Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Багацького Данііла Сергійовича*

академічної групи *125-19-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка моделей оцінки загроз інформаційній безпеці для аутсорсингової компанії*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Романюк Н.М.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Багацькому Данііlу Сергійовичу* **академічної групи** *125-19-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка моделей оцінки загроз інформаційній безпеці для аутсорсингової компанії***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № 350-с

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз галузі інформаційної безпеки для аутсорсингової компанії	29.03.2023
Розділ 2	Розробка моделей оцінки загроз інформаційній безпеці для аутсорсингової компанії	24.05.2023
Розділ 3	Розрахунок ефективності впровадження моделі системи підтримки прийняття рішень для аутсорсингової компанії	09.06.2023

Завдання видано _____ Мєшков В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 09.01.2023р.

Дата подання до екзаменаційної комісії: 09.06.2023р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 75 с., 8 рис., 8 табл., 4 додатків, 21 джерело.

Об’єкт розробки: система оцінки загроз інформаційній безпеці компаній, що надають послуги аутсорсингу.

Мета роботи: створення моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці з урахуванням особливостей роботи та проблем в забезпеченні інформаційної безпеки компаній, що надають послуги аутсорсингу.

У роботі наведено:

- оцінка особливостей роботи компаній у сфері аутсорсингу, виявлення проблем інформаційної безпеки та загроз;
- аналіз існуючих методів оцінки загроз, обрання оптимального варіанту;
- створення моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці;
- розробка рекомендацій по впровадженню та використанню створеної моделі.

В економічному розділі проведено розрахунок ефективності впровадження створеної моделі системи підтримки прийняття рішень.

Практичне значення роботи полягає розробці моделі підтримки прийняття рішень оцінки загроз для підприємств, що надають послуги аутсорсингу, для підвищення якості та спрощення роботи менеджерів безпеки таких підприємств.

АУТСОРСИНГ, ОЦІНКА ЗАГРОЗ, СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ, МОДЕЛЬ ЗАГРОЗ.

ABSTRACT

Explanatory message: 75 pages, 8 pictures, 8 tables, 4 additions, 21 sources.

Object of development: a system for assessing threats to information security of companies providing outsourcing services.

The purpose of the work: creation of a decision-making support model for assessing threats to information security, taking into account the specifics of work and problems in ensuring information security of companies that provide outsourcing services.

The work provides:

– assessment of the peculiarities of companies' work in the field of outsourcing, identification of information security problems and threats;

– analysis of existing threat assessment methods, selection of the best option;

– creation of a decision-making support model for assessing threats to information security;

– development of recommendations for implementation and use of the created model.

In the economic section, the effectiveness of the implementation of the created decision support system model was calculated.

The practical significance of the work is the development of a decision support model of threat assessment for enterprises providing outsourcing services, to improve the quality and simplify the work of security managers of such enterprises.

OUTSOURCING, THREAT ASSESSMENT, DECISION SUPPORT SYSTEM, THREAT MODEL.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

B2B	–	бізнес для бізнесу;
B2C	–	бізнес для кінцевого користувача;
АС	–	автоматизована система;
Д	–	доступність інформації;
ЗІ	–	захист інформації;
ІзОД	–	інформація з обмеженим доступом;
ІКС	–	інформаційно-комунікаційна система;
ІС	–	інформаційна система;
К	–	конфіденційність інформації;
КЗЗ	–	комплекс засобів захисту;
КС	–	комп'ютерна система;
КСЗІ	–	комплексна система захисту інформації;
ОІД	–	об'єкт інформаційної діяльності;
ПК	–	персональний комп’ютер;
СППР	–	система підтримки прийняття рішень;
СУБД	–	система управління базою даних;
СУБМ	–	система управління базою моделей;
Ц	–	цілісність інформації.

ЗМІСТ

С.

ВСТУП

В умовах постійно зростаючих об’ємів інформації, що надходить, все більше виникає труднощів та проблем з управлінням системами обробки та захисту цієї інформації.

У ситуації, що склалася та вимагає від керівників всіх рівнів управління прийняття швидких та оптимальних рішень, актуальним стає питання про створення систем, що підвищать рівень якості та оперативності обробки отриманої інформації, а також допоможуть у прийнятті зважених рішень, які в основі матимуть оцінку ситуації по багатьом обраним критеріям. Тому зростає потреба у створенні системи підтримки прийняття рішень для покращення показників роботи менеджерів та інших людей, що мають приймати важливі рішення.

Системи підтримки прийняття рішень використовуються у багатьох галузях життєдіяльності людини, та і сфера захисту інформації не стала винятком. Адже для створення комплексної системи захисту інформації, фахівцям потрібно проаналізувати та систематизувати безліч інформації, і все це потрібно зробити швидко, бо від цього залежить якісь, а іноді і взагалі можливість, роботи підприємства чи організації, для якої створюють цю систему.

В даній роботі буде розглянуто питання про використання системи підтримки прийняття рішень для одного з етапів створення КСЗІ, а саме оцінки загроз.

Темою роботи є синтез моделей підтримки прийняття рішень оцінки загроз інформаційній безпеці для компаній, що реалізують послуги аутсорсингу.

Об’єктом дослідження є система оцінки загроз інформаційній безпеці компаній, що надають послуги аутсорсингу.

Предметом дослідження стала модель підтримки прийняття рішень оцінки загроз інформаційній безпеці.

Актуальність даної проблеми полягає у необхідності розробки синтезованої моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компаній зі специфічним напрямом роботи, що полягає у наданні послуг аутсорсингу.

Головною метою роботи є створення моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці з урахуванням особливостей роботи та проблем в забезпеченні інформаційної безпеки компаній, що надають послуги аутсорсингу.

Для реалізації поставленої мети було виділенні задачі:

- оцінка особливостей роботи компаній у сфері аутсорсингу, виявлення проблем інформаційної безпеки та загроз;
- аналіз існуючих методів оцінки загроз, обрання оптимального варіанту;
- створення моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці;
- розробка рекомендацій по впровадженню та використанню створеної моделі.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Компанії, що надають послуги аутсорсингу

1.1.1 Особливості сфери роботи

В наш час ринок товарів та послуг, з точки зору бізнесу, розділяється на дві великі категорії B2C (Business to Consumer) та B2B (Business to Business). Перша з них існує давно та стабільно приносить прибутки компаніям, що отримують його за рахунок виробництва та реалізації товарів (послуг) безпосередньо для кінцевого користувача. Друга категорія лише недавно почала активний розвиток, але стрімко займає свою частку ринку.

По даним, що надає компанія Forrester Research, розподілення ринку бізнесу на B2B та B2C показане на рисунку 1.1.

Рисунок 1.1 – Розподілення ринку на B2B та B2C

Сутність B2B полягає у виробництві та реалізації товарів (послуг) для іншого бізнесу, тобто її ціллю не є кінцевий користувач. Таким чином, B2B являє собою систему економічних взаємовідносин, суб'єктами якої є юридичні особи – комерційні організації будь-якої форми власності.

Однією з головних задач систем B2B є налагодження взаємодії між компаніями та створення надійних захищених інформаційних каналів між ними, завдяки присутності яких стає можливою координація дій всіх учасників інформаційного обміну та їх спільний розвиток.

Здійснювати взаємодію використовуючи систему B2B її користувачі можуть на основі обміну технологіями чи досвідом, отриманими на протязі своєї діяльності у сфері виробництва, торгівлі чи інвестицій. Ціллю цієї взаємодії стає можливість знайти надійних постачальників чи покупців та налагодити партнерські відносини.

В цій системі, так як і в B2C та на будь-якому іншому ринку, існує конкуренція, але у даному випадку, в силу специфіки суб'єктів системи, вона буде мати деякі особливості. Компанії більш серйозно ставляться до вибору потенційних партнерів та ретельніше прораховують ризики взаємодії. Тому для таких компаній вирішальним аспектом є не презентаційна інформація про компанію-партнера, а його репутація, тобто імідж фірми.

Також ринок B2B виявляє високу чутливість до інновацій, тому для підтримання високого рівня конкурентоспроможності, підприємства мають постійно розвиватися та постійно слідкувати за появою нових можливостей у взаємодії з партнерами, наприклад таких як, автоматизація обміну та обробки інформації, впровадження технологій інформаційної безпеки. [1]

Одним з різновидів B2B є аутсорсинг. Аутсорсинг – передавання організацією певних бізнес-процесів чи виробничих функцій на обслуговування іншій компанії, що має вузьку спеціалізацію у цій області. Аутсорсинг має значущу відмінність від одноразових послуг сервісу або підтримки. Зазвичай на аутсорсинг передаються функції по професійній підтримці безперервної діяльності окремих систем та інфраструктури на основі довгострокового договору (не менше ніж один рік). Присутність бізнес-процесу являється відмінною рисою аутсорсингу від інших форм надання послуг абонентської підтримки. [2]

Однією з характерних рис аутсорсингу є скорочення витрат. Головним джерелом економії, у цьому випадку, є збільшення ефективності роботи підприємства в цілому та поява можливості вивільнення або перерозподілу відповідних фінансових та кадрових ресурсів. За рахунок використання аутсорсингу підприємство має можливість відкривати та розвивати нові напрямки, або сконцентрувати увагу та зусилля на вже існуючих напрямках, чим не допустити помилок та значно покращити загальний рівень роботи підприємства.

Теоретично, на аутсорсинг зовнішньому виконавцю можуть бути передані майже всі функції підприємства, але на практиці, зазвичай, перелік значно скорочується. До функцій, що передаються на аутсорсинг відносять:

- бухгалтерський облік та розрахунок податків, розрахунок заробітної плати працівників;
- юридичне забезпечення роботи підприємства;
- робота з персоналом (підбір та навчання кадрів);
- інформаційні системи та управління базами даних;
- маркетингові дослідження та зв'язки з громадськістю;
- послуги реклами та піару;
- послуги перекладачів;
- питання економічної, інформаційної та фізичної безпеки;
- послуги логістики та доставка;
- окремі види чи етапи виробництва;
- прибирання та обслуговування робочих приміщень (територій);
- керування транспортом, його технічне обслуговування та ремонт.

Більшість підприємств створювались по принципу повної автономності, тобто в їх структуру входили різні допоміжні підрозділи, необхідні для забезпечення виробничого циклу. У сьогоденні, більшість сучасних компаній, приходять у своїй управлінські діяльності до тієї думки, що для оптимізації роботи підприємства в умовах, що склалися, очевидною необхідністю є відмова від непрофільних активів та концентрування на одному вузькопрофільному

напрямку діяльності . Для вирішення цієї проблеми вони починають активно передавати ці функції на аутсорсинг іншим компаніям-партнерам. Але не у всіх випадках, таке рішення є виправданим, тому головним завданням на шляху прийняття рішення про передавання бізнес-процесу на аутсорсинг є аналіз інших можливих варіантів рішень, шляхом порівняння якісних, вартісних показників та показників безпечності роботи, компаній-аутсорсерів та власних можливостей. Для цього можна використовувати безліч методів оцінки, та найчастіше використовують матрицю аутсорсингу, бо даний метод є достатньо простим та наочним.

Також для прийняття рішень компанії повинні зважати на переваги та недоліки роботи з аутсорсерами, тобто компаніями, що являються спеціалізованими організаціями класу B2B та мають основний принцип в роботі – виділення в бізнесі головного процесу надання послуг, які для інших організацій є допоміжними. Ще однією відмінною ознакою аутсорсера є модель постійного надання сервісу.

Аутсорсинг надає можливість компанії-замовнику зменшити витрати та значно знизити трудомісткість й затрати на експлуатацію, сконцентруватися на основних бізнес-процесах та не відволікатися на допоміжні.

До суттєвих переваг використання аутсорсингу бізнес-процесів відносять.

Зменшення витрат на реалізацію бізнес-процесу, а саме:

- скорочення та контроль витрат;
- економія на виплату податків з заробітної плати штатного працівника;
- економія на оплату страхування працівників, за рахунок зменшення штату;
- вивільнення внутрішніх ресурсів компанії, можливість використати їх у іншому, більш важливому, напрямку діяльності.

Покращення якості отриманих товарів та послуг:

- концентрація підприємства на головній діяльності;
- можливість залучити краще устаткування та спеціалістів;
- можливість застосовувати нові технології;

– зниження ризиків, пов’язаних з реалізацією бізнес-процесу;

– використання, з власною вигодою, конкуренції на ринку надання послуг аутсорсингу;

– зменшення впливу некерованих факторів;

– розділення ризиків і відповідальності з аутсорсером.

Існування у аутсорсера готових рішень, самостійний пошук яких потребує від підприємства значних зусиль та коштів.

Можливість звільнити час для менеджерів та сконцентрувати їх увагу на рішенні більш важливих, стратегічних питань.

Але крім наочних позитивних сторін використання аутсорсингу, присутні ризики, що вони тягнуть за собою. Основні з них це:

– втрата операційного контролю над компанією;

– несанкціоноване розкриття інформації.

