Міністерство освіти і науки України
Тернопільський національний університет імені Івана Пулюя
Факультет комп'ютерно-інформаційних систем і програмної інженерії
Кафедра кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломної роботи

на тему: Порівняльний аналіз методик оцінювання ризиків інформаційної безпеки у вищих навчальних закладах

Виконав: студент VI курсу, групи СБм-61
спеціальності 125 “Кібербезпека”
_____ Кузьо М.О.
Керівник _____ к.т.н., Кареліна О.В.
Нормоконтроль _____ _____
Рецензент _____ _____

м. Тернопіль — 2019

АНОТАЦІЯ

Робота об’ємом 104 сторінки, яка містить 16 ілюстрацій, 18 таблиць, 46 бібліографічних джерел.

Метою даної роботи є порівняльний аналіз методів визначення інформаційних ризиків та вибору найоптимальнішого методу для подальшого створення системи управління інформаційною безпекою вищого навчального закладу.

Об’єктом дослідження є ризики безпеки інформаційних ресурсів вищого навчального закладу та методи їх виявлення.

Предметом дослідження є забезпечення належного рівня захисту інформації вищого навчального закладу.

Методами дослідження є огляд наукових публікацій по даній темі, профільної літератури в сфері захисту інформаційних ресурсів, зокрема міжнародних стандартів, аналіз методів виявлення інформаційних ризиків, порівняння інструментальних засобів для управління інформаційними ризиками, аналіз засобів захисту інформації, а також їх характеристик, аналіз вимог щодо захисту інформації у вищих навчальних закладах.

Результати даної роботи можна використати для створення системи захисту інформації в вищому навчальному закладі.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ІНФОРМАЦІЙНІ РИЗИКИ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ЗАХИСТ ІНФОРМАЦІЇ

ABSTRACT

A 103-page volume containing 16 illustrations, 18 tables, 46 references in the list of links.

The purpose of this paper is to comparatively analyze the methods of identifying information risks and selecting the most appropriate method to further create a system of information security management at a higher education institution.

The subject of the study is the risks of the information resources of the higher education institution and the methods of their detection.

The subject of the study is to ensure an adequate level of protection of information of the higher education institution.

The research method is review of scientific publications on the topic, profile literature in the field of protection of information resources, in particular international standards, analysis of methods of identification of information risks, comparison of tools for management of information risks, analysis of information security tools, as well as their characteristics, analysis of security requirements. information in higher education institutions.

The results of this work can be used to create a system of information security in higher education.

INFORMATION SECURITY, INFORMATION TECHNOLOGIES, INFORMATION RISKS, INFORMATION SECURITY MANAGEMENT SYSTEM, PROTECTION OF INFORMATION

ЗМІСТ

ВСТУП

На сучасному етапі науково-технічного прогресу, яскраво вирізняється стрімкий розвиток в сфері інформаційних технологій. Можливість використання новітнього обладнання, процес інтеграції інформаційних систем з метою раціоналізації інформаційних ресурсів сприяють зростанню інтенсивності роботи науково-педагогічних працівників у вищих навчальних закладах та значно модернізують процес навчання студентів, який з кожним кроком даної модернізації стає все більш дистанційним.

Пліч-о-пліч з даним процесом розвиваються й методи реалізації загроз, як внутрішніх так і зовнішніх, з метою впливу на інформаційний ресурс вищого навчального закладу, що становить ризик порушення конфіденційності, доступності та цілісності інформації.

Вдосконалення управління інформаційними ризиками досить складне завдання. Для його виконання необхідні глибокі дослідження як джерел загроз інформаційній безпеці, так і аналіз причин їх виникнення. Внаслідок цих дій, можна провести оцінку рівня вразливості інформаційного ресурсу, що дозволить створити модель порушника інформаційної безпеки. Результатом виконання цих завдань є когнітивна модель управління інформаційними ризиками.

Актуальність даної кваліфікаційної роботи випливає з необхідності створення системи інформаційної безпеки та підтримки її на належному рівні, що зумовлено потребою в захисті інтересів студентів та викладачів.

Метою даної роботи є дослідження методів та засобів захисту інформації, вибору оптимального методу для подальшого створення системи управління інформаційною безпекою, що дозволить забезпечити належний рівень безпеки даних при оптимальному використанні ресурсів для побудови та забезпечення функціонування інформаційної системи. Підсумком проведення даної роботи є

проведення аналізу захищеності інформаційних ресурсів вищого навчального закладу.

Для досягнення мети було поставлено наступні завдання:

- огляд та аналіз документації, що регламентує сферу визначення інформаційних ризиків;
- аналіз вимог захищеності інформаційного ресурсу відповідно до його класифікації;
- аналіз та систематизація одержаних результатів;
- вибір оптимального методу для визначення інформаційних ризиків.

Об’єктом дослідження є ризики інформаційних ресурсів вищого навчального закладу та методи їх виявлення.

Предметом дослідження є надання високого рівня захищеності інформаційному ресурсу вищого навчального закладу.

Методами дослідження є огляд наукових публікацій по даній темі, профільної літератури в сфері захисту інформаційних ресурсів, зокрема міжнародних стандартів, аналіз методів виявлення інформаційних ризиків, порівняння інструментальних засобів для управління інформаційними ризиками, аналіз засобів захисту інформації, а також їх характеристик, аналіз вимог щодо захисту інформації в вищих навчальних закладах.

Наукова новизна даної кваліфікаційної роботи полягає в використанні методів аналізу інформаційних ризиків в вищих навчальних закладах.

Практичне значення результатів роботи випливає з того, що використання вибраного методу аналізу інформаційних ризиків дозволяє не тільки охарактеризувати захищеність інформацій ресурсів вищого навчального закладу, а й визначає засоби запобігання даним ризикам та терміни їх вирішення.

1 МЕТОДИ ОЦІНЮВАННЯ РИЗИКІВ В СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Ризики в системах забезпечення інформаційної безпеки

Визначення терміну «інформаційна безпека» у вузькому значенні - це процес забезпечення цілісності, доступності та конфіденційності. Існує досить об'ємний клас систем для обробки інформації, при розробці яких безпека відіграє провідну роль (наприклад, інформаційні, економічні, лінгвістичні, банківські та медичні системи).

Одним з найважливіших організаційних заходів в сфері захисту інформації в комп'ютеризованих системах є визначення переліку загроз інформації, які порушують її властивості – цілісність, доступність та конфіденційність. Одна, а в більшості випадків й декілька загроз можуть використовувати множину уразливостей інформації.

Будь-яка з уразливостей та загроз може мати вагомий вплив на інформаційну безпеку підприємства. Знання про ці зміни збільшує можливості при прийнятті необхідних заходів для вивчення та запобіганню ризику та забезпечення безпеки інформаційно-телекомунікаційної системи загалом.

Поясненню визначення «інформаційна безпека» фахівцями приділяється багато зусиль, натомість поняття, такі як «загроза» і «небезпека» розглядаються не настільки широко, поза контекстом даного поняття.

Потребу у розробці такого поняття, як «загроза» можна визначити :

- відсутністю унікального підходу при дослідженні типового поняття інформаційної безпеки;

- недостатніми розробками поняття «загроза» і спробами його відокремлення від інших понять-синонімів, а саме «небезпека», «ризик», «виклик», і відповідно поняття «інформаційна загроза» і вже його

відокремлення від понять, наближених по значенню до нього, а саме «інформаційний тероризм», «інформаційна війна», «інформаційне протиборство»;

- присутністю невирішених проблем при формуванні категорійного апарату в теорії безпеки в інформаційних системах;

- можливістю використання теоретичних розробок категорійного апарату формувати відповідну вимогам систему управління загрозами та небезпеками, моніторингу в інформаційній сфері.

При вивченні загроз інформаційному ресурсу ми можемо розглядати їх як випадки технічного, антропогенного або природнього характеру, які здатні спричиняти небезпечний вплив на інформаційну систему в цілому, а в тому числі й на інформацію, що зберігається в ній. Виникнення загрози, а саме виявлення джерела інтеграції певних подій характеризується таким елементом безпеки інформації, як уразливість. Саме за наявності уразливості, як пункту характеристики системи, відбувається реалізація загроз. Безсумнівно, сама загроза, за своєю суттю, у відповідності до теорії множин, не може бути повністю описаною.

Вивчаючи різні підходи та пропозиції щодо вирішення цього питання, на мою думку можна виділити певний перелік загроз інформаційній безпеці, а саме:

- викриття інформаційного ресурсу;

- порушення його цілісності;

- збої в роботі обладнання.

Загроза порушення цілісності інформаційних ресурсів полягає в навмисному антропогенному впливі на дані, що зберігаються в інформаційній системі суб'єкта управління, а також розповсюджуються з даної інформаційної системи, захищеним з’єднанням, до інших інформаційних систем.

Загроза розкриття інформаційного ресурсу, насамперед, полягає у тому, що дані, стають відомими тим, хто не має доступу до цієї інформації. Тобто під

загрозою викриття можна розуміти таку ситуацію, коли вдало реалізований несанкціонований доступ до ресурсів системи, в тому числі йдеться і про загальнодоступні, і про ресурси з обмеженим доступом. Ці ресурси повинні передаватися виключно між персоналом і зберігатися у єдиній інформаційній системі даної установи.

Загроза збою в роботі обладнання виникає при спробі блокування доступу до ресурсів інформаційної системи. Загалом блокування може бути як перманентним, тобто ресурс, до якого виконується запит, вже ніколи не буде отриманий, так і може викликати певні затримки в отриманні ресурсу, до якого виконується запит, чого достатньо для того, щоб даний ресурс став некорисним.

Найнебезпечнішими та найрозповсюдженішими є ненавмисні помилки недосвідчених користувачів та системних адміністраторів. Та не варто забувати й про інших осіб, які входять в штаб обслуговуючого персоналу інформаційної системи. Інколи такі помилки є загрозами (похибки при введені даних, помилки в програмах, які викликають колапс системи), інколи вони спричиняють ситуації, що несуть загрозу безпосередньо об'єкту.

Загалом, в результаті проведених фахівцями з інформаційної безпеки досліджень, понад 65 % шкоди, що завдається інформаційному ресурсу, є наслідком випадкових помилок. Загрози природного характеру, а саме землетруси, повені та пожежі трапляються не часто . Звертаючи увагу на ці дані, доцільним є зосередження уваги на більш вагомому впровадженні комп'ютеризованих систем для забезпечення інформаційної безпеки.

За розмірами завданої шкоди, дещо поступаються згаданим вище загрозам крадіжки і фальсифікації. Зазвичай, виконавцями цих дій, насамперед, фігурують працівники штату організації, глибоко обізнані у принципі роботи інформаційної системи та в заходах безпеки установи. В даному аспекті надзвичайно небезпечними є співробітники, що не поділяють поглядів установи на яку вони працюють.

Загалом, діями цих співробітників керує насамперед намагання нанести збитку організації на яку вони працювали, та яка, в їх переконаннях, повелася з ними неправомірно. Такі прояви образи можуть бути відображені у здійсненні таких зловмисних дій:

- інтеграція шкідливого програмного забезпечення, яке повністю руйнує програми і дані;
- введення некоректних даних;
- знищення даних;
- модифікація даних;
- нанесення фізичної шкоди обладнанню;
- надання несанкціонованого доступу до даних із обмеженим доступом.

Співробітники, які знайомі з внутрішніми порядками даної установи, можуть нашкодити надзвичайно ефективно. Насамперед, надзвичайно важливо проводити ретельний контроль при звільненні певного співробітника на наявність персонального права доступу до інформаційного ресурсу та повністю його обмежити, а після звільнення, змінити всі паролі доступу до внутрішньої мережі. Окрім того, варто знизити імовірність його спілкування із працівниками, які продовжують мати доступ до цінної інформації.

Крім антропогенних, виділяють ще й загрози природного характеру. Ці загрози можна широко охарактеризувати. Для початку, можна відокремити порушення інфраструктури. Тут можна виділити проблеми з водопостачанням, зв’язком та електроенергією. Також небезпечними є стихійні лиха. Серед них землетруси, смерчі, бурани, урагани та тайфуни. В відсотковому співвідношенні кількість загроз інформаційній безпеці природного характеру за різними даними фахівців становить близько 15 відсотків від всієї кількості.

Серйозну загрозу також можуть нести програмні віруси. Проте банальне виконання правил безпечного користування комп'ютерною технікою та наявність у обслуговуючому штаті фахівця з питань інформаційної безпеки в декілька раз зменшить можливість результативного здійснення спроби

реалізації загрози. Дійсно, щодня інформаційні системи багатьох установ потерпають від атак хакерів, проте загальна частка заподіяної шкоди від хакерів, в порівнянні з загрозами інших типів відчутно менший.

Загрози в цілому можна класифікувати за кількома параметрами. Зазвичай джерелами помилок у програмному забезпеченні можуть бути:

- помилки розробників під час написання програмного забезпечення;

- збої, викликані модернізацією, встановленням чи заміною апаратних засобів та спроби встановлення не ліцензованого програмного забезпечення;

- програмні віруси, якими можуть бути інфіковані програми;

- програмні компоненти, що передбачені розробниками програмного забезпечення для різних цілей.

Віруси є самим втіленням небезпеки та можуть проявлятися у видачі системних повідомлень на екран монітора, пошкодженні інформації на дисках, зміни шляхів розташування файлів, зменшенні продуктивності комп'ютера, зборі внутрішньої інформації установи.

Розкраданню підлягають:

- програмно-апаратні засоби, якими обладнуються комп'ютери і самі мережі;

- програмне забезпечення та інформація збережена на носіях;

- фізичні копії із надрукованою інформацією.

Розкрадання також може бути виконаним з:

- робочого місця користувача;

- під час транспортування;

- з місця збереження.

Зважаючи на це можна розподілити загрози по видах. Зважаючи на їх кількість я зробив спробу, враховуючи існуючі напрацювання в сфері класифікації загроз національній безпеці, виділити загрози інформаційній безпеці.

За джерелами походження:

- загрози техногенного походження – складаються з транспортних аварій, пожеж, неспровокованих вибухів та загрози їх виникнення, раптового знищення каналів зв'язку, аварій на інженерних мережах чи спорудах життєзабезпечення, аварій головних серверів установи тощо;

- загрози природного походження – складаються з небезпечних геологічних, метеорологічних, гідрологічних морських та прісноводних явищ, деградації ґрунтів та надр, природних пожеж;

- загрози антропогенного походження – це насамперед спроба вчинення людиною різних дій з метою руйнування інформаційної системи, ресурсів та програмного забезпечення установи тощо. До цієї групи, поділяючи за змістом дій, можна віднести:

- ненавмисні - викликані помилковими діями користувача;

- навмисні – ті дії, що стали результатом цілеспрямованих злодіянь певних осіб.

За імовірністю реалізації можна поділити на:

- імовірні – це ті загрози, що при виконанні певного переліку умов неодмінно відбудуться;

- неможливі – це ті загрози, що при виконанні певного переліку умов нізащо не відбудуться. Ці загрози мають умовний характер, не підкріплений реальною та, навіть, потенційною можливістю для здійснення проголошених намірів;

- випадкові – це ті загрози, які при виконанні певного переліку умов завжди розвиваються різними сценаріями. Загрози цього рівня вірно аналізувати методом досліджень операцій, які розглядають логічні закономірності у випадкових явищах.

За повторюваністю вчинення можна поділити на:

- повторювані - ті загрози, що раніше були здійснені;

- продовжувані – повторюванні спроби втілення загроз, що складаються з ряду тотожних та об’єднуються спільною метою.

За рівнем детермінізму можна поділити на:

- випадкові – це ті загрози, в можливості виникнення яких ми не впевнені.

- закономірні – це ті загрози, які носять повторюваний характер. Вони зумовлені особливостями будови та розвитку системи інформаційної безпеки. Так, для прикладу, суб'єкт, в якому система забезпечення інформаційної безпеки функціонує некоректно, стає ціллю для інформаційних атак;

За сферами походження можна поділити на:

- екзогенні – у випадку, коли джерело виведення з ладу інформаційної системи знаходиться за її межами;

- ендогенні - у випадку, коли джерело виведення з ладу інформаційної системи перебуває безпосередньо у системі.

За значенням можна поділити на:

- допустимі – це ті загрози, які не здатні призвести до повного руйнування системи;

- недопустимі – це ті загрози, які, у випадку реалізації, можуть призвести до повного руйнування системи.

За структурою впливу можна поділити на:

- системні – це загрози, які впливають на суб’єкт установи комплексно. Зазвичай постійний вплив відбувається одночасно в кількох місцях з найбільшою вразливістю;

- структурні – це загрози, які впливають на окремі структурні частини системи;

- елементні - це загрози, що впливають на окремі частини структури системи. Ці загрози носять постійний характер. Вони небезпечні лише у випадку не проведення їх моніторингу.

За об’єктом впливу можна поділити на:

- особу;

- суспільство;

- державу.

За характером реалізації можна поділити на:

- реальні – введення в дію алгоритмів виведення з ладу інформаційної системи є неминучою з необмеженим інтервалом часу та простором дій;

- потенційні – введення в дію алгоритмів виведення з ладу інформаційної системи стає можливим при певних умовах функціонування структури установи;

- здійснені - вже реалізовані загрози;

- уявні – помилково визначенні спроби виведення з ладу інформаційної системи, які зазвичай такими не є.

За ставленням до них:

- об'єктивні – це ті загрози, що підтвердженні фактами. Проте ставлення управління до них не відіграє важливої ролі тому, що об'єктивні загрози можуть існувати незалежно від самого суб'єкта;

- суб'єктивні - це сукупність певних чинників об'єктивної дійсності. В даному випадку , рішення суб'єкта управління відіграє вирішальну роль в становленні визначених чинників в якості загроз безпеці.

1.2 Основні методи оцінювання ризиків в системах інформаційної безпеки

В сучасному світі інформаційні технології охопили всі сфери діяльності суспільства, і саме це підштовхує нас до модернізації та скурпульозного формування інформаційної системи починаючи з фізичного та закінчуючи користувацьким рівнем. Цей розвиток можна назвати вступом в еру інформації..

Швидкий ріст зацікавленості в розвитку сфери інформаційних технологій окрім великої користі приніс в свою чергу й широкий спектр проблем щодо

вирішення загроз безпеці інформаційних систем. Комп'ютерні злочини та такі загрози інформаційній безпеці, як хакерські атаки, витоки секретної інформації, віруси, переривання обслуговування, відмови систем невпинно ростуть в кількості спроб їх реалізації.

Зрештою невирішені проблеми в сфері інформаційної безпеки систем стали об'єктом пильної уваги фахівців у всіх сферах, частково чи повністю пов'язаних з інформаційними технологіями. Щоб уникнути величезних ризиків, внаслідок застосовування провідними фахівцями різних засобів нагляду, установи змушені на всіх рівнях підвищувати поінформованість і вводити в експлуатацію заходи спрямовані на оцінювання стану інформаційної безпеки.

Описуючи системи забезпечення безпеки не варто забувати, що вони повинні не лише обмежувати допуск користувачів до інформаційного ресурсу, а й визначати та розмежовувати їхні повноваження в даній системі, виявляти не притаманне даній системі використання ресурсів, аналізувати можливість виникнення аварійних ситуацій та усувати їх наслідки, вдало підлаштовуючи структуру мережі до виникнення відмов, неповної втрати або повного блокування ресурсів.

Проте, визначним фактором в побудові системи інформаційної безпеки є економічна доцільність при застосуванні програмно-апаратних методів, яка безумовно має відповідати цінності можливої втрати інформаційного ресурсу внаслідок реалізації можливих загроз.

Захищеність інформації визначається повнотою вирішення всього комплексу завдань. Тобто, сам по собі захист інформації являє собою сукупність засобів і методів, які регулярно використовуються та запобіжних заходів для систематичного забезпечення високого рівня надійності інформації, що зберігається та обробляється на об'єкті інформаційно-аналітичною системою та передається по каналах. Цей захист має мати системний характер, де для отримання бажаного результату усі розрізнені типи захисту інформації потрібно об'єднати й налаштувати їх функціонування в складі єдиної системи

як злагоджений механізм, який визначений для вирішення завдань із забезпечення безпеки інформації. Даний механізм повинен містити:

- нормативно-правовий базис захисту інформації;
- засоби, способи і методи захисту;
- органи і виконавців.

Визначення інформаційних ризиків — доволі складне завдання. Часто ці завдання розв’язують з допомогою експертних методів, які вносять суб’єктну частину в оцінку ризику. В даному випадку установа, яка спирається на цю оцінку, часто може затвердити не вірне рішення щодо інвестицій в інформаційну безпеку. Не вірно оцінені ризики здатні призвести до переоцінки, в кращому випадку, або, що в порівнянні набагато гірше, до недооцінки небезпеки. Саме тому вибір технічно обґрунтованої моделі для визначення інформаційних ризиків є актуальною проблемою в сфері захисту інформації.

Загалом, метод це сукупність послідовних кроків, яку необхідно виконати для розв’язання певного завдання та досягнення поставленої виконавцеві мети, тобто дати оцінку ризиків.

