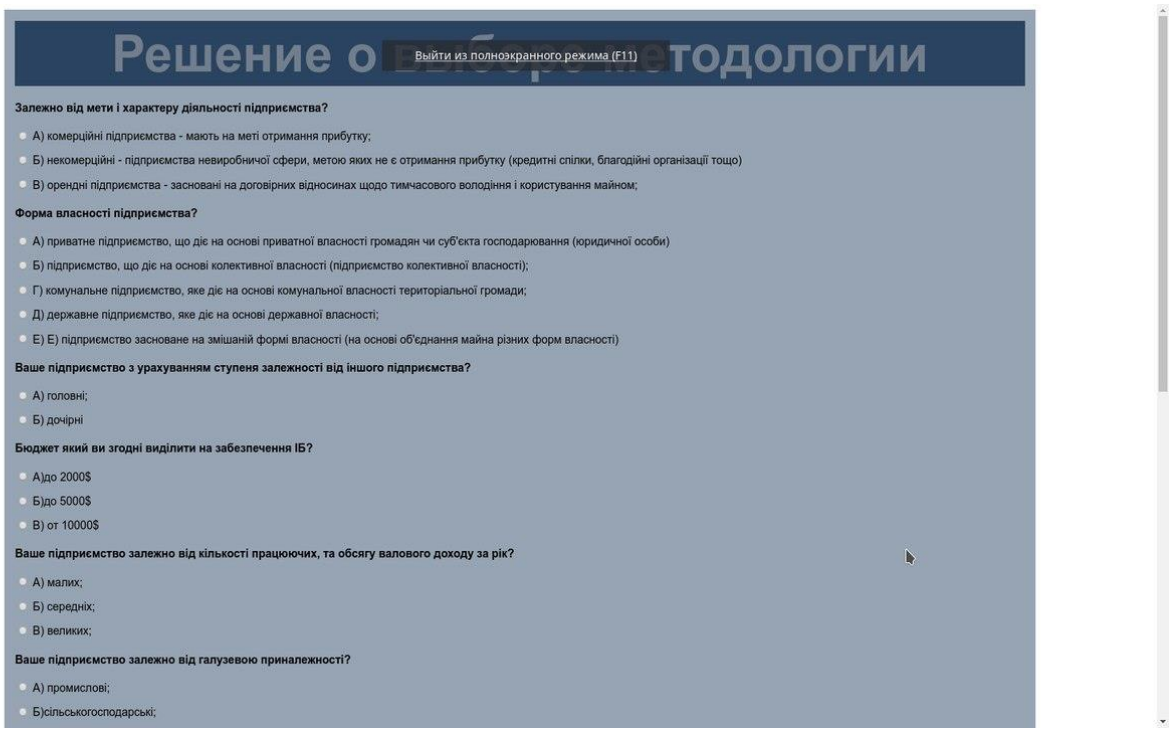

Рисунок 1.1 – інтерфейс програми

Рисунок 1.2 – інтерфейс програми