Також важливо зважати й на недоліки передавання бізнес-функцій на аутсорсинг:

– рівень професійності працівників аутсорсера може бути недостатнім для виконання робіт та надання послуг бажаного рівня;

– недостатність важелів керування може призвести до зниження ефективності процесів та збільшенню витрат на обслуговування;

– присутність ризику порушення цілісності майна, безпеки та витоку конфіденційної інформації, у результаті надання неконтрольованого доступу до документів, даних та матеріальних цінностей підприємства;

– збільшення часу вирішення проблем в аварійних ситуаціях, пов’язане з появою додаткової ланки та потребою погоджувати свої дії;

– в деяких ситуаціях, важливу роль відіграють знання національних чи місцевих культурно-соціальних особливостей, при умові співпраці з закордонними партнерами;

– постійна зміна кадрів в компаніях-аутсорсерах;

– штатний працівник має можливість своєчасно виявити деякі особливі помилки, на відміну від позаштатного працівника, який помічає стандартні, «шаблонні» помилки.

Ще одним важливим фактором впливу на передачу бізнес-функцій аутсорсеру є можливість застосування різних планів організації роботи компанії-аутсорсера.

Найбільш вигідним варіантом для аутсорсера є модель, коли «замовник купує людей». Це означає, що компанія-аутсорсер отримує гроші за робочий час своїх працівників, але рішення про заробітну плату, премії та бонуси приймає замовник. А також у цьому випадку, для аутсорсера значно зменшується ризик виникнення питань по кінцевому результату, так як вся відповідальність за результат лежить на замовнику.

Іншим варіантом взаємодії є модель «замовник довіряє завдання аутсорсеру». У цьому випадку, більшість важелів керування переходить до аутсорсера, замовник майже не бере участь в оперативному управлінні. Проєктом керує менеджер, що обирається аутсорсером. Тому ризики, пов'язані з опрацюванням отриманого від аутсорсера продукту (послуги), залишаються у замовника, а аутсорсер отримує право самостійно підбирати команду та варіант розв'язання поставленої задачі.

Тепер розглядається варіант, що є найбільш ризикованим для аутсорсера «замовник купує рішення». В цій ситуації, компанія-замовник вважає, що аутсорсер може повністю самостійно впоратися з проблемою, та передає всі повноваження аутсорсеру. Але за таких умов, аутсорсер отримує високий рівень ризику пов'язаного з невдалими діями, і ставить під загрозу свою репутацію.

З усіх можливих варіантів, найбільший попит має останній, тому компанії-аутсорсери зацікавлені в постійній підтримці та покращенні рівня безпеки своєї діяльності.

На даний час відсутня єдина загальновизнана методологія управління бізнес-функціями компанії. Тому при використані аутсорсингу, рішення про те,

які з функцій передати приймають використовуючи різні методи, але найбільш популярною є матриця прийняття рішень, розроблена консультантами IBS Group. Вони пропонують класифікувати бізнес-функції для того, щоб визначити, чи варто передавати їх на аутсорсинг.

В залежності від відповідності бізнес-функції стратегії компанії та її відношенню до кінцевого продукту, запропоновано розділити всі функції на основні, допоміжні та непрофільні.

Основні функції, що безпосередньо впливають на виробництво товарів та послуг і являються головним джерелом прибутку компанії, не рекомендують передавати на аутсорсинг, адже управління компанії повинне постійно здійснювати повний контроль за їх виконанням.

Допоміжні рекомендують оцінити за допомогою матриці, що представлена на рисунку 1.2. Й по результатам оцінки, винести рішення про передавання на аутсорсинг чи самостійне виконання.

По осі X цієї матриці відкладаються відношення вартості послуг всередині підприємства до аналогічних послуг на ринку. По осі У відображаються якісні характеристики бізнес-функцій також по відношенню до ринкових. В результаті матриця ділиться на дев'ять сегментів, кожному з яких відповідає одне з чотирьох рішень:

- аутсорсинг – відмова від послуг власних підрозділів та придбання цих послуг на ринку;
- розвиток – вдосконалення бізнес-функції в бік збільшення якості послуги чи зменшення собівартості;
- розвиток чи аутсорсинг – варіант, при якому можливі обидва рішення, остаточний варіант приймає менеджер;
- відділення – бізнес-функція є конкурентоспроможною та може бути виділена в окремий бізнес.

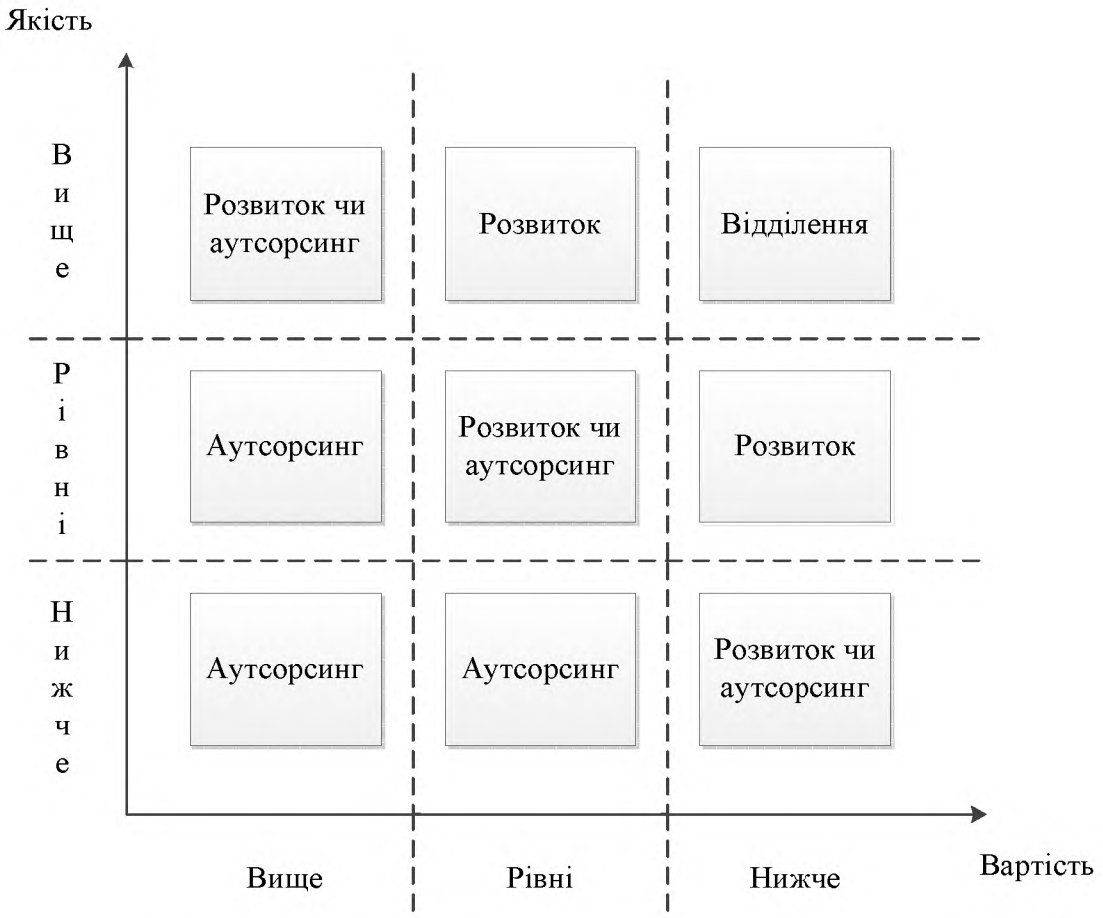

Рисунок 1.2 – Матриця оцінки допоміжних бізнес-функцій

Непрофільні бізнес-функції – по можливості взагалі виключають з складу компанії чи передають на аутсорсинг.

Після того як бізнес-функції компанії класифіковані, необхідно розрахувати і порівняти фінансові та якісні показники з аналогічними послугами (товарами), пропонованими на ринку.

До фінансових показників відносяться витрати на утримання бізнес-функції. Якісний показник - це оцінка якісних характеристик функції, яка, як правило, виражена в балах.

Основна складність цього етапу полягає в зборі й оцінці ринкової інформації про якість та вартість послуг, які компанія розглядає як можливі для виділення на аутсорсинг.

Для вирішення проблеми можливі два варіанти – проведення маркетингового дослідження із залученням спеціалізованих компаній та самостійна оцінка ринку послуг.

Потім потрібно провести аналіз потенціалу аутсорсингу.

У відповідності з моделлю, запропонованою The Boston Consulting Group, перевірка потенціалу аутсорсингу бізнес-функції повинна охоплювати п'ять ключових елементів:

- стратегічний вплив (чи буде створено стратегічна і конкурентна перевага);
- фінансовий вплив (чи є можливість знизити витрати);
- бізнес-вплив (чи є можливості поліпшення якості, отримання доступу до нових навичок і технологіями);
- бізнес-ризики (які існують ризики при використанні аутсорсингу: стратегічні, репутаційні, операційні);
- здійсненність (якими є доступність необхідних послуг, стабільність ринку аутсорсингу, наявність юридичних обмежень).

Рішення про аутсорсинг тієї чи іншої бізнес-функції в компанії, рекомендується приймати при одночасному виконанні наступних чотирьох умов:

- визнання цієї функції непрофільною, та її передача на аутсорсинг;
- вичерпання всіх можливостей щодо підвищення ефективності цієї бізнес-функції всередині компанії;
- наявність конкурентного ринку аналогічних послуг;
- впевненість в тому, що при використанні аутсорсингу вартість даної функції буде дешевше, а якість істотно вище.

Якщо прийнято рішення про передачу бізнес-функції на аутсорсинг, потрібно розробити план заходів. Цей документ повинен включати наступні розділи:

- техніко-економічне обґрунтування прийнятого рішення;

– врегулювання відносин з персоналом підрозділу, функції якого передаються на аутсорсинг (скорочення, переведення до штат аутсорсингової компанії, переклад в інші підрозділи);

– врегулювання майнових відносин (продаж майна, передача в оренду, інші варіанти);

– опис порядку взаємодії з компанією-аутсорсером. [3]

Для кожного пункту плану призначаються відповідальні виконавці та визначаються терміни реалізації. Формується бюджет реалізації даних змін.

Важливо відзначити, що ще на етапі укладання договору з аутсорсером не можна допустити його доступу до конфіденційної інформації. Можуть також виникнути ситуації, коли представники зовнішній компанії попросять детально роз'яснити виробничий процес та особливості роботи підприємства, обґрунтовуючи це тим, що якість послуг у такому випадку може бути значно вище. Розголошення цієї інформації, як і принципів прийняття управлінських рішень на підприємстві, допускати не можна, і кращим підходом при передачі інформації є дотримання принципу «розумної достатності». В іншому випадку велика ймовірність того, що компанія-замовник потрапить у залежність від компанії-аутсорсера. Потрібно також звертати особливу увагу на те, яким чином будуть розраховуватися плата за послуги сторонньої організації і оцінюватися якість, що також має бути прописано в договорі. Всі переговори і прийняті рішення до і після підписання договору слід документувати (вести протокол).

1.1.2 Проблеми інформаційної безпеки

Одним з важливих питань виведення бізнес-процесів на аутсорсинг є інформаційна безпека.

Потрібно зважати на те, що вся економічна ефективність аутсорсингу може бути втрачена, якщо відбудеться інцидент в частині інформаційної безпеки, в результаті якого компанія може зазнати збитків, незрівнянні з

отриманою від аутсорсингу економією. Збереження режиму інформаційної безпеки вимагає виконання певних вимог, яким повинні задовольняти як процеси забезпечення інформаційної безпеки, так і інші процеси. Одна з ключових вимог – налагоджена система з управління ризиками інформаційної безпеки з метою мінімізації їх наслідків або їх повного запобігання, а також сформована технологічна інфраструктура, що забезпечує мінімізацію основних технологічних ризиків. Аутсорсинг, як правило, відрізняється підвищеними вимогами замовника до конфіденційності. В умовах існуючої системи оподаткування та «чорної» бухгалтерії будь-який витік інформації потенційно небезпечний. Тим більше якщо постачальник вимагає для оперативності обслуговування виділений канал, щоб з зовні вирішувати проблеми замовника (створює небезпеку, що не тільки у аутсорсера є прямий доступ до фінансової інформації замовника). Це одна з найсерйозніших проблем на ринку, в силу якої організації бояться що-небудь віддавати на аутсорсинг. І хоча будь-який співробітник компанії-аутсорсера, який залучається для роботи за контрактом аутсорсингу, підписує угоду про нерозголошення, замовники часто намагаються «перестрахуватися», перевіряючи всю інформацію про компанії, з якими доведеться працювати.