Усі методи для оцінювання ризиків інформаційної безпеки можна поділити на кількісні, якісні або мішані.

Кількісні методи використовують об’єктивні дані для обрахунку числового значення вартості активів, імовірності втрат і пов’язаних із ними ризиків.

Для якісних методів використовується відносний показник ризику. Йдеться про поділ на три рівня:

- низький;
- середній;
- високий.

Для даного типу методів також використовується оцінка вартості активу на основі рейтингу, для прикладу, за шкалою від 1 до 10. Якісна модель оцінки ризиків розраховує імовірності втілення в життя ризиків у швидкий та

економічно ефективний спосіб. Групи ризиків, сформовані й проаналізовані згідно з якісною методикою, можуть виступати основою для проведення кількісної оцінки.

Останнім часом кількісні підходи домінували в сфері захисту інформаційних. Однак, віднедавна суто кількісні методи управління ризиками, все більше програє якісним методам оцінювання ризиків, що пов'язане зазвичай із надзвичайною трудомісткістю роботи, яка в результаті не дає відчутного виграшу. Якщо говорити про комбінації кількісних і якісних методів, то вони, загалом, поєднують в собі як переваги, так і недоліки цих груп методів.

Метою якісних методів оцінювання є визначення імовірних видів ризиків та рівня небезпеки загроз, відокремлення чинників, які впливають на рівень загроз, обґрунтованого подання різних можливих контрзаходів. Дані методики не дають жодних кількісних визначень. Вони достатньо прості. В основі їх розробки закладено зазвичай вимоги міжнародного стандарту ISO 17799:2002.

Кількісні методи оцінювання роблять можливим перехід від імовірнісної оцінки ризику до відповідних числових значень. Методики подають реальні й математично обґрунтовані числові значення усіх складових процесу аналізу інформаційних ризиків. Типовими складовими кількісних методів оцінки інформаційної безпеки є:

- вартість захисних заходів;
- цінність активу;
- збиток для бізнесу;
- частота виникнення загрози;
- ефективність захисних заходів;
- вірогідність використання уразливості.

Кількісний аналіз дозволяє обчислити конкретне значення (у відсотках) імовірності реалізації загрози.

Порівняльну характеристику кількісних і якісних методів наведено в таблиці 1.1.

Таблиця 1.1 Порівняльна характеристика кількісних і якісних методів

	Кількісні методи	**Якісні методи**
Переваги	• Дозволяють визначати наслідки виникнення інцидентів у кількісний спосіб. • Роблять можливим аналіз витрат і користі при виборі підходу до захисту. • Допомагають отримати достатньо точну картину ризикованої ситуації	• Дозволяють визначати сфери та осередки великої небезпеки в стислі терміни та без великих витрат. • Аналіз ризиків і переваг порівняно легкий
Недоліки	• Кількісні оцінки неодмінно залежні від розміру та точності вибраної шкали вимірювання. • Результати аналізу можуть бути неточні, зокрема й через відсутність вірогідних даних про перебіг відповідних подій. • Остаточні висновки здебільшого мають спиратися на якісний опис. • Вимагають значно більших витрат, ніж якісні методи.	• Непридатні для визначення ймовірностей результатів, здобутих чисельними засобами. • Аналіз переваг більш ускладнюється за рахунок вибору захисту. • Результати мають загальний характер, усі значення тільки наближені тощо

1.3 Класифікація загроз інформаційної безпеки вищого навчального закладу

Аналіз уразливості інформаційного ресурсу Вищого навчального закладу та їх наслідки в повній мірі відповідають таким негативним проявам, які притаманні іншим закладам і установам держави [14], це збільшення фактів протизаконного збору і використання інформації, несанкціонованого доступу і використання інформаційних ресурсів, незаконного копіювання інформації, викрадення інформації з бібліотек, архівів, банків і баз даних, порушення

технологій обробки інформації, запуску програм-вірусів, знищення та модифікації даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку. Разом з тим для Вищих навчальних закладів є і особливості, що пов’язані із блокуванням доступу до відкритої інформації при дистанційному навчанні, введення хибних теоретичних і оціночних даних, ведення електронного діалогу від особи викладача.

Оскільки організація забезпечення інформаційної безпеки повинна носити комплексний характер і ґрунтуватися на аналізі уразливості інформаційного ресурсу та негативних наслідків, то потрібна ідентифікація можливих джерел загроз, факторів, що сприяють їх прояву.

Джерела загроз – це потенційні антропогенні, техногенні та природні загрози інформаційної безпеки, де під самою загрозою в цілому розуміють потенційно можливу подію, вплив, процес або явище, яке може привести до нанесення збитку інтересам суб'єктів та стану об’єктів інформаційних систем, їх інформаційним відносинам, яке за допомогою впливу на інформацію або інші компоненти інформаційної системи може прямо або опосередковано призвести до нанесення шкоди інтересам даних суб'єктів.

Уразливість – це притаманні об'єкту інформаційної системи причини, що призводять до порушення інформаційної безпеки на конкретному об'єкті і обумовлені недоліками процесу функціонування об'єкта системи.

Наслідки – це можливі дії реалізації загрози при взаємодії джерела загрози через наявні уразливості. В наслідках саме збитки підлягають чисельним розрахункам втрати часу чи фінансовим затратам на відновлення. Тому до класифікаційної ознаки загроз обов’язково слід віднести такі наслідки:

- розкрадання (копіювання інформації);
- знищення інформації;
- модифікація (спотворення) інформації;
- порушення доступності (блокування) інформації;
- заперечення достовірності інформації;

- нав'язування неправдивої інформації.

На кінцевий результат найбільш впливова початкова ознака – джерела загроз, які доцільно поділити на три групи:

- антропогенні джерела – ті, що обумовлені діями суб'єкта, які можуть призвести до порушення безпеки інформації. Такі дії можуть бути кваліфіковані як навмисні або випадкові, а за адміністративно-правовими відносинами – злочинними. Незалежно від приналежності та місця джерела при розподілі їх на зовнішні і внутрішні їх можливо і доцільно прогнозувати, а отже планувати, закладати в ризики і вживати адекватних заходів для зменшення уразливості інформаційної системи.

- техногенні джерела, обумовлені технічними засобами. Ці джерела загроз менш і складніш прогнозуються, безпосередньо залежать від властивостей техніки, структури і архітектури мереж Вищого навчального закладу, наявності ліцензійного програмного забезпечення і додаткових програм захисту інформації, кваліфікації адміністраторів мереж та обслуговуючого персоналу, тому вимагають особливої уваги. Дані джерела загроз інформаційної безпеки, також можуть бути як внутрішніми, так і зовнішніми, а для синтезу їх моделі і оцінки ризиків [15] раціонально використовувати когнітивні моделі оцінки.

- стихійні джерела – група об'єднує обставини, що становлять непереборну силу (стихійні лиха, або ін. обставини, які неможливо передбачити або запобігти чи можливо передбачити, але неможливо запобігти), такі обставини, які носять об'єктивний і абсолютний характер, поширюється на всіх. Такі джерела загроз не піддаються прогнозуванню і тому заходи проти них повинні застосовуватися завжди. Стихійні джерела, як правило, є зовнішніми по відношенню до захищеного об'єкта і під ними, як правило, розуміються природні катаклізми. Для зменшення часу на відновлення самим дієвим засобом залишається резервування обладнання і програмного забезпечення, добове чергування, постійний моніторинг тощо.

Територіально розподілена, частіше кампусна структура інформаційної системи Вищих навчальних закладів, за визначенням повинна бути відкритою, тому створює ряд передумов для реалізації різноманітності потенційних загроз інформаційної безпеки, що можуть завдати шкоди всім складовим інформаційної системи. Різноманітність настільки значна, а випадковість появи атак, мета їх застосування і оснащеність стрімко зростає, що це не дозволяє передбачити кожну загрозу. Тому аналізуючи характеристики загроз треба вибирати протидії з позицій здорового глузду, одночасно виявляючи не тільки самі загрози, розмір потенційного збитку, але і поєднувати окремі випадки застосувань в підгрупи джерел і зменшувати загальну уразливість системи та застосовувати принцип диференціації рівня захисту на основі оцінювання ризиків.

Класифікація за ознакою «мета використання загроз» за якою запропонована Доктрина інформаційної безпеки України показує, що на першому місці по частоті виникнення стоять крадіжки інформації (65,8%), на другому місці - недбалість співробітників (55,1%), на третьому - вірусні атаки (41,7%). Співвідношення внутрішніх і зовнішніх загроз становить відповідно 43,5 і 56,5%. У категорію внутрішніх загроз були віднесені недбалість співробітників, саботаж і фінансове шахрайство, у категорію зовнішніх загроз — дія вірусів, хакерів і спаму. Найбільш небезпечною внутрішньою загрозою інформаційної безпеки виявилася витік конфіденційної інформації, що чинена інсайдерами (70%). Найбільший збиток при цьому пов'язаний з фінансовими збитками (46%), далі йдуть — погіршення іміджу і громадської думки (42,3%), втрата клієнтів (36,9%). Необхідно підкреслити, що отриманий загальний спектр загроз і тенденцій їх розвитку характерний і для освітніх установ [16].

Тоді модель порушника інформаційної безпеки повинна відображати причини і мотиви його дій, його можливості, апріорні знання, мету дій, їх пріоритетність, шляхи досягнення (способи реалізації вихідних загроз, місце і характер дії, можливу тактику, мотиви поведінки). Взагалі це може бути

декілька моделей дій зловмисника, що відображають різний рівень його підготовленості, що пояснює розподіл джерел за ознакою – категорія порушника інформаційної безпеки.

Для вищого навчального закладу типовими категоріями стають ті, що приймають участь в життєдіяльності закладу, суттєво впливають на стан інформаційної безпеки, мають наступні характеристики і оцінки:

- студент. Загрози з боку студентів йдуть по декількох напрямках. По-перше, це неконтрольований вихід в Інтернет, що тягне за собою різке збільшення трафіку і нецільове витрачання інформаційного ресурсу, а нелегальне скачування до зараження вірусами мережі, що відповідно призводить до обмеження доступу великого контингенту студентів і викладачів або навіть повного блокування мережі.

По-друге, вищий навчальний заклад - це місце підвищеної активності і концентрації хакерів-початківців. Юнацький максималізм, бажання випробувати свої знання і справити враження на однокурсників спонукає студентів зламати мережу, заблокувати вихід в Інтернет, отримати адміністративний доступ, влаштувати вірусну епідемію або вчиняти інші комп'ютерні правопорушення. Це веде до зриву занять або блокування доступу до мережі.

По-третє об’єктивна зміна життєвих цінностей і різке збільшення кількості студентів на комерційній основі вносить певні труднощі в забезпечення безпеки самого навчального процесу, бо застосовується:

– широке використання в студентському середовищі сучасних інформаційно-комунікаційних технологій для складання заліків та іспитів (ноутбуки, планшети, смартфони із бездротовим доступом до Інтернету);

– підробки залікових і екзаменаційних відомостей, залікових книжок, відпрацювання та захисту практичних і лабораторних занять, курсових робіт;

– плагіат на стадії виконання рефератів, курсових робіт і проектів тощо.

До четвертого напрямку загроз відносяться можливі розкрадання, в тому числі, комп'ютерного обладнання та бібліотечного фонду. Тут втрати мають суто матеріальний характер, пов'язаний з необхідністю відновлення ресурсів.

І останній напрям загроз - це ненавмисні помилки студентів, що має наслідки виходу з ладу обладнання, зриву занять, обмеження доступу інших користувачів до інформації;

- співробітник. Серед загроз з боку співробітників Вищого навчального закладу, можна виділити такі:

- в області відкритої інформації - це неправомірне використання веб-доступу, так як практично всі кафедри, викладачі та співробітники мають вільний, слабо контрольований доступ в Інтернет.

- в області конфіденційної інформації, що має характер службової таємниці, - це витік, розголошення, модифікація інформації, що може нанести шкоду діяльності чи іміджу закладу.

- в області комерційної інформації — привласнення чужої інтелектуальної власності або передачу їх третім особам.

- халатність і безвідповідальність співробітників, що тягне за собою реалізацію загроз і пов'язаний з цим збитків;

- ненавмисні помилки при роботі з обчислювальною технікою, так як не всі співробітники мають відповідну кваліфікацію;

- відвідувач. Дана категорія осіб практично не має фізичного доступу до інформаційної системи Вищого навчального закладу. Можливості їх обмежені, вони можуть здійснювати тільки поодинокі дії, скориставшись недбалістю або безвідповідальністю працівників, однак збиток від їх дій може бути істотним;

- хакер-одинак. Використовує стандартні комп'ютерні програми для реалізації відомих вразливостей. Це може бути і студент, що має доступ як з середини мережі, так і віддалений доступ. Дії його носять експериментальний характер, фінансова мотивація - не головне. Йому цікаво зламати сайт, отримати доступ до конфіденційної інформації, до серверів організації, до

систем адміністрування, контролю і управління інформаційною системою. Дії його можуть завдати шкоди цілісності мережі. Найчастіше його дії носять несистемний характер, і він зупиняється після першого успішно проведеного злому. У той же час, він може мати і чисто матеріальний інтерес, розраховуючи на підключення та використання каналів зв'язку з високою пропускною здатністю;

- хакерська трупа - переслідує суто матеріальний інтерес. Володіючи достатніми сумарними знаннями в області комп'ютерних технологій, такі зловмисники можуть організувати сканування інформаційної системи Вищого навчального закладу з метою виявлення нових вразливостей, самостійно написати програми для експлуатації цих вразливостей. Вони діють цілеспрямовано і можуть отримати доступ до різних фінансовим документів, влаштувати потужні атаки на інформаційну систему з повним виводом її з ладу, що може завдати істотної матеріальної шкоди закладу;

- конкуренти. Підвищилася в останні роки конкуренція між вузами за надання освітніх послуг, це змушує окремо виділити цю групу порушників. Разом з тим в рамках Вищого навчального закладу нерідко проводяться дослідницькі та дослідно-конструкторські розробки за договорами з різними підприємствами країни, зарубіжними організаціями, а також виграних грантів. У закладах існують відділи інтелектуальної власності, які проводять роботу по закріпленню інтелектуальної власності розробок та на договірних засадах обслуговує інші фірми. Дії конкурентів можуть носити як прихований, так і відкритий, демонстративний характер. Конкуренти можуть вживати серйозні зусилля за отримання відомостей, що становлять комерційну таємницю, відомостей щодо функціонування інформаційної системи Вищого навчального закладу, використовуючи для цього підкуп співробітників. Конкуренти мають свої потужні обчислювальні мережі, штат кваліфікованих співробітників в області IT-технологій і достатні фінансові кошти для здійснення протиправних дій;

- злочинні угрупування і організації. Вищі навчальні заклади виконують важливу соціально роль, спрямовану на виховання молоді, де зосереджена велика кількість людей у віці від 17 до 23 років. Тому заклади, стають мішенню для дії злочинних угруповань та організацій для проведення різних терористичних актів, поширення наркотиків і завоювання впливу на молоді незміцнілі уми з боку різних політичних партій, екстремістських угруповань і релігійних сект. Ця група зловмисників представляє серйозну загрозу як для закладу в цілому, так і для його інформаційного середовища. Залежно від цілей, подібні організації можуть мати досить високий фінансовий потенціал і підготовлених фахівців.

Заходи захисту інформації (протидії) від таких джерел повинні ретельно продумуватися, до них можна віднести:

- правові (закони, статути, накази, постанови);

- організаційні (розробка і затвердження функціональних обов'язків посадових осіб служби інформаційної безпеки; фізичний контроль доступу; розробка правил управління доступом до ресурсів системи; явний і прихований контроль за роботою персоналу; проведення регулярних семінарів, спецкурсів для адміністраторів мереж Вищого навчального закладу, з метою забезпечення відповідності рівня знань сучасним вимогам);

- технічні (передбачається наявність методів визначення загроз та каналів витоку інформації і знання засобів добування (зняття) інформації);

- інженерно-технічні (забезпечують унеможливлення несанкціонованого доступу сторонніх осіб на об'єкти захисту)

- програмно-технічні (методи ідентифікації і автентифікації користувачів; реєстрація дій користувачів; засоби захисту від НСД, міжмережеві екрани);

Список способів протидії повинен, у разі необхідності поповняться новими засобами захисту. Це необхідно для підтримки системи безпеки закладу в актуальному стані.

1.4 Модель інформаційної системи вищого навчального закладу

Сучасні технології навчання ґрунтуються на інтенсивному використанні інформаційних ресурсів та розподілених інформаційних систем [21]. Безпека цих систем має важливе значення як для нормального функціонування навчального закладу, так і для забезпечення належної якості освіти. Порушення конфіденційності, цілісності та доступності інформації в навчальних інформаційних систем може негативно впливати на навчальний процес, завдавати фінансових збитків, створювати незручності для студентів, викладачів та адміністративного персоналу. Навчальні інформаційні системи є складовими частинами інформаційних систем закладів освіти. Інформаційні системи закладів освіти мають низку особливостей, що відрізняють їх від інформаційних систем інших установ, організацій, підприємств. Сьогодні ще остаточно не сформовані уявлення щодо оптимального складу таких систем, їх архітектури, функцій, які вони реалізують, а також не випрацювані підходи до забезпечення безпеки інформації в таких системах з урахуванням їх специфіки.

Інформаційні ресурси кожного рівня можна уявляти як ієрархічну деревоподібну структуру, у яку входить інформаційний ресурс структурних підрозділів. Дана структура зображена на рисунку 1.1.

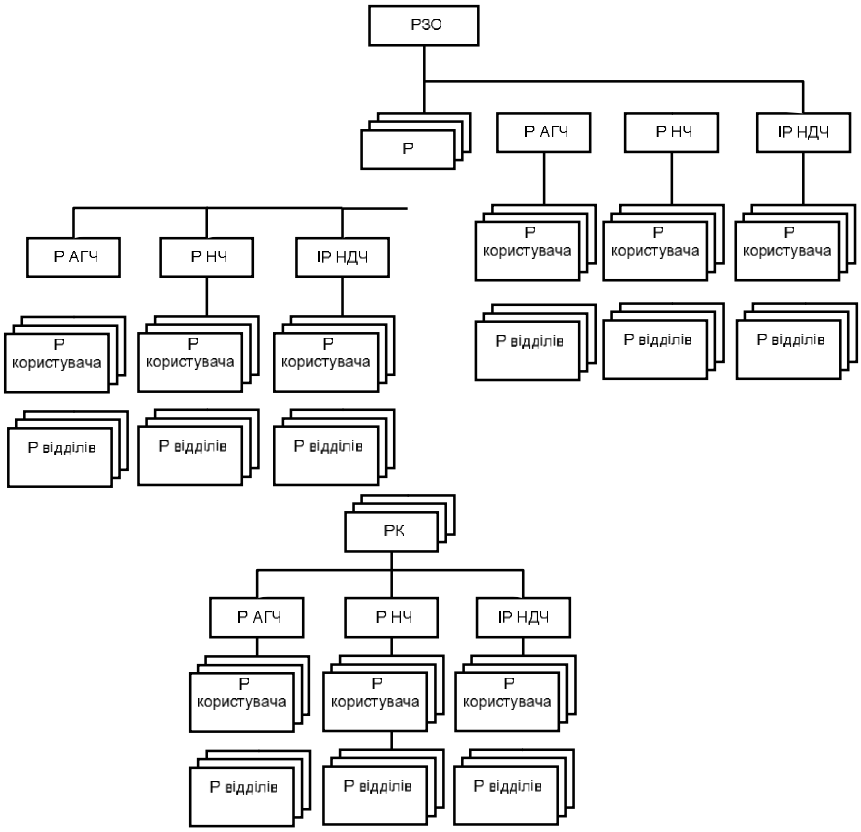

Рис. 1.1 Структура інформаційних ресурсів закладів освіти

Інформаційна система закладів освіти призначена для підтримки інформаційних ресурсів та потоків, надання користувачам інформаційно-обчислювального середовища та інших послуг, необхідних їм для виконання своїх функцій як викладача, науковця та адміністратора.

Інформаційна система закладів освіти – організаційно-технічна система, в котрій реалізуються інформаційні технології, і передбачається використання апаратного і програмного забезпечення, необхідного для реалізації процесів збирання, обробки, накопичення, зберігання, пошуку і поширення інформації. Основою інформаційної системи вищого навчального закладу є територіально розподілені комп’ютерні системи , елементи яких розміщені в окремих будівлях, на різних поверхах цих будівель і пов’язані між собою транспортним середовищем. Основу апаратних засобів таких систем становлять персональні

обчислювальні машини, периферійні та інші допоміжні пристрої, засоби зв’язку. Склад програмних засобів визначається можливостями апаратури і характером вирішуваних завдань в конкретній інформаційній системі.

Можна виділити такі елементи інформаційної системи:

- апаратне забезпечення;
- програмне забезпечення;
- інформаційні ресурси;
- автоматизовані робочі місця користувачів;
- власне користувачі.