Побудова ефективної системи управління інформаційною безпекою при аутсорсингу бізнес-процесів компанії - це не разовий проєкт, а комплексний процес, спрямований на мінімізацію зовнішніх і внутрішніх загроз при обліку обмежень на ресурси і час. На рисунку 1.3 представлений узагальнений процес управління інформаційною безпекою при виведенні на аутсорсинг бізнес-процесів компанії.

Визначення бізнес-процесів компанії.

Рисунок 1.3 – Узагальнений процес управління інформаційною безпекою при виведенні на аутсорсинг бізнес-процесів компанії

На даному етапі проводиться опис усіх основних бізнес-процесів з метою подальшої їх класифікації за ступенем критичності для бізнесу компанії в цілому і відбору процесів-кандидатів для виведення на аутсорсинг. Це необхідно для того, щоб подивитися на бізнес-процеси в загальному уявленні, визначити входи і виходи процесів, власників процесів та інформаційні потоки. Без цієї інформації якісно вибрати модель аутсорсингу, визначити ступінь важливості того чи іншого процесу в більшості випадків буває важко.

Класифікація бізнес-процесів компанії за ступенем критичності для бізнесу в цілому

Для того щоб зрозуміти, які бізнес-процеси компанії можна без загрози для бізнесу передавати на аутсорсинг, необхідно проаналізувати, чи оброблюється ними інформація, що є значущою для бізнесу. На етапі попереднього аналізу необхідно отримати перелік інформації, яка використовується в процесах. З точки зору значущості для бізнесу інформацію можна згрупувати за трьома групами.

Комерційна таємниця. Це інформація, розголошення якої може завдати серйозної шкоди компанії при попаданні, наприклад, до конкурентів. До даної категорії відноситься інформація про всі ноу-хау компанії, технологіях виготовлення продукції або виробництва послуг, управлінська та фінансова звітність, відомості про майбутні угодах, клієнтів і т.д. Процеси, які обробляють даний тип інформації (або через які проходить даний тип інформації), не рекомендується передавати на аутсорсинг, так як вони є однією з основ бізнесу, і якщо компанія передає частину бізнесу третій особі, то вона ризикує позбутися бізнесу в цілому.

Для службового користування. До даної категорії інформації відносяться відомості про співробітників та їх заробітної плати, оперативні плани продажів на короткостроковий період, поточна бухгалтерська звітність і т. д. Процеси, які обробляють дану категорію інформації, можливо передавати на аутсорсинг. При цьому слід забезпечити необхідний рівень інформаційної безпеки від несанкціонованого доступу третіх осіб, наприклад, за допомогою забезпечення

її шифрування, передачі по захищених каналах і реалізації рольового принципу доступу.

Відкрита інформація. Сюди відноситься вся маркетингова і рекламна інформація, інформація про продукти, вироблені компанією, і їх декларовані властивості. З процесів, що обробляють даний тип інформації, рекомендується починати виведення на аутсорсинг. Так як дані процеси містять відкриту інформацію, то помилки при виборі постачальника послуг або низька якість сервісу зможуть заподіяти незначну шкоду компанії. На даних процесах дуже добре перевіряти надійність постачальника і технологію виведення бізнес-процесів на аутсорсинг.

Вибір бізнес-процесів для передачі на аутсорсинг.

Після того, як виконані попередні етапи, необхідно визначити ті бізнес-процеси, які більшою мірою обробляють відкриту інформацію та інформацію для службового користування. З них і вибираються бізнес-процеси - кандидати для виведення на аутсорсинг. Для них визначаються вимоги до постачальника послуг аутсорсингу. Одною з основних вимог, поряд з рівнем надання сервісу, є вимоги до інформаційної безпеки, і при розрахунку фінансової віддачі від аутсорсингу ці витрати і ризики мають бути враховані.

Формування вимог до компанії-постачальника послуг аутсорсингу.

При визначенні вимог до інформаційної безпеки необхідно розглядати весь процес її обробки в цілому, і на кожному етапі забезпечувати необхідний рівень інформаційної безпеки. Вимоги до інформаційної безпеки поділяються на технічні вимоги і вимоги до постачальника. Технічні вимоги включають в себе вимоги до:

- безпеки каналів передачі інформації;
- механізму шифрування інформації;
- порядку авторизації інформації;
- порядку зберігання інформації;
- механізму розмежування прав доступу до інформації і т. д.

Важливо відзначити, що якість шифрування характеризується часом, необхідним для дешифрування. Вимоги до стійкості шифрування необхідні для того, щоб сформувати розумний компроміс між безпекою і вартістю. Наприклад, відомості про новий продукт є комерційною таємницею тільки до тих пір, поки він не почне продаватися на ринку. І подальші витрати із забезпечення збереження його в секреті не мають сенсу. При виборі постачальника слід враховувати:

- термін роботи на ринку послуг аутсорсингу;
- наявність власних потужностей;
- рівень технічної підтримки;
- наявність захищеного місця для обробки отриманої інформації;
- методи організації робіт та наявність сертифікатів;
- вартість обслуговування;
- репутацію постачальника і т.д.

Вибір компанії-постачальника.

Після того, як обрані процеси для передачі на аутсорсинг, сформовано вимоги до інформаційної безпеки і до постачальника, можна переходити до вибору постачальника і потім - до процедури контрактації.

Одним їх ефективних інструментів вибору постачальника послуг аутсорсингу є проведення відкритого або закритого тендеру. На основі його результатів здійснюється усвідомлений вибір постачальника послуг, для чого можна рекомендувати наступний метод. Формується таблиця, в якій по горизонталі перераховуються вимоги до інформаційної безпеки (критичні та некритичні), а по вертикалі наводяться найменування постачальника і рівень підтримки тієї чи іншої вимоги. Виграє той, хто підтримає всі критичні вимоги і максимальне число решти вимог. Приклад таблиці можна розглянути на таблиці 1.1 .

У даному випадку перемагає «Постачальник 1», так як він підтримав всі критичні вимоги замовника. Даний підхід дозволить ставитися до процесу

вибору постачальника з формальної точки зору, аналізуючи всі плюси і мінуси пропонованих рішень.

Таблиця 1.1 – Порівняння постачальників послуг аутсорсингу

Вимоги	Постачальник 1	Постачальник 2
Критична вимога до безпеки 1	Так	Так
Критична вимога до безпеки 2	Так	Так
Критична вимога до безпеки 3	Так	Так
Критична вимога до безпеки 4	Так	Так
Критична вимога до безпеки 5	Так	Ні
Вимога до безпеки 1	Ні	Так
Вимога до безпеки 2	Так	Так
Вимога до безпеки 3	Ні	Так
Висновок	5/1	4/3

Регламентація питань інформаційної безпеки у взаємовідносинах.

В угодах і договорах між замовником, який виводить бізнес-процеси на аутсорсинг, і виконавцем можуть регламентуватися наступні питання:

- угода про рівень сервісу;
- угода про нерозголошення інформації;
- регламент доступу до потужностей і каналах зв'язку, орендованим замовником;
- регламент інформування про спроби несанкціонованого доступу з зовні;
- порядок контролю замовником виконання зобов'язань постачальником і т. д.

При використанні аутсорсингу регламентація питань інформаційної безпеки носить обов'язковий характер, оскільки зони повноважень і відповідальності повинні бути визначені заздалегідь, у випадку інциденту потрібно чітко ідентифікувати відповідальних і визначити винних.

В даний час найбільш часто використовується такий механізм, як угоду про нерозголошення інформації, але його виконання не завжди можна

проконтролювати, особливо якщо до конфіденційної інформації має доступ безліч осіб. Тому для забезпечення режиму інформаційної безпеки необхідні ефективні системи як у постачальника, так і у підрядника. [4]

Управління ризиками в процесі аутсорсингу.

Процесу збору (ідентифікації) ризиків, мета якого - виявлення загроз для організації, які можуть завдати істотної шкоди при аутсорсингу бізнес-процесів.

Процес оцінки ризиків. Його мета полягає у визначенні характеристик ризиків при аутсорсингу бізнес-процесів. Основним результатом даного процесу є перелік всіх потенційних ризиків з їх кількісними та якісними оцінками збитків та можливості реалізації. Додатковим результатом даного процесу виступає перелік ризиків, які не будуть відслідковуватися в організації.

Процес планування заходів з метою визначення термінів та переліку робіт по виключенню або мінімізації збитку у разі реалізації ризику.

Процес реалізації заходів, націленого на виконання запланованих заходів з мінімізації ризиків та контроль якості отриманих результатів і термінів їх виконання. Результатом даного процесу є виконані роботи з мінімізації ризиків і час їх проведення.

Процес оцінки ефективності системи управління інформаційною безпекою при аутсорсингу бізнес-процесів. Це системний процес отримання та оцінки об'єктивних даних про поточний стан систем, дії і події, що відбуваються в ній, встановлює рівень їх відповідності певним критеріям.

Ключові показники ефективності, за якими можна відстежувати ефективність побудованої системи інформаційної безпеки, можуть бути інтегровані в систему управління ризиками і піддаватися регулярному моніторингу. Крім того, на цій стадії виконується моніторинг заздалегідь встановлених заходів, націлених на зменшення обсягу збитку або частоти появи ризиків. Результати даного процесу можуть використовуватися в цілях аудиту для підготовки компанії до сертифікації.

Потрібно відзначити, що, хоча забезпечення інформаційної безпеки при аутсорсингу процесів і являє собою досить складне завдання, при системному підході до даної проблеми і постійному поліпшенні процедур опису та аналізу бізнес-процесів з безперервною оцінкою ризиків можна досягти значного зниження витрат з одночасним поліпшенням якості надання сервісів. Разом з тим необхідно особливо уважно підходити до прийняття рішень з аутсорсингу та аналізувати питання інформаційної безпеки в контексті прийнятого рішення.

1.1.3 Основні загрози безпеці інформації

При огляді питання було складено перелік груп загроз інформаційній безпеці:

- фізичні загрози;
- нецільове використання комп'ютерного обладнання та доступу до мережі Інтернет працівниками організації;
- загрози витоку конфіденційної інформації;
- загрози витоку по технічним каналам;
- загрози несанкціонованого доступу до інформації;

Таблиця 1.2 – Системна класифікація загроз інформації

Параметри класифікації	Значення параметрів	Зміст значення
Види загроз	Порушення фізичної цілісності	Знищення або викривлення структури носія інформації
	Порушення логічної структури	Несанкціонована модифікація інформації
	Порушення змісту	
	Порушення конфіденційності	Несанкціоноване отримання доступу до інформації
	Порушення права особистості	Присвоєння чужого права на доступ чи володіння інформацією
	Порушення доступу до інформації	Блокування інформації

Параметри класифікації	Значення параметрів	Зміст значення
Природа походження	Випадкові	Відмови. Збої. Помилки. Стихійні лиха.
	Передбачені	Сторонні впливи. Зловмисні дії людей.
Передумови появи загроз	Об'єктивні	Кількісний недолік елементів системи. Якісний недолік елементів системи.
	Суб'єктивні	Розвід органи іноземних держав. Промисловий шпіонаж. Кримінальні елементи. Недобросовісні співробітники
Джерела загроз	Люди	Сторонні особи. Користувачі. Персонал
	Технічні пристрої	Реєстрації. Передачі. Зберігання. Переробки. Видачі
	Моделі, алгоритми, програми	Прикладні. Допоміжні.
	Технологічні схеми обробки	Ручні. Інтерактивні. Мережні Внутрішньомашинні.
	Зовнішнє середовище	Стан атмосфери. Сторонні шуми. Сторонні сигнали.

– загрози відсутності доступу до інформаційних сервісів та втрати інформаційних активів;

– загрози порушення цілісності та несанкціонованої модифікації інформації;

– загрози антропогенних та природніх катастроф;

– юридичні загрози. [5]

На сьогодні запропоновано декілька підходів до класифікації загроз інформаційній безпеці. Найпопулярніший комплексний системний підхід наведено у таблиці 1.2.

До основних загроз безпеці інформації при використанні аутсорсингу відносять:

– витік конфіденційної інформації;

- компрометація інформації;
- несанкціоноване використання інформаційних ресурсів;
- помилковий обмін інформацією між абонентами;
- відмова від інформації;
- порушення інформаційного обслуговування;
- незаконне використання привілеїв.

1.2 Методи оцінки загроз безпеці інформації

1.2.1 Аналіз існуючих методів

Аналіз загроз інформаційній безпеці дозволяє виділити складові сучасних загроз – їх джерела та рушійні сили, способи і наслідки реалізації. Аналіз виключно важливий для отримання всієї необхідної інформації про інформаційні загрози, визначення потенційної величини збитку, як матеріальної, так і нематеріальної, і вироблення адекватних заходів протидії.

При аналізі загроз інформаційної безпеки використовуються три основні методи.

Рисунок 1.4 – Основні аналітичні методи оцінки загроз

Розглянемо наведені методи детальніше:

Пряма експертна оцінка. Метод експертних оцінок заснований на тому, що параметри загроз задаються експертами. Експерти визначають переліки параметрів, що характеризують загрози інформаційної безпеки, і дають суб'єктивні коефіцієнти важливості кожного параметра.

Статистичний аналіз – це аналіз інформаційних загроз на основі накопичених даних про інциденти інформаційної безпеки, зокрема, про частоту виникнення загроз певного типу, їх джерела та причини успіху або неуспіху

реалізації. Наприклад, знання частоти появи загрози дозволяє визначити ймовірність її виникнення за певний проміжок часу. Для ефективного застосування статистичного методу потрібна наявність досить великий за обсягом бази даних про інциденти. Потрібно відзначити ще одну вимогу: при використанні об'ємних баз необхідні інструменти узагальнення даних і виявлення в базі вже відомої та нової інформації.

Факторний аналіз заснований на виявленні факторів, які з певною ймовірністю ведуть до реалізації загроз і тим або іншим негативних наслідків. Такими факторами можуть бути наявність привабливих для злочинців інформаційних активів, уразливості інформаційної системи, високий рівень вірусної активності в зовнішньому середовищі і т.д. Оскільки на сучасні інформаційні системи впливають безліч факторів, зазвичай використовується багатофакторний аналіз. [6]

При аналізі загроз інформаційної безпеки найбільш ефективно застосовувати комплекс різних аналітичних методів. Це значно підвищує точність оцінки.

Найбільш вдалим рішенням з оцінки загроз є створення моделі загроз, яка може бути описана багатьма способами, найчастіше використовується табличне представлення моделі загроз, але також популярні способи математичного опису та використання наочних схем.

1.2.2 Вибір методу оцінки загроз

В даній роботі був обраний комплексний метод аналітичної оцінки загроз інформаційній безпеці підприємств, працюючих у сфері надання послуг аутсорсингу. Модель загроз представлена у вигляді таблиці 1.3.

Шкала оцінювання ймовірності реалізації загроз:

0 … 0.24 – дуже низька ймовірність;

0.25 …0.49 – низька ймовірність;

0.5 … 0.74 – середня ймовірність;

0.75 … 1 – висока ймовірність.

Шкала оцінювання рівня збитку від реалізації загроз:

0 … 0.24 – незначні, або відсутні;

0.25 …0.49 – низький рівень;

0.5 … 0.74 – середній рівень;

0.75 … 1 – високий рівень збитку, можливі критичні ситуації.

Така шкала оцінювання була обрана, бо саме за допомогою такого розподілення можна виділити найбільш важливі компоненти та не втратити з поля зору ті, що також мають значний вплив на ситуацію.

Таблиця 1.3 – Загальна модель загроз для підприємств-аутсорсерів

Загроза	Ймовірність реалізації	Збиток від реалізації	Вразливість	Методи протидії
1	2	3	4	5
Техногенні загрози				
Збій в системі електропостачання	0,5	0,5	цілісність, доступність	Використання пристроїв неперервного електропостачання
Знищення (руйнування) інформації	0,2	1	цілісність, доступність	Резервне копіювання
Старіння носіїв інформації	0,2	0,5	цілісність, доступність	Резервне копіювання, оновлення бази носіїв
Модифікація інформації при передачі по каналах зв'язку і телекомунікації	0,2	0,75	цілісність	Використання контрольних сум
Загрози при стихійних лихах				
Знищення (руйнування)				
Приміщень	0,2	1	цілісність, доступність	Страхування, системи протипожежної безпеки
Технічних засобів обробки інформації	0,3	1	цілісність, доступність	Страхування, системи протипожежної безпеки
Носіїв інформації	0,3	1	цілісність, доступність	Страхування, системи протипожежної

				безпеки, вогнестійкі сейфи
Зникнення інформації в засобах обробки, при передачі	0,5	0,75	цілісність, доступність	Резервне копіювання, використання підтверджень про отримання
Антропогенні загрози				
Знищення				
електронної інформації	0,8	1	цілісність, доступність	Резервне копіювання
носіїв інформації (паперові, магнітні, оптичні)	0,5	1	цілісність, доступність	Контроль доступу у приміщення, система відеоспостереження,облік носіїв,резервне копіювання
програмного забезпечення	0,5	1	цілісність, доступність	Резервне копіювання, розмежування прав доступу для користувачів системи
засобів обробки інформації	0,5	1	цілісність, доступність	Контроль доступу у приміщення, система відеоспостереження, облік засобів обробки інформації
Крадіжка				
носіїв інформації (паперові, магнітні, оптичні)	0,8	1	конфіденцій-ність, доступність	Контроль доступу у приміщення, система відеоспостереження, облік носіїв, резервне копіювання
інформації (читання та несанкціоноване копіювання)	0,9	1	конфіденцій-ність, доступність	Контроль доступу у приміщення, система відеоспостереження, облік носіїв, криптографічний захист
засобів доступу (ключі та паролі)	0,75	1	конфіденцій-ність, цілісність, доступність	Використання антивірусного програмного забезпечення, криптографічних засобів захисту, контроль доступу у приміщення

Порушення встановленого режиму доступу	0,75	1	конфіденцій-ність, цілісність, доступність	Охорона приміщень, система контролю доступу
Порушення нормальної роботи (переривання) пропускної здатності каналів зв'язку	0,6	1	доступність	Використання міжмережевих екранів, аналіз трафіку
Помилки при використанні програмного забезпечення	0,6	0,75	цілісність, доступність	Резервне копіювання даних, підвищення кваліфікації працівників
Шкідливе програмне забезпечення	0,75	1	конфіденцій-ність, цілісність, доступність	Використання міжмережевих екранів, антивірусного програмного забезпечення,
Технічні канали витоку інформації				
ПЕМВ засобів обробки інформації	0,25	1	конфіденцій-ність	Використання генераторів ЕМ шуму, екранування приміщень
Наводки на лінії електроживлення	0,25	1	конфіденцій-ність	Використання генераторів шуму, фільтри
Несанкціонований знімання інформації	0,4	1	конфіденцій-ність	Система контролю доступу у приміщення, перевірки наявності закладних пристроїв
Акустичні канали	0,6	1	конфіденцій-ність	Використання генераторів шуму, звукоізоляція,
Оптичні канали	0,6	1	конфіденцій-ність	Контроль доступу, захист прозорих поверхонь за допомогою жалюзі

1.3 Системи підтримки прийняття рішень

1.3.1 Огляд існуючих систем

Прийняття різноманітних рішень – щоденна діяльність менеджерів різних організацій, від правильності вибору яких нерідко залежить ефективна діяльність підприємства в цілому. Обробка численних і суперечливих альтернатив і вибір «найкращої» є складним і відповідальним процесом, якому приділяється значна увага. Саме тому з'являються нові засоби вирішення організаційно-управлінських завдань – системи підтримки прийняття управлінських рішень.

Системи підтримки прийняття рішень (СППР) засновані на формалізації методів отримання вихідних і проміжних оцінок, які дають ОПР (особа, яка приймає рішення), і алгоритмізації самого процесу вироблення рішення. Людино-машинна процедура прийняття рішень за допомогою СППР являє собою циклічний процес взаємодії людини і комп'ютера .

Системи підтримки прийняття управлінських рішень на основі інформаційних технологій почали свій розвиток з кінця 70-х – початку 80-х рр., Завдяки широкому розповсюдженню персональних комп'ютерів, програмних продуктів, а також успіхи в області розвитку штучного інтелекту.

Однією з найважливіших особливостей інформаційних технологій підтримки прийняття управлінських рішень є якісно новий підхід до взаємодії комп'ютера і людини. Прийняття рішення є ітераційним процесом, в якому беруть участь:

- сама система підтримки прийняття управлінських рішень, як обчислювальний ланка і об'єкт управління;
- особа, що оцінює отриманий результат, і на його підставі приймає рішення.

Інформаційні технології підтримки прийняття рішень відрізняються рядом особливостей:

- орієнтація на вирішення погано структурованих завдань;
- поєднання традиційних методів доступу і обробки комп'ютерних даних з можливостями математичних моделей і методами вирішення завдань на їх основі;

– спрямованість на непрофесійного користувача комп'ютера;

– висока адаптивність, що забезпечує можливість пристосовуватися до особливостей наявного технічного і програмного забезпечення, а також вимогам користувача.

Основні компоненти СППР.

На рисунку 1.5 наведена структура, функції технологічних блоків і основні операції системи підтримки прийняття рішень.

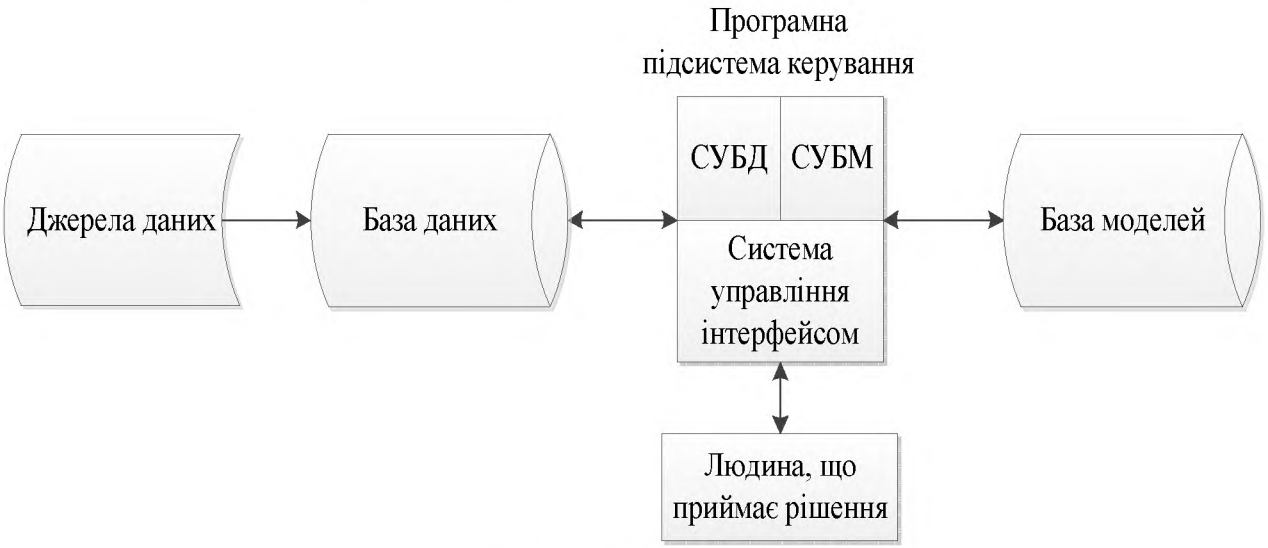

Рисунок 1.5 – Основні компоненти СППР

Основними компонентами інформаційної технології підтримки прийняття рішень є база даних, програмна підсистема і база моделей. Система управління базою даних (СУБД), система управління базою моделей (СУБМ) і система управління інтерфейсом входять до складу програмної підсистеми.

Інформація для бази даних може надходити від різних джерел:

– дані від інформаційної системи операційного рівня для ефективного використання повинні бути попередньо оброблені;

– для прийняття управлінських рішень необхідні дані про внутрішній стан системи, наприклад, рух персоналу, робота різних відділів тощо, які також необхідно обробляти і вводити в систему;

– дані від зовнішніх джерел мають важливе значення при прийнятті рішень на управлінських рівнях;

– до інших внутрішніх джерел даних відносять документи - накази, записи, виписки тощо.

Моделі створюються з метою опису та оптимізації конкретного об'єкта або процесу. Їх використання дає можливість аналізувати системи підтримки прийняття рішень. Математична інтерпретація проблеми, на якій базуються моделі, дозволяє знаходити інформацію, корисну для прийняття правильних рішень.

Специфічні особливості й основи побудови компонентів забезпечують у СППР реалізацію ряду важливих концепцій побудови ІС:

– інтерактивність,
– інтегрованість,
– потужність,
– доступність,
– гнучкість,
– надійність,
– керуємість.

Аналіз еволюції систем СППР дає можливість виділити 2 покоління СППР:

Перше покоління СППР майже цілком повторювало функції звичайних управлінських систем у відношенні допомоги (комп'ютеризованої) у прийнятті рішень. Основні компоненти СППР мали такі ознаки:

– керування даними – велика кількість інформації, внутрішні і зовнішні банки даних, обробка та оцінювання даних;

– керування обчисленням (моделюванням) – моделі, розроблені спеціалістами в галузі інформатики для спеціальних проблем;

– користувацькі інтерфейси (мова спілкування) – мови програмування, розроблені для великих ЕОМ, що використовуються винятково програмістами.

СППР другого покоління вже мають принципово нові ознаки:

– керування даними – необхідна і достатня кількість інформації про факти згідно з прийняттям рішень, що охоплюють приховані припущення, інтереси і якісні оцінки;

– керування обчисленням і моделюванням – гнучкі моделі, що відображають засіб мислення особи, приймаючої рішення, у процесі прийняття рішень;

– інтерфейс користувача – програмні засоби дружні користувачу, звична мова, безпосередня робота кінцевого користувача.