Апаратне забезпечення – це канали і засоби зв’язку, вузли комутації, сервери тощо.

Програмне забезпечення інформаційної системи закладу освіти об’єднує системне програмне забезпечення, необхідне для підтримки функціонування самої системи, інструментарій користувача та навчальне програмне забезпечення.

До навчальних інформаційних ресурсів належать матеріали в електронному вигляді, які можуть використовувати користувачі у навчальному процесі. Зокрема, до них зараховуватимемо підручники, монографії, конспекти лекцій, навчальні презентації, навчально-методичні матеріали, інструкції до виконання лабораторних робіт, завдання до самостійних, розрахункових, курсових, дипломних робіт, тестові завдання тощо.

Зважаючи на це, можна побудувати модель інформаційної системи закладу освіти. Дана модель інформаційної систем зображена на рисунку 1.2.

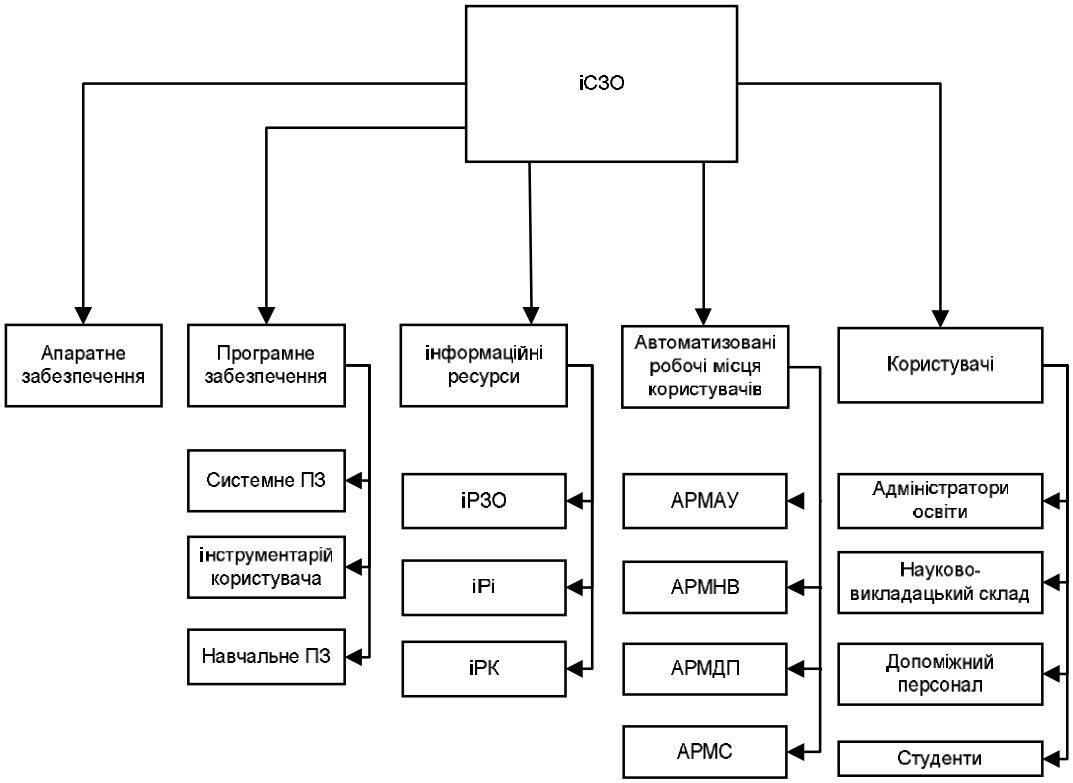

Рис. 1.2 Модель інформаційної системи закладу освіти

1.5 Висновки до розділу

В даному розділі розглянуто аспекти методів оцінки інформаційної безпеки як і у вищих навчальних закладах, так і за їх межами. Визначили чітке формулювання таких термінів, як «ризик», «уразливість», «загроза» в сфері захисту інформації, та провели чітку категоризацію останніх. Далі було розглянуто основні методи оцінювання ризиків в системах інформаційної безпеки, детально описано їх види та сфери їх застосування. Також проведено чітку класифікацію загроз інформаційної безпеки вищого навчального закладу, а саме розподіл джерел загроз:

- за походженням;
- за метою використання;
- за наслідками.

Проаналізовано структуру інформаційних ресурсів та модель інформаційної системи вищого навчального закладу, зокрема проведено її розподіл на такі елементи, як:

- апаратне забезпечення;
- програмне забезпечення;
- інформаційні ресурси;
- автоматизовані робочі місця користувачів;
- власне користувачі.

Виходячи з цих даних було сформовано модель порушника та наведено загальні заходи захисту інформації для вищого навчального закладу.

2 КЛАСИФІКАЦІЯ ТА СТАНДАРТИЗАЦІЯ ПРОГРАМНИХ ПРОДУКТІВ ДЛЯ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Класифікація програмних продуктів для аналізу та управління інформаційними ризиками

З ходом розвитку інформаційних технологій з’являється проблема збереження інформаційної безпеки та технічного захисту інформаційних ресурсів [2].

Проаналізувавши інформаційні джерела у галузі оцінки та управління інформаційними ризиками, в інформаційно-телекомунікаційних системах зараз мають вагому перевагу такі інструментальні засоби для оцінки як CRAMM, ГРИФ 2006, COBRA, RiskWatch, NIST, OCTAVE.

Загалом при оцінці управління ризиками виділяються такі компоненти, як:

- моніторинг організаційних ризиків функціонування системи захисту інформації;

- оцінювання ризиків технічних засобів захисту;

- винесення рішень в управлінні ризиками посилаючись на попередні оцінювання;

- власне проведення роботи з управління ризиками [4].

Загалом проблематика в сфері аналізу ризиків поділяється на дві групи. У першій знаходяться методи розроблення наукових методів для аналізу ризиків на основі загальновідомих теорій та вимог стандартів для створення системи управління інформаційною безпекою. У другій групі містяться спеціалізовані програмні продукти, що базуються на методах, що відносяться до першої групи, проте мають більш практичний характер та краще враховують структурну специфіку об’єкта захисту інформації.

Серед сформованих шляхом розвитку інформаційних технологій існуючих загроз, одну з найважливіших ролей відіграють засоби впливу на структуру інформаційно-телекомунікаційних систем та захищеність інформаційного ресурсу.

В відповідності з стандартами ISO/IEC TR 13335-2 та ISO/IEC 27005, процес оцінки інформаційних ризиків можна розділити на декілька етапів:

- оцінку імовірності загроз та уразливостей;

- обчислення рівня впливу, що несе певну загрозу кожному активу;

- визначення кількісної (виміряної) або якісної (описуваної) вартості ризику.

Оцінювання ризиків — це визначення якісних показників, обчислення кількісних показників, створення реєстру ризиків та їх класифікації за степенем впливу на інформаційну безпеку [11].

Використовуваний вибраним продуктом метод оцінювання ризиків інформаційної системи в інформаційно-телекомунікаційних системах має зрозумілим чином зображувати процес формування звітів про результати, оскільки ефективне використання продукту неможливе без доброго розуміння всіх його функцій та можливостей, а також від правильності виконаного перед тим встановлення та налаштування [11].

В розробці методу оцінки ризиків інформаційної безпеки в обов'язковому порядку має бути проведене визначення вже існуючого та граничнодопустимого ризику виникнення цих загроз протягом певного часу. Для цього потрібно обрахувати вірогідності виникнення цих загроз протягом певного інтервалу часу [12]. На практиці бачимо, що для більшості загроз інформаційній безпеці неможливо отримати вірні дані про можливість реалізації загрози, і саме тому при вирішенні даної проблеми зазвичай використовують методи кількісної оцінки для визначення ризиків інформаційної безпеки. При розробці методики визначення інформаційних ризиків часто використовуються методи системного аналізу. Далі наведені основні методи визначення ризиків інформаційної безпеки, які є найбільш поширеними в інформаційно-телекомунікаційних системах установ для забезпечення захисту інформації і в тому числі визначення ризиків, які можуть найближчим часом перерости в потенційну загрозу.

При аналізі інструментальних методів для визначення інформаційних ризиків, що мають найбільше поширення для вирішення задач протистояння інформаційним загрозам в інформаційно-телекомунікаційних системах. Загалом схема інструментальних методів визначення інформаційних ризиків зазвичай має вигляд, який приведено на рис. 2.1.

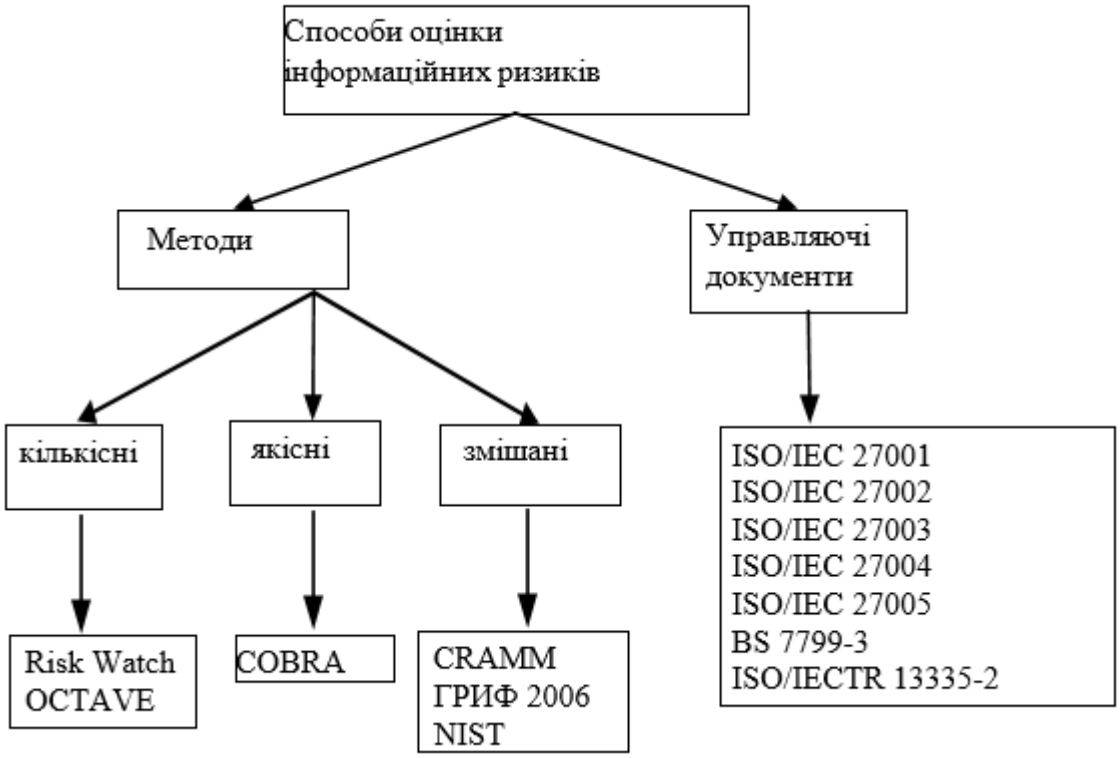

Рис. 2.1. Схематичний розподіл методів визначення ризиків в інформаційно-телекомунікаційних системах

Метод CRAMM – це інструментальний засіб для оцінки ризиків інформаційної безпеки.

Метод CRAMM розробили у службі безпеки Об'єднаного Королівства Великої Британії та Північної Ірландії та встановили як державний стандарт. Основою цього методу є ідея комплексного підходу до оцінки ризиків та поєднання кількісних та якісних методів аналізу. Даний метод універсальний та підходить для великих, середніх та малих організацій. Забезпечує отримання потрібних висновків при обчисленні витрат установи на забезпечення інформаційної безпеки [9].

Інтерфейс методу CRAMM наведено на рис. 2.2.

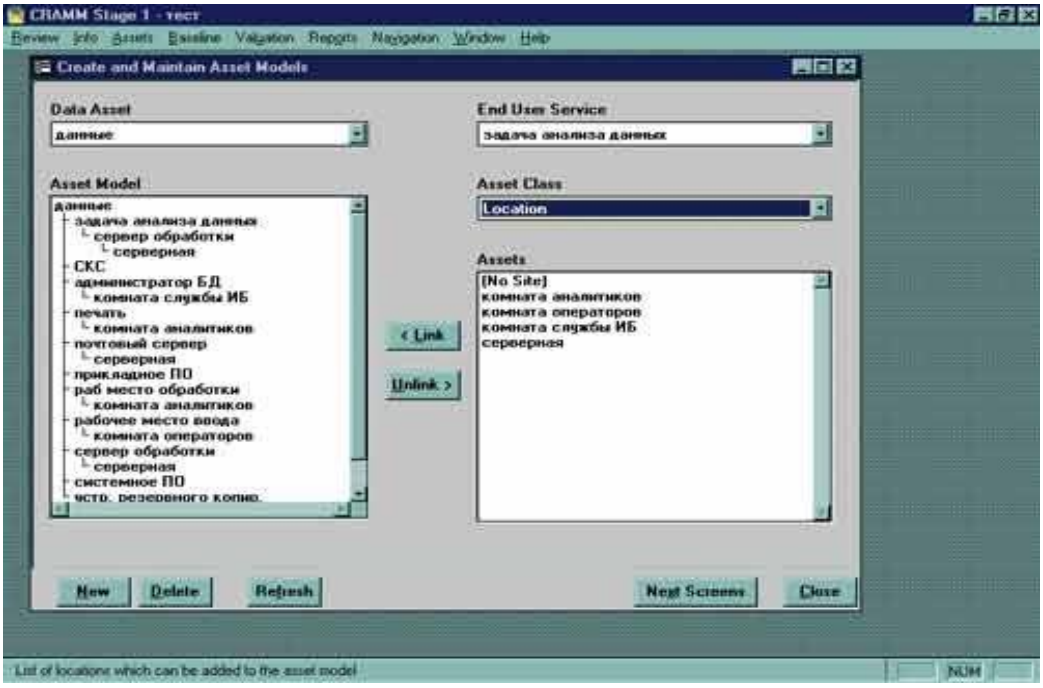

Рис. 2.2. Приклад інтерфейсу методу CRAMM

В методі CRAMM закладено великий набір типових рекомендацій на рахунок проведення контрзаходів з метою зменшення ризиків інформаційної безпеки інформаційно-телекомунікаційних систем, проте ефективне використання даної методики можливе лише в випадку використання її фахівцями вищої кваліфікації.

Даний метод містить цілу базу даних присвячену ризикам, їх видам, способам мінімізації, а також засоби для збору інформації стосовно них, сформування потрібних при аналізі звітів і виконує серію алгоритмів з метою обрахунку величини ризику [11].

Методом CRAMM пропонується усі процедури даного методу розділити на три послідовних етапи. Дані етапи розглянуто на рис. 2.3.

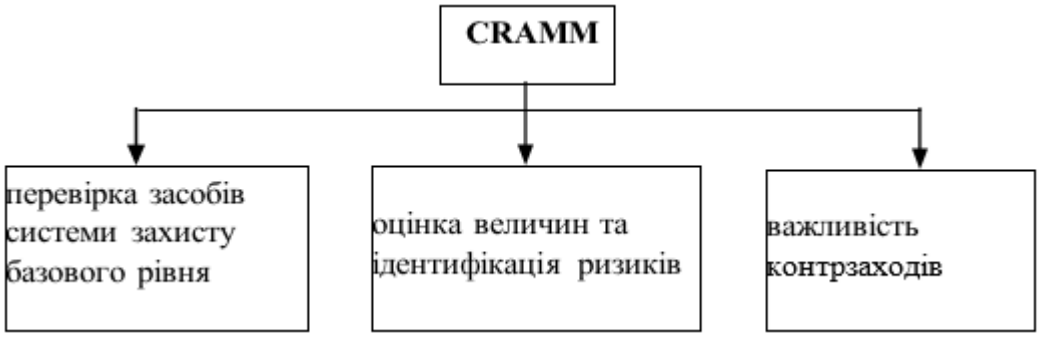

Рис. 2.3. Етапи проведення аналізу ризиків інформаційної безпеки методом CRAMM

До переваг методу CRAMM можна віднести:

- універсальність та можливість використання даної методик як в державних, так і в комерційних цілях;

- даній методиці притаманні кількісні та якісні властивості оцінки інформаційних ризиків;

- оптимальний рівень споживання витрат засобами захисту інформації;

- ефективність при вирішенні питань управління безпекою.

Недоліками методу CRAMM є:

- лише провідні фахівці можуть використовувати даний метод на відповідному рівні;

- вимагає від користувача великий обсяг часу та зусиль для опрацювання інформації;

- відсутня можливість модернізації бази даних шляхом внесення додатків в неї;

- використовує лише методи, розраховані на зменшення рівню ризиків інформаційної безпеки;

- програмне забезпечення, що реалізує цей метод є пропрієтарним (вартість від $1950 до $4900) [3].

Наступним програмним забезпеченням, який ми розглянемо, є експертна система Risk Watch. Дане програмне забезпечення презентує себе як продуктивний засіб аналізу та управління інформаційними ризиками.

Програмний продукт Risk Watch структурований на програмному ядрі загального призначення і створений для управління різними видами ризиків при підтримці багатьох стандартів [11].

Інтерфейс даної системи представлено на рис. 2.4.

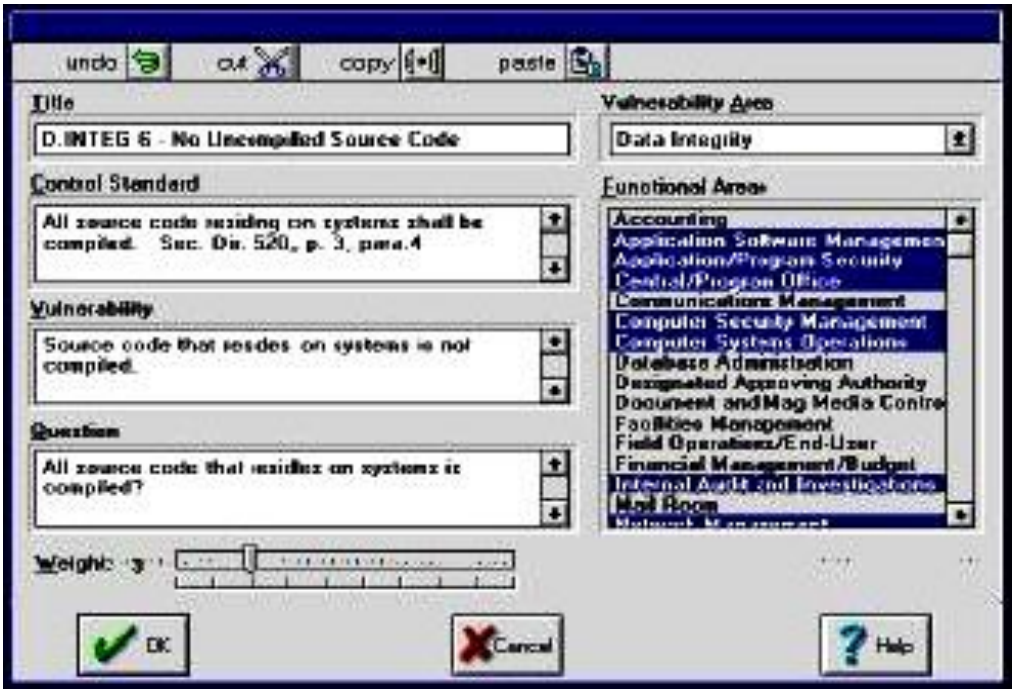

Рис. 2.4. Інтерфейс методу Risk Watch

В результаті проведеного аналізу системи Risk Watch я дійшов висновку, що відношення трудомісткості робіт до обсягу витраченого часу цим методом порівняно невелика. З погляду звичайного споживача основною перевагою Risk Watch є його простота, легка лінгвістична адаптація інтерфейсу і велика гнучкість в роботі. Саме це забезпечує можливість створення унікальних профілів захищеності та є одною з основних переваг цього методу.

Система аналізу та управління інформаційними ризиками Risk Watch допомагає зробити обґрунтований перелік заходів і засобів захисту інформаційної безпеки в інформаційно-телекомунікаційних системах. Даний метод дозволяє провести аналіз інформаційних ризиків і складається з чотирьох етапів [5]. Дані етапи проведення аналізу ризиків інформаційній безпеці представлено на рис. 2.5.

В результаті проведених досліджень в використанні методу Risk Watch можна констатувати, що не зважаючи на відчутні переваги для пересічного користувача, дана методика має й ряд недоліків, таких як:

- метод не ефективний при проведенні аналізу ризиків при урахування організаційних і адміністративних чинників;

- дуже дорога ліцензія, а саме $15000.