Ціль і призначення СППР другого покоління можна визначити так:

– допомога у розумінні розв'язуваної проблеми. Сюди належить структуризація проблеми, генерування постановок задач, визначення переваг, формування критеріїв;

– допомога у рішенні задач: генерування і вибір моделей і методів, збір і підготування даних, виконання обчислень, оформлення і видача результатів;

– допомога у проведенні аналізу типу «Що? Де? Коли?» і т.п., пояснення ходу рішення;

– пошук і видача аналогічних рішень у минулому і їхні результати.

Дружні людині системи підтримки прийняття рішень дають можливість вести рівноправний діалог із ПЕВМ, використовуючи звичайні мови спілкування. Системи можна підбудовувати під стиль мислення користувача, його знань і фахової підготовки, а також під засоби роботи. [7]

Для сучасних систем підтримки прийняття рішень характерна наявність таких характеристик.

1 СППР дає керівнику допомогу у процесі прийняття рішень і забезпечує підтримку у всьому діапазоні контекстів задач. Думка людини та інформація, що генерується ЕОМ, являють єдине ціле для прийняття рішень.

2 СППР підтримує і посилює (але не змінює і не відміняє) міркування та оцінку керівника. Контроль залишається за людиною. Користувач почуває себе комфортно у системі.

3 СППР підвищує ефективність прийняття рішень. На відміну від адміністративних систем, де робиться акцент на аналітичному процесі, у СППР більш важливою є ефективність процесу прийняття рішень.

4 СППР виконує інтеграцію моделей і аналітичних методів із стандартним доступом до даних і вибіркою з них. Для надання допомоги при прийнятті рішень активується одна або декілька моделей. Вміст БД охоплює історію поточних і попередніх операцій, а також інформацію зовнішнього характеру та інформацію про середовище.

5 СППР проста в роботі для осіб, що мають досвід роботи з ЕОМ.

6 Системи дружні до користувачів не потребують глибоких знань про обчислювальну техніку і забезпечують просте пересування по системі

7 СППР побудовані за принципом інтерактивного рішення задач. Користувач має можливість підтримувати діалог із СППР у безперервному режимі.

8 СППР орієнтована на гнучкість і адаптивність для пристосування до змін середовища або підходів до рішення задач, що обирає користувач. Керівник повинен пристосуватися до змінюваних умов сам і відповідно підготувати систему.

9 СППР не повинна нав'язувати користувачу визначеного процесу прийняття рішень. Користувач повинен мати вибір можливостей, щоб вибирати їх у формі і послідовності, що відповідають стилю його пізнавальної діяльності - стилю «моделей, що надаються».

1.3.2 Підготовка до розробки моделі підтримки прийняття рішень

Загальна схема етапів розробки системи підтримки прийняття рішень (СППР) представлена на рисунку 1.6.

Рисунок 1.6 – Етапи розробки СППР

Етап визначення задач СППР є попереднім, підготовчим етапом розробки системи. На даному етапі визначають основні завдання, які повинна вирішувати СППР, її функції і загальна структура. Також на даному етапі здійснюється збір і накопичення документації, яка містить інформацію про предметну область, яка використовується в процесі прийняття рішень.

На етапі моделювання СППР здійснюється побудова комплексу моделей для визначення подальшого алгоритму роботи.

Розроблюєма СППР є інтелектуальною інформаційною системою, тому одним з основних етапів є етап розробки бази знань. На даному етапі

проводиться визначення прецедентів і правил підтримки прийняття рішень, а також формування та підготовка необхідного набору даних і знань.

Реалізація системи підтримки прийняття рішень передбачає написання програмного коду, а також наповнення бази знань.

На заключному етапі проводиться оцінка ефективності побудованої СППР. А також аналіз можливостей розвитку та покращення отриманого результату. Процес аналізу та модифікації є циклічним.

1.4 Висновок

У першому розділі розглядалися теоретичні питання, проводився аналіз ринку бізнесу, компаній B2B, особливостей компаній, що надають послуги аутсорсингу. Також було оброблено матеріали щодо систем підтримки прийняття рішень, а саме принципи їх побудови, основні складові компоненти та принципи роботи таких систем. Були створені модель загроз для підприємств-аутсорсерів та алгоритм побудови системи підтримки прийняття рішень оцінки загроз інформаційній безпеці.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Розробка моделі системи підтримки прийняття рішень

Розробка схеми моделі системи підтримки прийняття рішень проходила по попередньо визначеному алгоритму. Інформація потрібна для синтезу моделі була розглянута у попередньому розділі.

Рекомендована структура моделі системи підтримки прийняття рішень оцінки загроз для компаній, що надають послуги аутсорсингу представлена на рисунку 2.1.

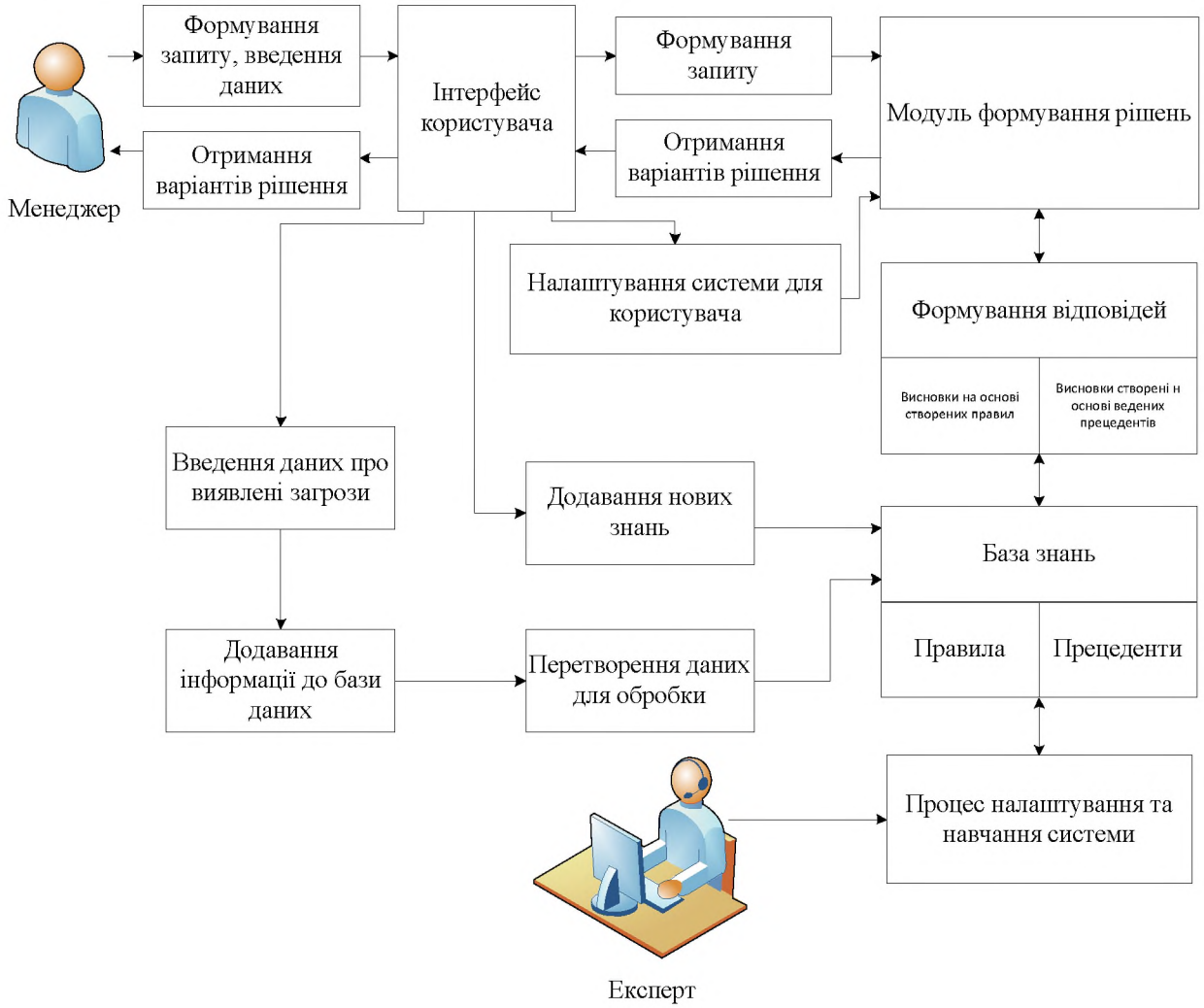

Рисунок 2.1 – Структура моделі системи підтримки прийняття рішень оцінки загроз

Створена система може виконувати три окремі взаємонезалежні функції.

Перша – це основна функція, а саме отримання варіантів рішення проблеми по веденим даним про загрози. При виконанні система повинна

запропонувати максимально можливу кількість вирішень та виділити найбільш оптимальні. В результаті менеджер повинен отримати модель загроз із зазначенням назви загрози, вразливості, ймовірності її реалізації, оцінкою ймовірного збитку та переліком методів протидії реалізації загрози.

Для виконання цієї функції менеджер служби безпеки повинен сформувати запит, далі через інтерфейс користувача, система модифікує запит до зрозумілого їй та передасть запит далі до модулю формування рішень. Після чого він потрапить у модуль формування відповідей та до бази знань, де пройде його обробка а сформується новий запит на отримання даних від користувача, необхідних для формування рішення. Отримавши інформацію від користувача, база знань опрацює її за допомогою правил та прецедентів, потім передасть до модулю формування відповідей, де продовжиться опрацювання інформації. Наступним місцем обробки буде модуль формування рішень, який обере оптимальний перелік варіантів та передасть їх до користувача за допомогою інтерфейсу. У результаті користувач отримає відповідь на свій опрацьований запит.

Друга – функція навчання системи користувачем. У разі виконання цієї функції користувач може додати нові правила та прецеденти для поліпшення ефективності роботи системи та отримання більш точного і розгорнутого результату.

Цю функцію рекомендовано використовувати менеджерам, що мають знання та досвід в оцінці загроз та побудові моделей загроз, адже у випадку використання цієї функцій не професіоналом можливий збій у роботі системи, або погіршення якості кінцевого результату.

При використанні функції навчання системи користувачем, потрібно сформувати запит, за допомогою інтерфейсу користувача, до бази знань. Після отримання запиту у відповідь, користувач повинен ввести нові правила та прецеденти, вказати системі як і коли їх використовувати. В кінці роботи зберегти всі нові налаштування та протестувати систему. При виявленні помилок у роботі, провести процедуру повторно.

Третя – функція навчання системи експертом. Цю функцію рекомендовано використати при встановлені системи для нового користувача та періодично проводити для покращення ефективності роботи системи. Для коректної роботи системи, вона повинна отримати створену експертом базу знань та пройти тестування під його ж керівництвом.

Ця функція схожа на попередню, але у ролі користувача виступає експерт з оцінки загроз, який повинен налаштувати систему для нового користувача. Експерт додає до системи всі початкові правила та прецеденти і відслідковує роботу системи протягом деякого часу, після чого, вносить корективи та передає систему у користування менеджеру.

Також є допоміжна функція налаштування системи під користувача. Вона потрібна для того, щоб отримані варіанти рішень були як найбільш зрозумілі для людини, що буде приймати рішення по отриманим варіантам від системи.

Для використання даної функції користувач повинен сформувати запит до модулю формування рішень, за допомогою інтерфейсу користувача, та встановити найбільш вподобаний вид подання результатів у відповідь.

2.2 Розробка моделі для підприємства та її оцінка

Розроблена модель була протестована на базі приватного підприємства.

Основним напрямом роботи підприємства є комплексне обслуговування бухгалтерських програм та надання послуг аутсорсингу бухгалтерської діяльності.

Основою діяльності компанії є продаж та обслуговування програмного забезпечення «1С», «БЕСТ ЗВІТ ПЛЮС» та систем «M.E.Doc», «ЛІГА:ЗАКОН», а також надання послуг аутсорсингу за допомогою вищезазначених програмних продуктів.

«1С» використовується для автоматизації обліку на підприємствах різних галузей і форм власності.