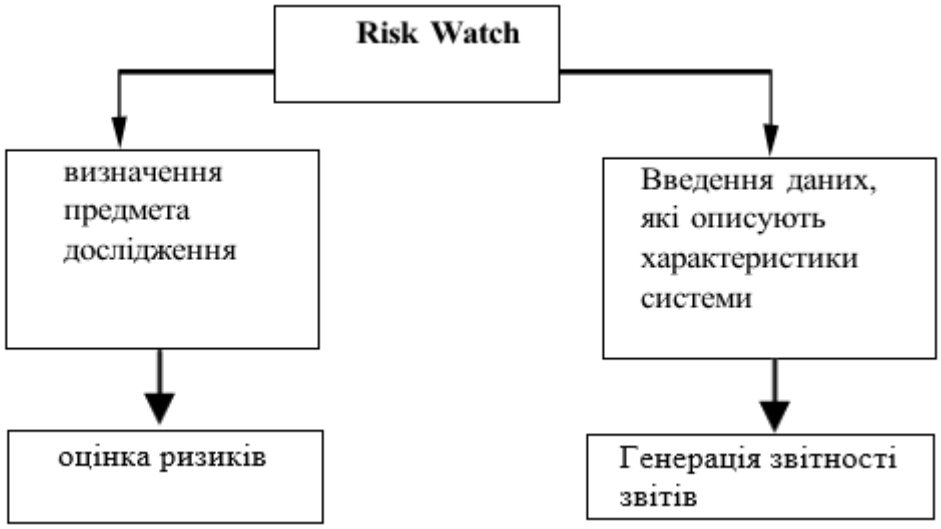

Рис. 2.5. Етапи проведення аналізу ризиків інформаційної безпеки методом Risk Watch

При побудові моделі автоматизованої системи, з точки зору інформаційної безпеки, актуальним є інструментальний метод ГРИФ 2006, який вирізняється дуже простим інтерфейсом.

Основною метою цього методу є можливість дати користувачу інструменти для самостійної оцінки рівня ризиків в інформаційних, для оцінки ефективності існуючої практики в сфері забезпечення безпеки системи. Визначення рівня ризиків за методом ГРИФ 2006 визначає кілька етапів роботи, що розглянуто на рис. 2.6.

В методі ГРИФ 2006 присутній модуль управління ризиками, який в свою чергу надає потужності для аналізу всіх причин значення ризику, отриманий

внаслідок обробки алгоритмів, які були внесенні в ході роботи для отримання заключних даних.

Знаючи що спричиняє інформаційні ризики, користувач володітиме абсолютно всіма нюансами необхідними для реалізації мір у відповідь [8].

Рис. 2.6. Характеристика етапів методу ГРИФ 2006 для проведення оцінки рівню ризиків

В результаті виконаної роботи в інтерфейсі ГРИФ 2006 формується звіт рівня ризиків в системі, які включають в себе причини виникнення даного ризику та, відповідно, аналіз уразливостей з економічною оцінкою ефективності всіх доступних даній установі контр мір.

До переваг методу ГРИФ 2006 можна віднести:

- простий в використанні програмний механізм для оцінки рівня ризиків в інформаційно-телекомунікаційній системі;

- можливість оцінки ризиків використовуючи різні інформаційні ресурси;

- ефективне втілення методів керування ризиками при виборі потрібних контрзаходів;

- доступність користування інтерфейсом користувачами без належного професійного рівня.

Недоліки методу ГРИФ 2006:

- відсутня функція прив'язки методів управління ризиками до бізнес-процесів установи;

- відсутність можливості проведення моніторингу звітності на різних етапах розробки комплексу контрзаходів для забезпечення захищеності інформації.

На рис. 2.7 продемонстровано інтерфейс даного методу.

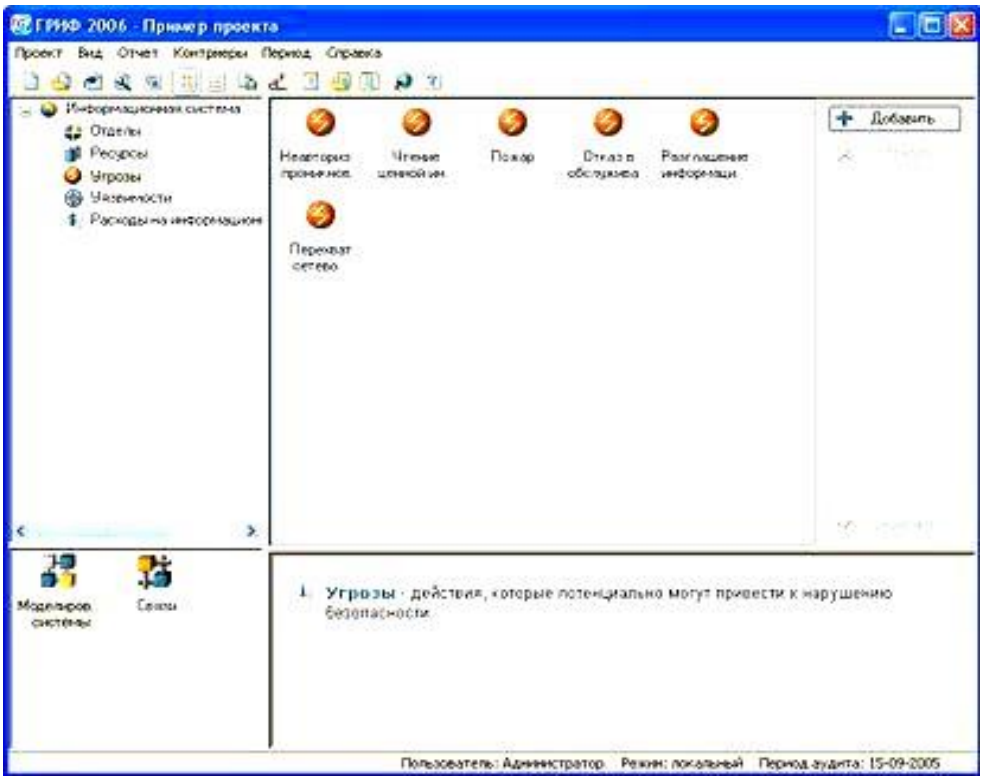

Рис. 2.7. Інтерфейс методу ГРИФ 2006

Метод NIST - метод оцінки ризиків інформаційної безпеки Національного інституту стандартів США.

Даний метод вимагає попередньої оцінки двох параметрів:

- імовірність інциденту;

- потенційний збиток.

Подібний механізм здійснення оцінювання ризику досить сильно обмежує точність результатів, але забезпечує оперативність та відтворюваність. Реалізація загрози інформаційної безпеки в цьому методі вимагає виконання широкого кола завдань, але головним з них є розробка власної системи для управління ризиками [3].

Процес управління ризиками інформаційної безпеки, запропонований даним методом представлено на рис. 2.8.

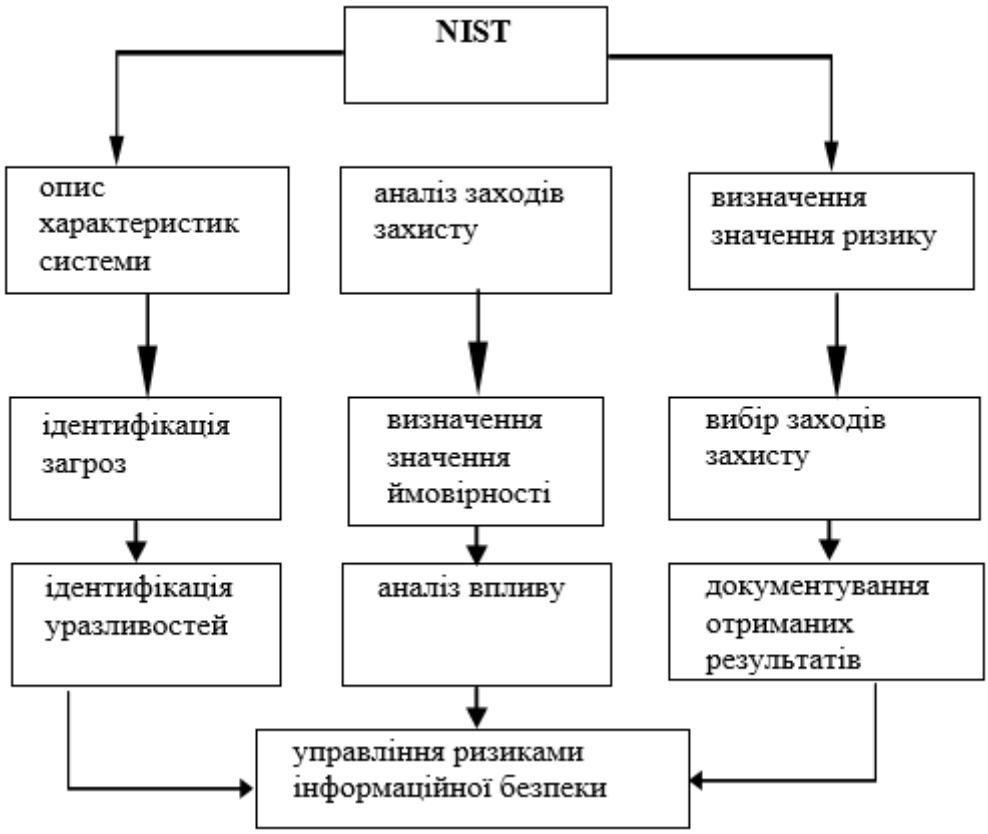

Рис. 2.8. Порядок роботи методу NIST по етапах

До переваг даного методу можна віднести:

- простота реалізації;

- детальний опис всіх можливих ризиків проаналізованих інформаційних активів;

- пропонує використання усіх можливих типів зниження ризиків таких, як перенесення, прийняття, уникнення ризику, зниження;

- відносно легке та зручне у використанні та застосуванні програмне забезпечення;

- порівняно мала вартість ліцензії з-поміж інших подібних експертних систем - $ 149 – $ 254.

Недоліки методу NIST:

- аналіз забирає багато часу;

- вимогливий до компетентності користувача в області інформаційної безпеки;

Інтерфейс даного методу продемонстровано на рис. 2.9.

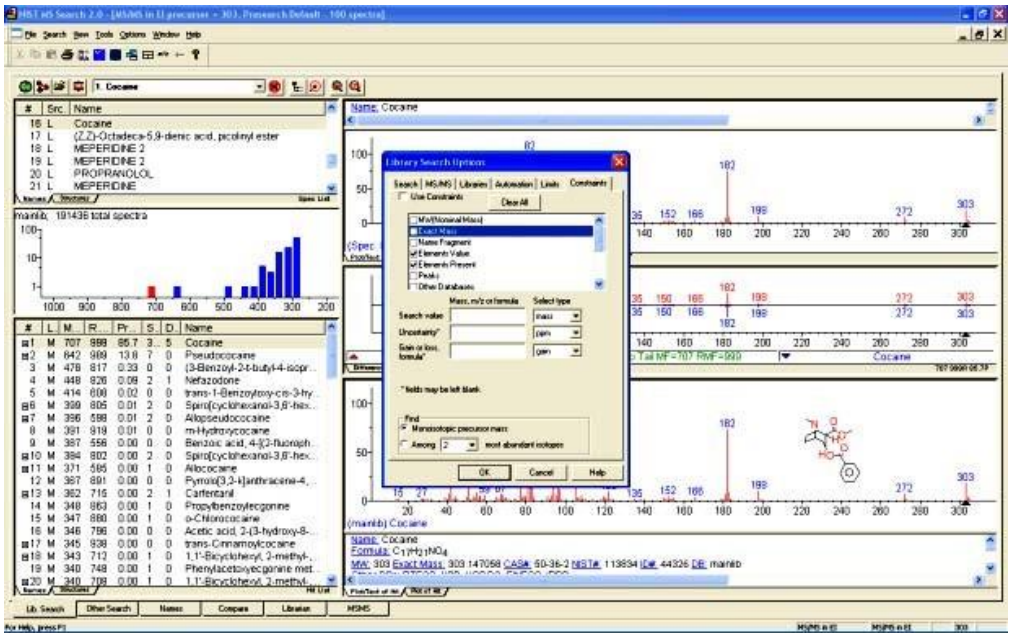

Рис. 2.9. Інтерфейс методу NIST

Цей метод є орієнтованим на всебічну підтримку вимог, що описані у стандарті ISO 17799. Комплект програмного забезпечення складається з модулів COBRA ISO 17799 Security Consultant, COBRA Policy Compliance

Analyst и COBRA Data Protection Consultant, а також менеджера модуля COBRA, що створений для налаштування та редагування вбудованої бази [10].

Даний метод дає змогу реалізувати в автоматизованому режимі найпростіші варіанти для оцінювання інформаційного ризику будь-якої установи. Він дає оцінку відносної важливості усіх загроз та вразливостей, проводить процес генерації відповідного рішення та рекомендацій для створення контрзаходів.

При виконанні цього завдання варто використовувати спеціалізовані бази знань в електронному форматі та засоби логічного виводу, що працюють у відповідності з стандартами [8].

Процес аналізу оцінки ризиків, в даному методі, проводиться розподілом на наступні категорії, які розглянуто на рис. 2.10.

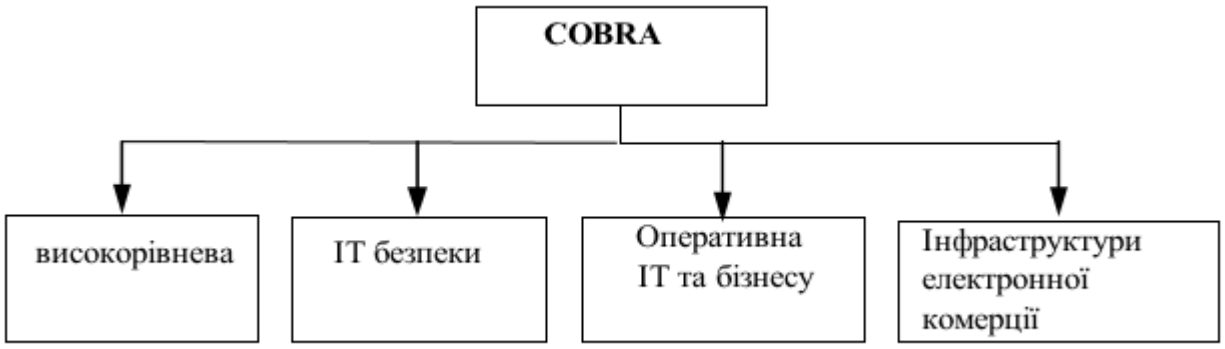

Рис. 2.10. Етапи оцінювання ризиків методу COBRA

Провівши процес опису даних категорій та створення структурованого переліку потенційних ризиків інформаційній безпеці, проводять контр міри, спрямовані на зниження шансу їх реалізації.

Внаслідок проведення аналізу системи COBRA стає зрозумілим, що аналіз інформаційних ризиків, який здійснений цим методом, є лише відповідністю базовому рівню безпеки, тобто при реалізації даного методу рівень небезпеки при втіленні в життя цих загроз не визначається, що є, мабуть, основним його недоліком.

До переваг методу COBRA можна віднести:

- простоту у використанні;

- прийнятну вартість.

Недоліки методу COBRA:

- незручний користувацький інтерфейс та відсутність підтримки спеціальних баз даних та процедур логічного виводу;

- визначається лише базовий рівень безпеки;

- нестабільна фаза генерації звітів та здебільшого нестабільна робота з застарілими операційними системами.

Інтерфейс методу COBRA представлено на рис. 2.11.

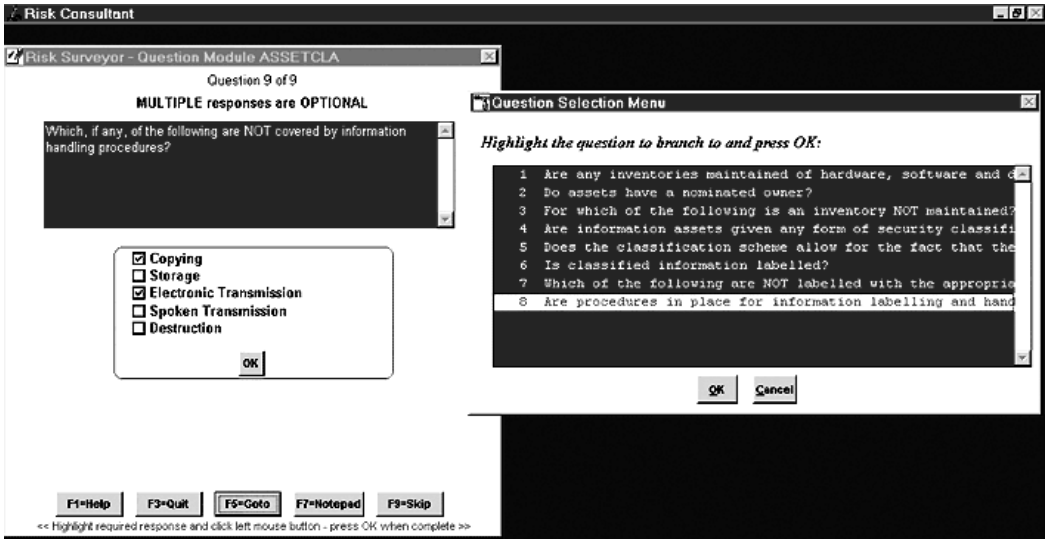

Рис. 2.11. Інтерфейс методу COBRA

Особливістю методу OCTAVE є те, що для оцінки ризиків використовуються лише працівники самої установи, без залучення фахівців з профільних організацій.

Цей метод складається з трьох фаз аналізу ризиків:

- створення профілю загроз, що пов’язані з активом;

- аналіз інфраструктури на наявність уразливостей;

- створення політики безпеки.

Метод OCTAVE передбачає створення профілю загроз і дерева варіантів. В профілі загрози містяться вказівники на актив, тип отримання доступу до активу, ядро даної загрози, мотив, результат, детальний опис загрози в загальнодоступних каталогах [3].

Даний метод в характеристиці профілю використовує «дерево варіантів». Подібне дерево представлено на рис. 2.12.

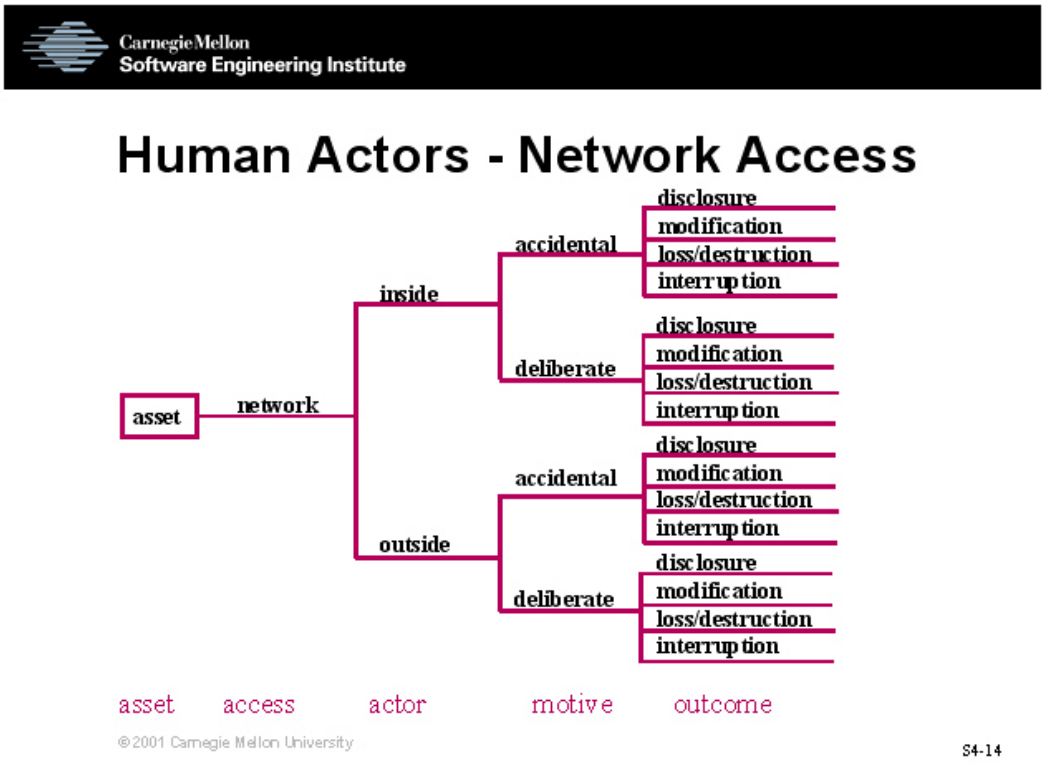

Рис. 2.12. Приклад дерева варіантів

Профіль загроз включає результат інвентаризації та оцінювання цінності активу, ідентифікації застосовних вимог законодавства та нормативно-правової бази, визначення організаційних заходів для збереження рівня підтримки режиму інформаційної безпеки [3].

Проаналізувавши методику OCTAVE можна зрозуміти, що цією експертною системою залюбки користуються у багатьох установах, виконуючи

оцінку ризиків інформаційної безпеки та впровадження процесів управління ризиками інформаційної безпеки в інформаційно-телекомунікаційних системах.

OCTAVE методи можна розділити на три типи, засновані на OCTAVE критеріях. Ці типи розподілені по застосуванню за розміром установ, в яких вони впроваджуються: OCTAVE Method (від 300 осіб і більше), OCTAVE-S (не більше 100 осіб) і OCTAVE Allegro (для малих підприємств, та відбувається без залучення фахівців).

Черговість етапів аналізу ризику за цим методом продемонстровано на рис. 2.13.

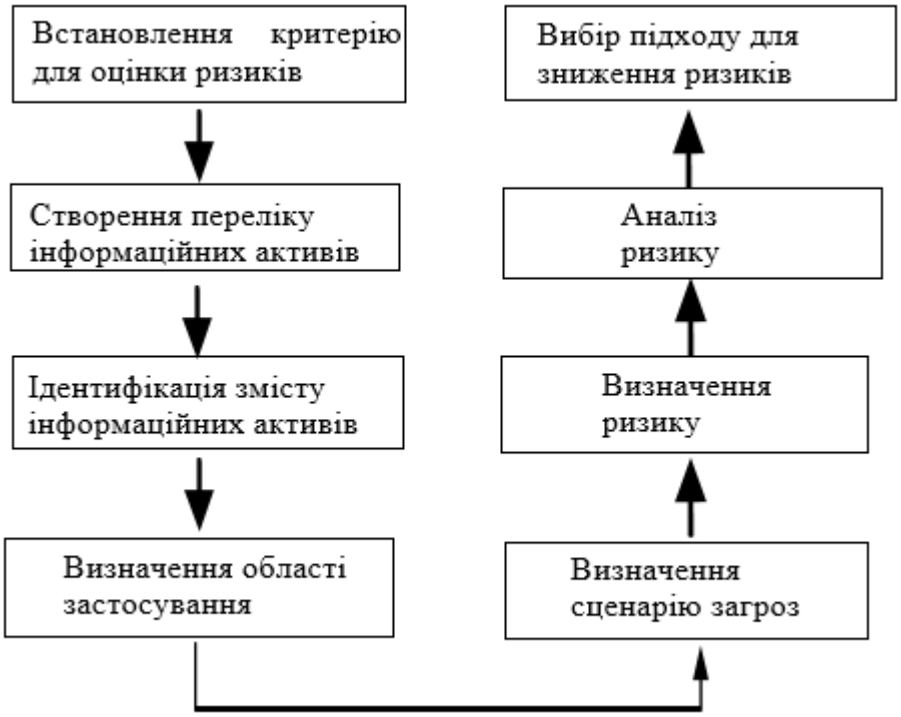

Рис. 2.13. Етапи аналізу ризику за методом OCTAVE

До переваг методу OCTAVE можна віднести:

- швидке впровадження;

- можливість застосування для установ різних розмірів та галузей функціонування;

- універсальність.

Недоліки методу OCTAVE:

- відсутня функція надання кількісної оцінки ризиків;

- вважає за можливе використання засобів зниження рівня ризиків та прийняття рішення;

- не актуальний в банківській сфері.

Інтерфейс методу OCTAVE представлено на рис. 2.14.

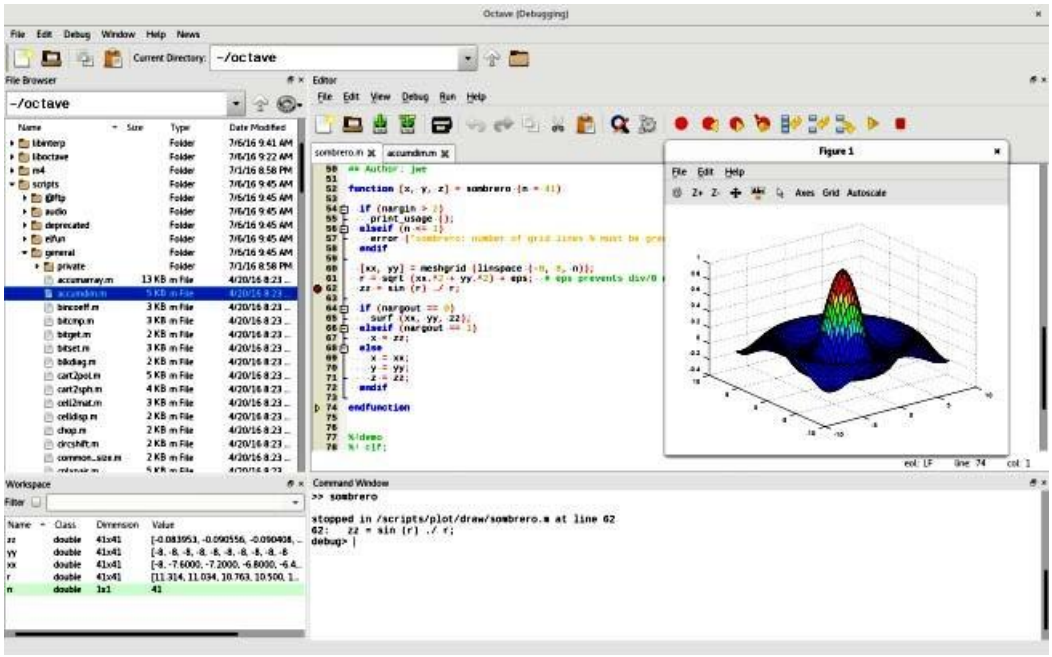

Рис. 2.14. Інтерфейс методу OCTAVE

2.2 Характеристика міжнародних стандартів з управління інформаційними ризиками

На сьогоднішній день існує окрема нормативно-правова база, що складається з документів, що регламентують питання інформаційної безпеки, і можуть розглядатися як основа для створення власних методів оцінювання інформаційних ризиків в інформаційно-телекомунікаційних системах [3].

Більша частина програмних експертних систем відповідають стандарту ISO/IEC 27001:2005. Дані стандарти формулюють вимоги до систем управління інформаційною безпекою, процесу управління ризиками, основні метрики і способи вимірювання, а також керування їх впровадженням [13].

Ключова модель, що використовується для керування ризиками інформаційної безпеки це модель, яка була відображена у всіх стандартних підходах до управління ризиками інформаційної безпеки і є основою ISO/IEC 27005 і BS 7799-3 [13].

В цій моделі вказано перелік та черговість використання ключових для управління ризиками інформаційної безпеки процесів, серед яких планування, реалізація, перевірка, дія. Згідно з цим стандартом вся документація, яка окреслює межі керування інформаційними ризиками установи, повинна включати:

- задокументовану заяву, або її копію, про політику та мету системи управління інформаційною безпекою;
- функціональної особливості програми системи управління інформаційною безпекою;
- процедури і інструменти управління для підтримки системи управління інформаційною безпекою;
- опис методики оцінки інформаційних ризиків;
- звітність по аналітичних оцінках ризиків;
- схеми використання контрзаходів.

Даний стандарт створений як модель для функціонування системи забезпечення інформаційної безпеки. Крім вищезгаданого міжнародного стандарту можна перерахувати ще багато схожих стандартів, які співіснують та взаємодоповнюють один одного у галузі забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах. Даний ряд стандартів розглянуто та детальніше охарактеризовано в табл. 2.1.

Стандарт	Назва стандарту	Коротка характеристика
ISO/IEC 27002-2012	Інструкція з менеджменту інформаційної безпеки для телекомунікацій них організацій	Цей стандарт надає додаткові рекомендації з реалізації та менеджменту інформаційної безпеки в телекомунікаційних організаціях. Визначає вимоги оцінки ризику до системи інформаційної безпеки та забезпечує контроль управління. Діючий Міжнародний стандарт пропонує рекомендації та основні принципи введення, реалізацію, підтримку й поліпшення менеджменту ІБ.
ISO/IEC 27003-2012	Інструкція з реалізації системи менеджменту інформаційної безпеки	У цьому Міжнародному стандарті розглядаються найважливіші аспекти, необхідні для успішної розробки та впровадження в СМІБ відповідно зі стандартом ISO/IEC 27001:2005, який розглядає процес визначення та розробку СМІБ від початку до стану впровадження
ISO/IEC 27004-2011	Менеджмент інформаційної безпеки вимірювання	Цей стандарт містить рекомендації з розробки та використання вимірювань і заходів вимірювання для проведення оцінки ефективності реалізованої СМІБ. Процес вимірювання реалізується у вигляді програми, пов'язаний з інформаційною безпекою. Програма вимірювань надає допомогу користувачу у виявленні і оцінюванні вимог, яким не відповідає процес ефективності контролю і управління СМІБ
ISO/IEC 27005-2010	Менеджмент ризику інформаційної безпеки який конкретизує поняття інформаційного ризику	Цей стандарт поданий у вигляді додатку прикладу типових загроз, уразливостей та потреб інформаційної безпеки. Проблема оцінювання та дослідження інформаційних ризиків насамперед асоціюється з британським стандартом BS 7799, а саме з його двома частинами: першою — BS 7799-1 «Звіт правил з менеджменту безпеки інформації» та другою — BS 7799-2 «Системи менеджменту безпекою інформації», у яких вперше питання аналізу стану безпеки інформації та формування її захисту були напряму пов'язані з інформаційними ризиками. Однак, безпосередньо, аспекти оцінювання та управління ризиками були докладніше розглянуті у третій частині стандарту BS 7799-3 «Настанови з менеджменту ризиками безпеки інформації»
ISO/IEC TR 13335-2:1997	Настанови з керування безпекою інформаційних технологій (IT)	Надати рекомендації, а не конкретні рішення з керування безпекою інформаційних технологій (IT). Кваліфікація осіб, відповідальних за безпеку IT у межах організацій повинна бути достатньою для адаптування матеріалів, поданих у цьому стандарті, до конкретних потреб організацій

Таблиця 2.1 Міжнародні стандарти з управління інформаційними ризиками

При аналізі основних міжнародних стандартів BS 7799-3 і ISO/IEC 27005, ми бачимо, що в них визначаються всі важливі нюанси, так чи інакше взаємопов'язані з інформаційними ризиками. Ця риса є спільною і для процесної моделі та елементів управління ризиками, для методів аналітичного визначення ризиків та для способів опрацювання цих ризиків. Стандарт BS 7799-3 не виключає можливості використання якісних і кількісних методів оцінки ризику водночас. Характерною особливістю даного стандарту є принцип усвідомленості процесів оцінювання, їх обробку, контроль ризиків в організації та оптимізацію ризиків [11]. Виходячи з цих даних, можна сформувати порівняльну таблицю експертних систем оцінювань ризиків – таблиця 2.2.

Таблиця 2.2 Порівняння експертних систем оцінювання ризиків

Критерії порівняння	CRAMM	Risk Watch	ГРИФ 2006	NIST	COBRA	OCTAVE
Відповідність стандартам ISO 2700x	+	+	+	+	+	+
Оцінка захищеності	+	+	+	+	+	+
Швидкодія	+	–	+	–	+	+
Облік послідовності контрзаходів при розрахунку ризиків	+	–	+	+	+	–
Визначення рівня ризиків для різних моделей ІТС	+	-	+	-	+	-
Можливість завдання власних контрзаходів	+	+	–	–	+	–
Оцінка аналізу ризиків	Змішана	Кількісна	Змішана	Змішана	Якісна	Якісна
Наявність ліцензії	+	+	+	+	+	+
Вартість	2000 - 5000 дол.США	Від 15 000 дол. США	Від 1000 дол. США	149–254 Дол США	7200–16 000 грн.	Від 2000 дол. США
Зручність інтерфейсу	Не зручний	Не зручний	Зручний	Не зручний	Зруний	Зручний
Необхідність спеціальної підготовки для роботи з засобами	+	+	+	+	–	–
Складність визначення ризику	Складна	Складна	Не дуже склад-на	Не дуже складна	Не дуже складна	Не складна
Оперативність визначення ризику	+	–	+	–	+	+

Проаналізувавши методом порівняння вищенаведені інструментальні засоби оцінювання ризиків, можна визначити найпоширеніші недоліки, серед яких можна виділити:

- складний процес отримання даних – потрібно довший час, ретельно оцінювати зміни в системі для отримання коректних результатів;

- при постійному оновленні програмного забезпечення, інформаційне середовище, в якому проходить процес аналізу, зазнає відчутних змін, в порівнянні з первинним виглядом

- витрати часу для проведення аналітики, здебільшого не відповідає вимогам шо до швидкості реагування на виявлені.

Якщо ж говорити про кількісні методи оцінювання інформаційних ризиків, можна зробити висновки, що дані методи досить таки не точні, та зовсім не надійні. І ось основні причини:

- для кількісної оцінки дуже складно зібрати актуальні дані, що пов’язано з потребою їх точної реєстрації на великому проміжку часу;

- сучасне інформаційне середовище швидко змінюється в зв’язку з невпинним вдосконаленням програмного забезпечення

- час, витрачений для аналізу зазвичай досить великий.

2.3 Опис методу OCTAVE Allegro

Метод OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), розроблено в стінах університету Карнегі-Меллон у травні 2007 року. Методика використовується для якісної оцінки ризиків інформаційної безпеки.

Нас цікавить найактуальніша на даний момент в ряді OCTAVE методологія, а саме OCTAVE Allegro. Метод має на меті узагальнення та оптимізацію процесу оцінювання ризиків інформаційної безпеки установи та забезпечити можливості отримання необхідних результатів, при цьому, з

мінімальною витратою ресурсів. Працівники, технології, інформаційні системи, об'єкти, що відносяться до інформації чи сфери інформаційних послуг, в межах якої вони знаходяться, розглядаються методом окремо. Оцінка ризиків проводиться персоналом та кваліфікованими спеціалістами, що є відповідальними за інформаційну безпеку на семінарах.

Згідно методики OCTAVE Allegro, управління ризиками інформаційної безпеки складається з восьми етапів, а також, допоміжний етап визначення пріоритетів.

На першому етапі проводиться визначення критеріїв вимірювання ризиків, які являються набором якісних параметрів, які і використовують для оцінки ризиків. Дані параметри також цілком можуть оцінювати імовірність виникнення ризику, можливі збитки чи інші наслідки для установи чи організації. Окрім того, на цьому етапі виділяються найбільш критичні напрями діяльності установи чи організації, для яких додатково можна встановити певні рівні прийнятного ризику.

На другому етапі здійснюють розробку профілів для IT-активів установи чи організації. Профіль — це опис активу, який включає унікальні характеристики, певні особливості та якості інформаційної безпеки, а також цінність і вимоги. Профіль кожного активу вказується на одному аркуші, які формують основу для подальшого процесу визначення загроз і ризиків.

На третьому етапі визначається оточення IT-активів, тобто проводиться опис місця, де обробляють, передають чи зберігають активи. Всі ризики оточення передаються на самі активи, що особливо актуально для активів, що надаються організації чи установі зовнішніми постачальниками.

Четвертий етап передбачає визначення областей для занепокоєння. Цей етап починає процес визначення ризиків за участі всієї проектної команди, шляхом визначення високорівневих областей та типів ризиків для IT-активів, які є об'єктом аналізу.

Під час п`ятого кроку проводиться визначення сценаріїв реалізації загроз.

Даний метод виділяє наступні типи загроз:

- користувацькі помилки під час використання технічних засобів;

- помилки користувачів під час фізичного доступу до активів;

- технічні чи проблеми іншого характеру.

Для всіх IT-активів можна визначити сценарії реалізації загроз, завдяки виділенню цих типів загроз, і описати їх можливий вплив на актив та визначити імовірність їх реалізації, яка вимірюється за трибальною шкалою. Для спрощення даний метод пропонує використовувати спеціальні опитувальники.

Шостий етап вміщує процес визначення ризиків на основі інформації про найімовірніші сценарії реалізації загроз, а також проводиться аналіз їх впливу на активи установи чи організації.

На сьомому етапі проводиться аналіз ризиків на основі інформації, що була отримана під час проведення попередніх етапів, а також здійснюється оцінка впливу всіх визначених загроз на основний напрям діяльності установи чи організації. Окрім цього проводиться групування цих ризиків відповідно до визначених на першому етапі критеріїв.

І на останньому кроці обирається підхід для обробки ризиків, тобто визначається стратегії, що буде використовуватися для їх обробки. Це відбувається на основі визначеного рівня впливу цих ризиків на установу чи організацію.

На основі цього опису можна виділити наступні переваги методології OCTAVE Allegro під час його практичного застосування:

- простота та прозорість методу під час аналізу та оцінки ризиків, що дозволяє розпочати процес в найкоротші терміни, без тривалого дослідження методики та документації;

- ітеративність дозволяє поетапно збільшувати глибину та якість аналізу ризиків для інформаційної системи на основі реальних потреб установи чи організації та доступних їй ресурсів;

- прийнятні трудовитрати на процес аналізу та оцінки ризиків роблять можливою їх реалізацію з використанням мінімальних ресурсів та короткі терміни;

- можливість повторення результатів спрощують реалізацію цих процесів для їх виконавців.

Проте, варто зазначити що методу OCTAVE Allegro притаманні наступні недоліки:

- не дозволяє оцінити ризики в грошовому еквіваленті, що суттєво використання методу в створенні техніко-економічного обґрунтування, визначенні необхідних інвестицій на введення в використання засобів захисту в установі чи організації;

- в методології відсутні допоміжні матеріали, а саме каталоги з загрозами, вразливостями, їх можливими наслідками та заходами по забезпеченню інформаційної безпеки, що збільшують необхідність фахових знань для тих, хто виконує процеси аналізу та управління ризиками даним методом;

Попри це, методологія OCTAVE отримала широке застосування для проведення якісної оцінки та управління ризиками інформаційної безпеки. Найбільше вона підходить установам та організаціям, які проводять процес впровадження управління ризиками інформаційних безпеки вперше, та відчувають потребу в покроковому поділі цих ризиків в залежності від рівня їх впливу. Також, з використанням даного методу в установи чи організації є можливість проводити інтеграцію процесу управління ризиками ітеративно.

2.4 Висновки з розділу

В даному розділі розглянуто класифікацію програмних продуктів для аналізу ризиків інформаційної безпеки, таких як CRAMM, ГРИФ 2006, COBRA, Risk Watch, NIST, OCTAVE, описано їх переваги та недоліки, проведено аналіз актуальних міжнародних сертифікатів з управління інформаційною безпекою,

наведено чітку характеристику відповідності інструментальних методів цим стандартам. Також обґрунтовано вибір методу OCTAVE Allegro для проведення подальшого аналізу інформаційної безпеки Вищого навчального закладу.

Внаслідок даного дослідження було виділено ключові переваги методу для проведення даного типу робіт, такі як:

- простота використання;

- можливість проведення аналізу інформаційної безпеки виключно співробітниками, без залучення фахівців з профільних організацій;

- безкоштовна ліцензія та відкритість всієї документації даного методу.

Також було описано загальний план проведення дослідження.

3 АНАЛІЗ ІНФОРМАЦІЙНИХ РИЗИКІВ ТЕРНОПІЛЬСЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ ІМЕНІ ІВАНА ПУЛЮЯ

В даному розділі ми будемо аналізувати інформаційні ризики університету на прикладі кафедри кібербезпеки.

3.1 Етап визначення пріоритетів та профілювання IT-активів

Щоб визначити цінності активів кафедри, потрібно розділити їх на матеріальні (Am) і нематеріальні (Anm). Розподіл подано в таблиці 3.1.

Таблиця 3.1 Активи кафедри

№	Матеріальні активи (A_m)	№	Нематеріальні активи (A_{nm})
1.1	Електронно-обчислювальна техніка	2.1	Персональні дані викладачів та студентів
1.2	Периферія	2.2	Звітність
1.3	Мультимедійна техніка	2.3	Інша конфіденційна інформація

На першому етапі для визначених активів потрібно провести оцінку їх імовірної вартості або той грошовий еквівалент збитку, який може бути нанесений внаслідок розголошення, видалення або зміни даного активу.

Щоб полегшити процес оцінки ризиків інформаційної безпеки, виразимо вартість даних активів за допомогою балів. Шкала оцінки подана в таблиці 3.2.

Таблиця 3.2 Оцінка активів

№	Підстава для оцінки активу	Вартість активу (S_i)	№	Підстава для оцінки активу	Вартість активу (S_i)
1.1	Електронно-обчислювальна техніка	10 балів	2.1	Персональні дані викладачів та студентів	6 балів
1.2	Периферія	2 бали	2.2	Звітність	6 балів
1.3	Мультимедійна техніка	6 балів	2.3	Інша конфіденційна інформація	2 бали

3.2 Етап ідентифікації загроз

На другому етапі оцінки ризиків інформаційної безпеки проводимо процес визначення загроз інформаційним ресурсам та у відповідність їм ставимо вразливості. Дана відповідність подана в таблиці 3.3.