Програма «1С» покриває різні види обліку (бухгалтерський, податковий, управлінський) та використовується у різних галузях. Головною цінністю цієї

програми вважають гнучкість, тобто можливість оптимального налаштування для кожного конкретного випадку. [8]

Програмний комплекс "БЕСТ ЗВІТ ПЛЮС" призначений для автоматизації процесів роботи зі звітною документацією встановленого зразка. Він забезпечує організацію електронного документообігу у всіх без винятку суб'єктів господарювання будь-якої форми власності та джерел фінансування або між ними та державними контролюючими органами, подача звітності яким передбачена чинним законодавством. [9]

Система «ЛІГА:ЗАКОН» – це найпотужніша комплексна система інформаційно-правового забезпечення, створена для фахівців великих, середніх та малих компаній. Завдяки оптимальному набору інформаційних ресурсів забезпечує успішну роботу всіх підрозділів підприємства. Містить документи по всіх видах господарської діяльності і галузям права, допомагає вирішувати професійні завдання юридичних, бухгалтерських, фінансових і кадрових служб компанії. [10]

Система «M.E.Doc» – це система електронного документообігу, що дає ряд можливостей:

- створення необхідних документів;
- підписання документу електронним цифровим підписом;
- обмін податковими накладними та квитанціями про їх реєстрацію з контрагентами;
- оформити запити та отримати виписки з реєстру;
- перевірити, зашифрувати та зберегти документи у єдиній системі;
- відправити звіти до контролюючих органів;
- отримати квитанції про отримання і обробку відправлених документів. [11]

Об’єктом інформаційної діяльності підприємства є приміщення, що займають приймальня директора, бухгалтерія, відділ продажу та відділ підтримки користувачів. [12]

Доступ до мережі Інтернет на приватному підприємстві.

На даному підприємстві існує своя локальна мережа Fast Ethernet, доступ до якої мають тільки службовці фірми. Доступ до Інтернету забезпечується провайдером «Фрегат».

Системи комунікацій підприємства приведено у таблиці 2.1

Таблиця 2.1 – Системи комунікацій підприємства

Тип комунікацій	Спосіб підключення
Електропостачання	Підключено до трансформаторної підстанції, у якої є сторонні споживачі, і знаходиться поза контрольованою заною
Система опалення	Підключена до міської системи опалення, знаходиться поза контрольованою заною (пластикові труби, однотрубна вертикальна система опалення)
Система каналізації	Підключена до міської системи, яка знаходиться поза контрольованою заною
Система водопостачання	Підключена до міськводоканалу, яка знаходиться поза контрольованою заною (пластикові труби)
Заземлення	Всі прилади і комп'ютери заземлені на загальний контур заземлення, який замкнутий і виходить за межі контрольованою заною
Система вентиляції	За допомогою кондиціонерів

Штат співробітників підприємства.

1 Директор. (2 особи) Секретар директора. (2 особи)

2 Працівники бухгалтерії. (2 особи)

3 Працівники відділу технічної підтримки, займаються обробкою запитів користувачів, надають допомогу у вирішенні проблем роботи з програмним забезпеченням. (6 осіб)

4 Працівники відділу продаж, займаються активним залученням нових клієнтів, формують та готують до підписання договори. (6 осіб)

5 Працівники відділу аутсорсингу, займаються виконанням поставлених керівництвом завдань, готують звіти та іншу документацію, за

допомогою програмного забезпечення, що пропонує на реалізацію підприємство. (12 особи)

6 Працівники служби безпеки. (3 особи)

7 Охоронці. (2 особи)

8 Прибиральниці. (2 особи)

Загальна кількість співробітників - 37 осіб.

Графік роботи підприємства

Підприємство працює з понеділка по неділю. Графік роботи з 9:00 до 19:00, без перерви. Прибирання приміщення проводиться кожного робочого дня з 8:00 до 8:45. Охорона працює цілодобово. Також приміщення знаходиться під охороною приватної охоронної фірми «Скіф» з 19:00 до 7:00. Ключі від офісу знаходяться у директора і охоронців. Доступ до приміщення сторонніх осіб можливий, тільки в робочий час.

На сьогодні підприємство налічує 37 працівників, що об'єднуються у організаційну структуру, зображену на рисунку 2.2.

Для проведення оцінки загроз та створення моделі загроз необхідно провести аналіз інформації, що циркулює на підприємстві . [13 – 15]

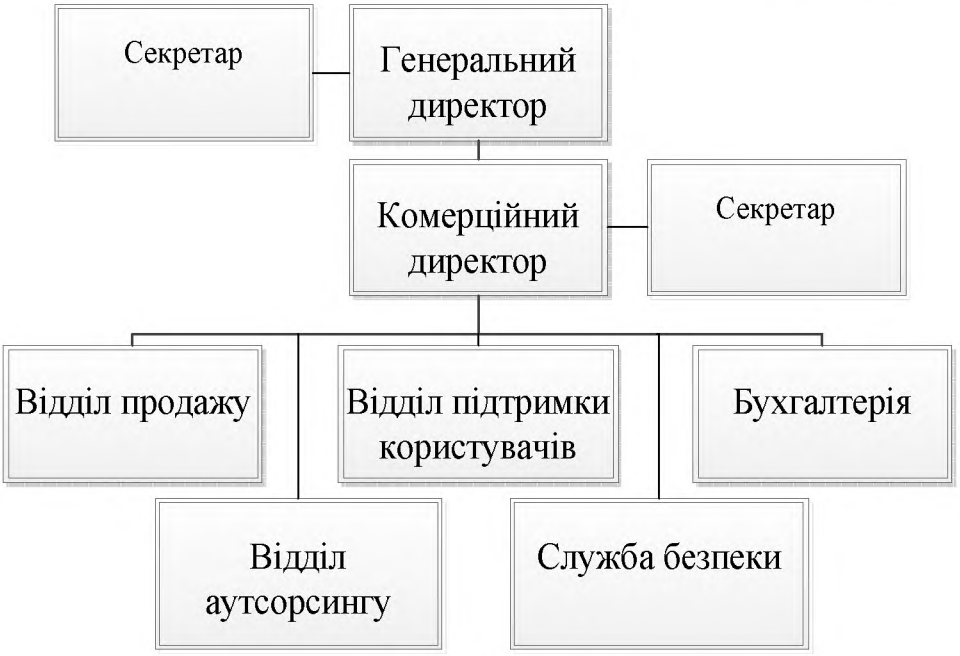

Рисунок 2.2 – Організаційна структура

Загальна класифікація інформації, яка циркулює на підприємстві знаходиться у таблиці 2.2.

Таблиця 2.2 – Інформація, яка циркулює на підприємстві

Інформація	Режим доступу	Правовий режим	Особи, які мають доступ
Організаційно-розпорядча документація (Зберігається в кабінеті директора на паперовому носії)	З обмеженим доступом	Конфіденційна	Всі співробітники фірми
Інформація про надання послуг, прайс-листи, контактна інформація фірми	Відкрита для працівників і клієнтів	Відкрита	Всі співробітники фірми і клієнти
Інформація про службовців (зберігається в кабінеті директора на паперовому носії в сейфі, у секретаря – в електронному вигляді на жорсткому диску комп'ютера)	З обмеженим доступом	Конфіденційна	Директор і його секретар, бухгалтер
Статутні документи підприємства (документи, які дозволяють займатися підприємницькою діяльністю) (зберігається в кабінеті директора на паперовому носії у сейфі)	Відкрита для працівників, клієнтів і перевіряючих	Відкрита	Всі співробітники фірми, клієнти та перевіряючі
Трудові договори працівників (зберігається в кабінеті директора на паперовому носії у сейфі)	З обмеженим доступом	Конфіденційна	Директор, його секретар

В таблиці 2.3 вказана інформація, що віднесена до комерційної таємниці підприємства.

Таблиця 2.3 – Комерційна таємниця

Інформація	Особи, які мають доступ	Місце зберігання
1	2	3
Відомості про фінанси підприємства (бухгалтерія)	Директор і його секретар, бухгалтер	Зберігається в кабінеті директора на паперовому носії та в електронному вигляді на жорсткому диску у бухгалтера
Про плани підприємства (плани закупівель, продажів, потокові і перспективні плани)	Директор і його секретар, дизайнери, фахівці із закупівель, бухгалтер	
Відомості про постачальників	Директор і його секретар, аутсорсери, фахівці з продаж, бухгалтер	
Відомості про способи придбання і реалізації продукції підприємства	Директор і його секретар, бухгалтер, фахівці з продаж	
Зміст і характер договорів, контрактів, однією зі сторін яких є підприємство	Директор і його секретар, бухгалтер	Зберігається в кабінеті директора на паперовому носії
Відомості про охорону сигналізацією та про місце її розміщення	Директор і його секретар, охоронці	

Для подальшої роботи було проведено категоріювання інформації, що циркулює на об’єкті інформаційної діяльності. Для цього були створені Наказ «Про створення комісії для проведення категоріювання виділеного приміщення та об’єктів обчислювальної техніки», Акт «Категоріювання приміщення та засобів обчислювальної техніки об’єкту інформаційної діяльності. По результатам проведених робіт виявлено, що вищий гриф секретності інформації, що циркулює у виділеному приміщенні – «Конфіденційно» та присвоєна четверта категорія. [16,17]

Для тестування моделі системи підтримки прийняття рішень, інженеру з забезпечення інформаційної безпеки підприємства було запропоновано відповісти на питання з «Лист-опитування», що був розроблений для проведення тестування. Після проведення опитування і використання моделі була створена модель загроз для приватного підприємства. Отримана модель загроз, що у достатній мірі описує стан загроз інформаційній безпеці на цьому підприємстві. Для її створення було витрачено значно менше часу, ніж на попередню, а результат є більш конкретизованим для оцінюваного підприємства.

При проведені опитування була отримана інформація, щодо стану захищеності інформації на підприємстві і з моделі були виключені ті загрози, що мають дуже низьку ймовірність та можуть призвести до незначних втрат при їх реалізації. [18]

Далі розглянемо «Лист-опитування», створений для підприємства.

«Лист-опитування для приватного підприємства

Запитання:

1 Яку частоту мають техногенні загрози?

2 Рівень збитку від реалізації техногенних загроз?

3 Як часто трапляються збої в системі електропостачання?

4 Рівень збитку при реалізації загрози?

5 Яку частоту мають знищення (руйнування) інформації від техногенних загроз?

6 Рівень збитку при реалізації загрози?

7 Чи присутнє у компанії старіння носіїв інформації?

8 Рівень збитку при реалізації загрози?

9 Чи можлива модифікація інформації при передачі по каналах зв'язку і телекомунікації?

10 Рівень збитку при реалізації загрози?

11 Яку частоту мають стихійні лиха на підприємстві?

12 Рівень збитку від стихійного лиха?

13 Як часто трапляються руйнування приміщень від стихійного лиха?

14 Рівень збитку при цьому?

15 Як часто трапляються знищення технічних засобів обробки інформації від стихійного лиха?

16 Рівень збитку при цьому?

17 Як часто трапляються знищення носіїв інформації від стихійного лиха?

18 Рівень збитку при цьому?

19 Як часто трапляються знищення інформації в засобах обробки,при передачі від стихійного лиха?

20 Рівень збитку при цьому?

21 Яку частоту мають антропогенні загрози?

22 Рівень збитку від антропогенних загроз?

23 Як часто трапляється знищення електронної інформації працівниками?

24 Рівень збитку від таких дій?

25 Як часто трапляється знищення електронної інформації зовнішніми порушниками?

26 Рівень збитку від таких дій?

27 Як часто трапляється знищення носіїв інформації працівниками?

28 Рівень збитку від таких дій?

29 Як часто трапляється знищення носіїв інформації зовнішніми порушниками?

30 Рівень збитку від таких дій?

31 Як часто трапляється знищення програмного забезпечення працівниками?

32 Рівень збитку від таких дій?

33 Як часто трапляється знищення програмного забезпечення зовнішніми порушниками?

34 Рівень збитку від таких дій?

35 Як часто трапляються збої обробки інформації в наслідок дій працівників?

36 Рівень збитку від таких дій?

37 Як часто трапляються збої обробки інформації в наслідок дій зовнішніх порушників?

38 Рівень збитку від таких дій?

39 Як часто трапляються крадіжки носіїв інформації в наслідок дій працівників?

40 Рівень збитку від таких дій?

41 Як часто трапляються крадіжки носіїв інформації в наслідок дій зовнішніх порушників?

42 Рівень збитку від таких дій?

43 Як часто трапляються крадіжки інформації (читання та несанкціоноване копіювання) в наслідок дій працівників?

44 Рівень збитку від таких дій?

45 Як часто трапляються крадіжки інформації (читання та несанкціоноване копіювання) в наслідок дій зовнішніх порушників?

46 Рівень збитку від таких дій?

47 Як часто трапляються крадіжки і засобів доступу (ключі та паролі) в наслідок дій працівників?

48 Рівень збитку від таких дій?

49 Як часто трапляються крадіжки засобів доступу (ключі та паролі) в наслідок дій зовнішніх порушників?

50 Рівень збитку від таких дій?

51 Як часто трапляються порушення встановленого режиму доступу в наслідок дій працівників?

52 Рівень збитку від таких дій?

53 Як часто трапляються порушення встановленого режиму доступу в наслідок дій зовнішніх порушників?

54 Рівень збитку від таких дій?

55 Як часто трапляються порушення нормальної роботи та пропускної здатності каналів зв'язку в наслідок дій працівників?

56 Рівень збитку від таких дій?

57 Як часто трапляються порушення нормальної роботи та пропускної здатності каналів зв'язку в наслідок дій зовнішніх порушників?