Таблиця 3.3 Загрози інформаційним ресурсам та відповідні їм вразливості

№	Загрози	Уразливості
1	Витік видової інформації	Відсутність жалюзі на вікнах
		Розташування ПК моніторами до вікон
2	Витік акустичної інформації	Відсутність генераторів шуму
3	Крадіжка носіїв інформації	Зберігання носіїв інформації за межами сейфа
		Відсутність системи контролю доступу
		Відсутність системи відеоспостереження
		Відсутність системи сигналізації
4	Витік інформації каналами ПЕМВН	Відсутність екранування кабельних комунікацій
5	Умисне знищення інформації	Відсутність затвердженого «Положення про розмежування доступу»
		Відсутність програмної системи розмежування доступу типу Secret Net
		Відсутність системи контролю доступу, КПП
		Відсутність затвердженого «Положення про захист конфіденційної інформації, що обробляється в організації»

Продовження таблиці 3.3

6	Ненавмисне знищення інформації	Відсутність системи резервного копіювання
7	Дії шкідливих програм	Не встановлено сертифіковане антивірусне програмне забезпечення
8	Віддалений запуск додатків	Відсутність засобів міжмережевого екранування
9	Стихійне лихо	Відсутність протипожежної системи
		Відсутність джерел безперебійного живлення

Також на даному етапі доцільно визначити імовірність реалізації загроз - Vry. Загрози та відповідні їм засоби нейтралізації подано в таблиці 3.4.

Таблиця 3.4 Загрози та відповідні їм засоби нейтралізації

№	Загроза	Засіб нейтралізації загрози	Чи присутній на об’єкті даний засіб захисту	
			Так	Ні
1	Витік видової інформації	Жалюзі на вікнах	+	
		Розташування ПК моніторами проти вікон	+	
2	Витік акустичної інформації	Генератор шуму		+
3	Крадіжка носіїв інформації	Сейфи для зберігання носіїв інформації	+	
		Система контролю доступу		+
		Система відеоспостереження		+
		Сигналізація		+

Продовження Таблиці 3.4

4	Витік інформації каналами ПЕМВН	Екранування провідних комунікацій	+	
5	Умисне знищення інформації	Система відеоспостереження		+
		Сигналізація		+
		Ґрати на вікнах	+	
		КПП		+
6	Ненавмисне знищення інформації	Облік доступу співробітників до конфіденційної інформації	+	
7	Дії шкідливих програм	Антивірусне сертифіковане ПО на ПК співробітників	+	
8	Віддалений запуск додатків	Засоби міжмережевого екранування	+	
9	Стихійне лихо	Протипожежна система	+	
		Джерела безперебійного живлення		+

3.3 Етап ідентифікації та обробки ризиків

Для визначення ризику інформаційної безпеки скористаємося формулою:

$$R = SiVry, \quad (3.1)$$

де Si - цінність активу; Vry - ймовірність реалізації загрози; R- ризик інформаційної безпеки.

В випадку наявності на об'єкті дослідження:

- всіх засобів захисту - Vry = 0;
- при наявності до 50% засобів захисту - Vry = 1;

- при наявності 50% засобів захисту - Vry = 5;
- в разі відсутності більше 80% засобів захисту - Vry = 10.

В опитувальній таблиці наведеній вище, ми бачимо, що відсутні 53% засобів захисту, отже, Vry = 5.

Оцінивши ступінь ризику, ми можемо сформувати план по його зниженню. Даний план наведений в таблиці 3.5.

Таблиця 3.5 План зниження ступеню ризику

V_{ry}	S_i	R	Величина ризику	План по зниженню ризику
1	2	2	Низька	Довготривалий
	6	6	Середня	
	10	10	Висока	
5	2	10	Низька	Не надто терміновий
	6	30	Середня	
	10	50	Висока	
10	2	20	Низька	Списки завдань на найближчий час
	6	60	Середня	
	10	100	Висока	

З наведених даних в таблиці 5, можна підсумувати, що план по зниженню ризику є індивідуальним для кожної імовірності реалізації загроз.

Тепер можна перейти до фінального етапу, а саме процесу оцінки ризику інформаційної безпеки по методиці OCTAVE Allegro. Результати даного дослідження наведені в таблицях 3.6 – 3.11.

Таблиця 3.6 Профіль активу

Актив організації	Електронно-обчислювальна техніка
Цінність активу, S_i	10

Імовірність реалізації загрози, V_{ry}	5

Продовження таблиці 3.6

Показник ризику інформаційної безпеки, R	50
Величина ризику	Висока
План по зниженню ризику	Не надто терміновий
Заходи для зниження ризику	Встановлення системи контролю доступу
	Встановлення системи відеоспостереження
	Встановлення сигналізації
	Встановлення джерела безперебійного живлення

Таблиця 3.7 Профіль активу

Актив організації	Периферія
Цінність активу, S_i	2
Імовірність реалізації загрози V_{ry}	5
Показник ризику інформаційної безпеки, R	10
Величина ризику	Низька
План по зниженню ризику	Не надто терміновий
Заходи для зниження ризику	Встановлення системи контролю доступу
	Встановлення системи відеоспостереження

	Встановлення сигналізації
	Встановлення джерела безперебійного живлення

Таблиця 3.8 Профіль активу

Актив організації	Мультимедійна техніка
Цінність активу, S_i	6
Імовірність реалізації загрози V_{ry}	5
Показник ризику інформаційної безпеки, R	30
Величина ризику	Середня
План по зниженню ризику	Не надто терміновий
Заходи для зниження ризику	Встановлення системи контролю доступу
	Встановлення системи відеоспостереження
	Встановлення сигналізації
	Встановлення джерела безперебійного живлення

Таблиця 3.9 Профіль активу

Актив організації	Персональні дані викладачів та студентів
Цінність активу, S_i	6
Імовірність реалізації загрози V_{ry}	5

Показник ризику інформаційної безпеки, R	30
Величина ризику	Середня
План по зниженню ризику	Не надто терміновий

Продовження таблиці 3.9

Заходи для зниження ризику	Встановлення генератора шуму
	Встановлення системи контролю доступу
	Встановлення системи відеоспостереження
	Встановлення сигналізація

Таблиця 3.10 Профіль активу

Актив організації	Звітність
Цінність активу, S_i	6
Імовірність реалізації загрози V_{ry}	5
Показник ризику інформаційної безпеки, R	30
Величина ризику	Середня
План по зниженню ризику	Не надто терміновий
Заходи для зниження ризику	Встановлення генератора шуму
	Встановлення системи контролю доступу
	Встановлення системи відеоспостереження

	Встановлення сигналізація

Таблиця 3.11 Профіль активу

Актив організації	Інша конфіденційна інформація
Цінність активу, S_i	2
Імовірність реалізації загрози V_{ry}	5

Продовження таблиці 3.11

Показник ризику інформаційної безпеки, R	10
Величина ризику	Низька
План по зниженню ризику	Не надто терміновий
Заходи для зниження ризику	Встановлення генератора шуму
	Встановлення системи контролю доступу
	Встановлення системи відеоспостереження
	Встановлення сигналізація

Насправді, методика OCTAVE Allegro не складний в користуванні метод якісної оцінки інформаційних ризиків. Вона дає змогу проведення процесу оцінювання персоналом будь-якої установи самостійно, без залучення фахівців з спеціалізованих організацій. Формуючи якісну оцінку системи безпеки можна виробити чіткий план проведення заходів для зниження ризиків. Аналізуючи проведену роботу, можна з впевненістю сказати, що система захисту інформацій кафедри знаходить в хорошому стані, а матеріальні та нематеріальні активи знаходяться під надійним захистом, хоча методи запобігання ризиків для перших та других дещо різняться між собою.

3.4 Висновки з розділу

В даному розділі проведено аналіз інформаційних ризиків університету, на прикладі кафедри кібербезпеки, визначено пріоритети та профілі IT-активів. Ми провели розподіл активів кафедри на матеріальні і нематеріальні, та дали оцінку вартості даних активів. Виходячи з цих даних провели процес визначення загроз інформаційним ресурсам та у відповідність їм поставили вразливості інформаційної безпеки. Також на даному етапі визначили імовірність реалізації загроз. Далі провели етап ідентифікації та обробки ризиків. Ми визначили ризик інформаційної безпеки та на основі отриманих даних розробили загальний план по зниженню ризику. В кінці провели процес оцінки ризику інформаційної безпеки для кожного з активів.

Результатом проведеного дослідження є профільні таблиці кожного активу. Загалом, інформаційна безпека кафедри в задовільному стані. Жоден з аспектів захисту інформації не потребує оперативного втручання, проте можна скористатись рекомендаціями для покращення стану системи інформаційної безпеки в перспективі. Актуальність даного плану по зниженню інформаційних ризиків наведено в техніко-економічному обґрунтуванні даної кваліфікаційної роботи.

4 АНАЛІЗ МІЖНАРОДНИХ СТАНДАРТІВ В ГАЛУЗІ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В останні кілька років у світі спостерігається тенденція до стандартизації складових систем управління в організаціях. Оцінка ризиків є зараз одним з найактуальніших напрямків у всіх сферах діяльності. Серед найбільш значущих з них є ризики інформаційній безпеці, такі як неадекватні або помилкові дії персоналу та внутрішні процеси.

У загальному випадку можна виділити наступні складові управління ризиками:

- моніторинг та оцінювання організаційних ризиків функціонування системи;
- моніторинг та оцінювання ризиків технічних засобів;
- прийняття рішення з управління ризиками на основі наявних оцінок;
- проведення безпосередньої роботи з управління ризиками.

Поступово відходить у минуле підхід, коли окремі вимоги нормативних актів та окремі проблеми інформаційної безпеки вирішуються в порядку виникнення. Багато компаній сьогодні приходять до того, що система захисту інформаційних ресурсів повинна будуватися, виходячи із загальноприйнятих норм і з урахуванням напрацьованих практик. Це допомагає уникнути розбудови інфраструктури інформаційної системи в «авральному режимі» під

будь-які вимоги і знижує рівень незапланованих витрат на обслуговування системи.

Сімейство Міжнародних Стандартів на Системи Управління Інформаційною Безпекою 27000 розробляється ISO/IEC JTC 1/SC 27. Це сімейство включає в себе Міжнародні стандарти, що визначають вимоги до системи управління інформаційної безпеки, управління ризиками, метрики і вимірювання, а також керівництво з впровадження. Даний розділ кваліфікаційної роботи я присвячу детальному опису двох стандартів, а саме ISO/IEC 27001:2013 та BS 7799-3:2017.

4.1 Стандарт ISO/IEC 27001:2013

Стандарт ISO/IEC 27001:2013 описує загальну методологію підходу до забезпечення інформаційної безпеки в організації і акцентує увагу на найбільш критичних складових інформаційної системи. Він охоплює елементи управління системою інформаційної безпеки, актуальні для всіх без винятку сфер бізнесу, такі як:

- політика інформаційної безпеки;
- розподіл відповідальності за інформаційною безпекою;
- проведення навчання в цій області;
- звітність по інцидентах;
- захист від вірусів;
- забезпечення безперервності роботи;
- контроль копіювання ліцензійного програмного забезпечення,
- захист архівної документації та захист персональних даних.

Цей стандарт дає компанії інструмент, що дозволяє управляти конфіденційністю, цілісністю і збереженням такого важливого активу компанії

як інформація. Елементи управління системою інформаційної безпеки розділені в стандарті по декількох групах, і включають в себе розділи:

- політика безпеки - підтримка політики у сфері інформаційної безпеки з боку керівництва підприємства;

- інфраструктура системи безпеки - створення організаційної структури, яка буде забезпечувати працездатність системи інформаційної безпеки в організації;

- класифікація ресурсів і управління - пріоретизація інформаційних ресурсів за ступенем їх цінності і розподіл відповідальності за них;

- співробітники - зниження ризику людських помилок, крадіжки і неправильного використання устаткування;

- фізична і зовнішня безпека - запобігання несанкціонованого доступу та порушення роботи інформаційної системи організації;

- управління мережами і комп'ютерними ресурсами - забезпечення безпечного функціонування комп'ютерів та мереж;

- управління доступом - управління доступом до бізнес-інформації;

- розвиток та обслуговування системи - виконання вимог безпеки при створенні або розвитку інформаційної системи організації, підтримку безпеки додатків і даних;

- забезпечення безперервності бізнесу - план дій у разі надзвичайних обставин для забезпечення безперервності роботи організації;

- відповідність вимогам законодавства – виконання вимог відповідного громадянського та кримінального законодавства, включаючи закони про авторські права і захист даних.

Стандарт складається з двох частин: в першій частині описані механізми контролю, необхідні для побудови системи управління інформаційною безпекою. Ця частина використовується в якості основи для проведення аудиту системи інформаційної безпеки в організації. У другій частині стандарту описуються ті критерії, по яких проводиться сертифікація системи

інформаційної безпеки. Виходячи з ідеології стандарту ключовим елементом системи інформаційної безпеки є система управління ризиками, найважливішою частина яких є аналіз цих ризиків з метою визначення, які ресурси від яких загроз необхідно захищати, а також якою мірою ресурси потребують захисту. Проведення аналізу ризиків дозволяє організації оцінити можливі збитки в кількісних і якісних показниках. Цей міжнародний стандарт був підготовлений для того, щоб надати модель для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримання в робочому стані і поліпшення системи управління інформаційною безпекою. Передбачається, що прийняття системи інформаційної безпеки є стратегічним для організації. Стандарт приймає процесний підхід для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримання в робочому стані і поліпшення системи інформаційної безпеки організації.

Організація для того, щоб задовольнити вимоги даного стандарту, повинна зробити наступне:

- визначити область програми і межі системи управління інформаційною безпекою в термінах характеристик бізнесу, її місця розташування, активів і технологій, також включаючи - подробиці та обґрунтування будь- яких винятків з області застосування;

- визначити політику щодо системи управління інформаційною безпекою в термінах характеристик бізнесу, організації, її місця розташування, активів і технологій, захистом інформації, враховувати законодавчі, нормативні вимоги;

- визначати стратегії управління інформаційними ризиками;

- визначити підхід до оцінки ризику в організації;

- виявити ризики, а саме проаналізувати ризик та оцінити значущість ризику;

- виявити та оцінити можливості для обробки ризиків;

- вибрати цілі та засоби керування для обробки ризику.

Стандарт рекомендує проводити постійний контроль результативності системи управління інформаційною безпекою, аналіз цілей управління, беручи до уваги результати аудиту та статистику виникнення порушень.

У відповідності з стандартом ISO/IEC 27001 документація, яка визначає управління інформаційними ризиками організації, повинна включати в себе:

- документовану заяву про політику та цілі системи управління інформаційною безпекою;

- область програми системи управління інформаційною безпекою;

- процедури і засоби управління на підтримку системи управління інформаційною безпекою;

- опис методології оцінки ризиків;

- звіт про оцінки ризиків;

-план обробки ризиків.

В стандарті наголошується відповідальність керівництва в організації управління інформаційними ризиками. У розділі розглядаються види зобов'язань керівництва, деякі принципи менеджменту ресурсів і забезпечення необхідного рівня компетентності персоналу. Стандарт розглядає основні цілі та принципи проведення аудиту захищеності організації від загроз в інформаційній сфері, а також аналіз системи управління інформаційною безпекою з точки зору керівництва. У стандарті зазначено основні вхідні і вихідні дані для внутрішнього аудиту. В якості важливих результатів аудиту можна виділити оновлення оцінки ризиків для організації та відповідно зміну методів управління ними. Заключна частина стандарту присвячена принципу постійного поліпшення в системі управління інформаційною безпекою.

4.2 Стандарт BS 7799-3:2017

Стандарт Великобританії BS 7799 присвячений управлінню інформаційною безпекою організації. Цей стандарт є одним з найбільш

авторитетних в світі. На його базі розроблено міжнародний стандарт ISO/IEC 17799, котрий згодом еволюціонував в ISO/IEC 27002. Третя частина даного стандарту присвячена питанням управління інформаційними ризиками.

Стандарт BS 7799-3:2017 гармонізований з ISO/IEC 17799:2005 щодо прикладів по компонентах системи захисту. Стандарт допускає використання будь-яких стратегій організації оцінки ризиків, зокрема викладених у ISO 13335-3.

Стандарт BS 7799-3 містить вступну частину, розділи з оцінки ризиків, обробці ризиків, безперервним дій з управління ризиками, а також має додаток з прикладами активів, погроз, вразливостей, методів оцінки ризиків. Стандарт дотримується самого загального поняття ризику, під яким розуміють комбінацію ймовірності події і його наслідків. Управління ризиків сформульовано як скоординовані безперервні дії з управління та контролю ризиків в організації.

Оцінка ризиків - перший етап в управлінні системи інформаційної безпеки, призначеної для ідентифікації джерел ризиків і визначення його рівня значущості. Оцінку розбивають на аналіз ризиків та оцінювання ризиків. У рамках аналізу проводиться інвентаризація та категоризація ресурсів, що захищаються, з'ясовуються нормативні, технічні, договірні вимоги до ресурсів в сфері інформаційної безпеки, а потім, з урахуванням цих вимог, визначається вартість ресурсів.

Наступним етапом аналізу ризиків є складання переліку значущих загроз та вразливостей для кожного ресурсу та обчислення ймовірності їх реалізації. Стандарт допускає двояке тлумачення поняття загрози інформаційної безпеки: як умова реалізації вразливості ресурсу, і, як загальне, потенційна подія, здатна призвести до компрометації ресурсу. Оцінювання ризику проводиться шляхом його обчислення і порівняння з заданою шкалою. Обчислення ризику полягає в множенні ймовірності компрометації ресурсу на значення величини збитку, пов'язаного з його компрометацією. BS 7799-3 допускає використання як

кількісних, так і якісних методів оцінки ризиків, але, на жаль, в документі немає обґрунтування та рекомендацій по вибору математичного і методичного апарату оцінки ризиків інформаційної безпеки. Додаток до стандарту містить єдиний приклад, який умовно можна віднести до якісного методу оцінки. Даний приклад використовує трьох- і п'ятибальні оціночні шкали:

- оцінюються рівні вартості ідентифікованого ресурсу за п'ятибальною шкалою: «незначний», «низький», «середній », «високий», «дуже високий»;

- оцінюються рівні можливості загрози за три- бальною шкалою: «низький», «середній », «високий»;

- оцінюються рівні ймовірності вразливості:
«низький», «середній », «високий»;

- за заданою таблицею розраховуються рівні ризику;

- проводиться ранжування інцидентів за рівнем ризику.

Після того як ризик оцінений, повинно бути ухвалено рішення щодо його обробки – точніше, вибору та реалізації заходів та засобів з мінімізації ризику. Крім оціненого рівня ризику, при прийнятті рішення можуть бути враховані витрати на впровадження та супровід механізмів безпеки, політика керівництва, простота реалізації, думка експертів та ін.

У результаті обробки ризику залишається так званий залишковий ризик, щодо якого приймається рішення про завершення етапу відпрацювання ризику. На жаль, в стандарті BS 7799-3 нічого не сказано про ефективність заходів, засобів і сервісів, які можуть бути використані при обробці ризику.

Розділ 7 BS 7799-3 «Безперервна діяльність з управління ризиками» відповідає на наступні дві фази менеджменту системи: контроль ризику та оптимізація ризику. Для контролю ризику рекомендуються технічні заходи, аналіз з боку керівництва, незалежні внутрішні аудити інформаційної безпеки. Фаза оптимізації ризику містить переоцінку ризику і, відповідно, перегляд політик, керівництва з управління ризиками, корегування та оновлення механізмів забезпечення безпеки.

Процедури контролю ризиків і оптимізації, включаючи використання політик, заходів і засобів безпеки, ідентифікацію ресурсів, загроз та вразливостей, документування, гармонізовані з ISO/IEC 27001 та 27002. Відмінною рисою стандарту є принцип обізнаності про процеси оцінки, відпрацювання, контролю та оптимізації ризиків в організації. На кожному етапі управління ризиками передбачено інформування всіх учасників процесу управління безпекою, а також фіксування подій системи управління інформаційною безпекою. Стандарт перераховує обов'язки і задає вимоги до категорії осіб, що безпосередньо беруть участь при управлінні ризиками, а саме:

- експертам з оцінки ризиків;
- менеджерам з безпеки;
- менеджерам ризиків безпеки;
- власникам ресурсів;
- керівництву організації.

Основними видами інформаційних активів, які зачіпаються при управлінні інформаційними ризиками, відповідно до документа, є: процеси та служби інформаційної системи; програмне забезпечення; технічні засоби; людські ресурси; нематеріальні ресурси - репутація, імідж організації, а також інші нематеріальні фактори, що впливають на ведення бізнесу.

Наведений у стандарті метод оцінки ризиків є універсальним, але при цьому не передбачає використання якоїсь певної методології оцінки ризиків. Це породжує певну неоднозначність у виборі методів управління ризиками. В основі наведеного в стандарті методу оцінки зазвичай лежать зважені якісні оцінки. Природно, такий метод не позбавлений недоліків, а саме:

- проблеми завдання масштабу при побудові якісних шкал;
- проблеми адекватності експертної оцінки;
- неможливості визначити, які параметри системи і якою мірою впливають на загальний рівень ризику.

Це ускладнює управління ризиками та говорить про актуальність розробки універсальної методології оцінки та управління інформаційними ризиками, яка б дозволяла спільно використовувати аналітичні та якісні методи.

4.3 Висновки до розділу

В даному розділі кваліфікаційної роботи було проведено аналіз міжнародних стандартів, які регулюють процеси створення та впровадження систем управління інформаційною безпекою в організаціях. В підрозділі 4.1 розглянутий стандарт стандарт ISO/IEC 27001:2013, а в підрозділі 4.2 йдеться про стандарт стандарт BS 7799-3:2017.

5 ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

Метою даної кваліфікаційної роботи є дослідження методів та засобів захисту інформації та вибір найоптимальнішого з них. Головною метою розділу є встановлення економічної доцільності подальшого створення системи управління інформаційною безпекою.

5.1 Приклади технічних засобів захисту інформації

З проведеного в третьому розділі дослідження випливає, що для покращення системи інформаційної безпеки потрібно встановити наступні компоненти:

- генератор шуму;
- система контролю доступу;
- сигналізація;
- система відеоспостереження;
- ґрати на вікнах;
- джерела безперебійного живлення.

5.2 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{ві} = q_i \cdot p_i \,, \tag{5.1}$$

де: q_i – кількість витраченого матеріалу і–го виду; p_i – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{ві} \,. \tag{5.2}$$

Проведені розрахунки занесемо у таблицю 5.1.

Таблиця 5.1 Загальні матеріальні витрати

Найменування матеріальних ресурсів	Один. виміру	Норма витрат	Ціна за один., грн.	Загальна сума витрат на матер., грн.
1	2	3	4	7
Генератор шуму AD-31	штук	1	13780	13780
Замок Atis Lock SS	штук	5	710	3550
Безпровідний датчик руху Ajax MotionProtect	штук	5	1010	5050
Комплект відеонагляду HIKVISION DS-J142I/7104HGHI-F1 (4 OUT)	штук	1	4805	4805
Металеві ґрати на вікна	$м^2$	10	445	4450
Джерело безперебійного живлення APC Back-UPS Pro 1200VA (BR1200GI)	штук	2	10775	21550
			Разом:	53185

5.3 Розрахунок норм часу на виконання науково-дослідної роботи

Ефективне використання часу має велике значення тому, що коефіцієнт корисної дії залежить від оптимального використання часу.

Організацію системи захисту інформації можна розділити на декілька етапів, що дозволить полегшити і структурувати процес її впровадження.

Основні етапи впровадження:

- обґрунтування необхідності створення системи захисту інформації;
- обстеження середовища, в якому проводяться роботи з встановлення;
- визначення потенційних загроз інформації;
- розробка документів політики безпеки;
- складання плану захисту;
- підготовка до введення в дію системи;
- попереднє випробування системи захисту інформації;
- введення в дію системи захисту інформації.

Для оцінки тривалості виконання окремих робіт використовують нормативи часу. В даному випадку розглянемо тривалість встановлення засобів технічного захисту інформації. Виконавцями виступають як фахівці зовнішніх організацій, так і персонал університету, що зумовлено особливостями даної методики. Витрати часу по окремих операціях технологічного процесу відображені в таблиці 5.2.

Таблиця 5.2 Оцінка тривалості виконання робіт

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	обґрунтування необхідності створення системи захисту інформації	персонал	4

2.	обстеження середовища, в якому проводяться роботи з встановлення	фахівці	4
3.	визначення потенційних загроз інформації	персонал	4
4.	розробка документів політики безпеки	персонал	8
5.	складання плану захисту	персонал	8
6.	підготовка до введення в дію системи	фахівці	36
7.	попереднє випробування системи захисту інформації	фахівці	24
8.	введення в дію системи захисту інформації	фахівці	24
		Разом	112

5.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1–ці обладнання визначаються за формулою:

$$З_в = W \cdot T \cdot S, \qquad (5.3)$$

де W – необхідна потужність, кВт; T – кількість годин роботи обладнання; S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів (1,40 грн. + 20% ПДВ за 1 кВт). Отже, 1 кВт з ПДВ коштує 1,68 грн.

Потужність комп’ютера для створення проекту – 400 Вт. Комп’ютер потрібен для використання в пунктах 1,2,3,4,5. Загальна кількість використаного часу 28 годин.

Тоді, згідно з (5.3):

$$З_в = 0{,}4 \cdot 28 \cdot 1{,}68 = 18.82 \text{ грн.}$$

5.5 Оплата праці

При введені експлуатацію системи захисту інформації залучають фахівців з зовнішніх організацій. В таблиці 5.3 наведено час виконання операцій даними фахівцями.

Таблиця 5.3

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	обстеження середовища, в якому проводяться роботи з встановлення	фахівці	4
2.	підготовка до введення в дію системи	фахівці	36

Продовження таблиці 5.3

3.	попереднє випробування системи захисту інформації	фахівці	24
4.	введення в дію системи захисту інформації	фахівці	24
		Разом	88

При середній вартості погодинної оплати праці фахівців з встановлення систем захисту інформації 100 грн., можна обчислити витрати на залучення працівників з зовнішніх організацій. При використаному часі, наведеному в таблиці 5.3, розрахунки здійснюємо за формулою:

$$L = P \cdot t,$$

(5.4)

де t – використаний час, P – вартість погодинної оплати. В результаті, $L = 8800$ грн.

5.6 Складання кошторису витрат та визначення собівартості впровадження системи захисту інформації

Результати проведених вище обчислень зведемо у таблицю 5.4.

Таблиця 5.4 Визначення собівартості системи захисту інформації

Зміст витрат	Сума, грн.	В % до загальної суми
1	2	3
матеріальні витрати	53185	85,74
витрати на електроенергію	18,82	0,03

Продовження таблиці 5.4

оплата праці	8800	14,23
собівартість	62003,82	100,00

З проведеного аналізу цінності активів в третьому розділі, можемо розрахувати імовірні збитки шляхом присвоєння якісним показникам грошового еквіваленту. Використовуватимемо крок 1 бал = 5000 грн.

$$L = (S_1 + S_2 + \cdots S_n)V_{ry} \tag{5.2}$$

де: S_n – цінність активу; V_{ry} – ймовірність реалізації ризиків інформаційної безпеки (53% за підрахунками третього розділу).

Отже, L = 84800 грн., що доводить економічну обгрунтованість даної кваліфікаційної роботи, оскільки витрати на встановлення системи захисту інформації не перевищують вартості активів.

5.7 Висновки до розділу

В даному розділі я провів аналіз своєї роботи на економічну ефективність.

Було обчислено матеріальні витрати на встановлення системи захисту інформації, а саме створено перелік технічних засобів та опис їх середньої ринкової вартості. Далі було проведено поетапний аналіз виконання роботи, в ході якого було розподілено дані етапи виконання роботи між працівниками університету та фахівцями з зовнішніх організацій. Також підраховано час, витрачений на створення даної системи захисту інформації та вирахувано витрати на оплату праці запрошених працівників. В результаті проведеного аналізу було доведено раціональність використання даної методики, оскільки витрати на встановлення системи захисту інформації не перевищили цінність активу, який підлягав дослідженню.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Охорона праці

Згідно статті 8 Конституції України - основним правовим документом України є Конституція України. Конституція України має найвищу юридичну силу. Закони і інші нормативно-правові акти приймаються на підставі Конституції України і повинні відповідати їй. На підставі Конституції України прийнятий Закон України “про охорону праці”.

Згідно закону України "про охорону праці" ст.1, охорона праці - це система правових, соціально-економічних, організаційно-технічних заходів, а так само санітарно-гігієнічних і лікувально-профілактичних засобів, направлених на збереження здоров'я і працездатності людини в процесі праці.

Згідно ст.2 закону «про охорону праці» дія Закона "про охорону праці" розповсюджується на всі підприємства, установи і організації не залежно від форми власності і видів їх діяльності, на всіх громадян, які працюють, а також привернуті до праці на цих підприємствах.

Згідно ст.4 Закону України «про охороні праці» державна політика в області охорони праці визначається відповідно Конституції України Верховною Радою України і направлена на створення належних, безпечних і здорових умов праці, запобігання нещасним випадкам і професійним захворюванням.

За порушення законів і інших нормативно-правових актів про охорону праці, створення перешкод в діяльності посадовців органів державного нагляду за охороною праці, а також представників профспілок, їх організацій і об'єднань винні особи притягуються до дисциплінарної, адміністративної, матеріальної, кримінальної відповідальності згідно закону (ст. 44 Закону "про охорону праці").

Виходячи із загальних завдань в області охорони праці, в даному дипломному проекті розглядаються наступні завдання:

- характеристика робочого приміщення;
- мікроклімат робочого приміщення;
- освітлення приміщення;
- шум та вібрація у робочому приміщенні;
- оцінка електробезпеки;
- електромагнітне випромінювання.

Характеристика робочого приміщення.

В даному приміщенні є 2 робочих місця. Для зберігання документів використовується маленька тумба. Вікно розташоване навпроти робочих місць. Двері розташовані в куті приміщення. Повна характеристика виглядає так:

- довжина (a) – 5 метрів;
- ширина (b) – 5 метрів;
- висота (h) – 3 метра ;
- кількість робочих місць (n) – 2;
- площа (S) – 25 $м^2$;
- об’єм (V) – 75 $м^3$.

Порівнявши дані приміщення з вимогами до організації робочого місця [19], бачимо, що воно відповідає вимогам щодо охорони праці при організації роботи з ВДТ електронно-обчислювальних машин.

Мікроклімат робочого приміщення.

Згідно з ДСН 3.3.6.042-99 роботи, які виконуються користувачами електронно – обчислювальних машин відносяться до легких фізичних робіт категорії Іа, тому на даних робочих місцях мають забезпечуватись оптимальні значення параметрів мікроклімату.

Освітлення приміщення.

Згідно [20] приміщення повинне мати природне і штучне освітлення.

Природне освітлення приміщення відбувається за системою однобічного бічного освітлення. Природне світло проникає у приміщення через два вікна. Також наявні жалюзі з можливістю регулювання рівня освітленості. Вікна приміщення орієнтовані на схід. Всередині приміщення стіни та стеля білого кольору.

В даному приміщенні використовується система загального рівномірного штучного освітлення. Мається ряд світильників Л201Б 4х40-0.3, у кожному з яких знаходиться по чотири лампи типу ЛБ-40.

Для загального штучного освітлення нормуються такі параметри:

- найменша припустима освітленість - Е (лк);

- показник дискомфорту - М;

- коефіцієнт пульсації освітленості - Кп (%).

Визначимо фактичну освітленість в кабінеті з формули світлового потоку:

$$E_{\Phi} = \frac{\Phi_{л} \cdot \eta \cdot N}{S \cdot K_{З} \cdot Z}$$

(6.1)

де

N - число світильників у приміщенні, N = 4*4=16;

η - коефіцієнт використання світлового потоку;

Фл - світловий потік лампи;

Кз - коефіцієнт запасу, Кз = 1.5;

Z - коефіцієнт нерівномірності, Z=1.1 для люмінісцентних ламп;

S - площа приміщення;

Еф - фактична освітленість, створювана всіма світильниками.

Підвісна стеля білого кольору має коефіцієнт відбиття ρст = 0.5, стіни пофарбовані теж в білий колір -ρсн = 0.3.

Розрахуємо параметр і:

$$i = \frac{a \cdot b}{h(a+b)}$$

(6.2)

Для вказаного параметру і та коефіцієнтів відбиття стелі і стін коефіцієнт використання світлового потоку η=0,44.

Нормативне значення освітленості для кабінету, де працюють з використанням ВДТ, згідно таблиці Д.1 дод. Д ДБН В.2.5-28-2018 становить 200 лк. Допустимі межі відхилення 10%. Згідно формули (6.1) $E\phi$=180.9, що потрапляє в допустимі вдхилення.

Шум та вібрація у робочому приміщенні.

У приміщенні є такі джерела постійного шуму:

- вентилятори комп’ютерів,

- принтер,

- аудіо-система.

Зовнішніми джерелами шуму і вібрації в приміщенні є проїжджаючі транспортні засоби. Даний шум є постійним. Фактичний рівень шуму склав 48 дБА. Норма складає не більше 50 дБА, тому даний аспект покращення не потребує.

Оцінка електробезпеки.

Проаналізуємо стан електробезпеки в робочому приміщенні:

- напруга всіх приладів 220 В;

- проводка захована і ізольована;

- кожне робоче місце обладнане окремими розетками по 220 В;

- підлога ізолююча – лінолеум.

Проаналізувавши наведене вище, можемо сказати, що кабінет відноситься до приміщень без підвищеної електронебезпеки.

Електромагнітне випромінювання.

Джерелом електромагнітного випромінювання в сучасному офісі є візуальні дисплейні термінали. Нормування електромагнітного випромінювання здійснюється згідно положень ДСанПіН 3.3.2-007-98.

Джерелом електромагнітного випромінювання в приміщенні є 2 дисплеї SONY Powercolor 3220, які повністю відповідають міжнародному стандарту ТСО-03.

6.2 Фактори виробничого середовища і їх вплив на життєдіяльність людини

Деякі фактори праці, умови і види носять постійний характер при впливі на людину і пов'язані з його фізичним і психічним здоров'ям. Вони можуть впливати на здоров'я поряд з іншими соціальними чинниками.

Трудовий процес здійснюється в певних умовах виробничого середовища, що характеризуються сукупністю елементів та факторів матеріально-виробничого середовища, що впливають на працездатність та стан здоров'я людини в процесі роботи. Виробнича середовище й фактори трудового процесу становлять в сукупності умови праці.

На здоров'я людини, її життєдіяльність великий вплив мають небезпечні і шкідливі фактори.

Небезпека - це наслідок такої дії деяких факторів на людину, яке при їх невідповідності фізіологічним характеристикам останнього зумовлює феномен самої небезпеки.

Небезпечний фактор - це дія на людину, що в певних умовах призводить до травми, а в окремих випадках - до раптового погіршення здоров'я або до смерті.

Шкідливий фактор - це дія на людину, яке в певних умовах призводить до захворювань або зниження працездатності.

До значимих ознак небезпечних і шкідливих факторів відносяться наступні:

- можливість безпосередньої негативної дії на організм людини;

- ускладнення нормального функціонування органів людини;

- можливість порушення нормального стану елементів виробничого процесу, в результаті якого можуть виникнути аварії, вибухи, пожежі, травми.

Небезпечні та шкідливі фактори, що впливають на людину, діляться на три групи: активні, пасивно-активні і пасивні.

До активних належать фактори, що можуть вплинути на людину, впливаючи своєю енергією:

- механічні, що характеризуються кінетичною і потенціальною енергією і механічним впливом на людину;

- термічні, що характеризуються тепловою енергією та аномальною температурою;

- електричні: електричний струм, статичний електричний заряд, електричне поле, аномальна іонізація повітря;

- електромагнітні: радіохвилі, видиме світло, ультрафіолетові та інфрачервоні промені, іонізуючі випромінювання, магнітні поля;

- хімічні: їдкі, отруйні речовини, а також порушення природного газового складу повітря, наявність шкідливих домішок у повітрі;

- біологічні: небезпечні властивості мікро- і макроорганизмов, продукти життєдіяльності людей і інших біологічних об'єктів;

- психофізіологічні: стрес, втома та ін.

До пасивно-активної групи належать фактори, що активізуються за рахунок енергії, носіями якої є людина або обладнання: гострі нерухомі предмети, малий коефіцієнт тертя, нерівність поверхні, по якій переміщується людина і машина, а також нахил і підйом.

До пасивних належать ті фактори, які впливають опосередковано, небезпечні властивості яких пов'язані з корозією матеріалів, накипом, недостатньою міцністю конструкцій, підвищеними навантаженнями на механізми і машини та ін. Формою прояву цих факторів є руйнування, вибухи та інші види аварій.

Істотне значення для продуктивності праці і охорони здоров'я мають спрямованість виробничої діяльності, конкретні виробничі операції, знаряддя праці, форми організації праці та ін. Кожен з цих показників вимагає певних фізичних і психофізіологічних якостей.

Продуктивність праці, стан здоров'я та рівень працездатності людини значною мірою залежать від впливу факторів зовнішнього виробничого середовища.

Ці фактори окремо і особливо в комплексі можуть надавати несприятливий вплив на організм людини в процесі виробничої діяльності

Освітлення робочого місця - один з найважливіших факторів трудової діяльності. Головні проблеми, пов'язані з органами зору, на виробництві стосуються адекватності і зручності освітлення. Достатня (оптимальна) освітленість робочого місця позитивно впливає на органи зору, знижує втому. Незадовільне освітлення викликає передчасне стомлення, очні хвороби, головні болі і може бути причиною травматизму.

6.3 Висновки до розділу

В даному розділі було проаналізовано основні проблеми охорони праці, що можуть виникнути під час роботи працівника. Було виділено основні

вимоги до приміщення, мікроклімату в приміщенні, освітлення та основних ергономічних характеристик.

У приміщенні застосовується бокове природне освітлення та штучне (ряд світильників Л201Б 4х40-0.3, у кожному з яких знаходиться по чотири лампи типу ЛБ-40). Встановлено, що рівень електромагнітного випромінювання не перевищує норми. Зазначено, що приміщення за групою електронебезпечності відноситься до приміщень без підвищеної небезпеки ураження струмом.

Також окремо було розглянуто Фактори виробничого середовища і їх вплив на життєдіяльність людини. Небезпечні та шкідливі фактори, що впливають на людину, діляться на три групи: активні, пасивно-активні і пасивні.

До активних належать фактори, що можуть вплинути на людину, впливаючи своєю енергією:

- механічні;
- термічні;
- електричні;
- електромагнітні;
- хімічні;
- біологічні;
- психофізіологічні.

До пасивно-активної групи належать фактори, що активізуються за рахунок енергії, носіями якої є людина або обладнання.

До пасивних належать ті фактори, які впливають опосередковано життєдіяльність людини.

7 ЕКОЛОГІЯ

7.1 Інформаційне забезпечення еколого - статистичних досліджень

Екологічна інформація представляє собою сукупність даних про динаміку кількісних та якісних змін стану природних об'єктів довкілля, їх взаємозв'язок і закономірності розвитку. Накопичена екологічна інформація за багаторічний період формує банки еколого-економічних даних, які мають велике значення для створення ефективної інформаційної екологічної системи [17].

Інформацію про середовище та його екологічний стан можна одержати з різних джерел, до яких перш за все треба віднести:

- джерела первинної інформації, які є результатами первинних досліджень через спостереження, експеримент та під час експедицій

- джерела вторинної інформації, які дають зведену інформацію про стан довкілля і здоров'я людей, ступінь екологічної безпеки господарської діяльності та екологічні ситуації в окремих регіонах і на окремих об'єктах.

- джерела науково-теоретичної інформації, що відображають здобутки знань чи діяльності й викладені у формі карт, таблиць, описів чи фізичних теорій;

- джерела правової інформації, що дають знання про правову базу, правові основи природокористування.

Додатковим джерелом інформації є одноразові обстеження, інвентаризація викидів шкідливих речовин в атмосферу, воду і грунт, вибіркове обстеження причин простоїв і неефективної роботи очисних споруджень.

Екологічна інформація має різні аспекти і носить різний характер. Можна поділити за характером на:

- синтетичний характер інформації має значення для глобального впливу на великомасштабні екосистеми шляхом обліку обставин, що відносяться до охорони навколишнього середовища і раціонального використання природних ресурсів;

- аналітичний характер інформації диктується наявністю великого обсягу різнорідних і децентралізованих даних, що повинні бути приведені в порівнянний вигляд;

- оперативний характер випливає з задач оперативного впливу на локальні важелі деградації навколишнього середовища і виконує попереджувальні функції в найрізноманітніших напрямках підтримки рівноваги й охорони навколишнього середовища.

При зборі й обробці інформації варто брати до уваги наступні аспекти:

- новизну і розширення масштабів екологічної статистики;
- інерційність інформації;
- вплив фонових факторів;
- багатоетапний збір статистичних даних і нормативних параметрів.

Варто розрізняти первинну і похідну інформацію.

Первинна інформація утримується в статистичній звітності. Розробка статистичних даних ведеться по всіх міністерствах і відомствах, у веденні яких знаходяться підприємства і організації, що звітують. Дані статистики екології навколишнього середовища розробляються, як правило, в територіальному розрізі. По більшості форм звітності розробка зведених звітів централізована в органах державної статистики.

Похідна (вторинна) інформація про екологію утримується в еколого-економічному паспорті підприємства. Еколого-економічний паспорт підприємства зведений документ, що заповнюється у місцевих статистичних органах на підставі статистичної звітності, містить характеристики впливу на

навколишнє середовище, з вказівкою заходів для його охорони, напрямків використання відходів виробництва і найважливіших техніко-економічних показників роботи підприємства.

Екологічні дослідження вимагають систематичного дотримання чотирьох послідовних етапів:

- спостереження;

- формулювання на основі спостережень теорії про закономірність досліджуваного явища;

- перевірка теорії наступними спостереженнями і експериментами;

- спостереження за тим, чи є правдивими передбачення, основані на цій теорії.