58 Рівень збитку від таких дій?

59 Як часто трапляються помилки при використанні програмного забезпечення в наслідок дій працівників?

60 Рівень збитку від таких дій?

61 Як часто трапляються помилки при використанні програмного забезпечення в наслідок дій зовнішніх порушників?

62 Рівень збитку від таких дій?

63 Як часто трапляються факти використання шкідливого програмного забезпечення в наслідок дій працівників?

64 Рівень збитку від таких дій?

65 Як часто трапляються факти використання шкідливого програмного забезпечення в наслідок дій зовнішніх порушників?

66 Рівень збитку від таких дій?

67 Яку частоту має витік інформації, що підлягає захисту, технічними каналами витоку інформації?

68 Рівень збитку?

69 Яку частоту має витік інформації, що підлягає захисту, завдяки побічним електромагнітним випромінюванням засобів обробки інформації?

70 Рівень збитку?

71 Яку частоту має витік інформації, що підлягає захисту, завдяки наводкам на лінії електропостачання?

72 Рівень збитку?

73 Яку частоту має витік інформації, що підлягає захисту, завдяки несанкціонованому зніманні інформації?

74 Рівень збитку?

75 Яку частоту має витік інформації, що підлягає захисту, завдяки акустичним каналам?

76 Рівень збитку?

77 Яку частоту має витік інформації, що підлягає захисту, завдяки оптичним каналам?

78 Рівень збитку?

По результатам опитування було складено первинну модель загроз, з якою можна ознайомитись у таблиці 2.4. Після обробки було отримано кінцевий результат, з яким можна ознайомитись у таблиці 2.5. [19 - 21]

Шкала оцінювання ймовірності реалізації загроз:

0 … 0.24 – дуже низька ймовірність;

0.25 …0.49 – низька ймовірність;

0.5 … 0.74 – середня ймовірність;

0.75 … 1 – висока ймовірність.

Шкала оцінювання рівня збитку від реалізації загроз:

0 … 0.24 – незначні, або відсутні;

0.25 …0.49 – низький рівень;

0.5 … 0.74 – середній рівень;

0.75 … 1 – високий рівень збитку, можливі критичні ситуації.

Результати опитування головного інженера служби безпеки:

1) 0,2
2) 0,2
3) 0,2
4) 0,2
5) 0,2
6) 0,2
7) 0,2
8) 0,1
9) 0,2
10) 0,2
11) 0,2
12) 0,2
13) 0,2
14) 1
15) 0,2
16) 0,8
17) 0,2
18) 0,5
19) 0,2
20) 0,75

21) 0,75
22) 1
23) 0,8
24) 1
25) 0,5
26) 1
27) 0,7
28) 1
29) 0,5
30) 1
31) 0,5
32) 1
33) 0,5
34) 1
35) 0,5
36) 1
37) 0,3
38) 1
39) 0,8
40) 1
41) 0,5
42) 1
43) 0,9
44) 1
45) 0,5
46) 1
47) 0,75
48) 1
49) 0,5
50) 1
51) 0,5
52) 1
53) 0,3
54) 1
55) 0,5
56) 1
57) 0,5
58) 1
59) 0,6
60) 0,75
61) 0,4
62) 0,75
63) 0,75
64) 1
65) 0,3
66) 1
67) 0,2
68) 0,2
69) 0,2
70) 0,2
71) 0,2
72) 0,2
73) 0,2
74) 0,2
75) 0,2
76) 0,2
77) 0,2
78) 0,2

Отже, отримавши результати можна переходити до створення моделі загроз для підприємства

Таблиця 2.4 – Модель загроз після проведення опитування

Загроза	Ймовірність реалізації	Збиток від реалізації	Вразливість
1	2	3	4
Техногенні загрози			
Збій в системі електропостачання	0,2	0,2	цілісність, доступність
Знищення (руйнування) інформації	0,2	0,2	цілісність, доступність
Старіння носіїв інформації	0,2	0,1	цілісність, доступність
Модифікація інформації при передачі по каналах зв'язку і телекомунікації	0,2	0,2	цілісність
Загрози при стихійних лихах			
Знищення (руйнування)			
Приміщень	0,2	1	цілісність, доступність
Технічних засобів обробки інформації	0,2	0,8	цілісність, доступність
Носіїв інформації	0,2	0,5	цілісність, доступність
Зникнення інформації в засобах обробки, при передачі	0,2	0,75	цілісність, доступність
Антропогенні загрози			
Знищення			
електронної інформації	0,8	1	цілісність, доступність
носіїв інформації (паперові, магнітні, оптичні)	0,7	1	цілісність, доступність
програмного забезпечення	0,5	1	цілісність, доступність
засобів обробки інформації	0,5	1	цілісність, доступність

Загроза	Ймовірність реалізації	Збиток від реалізації	Вразливість
1	2	3	4
Крадіжка			
носіїв інформації (паперові, магнітні, оптичні)	0,8	1	конфіденційність, доступність
інформації (читання та несанкціоноване копіювання)	0,9	1	конфіденційність, доступність
засобів доступу (ключі та паролі)	0,75	1	конфіденційність, цілісність, доступність
Порушення встановленого режиму доступу	0,7	1	конфіденційність, цілісність, доступність
Порушення нормальної роботи (переривання) пропускної здатності каналів зв'язку	0,5	1	доступність
Помилки при використанні програмного забезпечення	0,6	0,75	цілісність, доступність
Шкідливе програмне забезпечення	0,75	1	конфіденційність, цілісність, доступність
Технічні канали витоку інформації			
ПЕМВ засобів обробки інформації	0,2	0,2	конфіденційність
Наводки на лінії електроживлення	0,2	0,2	конфіденційність
Несанкціонований знімання інформації	0,2	0,2	конфіденційність
Акустичні канали	0,2	0,2	конфіденційність
Оптичні канали	0,2	0,2	конфіденційність

Таблиця 2.5 – Модель загроз для приватного підприємства

Загроза	Ймовірність реалізації	Збиток від реалізації	Вразливість
Загрози при стихійних лихах			
Знищення (руйнування)			
Приміщень	0,2	1	Ц, Д
Технічних засобів обробки інформації	0,2	0,8	Ц, Д
Носіїв інформації	0,2	0,5	Ц, Д
Зникнення інформації в засобах обробки, при передачі	0,2	0,75	Ц, Д
Антропогенні загрози			
Знищення			
електронної інформації	0,8	1	Ц, Д
носіїв інформації (паперові, магнітні, оптичні)	0,7	1	Ц, Д
програмного забезпечення	0,5	1	Ц, Д
засобів обробки інформації	0,5	1	Ц, Д
Крадіжка			
носіїв інформації (паперові, магнітні, оптичні)	0,8	1	К, Д
інформації (читання та несанкціоноване копіювання)	0,9	1	К, Д
засобів доступу (ключі та паролі)	0,75	1	К, Ц, Д
Порушення встановленого режиму доступу	0,7	1	К, Ц, Д
Порушення нормальної роботи (пропускної здатності каналів зв'язку	0,5	1	Д
Помилки при використанні програмного забезпечення	0,6	0,75	Ц, Д
Шкідливе програмне забезпечення	0,75	1	К, Ц, Д

2.3 Висновок

У спеціальній частині було розглянуте приватне підприємство, для нього були проведені класифікація інформації, що циркулює на підприємстві проведено категоріювання цієї інформації.

Модель була розроблена для компаній, що надають послуги аутсорсингу, але при незначних змінах у структурі може використовуватись й іншими підприємствами, при умові виконання навчання системи експертом. У перспективі роботи над створеною моделлю є її опрацювання та створення програмного рішення для її успішної реалізації.

Після розробки програмного рішення, його оцінки та тестування, її буде рекомендовано для впровадження на підприємствах та в організаціях для покращення роботи менеджерів служб захисту інформації.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Постановка задачі

Метою економічного розділу є обґрунтування доцільності впровадження моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компаній, що реалізують послуги аутсорсингу.

Завданням був розрахунок капітальних та експлуатаційних витрат на розробку моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компаній-аутсорсерів. А також визначення та аналіз показників економічної ефективності створеної моделі.

3.2 Визначення капітальних витрат на створення моделі

3.2.1 Визначення трудомісткості розробки та опрацювання моделі

При проведенні нормування праці робітників, що займаються створенням моделі, виникає проблема, пов'язана з тим, що ця праця є творчою. У цій ситуації доцільно проводити розрахунки на основі системи моделей з певною точністю оцінки.

Трудомісткість створення моделі визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи опрацюванням методу на об'єкті. При умові, що весь об'єм робіт буде виконано одним робітником, розраховується за формулою 3.1:

$$t = t_{mз} + t_{в} + t_{а} + t_{пр} + t_{опр}, \text{ годин}, \qquad (3.1)$$

де $t_{mз}$ – тривалість складання технічного завдання на розробку моделі;

$t_{в}$ – тривалість вивчення технічного завдання (ТЗ), літературних джерел за темою тощо;

$t_{а}$ – тривалість розробки алгоритму створення моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компаній, що реалізують послуги аутсорсингу;

$tпр$ – тривалість розробки моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компаній, що реалізують послуги аутсорсингу;

$tопр$ – тривалість опрацювання моделі.

Отже трудомісткість створеної моделі складає:

$$t = 20 + 20 + 20 + 30 + 30 = 120, \text{ годин.}$$

3.2.2 Розрахунок витрат на створення моделі

При підрахунку витрати на створення моделі Км за формулою 3.2 треба знайти загальні витрати на оплату заробітної плати розробнику моделі Ззп та вартість машинного часу, що необхідний для розробки та опрацювання моделі на ПЕОМ Змч:

$$К_м = З_{зп} + З_{мч} . \quad (3.2)$$

Заробітна плата розробника моделі враховує основну і додаткову заробітну плату, відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою 3.3:

$$Ззп = t \cdot Зпр, \text{ грн,} \quad (3.3)$$

де t – загальна тривалість створення моделі, годин;

Зпр – средньогодинна заробітна плата розробника з нарахуваннями, грн/годину.

Таким чином, заробітна плата розробника за весь період праці складатиме:

$$З_{зп} = 120 \cdot 90 = 10800, \text{ грн.}$$

До загальної суми потрібно включити вартість машинного часу для розробки моделі на ПЕОМ, що визначається за формулою 3.4:

$$З_{мч} = t_{опр} \cdot С_{мч} \text{ , грн,} \quad (3.4)$$

де $t_{опр}$ – трудомісткість розробки моделі на ПЕОМ, годин;

$С_{мч}$ – вартість 1 години машинного часу ПЕОМ, грн./година.

Вартість 1 години машинного часу ПЕОМ визначається за формулою 3.5:

$$Смч = P \cdot Ce + \frac{Фзал \cdot Ha}{Fp} + \frac{Клпз \cdot Hапз}{Fp}, \text{ грн./година,} \quad (3.5)$$

де Р – встановлена потужність ПЕОМ (0,6 кВт);

$С_е$ – тариф на електричну енергію (1,44 грн/кВт·година);

$Ф_{зал}$– залишкова вартість ПЕОМ на поточний рік (15000 грн.);

$Н_а$ – річна норма амортизації на ПЕОМ, частки одиниці (0,3);

$К_{лпз}$ – вартість ліцензійного програмного забезпечення (ОС Microsoft Windows 11 – 5800 грн., Microsoft Office 365 – 8300 грн.);

$Н_{апз}$– річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці (0,3);

$F_р$– річний фонд робочого часу (2080 годин).

Отже, 1 година машинного часу ПЕОМ вартує:

$$С_{мч} = 0{,}6 \cdot 1{,}44 + \frac{15000 \cdot 0{,}3}{2080} + \frac{(5800+8300) \cdot 0{,}3}{2080} = 5.06 \text{ , грн./година.}$$

$$З_{мч} = 120 \cdot 5.06 = 607.20 \text{ , грн.}$$

$$К_м = 10800 + 607.20 = 11407.20 \text{ , грн.}$$

Таким чином, після всіх проведених розрахунків, загальні витрати на розробку моделі системи підтримки прийняття рішень оцінки загроз інформаційній безпеці для компаній, що реалізують послуги аутсорсингу, складають 11407.20 гривень.

3.3. Розрахунок експлуатаційних витрат

До експлуатаційних витрат віднесено:

− річну заробітну плату співробітника, що проводить оцінку загроз інформаційній безпеці, за допомогою створеної моделі ;

– відрахування на соціальні заходи від річної заробітної плати співробітника, що проводить оцінку загроз інформаційній безпеці, за допомогою створеної моделі;

– витрати машинного часу.

3.3.1 Річна заробітна плата співробітника, що проводить оцінку загроз інформаційній безпеці, за допомогою створеної моделі

Годинна заробітна плата становить:

Зпрс= 135 грн./год.