Факти базуються на прямих або непрямих спостереженнях, що виконані за допомогою органів відчуття або приладів. Всі факти, які належать до конкретної проблеми, називають даними. Спостереження можуть бути якісними або кількісними. Кількісні спостереження є точнішими. Вони включають вимірювання величини або кількості, наочним виразом яких можуть бути якісні ознаки.

В екології найбільше поширені польові біометричні методи і експерименти: перші дають змогу одержати інформацію методом безпосередніх спостережень, другі забезпечують інформацією в процесі лабораторних досліджень. Збирається інформація за допомогою таких методів:

- польовий метод;

- метод безпосередніх спостережень;

- ландшафтно-екологічний підхід;

- ландшафтно-індикаційні;

- гідрохімічні, біохімічні;

- грунтовогазові;

- гідрогеологічні;

- радіоекологічні спостереження;

- геохімічні спостереження ландшафтів;
- дистанційні спостереження;
- експериментальні дослідження.

7.2 Класифікація показників екологічності виробництва

Загальна класифікація еколого-економічних показників з метою оцінки й аналізу екологічності виробництва у промисловості може бути подана за такими ознаками [18]:

- за змістом;
- за рівнем визначення;
- за часовим інтервалом;
- за об'єктом оцінки;
- за характером використання.

За змістом еколого-економічних показників: •

- натуральні - показники екологічності технологічних процесів, техніки, виробничо-господарської діяльності в цілому та її окремих складових.;
- натурально-вартісні - еколого-економічний збиток у розрахунку на одиницю товарної продукції в натуральному вираженні, збиткоємність маси викиду, екологічний результат у розрахунку на одну гривню капітальних вкладень;
- вартісні - розмір економічного збитку в розрахунку на одиницю продукції у вартісному вираженні, повні екологічні витрати виробництва, екологічні платежі за забруднення довкілля;
- локальні - показники вимірюють окремий параметр ЕЕРВ і можуть бути основою формування інтегральних показників, а також використовуватися для аналізу впливу екологічних чинників (показників) на узагальнюючі результати виробничо-господарської діяльності;

- узагальнюючі - показники є головною, підсумковою і регулюючою оцінкою еколого-економічної ефективності технологічних процесів, забезпеченості підприємства основними природоохоронними фондами, рівня впливу виробництва на навколишнє природне середовище і т.д.

За рівнем визначення:

- народногосподарський рівень - аналізуються макроекономічні показники екологічної спрямованості;

- галузевий рівень - галузь розглядається в основному як сукупність підприємств, які об'єднуються за схожими характерними організаційно-технічними ознаками, оскільки сьогодні в основному відсутній дієвий галузевий організаційно-адміністративний розподіл матеріального виробництва;

- регіональний рівень - область, район;

- мікрорівень - підприємство;

- рівень внутрішньовиробничих підрозділів підприємств.

За часовим інтервалом:

- ретроспективні, поточні,

- фактичні, оперативні,

- прогнозні, планові.

За об'єктом оцінки:

- виробництво в цілому, окремі етапи відтворювальних процесів;

- виробництво конкретних видів продукції;

- види виробничо-господарської діяльності підприємств.

За характером використання:

- регулюючі (дієві) - це показники, що безпосередньо застосовуються в процесі регулювання (управління) екологічності виробництва і якості навколишнього середовища, а також стану екосистем у процесі використання;

- індикаторні - показники, за допомогою яких може здійснюватися узагальнююча характеристика ЕВ у процесі аналізу;

- допоміжні показники забезпечують розрахунок комплексних, узагальнюючих еколого-економічних показників; можуть відігравати допоміжну роль при прийнятті складних, управлінських рішень.

7.3 Висновки до розділу

Екологія є важливою наукою про навколишнє середовище і один з її напрямів вивчає вплив людини, прогресу і технологій на довкілля та організми. Саме завдяки цій науці ми знаємо про те наскільки згубною є діяльність людського виду і можемо шукати способи послабити цей негативний вплив.

Зокрема, у даному розділі розглянуто інформаційне забезпечення еколого - статистичних досліджень та класифікація показників екологічності виробництва за допомогою даного програмного забезпечення.

ВИСНОВКИ

Дана кваліфікаційна робота дає змогу провести аналіз поточного стану інформаційної безпеки вищого навчального закладу, виробити перелік рекомендації для гарантування або підвищення такої безпеки, збільшити стійкість функціонування інформаційної мережі, розробити концепцію та політику безпеки, а також запропонувати плани захисту інформаційних ресурсів від умисного спотворення, знищення, несанкціонованого доступу, копіювання або використання.

На даний момент інформаційні технології охопили всі сфери діяльності суспільства. Цей розвиток можна назвати вступом в еру інформації. Швидкий ріст зацікавленості в розвитку сфери інформаційних технологій окрім великої користі приніс в свою чергу й широкий спектр проблем щодо вирішення загроз безпеці інформаційних систем.

Описуючи системи забезпечення безпеки не варто забувати, що вони повинні не лише обмежувати допуск користувачів до інформаційного ресурсу, а й визначати та розмежовувати їхні повноваження в даній системі. Захищеність інформації визначається повнотою вирішення всього комплексу завдань. Цей захист має мати системний характер, де для отримання бажаного результату усі розрізнені типи захисту інформації потрібно об’єднати й налаштувати їх функціювання в складі єдиної системи як злагоджений механізм, який визначений для вирішення завдань із забезпечення безпеки інформації.

Ключовим етапом в ході побудови комплексної системи захисту інформації можна назвати вибір відповідного методу та інструментів. Часто установи гадки не мають, які серед створених методів оцінювання ризиків продуктивніші в їх випадку. Тому процес оцінки має бути суміжним з індивідуальними особливостями установи, але водночас узгоджений із

найкращими стандартами та провідними практиками. Я ж зупинився на виборі методу OCTAVE Allegro, як найбільш підходящого для проведення даного типу робіт. Цей метод має на меті узагальнення та оптимізацію процесу оцінювання ризиків інформаційної безпеки установи та забезпечити можливості отримання необхідних результатів, при цьому, з мінімальною витратою ресурсів. Працівники, технології, інформаційні системи, об'єкти, що відносяться до інформації чи сфери інформаційних послуг, в межах якої вони знаходяться, розглядаються методом окремо. Оцінка ризиків проводиться персоналом та кваліфікованими спеціалістами, що є відповідальними за інформаційну безпеку на семінарах.

З допомогою цього методу й було проведено аналіз інформаційної безпеки Тернопільського національного технічного університету імені Івана Пулюя. Для систематизації отриманих результатів було вирішено провести розподіл на матеріальні та не матеріальні активи. Для кожного з активів було розраховано цінність та проведено дослідження для пошуку загроз цим інформаційним ресурсам. Оцінивши імовірність реалізації загроз інформаційній безпеці, керуючись даними отриманим на попередніх етапах, складено плани запобігання даним загроз. Як спосіб зменшення рівню ризику для більшості активів можна виокремити такі основні засоби технічного захисту інформації, як:

- система контролю доступу;
- система відеоспостереження;
- генератор шуму.

В результаті проведеного дослідження створено профілі активів з чітким описом їх цінності, імовірності втрати або пошкодження, планом по покращенню безпеки даного активу.

В сучасному світі, в усіх сферах життєдіяльності ми стикаємось з чіткими вимогами до виконання будь-якого типу робіт. В світі інформаційної безпеки, цими правилами є стандарти ISO/IEC. Безумовне виконання вимог цих

стандартів є обов’язковим при виконанні подібного типу робіт. Проте, визначним фактором в побудові системи інформаційної безпеки є економічна доцільність при застосуванні програмно-апаратних методів, яка безумовно має відповідати цінності можливої втрати інформаційного ресурсу внаслідок реалізації можливих загроз.

Перспективи подальших досліджень у даному напрямку зумовлюються актуальністю і нагальністю порушеної проблематики, що зумовлено безупинним розвитком інформаційних систем в цілому. Водночас пліч-о-пліч з розвитком інформаційних систем розвиваються й методи реалізації ризиків інформаційних ресурсів. Це зумовлює ріст цінності інформаційних активів організацій, що в свою чергу ще більше спонукає злодіїв до її викрадення або пошкодження. Проте вчасне їх виявлення дозволяє гідно захисти власний інформаційний ресурс та запобігти даним загрозам в довгочасній перспективі, що й доведено в даній роботі.

БІБЛІОГРАФІЯ

1. Юдін О. К. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія / О. К. Юдін, С. С. Бучик. — К. : НАУ, 2015. — 213 с.

2. Чунарьова А. В. Аналіз підходів та програмних рішень оцінки і контролю інформаційних ризиків в комп'ютеризованих системах / А. В. Чунарьова, І. І. Пархоменко, І. І. Сащук // Вісник Інже- нерної академії України. — Х. — 2014. — Вип. 2. — С. 138–142.

3. Пузиренко О. Г. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних сис- тем / О. Г. Пузиренко, С. О. Івко, О. О. Лаврут // Системи обробки інформації. — Л. : Академія сухопутних військ імені гетьмана Петра Сагайдачно- го, 2014. — Вип. 8 (124).— ISSN 1681–7710. — С. 128–134.

4. Бучик С. С. Методика оцінювання інформа- ційних ризиків в автоматизованій системі // С. С. Бучик, С. В. Мельник // Проблеми створення, випробування, застосування та експлуатації склад- них інформаційних систем : зб. наук. праць. — Житомир: ЖВІ ДУТ, 2015. — Вип. 11. — С. 33–43.

5. Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах / О. Г. Пузиренко, С. О. Івко, О. О. Лаврут, О. К. Климович // Системи обробки інформації. — Л. : Академія сухопутних військ імені гетьмана Петра Сагайдачного, 2015. — Вип. 3 (128). — ISSN 1681-7710. — С. 75–79.

6. Корнієнко Б. Я. Прикладні програми управління інформаційними ризиками / Б. Я. Корнієнко, Ю. О. Максімов, Н. М. Марутовська // Захист інформації. — К. : Науково-практичний журнал, 2012. — Вип. 4. — С. 60–64.

7. Астахов А. М. Искусство управления информационными рисками / А. М. Астахов. — М. : ДМК Пресс, 2010. — 312 с.

8. Замула О. А. Аналіз міжнародних стандартів у галузі оцінювання ризиків інформаційної безпеки / О. А. Замула, В. І. Черниш // Системи обробки інформації. — Х. : Харківський національний університет радіоелектроніки, 2011. — Вип. 2 (92). — ISSN 1681-7710. — С. 53–55.

9. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. — М. : Компания АйТи ; ДМК Пресс, 2004. — 384 с.

10. Сергей Петренко. Методики и технологии управления информационными рисками / Сергей Петренко, Сергей Симонов [Електронный ресурс]. — Режим доступу: http://citforum.ru/security/articles/risk/

11. Куканова Наталья. Современные методы и средства анализа и управление рисками информационных систем компаний / Наталья Куканова [Електронний ресурс]. — Режим доступу: http://dsec.ru/ipm-research-center/article/ modern_ methods_and_ means_for_analysis_and_risk_ management_ of_information_systems_of_companies

12. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев // — К. : ТИД Диасофт, 202. — С. 423–436.

13. Information technology — Security techniques–Information security risk management: ISO/IEC 27005 : 2008 [Електронний ресурс]. — Режим доступу:

http://www.iso.org/iso/catalogue_detail?csnumber=42107.

14. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук. : спец. 12.00.01 / Максименко Ю. Є. – К., 2007. – 22 с.

15. Берко А. Ю. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції / Берко А. Ю., Висоцька В. А., Рішняк І. В. // Вісник Національного університету ―Львівська політехніка‖. – 2008. – № 610. – С. 20–33.

16. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 року № 514/2009 [Електронний ресурс]. – Режим доступу : Офіційне Інтернет-представництво Президента України http: // www.president.gov.ua

17. Тарасова В.В. Екологічна статистика.[Текст]/В.В.Тарасова.- Київ: «Центр учбово\ї літератури», 2008 ро.-391с.

18. Хижняк М.І., Нагорна А.М. Здоровя людини та екологія. Київ, Здоровя, 1995.

19. Качан О. Інформаційна безпека підприємства в умовах глобалізації. URL: https://conf.ztu.edu.ua/wp–content/uploads/2017/09/234.pdf.

20. Кириленко А., Бабинюк О. Кібербезпека на захисті бізнесу. URL: https://ir.kneu.edu.ua/bitstream/handle/2018/31417/ZE_2019_118.pdf?sequence=1.

21. Кіпчарська Я. Методичні засади забезпечення інформаційної безпеки поліграфічного підприємства. URL: http://nz.uad.lviv.ua/static/media/4–45/13.pdf.

22. Ключник Т. Кібербезпека як новий виклик сучасності. URL: http://elar.naiau.kiev.ua/bitstream/123456789/7055/1/%D0%90%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%20%D0%BF%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D0%B8%20%D0%B4%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%B8_p052-053.pdf.

23. Ковальов І. Оцінка ризиків інформаційної безпеки з використанням алгоритму нечіткої кластеризації k-середніх. Дипломна робота магістра / І. Ковальов. – Дніпро, 2018. – 78 с.

24. Кожедуб Ю. Реалізація процесного підходу до керування ризиками інформаційної безпеки в документах NIST. URL: https://ela.kpi.ua/bitstream/123456789/23949/1/ITS2017.5.2(9)_09.pdf.

25. Козак Н., Цимбал П., Варшавець Я. Деякі аспекти виявлення і попередження інцидентів кібербезпеки. URL: http://ir.nusta.edu.ua/jspui/bitstream/123456789/2339/1/2219_IR.pdf.

26. Корченко О. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія / О. Корченко, С. Казмірчук, Б. Ахметов. – Київ, 2017. – 435 с.

27. Крижанівський В. Безпека інформаційних систем. Конспект лекцій / В. Крижанівський. – Житомир, 2012. – 110 с.

28. Лисенко Ю. Модель ефективності IT-аутсорсингу в контексті розвитку інформаційних систем економічних об'єктів / Ю. Лисенко, Є. Бізянов // Проблеми економіки. – 2013. – № 2. – С. 190–195.

29. Маркіна І., Дячков Д. Основи формування системи менеджменту інформаційної безпеки підприємства. URL: http://dspace.pdaa.edu.ua:8080/bitstream/123456789/3092/1/piprp_2016_3%281%29__18.pdf.

30. Мельник М. О. Аналіз побудови моделі політики інформаційної безпеки підприємства / М. Мельник, Г. Нікітин, К. Мезенцева // Системи обробки інформації. – 2017. – Вип. 2. – С. 126–128.

31. Микитенко Т. Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в сучасних умовах / Т. Микитенко, І. Петровська, П. Рогов, А. Гаркуша // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. – 2016. – № 2. – С. 24–31.

32. Мохор В., Бакалинський О., Цуркан В. Представлення оцінок ризиків інформаційної безпеки картою ризиків. URL: http://nbuv.gov.ua/j–pdf/inftech_2018_6_2_10.pdf.

33. Нашинець-Наумова А. Питання забезпечення економічної безпеки підприємства. URL:

http://law.nau.edu.ua/images/Nauka/Naukovij_jurnal/2012/statji_n3_24_2012/Nashinec_Naumova_58.pdf.

34. Нехай В., Нехай В. Інформаційна безпека як складова економічної безпеки підприємств. URL: http://www.vestnik–econom.mgu.od.ua/journal/2017/24–2–2017/30.pdf.

35. Новікова А. Питання кібербезпеки у світі юриспруденції. URL: https://sud.ua/ru/news/publication/138379–pitannya–kiberbezpeki–u–sviti–yurisprudentsiyi.

36. Печенюк А. Особливості організації інформаційної безпеки сучасного підприємства. URL: http://ibo.tneu.edu.ua/index.php/ibo/article/view/124/123.

37. Піляй А. Інформаційна безпека. Чи працює Політика ІБ у Вашій компанії? URL: https://legalitgroup.com/informaciyna–bezpeka–v–kompanii/.

38. Пузиренко О. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних систем / О. Пузиренко, С. Івко, О. Лаврут // Системи обробки інформації. – 2014. – Вип. 8. – С. 128–134.

39. Рудий Т. Засади захисту інформації в інформаційних системах підприємств / Т. Рудий, Л. Томаневич, О. Руда // Актуальні проблеми економіки. – № 2 (152). – 2014. – С. 551–557.

40. Савельєва Т., Панаско О., Пригодюк О. Аналіз методів і засобів для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства / Т. Савельєва, О. Панаско, О. Пригодюк // Вісник Черкаського державного технологічного університету. Серія: Технічні науки. – 2018. – Т. 1, № 4. – С. 81–89.

41. Сазонець О., Сіпайло Л. Інноваційна діяльність підприємств у контексті забезпечення інформаційної безпеки. URL: https://www.problecon.com/export_pdf/problems–of–economy–2015–3_0–pages–156_161.pdf.

42. Самедова Л. Ідентифікація поняття інформаційної безпеки в сучасних економічних умовах. URL: http://ep3.nuwm.edu.ua/11750/1/%D0%A1%D0%B0%D0%BC%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0_%D0%9B_%D0%A0%20%D0%B7%D0%B0%D1%85.pdf.

43. Северина С. Інформаційна безпека та методи захисту інформації / С. Северина // Вісник Запорізького національного університету. Економічні науки. – 2016. – № 1. – С. 155–161.

44. Сотниченко В. Інформаційна безпека як базова складова економічної безпеки телекомунікаційного підприємства. URL: http://www.dut.edu.ua/uploads/p_1010_25433567.pdf.

45. Твердохліб І. Управління інцидентами кібербезпеки на малих комерційних підприємствах. Дипломна робота магістра / І. Твердохліб. – Дніпро, 2018. – 132 с.

46. Цвілій О. Безпека інформаційних технологій: сучасний стан стандартів ISO27k системи управління інформаційною безпекою / О. Цвілій // Телекомунікаційні та інформаційні технології. – 2014. – № 2. – С. 73–79.

ДОДАТКИ

ДОДАТОК А

УДК 004.056.5

М.О. Кузьо

Тернопільський національний технічний університет імені Івана Пулюя

Оцінка ризиків інформаційної безпеки Тернопільського національного технічного університету

Неконтрольований доступ до інформаційного ресурсу Вищого навчального закладу, стан інформаційної безпеки, низька захищеність від зовнішніх та внутрішніх загроз мають негативні наслідки – ризик порушення цілісності, доступності та конфіденційності інформації.

Визначення інформаційних ризиків — складне завдання.Усі методи оцінювання ризиків можна поділити на кількісні, якісні або мішані (комбінація кількісних і якісних методів).Кількісні методи використовують вимірні, об’єктивні дані для визначення числових значень вартості активів, імовірності втрат і пов’язаних із ними ризиків. Якісні методи використовують відносний показник ризику (низький, середній, високий) чи вартості активу на основі рейтингу або за шкалою від 1 до 10. Якісна модель оцінює дії та ймовірності виявлених ризиків у швидкий і економічно ефективний спосіб. Набори ризиків, сформовані й проаналізовані згідно з якісною оцінкою, можуть виступати основою для цілеспрямованої кількісної оцінки.

Внаслідок проведених досліджень доцільно запропонувати таку модель реалізації загроз інформаційої безпеки. Центральний маршрутизатор пов'язаний з локальними мережами корпусів Вищого навчального закладу за допомогою проводових ліній зв'язку. Через корпусні маршрутизатори здійснюється зв'язок з комутаторами кафедр та інших підрозділів вузу. Доступ в Інтернет здійснюється через центр інформаційних технологій. Деякі комп'ютери мережі можуть мати зовнішні IP-адреси, що робить їх доступними через Інтернет, минаючи ЦІТ. Інформаційна інфраструктура вузу може бути представлена у вигляді ієрархії наступних основних рівнів:фізичного (лінії зв'язку, апаратні засоби тощо); мережевого (мережеві апаратні засоби, маршрутизатори, комутатори тощо); мережевих додатків і сервісівопераційних систем (ОС); систем управління базами даних (СУБД); технологічних процесів і додатків; бізнес-процесів Вищого навчального закладу.

Як висновок хочу додади,що в ВНЗ повинні ретельно продумуватися заходи захисту інформації до яких можна віднести:правові (закони, статути, накази, постанови); організаційні (розробка і затвердження функціональних обов'язків посадових осіб служби ІБ; фізичний контроль доступу; розробка правил управління доступом до ресурсів системи; явний і прихований контроль за роботою персоналу; технічні (передбачається наявність методик визначення загроз та каналів витоку інформації і знання засобів добування (зняття) інформації); інженерно-технічні (забезпечують унеможливлення несанкціонованого доступу

сторонніх осіб на об'єкти захисту); програмно-технічні (методи ідентифікації і аутентифікації користувачів; реєстрація дій користувачів; засоби захисту від НСД, міжмережеві екрани).

Список способів протидії повинен, у разі необхідності поповняться новими засобами захисту. Це необхідно для підтримки системи безпеки закладу в актуальному стані.