Для підрахунку заробітної плати працівника, що проводить оцінку загроз інформаційній безпеці, за допомогою створеної моделі, використовується формула 3.6:

$$Ззпс = t * Зпрс, грн., \quad (3.6)$$

де t – загальна тривалість роботи працівника за рік, годин.

Середня тривалість одного сеансу роботи з моделлю становить 4 години, з періодичністю 1 раз на місяць. Тобто за рік t = 12 * 4 = 48 години.

Витрати на оплату заробітної плати за рік:

Ззпс = 48 * 135 = 6480, грн.

3.3.2 Відрахування на соціальні заходи від річної заробітної плати співробітника, що проводить оцінку загроз інформаційній безпеці, за допомогою створеної моделі

Відрахування на соціальні заходи від річної заробітної плати співробітника, що проводить оцінку загроз інформаційній безпеці, за допомогою створеної моделі, розраховують за формулою 3.7:

$$Зєсв= 22\% * Ззпс , грн. \quad (3.7)$$

Що, з урахуванням 48 годин робочого часу в рік, складуть:

Зєсв= 0,22 * 1680 = 1425.60 , грн.

3.3.3 Витрати машинного часу

Година машинного часу була розрахована раніше та становить:

$$С_{мч} = 0,6 \cdot 1,44 + \frac{15000 \cdot 0,3}{2080} + \frac{(5800+8300) \cdot 0,3}{2080} = 5.06 \text{ , грн./година.}$$

Тобто, за рік роботи з моделлю потрібно витратити, розрахувавши за формулою 3.8:

$$Вмч = t * Смч \text{ , грн.} \quad (3.8)$$

Що становитиме:

$$Вмч = 48 * 5.06 = 242,88 \text{ , грн.}$$

3.3.4 Загальні витрати на експлуатацію

Загальні витрати на експлуатацію розраховуються за формулою 3.9:

$$Векп = Ззпс + Зєсв + Вмч \text{ , грн.} \quad (3.9)$$

$$Векп = 6480 + 1425,60 + 242,88 = 8148,48 \text{ , грн.}$$

3.4 Визначення збитку від поломок обладнання

Запобігти поломкам обладнання практично не можливо. Природно, первинна передумова наступна: витрати на ремонт або заміну деяких деталей обладнання не повинні перевищувати вартість самого обладнання.

Вихідні дані для підрахунку збитку:

- час простою внаслідок поломки, $t_п$ (в годинах), $t_п = 3$ год;
- час відновлення після поломки, $t_в$ (в годинах), $t_в = 2$ год;
- час повторного введення втраченої інформації, $t_{ви}$ (в годинах), $t_{ви} = 1$ год;
- заробітна плата обслуговуючого персоналу, Z_0 (грн. в місяць з податками), $Z_0 = 14500$ грн.;
- заробітна плата співробітників, Z_c (грн. в місяць з податками), $Z_c = 15000$ грн.;
- кількість обслуговуючого персоналу, N_0, $N_0 = 2$;
- число співробітників, N_c, $N_c = 35$;

– прибуток , О (грн. на рік), О = 42000000 грн.;

– вартість заміни обладнання та запасних частин, виправлення помилок в роботі системи, $П_{зч}$ (грн.), $П_{зч}$ = 0 грн;

– число зламаного обладнання, I, I = 1;

– число поломок на рік, n, n = 7.

Вартість втрат від зниження продуктивності співробітників несправного обладнання розраховується за формулою 3.10:

$$П_п = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_п, \text{ грн.}, \quad (3.10)$$

де місячний фонд робочого часу при 40-а годинний робочий тиждень 176 годин.

Підставивши вихідні дані отримаємо:

$П_п$ = (35*15000/160)*3 = 9843.75 , грн.

Вартість відновлення зламаного обладнання розраховується за формулою 3.11:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.} \quad (3.11)$$

де $П_{ВИ}$ – вартість повторного введення інформації(формула 3.12),

$П_{ПВ}$ – вартість відновлення обладнання(формула 3.13).

$$П_{ви} = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_{ви}, \text{ грн.} \quad (3.12)$$

$$П_{пв} = \frac{\sum Z_o}{\frac{N_o}{160}} \cdot t_в, \text{ грн.} \quad (3.13)$$

Отримаємо:

$П_{ВИ}$ = (35*15000/160)*1 = 3281.25 , грн.

$П_{ПВ}$ = (2*14500/160)*2 = 365.50 , грн.

Вартість заміни обладнання та запасних частин, виправлення помилок в системі, $П_{зч}$ (грн.)

$$П_{зч} = 0 \text{ грн.}$$

Підставивши отримані результати в загальну формулу отримаємо:

$$П_в = 3281.25 + 365.50 + 0 = 3643.75, \text{ грн.}$$

Втрачена вигода від простою зламаного обладнання становить та розраховується за формулою 3.14 й 3.15 відповідно:

$$U = П_п + П_в + V, \text{ грн.} \quad (3.14)$$

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви}), \text{ грн,} \quad (3.15)$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить 2080 годин.

$$V = (42000000/2080)*(3+2+1) = 121153{,}85 \text{ , грн.}$$

$$U = 9843.75 + 3648.75 + 121153.85 = 134646.35, \text{ грн.}$$

Таким чином, загальний збиток від поломки обладнання, повторного введення інформації в системі, виявлення та усунення помилок в системі складе (формула 3.16):

$$ОУ = \sum_n \sum_I U, \text{ грн.} \quad (3.16)$$

$$ОУ = 7 * 1 * 134646.35 = 942524.45, \text{ грн.}$$

3.5 Загальний ефект від впровадження моделі

Загальний ефект від впровадження моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компаній, що реалізують послуги аутсорсингу, визначається за формулою 3.17 з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = ОУ \cdot R - C, \text{ грн,} \quad (3.17)$$

де ОУ– загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

С – щорічні витрати на експлуатацію моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компаній, що реалізують послуги аутсорсингу, грн.

Таким чином, загальний ефект від впровадження становить:

$$E = 942524.45 * 0,4 – 8148,48 = 380861.30, \text{ грн.}$$

3.6 Визначення та аналіз показників економічної ефективності моделі

Оцінка економічної ефективності моделі, розглянутої у спеціальній частині роботи, здійснюється на основі визначення та аналізу коефіцієнта повернення інвестицій ROSI (Return on Investment for Security) за формулою 3.18 та терміну окупності капітальних інвестицій T_o за формулою 3.19.

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \quad (3.18)$$

де Е – загальний ефект від впровадження системи захисту, грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Підставивши відповідні значення, маємо:

$$ROSI = 380861.30 / 11407.20 = 33.4$$

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань).

Проєкт визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта формула 3.20:

$$ROSI > (N_{деп} – N_{інф})/100) \quad (3.20)$$

де $N_{деп}$ – річна депозитна ставка, (18% - Юнекс Банк, Укрбудінвестбанк, Банк Кредит Дніпро);

$N_{інф}$ – річний рівень інфляції, (3% - період січень-березень 2023).

Підставивши відповідні значення, маємо:

$$ROSI > (18 - 3)/100),$$

$$33,4 > 0,15.$$

Отже, проєкт є економічно доцільним.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років.} \quad (3.19)$$

Підставимо значення:

$$T_o = 1 / 33,4 = 0,03 \text{ року.}$$

3.7 Висновок

Розрахувавши збитки від реалізації можливих несправностей, які склали 942524.45 грн., і порівнявши їх з витратами на забезпечення підтримки працездатності системи 8148,48 грн., та витратами на розробку моделі 11407.20 грн., можна зробити висновок, що витрати на забезпечення інформаційної безпеки є не значними у співвідношенні до збитків, впровадження системи є економічно доцільним заходом (ROSI = 33,4), термін окупності системи безпеки становить 0,03 року. Та для подальшого розвитку діяльності підприємства впровадження даних заходів є необхідною умовою для виконання.

ВИСНОВКИ

В роботі було проведене дослідження специфіки роботи компаній-аутсорсерів, розроблена узагальнена модель загроз інформаційній безпеці такого підприємства та розроблена модель системи підтримки прийняття рішень оцінки загроз інформаційній безпеці для компаній, що реалізують послуги аутсорсингу.

У розділі «СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ» опрацьовувався теоретичний матеріал про ринок B2B, особливості роботи компаній-аутсорсерів, методи розробки систем підтримки прийняття рішень, загальну модель загроз та схема системи підтримки прийняття рішень.

У розділі «СПЕЦІАЛЬНА ЧАСТИНА» розроблялась модель системи підтримки прийняття рішень оцінки загроз інформаційній безпеці для компаній, що реалізують послуги аутсорсингу та рекомендації по її використанню. А також проводився аналіз підприємства, його інформації та проходила класифікація та категоріювання отриманої інформації. Для проведення тестування розробленої моделі підтримки прийняття рішень оцінки загроз був створений «Лист-опитування», який був заповнений головним інженером служби захисту підприємства та на основі відповідей була створена модель загроз.

У частині «ЕКОНОМІЧНИЙ РОЗДІЛ» робота проводилась з ціллю економічного обґрунтування створеної моделі. Було проведено визначення капітальних витратна створення моделі, розрахунок експлуатаційних витрат, визначення збитку від поломок обладнання, також визначення загального ефекту від впровадження моделі та аналіз економічних показників.

Розрахувавши збитки від реалізації можливих несправностей, які склали 942524.45 грн., і порівнявши їх з витратами на забезпечення підтримки працездатності системи 8148,48 грн., та витратами на розробку моделі 11407.20 грн., можна зробити висновок, що витрати на забезпечення інформаційної безпеки є не значними у співвідношенні до збитків, впровадження системи є

економічно доцільним заходом (ROSI = 33,4), термін окупності системи безпеки становить 0,03 року. Та для подальшого розвитку діяльності підприємства впровадження даних заходів є необхідною умовою для виконання.

ПЕРЕЛІК ПОСИЛАНЬ

1 Термін B2B (Електронний ресурс)/ Спосіб доступу: URL:http://www.marketingnews.com/termin/108/. – Заголовок з екрана.

2 Аутсорсер (Електронний ресурс)/ Спосіб доступу: URL:http://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D1%81%D0%BE%D1%80%D1%81%D0%B5%D1%80 – Заголовок з екрана.

3 Менеджмент корпорацій (Електронний ресурс)/ Спосіб доступу: URL:http://www.cfin.com/management/strategy/change/outsourcing.shtml?printversion – Заголовок з екрана.

4 Питання інформаційної безпеки при використанні аутсорсингу (Електронний ресурс)/ Спосіб доступу: URL:http://www.nestor.minsk.com/sr/2007/08/sr70812.html 80 – Заголовок з екрана.

5 Астахов О.М. Мистецтво управляти інформаційними ризиками. – Львів., 2010, - 312 с., ил

6 Аналіз загроз інформаційній безпеці (Електронний ресурс)/ Спосіб доступу: URL:http://www.arinteg.com/articles/analiz-ugroz-informatsionnoy-bezopasnosti-27291.html – Заголовок з екрана.

7 Системи підтримки прийняття рішень (Електронний ресурс)/ Спосіб доступу: URL:http://ua.textreferat.com/referat-7752-2.html – Заголовок з екрана.

8 Програмне забезпечення «1С» (Електронний ресурс).

9 БЕСТ ЗВІТ ПЛЮС (Електронний ресурс)/ Спосіб доступу: URL: http://www.bestzvit.com.ua//– Заголовок з екрана.

10 ЛІГА:ЗАКОН (Електронний ресурс)/ Спосіб доступу: URL: http://www.ligazakon.ua/– Заголовок з екрана.

11 M.E.Doc (Електронний ресурс)/ Спосіб доступу: URL: http://www.me-doc.com.ua/– Заголовок з екрана.

12 НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

13 ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

14 ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Основні положення.

15 Закон України «Про інформацію».

16 НД ТЗІ 3.1-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроєктні роботи.

17 НД ТЗІ 1.6-005-2013. Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

18 Закон України «Про захист інформації в інформаційно-комунікаційних системах».

19 НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

20 НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

21 Закон України «Про захист персональних даних».

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	31	
6	А4	2 Розділ	18	
7	А4	3 Розділ	9	
8	А4	Висновки	2	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
Розробка моделей оцінки загроз інформаційній безпеці для аутсорсингової компанії
студента групи 125-19-1
Багацького Даніїла Сергійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 75 сторінках та містить 8 рисунків, 8 таблиць, 21 джерел та 4 додатка.

Об'єкт розробки: система оцінки загроз інформаційній безпеці компаній, що надають послуги аутсорсингу.

Мета роботи: створення моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці з урахуванням особливостей роботи та проблем в забезпеченні інформаційної безпеки компаній, що надають послуги аутсорсингу.

У роботі наведено:

- оцінка особливостей роботи компаній у сфері аутсорсингу, виявлення проблем інформаційної безпеки та загроз;
- аналіз існуючих методів оцінки загроз, обрання оптимального варіанту;
- створення моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці;
- розробка рекомендацій по впровадженню та використанню створеної моделі.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник